HSSEDI
Homeland Security Systems Engineering & Development Institute

Prepared for:
Department of Homeland Security

Enhanced Cyber Threat Model for Financial Services Sector (FSS) Institutions

Threat Model ATT&CK/CAPEC Version

June 28, 2018

Authors:

David B. Fox
Eric I. Arnoth
Clement W. Skorupka
Catherine D. McCollum
Deborah J. Bodeau

The Homeland Security Systems Engineering and Development Institute (HSSEDI)™
Operated by The MITRE Corporation

Approved for Public Release; Distribution Unlimited.
Case Number 18-1725/ DHS reference number 16-J-00184-10

This document is a product of the Homeland Security Systems Engineering and Development Institute (HSSEDI™).

HSSEDI
Homeland Security Systems Engineering & Development Institute

Homeland Security Systems Engineering & Development Institute

The Homeland Security Act of 2002 (Section 305 of PL 107-296, as codified in 6 U.S.C. 185), herein referred to as the "Act," authorizes the Secretary of the Department of Homeland Security (DHS), acting through the Under Secretary for Science and Technology, to establish one or more federally funded research and development centers (FFRDCs) to provide independent analysis of homeland security issues. MITRE Corp. operates the Homeland Security Systems Engineering and Development Institute (HSSEDI) as an FFRDC for DHS under contract HSHQDC-14-D-00006.

The HSSEDI FFRDC provides the government with the necessary systems engineering and development expertise to conduct complex acquisition planning and development; concept exploration, experimentation and evaluation; information technology, communications and cyber security processes, standards, methodologies and protocols; systems architecture and integration; quality and performance review, best practices and performance measures and metrics; and, independent test and evaluation activities. The HSSEDI FFRDC also works with and supports other federal, state, local, tribal, public and private sector organizations that make up the homeland security enterprise. The HSSEDI FFRDC's research is undertaken by mutual consent with DHS and is organized as a set of discrete tasks. This report presents the results of research and analysis conducted under:

HSHQDC-16-J-00184
Next Generation Cyber Infrastructure (NGCI) Apex Cyber Risk Metrics and Threat Model Assessment

This HSSEDI task order is to enable DHS Science and Technology Directorate (S&T) to facilitate improvement of cybersecurity within the Financial Services Sector (FSS). To support NGCI Apex use cases and provide a common frame of reference for community interaction to supplement institution-specific threat models, HSSEDI developed an integrated suite of threat models identifying attacker methods from the level of a single FSS institution up to FSS systems of systems, and a corresponding cyber wargaming framework linking technical and business views. HSSEDI assessed risk metrics and risk assessment frameworks, provided recommendations toward development of scalable cybersecurity risk metrics to meet the needs of the NGCI Apex program, and developed representations depicting the interdependencies and data flows within the FSS.

The results presented in this report do not necessarily reflect official DHS opinion or policy.

For more information about this publication contact:

Homeland Security Systems Engineering & Development Institute

The MITRE Corporation
7515 Colshire Drive
McLean, VA 22102

Email: HSSEDI_info@mitre.org

http://www.mitre.org/HSSEDI

Abstract

The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) Next Generation Cyber Infrastructure (NGCI) Apex program is seeking to integrate innovative cyber technologies into use in the Financial Services Sector (FSS). As part of the NGCI Apex program, The Homeland Security Systems Engineering and Development Institute (HSSEDI) is developing a cyber threat model for FSS institutions. The NGCI Apex program will use threat modeling and cyber wargaming to inform the development and evaluation of risk metrics, technology foraging, and the evaluation of how identified technologies could decrease risks. The threat model is intended both to support NGCI Apex use cases and to provide a common, consistent frame of reference for community interaction, supplementing institution-specific threat models maintained internally within individual institutions. HSSEDI previously developed and populated a high-level framework and high-level threat model tailored to the FSS. In this report, the high-level model is expanded into a more detailed threat model, reflecting attacker methods at a level relevant to implementation with respect to a generic FSS institution. Attacker methods are drawn from MITRE and cyber defense community sources including Adversary Tactics Techniques and Common Knowledge (ATT&CK), ATT&CK for Left of Exploit (PRE-ATT&CK), and Common Attack Pattern Enumeration and Classification (CAPEC).

Key Words

1. Cyber Threat Models
2. Next Generation Cyber Infrastructure
3. Cybersecurity
4. Cyber Threat Events
5. Cyber Attack Scenarios

This page intentionally left blank

Table of Contents

1 Introduction 1
1.1 Purpose 2
1.2 Scope 2
1.3 Audience 3
1.4 Organization of Report 3
2 Background 4
2.1 Threat Model Assessment 4
2.2 Goal of Expanded Threat Model 5
2.3 Assumptions 7
2.3.1 Information Technology Environment 7
2.3.2 Risk Factors 7
3 Approach 9
3.1 Threat Modeling Framework 9
3.2 High-Level Threat Model 9
3.2.1 Adversary Characteristics 10
3.2.2 Cyber Attack Vectors 10
3.2.3 Threat Events 11
3.3 Sources 11
3.3.1 ATT&CK for Enterprise 12
3.3.2 ATT&CK Mobile Profile 12
3.3.3 PRE-ATT&CK 13
3.3.4 CAPEC 13
4 Expanded Threat Model 15
4.1 Threat Characteristics 15
4.2 Threat Events 15
4.3 Scenarios 15
4.3.1 Generic Scenarios 15
4.3.2 Real-World Examples 18
4.3.2.1 Real-World Cyber Attack Scenario: Carbanak 19
4.3.2.2 Real-World Cyber Attack Scenario: Buhtrap 20
5 Discussion 22
5.1 Integration of Models 22
5.2 FSS Relevance 22

6 Support for Example Use Cases 24
6.1 Technology Foraging 24
6.2 Test Case Development for Technology Validation 26
6.3 Cyber Wargaming Scenario Development 27
7 Conclusion 28
Appendix A Expanded Threat Model 29
Appendix B External Threat Events 96
Appendix C Scenario Building Blocks 99
List of Acronyms 107
List of References 110

List of Figures

Figure 1. Cyber Threat Modeling Frameworks and Methods 4
Figure 2. Three Levels of Cyber Threat Modeling 5
Figure 3. Key Constructs in Cyber Threat Modeling 9
Figure 4. Relationships Between Adversary Characteristics and Threat Events 10
Figure 5. Notional Example of Elements of a Detailed Threat Scenario 18
Figure 6. The Cyber Defense Matrix 25
Figure 7. Notional Example of a Coverage Map 26

List of Tables

Table 1. Assumed Risk Factors 8
Table 2. Characterizing Generic Threat Scenarios 17
Table 3. Carbanak Banking Cyber Attack Campaign 19
Table 4. Buhtrap Banking Cyber Attack Campaign 20
Table 5. Example of Value Scale for Assessing Coverage of a Detailed Threat Event 25
Table 6. Expanded Threat Model Events 29
Table 7. External Threat Events 96
Table 8. Scenario Building Blocks Using Threat Events 99

1 Introduction

A cyber threat model captures information about potential means of cyber attack on an enterprise's operations, through its computer systems and networks, that it must be prepared to withstand or defend against. This information includes the characteristics of potential adversaries and specific techniques or events that might be used as part of a cyber attack. Cyber threat models are needed for different kinds of tasks, such as:

- Developing secure software components and systems
- Assessing what cybersecurity technologies and processes are needed in a particular systems environment
- Creating scenarios for security testing or cyber wargaming
- Developing a playbook for how to respond in different attack situations to defend an organization's systems and operations
- Anticipating, identifying, and responding to attacks during live operation of systems
- Informing organizational risk management and metrics

The level of detail needed in a cyber threat model depends on its intended use. For strategic planning, a model that limits the detail to high-level classes of adversaries and attacks is sufficient. For live operations, the greatest available level of detail that is known about specific adversary groups and attack methods is essential, to allow defenders to detect attacks and respond to counter them and eliminate their incursions. An intermediate level of detail, identifying adversary tactics, techniques, and procedures (TTPs), enables test scenarios and cyber wargames to be developed.

These tasks are not, however, independent. The high-level threat model on which an organization bases its strategic planning and risk management should be representative of and consistent with the detailed threat models describing the kinds of attacks it expects it may encounter in live operations. A coherent suite of threat models at differing levels of detail can help avoid gaps in the understanding of adversaries and attacks, enabling the organization to be prepared for current and evolving cybersecurity challenges it is likely to face.

The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) Next Generation Cyber Infrastructure (NGCI) Apex Program is seeking to accelerate the adoption of innovative and effective cybersecurity technologies in the Financial Services Sector (FSS). As part of that effort, it is developing a cyber threat model applicable to the FSS that can provide a consistent frame of reference complementary to the threat models maintained internally by individual FSS institutions.

A previous report, [Bodeau 2018], provided a threat model geared toward high-level tasks such as strategic planning or development of scenarios for a tabletop cyber exercise. That model describes attackers and attack events in essential terms, with the details abstracted away. This report draws upon several cybersecurity community attack information repositories to provide an expanded version of that initial cyber threat model, at a moderate level of detail. The expanded cyber threat model documents potential attack events at a level understandable to both strategic

and implementation-level staff, without diving into the kind of implementation detail needed for cybersecurity development and cyber defense operations.

1.1 Purpose

This report provides a new, expanded version of the cyber threat model framework previously developed for FSS institutions, populated in further detail. The expanded threat model describes concrete building blocks that adversaries use in conducting cyber attacks. These building blocks are drawn from entries in community cyber attack information repositories.

The expanded threat model provides threat information needed to enable NGCI Apex use cases including the following:

- Cybersecurity technology foraging
- Cybersecurity test case development for technology validation
- Cyber wargaming scenario development

The expanded threat model is also meant to have broader value for the FSS. First, it may be helpful to FSS institutions in their internal threat modeling and risk management activities, particularly in cybersecurity requirements development and gap analysis. In addition, it offers a common, consistent frame of reference for discussion of cybersecurity threats among FSS institutions across the sector.

1.2 Scope

The focus of this expanded threat model is on information technology (IT) environments of enterprises within the FSS, and some of the discussion is tailored to FSS resources and impact. However, it is applicable more broadly. It could be applied to other critical infrastructures, with appropriate extension for infrastructure-specific aspects such as unique cyber-physical elements, or to information technology environments of large government and private sector enterprises in general.

In the context of the FSS, the expanded threat model presented in this report captures adversary characteristics and potential threat events from the perspective of a single FSS institution, on a generical basis. An illustration of the tailoring and use of the threat model for a specific hypothetical FSS enterprise is provided in [Fox 2018].

While the expanded threat model includes threats due to an institution's interfaces with external parties such as other FSS institutions, it does not consider threats in relation to multiple cooperating institutions or systemic sector functions. In a companion report [Bodeau 2018b], the threat context is explored from a system-of-systems perspective and system-of-systems-oriented additions to the threat model are identified.

The threat model is limited to potential cyber threats from cyber adversaries to IT infrastructure. Out of scope are:

- Threats unique to cyber-physical systems, or threats due to dependencies on non-IT infrastructure
- Cybersecurity technologies and mitigations to counter, eliminate, or reduce the risk of threats

- Threats due to fraudulent activities or attempts, rather than cyber attack

1.3 Audience

While this report may be of interest more broadly, its primary audience includes the Department of Homeland Security (DHS) and members of the FSS. Within FSS institutions, it is most relevant to the office of the chief information security officer (CISO), risk management personnel, and technical staff engaged in cybersecurity engineering and operations.

The report is written with the assumption that readers have at least moderate familiarity with cybersecurity concepts and terminology.

1.4 Organization of Report

The remainder of this report is organized as follows:

- Section 2 provides background on the previous assessment of threat models and the goals and assumptions of the expanded threat model
- Section 3 explains the approach taken in creating the expanded threat model, including the high-level model on which it is based and the sources from which detailed events are drawn
- Section 4 describes the expanded threat model, discusses how it can be used in scenarios, and presents two examples real-world cyber attack scenarios mapped to the model
- Section 0 discusses some of the challenges encountered in integrating threat events from the sources used and limitations of the expanded threat model
- Section 6 covers how the expanded threat model can be used to support tech foraging, test case development, and wargame scenario development
- Section 7 concludes the document
- More detailed information is provided in the following appendices:
  - Appendix A: the detailed threat events of the expanded threat model
  - Appendix B: threat events that occur outside the IT system, such as intelligence-gathering and weaponizing prior to an attack
  - Appendix C: scenario building blocks

2 Background

This section provides brief background on the previous threat model analysis the Homeland Security Systems Engineering and Development Institute (HSSEDI) conducted for the NGCI Apex program, the goals of the expanded threat model in this report, and assumptions made in developing the expanded threat model.

2.1 Threat Model Assessment

In previous work, HSSEDI conducted a survey of cyber threat models and threat modeling frameworks relevant to the goals and use cases of the NGCI Apex Program. This survey included a literature survey of 21 threat models and frameworks that are in broad use for managing cybersecurity, as well as interviews with executives at 11 large FSS institutions who are responsible for cyber threat modeling, risk assessment, and mitigation. Figure 1 illustrates the range of models and frameworks surveyed.[1]

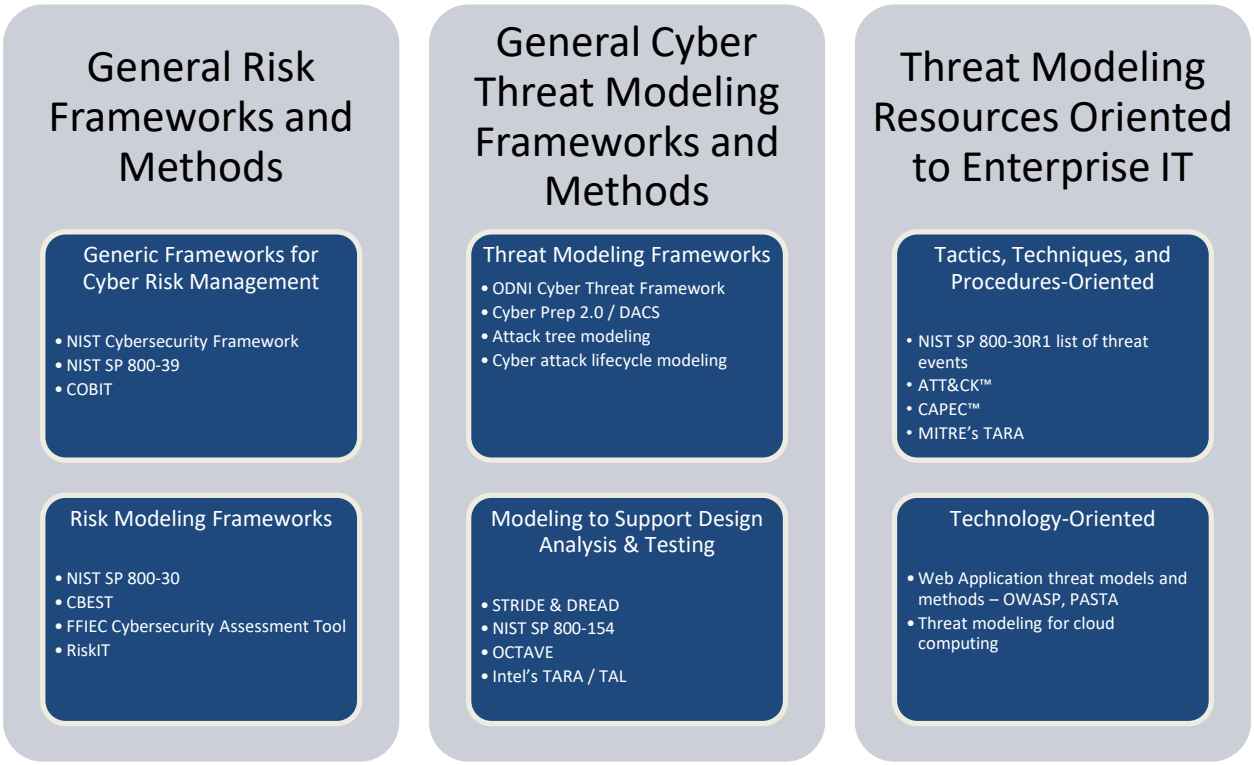

Figure 1. Cyber Threat Modeling Frameworks and Methods

[1] Models surveyed include NIST SP 800-30R1 [NIST 2012], NIST SP 800-39 [NIST 2011], and the NIST Cybersecurity Framework [NIST 2014] [NIST 2017]; COBIT [ISACA 2012] and RiskIT [ISACA 2009]; CBEST [Bank of England 2016] and the FFIEC Cybersecurity Assessment Tool [FFIEC 2016]; the ODNI Cyber Threat Framework [ODNI 2017]; Cyber Prep 2.0 [Bodeau 2016] and the DACS Framework [Bodeau 2014]; Microsoft's STRIDE and DREAD methodologies [Microsoft 2005]; SEI's OCTAVE [Cebula 2014]; Intel's TARA [Intel 2009] [Intel 2015] and Threat Agent Library [Intel 2007]; ATT&CK [MITRE 2015], CAPEC [MITRE 2016], and MITRE's TARA [Wynn]; and the OWASP threat model [OWASP 2016]. For more information on these and others, see [Bodeau 2018].

HSSEDI defined criteria to assess the characteristics of the various threat models and their suitability for NGCI Apex. The analysis found that the models clustered into groups best suited for either strategic planning, engineering and acquisition, or operations. There was no one model, nor a cohesive suite of models, well suited for use at these three different levels of detail.

HSSEDI determined that there would be value in a coordinated suite of threat models to enable clear and consistent communication and to minimize gaps, both within and among FSS institutions or other enterprises. HSSEDI therefore laid out a framework within which such a coherent suite of threat models can be defined and populated, drawing upon extensive cyber attack information resources maintained and shared within the cybersecurity community. This is illustrated in Figure 2.

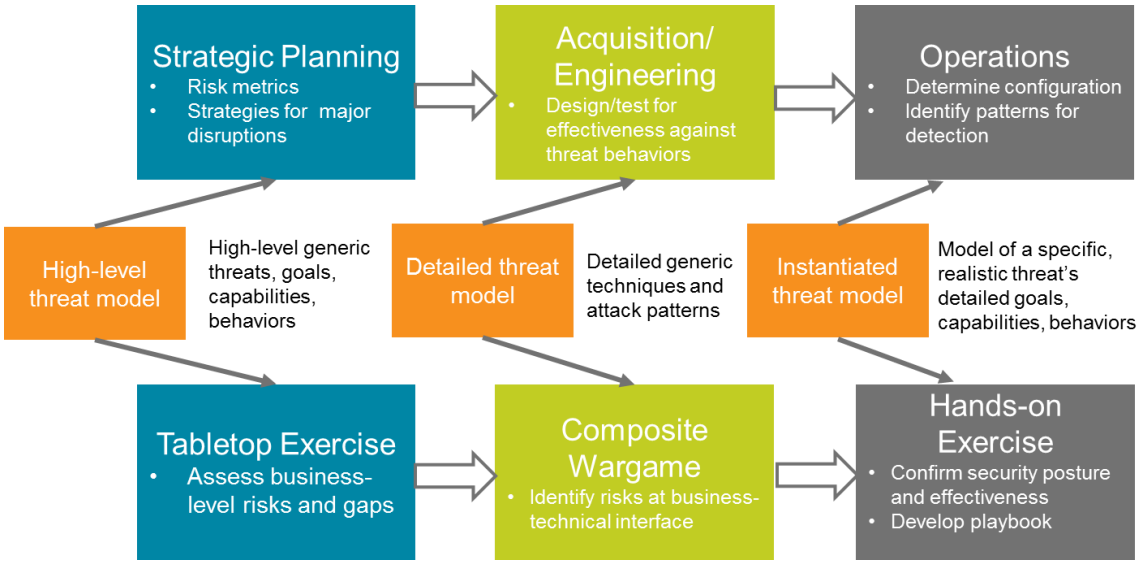

Figure 2. Three Levels of Cyber Threat Modeling

An initial, populated high-level threat model was provided as part of the report [Bodeau 2018]. This populated threat model corresponds to the strategic planning level of abstraction and serves as the top tier of a coordinated suite of threat models. The expanded threat model provided in this report serves as the middle tier, corresponding to the engineering and acquisition level of abstraction. It is populated with more detailed threat events that can be used to carry out each of the high-level threat events in the top tier.

2.2 Goal of Expanded Threat Model

The primary goal of the expanded threat model is to provide information to enable those who are developing threat models for one or more of the NGCI Apex use cases to base them on realistic information about adversary behaviors and types of attacks. This is done by providing amplifying detail on methods by which adversaries might accomplish each of the threat events in the high level threat model.

The focus is on cyber attack activities that can be prevented or mitigated by cyber technologies or cybersecurity posture within the defended system IT environment. Thus, the expanded threat model emphasizes threat events that touch or interact with the IT system in some way. For

instance, if a threat event occurs on an internal system component, or is executed from outside the system but communicates with it to scan or probe the system, or takes place at an external network location but is able to observe network traffic originating from the IT system, it is touching or interacting with either the IT system or its communications.

Examples such as these are in contrast to adversary activities that, while they undeniably contribute to preparation or execution of a cyber attack, do not directly involve the defended IT system. For example, gathering information from people's resumes on an industry recruitment site can help an adversary learn about an organization, its processes, and its staff in order to determine where and how to target a cyber attack to bring about the desired business impact. Social engineering of employees can allow an adversary to steal credentials that can be used to gain illicit access to a system. But both of these example activities take place entirely outside the defended IT system.

For completeness of the high-level overview in [Bodeau 2018], the high-level threat model included both types of threat events. In the expanded threat model in this report, to avoid providing excessive detail on threat events not directly applicable to NGCI use cases, the main discussion is limited to threat events that interact with the defended IT system environment. Some information is provided in Appendix B on threat events that occur entirely outside the system.

A further goal for the expanded threat model is that the information be grounded in cybersecurity community knowledge of real-world attacks and tactics, techniques, and procedures used by adversaries. This is ensured by drawing from community models and repositories of cyber attack methods. These include Attack Tactics, Techniques, and Common Knowledge™ (ATT&CK™) [MITRE 2015], ATT&CK for Left of Exploit (PRE-ATT&CK) [MITRE 2016b], and Common Attack Pattern Enumeration and Classification™ (CAPEC™) [MITRE 2016].

The expanded threat model seeks to provide threat information at a deep enough level of detail to represent the range of technical approaches available to adversaries to achieve a high-level event without including excessive detail that would be system implementation-specific.

Finally, the expanded threat model seeks to cover not just the threat events that try to break into and exploit a system via a network interface, but also other modes such as denial of service, threat events achieved through the IT system supply chain, or threat events carried out by insiders with legitimate access to the IT system environment.

It is important to recognize, however, that in today's cybersecurity environment, no threat model is static. Adversary capabilities, cyber attack methods, and toolsets are continually evolving, and threat models must evolve with them. The expanded threat model herein draws from well-established community repositories of threat information, and describes cyber attack methods in terms general enough to transcend frequently changing, transient details. However, these repositories themselves will necessarily continue changing as new adversary behaviors are discovered.

This expanded threat model thus should be regarded as a snapshot of attack methods known at this time. An organization wishing to make use of it at some future date should review the source repositories for cyber attack methods that have been added subsequently and need to be considered.

2.3 Assumptions

The expanded threat model in this document assumes that the defended system is the networked IT system of a single enterprise, generically representative of FSS institutions in its business and technical environments.

2.3.1 Information Technology Environment

The more detailed a threat model is, the more the threat events it includes are specific to a particular IT environment. While the high-level threat model provided in [Bodeau 2018] is largely generic with respect to the technology environment, the expanded threat model in this report deals with threat events closer to the implementation level. Thus, choices about which threat events to include necessarily rely on some broad assumptions about the IT environment.

The expanded threat model described in this report assumes that the generic FSS institution's IT environment includes a typical suite of platforms and software such as:

- Windows machines, Unix servers, and mainframe hosts
- Internet Protocol (IP) Networking
- Mobile networking
- Virtualization
- Web interfaces
- Data repositories
- Internet-facing services
- Business-to-business (B2B) / Business service interfaces

The threat model further assumes that computing takes place only in owned, dedicated facilities and that the generic FSS institution's IT environment does not include the use of external cloud services shared with other tenants. [2]

2.3.2 Risk Factors

In addition to assumptions about the technologies in use, the threat model makes assumptions about fundamental elements of the generic organization's risk posture. The organization is assumed to have appropriate state-of-practice cybersecurity technology components and policies. In terms of the Federal Financial Institutions Examination Council (FFIEC) Inherent Risk Profile [FFIEC 2016] [FFIEC 2017], the representative institution is assumed to have the profile shown in Table 1, with respect to the categories and factors identified.

[2] An initial survey of FSS institution architectures HSSEDI conducted in late 2015 as part of the NGCI Apex program did not indicate widespread use of external multi-tenant cloud services. Nevertheless, adoption may increase over time, and on-premises data center architectures make extensive use of virtualization for efficiency reasons. The expanded threat model therefore incorporates some threat information relevant to multi-tenant cloud computing and virtualization based on information published by the Cloud Security Alliance [Cloud Security Alliance 2017]. However, mature community-consensus cyber repositories of attack information for cloud computing and virtualization that would allow a full treatment of threats associated with cloud computing infrastructure and virtualization have yet to emerge.

Table 1. Assumed Risk Factors

Category	Factor	Risk Level
Technologies and Connection Types	Total number of internet service provider (ISP) connections (including branch connections)	At least Minimal
	Unsecured external connections, number of connections not users (e.g., file transfer protocol (FTP), Telnet, rlogin)	None
	Personal devices allowed to connect to the corporate network	At least Minimal
	Third parties, including number of organizations and number of individuals from vendors and subcontractors, with access to internal systems (e.g., virtual private network, modem, intranet, direct connection)	At least Minimal
	Wholesale customers with dedicated connections	At least Minimal
	Internally hosted and developed or modified vendor applications supporting critical activities	At least Minimal
	Internally hosted, vendor-developed applications supporting critical activities	At least Minimal
	User-developed technologies and user computing that support critical activities (includes Microsoft Excel spreadsheets and Access databases or other user-developed tools)	At least Minimal
	End-of-life (EOL) systems	No systems
	Open Source Software (OSS)	No OSS
	Network devices (e.g., servers, routers, and firewalls; include physical and virtual)	At least Minimal
	Third-party service providers storing and/or processing information that support critical activities (Do not have access to internal systems, but the institution relies on their services)	No third parties that support critical activities
	Cloud computing services hosted externally to support critical activities	No cloud providers
Delivery Channels	Online presence (customer)	At least Moderate
	Mobile presence	At least Moderate
	Automated Teller Machines (ATM) (Operation)	At least Minimal
	Issue debit or credit cards	At least Minimal
	Prepaid cards	No assumption
	Emerging payments technologies (e.g., digital wallets, mobile wallets)	No assumption
	Person-to-person payments (P2P)	No assumption
	Originating automated clearing house (ACH) payments	No assumption
	Originating wholesale payments (e.g., Clearing House Interbank Payments System [CHIPS])	No assumption
	Wire transfers	No assumption
	Merchant remote deposit capture (RDC)	No assumption
	Global remittances	No assumption
	Treasury services and clients	No assumption
	Trust services	No assumption
	Act as a correspondent bank (Interbank transfers)	No assumption
	Merchant acquirer (sponsor merchants or card processor activity into the payment system)	No assumption
	Host IT services for other organizations (either through joint systems or administrative support)	Do not provide IT services for other organizations
Organizational Characteristics	Privileged access (Administrators–network, database, applications, systems, etc.)	At least Minimal

3 Approach

The approach to developing the expanded threat model is to build on the threat modeling framework and high-level threat model presented in [Bodeau 2018]. Section 3.1 reviews the framework, and Section 3.2 summarizes the high-level threat model. The expanded threat model presented in this report extends the high-level threat model, drawing from well-established repositories of adversary TTPs and attack patterns. These repositories are described in Section 3.3.

3.1 Threat Modeling Framework

As illustrated in Figure 3, the high-level threat modeling framework identifies key constructs for threat modeling and relationships among them.

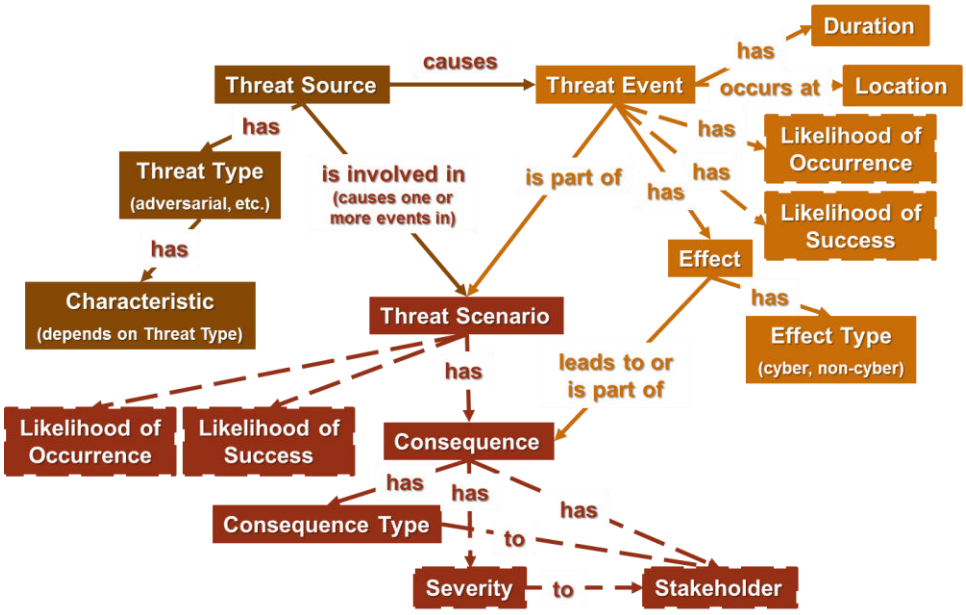

Figure 3. Key Constructs in Cyber Threat Modeling

The high-level threat modeling framework is based on the National Institute of Standards and Technology (NIST) 800-30R1 framework [NIST 2012], elaborated and fusing in material from other frameworks to meet the needs of NGCI Apex. It provides representative values for key constructs and relationships and describes how threat scenarios can be generated from the framework. (Details for adversarial threats are not shown.) Constructs and relationships in dotted lines are included to indicate linkages to risk modeling. While they are not part of the threat model presented in this report, these constructs are used in risk assessment, and relate to the system model or the asset model which is part of a detailed threat model.

3.2 High-Level Threat Model

The high-level threat model populates the framework for FSS institutions. It identifies adversary characteristics, attack vectors, and threat events.

3.2.1 Adversary Characteristics

The identification of adversary characteristics in the model enables different classes of threat actors to be defined and representative adversaries to be profiled for use in wargaming. An adversary profile describes the attacker's goals (and corresponding targets), timeframe, persistence, concern for stealth, and capabilities. As illustrated in Figure 4, these characteristics determine whether and how likely the attacker is to choose to cause a threat event or to target a given resource or location.[3]

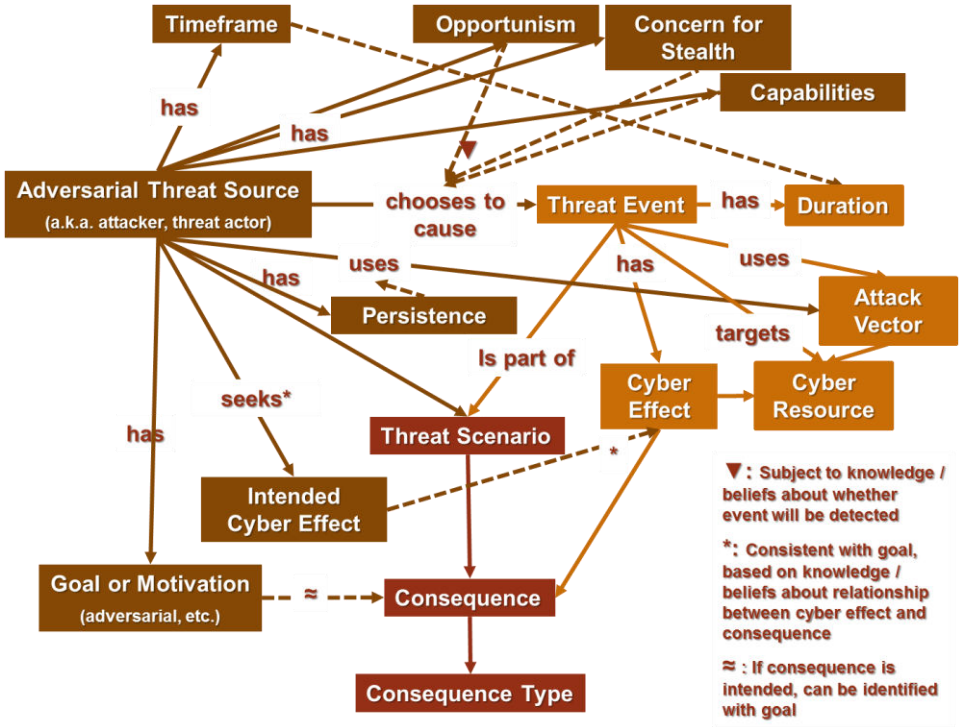

Figure 4. Relationships Between Adversary Characteristics and Threat Events

3.2.2 Cyber Attack Vectors

Cyber attack vectors may be thought of as the paths by which an adversary might mount an attack against the defended system. They include:

- Maintenance environments
- External network connections
- Trusted or partner network connections
- Internal networks
- Actions of non-privileged or privileged users
- Actions of individuals with physical access to enterprise facilities, device ports (e.g., removable media), and data.

[3] This figure updates Figure 17 of [Bodeau 2018].

Physical attack vectors, such as physical damage to a computing facility, and human attack vectors, such as pressuring an employee via relationships or personal vulnerabilities, are out of scope.

3.2.3 Threat Events

Threat events are the individual steps or behaviors that an adversary can use in conducting an attack. The high-level threat model includes a list of 66 adversarial threat events. Those events are drawn from NIST SP 800-30R1 [NIST 2012], with a few entries added to accommodate more recent work – in particular, the Cyber Threat Framework (CTF) promulgated by the Office of the Director of National Intelligence (ODNI) [ODNI 2017]. They are organized by stages in the cyber attack lifecycle (CAL) [NIST 2012].

Note that, to provide a full picture of how attacks may transpire, the high-level model includes some event types that take place entirely externally, with no interaction with the system or its communications, as well as event types that involve the system directly (i.e., occur within the system, interact with its interfaces, or interact with its communications, even if from a remote location.)

3.3 Sources

For each threat event from the high-level model, detailed threat events that an adversary could use to carry out the high-level event have been identified. These more detailed events are drawn from one or more public cybersecurity information repositories (except in cases where the high-level model's threat events, originating from NIST SP 800-30R1, are already sufficiently specific that no additional details from other models are needed.)

The expanded threat model draws from several well-established and complementary catalogs of attacker techniques and attack events[4], each of which focuses on a different segment of attacker activity:

- ATT&CK for Enterprise: post-exploit activities, after an attacker has gained access to a system [MITRE 2015]
- PRE-ATT&CK: pre-exploit activities, as an attacker prepares for an attack against a system [MITRE 2016b]
- ATT&CK Mobile Profile: attacker activities in relation to mobile devices [MITRE 2017]
- CAPEC: attacker activities conducted to gain access to a system [MITRE 2016]

Each of these catalogs is described briefly in the following sections.

The catalogs chosen as sources for threat events are well documented and represent community consensus. In the expanded threat model, they have been supplemented, in a few cases, with events that were not covered within their scope.

[4] As discussed in [Bodeau 2018], most publicly available threat modeling frameworks or models do not identify attack events. The OWASP handbook [OWASP 2016] does, but maps its threat events to CAPEC.

Additional models were considered, as they had aspects that appeared relevant, including the Common Weakness Enumeration (CWE)[5] and the Common Vulnerability Scoring System (CVSS)[6]. These, however, had a different focus, more on vulnerabilities than on threat behaviors. They were not found to contribute materially to the expanded threat model presented in this report.

The detailed entries in the expanded threat model focus on behaviors that can be detected by, or countered by, the organization's systems. Therefore, the expanded threat model excludes some categories of events specified in the high-level threat model that take place entirely outside and without interaction with the system or its communications. Details for some of these events, however, are available in one or more of the threat information sources (particularly PRE-ATT&CK) and are of value in other contexts, such as development of wargaming scenarios with a broad view incorporating human interactions that can be exploited. They are therefore provided in Appendix B.

3.3.1 ATT&CK for Enterprise

ATT&CK is a curated knowledge base for cyber adversary behavior, reflecting the various phases of an adversary's CAL and the platforms they are known to target. As such, ATT&CK content can be used as an input to the construction of threat models but is not in itself a threat model. ATT&CK for Enterprise is an advanced persistent threat (APT)-focused framework that describes the actions an adversary may take while operating within an enterprise network. ATT&CK focuses predominantly on post-delivery/post exploit activity typical of APT actors interested in cyber espionage and data exfiltration.

ATT&CK for Enterprise is organized as a set of categories known as tactics, which correspond to key activities attackers perform as they move through the cyber attack lifecycle, such as establishing persistence, escalating privileges, moving laterally, and exfiltrating data. Individual entries within each category (or tactic) describe specific techniques and behaviors employed by adversaries, based on analysis of actual APT incidents.

The level of detail is targeted for technical review or gap analysis of detection capabilities such as sensors and data analytics used in cybersecurity operations.

Though many of the techniques described in ATT&CK for Enterprise are relevant, its focus on APT actor activities excludes a number of common, high-risk threat behaviors such as denial of service attacks, data destruction, extortion, financial theft, and human-assisted or physical-layer attacks. Also, ATT&CK for Enterprise, with its focus on post-exploit phases of an APT cyber attack lifecycle, does not cover common delivery and exploit phase activity such as phishing or direct server attacks.

3.3.2 ATT&CK Mobile Profile

With user internet access and financial transactions becoming more common via mobile devices than traditional personal computers, attackers have developed techniques specific to mobile technology and protocols. At the same time, enterprises have incorporated mobile devices into

[5] https://cwe.mitre.org/

[6] https://www.first.org/cvss/

their enterprise architectures to enable their staff to work productively when not physically connected to the enterprise network.

Like ATT&CK for Enterprise, ATT&CK Mobile Profile [MITRE 2017b] is a curated knowledge base for cyber adversary behavior, but with a focus on attack techniques specific to mobile devices such as smartphones. ATT&CK Mobile Profile includes links to NIST's Mobile Threat Catalog.[7]

Unlike ATT&CK for Enterprise, ATT&CK Mobile Profile is not limited to post-exploit APT activity; it covers pre- and post-delivery aspects of attacker behavior and techniques. Because of the importance of app store distribution of software in the mobile ecosystem, ATT&CK Mobile Profile also includes some consideration of supply chain threat events, such as corruption of applications in app stores.

ATT&CK Mobile Profile is, however, relatively new compared to ATT&CK for Enterprise, so its content is somewhat less complete.

3.3.3 PRE-ATT&CK

PRE-ATT&CK builds on the ATT&CK framework and extends the identified threat tactics and techniques to pre-compromise activities that are largely outside of direct execution of cyber attacks against primary technology targets. These range from initial target information-gathering from non-target-related sources, such as social media, third party business partners, or employee behaviors, to compromise activity designed to gather technology information about deployed networks and systems.

Many of the defined tactics and techniques used by adversaries to launch a campaign correspond to the reconnaissance, weaponization, and delivery phases of attacks against technology deployments and are included in the PRE-ATT&CK catalog. PRE-ATT&CK lists ways that adversaries perform each tactic and provides an ability to track adversary patterns so that defenders can determine technical or policy-based mitigations. The resulting model supports defenders' ability to analyze their environment for signs that an adversary might be targeting it, be aware of commonly used techniques that could be used against it, and determine if cyber threat intelligence could be used to gain insights to "see" the adversary before an exploit occurs.

Elements of PRE-ATT&CK that are outside the system but enable preparation for target selection are included in Appendix B. This information includes areas adversaries may focus on to find information that helps them identify potential target components that could be vulnerable and weaknesses in operations. These are included here to provide insights into methods for data-gathering in the early stages of an adversary's preparation for an attack. They can used to help the defender understand where efforts can be made to limit external dissemination of relevant enterprise information.

3.3.4 CAPEC

The CAPEC repository [MITRE 2016] enumerates common attack patterns that have been observed in use, creating an organized catalog for meaningful and intuitive classification. It is

[7] https://pages.nist.gov/mobile-threat-catalogue/

intended to aid in secure software development practices and in penetration testing to evaluate the security of software.

The core component of CAPEC is an attack pattern. Attack patterns describe common methods for exploiting software, expressed from the attacker's perspective. In contrast to ATT&CK for Enterprise, whose main focus is on attacker behavior after a successful exploit, and PRE-ATT&CK, whose primary focus is on adversary activities in preparation for an attack on a system, CAPEC concentrates on methods of exploit that attackers may use to gain access into a system. Each attack pattern entry also provides guidance for mitigation, lists relevant environments, provides indicator descriptions, and gives examples. In the CAPEC repository, attack patterns are grouped into categories and meta-attack patterns. CAPEC elements also have links to the CWE repository[8] that catalogs the weaknesses and vulnerabilities that may be taken advantage of to successfully exploit a system.

In the expanded threat model, patterns devoted to external elicitation of information about the system have not been included.

[8] https://cwe.mitre.org/

4 Expanded Threat Model

This section describes the expanded threat model and discusses scenarios using the detailed threat events in the expanded model.

4.1 Threat Characteristics

The expanded threat model retains the general profiles of insiders, criminals, political or ideological activists, and nation-state-aligned professional criminal enterprises defined in the high-level model. These profiles are used in generic threat scenarios in Section 4.3.1. In addition to identifying the ultimate targets of threat actors, the generic threat scenarios identify intermediate targets of attack activities.

4.2 Threat Events

Due to the size of the expanded threat model, its threat events are provided in Appendix A rather than in this section. These events describe adversary actions or behaviors that can be used as part of an attack. Note that the term "event" is not meant in the sense typically used by cyber defense analysts, of potentially suspicious occurrences that, when assessed, might be determined to be security incidents requiring an investigation. Here, it instead refers to individual techniques or activities that attackers can use as part of a goal-oriented cyber attack.

In Appendix A, the threat events from the high-level threat model are expanded to their equivalents in the more detailed cyber attack information repositories.

4.3 Scenarios

This section characterizes a number of generic scenarios and explains how such a generic scenario would be populated with events from the expanded threat model. In addition, it provides two examples of past real-world cyber attack scenarios carried out against financial services institutions and shows how the steps taken by attackers correspond to events from the expanded threat model.

4.3.1 Generic Scenarios

The following small set of highly general threat scenarios[9] can serve as a starting point for development of more detailed, but still institution-independent, scenarios:

1. *Breach: An adversary obtains sensitive information from the institution's systems.* This scenario includes data breaches of personally identifiable information (PII), as well as large-scale exfiltration of proprietary information, trade secrets, or other highly sensitive information.
2. *Fraud: An adversary modifies or fabricates information on the institution's systems so that the institution will disburse money or transfer other assets at the adversary's direction.* This scenario focuses on fraudulent transactions resulting from cyber attack, and excludes fraud resulting from non-cyber methods.

[9] This list is adapted from [Bodeau 2016].

3. *Misuse: An adversary modifies or fabricates software or configuration data on the institution's systems so that the adversary can direct their use (typically to resell capacity, as with botnet farms or cryptocurrency mining).* This scenario focuses on usurpation of resources, which is typically highly surreptitious.
4. *Destruction: An adversary modifies or destroys institutional assets in order to prevent the institution from accomplishing its primary business functions.* This scenario includes adversary denial, disruption, or subversion of business operations.
5. *Friendly Fire: An adversary deceives business area managers or cyber defense staff into taking operationally-disruptive actions.* This scenario focuses on modification or fabrication of business or configuration data, as well as on modification or disruption of business functions.
6. *Upstream Attack: An adversary compromises a supplier or partner in order to increase the institution's vulnerability to attack.* This scenario includes attacks on partner institutions as well as those in the institution's supply chain.
7. *Reputation Damage: An adversary disrupts institutional operations or fabricates information the institution presents to its constituency, damaging its reputation and the trust of its constituency.* This scenario is closely related to those involving disruption or denial of mission functions, but also includes modification of inessential but externally visible information or services in ways that undermine confidence in the institution.
8. *Stepping-Stone Attack: An adversary compromises the institution's systems in order to attack downstream entities (e.g., customers, customers of customers).* Like the preceding scenario, this scenario is related to those involving disruption of mission functions. However, it is also related to scenarios involving acquisition of sensitive information, or fraudulent transactions.
9. *Extortion: An adversary modifies or incapacitates business assets for financial gain (e.g., ransomware, distributed denial-of-service (DDoS) attack).* This scenario is closely related to those involving modification for purposes of fraud and for disruption or denial of business functions.

For each generic scenario, typical threat actors and their ultimate targets can be identified, as well as typical intermediate targets which must be compromised in the course of the attack. Table 2 provides examples.

Table 2. Characterizing Generic Threat Scenarios

Scenario	Typical Threat Actor	Typical Ultimate Targets	Typical Intermediate Targets
Breach	Criminal (individual or organized group) Subverted / suborned insider, criminal (individual or organized group) seeking competitive information on behalf of or for sale to competitors or insider trading customers	Customer information databases Strategic planning information; forecasting applications and databases	Identity and Access Management (IdAM) services and data (to gain access to ultimate targets); Directory Services (to identify ultimate targets); firewalls and external connections (to exfiltrate sensitive information); audit services and data (to hid evidence of actions)
Fraud	Insider, criminal (individual or organized group)	Financial Service (FS) databases; FS transaction message traffic	Same as for Breach
Misuse	Criminal (individual or organized group)	Any processing platform	Directory Services (to identify ultimate targets); firewalls and external connections (to enable communications with usurped resources)
Destruction	Disgruntled insider or former insider; political or ideological activists	FS databases; strategic planning information	IdAM services and data (to gain access to ultimate targets); Directory Services (to identify ultimate targets)
Friendly Fire	Subverted or disgruntled insider; political or ideological activists	FS workflows	Audit services and data; intrusion detection and response (IDR) capabilities
Upstream Attack	Criminal (individual or organized group); political or ideological activists; nation-state-aligned professional criminal enterprise	FS applications and services; supporting hardware and software elements	Directory Services and asset inventories (to identify critical hardware and software components)
Reputation Damage	Disgruntled insider or former insider; political or ideological activists	FS databases; customer information databases	IdAM services and data (to gain access to ultimate targets); Directory Services (to identify ultimate targets)
	Hackers, taggers, and "script kiddies;" small disaffected groups of the above	Outward-facing services and data (e.g., Web pages)	None
Stepping-Stone Attack	Criminal (individual or organized group); political or ideological activists; nation-state-aligned professional criminal enterprise	Outward-facing services and data (e.g., Web pages); partner-facing services, data, and transaction message traffic	Same as for Breach

Scenario	Typical Threat Actor	Typical Ultimate Targets	Typical Intermediate Targets
Extortion	Criminal (individual or organized group)	Critical services and data (ransomware)	Directory Services (to identify ultimate targets); backup and restore services (to damage or deny backups)
		Externally-facing services and data (DDoS)	None

As described in [Bodeau 2018], small groups of high-level threat events constitute building blocks which can be used in multiple scenarios. Table 16 of [Bodeau 2018] provides a number of examples. These groups can be expanded, using the more detailed threat events; a representative expansion is provided in Appendix C.

Figure 5 provides a notional example of how detailed threat events can be identified for the Breach scenario, assuming that an adversary has established a presence on an institution's IT system. A detailed threat scenario for post-Exploit Breach can use the detailed events shown in Figure 5 repeatedly, ordered in different ways, to affect different targets.

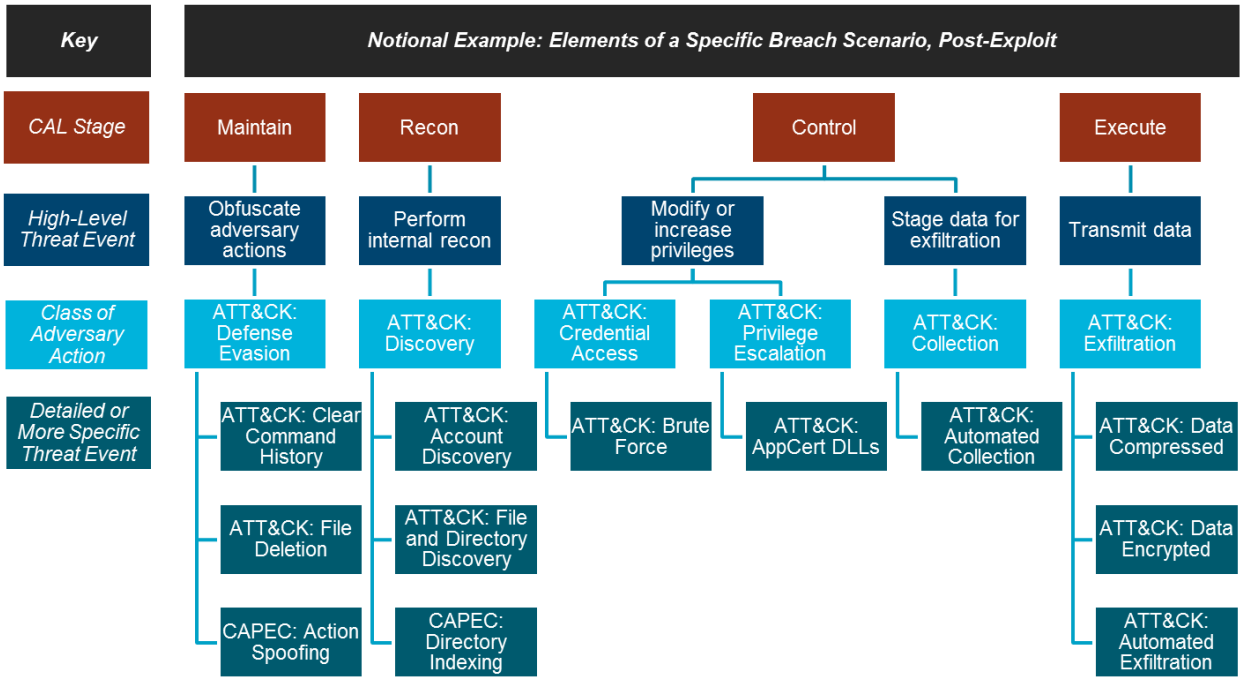

Figure 5. Notional Example of Elements of a Detailed Threat Scenario

4.3.2 Real-World Examples

To understand how potential attack scenarios are grounded in the threat events and behaviors captured in the expanded threat model, it is useful to review examples of cyber attack campaigns targeting the FSS that were actually conducted by real-world cyber attackers.

4.3.2.1 Real-World Cyber Attack Scenario: Carbanak

Table 3 recounts the actions taken by cyber attackers in the Carbanak Banking Campaign, which, from late 2013 through 2015, attacked banks in 30 countries and stole hundreds of millions of dollars.

In the table, the narrative description is juxtaposed with the events in the threat model corresponding to the behavior being described.

Table 3. Carbanak Banking Cyber Attack Campaign

Adversary Goal: Fraud against or theft from the organization

Actor Type: criminal (individual or organized group)

Cyber Effect: Corruption, Modification, or Insertion

Organizational Consequences: Financial loss, Reputation damage

Threat Scenario Summary:

Infect systems in banks using spear phishing, gather information about user roles and systems, use user accesses to steal money by multiple means including transferring money from other accounts to their own via funds transfer or on-line banking, modifying account databases, and dispensing cash through ATMs.

Threat Model Element	Incident Narrative Excerpt[10]
Threat Event: "Deliver targeted malware for control of internal systems and exfiltration of data."	Adversaries infected bank employee computers and delivered Carbanak malware, which provides remote access and control facilities to human adversaries. They were then able to monitor the compromised systems and find ways to expand their control to other platforms within the target organization.
Threat Event: Acquire privileges associated with a user account, process, service, or domain. [See ATT&CK: Credential Access]	After compromise, the malware made video captures of the employee's desktop computer display. This video was used by the adversary to learn about the business processes of the target organization.
Threat Event:" Cause integrity loss by polluting or corrupting critical data. [See CTF: Alter data on the victim's system(s)]"	By compromising the systems of different users, the adversary was able to take advantage of different aspects of the business, based upon each victim's role. Different examples of this from the observed breaches include manipulating business databases of the bank to add money to accounts for later transfer, and extending the compromise to the ATM network to force cash dispensing.
ATT&CK "Remote Services T1021"	Use of the same tools that the bank administrators relied on allowed the adversaries to evade detection. For example, tools like virtual network computing (VNC), PuTTY, and secure shell (SSH) were leveraged by the threat actors.
ATT&CK "Code Signing" T1116	The Carbanak threat actors used digital signing to further minimize the risk of detection.

[10] Derived from [Williamson 2015] and [Kaspersky 2015].

Threat Model Element	Incident Narrative Excerpt[10]
[PRE-ATT&CK "Targeted client-side exploitation" PRE-T1148, "Spear phishing messages with malicious links" PRE-T1146]	By avoiding detection for extended periods of time, the adversaries were able to achieve considerable success in stealing money from the victim institution.
ATT&CK "Network Service Scanning" T1046	During their activities, the adversaries learned the details of the networks in the compromised institution.
ATT&CK "Lateral Movement"	During their activities, the Carbanak threat actors moved laterally by observing users and stealing credentials.
[ATT&CK Collection and Exfiltration various]	Throughout their operation, the adversaries gathered and exfiltrated valuable data.
[ATT&CK Command and Control various]	Adversaries used remote control facilities of the Carbanak software to execute and coordinate actions on the attacked systems.

4.3.2.2 Real-World Cyber Attack Scenario: Buhtrap

Another example of targeted attacks against financial institutions is the activity of the "Buhtrap" group, which, in 2015 and 2016, shifted focus from the common practice of attacking banking client software, to attacking internal banking systems in Russia and the Ukraine. These attacks were able to steal a significant amount of money, and forced banks to shut down to remove their malware, which was spread internally by a worm. Table 4 maps events from the detailed threat model to the attack narrative.

Table 4. Buhtrap Banking Cyber Attack Campaign

Adversary Goal: Fraud against or theft from the organization
Actor Type: criminal (individual or organized group)
Cyber Effect: Corruption, Modification, or Insertion
Organizational Consequences: Financial loss, Reputation damage
Threat Scenario Summary:
Target key employees via spear phishing, install a backdoor, move laterally using a worm, steal credentials, and insert fraudulent payment transactions.

Threat Model Element	Incident Narrative Excerpt[11]
Threat Event: Deliver known malware to internal organizational information systems (e.g., virus via email). [See PREATT&CK: Spear phishing with email attachment]	Buhtrap identified members of the so-called “Anti-drop” club, which included security specialists from several hundred banks, and launched a spear-phishing campaign against these members, either with an infected attachment or via a link to a compromised website that hosted the Nitiris exploit kit.
Threat Event: ”Insert targeted malware into organizational information systems and information system components.”	The malware checked the user system, and if the system locale was Russian or Ukrainian, then the malware was installed.
ATT&CK “Remote Services”, ATT&CK “Two-Factor Authentication Interception”	The attackers employed a legitimate remote access tool (LiteManager) that allows remote control of a system, and leveraged another legitimate program (Guide) to load the command and control module. This module performed keylogging, and enumerated the smart cards on the system.
ATT&CK “Lateral Movement” various	After gaining a foothold on the targeted network, the attackers moved laterally across the network via a crafted worm named the “BuhtrapWorm”. This action, though not stealthy, ensured that it would be difficult to remove the attackers from the network.
ATT&CK “Credential Dumping”	The attackers used a modified version of the Mimikatz program to collect credentials of domain accounts, and leverage the associated privileges.
ATT&CK “System Information Discovery”	The malware searched for the presence of the Automated Working Station of the Central Bank Client (AWS CBC), which is used to batch multiple payment transactions and deliver payment documents on behalf of the Central Bank.
Threat Event: Cause integrity loss by polluting or corrupting critical data. [See CTF: Alter data on the victim’s system(s)]	The attackers then replaced payment documents addressed to the Central Bank, which processed them.
ATT&CK Defensive Evasion	In order to interfere with incident response and forensics, the attackers would disable the compromised systems by deleting the master boot record (MBR).

[11] Derived from [IB Group 2016].

5 Discussion

This section provides some observations on issues encountered in integrating threat events from the multiple sources used and relevance of the threat model to the FSS.

5.1 Integration of Models

The expanded threat model in Appendix A takes a broad view of possible attacker actions from the perspective of an enterprise's IT environment. To do so, it stitches together attack information from multiple well-established, validated cyber defense community repositories. These repositories were developed over time, and each has a defined and narrower scope suited to its purpose. Combining the information from these repositories revealed some areas that are gaps between them at the seams. Events were added to the threat model in cases where straightforward when such gaps were recognized; however, other cases (such as threat events applicable in cloud and virtualization infrastructure environments may be areas for additional community modeling initiatives in the future.

In addition, there were differences in the level of abstraction both from one repository to another and sometimes within the same repository or model. (For instance, the level of events described in NIST 800-30R1, and incorporated from there into the high-level threat model, varies considerably in a few cases.) Where possible, the expanded threat model smooths out these differences by first focusing on sources at a suitable level of detail and then choosing elements from higher or lower levels of their internal ontologies as needed.

This situation suggests there may be an opportunity for a more general ontology that can navigate the levels in a consistent way. Consistency is important for reasons including:

- Clarity of communication
- Facilitating automation of emulated threat behaviors for testing or simulation
- Enabling consistent, meaningful metrics.

Consistency and the ability to combine threat events from the various sources without extensive manual item-by-item analysis is also important to enable an integrated model to evolve as attacks continue to evolve, and new threat events and types are captured in the individual repositories.

5.2 FSS Relevance

The expanded threat model presented in this report takes an encompassing view of possible attacker actions from the perspective of a representative enterprise's IT environment. This has the potential to provide a consistent basis for communicating and coordinating across institutions about threats and mitigations.

In addition, by providing an inclusive and moderately detailed enumeration of threat behaviors that might be encountered, it may have value in helping to estimate and derive information about likelihood, impact, and potential mitigations, as part of an individual organization's cyber risk management. (Organizations may of course already be using threat models at more or less detail for this purpose internally.)

A limitation of the expanded threat model is that it does not go extensively into attacks specific to the FSS. While it does suggest FSS-relevant impacts that attackers might be seeking, it does

not define purely financially-oriented attacks. It also does not examine industry-specific software and associated threats. However, the majority of IT systems used in FSS institutions are based on the same commodity commercial and open source technologies that are reflected in the cybersecurity community repositories from which the threat events are drawn. For instance, a funds transfer network may use a system-specific message format but be based on a broadly used protocol and therefore subject to the threat events associated with the technology more generally.

6 Support for Example Use Cases

The expanded threat model is intended to support (at a minimum):

- Cybersecurity technology foraging
- Cybersecurity test case development for technology validation
- Cyber wargaming scenario development

The following sections illustrate these uses.

6.1 Technology Foraging

An institution can use the list of threat events, winnowed by assumptions about adversary characteristics and by knowledge of its enterprise architecture, to identify gaps in the technologies it uses to address threats. Solutions can be profiled with respect to these gaps.

For each high-level event, a determination is first made as to its feasibility, i.e., whether the enterprise is exposed to the threat event. For example, if the institution does not have public-facing systems, it is not exposed to the "Cause integrity loss by creating, deleting, and/or modifying data on publicly accessible information systems (e.g., web defacement)" threat event.[12] For each feasible event, the relevance of each of the more detailed threat events is determined. For example, for the high-level "Obfuscate adversary actions" event, the more detailed "Rundll32" is relevant to Windows systems, but not to Unix-based systems.

For each relevant event, a determination is made of where and how the event is (or could be) addressed. The characterization of "where and how" can use the Cyber Defense Matrix, as illustrated in Figure 6. For example, for the high-level "Compromise information critical to mission / business functions" event with cyber effects of corruption, modification, or insertion, "where" is "at the Data layer" and "how" is "Protect, Detect, or Recover."[13]

[12] In a risk assessment, the extent or level of the exposure can be considered, as in the Inherent Risk Profile of the FFIEC Cybersecurity Assessment Tool [FFIEC 2017].

[13] Alternatively or in addition, a more nuanced set of effects on adversary activities can be used. See, for example, the list of effects in [NIST 2018].

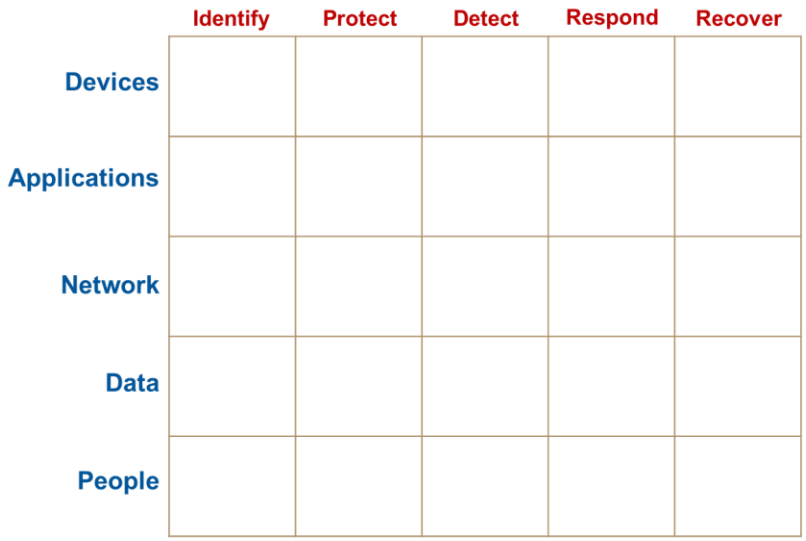

Figure 6. The Cyber Defense Matrix

For each relevant detailed event, a determination is made of how well the event is addressed or covered by the technologies and processes the institution already has in place to address threats. If the list of events were used in risk assessment, an assessment of the event likelihood could also be made. However, this level of detail is unnecessary for technology foraging.

As illustrated in Table 5, the determination can take into consideration whether the event can be addressed in more than one way (e.g., both Protect and Detect).

Table 5. Example of Value Scale for Assessing Coverage of a Detailed Threat Event

Value	Description
High	The threat event can be prevented, or its likelihood reduced to an acceptable level *or* the cyber effects of the threat event can be eliminated or reduced to an acceptable level *and* the threat event can be detected
Medium	The threat event can be prevented, or its likelihood reduced to an acceptable level *or* the cyber effects of the threat event can be eliminated or reduced to an acceptable level *or* the threat event can be detected
Low	The likelihood of the threat event cannot be reduced to an acceptable level, the cyber effects of the threat event cannot be reduced to an acceptable level, and the threat event cannot be reliably detected
N/A	The threat event is not relevant

This assessment can then be aggregated to an assessment of the relevant high-level threat events. The results of this analysis can be displayed visually. The illustration in Figure 7uses four phases of a cyber attack, with the first two phases including reconnaissance, weaponization, delivery, and exploit, and the second two phases including control, execution, and maintenance [Dinsmore 2016].

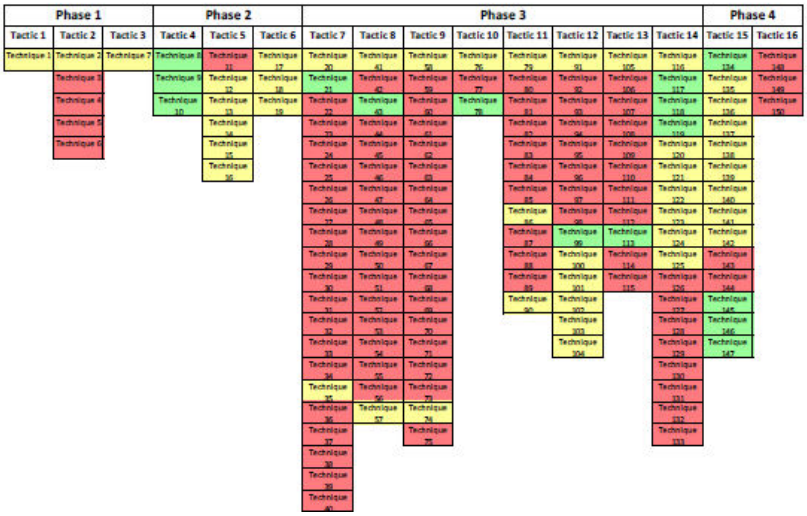

Figure 7. Notional Example of a Coverage Map

The results of the assessment indicate gaps in coverage. These gaps inform technology foraging as follows: an identified solution (e.g., a product, a product suite, a novel technology, a novel way to use existing technologies and products) is mapped to the detailed threat events it addresses. If all of those events are already adequately covered, no further consideration need be given to the solution. Otherwise, the analysis focuses first on events for which coverage is Low, and then on events for which coverage is Medium. A new assessment of coverage for each threat event is made, assuming that the solution is applied correctly. The results of the new assessment can then be aggregated to an assessment of the relevant high-level threat events, and the results displayed visually to understand what additional threat events the new solution would help to defend against.

The development of threat scenarios is not central to analysis in this use case. However, one or two threat scenarios can be developed for expository purposes, to illustrate how the insertion of a technology to fill a gap could reduce risk.

6.2 Test Case Development for Technology Validation

As described in Section 6.1, a profile of a solution can identify which threat events it is expected to address, how, and to what extent (e.g., turning coverage from red to yellow, or from yellow to green). However, such coverage claims can involve more threat events than can reasonably be tested. One or more representative threat scenarios, as described in Section 4.3, can be tailored to motivate and structure test cases to validate claims about the effectiveness of technologies or solutions.

For this use case, the scenarios consist of detailed threat events, winnowed by assumptions about adversary characteristics and by knowledge of the enterprise architecture. Technology validation is typically carried out in a representative laboratory or cyber range environment. Therefore, the scenarios in a technology validation test case will use general characterizations of intermediate and ultimate targets of adversary activities, rather than exact representations of the institution's operational IT system.

In addition, test cases can be developed to validate assumptions that some high-level threat events are infeasible.

6.3 Cyber Wargaming Scenario Development

In the preceding two use cases, characteristics of the adversary are used in a general way, to determine whether the institution's cyber attackers can be expected to attempt a given threat scenario and, if so, whether they can be expected to take a specific action, use a TTP, or follow an attack pattern. In the development of a cyber wargaming scenario, adversary characteristics may be represented more specifically, by creating a profile of the adversary (or adversaries) involved in the scenario.

The scenario itself can be selected and tailored from the representative scenarios in Section 4.3, or from the Financial and Banking Information Infrastructure Committee (FBIIC) Financial Sector Cyber Exercise Template [FBIIC 2017]. Tailoring takes into consideration the institution's cyber playbook, i.e., its documented roles, responsibilities, decision-making processes, and technologies which inform or implement operational cybersecurity decisions.

Lessons learned by executing a cyber wargaming exercise that was based upon the constructed scenario could possibly provide a feedback loop into the threat model and representative scenarios, providing more detail, clarification, or even new content.

7 Conclusion

This report has presented an expanded threat model that provides implementation-relevant events in sufficient detail for selected use cases involving technology foraging and developing test cases for technology security assessment and scenarios for wargaming. It is based on broad categories of technologies expected to be in the enterprise's IT environment, but at the same time, it remains at a high enough level to be generic in terms of specific implementations.

The threat model is further examined in a companion report [Fox 2016] that defines a specific IT system architecture for a notional FSS institution, accompanied by a representation of its relevant business functions and processes, and examines the use cases and value of such an instantiated threat model.

The threat model presented herein, and the high-level threat model on which it builds, are defined in relation to a single enterprise, with its interfaces to partners and the outside world. A related report, [Bodeau 2018], examines what additional elements would be required in a threat model to allow it to be used to capture and assess systemic or sector-wide risks to which the FSS may be subject as a result of cyber attack.

Existing attack repositories used in this report served as a strong foundation for populating the modeling framework with detailed events. However, the analysis also revealed some areas that remain as gaps, with growing attack vectors being introduced by technology changes such as use of cloud and virtualization environments.

For cloud environments, events were added to the threat model for common existing attack methods that are being exploited. These include events such as misconfigured data storage and encryption material breaches. While adoption of commercial cloud offerings by financial services companies that are part of the critical infrastructure continue to be minimal for riskier applications, the market trends to further adoption will continue to push more critical work to the environment, driven by cost avoidance and scaling agility. The abstraction of disk, operating system (OS), and hardware infrastructure components in virtualized environments allows the possibility of more sophisticated attack vectors that are not visible to current OS layer controls and monitoring, such as that exhibited by the data store vulnerabilities being seen today.

The hypervisor infrastructure providing the foundation for abstracting the physical hardware serves as an additional potential path of vulnerability by adding a layer of access, resource management, and monitoring outside of the scope of current frameworks, enabling potential attack techniques not covered by traditional modeling frameworks.

As the cybersecurity community gains more experience with patterns of attack and techniques used by attackers in association with such technologies, it is expected that community repositories of attack information will be augmented in these areas. Additional threat event information can then be incorporated into the expanded threat model to support use cases for systems that rely on these technologies.

More broadly, threat models must be updated as distinct new threat behaviors become known, as a result of evolution in adversary capabilities and in the technology base over time.

Appendix A Expanded Threat Model

This appendix provides the details of the expanded threat model, in Table 6. The "High-Level Threat Event" column lists the events defined in the high-level threat model. In cases where the high-level threat event is closely related to a higher level concept in the ODNI CTF [ODNI 2017] or ATT&CK [MITRE 2015], the corresponding CTF objective or ATT&CK tactic is also noted.

In the remaining columns, each of high-level threat events is characterized as to the cyber attack lifecycle stage in which it is likely to be used, the attack vectors through which it can be actuated, and the general cyber effect it seeks to create.

In the "Detailed Threat Event and Source column," more specific threat behaviors that can be used to accomplish the high-level event are provided. Along with each threat behavior, the source from which it is drawn is identified. Sources include ATT&CK [MITRE 2015], CAPEC [MITRE 2016], PRE-ATT&CK [MITRE 2016b], ATT&CK for Mobile [MITRE 2017b], and Cloud Security Alliance (CSA) [Cloud Security Alliance 2017].

Table 6. Expanded Threat Model Events

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Recon	Perform perimeter network reconnaissance/scanning.	External network connection	Interception	Conduct active scanning-PRE-ATT&CK
Recon	Perform perimeter network reconnaissance/scanning.	External network connection	Interception	Conduct passive scanning-PRE-ATT&CK
Recon	Perform network sniffing of external networks (e.g., ISPs) to which organizational networks are connected.	External network connection	Interception	Determine domain and IP address space-PRE-ATT&CK
Recon	Perform network sniffing of external networks (e.g., ISPs) to which organizational networks are connected.	External network connection	Interception	Determine external network trust dependencies-PRE-ATT&CK
Recon	Perform network sniffing of external networks (e.g., ISPs) to which organizational networks are connected.	External network connection	Interception	Discover target logon/email address format-PRE-ATT&CK
Recon	Perform network sniffing of external networks (e.g., ISPs) to which organizational networks are connected.	External network connection	Interception	Enumerate client configurations-PRE-ATT&CK

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Recon	Perform network sniffing of external networks (e.g., ISPs) to which organizational networks are connected.	External network connection	Interception	Enumerate externally facing software applications technologies, languages, and dependencies-PRE-ATT&CK
Recon	Analyze network traffic based on network sniffing.	External network connection / Internal network (when CAL is applied recursively)	Interception	Determine 3rd party infrastructure services-PRE-ATT&CK
Recon	Analyze network traffic based on network sniffing.	External network connection / Internal network (when CAL is applied recursively)	Interception	Determine domain and IP address space-PRE-ATT&CK
Recon	Analyze network traffic based on network sniffing.	External network connection / Internal network (when CAL is applied recursively)	Interception	Determine external network trust dependencies-PRE-ATT&CK
Recon	Analyze network traffic based on network sniffing.	External network connection / Internal network (when CAL is applied recursively)	Interception	Identify security defensive capabilities-PRE-ATT&CK
Recon	Analyze network traffic based on network sniffing.	External network connection / Internal network (when CAL is applied recursively)	Interception	Map network topology-PRE-ATT&CK
Recon	Analyze network traffic based on network sniffing.	External network connection / Internal network (when CAL is applied recursively)	Interception	Identify technology usage patterns-PRE-ATT&CK
Recon	Perform malware-directed internal reconnaissance.	Maintenance environment, actions of privileged user, trusted or partner network connection	Interception	
Recon	Perform malware-directed internal reconnaissance.	Maintenance environment, actions of privileged user, trusted or partner network connection	Interception	Account Discovery-ATT&CK
Recon	Perform malware-directed internal reconnaissance.	Maintenance environment, actions of privileged user, trusted or partner network connection	Interception	Application Window Discovery-ATT&CK
Recon	Perform malware-directed internal reconnaissance.	Maintenance environment, actions of privileged user, trusted or partner network connection	Interception	File and Directory Discovery-ATT&CK

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Recon	Perform malware-directed internal reconnaissance.	Maintenance environment, actions of privileged user, trusted or partner network connection	Interception	Network Service Scanning-ATT&CK
Recon	Perform malware-directed internal reconnaissance.	Maintenance environment, actions of privileged user, trusted or partner network connection	Interception	Network Share Discovery-ATT&CK
Recon	Perform malware-directed internal reconnaissance.	Maintenance environment, actions of privileged user, trusted or partner network connection	Interception	Peripheral Device Discovery-ATT&CK
Recon	Perform malware-directed internal reconnaissance.	Maintenance environment, actions of privileged user, trusted or partner network connection	Interception	Permission Groups Discovery-ATT&CK
Recon	Perform malware-directed internal reconnaissance.	Maintenance environment, actions of privileged user, trusted or partner network connection	Interception	Process Discovery-ATT&CK
Recon	Perform malware-directed internal reconnaissance.	Maintenance environment, actions of privileged user, trusted or partner network connection	Interception	Remote System Discovery-ATT&CK
Recon	Perform malware-directed internal reconnaissance.	Maintenance environment, actions of privileged user, trusted or partner network connection	Interception	Security Software Discovery-ATT&CK
Recon	Perform malware-directed internal reconnaissance.	Maintenance environment, actions of privileged user, trusted or partner network connection	Interception	System Information Discovery-ATT&CK
Recon	Perform malware-directed internal reconnaissance.	Maintenance environment, actions of privileged user, trusted or partner network connection	Interception	System Network Configuration Discovery-ATT&CK

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Recon	Perform malware-directed internal reconnaissance.	Maintenance environment, actions of privileged user, trusted or partner network connection	Interception	System Network Connections Discovery-ATT&CK
Recon	Perform malware-directed internal reconnaissance.	Maintenance environment, actions of privileged user, trusted or partner network connection	Interception	System Owner/User Discovery-ATT&CK
Recon	Perform malware-directed internal reconnaissance.	Maintenance environment, actions of privileged user, trusted or partner network connection	Interception	System Service Discovery-ATT&CK
Recon	Perform malware-directed internal reconnaissance.	Maintenance environment, actions of privileged user, trusted or partner network connection	Interception	System Time Discovery-ATT&CK
Weaponize	Create counterfeit/spoof web site.	External network connection	(no immediate effects)	Content Spoofing-CAPEC
Weaponize	Craft counterfeit certificates.	External network connection, trusted or partner network connection	(no immediate effects)	Content Spoofing-CAPEC
Weaponize	Create and operate false front organizations to inject malicious components into the supply chain.	Supply chain	(no immediate effects)	Content Spoofing-CAPEC
Deliver	Establish or use a communications channel to the enterprise as a whole or to a targeted system.	External network connection, trusted or partner network connection	(no immediate effects)	Compromise of externally facing system-PRE-ATT&CK
Deliver	Establish or use a communications channel to the enterprise as a whole or to a targeted system.	External network connection, trusted or partner network connection	(no immediate effects)	Leverage compromised 3rd party resources-PRE-ATT&CK
Deliver	Deliver commands to a targeted system (e.g., login).	(no immediate effects)	Unauthorized use	Authentication attempt-PRE-ATT&CK
Deliver	Deliver commands to a targeted system (e.g., login).	(no immediate effects)	Unauthorized use	Authentication Abuse-CAPEC
Deliver	Deliver commands to a targeted system (e.g., login).	(no immediate effects)	Unauthorized use	Authentication Bypass-CAPEC

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Deliver	Deliver commands to a targeted system (e.g., login).	(no immediate effects)	Unauthorized use	Code Injection-CAPEC
Deliver	Deliver commands to a targeted system (e.g., login).	(no immediate effects)	Unauthorized use	Command Injection-CAPEC
Deliver	Deliver commands to a targeted system (e.g., login).	(no immediate effects)	Unauthorized use	Communication Channel Manipulation-CAPEC
Deliver	Deliver commands to a targeted system (e.g., login).	(no immediate effects)	Unauthorized use	Exploitation of Trusted Credentials-CAPEC
Deliver	Deliver commands to a targeted system (e.g., login).	(no immediate effects)	Unauthorized use	Exploiting Trust in Client-CAPEC
Deliver	Deliver commands to a targeted system (e.g., login).	(no immediate effects)	Unauthorized use	Identity Spoofing-CAPEC
Deliver	Deliver commands to a targeted system (e.g., login).	(no immediate effects)	Unauthorized use	Input Data Manipulation-CAPEC
Deliver	Deliver known malware to internal organizational information systems (e.g., virus via email). [See CTF: Interact with intended victim]	External network connection, email	Corruption, Modification, or Insertion	Replace legitimate binary with malware-PRE-ATT&CK
Deliver	Deliver known malware to internal organizational information systems (e.g., virus via email). [See CTF: Interact with intended victim]	External network connection, email	Corruption, Modification, or Insertion	Spear phishing messages with malicious attachments-PRE-ATT&CK
Deliver	Deliver known malware to internal organizational information systems (e.g., virus via email). [See CTF: Interact with intended victim]	External network connection, email	Corruption, Modification, or Insertion	Credential pharming-PRE-ATT&CK
Deliver	Deliver known malware to internal organizational information systems (e.g., virus via email). [See CTF: Interact with intended victim]	External network connection, email	Corruption, Modification, or Insertion	Conduct social engineering or HUMINT operation-PRE-ATT&CK
Deliver	Deliver known malware to internal organizational information systems (e.g., virus via email). [See CTF: Interact with intended victim]	External network connection, email	Corruption, Modification, or Insertion	Spear phishing messages with text only-PRE-ATT&CK

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Deliver	Deliver known malware to internal organizational information systems (e.g., virus via email). [See CTF: Interact with intended victim]	External network connection, email	Corruption, Modification, or Insertion	Targeted social media phishing-PRE-ATT&CK
Deliver	Deliver known malware to internal organizational information systems (e.g., virus via email). [See CTF: Interact with intended victim]	External network connection, email	Corruption, Modification, or Insertion	Unconditional client-side exploitation/Injected Website/Driveby-PRE-ATT&CK
Deliver	Deliver known malware to internal organizational information systems (e.g., virus via email). [See CTF: Interact with intended victim]	External network connection, email	Corruption, Modification, or Insertion	Authorized user performs requested cyber action-PRE-ATT&CK
Deliver	Deliver known malware to internal organizational information systems (e.g., virus via email). [See CTF: Interact with intended victim]	External network connection, email	Corruption, Modification, or Insertion	DNS poisoning-PRE-ATT&CK
Deliver	Deliver known malware to internal organizational information systems (e.g., virus via email). [See CTF: Interact with intended victim]	External network connection, email	Corruption, Modification, or Insertion	App delivered via email attachment-Mobile_ATT&CK
Deliver	Deliver known malware to internal organizational information systems (e.g., virus via email). [See CTF: Interact with intended victim]	External network connection, email	Corruption, Modification, or Insertion	App delivered via web content-Mobile_ATT&CK
Deliver	Deliver modified malware to internal organizational information systems. [See CTF: Interact with intended victim]	Internal network, authorized actions of non-privileged user, authorized actions of privileged user, device port (e.g., removable media)	Corruption, Modification, or Insertion	Deploy exploit using advertising-PRE-ATT&CK
Deliver	Deliver modified malware to internal organizational information systems. [See CTF: Interact with intended victim]	Internal network, authorized actions of non-privileged user, authorized actions of privileged user, device port (e.g., removable media)	Corruption, Modification, or Insertion	App delivered via email attachment-Mobile_ATT&CK
Deliver	Deliver modified malware to internal organizational information systems. [See CTF: Interact with intended victim]	Internal network, authorized actions of non-privileged user, authorized actions of privileged user, device port (e.g., removable media)	Corruption, Modification, or Insertion	App delivered via web content-Mobile_ATT&CK

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Deliver	Deliver targeted malware for control of internal systems and exfiltration of data.	Internal network, authorized actions of non-privileged user, authorized actions of privileged user, device port (e.g., removable media)	Corruption, Modification, or Insertion	
Deliver	Deliver malware by providing removable media.	Authorized actions of non-privileged user, authorized actions of privileged user, device port (e.g., removable media)	Corruption, Modification, or Insertion	Disseminate removable media-PRE-ATT&CK
Deliver	Deliver malware by providing removable media.	Authorized actions of non-privileged user, authorized actions of privileged user, device port (e.g., removable media)	Corruption, Modification, or Insertion	Attack PC via USB Connection-Mobile_ATT&CK
Deliver	Insert untargeted malware into downloadable software and/or into commercial information technology products.	Supply chain	Corruption, Modification, or Insertion	Spear phishing messages with malicious links-PRE-ATT&CK
Deliver	Insert untargeted malware into downloadable software and/or into commercial information technology products.	Supply chain	Corruption, Modification, or Insertion	Replace legitimate binary with malware-PRE-ATT&CK
Deliver	Insert untargeted malware into downloadable software and/or into commercial information technology products.	Supply chain	Corruption, Modification, or Insertion	Repackaged Application-Mobile_ATT&CK
Deliver	Insert targeted malware into organizational information systems and information system components.	Supply chain, maintenance environment	Corruption, Modification, or Insertion	Targeted client-side exploitation-PRE-ATT&CK
Deliver	Insert targeted malware into organizational information systems and information system components.	Supply chain, maintenance environment	Corruption, Modification, or Insertion	Repackaged Application-Mobile_ATT&CK
Deliver	Insert specialized malware into organizational information systems based on system configurations.	Supply chain, maintenance environment	Corruption, Modification, or Insertion	Untargeted client-side exploitation-PRE-ATT&CK

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Deliver	Insert specialized malware into organizational information systems based on system configurations.	Supply chain, maintenance environment	Corruption, Modification, or Insertion	Authentication Bypass-CAPEC
Deliver	Insert specialized malware into organizational information systems based on system configurations.	Supply chain, maintenance environment	Corruption, Modification, or Insertion	Code Inclusion-CAPEC
Deliver	Insert specialized malware into organizational information systems based on system configurations.	Supply chain, maintenance environment	Corruption, Modification, or Insertion	Code Injection-CAPEC
Deliver	Insert specialized malware into organizational information systems based on system configurations.	Supply chain, maintenance environment	Corruption, Modification, or Insertion	Command Injection-CAPEC
Deliver	Insert specialized malware into organizational information systems based on system configurations.	Supply chain, maintenance environment	Corruption, Modification, or Insertion	Configuration/Environment Manipulation-CAPEC
Deliver	Insert specialized malware into organizational information systems based on system configurations.	Supply chain, maintenance environment	Corruption, Modification, or Insertion	Exploitation of Trusted Credentials-CAPEC
Deliver	Insert specialized malware into organizational information systems based on system configurations.	Supply chain, maintenance environment	Corruption, Modification, or Insertion	Exploiting Trust in Client-CAPEC
Deliver	Insert specialized malware into organizational information systems based on system configurations.	Supply chain, maintenance environment	Corruption, Modification, or Insertion	File Manipulation-CAPEC
Deliver	Insert specialized malware into organizational information systems based on system configurations.	Supply chain, maintenance environment	Corruption, Modification, or Insertion	Functionality Bypass-CAPEC
Deliver	Insert specialized malware into organizational information systems based on system configurations.	Supply chain, maintenance environment	Corruption, Modification, or Insertion	Functionality Misuse-CAPEC
Deliver	Insert specialized malware into organizational information systems based on system configurations.	Supply chain, maintenance environment	Corruption, Modification, or Insertion	Identity Spoofing-CAPEC
Deliver	Insert specialized malware into organizational information systems based on system configurations.	Supply chain, maintenance environment	Corruption, Modification, or Insertion	Input Data Manipulation-CAPEC

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Deliver	Insert specialized malware into organizational information systems based on system configurations.	Supply chain, maintenance environment	Corruption, Modification, or Insertion	Malicious Logic Insertion-CAPEC
Deliver	Insert specialized malware into organizational information systems based on system configurations.	Supply chain, maintenance environment	Corruption, Modification, or Insertion	Manipulating User State-CAPEC
Deliver	Insert specialized malware into organizational information systems based on system configurations.	Supply chain, maintenance environment	Corruption, Modification, or Insertion	Parameter Injection-CAPEC
Deliver	Insert specialized malware into organizational information systems based on system configurations.	Supply chain, maintenance environment	Corruption, Modification, or Insertion	Privilege Abuse-CAPEC
Deliver	Insert specialized malware into organizational information systems based on system configurations.	Supply chain, maintenance environment	Corruption, Modification, or Insertion	Traffic Injection-CAPEC
Deliver	Insert counterfeit or tampered hardware into the supply chain.	Supply chain	Corruption, Modification, or Insertion	Malicious or Vulnerable Built-in device functionality-Mobile_ATT&CK
Deliver	Insert counterfeit or tampered hardware into the supply chain.	Supply chain	Corruption, Modification, or Insertion	Hardware Integrity Attack-CAPEC
Deliver	Insert counterfeit or tampered hardware into the supply chain.	Supply chain	Corruption, Modification, or Insertion	Manipulation During Distribution-CAPEC
Deliver	Insert counterfeit or tampered hardware into the supply chain.	Supply chain	Corruption, Modification, or Insertion	Modification During Manufacture-CAPEC
Deliver	Insert tampered critical components into organizational systems.	Supply chain, maintenance environment	Corruption, Modification, or Insertion	Component firmware-ATT&CK
Deliver	Insert tampered critical components into organizational systems.	Supply chain, maintenance environment	Corruption, Modification, or Insertion	Software Integrity Attack-CAPEC
Deliver	Insert tampered critical components into organizational systems.	Supply chain, maintenance environment	Corruption, Modification, or Insertion	Manipulation During Distribution-CAPEC

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Deliver	Insert tampered critical components into organizational systems.	Supply chain, maintenance environment	Corruption, Modification, or Insertion	Modification During Manufacture-CAPEC
Deliver	Insert tampered critical components into organizational systems.	Supply chain, maintenance environment	Corruption, Modification, or Insertion	Hardware Integrity Attack-CAPEC
Deliver	Compromise information systems or devices used externally and reintroduced into the enterprise.	Mobile or transiently connected devices	Corruption, Modification, or Insertion, unauthorized use	Software Integrity Attack-CAPEC
Deliver	Compromise information systems or devices used externally and reintroduced into the enterprise.	Mobile or transiently connected devices	Corruption, Modification, or Insertion, unauthorized use	Manipulation During Distribution-CAPEC
Deliver	Compromise information systems or devices used externally and reintroduced into the enterprise.	Mobile or transiently connected devices	Corruption, Modification, or Insertion, unauthorized use	Modification During Manufacture-CAPEC
Deliver	Compromise information systems or devices used externally and reintroduced into the enterprise.	Mobile or transiently connected devices	Corruption, Modification, or Insertion, unauthorized use	Hardware Integrity Attack-CAPEC
Deliver / Exploit	Install general-purpose sniffers on organization-controlled information systems or networks.	Internal network, authorized actions of privileged user, device port (e.g., removable media)	Modification or Insertion	
Deliver / Exploit	Install persistent and targeted sniffers on organizational information systems and networks.	Internal network, authorized actions of privileged user, device port (e.g., removable media)	Modification or Insertion	
Deliver / Exploit	Install persistent and targeted sniffers on organizational information systems and networks.	Internal network, authorized actions of privileged user, device port (e.g., removable media)	Modification or Insertion	Network Sniffing-ATT&CK
Deliver / Exploit	Install persistent and targeted sniffers on organizational information systems and networks.	Internal network, authorized actions of privileged user, device port (e.g., removable media)	Modification or Insertion	Rogue WIFI Access Points-Mobile_ATT&CK

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Deliver / Exploit	Install persistent and targeted sniffers on organizational information systems and networks.	Internal network, authorized actions of privileged user, device port (e.g., removable media)	Modification or Insertion	Protocol Analysis-CAPEC
Deliver / Exploit	Insert malicious scanning devices (e.g., wireless sniffers) inside facilities.	Immediate physical proximity	Modification or Insertion	Network Sniffing-ATT&CK
Deliver / Exploit	Insert malicious scanning devices (e.g., wireless sniffers) inside facilities.	Immediate physical proximity	Modification or Insertion	Network Traffic capture or redirection-Mobile-ATT&CK
Deliver / Exploit	Insert malicious scanning devices (e.g., wireless sniffers) inside facilities.	Immediate physical proximity	Modification or Insertion	Protocol Analysis-CAPEC
Exploit	Exploit physical access of authorized staff to gain access to organizational facilities.	Immediate physical proximity	(no immediate effects)	Human performs requested action of physical nature-PRE-ATT&CK
Exploit	Exploit physical access of authorized staff to gain access to organizational facilities.	Immediate physical proximity	(no immediate effects)	Manipulate Human Behavior-CAPEC
Exploit	Exploit physical access of authorized staff to gain access to organizational facilities.	Immediate physical proximity	(no immediate effects)	Information Elicitation-CAPEC
Exploit	Exploit physical access of authorized staff to gain access to organizational facilities.	Immediate physical proximity	(no immediate effects)	Bypassing Physical Security-CAPEC
Exploit	Exploit poorly configured or unauthorized information systems exposed to the internet.	External network connection	Corruption, Modification, or Insertion	Compromise of externally facing system-PRE-ATT&CK
Exploit	Exploit poorly configured or unauthorized information systems exposed to the internet.	External network connection	Corruption, Modification, or Insertion	Exploit Vulnerability-ATT&CK
Exploit	Exploit poorly configured or unauthorized information systems exposed to the internet.	External network connection	Corruption, Modification, or Insertion	API Manipulation-CAPEC
Exploit	Exploit poorly configured or unauthorized information systems exposed to the internet.	External network connection	Corruption, Modification, or Insertion	Authentication Abuse-CAPEC

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Exploit	Exploit poorly configured or unauthorized information systems exposed to the internet.	External network connection	Corruption, Modification, or Insertion	Authentication Bypass-CAPEC
Exploit	Exploit poorly configured or unauthorized information systems exposed to the internet.	External network connection	Corruption, Modification, or Insertion	Buffer Manipulation-CAPEC
Exploit	Exploit poorly configured or unauthorized information systems exposed to the Iinternet.	External network connection	Corruption, Modification, or Insertion	Brute Force-CAPEC
Exploit	Exploit poorly configured or unauthorized information systems exposed to the internet.	External network connection	Corruption, Modification, or Insertion	Code Inclusion-CAPEC
Exploit	Exploit poorly configured or unauthorized information systems exposed to the internet.	External network connection	Corruption, Modification, or Insertion	Code Injection-CAPEC
Exploit	Exploit poorly configured or unauthorized information systems exposed to the internet.	External network connection	Corruption, Modification, or Insertion	Command Injection-CAPEC
Exploit	Exploit poorly configured or unauthorized information systems exposed to the internet.	External network connection	Corruption, Modification, or Insertion	Communication Channel Manipulation-CAPEC
Exploit	Exploit poorly configured or unauthorized information systems exposed to the internet.	External network connection	Corruption, Modification, or Insertion	Content Spoofing-CAPEC
Exploit	Exploit poorly configured or unauthorized information systems exposed to the internet.	External network connection	Corruption, Modification, or Insertion	Excavation-CAPEC
Exploit	Exploit poorly configured or unauthorized information systems exposed to the internet.	External network connection	Corruption, Modification, or Insertion	Exploitation of Trusted Credentials-CAPEC
Exploit	Exploit poorly configured or unauthorized information systems exposed to the internet.	External network connection	Corruption, Modification, or Insertion	Exploiting Trust in Client-CAPEC
Exploit	Exploit poorly configured or unauthorized information systems exposed to the internet.	External network connection	Corruption, Modification, or Insertion	File Manipulation-CAPEC

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Exploit	Exploit poorly configured or unauthorized information systems exposed to the internet.	External network connection	Corruption, Modification, or Insertion	Fingerprinting-CAPEC
Exploit	Exploit poorly configured or unauthorized information systems exposed to the internet.	External network connection	Corruption, Modification, or Insertion	Flooding-CAPEC
Exploit	Exploit poorly configured or unauthorized information systems exposed to the internet.	External network connection	Corruption, Modification, or Insertion	Footprinting-CAPEC
Exploit	Exploit poorly configured or unauthorized information systems exposed to the internet.	External network connection	Corruption, Modification, or Insertion	Functionality Bypass-CAPEC
Exploit	Exploit poorly configured or unauthorized information systems exposed to the internet.	External network connection	Corruption, Modification, or Insertion	Functionality Misuse-CAPEC
Exploit	Exploit poorly configured or unauthorized information systems exposed to the internet.	External network connection	Corruption, Modification, or Insertion	Identity Spoofing-CAPEC
Exploit	Exploit poorly configured or unauthorized information systems exposed to the internet.	External network connection	Corruption, Modification, or Insertion	Input Data Manipulation-CAPEC
Exploit	Exploit poorly configured or unauthorized information systems exposed to the internet.	External network connection	Corruption, Modification, or Insertion	Malicious Logic Insertion-CAPEC
Exploit	Exploit poorly configured or unauthorized information systems exposed to the internet.	External network connection	Corruption, Modification, or Insertion	Parameter Injection-CAPEC
Exploit	Exploit poorly configured or unauthorized information systems exposed to the internet.	External network connection	Corruption, Modification, or Insertion	Privilege Abuse-CAPEC
Exploit	Exploit poorly configured or unauthorized information systems exposed to the internet.	External network connection	Corruption, Modification, or Insertion	Privilege Escalation-CAPEC
Exploit	Exploit poorly configured or unauthorized information systems exposed to the internet.	External network connection	Corruption, Modification, or Insertion	Resource Injection-CAPEC

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Exploit	Exploit poorly configured or unauthorized information systems exposed to the internet.	External network connection	Corruption, Modification, or Insertion	Resource Location Spoofing-CAPEC
Exploit	Exploit split tunneling on an end-user system to gain access to enterprise systems.	External network connection, end-user system	Exfiltration, Interception	
Exploit	Exploit split tunneling on an end-user system to gain access to enterprise systems.	External network connection, end-user system	Exfiltration, Interception	External Remote Services-ATT&CK
Exploit	Exploit split tunneling on an end-user system to gain access to enterprise systems.	External network connection, end-user system	Exfiltration, Interception	Alternate Network Mediums-Mobile_ATT&CK
Exploit	Exploit split tunneling on an end-user system to gain access to enterprise systems.	External network connection, end-user system	Exfiltration, Interception	Communication Channel Manipulation-CAPEC
Exploit	Obtain a legitimate account. [See CTF]	External network connection	(no immediate effects)	Unauthorized user introduces compromise delivery mechanism-PRE-ATT&CK
Exploit	Obtain a legitimate account. [See CTF]	External network connection	(no immediate effects)	Create Account-ATT&CK
Exploit	Obtain a legitimate account. [See CTF]	External network connection	(no immediate effects)	Valid account-ATT&CK
Exploit	Obtain a legitimate account. [See CTF]	External network connection	(no immediate effects)	account manipulation-ATT&CK
Exploit	Obtain a legitimate account. [See CTF]	External network connection	(no immediate effects)	Fake Developer accounts-Mobile_ATT&CK
Exploit	Obtain a legitimate account. [See CTF]	External network connection	(no immediate effects)	Exploitation of Trusted Credentials-CAPEC
Exploit	Obtain a legitimate account. [See CTF]	External network connection	(no immediate effects)	Exploiting Trust in Client-CAPEC
Exploit	Obtain a legitimate account. [See CTF]	External network connection	(no immediate effects)	Identity Spoofing-CAPEC
Exploit	Obtain a legitimate account. [See CTF]	External network connection	(no immediate effects)	Privilege Abuse-CAPEC
Exploit	Obtain a legitimate account. [See CTF]	External network connection	(no immediate effects)	Privilege Escalation-CAPEC

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Exploit	Exploit known vulnerabilities in mobile systems (e.g., laptops, personal digital assistants (PDAs), smart phones). [See CTF: Establish illicit user access]	Mobile or transiently connected devices	Corruption, Interception	
Exploit	Exploit known vulnerabilities in mobile systems (e.g., laptops, PDAs, smart phones). [See CTF: Establish illicit user access]	Mobile or transiently connected devices	Corruption, Interception	Exploit Vulnerability-ATT&CK
Exploit	Exploit known vulnerabilities in mobile systems (e.g., laptops, PDAs, smart phones). [See CTF: Establish illicit user access]	Mobile or transiently connected devices	Corruption, Interception	Malicious or vulnerable built-in device functionality-Mobile_ATT&CK
Exploit	Exploit known vulnerabilities in mobile systems (e.g., laptops, PDAs, smart phones). [See CTF: Establish illicit user access]	Mobile or transiently connected devices	Corruption, Interception	Exploit baseband vulnerability-Mobile_ATT&CK
Exploit	Exploit known vulnerabilities in mobile systems (e.g., laptops, PDAs, smart phones). [See CTF: Establish illicit user access]	Mobile or transiently connected devices	Corruption, Interception	API Manipulation-CAPEC
Exploit	Exploit known vulnerabilities in mobile systems (e.g., laptops, PDAs, smart phones). [See CTF: Establish illicit user access]	Mobile or transiently connected devices	Corruption, Interception	Authentication Abuse-CAPEC
Exploit	Exploit known vulnerabilities in mobile systems (e.g., laptops, PDAs, smart phones). [See CTF: Establish illicit user access]	Mobile or transiently connected devices	Corruption, Interception	Authentication Bypass-CAPEC
Exploit	Exploit known vulnerabilities in mobile systems (e.g., laptops, PDAs, smart phones). [See CTF: Establish illicit user access]	Mobile or transiently connected devices	Corruption, Interception	Buffer Manipulation-CAPEC
Exploit	Exploit known vulnerabilities in mobile systems (e.g., laptops, PDAs, smart phones). [See CTF: Establish illicit user access]	Mobile or transiently connected devices	Corruption, Interception	Code Inclusion-CAPEC

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Exploit	Exploit known vulnerabilities in mobile systems (e.g., laptops, PDAs, smart phones). [See CTF: Establish illicit user access]	Mobile or transiently connected devices	Corruption, Interception	Code Injection-CAPEC
Exploit	Exploit known vulnerabilities in mobile systems (e.g., laptops, PDAs, smart phones). [See CTF: Establish illicit user access]	Mobile or transiently connected devices	Corruption, Interception	Command Injection-CAPEC
Exploit	Exploit known vulnerabilities in mobile systems (e.g., laptops, PDAs, smart phones). [See CTF: Establish illicit user access]	Mobile or transiently connected devices	Corruption, Interception	Exploit OS vulnerability-Mobile_ATT&CK
Exploit	Exploit known vulnerabilities in mobile systems (e.g., laptops, PDAs, smart phones). [See CTF: Establish illicit user access]	Mobile or transiently connected devices	Corruption, Interception	Exploiting Trust in Client-CAPEC
Exploit	Exploit known vulnerabilities in mobile systems (e.g., laptops, PDAs, smart phones). [See CTF: Establish illicit user access]	Mobile or transiently connected devices	Corruption, Interception	Fault Injection-CAPEC
Exploit	Exploit known vulnerabilities in mobile systems (e.g., laptops, PDAs, smart phones). [See CTF: Establish illicit user access]	Mobile or transiently connected devices	Corruption, Interception	Functionality Bypass-CAPEC
Exploit	Exploit known vulnerabilities in mobile systems (e.g., laptops, PDAs, smart phones). [See CTF: Establish illicit user access]	Mobile or transiently connected devices	Corruption, Interception	Functionality Misuse-CAPEC
Exploit	Exploit known vulnerabilities in mobile systems (e.g., laptops, PDAs, smart phones). [See CTF: Establish illicit user access]	Mobile or transiently connected devices	Corruption, Interception	Insecure Third-Party Libraries-Mobile_ATT&CK
Exploit	Exploit known vulnerabilities in mobile systems (e.g., laptops, PDAs, smart phones). [See CTF: Establish illicit user access]	Mobile or transiently connected devices	Corruption, Interception	Leveraging Race Conditions-CAPEC

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Exploit	Exploit known vulnerabilities in mobile systems (e.g., laptops, PDAs, smart phones). [See CTF: Establish illicit user access]	Mobile or transiently connected devices	Corruption, Interception	Local Execution of Code-CAPEC
Exploit	Exploit known vulnerabilities in mobile systems (e.g., laptops, PDAs, smart phones). [See CTF: Establish illicit user access]	Mobile or transiently connected devices	Corruption, Interception	Malicious Logic Insertion-CAPEC
Exploit	Exploit known vulnerabilities in mobile systems (e.g., laptops, PDAs, smart phones). [See CTF: Establish illicit user access]	Mobile or transiently connected devices	Corruption, Interception	Manipulating User State-CAPEC
Exploit	Exploit known vulnerabilities in mobile systems (e.g., laptops, PDAs, smart phones). [See CTF: Establish illicit user access]	Mobile or transiently connected devices	Corruption, Interception	Parameter Injection-CAPEC
Exploit	Exploit known vulnerabilities in mobile systems (e.g., laptops, PDAs, smart phones). [See CTF: Establish illicit user access]	Mobile or transiently connected devices	Corruption, Interception	Privilege Escalation-CAPEC
Exploit	Exploit known vulnerabilities in mobile systems (e.g., laptops, PDAs, smart phones). [See CTF: Establish illicit user access]	Mobile or transiently connected devices	Corruption, Interception	Protocol Manipulation-CAPEC
Exploit	Exploit known vulnerabilities in mobile systems (e.g., laptops, PDAs, smart phones). [See CTF: Establish illicit user access]	Mobile or transiently connected devices	Corruption, Interception	Resource Injection-CAPEC
Exploit	Exploit known vulnerabilities in mobile systems (e.g., laptops, PDAs, smart phones). [See CTF: Establish illicit user access]	Mobile or transiently connected devices	Corruption, Interception	Software Integrity Attack-CAPEC
Exploit or Control	Exploit recently discovered vulnerabilities. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion, unauthorized use	

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Exploit or Control	Exploit recently discovered vulnerabilities. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion, unauthorized use	Exploit Vulnerability-ATT&CK
Exploit or Control	Exploit recently discovered vulnerabilities. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion, unauthorized use	API Manipulation-CAPEC
Exploit or Control	Exploit recently discovered vulnerabilities. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion, unauthorized use	Authentication Abuse-CAPEC
Exploit or Control	Exploit recently discovered vulnerabilities. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion, unauthorized use	Authentication Bypass-CAPEC
Exploit or Control	Exploit recently discovered vulnerabilities. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion, unauthorized use	Buffer Manipulation-CAPEC
Exploit or Control	Exploit recently discovered vulnerabilities. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion, unauthorized use	Code Inclusion-CAPEC
Exploit or Control	Exploit recently discovered vulnerabilities. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion, unauthorized use	Code Injection-CAPEC
Exploit or Control	Exploit recently discovered vulnerabilities. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion, unauthorized use	Command Injection-CAPEC
Exploit or Control	Exploit recently discovered vulnerabilities. [See ATT&CK: Lateral Movement]	Mobile or transiently connected devices	Corruption, Interception	Exploit baseband vulnerability-Mobile_ATT&CK
Exploit or Control	Exploit recently discovered vulnerabilities. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion, unauthorized use	Exploiting Trust in Client-CAPEC

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Exploit or Control	Exploit recently discovered vulnerabilities. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion, unauthorized use	Fault Injection-CAPEC
Exploit or Control	Exploit recently discovered vulnerabilities. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion, unauthorized use	Functionality Bypass-CAPEC
Exploit or Control	Exploit recently discovered vulnerabilities. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion, unauthorized use	Functionality Misuse-CAPEC
Exploit or Control	Exploit recently discovered vulnerabilities. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion, unauthorized use	Leveraging Race Conditions-CAPEC
Exploit or Control	Exploit recently discovered vulnerabilities. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion, unauthorized use	Local Execution of Code-CAPEC
Exploit or Control	Exploit recently discovered vulnerabilities. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion, unauthorized use	Malicious Logic Insertion-CAPEC
Exploit or Control	Exploit recently discovered vulnerabilities. [See ATT&CK: Lateral Movement]	Mobile or transiently connected devices	Corruption, Interception	Malicious or vulnerable built-in device functionality-Mobile_ATT&CK
Exploit or Control	Exploit recently discovered vulnerabilities. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion, unauthorized use	Manipulating User State-CAPEC
Exploit or Control	Exploit recently discovered vulnerabilities. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion, unauthorized use	Parameter Injection-CAPEC
Exploit or Control	Exploit recently discovered vulnerabilities. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion, unauthorized use	Privilege Escalation-CAPEC

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Exploit or Control	Exploit recently discovered vulnerabilities. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion, unauthorized use	Protocol Manipulation-CAPEC
Exploit or Control	Exploit recently discovered vulnerabilities. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion, unauthorized use	Resource Injection-CAPEC
Exploit or Control	Exploit recently discovered vulnerabilities. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion, unauthorized use	Software Integrity Attack-CAPEC
Control	Acquire privileges associated with a user account, process, service, or domain. [See ATT&CK: Credential Access]	Internal network, internal shared or infrastructure services	Unauthorized use	Access Token Manipulation-ATT&CK
Control	Acquire privileges associated with a user account, process, service, or domain. [See ATT&CK: Credential Access]	Internal network, internal shared or infrastructure services	Unauthorized use	Account Manipulation-ATT&CK
Control	Acquire privileges associated with a user account, process, service, or domain. [See ATT&CK: Credential Access]	Internal network, internal shared or infrastructure services	Unauthorized use	Authentication Abuse-CAPEC
Control	Acquire privileges associated with a user account, process, service, or domain. [See ATT&CK: Credential Access]	Internal network, internal shared or infrastructure services	Unauthorized use	Authentication Bypass-CAPEC
Control	Acquire privileges associated with a user account, process, service, or domain. [See ATT&CK: Credential Access]	Internal network, internal shared or infrastructure services	Unauthorized use	Brute Force-ATT&CK
Control	Acquire privileges associated with a user account, process, service, or domain. [See ATT&CK: Credential Access]	Internal network, internal shared or infrastructure services	Unauthorized use	Credential Dumping-ATT&CK

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Control	Acquire privileges associated with a user account, process, service, or domain. [See ATT&CK: Credential Access]	Internal network, internal shared or infrastructure services	Unauthorized use	Credentials in Files-ATT&CK
Control	Acquire privileges associated with a user account, process, service, or domain. [See ATT&CK: Credential Access]	Internal network, internal shared or infrastructure services	Unauthorized use	Forced Authentication-ATT&CK
Control	Acquire privileges associated with a user account, process, service, or domain. [See ATT&CK: Credential Access]	Internal network, internal shared or infrastructure services	Unauthorized use	Identity Spoofing-CAPEC
Control	Acquire privileges associated with a user account, process, service, or domain. [See ATT&CK: Credential Access]	Internal network, internal shared or infrastructure services	Unauthorized use	Input Capture-ATT&CK
Control	Acquire privileges associated with a user account, process, service, or domain. [See ATT&CK: Credential Access]	Internal network, internal shared or infrastructure services	Unauthorized use	Keychain-ATT&CK
Control	Acquire privileges associated with a user account, process, service, or domain. [See ATT&CK: Credential Access]	Internal network, internal shared or infrastructure services	Unauthorized use	LLMNR/NBT-NS Poisoning-ATT&CK
Control	Acquire privileges associated with a user account, process, service, or domain. [See ATT&CK: Credential Access]	Internal network, internal shared or infrastructure services	Unauthorized use	Manipulating User State-CAPEC
Control	Acquire privileges associated with a user account, process, service, or domain. [See ATT&CK: Credential Access]	Internal network, internal shared or infrastructure services	Unauthorized use	Network Sniffing-ATT&CK
Control	Acquire privileges associated with a user account, process, service, or domain. [See ATT&CK: Credential Access]	Internal network, internal shared or infrastructure services	Unauthorized use	Password Filter DLL-ATT&CK

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Control	Acquire privileges associated with a user account, process, service, or domain. [See ATT&CK: Credential Access]	Internal network, internal shared or infrastructure services	Unauthorized use	Private Keys-ATT&CK
Control	Acquire privileges associated with a user account, process, service, or domain. [See ATT&CK: Credential Access]	Internal network, internal shared or infrastructure services	Unauthorized use	Two-Factor Authentication Interception-ATT&CK
Control	Acquire privileges associated with a user account, process, service, or domain. [See ATT&CK: Credential Access]	Internal network, internal shared or infrastructure services	Unauthorized use	Fake Developer Accounts-Mobile_ATT&CK
Control	Acquire privileges associated with a user account, process, service, or domain. [See ATT&CK: Credential Access]	Internal network, internal shared or infrastructure services	Unauthorized use	Exploitation of Trusted Credentials-CAPEC
Control	Acquire privileges associated with a user account, process, service, or domain. [See ATT&CK: Credential Access]	Internal network, internal shared or infrastructure services	Unauthorized use	Exploiting Trust in Client-CAPEC
Control	Acquire privileges associated with a user account, process, service, or domain. [See ATT&CK: Credential Access]	Internal network, internal shared or infrastructure services	Unauthorized use	Privilege Abuse-CAPEC
Control	Acquire privileges associated with a user account, process, service, or domain. [See ATT&CK: Credential Access]	Internal network, internal shared or infrastructure services	Unauthorized use	Privilege Escalation-CAPEC
Control	Modify or increase privileges associated with a user account, process, service, or domain. [See ATT&CK: Privilege Escalation]	Internal network, internal shared or infrastructure services	Modification or Insertion	Access Token Manipulation-ATT&CK
Control	Modify or increase privileges associated with a user account, process, service, or domain. [See ATT&CK: Privilege Escalation]	Internal network, internal shared or infrastructure services	Modification or Insertion	Accessibility Features-ATT&CK

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Control	Modify or increase privileges associated with a user account, process, service, or domain. [See ATT&CK: Privilege Escalation]	Internal network, internal shared or infrastructure services	Modification or Insertion	Application Shimming-ATT&CK
Control	Modify or increase privileges associated with a user account, process, service, or domain. [See ATT&CK: Privilege Escalation]	Internal network, internal shared or infrastructure services	Modification or Insertion	Authentication Abuse-CAPEC
Control	Modify or increase privileges associated with a user account, process, service, or domain. [See ATT&CK: Privilege Escalation]	Internal network, internal shared or infrastructure services	Modification or Insertion	Authentication Bypass-CAPEC
Control	Modify or increase privileges associated with a user account, process, service, or domain. [See ATT&CK: Privilege Escalation]	Internal network, internal shared or infrastructure services	Modification or Insertion	Bypass User Account Control-ATT&CK
Control	Modify or increase privileges associated with a user account, process, service, or domain. [See ATT&CK: Privilege Escalation]	Internal network, internal shared or infrastructure services	Modification or Insertion	DLL Search Order Hijacking-ATT&CK
Control	Modify or increase privileges associated with a user account, process, service, or domain. [See ATT&CK: Privilege Escalation]	Internal network, internal shared or infrastructure services	Modification or Insertion	Exploitation of Vulnerability-ATT&CK
Control	Modify or increase privileges associated with a user account, process, service, or domain. [See ATT&CK: Privilege Escalation]	Internal network, internal shared or infrastructure services	Modification or Insertion	Extra Window Memory Injection-ATT&CK
Control	Modify or increase privileges associated with a user account, process, service, or domain. [See ATT&CK: Privilege Escalation]	Internal network, internal shared or infrastructure services	Modification or Insertion	File System Permissions Weakness-ATT&CK
Control	Modify or increase privileges associated with a user account, process, service, or domain. [See ATT&CK: Privilege Escalation]	Internal network, internal shared or infrastructure services	Modification or Insertion	Hooking-ATT&CK

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Control	Modify or increase privileges associated with a user account, process, service, or domain. [See ATT&CK: Privilege Escalation]	Internal network, internal shared or infrastructure services	Modification or Insertion	Identity Spoofing-CAPEC
Control	Modify or increase privileges associated with a user account, process, service, or domain. [See ATT&CK: Privilege Escalation]	Internal network, internal shared or infrastructure services	Modification or Insertion	Image File Execution Options Injection-ATT&CK
Control	Modify or increase privileges associated with a user account, process, service, or domain. [See ATT&CK: Privilege Escalation]	Internal network, internal shared or infrastructure services	Modification or Insertion	Launch Daemon-ATT&CK
Control	Modify or increase privileges associated with a user account, process, service, or domain. [See ATT&CK: Privilege Escalation]	Internal network, internal shared or infrastructure services	Modification or Insertion	Manipulating User State-CAPEC
Control	Modify or increase privileges associated with a user account, process, service, or domain. [See ATT&CK: Privilege Escalation]	Internal network, internal shared or infrastructure services	Modification or Insertion	New Service-ATT&CK
Control	Modify or increase privileges associated with a user account, process, service, or domain. [See ATT&CK: Privilege Escalation]	Internal network, internal shared or infrastructure services	Modification or Insertion	Path Interception-ATT&CK
Control	Modify or increase privileges associated with a user account, process, service, or domain. [See ATT&CK: Privilege Escalation]	Internal network, internal shared or infrastructure services	Modification or Insertion	Plist Modification-ATT&CK
Control	Modify or increase privileges associated with a user account, process, service, or domain. [See ATT&CK: Privilege Escalation]	Internal network, internal shared or infrastructure services	Modification or Insertion	Process Injection-ATT&CK
Control	Modify or increase privileges associated with a user account, process, service, or domain. [See ATT&CK: Privilege Escalation]	Internal network, internal shared or infrastructure services	Modification or Insertion	SID-History Injection-ATT&CK

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Control	Modify or increase privileges associated with a user account, process, service, or domain. [See ATT&CK: Privilege Escalation]	Internal network, internal shared or infrastructure services	Modification or Insertion	Service Registry Permissions Weakness-ATT&CK
Control	Modify or increase privileges associated with a user account, process, service, or domain. [See ATT&CK: Privilege Escalation]	Internal network, internal shared or infrastructure services	Modification or Insertion	Setuid and Setgid-ATT&CK
Control	Modify or increase privileges associated with a user account, process, service, or domain. [See ATT&CK: Privilege Escalation]	Internal network, internal shared or infrastructure services	Modification or Insertion	Sudo-ATT&CK
Control	Modify or increase privileges associated with a user account, process, service, or domain. [See ATT&CK: Privilege Escalation]	Internal network, internal shared or infrastructure services	Modification or Insertion	Valid Accounts-ATT&CK
Control	Modify or increase privileges associated with a user account, process, service, or domain. [See ATT&CK: Privilege Escalation]	Internal network, internal shared or infrastructure services	Modification or Insertion	Exploit OS vulnerability-Mobile_ATT&CK
Control	Modify or increase privileges associated with a user account, process, service, or domain. [See ATT&CK: Privilege Escalation]	Internal network, internal shared or infrastructure services	Modification or Insertion	Exploitation of Trusted Credentials-CAPEC
Control	Modify or increase privileges associated with a user account, process, service, or domain. [See ATT&CK: Privilege Escalation]	Internal network, internal shared or infrastructure services	Modification or Insertion	Exploiting Trust in Client-CAPEC
Control	Modify or increase privileges associated with a user account, process, service, or domain. [See ATT&CK: Privilege Escalation]	Internal network, internal shared or infrastructure services	Modification or Insertion	Privilege Abuse-CAPEC
Control	Modify or increase privileges associated with a user account, process, service, or domain. [See ATT&CK: Privilege Escalation]	Internal network, internal shared or infrastructure services	Modification or Insertion	Privilege Escalation-CAPEC

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Control	Perform internal reconnaissance. [See ATT&CK: Discovery; enabled by Install sniffer, Acquire privileges, or Modify privileges]	Internal network, internal shared or infrastructure services	Interception	Account Discovery-ATT&CK
Control	Perform internal reconnaissance. [See ATT&CK: Discovery; enabled by Install sniffer, Acquire privileges, or Modify privileges]	Internal network, internal shared or infrastructure services	Interception	Application Window Discovery-ATT&CK
Control	Perform internal reconnaissance. [See ATT&CK: Discovery; enabled by Install sniffer, Acquire privileges, or Modify privileges]	Internal network, internal shared or infrastructure services	Interception	File and Directory Discovery-ATT&CK
Control	Perform internal reconnaissance. [See ATT&CK: Discovery; enabled by Install sniffer, Acquire privileges, or Modify privileges]	Internal network, internal shared or infrastructure services	Interception	Network Service Scanning-ATT&CK
Control	Perform internal reconnaissance. [See ATT&CK: Discovery; enabled by Install sniffer, Acquire privileges, or Modify privileges]	Internal network, internal shared or infrastructure services	Interception	Network Share Discovery-ATT&CK
Control	Perform internal reconnaissance. [See ATT&CK: Discovery; enabled by Install sniffer, Acquire privileges, or Modify privileges]	Internal network, internal shared or infrastructure services	Interception	Peripheral Device Discovery-ATT&CK
Control	Perform internal reconnaissance. [See ATT&CK: Discovery; enabled by Install sniffer, Acquire privileges, or Modify privileges]	Internal network, internal shared or infrastructure services	Interception	Permission Groups Discovery-ATT&CK
Control	Perform internal reconnaissance. [See ATT&CK: Discovery; enabled by Install sniffer, Acquire privileges, or Modify privileges]	Internal network, internal shared or infrastructure services	Interception	Process Discovery-ATT&CK
Control	Perform internal reconnaissance. [See ATT&CK: Discovery; enabled by Install sniffer, Acquire privileges, or Modify privileges]	Internal network, internal shared or infrastructure services	Interception	Remote System Discovery-ATT&CK

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Control	Perform internal reconnaissance. [See ATT&CK: Discovery; enabled by Install sniffer, Acquire privileges, or Modify privileges]	Internal network, internal shared or infrastructure services	Interception	Security Software Discovery-ATT&CK
Control	Perform internal reconnaissance. [See ATT&CK: Discovery; enabled by Install sniffer, Acquire privileges, or Modify privileges]	Internal network, internal shared or infrastructure services	Interception	System Information Discovery-ATT&CK
Control	Perform internal reconnaissance. [See ATT&CK: Discovery; enabled by Install sniffer, Acquire privileges, or Modify privileges]	Internal network, internal shared or infrastructure services	Interception	System Network Configuration Discovery-ATT&CK
Control	Perform internal reconnaissance. [See ATT&CK: Discovery; enabled by Install sniffer, Acquire privileges, or Modify privileges]	Internal network, internal shared or infrastructure services	Interception	System Network Connections Discovery-ATT&CK
Control	Perform internal reconnaissance. [See ATT&CK: Discovery; enabled by Install sniffer, Acquire privileges, or Modify privileges]	Internal network, internal shared or infrastructure services	Interception	System Owner/User Discovery-ATT&CK
Control	Perform internal reconnaissance. [See ATT&CK: Discovery; enabled by Install sniffer, Acquire privileges, or Modify privileges]	Internal network, internal shared or infrastructure services	Interception	System Service Discovery-ATT&CK
Control	Perform internal reconnaissance. [See ATT&CK: Discovery; enabled by Install sniffer, Acquire privileges, or Modify privileges]	Internal network, internal shared or infrastructure services	Interception	System Time Discovery-ATT&CK
Control	Perform internal reconnaissance. [See ATT&CK: Discovery; enabled by Install sniffer, Acquire privileges, or Modify privileges]	Internal network, internal shared or infrastructure services	Interception	Discovery-Mobile_ATT&CK
Control	Perform internal reconnaissance. [See ATT&CK: Discovery; enabled by Install sniffer, Acquire privileges, or Modify privileges]	Internal network, internal shared or infrastructure services	Interception	Fingerprinting-CAPEC

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Control	Perform internal reconnaissance. [See ATT&CK: Discovery; enabled by Install sniffer, Acquire privileges, or Modify privileges]	Internal network, internal shared or infrastructure services	Interception	Footprinting-CAPEC
Control	Exploit multi-tenancy in a cloud environment. [See ATT&CK: Lateral Movement; enabled by Obtain a legitimate account]	Internal shared or infrastructure services	Corruption, Interception	Data from Network Drive - ATT&CK
Control	Exploit multi-tenancy in a cloud environment. [See ATT&CK: Lateral Movement; enabled by Obtain a legitimate account]	Internal shared or infrastructure services	Corruption, Interception	Denial of Service (resource consumption) - CSA
Control	Exploit multi-tenancy in a cloud environment. [See ATT&CK: Lateral Movement; enabled by Obtain a legitimate account]	Internal shared or infrastructure services	Corruption, Interception	Encryption Key Management - CSA
Control	Exploit multi-tenancy in a cloud environment. [See ATT&CK: Lateral Movement; enabled by Obtain a legitimate account]	Internal shared or infrastructure services	Corruption, Interception	Hypervisor-ATT&CK
Control	Exploit multi-tenancy in a cloud environment. [See ATT&CK: Lateral Movement; enabled by Obtain a legitimate account]	Internal shared or infrastructure services	Corruption, Interception	Infrastructure & Virtualization Security – Audit Logging/Intrusion Detection - CSA
Control	Exploit multi-tenancy in a cloud environment. [See ATT&CK: Lateral Movement; enabled by Obtain a legitimate account]	Internal shared or infrastructure services	Corruption, Interception	Infrastructure & Virtualization Security – Segmentation - CSA
Control	Exploit multi-tenancy in a cloud environment. [See ATT&CK: Lateral Movement; enabled by Obtain a legitimate account]	Internal shared or infrastructure services	Corruption, Interception	Network Saturation - CSA
Control	Exploit multi-tenancy in a cloud environment. [See ATT&CK: Lateral Movement; enabled by Obtain a legitimate account]	Internal shared or infrastructure services	Corruption, Interception	Obtain Device Cloud Backups-Mobile_ATT&CK

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Control	Exploit vulnerabilities on internal organizational information systems. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion, unauthorized use	Exploit Vulnerability-ATT&CK
Control	Exploit vulnerabilities on internal organizational information systems. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion, unauthorized use	API Manipulation-CAPEC
Control	Exploit vulnerabilities on internal organizational information systems. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion, unauthorized use	Authentication Abuse-CAPEC
Control	Exploit vulnerabilities on internal organizational information systems. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion, unauthorized use	Authentication Bypass-CAPEC
Control	Exploit vulnerabilities on internal organizational information systems. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion, unauthorized use	Buffer Manipulation-CAPEC
Control	Exploit vulnerabilities on internal organizational information systems. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion, unauthorized use	Code Inclusion-CAPEC
Control	Exploit vulnerabilities on internal organizational information systems. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion, unauthorized use	Code Injection-CAPEC
Control	Exploit vulnerabilities on internal organizational information systems. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion, unauthorized use	Command Injection-CAPEC
Control	Exploit vulnerabilities on internal organizational information systems. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion, unauthorized use	Exploiting Trust in Client-CAPEC

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Control	Exploit vulnerabilities on internal organizational information systems. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion, unauthorized use	Fault Injection-CAPEC
Control	Exploit vulnerabilities on internal organizational information systems. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion, unauthorized use	Functionality Bypass-CAPEC
Control	Exploit vulnerabilities on internal organizational information systems. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion, unauthorized use	Functionality Misuse-CAPEC
Control	Exploit vulnerabilities on internal organizational information systems. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion, unauthorized use	Leveraging Race Conditions-CAPEC
Control	Exploit vulnerabilities on internal organizational information systems. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion, unauthorized use	Local Execution of Code-CAPEC
Control	Exploit vulnerabilities on internal organizational information systems. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion, unauthorized use	Malicious Logic Insertion-CAPEC
Control	Exploit vulnerabilities on internal organizational information systems. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion, unauthorized use	Manipulating User State-CAPEC
Control	Exploit vulnerabilities on internal organizational information systems. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion, unauthorized use	Parameter Injection-CAPEC
Control	Exploit vulnerabilities on internal organizational information systems. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion, unauthorized use	Privilege Escalation-CAPEC

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Control	Exploit vulnerabilities on internal organizational information systems. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion, unauthorized use	Protocol Manipulation-CAPEC
Control	Exploit vulnerabilities on internal organizational information systems. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion, unauthorized use	Resource Injection-CAPEC
Control	Exploit vulnerabilities on internal organizational information systems. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion, unauthorized use	Software Integrity Attack-CAPEC
Control	Exploit vulnerabilities using zero-day attacks. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network, mobile or transiently connected devices	Corruption, Modification, or Insertion, unauthorized use	Exploit Vulnerability-ATT&CK
Control	Exploit vulnerabilities using zero-day attacks. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network, mobile or transiently connected devices	Corruption, Modification, or Insertion, unauthorized use	API Manipulation-CAPEC
Control	Exploit vulnerabilities using zero-day attacks. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network, mobile or transiently connected devices	Corruption, Modification, or Insertion, unauthorized use	Authentication Abuse-CAPEC
Control	Exploit vulnerabilities using zero-day attacks. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network, mobile or transiently connected devices	Corruption, Modification, or Insertion, unauthorized use	Authentication Bypass-CAPEC
Control	Exploit vulnerabilities using zero-day attacks. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network, mobile or transiently connected devices	Corruption, Modification, or Insertion, unauthorized use	Buffer Manipulation-CAPEC

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Control	Exploit vulnerabilities using zero-day attacks. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network, mobile or transiently connected devices	Corruption, Modification, or Insertion, unauthorized use	Code Inclusion-CAPEC
Control	Exploit vulnerabilities using zero-day attacks. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network, mobile or transiently connected devices	Corruption, Modification, or Insertion, unauthorized use	Code Injection-CAPEC
Control	Exploit vulnerabilities using zero-day attacks. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network, mobile or transiently connected devices	Corruption, Modification, or Insertion, unauthorized use	Command Injection-CAPEC
Control	Exploit vulnerabilities using zero-day attacks. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network, mobile or transiently connected devices	Corruption, Modification, or Insertion, unauthorized use	Exploiting Trust in Client-CAPEC
Control	Exploit vulnerabilities using zero-day attacks. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network, mobile or transiently connected devices	Corruption, Modification, or Insertion, unauthorized use	Fault Injection-CAPEC
Control	Exploit vulnerabilities using zero-day attacks. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network, mobile or transiently connected devices	Corruption, Modification, or Insertion, unauthorized use	Functionality Bypass-CAPEC
Control	Exploit vulnerabilities using zero-day attacks. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network, mobile or transiently connected devices	Corruption, Modification, or Insertion, unauthorized use	Functionality Misuse-CAPEC
Control	Exploit vulnerabilities using zero-day attacks. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network, mobile or transiently connected devices	Corruption, Modification, or Insertion, unauthorized use	Leveraging Race Conditions-CAPEC

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Control	Exploit vulnerabilities using zero-day attacks. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network, mobile or transiently connected devices	Corruption, Modification, or Insertion, unauthorized use	Local Execution of Code-CAPEC
Control	Exploit vulnerabilities using zero-day attacks. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network, mobile or transiently connected devices	Corruption, Modification, or Insertion, unauthorized use	Malicious Logic Insertion-CAPEC
Control	Exploit vulnerabilities using zero-day attacks. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network, mobile or transiently connected devices	Corruption, Modification, or Insertion, unauthorized use	Manipulating User State-CAPEC
Control	Exploit vulnerabilities using zero-day attacks. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network, mobile or transiently connected devices	Corruption, Modification, or Insertion, unauthorized use	Parameter Injection-CAPEC
Control	Exploit vulnerabilities using zero-day attacks. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network, mobile or transiently connected devices	Corruption, Modification, or Insertion, unauthorized use	Privilege Escalation-CAPEC
Control	Exploit vulnerabilities using zero-day attacks. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network, mobile or transiently connected devices	Corruption, Modification, or Insertion, unauthorized use	Protocol Manipulation-CAPEC
Control	Exploit vulnerabilities using zero-day attacks. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network, mobile or transiently connected devices	Corruption, Modification, or Insertion, unauthorized use	Resource Injection-CAPEC
Control	Exploit vulnerabilities using zero-day attacks. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network, mobile or transiently connected devices	Corruption, Modification, or Insertion, unauthorized use	Software Integrity Attack-CAPEC

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Control or Execute	Exploit vulnerabilities in information systems timed with organizational mission/business operations tempo.	External network connection, trusted or partner network connection, internal network	Degradation, Interruption, Corruption, Modification, or Insertion, unauthorized use	Scheduled Task-ATT&CK
Control or Execute	Exploit vulnerabilities in information systems timed with organizational mission/business operations tempo.	External network connection, trusted or partner network connection, internal network	Degradation, Interruption, Corruption, Modification, or Insertion, unauthorized use	Scheduled Transfer-ATT&CK
Control or Execute	Exploit vulnerabilities in information systems timed with organizational mission/business operations tempo.	External network connection, trusted or partner network connection, internal network	Degradation, Interruption, Corruption, Modification, or Insertion, unauthorized use	API Manipulation-CAPEC
Control or Execute	Exploit vulnerabilities in information systems timed with organizational mission/business operations tempo.	External network connection, trusted or partner network connection, internal network	Degradation, Interruption, Corruption, Modification, or Insertion, unauthorized use	Authentication Abuse-CAPEC
Control or Execute	Exploit vulnerabilities in information systems timed with organizational mission/business operations tempo.	External network connection, trusted or partner network connection, internal network	Degradation, Interruption, Corruption, Modification, or Insertion, unauthorized use	Authentication Bypass-CAPEC
Control or Execute	Exploit vulnerabilities in information systems timed with organizational mission/business operations tempo.	External network connection, trusted or partner network connection, internal network	Degradation, Interruption, Corruption, Modification, or Insertion, unauthorized use	Buffer Manipulation-CAPEC

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Control or Execute	Exploit vulnerabilities in information systems timed with organizational mission/business operations tempo.	External network connection, trusted or partner network connection, internal network	Degradation, Interruption, Corruption, Modification, or Insertion, unauthorized use	Code Inclusion-CAPEC
Control or Execute	Exploit vulnerabilities in information systems timed with organizational mission/business operations tempo.	External network connection, trusted or partner network connection, internal network	Degradation, Interruption, Corruption, Modification, or Insertion, unauthorized use	Code Injection-CAPEC
Control or Execute	Exploit vulnerabilities in information systems timed with organizational mission/business operations tempo.	External network connection, trusted or partner network connection, internal network	Degradation, Interruption, Corruption, Modification, or Insertion, unauthorized use	Command Injection-CAPEC
Control or Execute	Exploit vulnerabilities in information systems timed with organizational mission/business operations tempo.	External network connection, trusted or partner network connection, internal network	Degradation, Interruption, Corruption, Modification, or Insertion, unauthorized use	Exploiting Trust in Client-CAPEC
Control or Execute	Exploit vulnerabilities in information systems timed with organizational mission/business operations tempo.	External network connection, trusted or partner network connection, internal network	Degradation, Interruption, Corruption, Modification, or Insertion, unauthorized use	Fault Injection-CAPEC
Control or Execute	Exploit vulnerabilities in information systems timed with organizational mission/business operations tempo.	External network connection, trusted or partner network connection, internal network	Degradation, Interruption, Corruption, Modification, or Insertion, unauthorized use	Functionality Bypass-CAPEC

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Control or Execute	Exploit vulnerabilities in information systems timed with organizational mission/business operations tempo.	External network connection, trusted or partner network connection, internal network	Degradation, Interruption, Corruption, Modification, or Insertion, unauthorized use	Functionality Misuse-CAPEC
Control or Execute	Exploit vulnerabilities in information systems timed with organizational mission/business operations tempo.	External network connection, trusted or partner network connection, internal network	Degradation, Interruption, Corruption, Modification, or Insertion, unauthorized use	Leveraging Race Conditions-CAPEC
Control or Execute	Exploit vulnerabilities in information systems timed with organizational mission/business operations tempo.	External network connection, trusted or partner network connection, internal network	Degradation, Interruption, Corruption, Modification, or Insertion, unauthorized use	Local Execution of Code-CAPEC
Control or Execute	Exploit vulnerabilities in information systems timed with organizational mission/business operations tempo.	External network connection, trusted or partner network connection, internal network	Degradation, Interruption, Corruption, Modification, or Insertion, unauthorized use	Malicious Logic Insertion-CAPEC
Control or Execute	Exploit vulnerabilities in information systems timed with organizational mission/business operations tempo.	External network connection, trusted or partner network connection, internal network	Degradation, Interruption, Corruption, Modification, or Insertion, unauthorized use	Manipulating User State-CAPEC
Control or Execute	Exploit vulnerabilities in information systems timed with organizational mission/business operations tempo.	External network connection, trusted or partner network connection, internal network	Degradation, Interruption, Corruption, Modification, or Insertion, unauthorized use	Parameter Injection-CAPEC

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Control or Execute	Exploit vulnerabilities in information systems timed with organizational mission/business operations tempo.	External network connection, trusted or partner network connection, internal network	Degradation, Interruption, Corruption, Modification, or Insertion, unauthorized use	Privilege Escalation-CAPEC
Control or Execute	Exploit vulnerabilities in information systems timed with organizational mission/business operations tempo.	External network connection, trusted or partner network connection, internal network	Degradation, Interruption, Corruption, Modification, or Insertion, unauthorized use	Protocol Manipulation-CAPEC
Control or Execute	Exploit vulnerabilities in information systems timed with organizational mission/business operations tempo.	External network connection, trusted or partner network connection, internal network	Degradation, Interruption, Corruption, Modification, or Insertion, unauthorized use	Resource Injection-CAPEC
Control or Execute	Exploit vulnerabilities in information systems timed with organizational mission/business operations tempo.	External network connection, trusted or partner network connection, internal network	Degradation, Interruption, Corruption, Modification, or Insertion, unauthorized use	Software Integrity Attack-CAPEC
Control	Establish command and control (C2) channels to malware or compromised components. [See ATT&CK: Command and Control]	External network connection, trusted or partner network connection, internal network, internal shared or infrastructure services	Corruption, Modification, or Insertion, unauthorized use, Exfiltration	Commonly Used Port-ATT&CK
Control	Establish command and control (C2) channels to malware or compromised components. [See ATT&CK: Command and Control]	External network connection, trusted or partner network connection, internal network, internal shared or infrastructure services	Corruption, Modification, or Insertion, unauthorized use, Exfiltration	Communication Through Removable Media-ATT&CK
Control	Establish command and control (C2) channels to malware or compromised components. [See ATT&CK: Command and Control]	External network connection, trusted or partner network connection, internal network, internal shared or infrastructure services	Corruption, Modification, or Insertion, unauthorized use, Exfiltration	Connection Proxy-ATT&CK

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Control	Establish command and control (C2) channels to malware or compromised components. [See ATT&CK: Command and Control]	External network connection, trusted or partner network connection, internal network, internal shared or infrastructure services	Corruption, Modification, or Insertion, unauthorized use, Exfiltration	Custom Command and Control Protocol-ATT&CK
Control	Establish command and control (C2) channels to malware or compromised components. [See ATT&CK: Command and Control]	External network connection, trusted or partner network connection, internal network, internal shared or infrastructure services	Corruption, Modification, or Insertion, unauthorized use, Exfiltration	Custom Cryptographic Protocol-ATT&CK
Control	Establish command and control (C2) channels to malware or compromised components. [See ATT&CK: Command and Control]	External network connection, trusted or partner network connection, internal network, internal shared or infrastructure services	Corruption, Modification, or Insertion, unauthorized use, Exfiltration	Data Encoding-ATT&CK
Control	Establish command and control (C2) channels to malware or compromised components. [See ATT&CK: Command and Control]	External network connection, trusted or partner network connection, internal network, internal shared or infrastructure services	Corruption, Modification, or Insertion, unauthorized use, Exfiltration	Data Obfuscation-ATT&CK
Control	Establish command and control (C2) channels to malware or compromised components. [See ATT&CK: Command and Control]	External network connection, trusted or partner network connection, internal network, internal shared or infrastructure services	Corruption, Modification, or Insertion, unauthorized use, Exfiltration	Domain Fronting-ATT&CK
Control	Establish command and control (C2) channels to malware or compromised components. [See ATT&CK: Command and Control]	External network connection, trusted or partner network connection, internal network, internal shared or infrastructure services	Corruption, Modification, or Insertion, unauthorized use, Exfiltration	Fallback Channels-ATT&CK
Control	Establish command and control (C2) channels to malware or compromised components. [See ATT&CK: Command and Control]	External network connection, trusted or partner network connection, internal network, internal shared or infrastructure services	Corruption, Modification, or Insertion, unauthorized use, Exfiltration	Multi-Stage Channels-ATT&CK
Control	Establish command and control (C2) channels to malware or compromised components. [See ATT&CK: Command and Control]	External network connection, trusted or partner network connection, internal network, internal shared or infrastructure services	Corruption, Modification, or Insertion, unauthorized use, Exfiltration	Multi-hop Proxy-ATT&CK

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Control	Establish command and control (C2) channels to malware or compromised components. [See ATT&CK: Command and Control]	External network connection, trusted or partner network connection, internal network, internal shared or infrastructure services	Corruption, Modification, or Insertion, unauthorized use, Exfiltration	Multiband Communication-ATT&CK
Control	Establish command and control (C2) channels to malware or compromised components. [See ATT&CK: Command and Control]	External network connection, trusted or partner network connection, internal network, internal shared or infrastructure services	Corruption, Modification, or Insertion, unauthorized use, Exfiltration	Multilayer Encryption-ATT&CK
Control	Establish command and control (C2) channels to malware or compromised components. [See ATT&CK: Command and Control]	External network connection, trusted or partner network connection, internal network, internal shared or infrastructure services	Corruption, Modification, or Insertion, unauthorized use, Exfiltration	Remote File Copy-ATT&CK
Control	Establish command and control (C2) channels to malware or compromised components. [See ATT&CK: Command and Control]	External network connection, trusted or partner network connection, internal network, internal shared or infrastructure services	Corruption, Modification, or Insertion, unauthorized use, Exfiltration	Standard Application Layer Protocol-ATT&CK
Control	Establish command and control (C2) channels to malware or compromised components. [See ATT&CK: Command and Control]	External network connection, trusted or partner network connection, internal network, internal shared or infrastructure services	Corruption, Modification, or Insertion, unauthorized use, Exfiltration	Standard Cryptographic Protocol-ATT&CK
Control	Establish command and control (C2) channels to malware or compromised components. [See ATT&CK: Command and Control]	External network connection, trusted or partner network connection, internal network, internal shared or infrastructure services	Corruption, Modification, or Insertion, unauthorized use, Exfiltration	Standard Non-Application Layer Protocol-ATT&CK
Control	Establish command and control (C2) channels to malware or compromised components. [See ATT&CK: Command and Control]	External network connection, trusted or partner network connection, internal network, internal shared or infrastructure services	Corruption, Modification, or Insertion, unauthorized use, Exfiltration	Uncommonly Used Port-ATT&CK
Control	Establish command and control (C2) channels to malware or compromised components. [See ATT&CK: Command and Control]	External network connection, trusted or partner network connection, internal network, internal shared or infrastructure services	Corruption, Modification, or Insertion, unauthorized use, Exfiltration	Web Service-ATT&CK

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Control	Employ anti-IDS measures. [See CTF; see ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services	Modification, Insertion	Defense Evasion: various-ATT&CK
Control	Employ anti-IDS measures. [See CTF; see ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services	Modification, Insertion	Data Obfuscation-ATT&CK
Control	Employ anti-IDS measures. [See CTF; see ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services	Modification, Insertion	Obfuscated or encrypted payload-Mobile_ATT&CK
Control	Employ anti-IDS measures. [See CTF; see ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services	Modification, Insertion	Action Spoofing-CAPEC
Control	Employ anti-IDS measures. [See CTF; see ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services	Modification, Insertion	Identity Spoofing-CAPEC
Control	Employ anti-IDS measures. [See CTF; see ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services	Modification, Insertion	Protocol Manipulation-CAPEC
Control	Employ anti-IDS measures. [See CTF; see ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services	Modification, Insertion	Resource Location Spoofing-CAPEC
Control	Employ anti-forensics measures. [See CTF; see ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, internal system	Modification, Insertion	Clear Command History-ATT&CK
Control	Employ anti-forensics measures. [See CTF; see ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, internal system	Modification, Insertion	Access Token Manipulation-ATT&CK
Control	Employ anti-forensics measures. [See CTF; see ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, internal system	Modification, Insertion	Disabling security tools-ATT&CK
Control	Employ anti-forensics measures. [See CTF; see ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, internal system	Modification, Insertion	File deletion-ATT&CK
Control	Employ anti-forensics measures. [See CTF; see ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, internal system	Modification, Insertion	Indicator blocking-ATT&CK

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Control	Employ anti-forensics measures. [See CTF; see ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, internal system	Modification, Insertion	Masquerading-ATT&CK
Control	Employ anti-forensics measures. [See CTF; see ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, internal system	Modification, Insertion	Modify Registry-ATT&CK
Control	Employ anti-forensics measures. [See CTF; see ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, internal system	Modification, Insertion	Obfuscated Files or Information-ATT&CK
Control	Employ anti-forensics measures. [See CTF; see ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, internal system	Modification, Insertion	Software Packing-ATT&CK
Control	Employ anti-forensics measures. [See CTF; see ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, internal system	Modification, Insertion	Timestomp-ATT&CK
Control	Employ anti-forensics measures. [See CTF; see ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, internal system	Modification, Insertion	Defensive evasion-Mobile_ATT&CK
Control	Employ anti-forensics measures. [See CTF; see ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, internal system	Modification, Insertion	Wipe device data-Mobile_ATT&CK
Control	Employ anti-forensics measures. [See CTF; see ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, internal system	Modification, Insertion	Action Spoofing-CAPEC
Control	Employ anti-forensics measures. [See CTF; see ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, internal system	Modification, Insertion	Identity Spoofing-CAPEC
Control	Employ anti-forensics measures. [See CTF; see ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, internal system	Modification, Insertion	Protocol Manipulation-CAPEC
Control	Employ anti-forensics measures. [See CTF; see ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, internal system	Modification, Insertion	Resource Location Spoofing-CAPEC

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Control	Compromise critical information systems via physical access.	Immediate physical proximity	Degradation, InterruptionCorruption, Modification, or Insertion, Unauthorized use	Exploitation of Trusted Credentials-CAPEC
Control	Compromise critical information systems via physical access.	Immediate physical proximity	Degradation, InterruptionCorruption, Modification, or Insertion, Unauthorized use	Exploiting Trust in Client-CAPEC
Control	Compromise critical information systems via physical access.	Immediate physical proximity	Degradation, InterruptionCorruption, Modification, or Insertion, Unauthorized use	File Manipulation-CAPEC
Control	Compromise critical information systems via physical access.	Immediate physical proximity	Degradation, InterruptionCorruption, Modification, or Insertion, Unauthorized use	Functionality Bypass-CAPEC
Control	Compromise critical information systems via physical access.	Immediate physical proximity	Degradation, InterruptionCorruption, Modification, or Insertion, Unauthorized use	Hardware Integrity Attack-CAPEC
Control	Compromise critical information systems via physical access.	Immediate physical proximity	Degradation, InterruptionCorruption, Modification, or Insertion, Unauthorized use	Identity Spoofing-CAPEC

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Control	Compromise critical information systems via physical access.	Immediate physical proximity	Degradation, InterruptionCorruption, Modification, or Insertion, Unauthorized use	Local Execution of Code-CAPEC
Control	Compromise critical information systems via physical access.	Immediate physical proximity	Degradation, InterruptionCorruption, Modification, or Insertion, Unauthorized use	Manipulate Human Behavior-CAPEC
Control	Compromise critical information systems via physical access.	Immediate physical proximity	Degradation, InterruptionCorruption, Modification, or Insertion, Unauthorized use	Manipulating User State-CAPEC
Control	Compromise critical information systems via physical access.	Immediate physical proximity	Degradation, InterruptionCorruption, Modification, or Insertion, Unauthorized use	Privilege Abuse-CAPEC
Control	Compromise critical information systems via physical access.	Immediate physical proximity	Degradation, InterruptionCorruption, Modification, or Insertion, Unauthorized use	Software Integrity Attack-CAPEC
Control	Compromise organizational information systems to facilitate exfiltration of data/information. [See CTF: Relocate and store data on victim's computer, information system(s), network(s), and/or data stores]	Maintenance environment, internal network, internal shared or infrastructure services, authorized action of privileged user, device port	Corruption, Modification, or Insertion, unauthorized use, Exfiltration, Exfiltration, Interception	Exploit Enterprise Resources-Mobile_ATT&CK

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Control	Stage data for exfiltration. [See CTF: Relocate and store data on victim's computer, information system(s), network(s), and/or data stores; see ATT&CK: Collection]	Internal network, internal shared or infrastructure services, internal system	Insertion	Collection-ATT&CK
Control	Stage data for exfiltration. [See CTF: Relocate and store data on victim's computer, information system(s), network(s), and/or data stores; see ATT&CK: Collection]	Internal network, internal shared or infrastructure services, internal system	Insertion	Audio Capture-ATT&CK
Control	Stage data for exfiltration. [See CTF: Relocate and store data on victim's computer, information system(s), network(s), and/or data stores; see ATT&CK: Collection]	Internal network, internal shared or infrastructure services, internal system	Insertion	Automated Collection-ATT&CK
Control	Stage data for exfiltration. [See CTF: Relocate and store data on victim's computer, information system(s), network(s), and/or data stores; see ATT&CK: Collection]	Internal network, internal shared or infrastructure services, internal system	Insertion	Browser Extensions-ATT&CK
Control	Stage data for exfiltration. [See CTF: Relocate and store data on victim's computer, information system(s), network(s), and/or data stores; see ATT&CK: Collection]	Internal network, internal shared or infrastructure services, internal system	Insertion	Clipboard Data-ATT&CK
Control	Stage data for exfiltration. [See CTF: Relocate and store data on victim's computer, information system(s), network(s), and/or data stores; see ATT&CK: Collection]	Internal network, internal shared or infrastructure services, internal system	Insertion	Data Staged-ATT&CK
Control	Stage data for exfiltration. [See CTF: Relocate and store data on victim's computer, information system(s), network(s), and/or data stores; see ATT&CK: Collection]	Internal network, internal shared or infrastructure services, internal system	Insertion	Data from Local System-ATT&CK
Control	Stage data for exfiltration. [See CTF: Relocate and store data on victim's computer, information system(s), network(s), and/or data stores; see ATT&CK: Collection]	Internal network, internal shared or infrastructure services, internal system	Insertion	Data from Network Shared Drive-ATT&CK

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Control	Stage data for exfiltration. [See CTF: Relocate and store data on victim's computer, information system(s), network(s), and/or data stores; see ATT&CK: Collection]	Internal network, internal shared or infrastructure services, internal system	Insertion	Data from Removable Media-ATT&CK
Control	Stage data for exfiltration. [See CTF: Relocate and store data on victim's computer, information system(s), network(s), and/or data stores; see ATT&CK: Collection]	Internal network, internal shared or infrastructure services, internal system	Insertion	Email Collection-ATT&CK
Control	Stage data for exfiltration. [See CTF: Relocate and store data on victim's computer, information system(s), network(s), and/or data stores; see ATT&CK: Collection]	Internal network, internal shared or infrastructure services, internal system	Insertion	Input Capture-ATT&CK
Control	Stage data for exfiltration. [See CTF: Relocate and store data on victim's computer, information system(s), network(s), and/or data stores; see ATT&CK: Collection]	Internal network, internal shared or infrastructure services, internal system	Insertion	Man in the Browser-ATT&CK
Control	Stage data for exfiltration. [See CTF: Relocate and store data on victim's computer, information system(s), network(s), and/or data stores; see ATT&CK: Collection]	Internal network, internal shared or infrastructure services, internal system	Insertion	Screen Capture-ATT&CK
Control	Stage data for exfiltration. [See CTF: Relocate and store data on victim's computer, information system(s), network(s), and/or data stores; see ATT&CK: Collection]	Internal network, internal shared or infrastructure services, internal system	Insertion	Video Capture-ATT&CK
Control	Compromise information critical to mission / business functions.	Internal network, internal shared or infrastructure services, authorized action of non-privileged user, authorized action of privileged user, device port, data	Corruption, Modification, or Insertion	Exploitation of Trusted Credentials-CAPEC

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Control	Compromise information critical to mission / business functions.	Internal network, internal shared or infrastructure services, authorized action of non-privileged user, authorized action of privileged user, device port, data	Corruption, Modification, or Insertion	Exploiting Trust in Client-CAPEC
Control	Compromise information critical to mission / business functions.	Internal network, internal shared or infrastructure services, authorized action of non-privileged user, authorized action of privileged user, device port, data	Corruption, Modification, or Insertion	File Manipulation-CAPEC
Control	Compromise information critical to mission / business functions.	Internal network, internal shared or infrastructure services, authorized action of non-privileged user, authorized action of privileged user, device port, data	Corruption, Modification, or Insertion	Functionality Bypass-CAPEC
Control	Compromise information critical to mission / business functions.	Internal network, internal shared or infrastructure services, authorized action of non-privileged user, authorized action of privileged user, device port, data	Corruption, Modification, or Insertion	Hardware Integrity Attack-CAPEC
Control	Compromise information critical to mission / business functions.	Internal network, internal shared or infrastructure services, authorized action of non-privileged user, authorized action of privileged user, device port, data	Corruption, Modification, or Insertion	Identity Spoofing-CAPEC
Control	Compromise information critical to mission / business functions.	Internal network, internal shared or infrastructure services, authorized action of non-privileged user, authorized action of privileged user, device port, data	Corruption, Modification, or Insertion	Local Execution of Code-CAPEC

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Control	Compromise information critical to mission / business functions.	Internal network, internal shared or infrastructure services, authorized action of non-privileged user, authorized action of privileged user, device port, data	Corruption, Modification, or Insertion	Manipulate Human Behavior-CAPEC
Control	Compromise information critical to mission / business functions.	Internal network, internal shared or infrastructure services, authorized action of non-privileged user, authorized action of privileged user, device port, data	Corruption, Modification, or Insertion	Manipulating User State-CAPEC
Control	Compromise information critical to mission / business functions.	Internal network, internal shared or infrastructure services, authorized action of non-privileged user, authorized action of privileged user, device port, data	Corruption, Modification, or Insertion	Privilege Abuse-CAPEC
Control	Compromise information critical to mission / business functions.	Internal network, internal shared or infrastructure services, authorized action of non-privileged user, authorized action of privileged user, device port, data	Corruption, Modification, or Insertion	Software Integrity Attack-CAPEC
Execute	Obtain sensitive information through network sniffing of external networks. [See ATT&CK: Collection]	External network connection, trusted or partner network connection	Interception	Network Sniffing-ATT&CK
Execute	Obtain sensitive information through network sniffing of external networks. [See ATT&CK: Collection]	External network connection, trusted or partner network connection	Interception	Exploit Baseband Vulnerability-Mobile_ATT&CK
Execute	Obtain sensitive information through network sniffing of external networks. [See ATT&CK: Collection]	External network connection, trusted or partner network connection	Interception	Rogue Cellular Base Station-Mobile_ATT&CK
Execute	Obtain sensitive information through network sniffing of external networks. [See ATT&CK: Collection]	External network connection, trusted or partner network connection	Interception	Rogue WIFI Access Points-Mobile_ATT&CK

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Execute	Obtain sensitive information through network sniffing of external networks. [See ATT&CK: Collection]	External network connection, trusted or partner network connection	Interception	Exploit SS7 to redirect phonecalls and SMS-Mobile_ATT&CK
Execute	Cause degradation or denial of attacker-selected services or capabilities. [See CTF: Deny access]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Degradation, Interruption	Jamming or Denial of Service-Mobile_ATT&CK
Execute	Cause degradation or denial of attacker-selected services or capabilities. [See CTF: Deny access]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Degradation, Interruption	Flooding-CAPEC
Execute	Cause degradation or denial of attacker-selected services or capabilities. [See CTF: Deny access]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Degradation, Interruption	Obstruction-CAPEC
Execute	Cause degradation or denial of attacker-selected services or capabilities. [See CTF: Deny access]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Degradation, Interruption	Protocol Manipulation-CAPEC
Execute	Cause deterioration/ destruction of critical information system components and functions. [See CTF: Destroy hardware / software / data]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Degradation, Interruption	File Manipulation-CAPEC
Execute	Cause deterioration/ destruction of critical information system components and functions. [See CTF: Destroy hardware / software / data]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Degradation, Interruption	Hardware Integrity Attack-CAPEC
Execute	Cause deterioration/ destruction of critical information system components and functions. [See CTF: Destroy hardware / software / data]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Degradation, Interruption	Software Integrity Attack-CAPEC
Execute	Cause integrity loss by creating, deleting, and/or modifying data on publicly accessible information systems (e.g., web defacement).	External network	Corruption, Modification, or Insertion	Wipe Device Data-Mobile_ATT&CK

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Execute	Cause integrity loss by creating, deleting, and/or modifying data on publicly accessible information systems (e.g., web defacement).	External network	Corruption, Modification, or Insertion	File Manipulation-CAPEC
Execute	Cause integrity loss by polluting or corrupting critical data. [See CTF: Alter data on the victim's system(s)]	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, data	Corruption, Modification	Action Spoofing-CAPEC
Execute	Cause integrity loss by polluting or corrupting critical data. [See CTF: Alter data on the victim's system(s)]	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, data	Corruption, Modification	Content Spoofing-CAPEC
Execute	Cause integrity loss by polluting or corrupting critical data. [See CTF: Alter data on the victim's system(s)]	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, data	Corruption, Modification	Fault Injection-CAPEC
Execute	Cause integrity loss by polluting or corrupting critical data. [See CTF: Alter data on the victim's system(s)]	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, data	Corruption, Modification	Identity Spoofing-CAPEC
Execute	Cause integrity loss by polluting or corrupting critical data. [See CTF: Alter data on the victim's system(s)]	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, data	Corruption, Modification	Parameter Injection-CAPEC
Execute	Cause integrity loss by polluting or corrupting critical data. [See CTF: Alter data on the victim's system(s)]	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, data	Corruption, Modification	Resource Injection-CAPEC

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Execute	Cause integrity loss by polluting or corrupting critical data. [See CTF: Alter data on the victim's system(s)]	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, data	Corruption, Modification	Resource Location Spoofing-CAPEC
Execute	Cause integrity loss by polluting or corrupting critical data. [See CTF: Alter data on the victim's system(s)]	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, data	Corruption, Modification	Traffic Injection-CAPEC
Execute	Cause integrity loss by injecting false but believable data into organizational information systems.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, data	Insertion	Action Spoofing-CAPEC
Execute	Cause integrity loss by injecting false but believable data into organizational information systems.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, data	Insertion	Content Spoofing-CAPEC
Execute	Cause integrity loss by injecting false but believable data into organizational information systems.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, data	Insertion	Fault Injection-CAPEC
Execute	Cause integrity loss by injecting false but believable data into organizational information systems.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, data	Insertion	Identity Spoofing-CAPEC

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Execute	Cause integrity loss by injecting false but believable data into organizational information systems.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, data	Insertion	Parameter Injection-CAPEC
Execute	Cause integrity loss by injecting false but believable data into organizational information systems.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, data	Insertion	Resource Injection-CAPEC
Execute	Cause integrity loss by injecting false but believable data into organizational information systems.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, data	Insertion	Resource Location Spoofing-CAPEC
Execute	Cause integrity loss by injecting false but believable data into organizational information systems.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, data	Insertion	Traffic Injection-CAPEC
Execute	Reduce or deny availability by jamming communications.	External network, trusted or partner network connection, internal network	Degradation, Interruption	Jamming or denial of service-Mobile_ATT&CK
Execute	Reduce or deny availability by jamming communications.	External network, trusted or partner network connection, internal network	Degradation, Interruption	Flooding-CAPEC
Execute	Reduce or deny availability by jamming communications.	External network, trusted or partner network connection, internal network	Degradation, Interruption	Obstruction-CAPEC
Execute	Transmit sensitive information from the internal network to an external destination covertly. [See CTF: Exfiltrate data / information and ATT&CK: Exfiltration]	External network, trusted or partner network connection, internal network	Exfiltration	Commonly Used Port-ATT&CK

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Execute	Transmit sensitive information from the internal network to an external destination covertly. [See CTF: Exfiltrate data / information and ATT&CK: Exfiltration]	External network, trusted or partner network connection, internal network	Exfiltration	Communication Through Removable Media-ATT&CK
Execute	Transmit sensitive information from the internal network to an external destination covertly. [See CTF: Exfiltrate data / information and ATT&CK: Exfiltration]	External network, trusted or partner network connection, internal network	Exfiltration	Connection Proxy-ATT&CK
Execute	Transmit sensitive information from the internal network to an external destination covertly. [See CTF: Exfiltrate data / information and ATT&CK: Exfiltration]	External network, trusted or partner network connection, internal network	Exfiltration	Custom Command and Control Protocol-ATT&CK
Execute	Transmit sensitive information from the internal network to an external destination covertly. [See CTF: Exfiltrate data / information and ATT&CK: Exfiltration]	External network, trusted or partner network connection, internal network	Exfiltration	Custom Cryptographic Protocol-ATT&CK
Execute	Transmit sensitive information from the internal network to an external destination covertly. [See CTF: Exfiltrate data / information and ATT&CK: Exfiltration]	External network, trusted or partner network connection, internal network	Exfiltration	Data Encoding-ATT&CK
Execute	Transmit sensitive information from the internal network to an external destination covertly. [See CTF: Exfiltrate data / information and ATT&CK: Exfiltration]	External network, trusted or partner network connection, internal network	Exfiltration	Data Obfuscation-ATT&CK
Execute	Transmit sensitive information from the internal network to an external destination covertly. [See CTF: Exfiltrate data / information and ATT&CK: Exfiltration]	External network, trusted or partner network connection, internal network	Exfiltration	Domain Fronting-ATT&CK
Execute	Transmit sensitive information from the internal network to an external destination covertly. [See CTF: Exfiltrate data / information and ATT&CK: Exfiltration]	External network, trusted or partner network connection, internal network	Exfiltration	Fallback Channels-ATT&CK

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Execute	Transmit sensitive information from the internal network to an external destination covertly. [See CTF: Exfiltrate data / information and ATT&CK: Exfiltration]	External network, trusted or partner network connection, internal network	Exfiltration	Multi-Stage Channels-ATT&CK
Execute	Transmit sensitive information from the internal network to an external destination covertly. [See CTF: Exfiltrate data / information and ATT&CK: Exfiltration]	External network, trusted or partner network connection, internal network	Exfiltration	Multi-hop Proxy-ATT&CK
Execute	Transmit sensitive information from the internal network to an external destination covertly. [See CTF: Exfiltrate data / information and ATT&CK: Exfiltration]	External network, trusted or partner network connection, internal network	Exfiltration	Multiband Communication-ATT&CK
Execute	Transmit sensitive information from the internal network to an external destination covertly. [See CTF: Exfiltrate data / information and ATT&CK: Exfiltration]	External network, trusted or partner network connection, internal network	Exfiltration	Multilayer Encryption-ATT&CK
Execute	Transmit sensitive information from the internal network to an external destination covertly. [See CTF: Exfiltrate data / information and ATT&CK: Exfiltration]	External network, trusted or partner network connection, internal network	Exfiltration	Remote File Copy-ATT&CK
Execute	Transmit sensitive information from the internal network to an external destination covertly. [See CTF: Exfiltrate data / information and ATT&CK: Exfiltration]	External network, trusted or partner network connection, internal network	Exfiltration	Standard Application Layer Protocol-ATT&CK
Execute	Transmit sensitive information from the internal network to an external destination covertly. [See CTF: Exfiltrate data / information and ATT&CK: Exfiltration]	External network, trusted or partner network connection, internal network	Exfiltration	Standard Cryptographic Protocol-ATT&CK
Execute	Transmit sensitive information from the internal network to an external destination covertly. [See CTF: Exfiltrate data / information and ATT&CK: Exfiltration]	External network, trusted or partner network connection, internal network	Exfiltration	Standard Non-Application Layer Protocol-ATT&CK

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Execute	Transmit sensitive information from the internal network to an external destination covertly. [See CTF: Exfiltrate data / information and ATT&CK: Exfiltration]	External network, trusted or partner network connection, internal network	Exfiltration	Uncommonly Used Port-ATT&CK
Execute	Transmit sensitive information from the internal network to an external destination covertly. [See CTF: Exfiltrate data / information and ATT&CK: Exfiltration]	External network, trusted or partner network connection, internal network	Exfiltration	Web Service-ATT&CK
Execute	Transmit sensitive information from the internal network to an external destination covertly. [See CTF: Exfiltrate data / information and ATT&CK: Exfiltration]	External network, trusted or partner network connection, internal network	Exfiltration	Exfiltration-Mobile_ATT&CK
Execute	Inject crafted network traffic.	External network, trusted or partner network connection, internal network	Corruption, Modification, or Insertion	Traffic Injection-CAPEC
Execute	Transmit messages to a targeted range of perimeter network addresses to deny service.	External network, trusted or partner network connection	Degradation, Interruption	Jamming or Denial of Service-Mobile_ATT&CK
Execute	Transmit messages to a targeted range of perimeter network addresses to deny service.	External network, trusted or partner network connection	Degradation, Interruption	Flooding-CAPEC
Execute	Transmit messages to a targeted range of perimeter network addresses to deny service.	External network, trusted or partner network connection	Degradation, Interruption	Obstruction-CAPEC
Execute	Download sensitive information to information systems or devices used externally and reintroduced into the enterprise.	Internal network	Exfiltration, Interception	Removable Media-ATT&CK
Execute	Obtain information by externally-located interception of wireless network traffic.	Internal network	Interception	Network Sniffing-ATT&CK
Execute	Obtain information by externally-located interception of wireless network traffic.	Internal network	Interception	Rogue WIFI access points-Mobile_ATT&CK

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Execute	Obtain information by externally-located interception of wireless network traffic.	Internal network	Interception	Rogue Cellular Access Points-Mobile_ATT&CK
Execute	Obtain unauthorized access.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, social engineering	Unauthorized use	Account Manipulation-ATT&CK
Execute	Obtain unauthorized access.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, social engineering	Unauthorized use	Brute Force-ATT&CK
Execute	Obtain unauthorized access.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, social engineering	Unauthorized use	Credential Dumping-ATT&CK
Execute	Obtain unauthorized access.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, social engineering	Unauthorized use	Credentials in Files-ATT&CK
Execute	Obtain unauthorized access.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, social engineering	Unauthorized use	Forced Authentication-ATT&CK
Execute	Obtain unauthorized access.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, social engineering	Unauthorized use	Input Capture-ATT&CK

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Execute	Obtain unauthorized access.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, social engineering	Unauthorized use	Compromise Password Vault-ATT&CK
Execute	Obtain unauthorized access.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, social engineering	Unauthorized use	Network Sniffing-ATT&CK
Execute	Obtain unauthorized access.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, social engineering	Unauthorized use	Password Filter DLL-ATT&CK
Execute	Obtain unauthorized access.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, social engineering	Unauthorized use	Private Keys-ATT&CK
Execute	Obtain unauthorized access.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, social engineering	Unauthorized use	Two-Factor Authentication Interception-ATT&CK
Execute	Obtain unauthorized access.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, social engineering	Unauthorized use	Authentication Abuse-CAPEC

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Execute	Obtain unauthorized access.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, social engineering	Unauthorized use	Authentication Bypass-CAPEC
Execute	Obtain unauthorized access.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, social engineering	Unauthorized use	Brute Force-CAPEC
Execute	Obtain unauthorized access.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, social engineering	Unauthorized use	Bypassing Physical Security-CAPEC
Execute	Obtain unauthorized access.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, social engineering	Unauthorized use	Code Inclusion-CAPEC
Execute	Obtain unauthorized access.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, social engineering	Unauthorized use	Code Injection-CAPEC
Execute	Obtain unauthorized access.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, social engineering	Unauthorized use	Command Injection-CAPEC

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Execute	Obtain unauthorized access.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, social engineering	Unauthorized use	Communication Channel Manipulation-CAPEC
Execute	Obtain unauthorized access.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, social engineering	Unauthorized use	Configuration/Environment Manipulation-CAPEC
Execute	Obtain unauthorized access.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, social engineering	Unauthorized use	Exploitation of Trusted Credentials-CAPEC
Execute	Obtain unauthorized access.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, social engineering	Unauthorized use	Exploiting Trust in Client-CAPEC
Execute	Obtain unauthorized access.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, social engineering	Unauthorized use	File Manipulation-CAPEC
Execute	Obtain unauthorized access.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, social engineering	Unauthorized use	Functionality Bypass-CAPEC

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Execute	Obtain unauthorized access.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, social engineering	Unauthorized use	Functionality Misuse-CAPEC
Execute	Obtain unauthorized access.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, social engineering	Unauthorized use	Hardware Integrity Attack-CAPEC
Execute	Obtain unauthorized access.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, social engineering	Unauthorized use	Identity Spoofing-CAPEC
Execute	Obtain unauthorized access.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, social engineering	Unauthorized use	Input Data Manipulation-CAPEC
Execute	Obtain unauthorized access.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, social engineering	Unauthorized use	Leveraging Race Conditions-CAPEC
Execute	Obtain unauthorized access.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, social engineering	Unauthorized use	Malicious Logic Insertion-CAPEC

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Execute	Obtain unauthorized access.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, social engineering	Unauthorized use	Manipulate Human Behavior-CAPEC
Execute	Obtain unauthorized access.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, social engineering	Unauthorized use	Parameter Injection-CAPEC
Execute	Obtain unauthorized access.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, social engineering	Unauthorized use	Privilege Abuse-CAPEC
Execute	Obtain unauthorized access.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, social engineering	Unauthorized use	Privilege Escalation-CAPEC
Execute	Obtain unauthorized access.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, social engineering	Unauthorized use	Protocol Manipulation-CAPEC
Execute	Obtain unauthorized access.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, social engineering	Unauthorized use	Resource Injection-CAPEC

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Execute	Obtain unauthorized access.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, social engineering	Unauthorized use	Software Integrity Attack-CAPEC
Execute	Obtain unauthorized access.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, social engineering	Unauthorized use	Traffic Injection-CAPEC
Execute	Obtain sensitive data/information from publicly accessible information systems.	External network	Exfiltration, Interception	Exploit Vulnerability-ATT&CK
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Access Token Manipulation-ATT&CK
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Binary Padding-ATT&CK
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Bypass User Account Control-ATT&CK
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Clear Command History-ATT&CK
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Code Signing-ATT&CK
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Component Firmware-ATT&CK

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Component Object Model Hijacking-ATT&CK
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	DLL Search Order Hijacking-ATT&CK
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	DLL Side-Loading-ATT&CK
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Deobfuscate/Decode Files or Information-ATT&CK
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Disabling Security Tools-ATT&CK
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Exploitation of Vulnerability-ATT&CK
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Extra Window Memory Injection-ATT&CK
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	File Deletion-ATT&CK
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	File System Logical Offsets-ATT&CK

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Gatekeeper Bypass-ATT&CK
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	HISTCONTROL-ATT&CK
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Hidden Files and Directories-ATT&CK
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Hidden Users-ATT&CK
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Hidden Window-ATT&CK
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Image File Execution Options Injection-ATT&CK
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Indicator Blocking-ATT&CK
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Indicator Removal from Tools-ATT&CK
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Indicator Removal on Host-ATT&CK

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Install Root Certificate-ATT&CK
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	InstallUtil-ATT&CK
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Masquerading-ATT&CK
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Modify Registry-ATT&CK
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Mshta-ATT&CK
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	NTFS Extended Attributes-ATT&CK
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Network Share Connection Removal-ATT&CK
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Obfuscated Files or Information-ATT&CK
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Plist Modification-ATT&CK

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Process Doppelganging-ATT&CK
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Process Hollowing-ATT&CK
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Process Injection-ATT&CK
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Redundant Access-ATT&CK
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Regsvcs/Regasm-ATT&CK
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Regsvr32-ATT&CK
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Rootkit-ATT&CK
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Rundll32-ATT&CK
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Scripting-ATT&CK

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Software Packing-ATT&CK
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Space after Filename-ATT&CK
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Timestomp-ATT&CK
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Trusted Developer Utilities-ATT&CK
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Valid Accounts-ATT&CK
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Defensive evasion-Mobile_ATT&CK
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Action Spoofing-CAPEC
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Content Spoofing-CAPEC
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Fault Injection-CAPEC

CAL Stage	High-Level Threat Event	Attack Vector	Cyber Effect	Detailed Threat Event and Source
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Identity Spoofing-CAPEC
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Parameter Injection-CAPEC
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Resource Injection-CAPEC
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Resource Location Spoofing-CAPEC
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Traffic Injection-CAPEC

Appendix B External Threat Events

Adversary activities prior to compromise of a defended system are largely executed outside the enterprise's field of view. This appendix catalogs additional threat events excluded from the expanded threat model because they do not directly interact with the defended system or its communications and therefore cannot be detected or mitigated by cyber defense technologies implemented within the system. They represent attacker activities that are not direct actions against technology assets but are instead executed during the attack planning and preparation phase to gather information about potential targets.

These events can be used to inform an enterprise's efforts to understand and minimize information about the organization and its systems that is available from external or public sources and would be useful to adversaries in planning an attack.

The external threat events are listed in Table 7. These events are taken from the PRE-ATT&CK repository [MITRE 2016b]. In the table, the "Tactics" column includes categories of events that take place externally to the system. Each of these categories is further characterized as to the cyber attack lifecycle stage in which it is likely to be used. The "Techniques" column identifies more specific threat behaviors that can be used to carry out that tactic.

Table 7. External Threat Events

CAL Stage	Tactics	Techniques
Target Identification	Priority Definition Planning	Assess Key Intelligence Topics (KIT)s/Key Intelligence Questions (KIQ)s benefits
Target Identification	Priority Definition Planning	Assess current holdings, needs, and wants
Target Identification	Priority Definition Planning	Assess leadership areas of interest
Target Identification	Priority Definition Planning	Assign Key Intelligence Topics (KIT)s/Key Intelligence Questions (KIQ)s into categories
Target Identification	Priority Definition Planning	Conduct cost/benefit analysis
Target Identification	Priority Definition Planning	Create implementation plan
Target Identification	Priority Definition Planning	Create strategic plan
Target Identification	Priority Definition Planning	Derive intelligence requirements
Target Identification	Priority Definition Planning	Develop Key Intelligence Topics (KIT)s/Key Intelligence Questions (KIQ)s
Target Identification	Priority Definition Planning	Generate analyst intelligence requirements
Target Identification	Priority Definition Planning	Identify analyst level gaps
Target Identification	Priority Definition Planning	Identify gap areas
Target Identification	Priority Definition Planning	Receive operator Key Intelligence Topics (KIT)s/Key Intelligence Questions (KIQ)s tasking
Target Identification	Priority Definition Direction	Assign Key Intelligence Topics (KIT)s, Key Intelligence Questions (KIQ)s, and/or intelligence requirements
Target Identification	Priority Definition Direction	Receive Key Intelligence Topics (KIT)s/Key Intelligence Questions (KIQ)s and determine requirements
Target Identification	Priority Definition Direction	Submit Key Intelligence Topics (KIT)s, Key Intelligence Questions (KIQ)s, and intelligence requirements

CAL Stage	Tactics	Techniques
Target Identification	Priority Definition Direction	Task requirements
Target Identification	Target Selection	Determine approach/attack vector
Target Identification	Target Selection	Determine highest level tactical element
Target Identification	Target Selection	Determine operational element
Target Identification	Target Selection	Determine secondary level tactical element
Target Identification	Target Selection	Determine strategic target
Recon	Technical Information Gathering	Acquire open source intelligence (OSINT) data sets and information
Recon	Technical Information Gathering	Discover target logon/email address format
Recon	Technical Information Gathering	Identify job postings and needs/gaps
Recon	Technical Information Gathering	Identify supply chains
Recon	Technical Information Gathering	Identify web defensive services
Recon	Technical Information Gathering	Mine technical blogs/forums
Recon	Technical Information Gathering	Obtain domain/IP registration information
Recon	People Information Gathering	Aggregate individual's digital footprint
Recon	People Information Gathering	Conduct social engineering
Recon	People Information Gathering	Identify business relationships
Recon	People Information Gathering	Identify groups/roles
Recon	People Information Gathering	Identify job postings and needs/gaps
Recon	People Information Gathering	Identify people of interest
Recon	People Information Gathering	Identify personnel with an authority/privilege
Recon	People Information Gathering	Identify sensitive personnel information
Recon	Organizational Information Gathering	Mine social media
Recon	Organizational Information Gathering	Conduct social engineering
Recon	Organizational Information Gathering	Determine 3rd party infrastructure services
Recon	Organizational Information Gathering	Determine centralization of IT management
Recon	Organizational Information Gathering	Determine physical locations
Recon	Organizational Information Gathering	Dumpster dive
Recon	Organizational Information Gathering	Identify business processes/tempo
Recon	Organizational Information Gathering	Identify business relationships
Recon	Organizational Information Gathering	Identify job postings and needs/gaps
Recon		Obtain templates/branding materials
Weaponize	Build Capabilities	Build and configure delivery systems
Weaponize	Build Capabilities	Build or acquire exploits
Weaponize	Build Capabilities	C2 protocol development
Weaponize	Build Capabilities	Compromise 3rd party or closed-source vulnerability/exploit information
Weaponize	Build Capabilities	Create custom payloads
Weaponize	Build Capabilities	Discover new exploits and monitor exploit-provider forums

CAL Stage	Tactics	Techniques
Weaponize	Build Capabilities	Identify resources required to build capabilities
Weaponize	Build Capabilities	Obtain/re-use payloads
Weaponize	Build Capabilities	Post compromise tool development
Weaponize	Build Capabilities	Remote access tool development

Appendix C Scenario Building Blocks

Table 8 provides a representative set of scenario building blocks. In the table, the "Approach" and "Typical High-Level Events" columns are taken from the example scenario building blocks in [Bodeau 2018]. The "Scenario Component" column is added to explain the attacker's goal and approach in more detail, while the "Detailed Threat Events" column cites specific threat events from the expanded threat model that could be used to carry them out.

For several rows, detailed threat events did not exist because they were outside the scope of the work (e.g. Physical Access) or are not represented in the ATT&CK, CAPEC, or other event sources. Those rows are noted with "*" in last two columns.

Table 8. Scenario Building Blocks Using Threat Events

Approach	Typical High-Level Events	Scenario Component	Detailed Threat Events
Conduct communications interception attacks.	Perform perimeter network reconnaissance/scanning.	Adversary identifies hosts that are trusted by the target domain by monitoring network communications.	Determine external network trust dependencies-PRE-ATT&CK
		Adversary identifies the formats of target accounts and email addresses in the victim environment by monitoring network communications and analyzing unencrypted traffic.	Discover target logon/email address format-PRE-ATT&CK
		Adversary identifies the configuration of servers and/or clients by analyzing protocol usage and anomalies observed by recording live network traffic.	Enumerate client configurations-PRE-ATT&CKEnumerate externally facing software applications technologies, languages, and dependencies-PRE-ATT&CK
Conduct attacks using unauthorized ports, protocols and services.	Perform perimeter network reconnaissance/scanning. Perform network sniffing of exposed networks.	Adversary scans network to identify available services to start identifying the potential attack surface	Conduct active scanning-PRE-ATT&CK Conduct passive scanning-PRE-ATT&CK

Approach	Typical High-Level Events	Scenario Component	Detailed Threat Events
	Exploit poorly configured or unauthorized information systems exposed to the internet.	Adversary attacks and compromises one or more identified vulnerable services through an overflow or injection attack.	Exploit Vulnerability-ATT&CK Buffer Manipulation-CAPEC Code Injection-CAPEC Input Data Manipulation-CAPEC Parameter Injection-CAPEC Privilege Escalation-CAPEC
Conduct attacks leveraging traffic / data movement allowed across perimeter.	Establish command and control (C2) channels to malware or compromised components. Compromise organizational information systems to facilitate exfiltration of data/information. Cause disclosure of critical and/or sensitive information by authorized users. *Or* Cause unauthorized disclosure and/or unavailability by spilling sensitive information. *Or* Transmit sensitive information from the internal network to an external destination covertly.	Adversary implants a Remote Access Tool (RAT) on a target desktop inside of the perimeter after compromising the system. The desktop then phones home via the company's own outbound web proxy to receive further instructions, enabling the adversary to operate within the company WAN.	Connection Proxy-ATT&CK Data Encoding-ATT&CK Data Obfuscation-ATT&CK Domain Fronting-ATT&CK Standard Application Layer Protocol-ATT&CK Standard Cryptographic Protocol-ATT&CK Web Service-ATT&CK
		Adversary finds a dataset containing proprietary information and transmits it to an external site on the internet.	Connection Proxy-ATT&CK Data Encoding-ATT&CK Domain Fronting-ATT&CK Standard Application Layer Protocol-ATT&CK Standard Cryptographic Protocol-ATT&CK Web Service-ATT&CK
Conduct Distributed Denial of Service (DDoS) attacks.	Perform perimeter network reconnaissance/scanning. Transmit messages to a targeted range of perimeter network addresses to deny service.	Adversary performs a SYN flood to overwhelm the webservers of the target company.	Flooding-CAPEC
		Adversary attacks the web application of the target company, overwhelming its search function by passing high volumes of queries that will produce empty results	Flooding-CAPEC

Approach	Typical High-Level Events	Scenario Component	Detailed Threat Events
Conduct targeted Denial of Service (DoS) attacks.	Install persistent and targeted sniffers on organizational information systems and networks. Cause degradation or denial of attacker-selected services or capabilities.	*	*
Conduct physical attacks on organizational facilities.[14]	(depends on physical characteristics of organizational facilities)	*	*
Conduct physical attacks on infrastructures supporting organizational facilities.[15]	(depends on physical characteristics of supporting infrastructures)	*	*
Conduct cyber-physical attacks on organizational facilities.[15]	(depends on cyber-physical characteristics of organizational facilities)	Example: Adversary attacks the data center of the target company by gaining access to the facility through impersonation as a repair technician of 3rd party contractor, and damages heating, ventilation, and air conditioning (HVAC) equipment, causing overheating.	Human performs requested action of physical nature-PRE-ATT&CK Manipulate Human Behavior-CAPEC Information Elicitation-CAPEC Bypassing Physical Security-CAPEC
Conduct data scavenging attacks in a cloud environment.	Establish command and control (C2) channels to malware or compromised components. Exploit insecure or incomplete data deletion in multi-tenant environment. *Or* Violate isolation in multi-tenant environment.	*	*

[14] Physical attacks are outside the scope of this report; however, physical attacks on organizational facilities or supporting infrastructures can have denial-of-service effects from the cyber perspective through the destruction of components of the IT system.

[15] While a detailed treatment of threat events on IT systems via their cyber-physical aspects and dependencies is beyond the scope of this report, this high-level event is included to indicate the potential for such events in general.

Approach	Typical High-Level Events	Scenario Component	Detailed Threat Events
Conduct brute force login attempts/password guessing attacks.	Establish or use a communications channel to the enterprise as a whole or to a targeted system. Deliver commands to a targeted system (e.g., login).	Adversary gains access to endpoint system through a RAT tool, email user names are used throughout the enterprise for business process applications. Using a script all IDs are tried for two common passwords, gaining access to several accounts.	Brute Force-ATT&CK Credential Dumping-ATT&CK Identity Spoofing-CAPEC Privilege Escalation-CAPEC
Conduct non-targeted zero-day attacks.	(Depends on the enterprise architecture)	*	*
Conduct externally-based session hijacking.	Perform network sniffing of exposed networks.	*	*
Conduct internally-based session hijacking.	Perform network sniffing of exposed networks. *Or* Perform malware-directed internal reconnaissance.	*	*
Conduct externally-based network traffic modification (man in the middle) attacks.	Perform network sniffing of external networks (e.g., ISPs) to which organizational networks are connected. Analyze network traffic based on network sniffing. Inject crafted network traffic.	*	*
Conduct internally-based network traffic modification (man in the middle) attacks.	Analyze network traffic based on network sniffing. Inject crafted network traffic.	Adversary gains access to network and uses a packet capture tool to reconstruct an application DB call, then, using replayable API identity assertion, reads customer PII records to unauthorized data store.	Protocol Manipulation-CAPEC API Manipulation-CAPEC Authentication Abuse-CAPEC Command Injection-CAPEC Collection-ATT&CK

Approach	Typical High-Level Events	Scenario Component	Detailed Threat Events
Conduct outsider-based social engineering to obtain information.	Gather information using open source discovery of organizational information. Craft psychological manipulation attacks on key staff.	Adversary uses social media business connection site to identify employees of the financial staff of target company through professional associations, sends forged legal documents for information on company bank relationships.	Acquire OSINT data sets and information-PRE-ATT&CK Aggregate individual's digital footprint-PRE-ATT&CK Conduct social engineering-PRE-ATT&CK Identify business relationships-PRE-ATT&CK Identify groups/roles-PRE-ATT&CK Identify personnel with an authority/privilege-PRE-ATT&CK
Conduct insider-based social engineering to obtain information.	Craft psychological manipulation attacks on key staff.	Identify Key staff from internal directory shared by insider Spoof a personal email address of key personnel and craft a phishing email soliciting discussion of business plans	Manipulate Human Behavior-CAPEC Spear-phishing messages with text only-PRE-ATT&CK
Conduct attacks targeting and compromising personal devices of critical employees.	Gather information using open source discovery of organizational information. Craft spear phishing attacks. *Or* Create counterfeit/spoof web site. Exploit known vulnerabilities in mobile systems (e.g., laptops, PDAs, smart phones). Compromise information systems or devices used externally and reintroduced into the enterprise. Compromise organizational information systems to facilitate exfiltration of data/information. *Or* Download sensitive information to information systems or devices used externally and reintroduced into the enterprise.	Gather information using open source discovery of organizational information Identify accounts of critical employees Craft spear phishing attack likely to deliver malware on employee personal device	Acquire OSINT data sets and information-PRE-ATT&CK Identify personnel with an authority/privilege"PRE-ATT&CK App Delivered via Email Attachment-Mobile_ATT&CK

Approach	Typical High-Level Events	Scenario Component	Detailed Threat Events
Conduct supply chain attacks targeting and exploiting critical hardware, software, or firmware.	Gather information using open source discovery of organizational information. Create and operate false front organizations to inject malicious components into the supply chain. *Or* Compromise systems in another organization to establish a presence in the supply chain. Insert counterfeit or tampered hardware into the supply chain.	Conduct open source identifying software suppliers for target Identify developers at supplier from social media Compromise developer workstation via targeted malware Insert malicious code into software destined for target	Identify supply chains-PRE-ATT&CK Identify people of interest-PRE-ATT&CK Malicious Logic Insertion-CAPEC
Coordinate a campaign of multi-staged attacks (e.g., hopping).	Insert targeted malware into organizational information systems and information system components. Exploit vulnerabilities on internal organizational information systems.	Compromise initial host via spear-phishing Compromise additional internal systems Establish one compromised host as a C2 “proxy” to external controller	Spear phishing messages with malicious links-PRE-ATT&CK Exploitation of Vulnerability-ATT&CK Connection Proxy-ATT&CK
Coordinate a campaign that combines internal and external attacks across multiple information systems and information technologies.	[Other scenarios can be used as building blocks]	Attackers conduct distributed denial of service attack employing botnet, in order to distract cyber defenders. Attackers employ a crafted spear phishing email spoofing the cybersecurity organization with a message related to the DDoS attack. Compromised hosts are used to further achieve attacker goals, such as collect emails	Flooding-CAPEC Spear phishing messages with malicious links-PRE-ATT&CK Email Collection-ATT&CK

Approach	Typical High-Level Events	Scenario Component	Detailed Threat Events
Coordinate campaigns across multiple organizations to acquire specific information or achieve desired outcome.	Compromise systems in a partner organization. *Or* Compromise information systems or devices used externally and reintroduced into the enterprise. *Or* Compromise systems in another organization to establish a presence in the supply chain. Establish or use a communications channel to the enterprise as a whole or to a targeted system. Insert targeted malware into organizational information systems and information system components.	Deliver targeted malware via compromising site visited by organizations of interest ("watering hole") Employ enterprise email for command and control channel to execute commands and exfiltrate data	Targeted client-side exploitation-PRE-ATT&CK Standard Application Layer Protocol-ATT&CK
Coordinate a campaign that spreads attacks across organizational systems from existing presence.	Establish command and control (C2) channels to malware or compromised components. Violate isolation in multi-tenant environment. *Or* Exploit vulnerabilities on internal organizational information systems.	Malware on internal host connects to compromised external website to receive further instructions Additional tools are downloaded and used to scan internal organization for vulnerabilities. Attacker employs exploits to move laterally across organization	Web Service-ATT&CK Remote System Discovery-ATT&CK Exploitation of Vulnerability-ATT&CK
Coordinate a campaign of continuous, adaptive and changing cyber attacks based on detailed surveillance.	[Other scenarios can be used as building blocks]	Initial compromise of host via spear-phishing vector Download additional malware and tools to capture user credentials Move laterally across enterprise via RDP Employ user credentials to conduct additional reconnaissance and surveillance to identify security tools and procedures	Spear phishing messages with malicious links-PRE-ATT&CK Credential Dumping-ATT&CK Remote Desktop Protocol-ATT&CK Valid Accounts-ATT&CK

Approach	Typical High-Level Events	Scenario Component	Detailed Threat Events
Coordinate cyber attacks using external (outsider), internal (insider), and supply chain (supplier) attack vectors.	[Other scenarios can be used as building blocks]	Induce insider to gather information on key suppliers and components Compromise supply chain component Implant Exfiltrate data from target via remote C2 to external attacker	Manipulate Human Behavior-CAPEC Hardware or software supply chain implant-PRE-ATT&CK Exfiltration Over Command and Control Channel-ATT&CK

List of Acronyms

Acronym	Definition
ACH	Automated Clearing House
AFCEA	Armed Forces Communications and Electronics Association
API	Application Programming Interface
APT	Advanced Persistent Threat
ATM	Automated Teller Machine
ATT&CK	Adversarial Tactics, Techniques and Common Knowledge
AWS CBC	Automated Working Station of the Central Bank Client
B2B	Business-to-Business
C2	Command and Control
CAL	Cyber Attack Lifecycle
CAPEC	Common Attack Pattern Enumeration and Classification
CHIPS	Clearing House Interbank Payments System
CISO	Chief Information Security Officer
COBIT	Control Objectives for IT
CSA	Cloud Security Alliance
CTF	Cyber Threat Framework
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
DACS	Describing and Analyzing Cyber Strategies
DDoS	Distributed Denial-of-Service
DHS	Department of Homeland Security
DLL	Dynamic Link Library
EOL	End-of-Life
FBIIC	Financial and Banking Information Infrastructure Committee
FFIEC	Federal Financial Institutions Examination Council

Acronym	Definition
FFRDC	Federally Funded Research and Development Center
FS	Financial Service
FSS	Financial Services Sector
FTP	File Transfer Protocol
HSSEDI	Homeland Security Systems Engineering & Development Institute
HVAC	Heating, Ventilation, and Air Conditioning
IdAM	Identity and Access Management
IDR	Intrusion Detection and Response
IP	Internet Protocol
ISACA	Information Systems Audit and Control Association
ISP	Internet Service Provider
IT	Information Technology
KIQ	Key Intelligence Question
KIT	Key Intelligence Topic
MBR	Master Boot Record
NGCI	Next Generation Cyber Infrastructure
NIST	National Institute of Standards and Technology
NTFS	New Technology File System
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
ODNI	Office of the Director of National Intelligence
OS	Operating System
OSINT	Open Source Intelligence
OSS	Open Source Software
OWASP	Open Web Application Security Project
P2P	Person to Person
PASTA	Process for Attack Simulation and Threat Analysis

Acronym	Definition
PDA	Personal Digital Assistant
PII	Personally Identifiable Information
PRE-ATT&CK	Adversary Tactics, Techniques, and Common Knowledge (ATT&CK) for Left of Exploit
RAT	Remote Access Tool
RDC	Remote Deposit Capture
S&T	Science and Technology Directorate
SP	(NIST) Special Publication
SSH	Secure Shell
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege
TAL	Threat Agent Library
TARA	(Intel) Threat Agent Risk Assessment
TARA	(MITRE) Threat Assessment and Remediation Analysis
TTP	Tactics, Techiniques, and Procedures
VNC	Virtual Network Computing

List of References

1. Bank of England. 2016. "CBEST Intelligence-Led Testing, An Introduction to Cyber Threat Modelling, Version 2.0," Bank of England, 2016. http://www.bankofengland.co.uk/financialstability/fsc/Documents/anintroductiontocbest.pdf.

2. Battaglia, J., Kupersanin, W., Miller, D., Wampler, C., Whitley, S., and Wolf, R. 2017. "Finding Cyber Threats with ATT&CK™-Based Analytics," MTR 170202, The MITRE Corporation, June 2017. https://www.mitre.org/sites/default/files/publications/16-3713-finding-cyber-threats%20with%20att%26ck-based-analytics.pdf.

3. Bodeau, D., and Graubart, R. 2014. "A Framework for Describing and Analyzing Cyber Strategies and Strategic Effects," MTR 140346, PR 14-3407, The MITRE Corporation, 2014.

4. Bodeau, D., and Graubart, R. 2016. "Cyber Prep 2.0: Motivating Organizational Cyber Strategies in Terms of Preparedness," MTR 150264, PR 16-0939, The MITRE Corporation, April 2016.

5. Bodeau, D., McCollum, C., and Fox, D. 2018. "Cyber Threat Modeling: Survey, Assessment, and Representative Framework," HSSEDI, The MITRE Corporation, 2018.

6. Bodeau, D., and McCollum, C. 2018b. "System of Systems Threat Model," HSSEDI, The MITRE Corporation, 2018.

7. Cebula, J., Popeck, M., and Young, L. 2014. "A Taxonomy of Operational Cyber Security Risks Version 2," CMU/SEI-2014-TN-006, Carnegie Mellon University Software Engineering Institute, May 2014. http://resources.sei.cmu.edu/asset_files/TechnicalNote/2014_004_001_91026.pdf.

8. Cloud Security Alliance. 2017. "Top Threats to Cloud Computing Plus: Industry Insights," Cloud Security Alliance, 2017. https://cloudsecurityalliance.org/download/top-threats-cloud-computing-plus-industry-insights/.

9. Dinsmore, P. 2016. "NIPRNET/SIPRNET Cyber Security Architecture Review," AFCEA Defensive Cyber Operations Symposium, April 2016.

10. Fox, D., McCollum, C., Arnoth, E., and Mak, D. 2018. "Cyber Wargaming: Framework for Enhancing Cyber Wargaming with Realistic Business Context," HSSEDI, The MITRE Corporation, 2018.

11. FBIIC. 2017. "Financial Sector Cyber Exercise Template," August 18, 2017. https://www.fbiic.gov/public/2017/Financial_Sector_Cyber_Exercise_Template.pdf.

12. FFIEC. 2017. "FFIEC Cybersecurity Assessment Tool," FFIEC, May 2017. https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017.pdf.

13. Federal Financial Institutions Examination Council (FFIEC). 2016. "IT Examination Handbook for Information Security," FFIEC, September 2016. http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_InformationSecurity.pdf.

14. Fox, D., Arnoth, E., Skorupka, C., and McCollum, C. 2018. "Enterprise Threat Model Technical Report, Cyber Threat Model for a Notional Financial Services Sector Institution," HSSEDI, The MITRE Corporation, 2018.

15. IB Group. 2016. "Buhtrap, the evolution of targeted attacks against financial institutions," IB Group, March 2016. https://www.group-ib.com/brochures/gib-buhtrap-report.pdf.

16. Intel. 2007. "Threat Agent Library Helps Identify Information Security Risks," Intel, September 2007. https://communities.intel.com/docs/DOC-23853.

17. Intel. 2009. IT@Intel White Paper, Intel Information Technology Security "Prioritizing Information Security Risks with Threat Agent Risk Assessment," December 2009.

18. Intel. 2015. "Understanding Cyberthreat Motivations to Improve Defense," February 13, 2015. https://communities.intel.com/servlet/JiveServlet/previewBody/23856-102-1-28290/understanding-cyberthreat-motivations-to-improve-defense-paper-l.pdf.

19. ISACA. 2009. "The Risk IT Framework," ISACA, 2009. http://www.isaca.org/Knowledge-Center/Research/Documents/Risk-IT-Framework-Excerpt_fmk_Eng_0109.pdf.

20. ISACA. 2012. "COBIT Version 5," ISACA, April 2012. http://www.isaca.org/cobit.

21. Kaspersky. 2015. "Carbanak APT, the Great Bank Robbery," Version 2.1, Kaspersky Lab, February 2015.

22. Microsoft. 2005. "The STRIDE Threat Model," Microsoft, 2005. http://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx.

23. MITRE. 2015. "Adversarial Tactics, Techniques, & Common Knowledge," The MITRE Corporation, 2015. http://attack.mitre.org.

24. MITRE. 2016b. "PRE-ATT&CK: Adversarial Tactics, Techniques, & Common Knowledge for Left-of-Exploit," The MITRE Corporation, 2016. http://attack.mitre.org/pre-attack.

25. MITRE. 2016. "Common Attack Pattern Enumeration and Classification, A Community Resource for Identifying and Understanding Attacks," The MITRE Corporation, June 2016. http://capec.mitre.org.

26. MITRE. 2017. "ATT&CK for Mobile," PR 17-0351,The MITRE Corporation, March 2, 2017.

27. MITRE. 2017b "ATT&CK Mobile Profile," https://attack.mitre.org/mobile/index.php/Main_Page.

28. NIST. 2011. "NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View," NIST, March 2011. http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf.

29. NIST. 2012. "Guide for Conducting Risk Assessments, NIST SP 800-30 Rev.1," NIST, September 2012. http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf.

30. NIST. 2014. "Framework for Improving Critical Infrastructure Security, Version 1.0," NIST, February 12, 2014. http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

31. NIST. 2017. "Framework for Improving Critical Infrastructure Cybersecurity, Draft Version 1.1," NIST, January 10, 2017. https://www.nist.gov/sites/default/files/documents/2017/01/17/draft-cybersecurity-framework-v1.1.pdf.

32. NIST. 2018. "Systems Security Engineering: Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems," NIST Special Publication 800-160 Volume 2 (Draft), NIST, March 2018. https://csrc.nist.gov/CSRC/media/Publications/sp/800-160/vol-2/draft/documents/sp800-160-vol2-draft.pdf.

33. ODNI. 2017. "The Cyber Threat Framework." March 13, 2017. https://www.dni.gov/index.php/cyber-threat-framework, Overview: https://www.dni.gov/files/ODNI/documents/features/A_Common_Cyber_Threat_Framework_Overview.pdf, How to Use: https://www.dni.gov/files/ODNI/documents/features/A_Common_Cyber_Threat_Framework.pdf, Lexicon: https://www.dni.gov/files/ODNI/documents/features/Cyber_Threat_Framework_Lexicon.pdf, and Detailed Description: https://www.dni.gov/files/ODNI/documents/features/Threat_Framework_A_Foundation_for_Communication.pdf.

34. OWASP. 2016. "OWASP Automated Threat Handbook: Web Applications, Version 1.1," OWASP, November 3, 2016. https://www.owasp.org/images/3/33/Automated-threat-handbook.pdf.

35. Williamson, W. 2015. "Banking Malware Redefined," Security Week, February 18, 2015. https://www.securityweek.com/banking-malware-redefined.

36. Wynn, J., Whitmore, J., Upton, G., Spriggs, L., McKinnon, D., McInnes, R., Graubart, R., and Clausen, L. 2011. "Threat Assessment and Remediation Analysis (TARA) Methodology Description, V. 1.0," MTR 110176, PR 11-4982, The MITRE Corporation, October 2011. http://www.mitre.org/sites/default/files/pdf/11_4982.pdf.

ATT&CK™ is a registered trademark of The MITRE Corporation

CAPEC™ is a registered trademark of The MITRE Corporation