Science of Cybersecurity: Terminology and Taxonomy

CS 459/559: Science of Cyber Security
2nd Lecture

Instructor:

Guanhua Yan

What we have learned from the last lecture

- What is cybersecurity?
- What is science of cybersecurity?
- Syllabus of this course

What we are going to learn

- Attack surface and vector
- Security risk analysis
- Security models

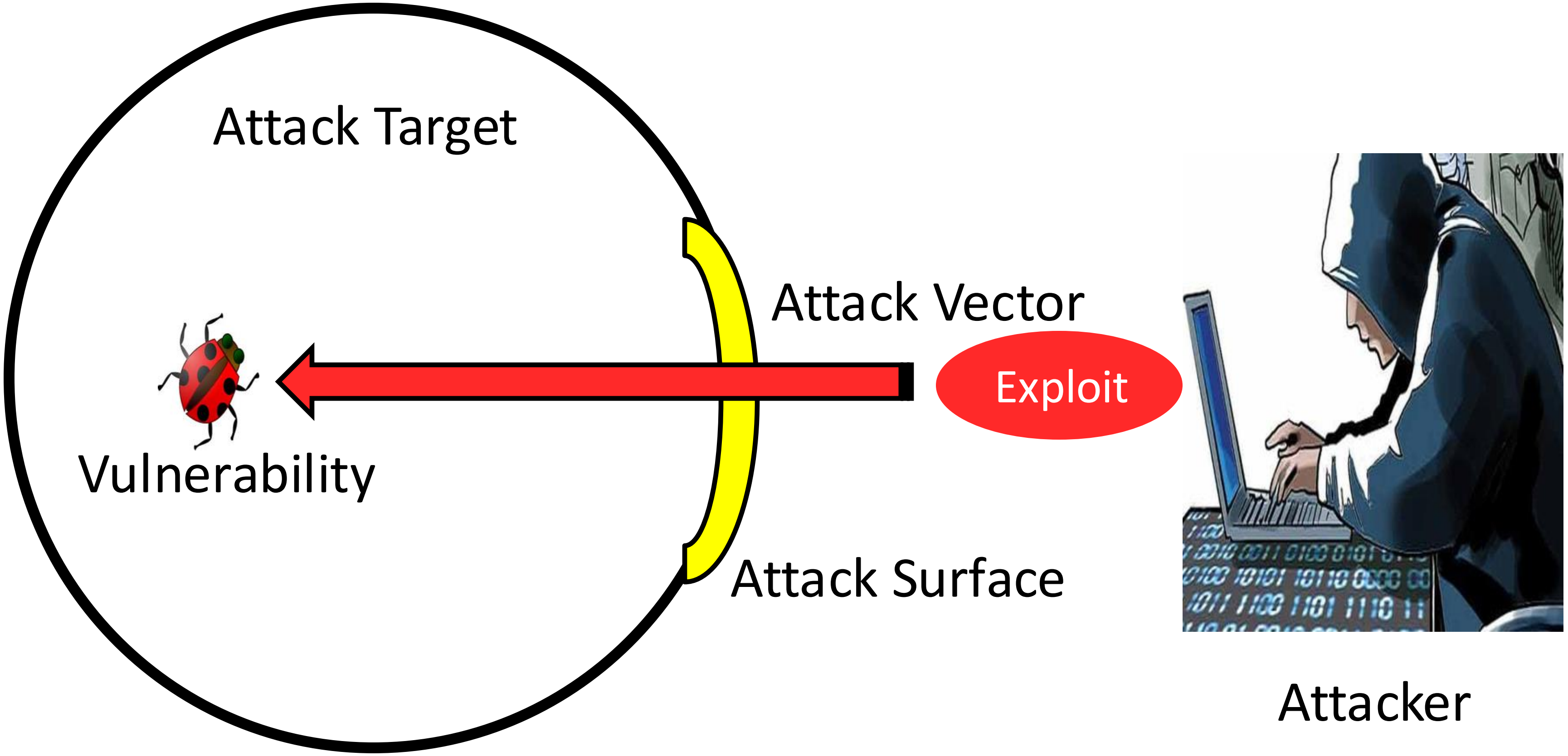
Terminology & taxonomy

- Terminology: special words or expressions used in relation to a particular subject or activity

- Taxonomy: a classification scheme that partitions a body of knowledge and defines the relationship of the pieces

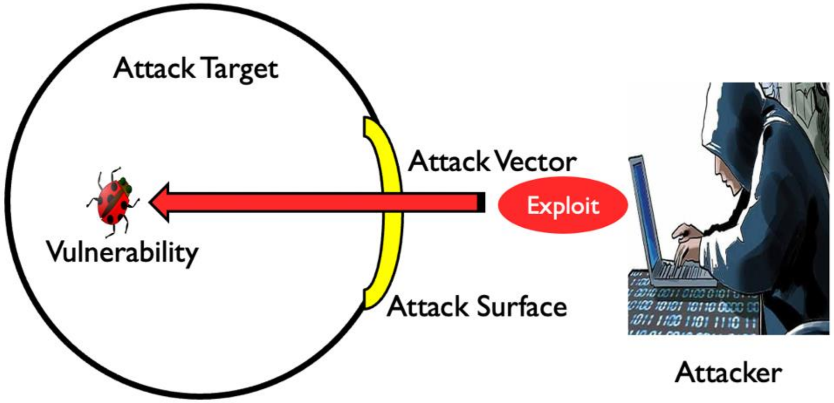
Attack Surface and Vector

How does a cyber attack occur?



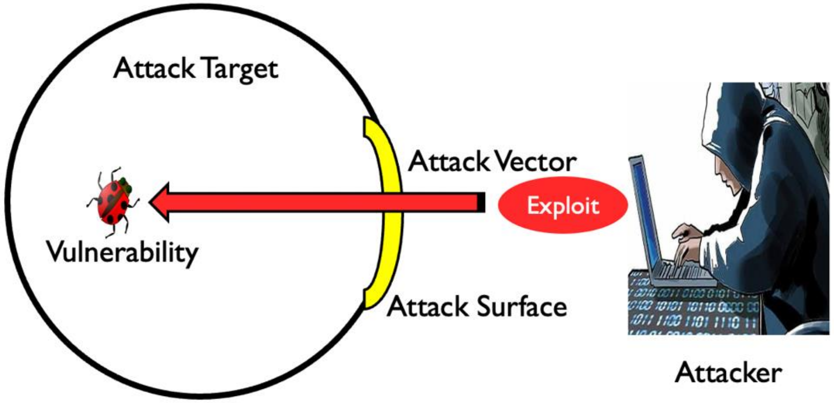
Terminology: attacker side

- ***Attack Vector***: the 'route' by which an attack was carried out. SQL injection attack is typically carried out using a browser client to the web application. The web application is the attack vector.
- ***Exploit***: the method of taking advantage of a vulnerability. The code used to send SQL commands to a web application in order to take advantage of the unsanitized user inputs is an 'exploit'.



Terminology: target side

- ***Attack Surface***: describes how exposed one is to attacks. Without a firewall to limit how many ports are blocked, then your 'attack surface' is all the ports. Blocking all ports but port 80 reduces your 'attack surface' to a single port.
- ***Vulnerability***: a weakness that exposes risk. Unsanitized user inputs can pose a 'vulnerability' by a SQL injection method.



Quiz: PDF malware

- An attacker sends an infected PDF as an email attachment to a user. The user opens the PDF, gets infected, and malware is installed.

Attack Vector

Exploit

Vulnerability

Attack Surface

User and email system

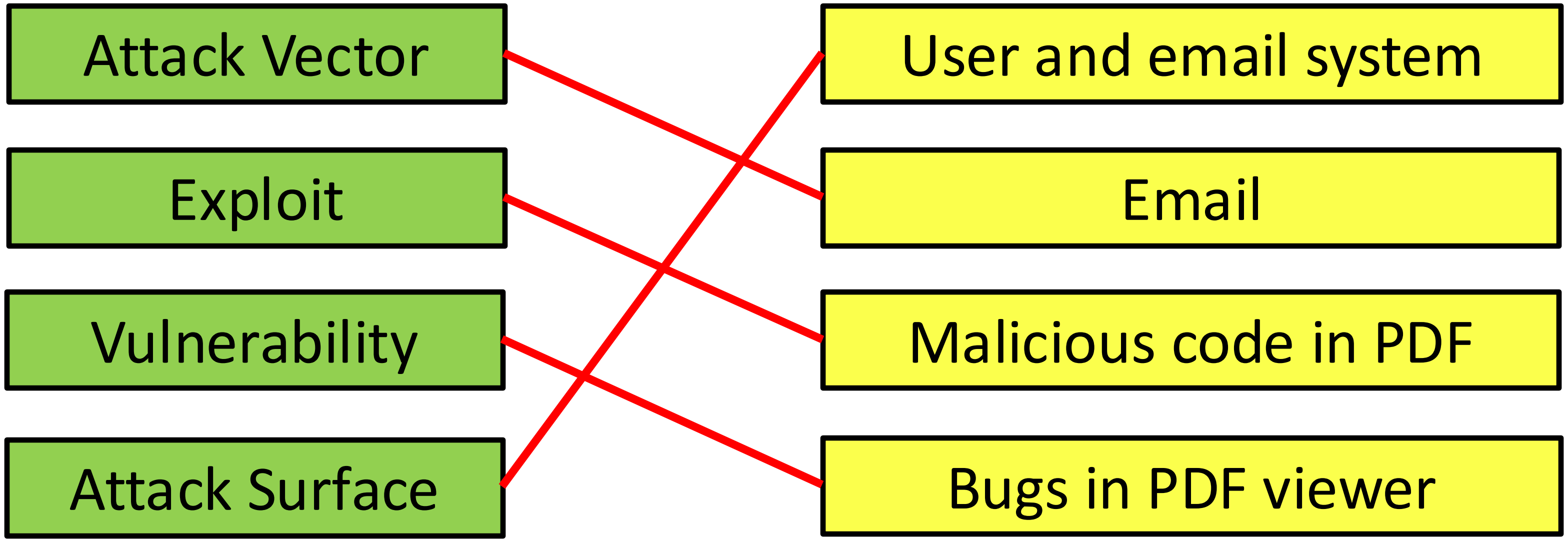
Email

Malicious code in PDF

Weakness in PDF viewer

Quiz: PDF malware

- An attacker sends an infected PDF as an email attachment to a user. The user opens the PDF, gets infected, and malware is installed.



Attack Vector

Exploit

Vulnerability

Attack Surface

User and email system

Email

Malicious code in PDF

Bugs in PDF viewer

Security Risk Analysis

Security risk analysis

- Risk
- Vulnerabilities
- Threats
- Attacks
- Defenses

Risks

To mitigate the risks to computing systems we need to

1. learn what the threats are to the security;
2. learn how vulnerabilities arise when we develop the system;
3. know what mechanisms are available to reduce or block these threats.

Vulnerabilities

Definition (Vulnerability)

A vulnerability is a weakness in the security of a computer system that allows a malicious user to "do something bad."

- A vulnerability could be exploited for different reasons to affect many different assets.
- Something bad:
    - take control of the system,
    - slow down the system so that it's unusable,
    - access private data,
    - ...

Threats

Definition (Threat)

A threat is a set of circumstances that could possibly cause harm, a potential violation of security.

- Threats include
  - who might attack against what assets,
  - what resources they might use,
  - what goal they have in mind,
  - when/where/why they might attack,
  - with what probability they might attack.
- A threat is blocked by a control of vulnerabilities.

Threats vs. Vulnerabilities — Examples

Threat: Adversaries might install keyloggers in the computers in our Personnel Department so they can steal social security numbers.

Vulnerability: The computers in the Personnel Department do not have up to date anti-malware software

Attacks

- An attack is an attempt by an adversary to cause damage to valuable assets, by exploiting vulnerabilities.
- We analyze potential attacks to determine what kind of damage they could cause:
  - theft, sabotage, destruction, espionage, tampering, or adulteration.

Defenses

- We want to develop methods that will defend against attacks.
- Actions to be taken to defend against attack:
  - identify compromised machines,
  - removing malicious code,
  - patching systems to remove vulnerabilities, . . .

Design, Implementation and Deployment

- The design of secure systems must take usability into account.
- Users will ignore inconvenient or hard-to-understand security measures.
- The implementation of a secure system needs to be tested.
- A deployed system must be continuously monitored:
  - detect security breaches
  - react to security breaches
- Security patches must be applied when they become available.

Security Models

Security models

- Why models?
- Microsoft STRIDE
- Attack trees
- Cyber kill chain
- MITRE ATT&CK

Models

- To build secure systems, we need sound models.
- Which security properties should be assured?
- What type of attacks can be launched?

Security models

- Why models?
- Microsoft STRIDE
- Attack trees
- Cyber kill chain
- MITRE ATT&CK

Microsoft STRIDE model

- Developed by Praerit Garg and Loren Kohnfelder at Microsoft
- The STRIDE model categorizes different types of threats and simplifies the overall security conversations.
- Include:
  - Spoofing
  - Tampering
  - Repudiation
  - Information disclosure
  - Denial of service
  - Elevation of privilege

https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats

Spoofing

- Involves illegally accessing and then using another user's authentication information, such as username and password

Tampering

- Involves the malicious modification of data.
- Examples include unauthorized changes made to persistent data, such as that held in a database, and the alteration of data as it flows between two computers over an open network, such as the Internet

Repudiation

- Associated with users who deny performing an action without other parties having any way to prove otherwise
  - For example, a user performs an illegal operation in a system that lacks the ability to trace the prohibited operations.

- Non-Repudiation refers to the ability of a system to counter repudiation threats.
  - For example, a user who purchases an item might have to sign for the item upon receipt. The vendor can then use the signed receipt as evidence that the user did receive the package

Information disclosure

- Involves the exposure of information to individuals who are not supposed to have access to it

- For example, the ability of users to read a file that they were not granted access to, or the ability of an intruder to read data in transit between two computers

Denial of service

- Denial of service (DoS) attacks deny service to valid users

- For example, by making a Web server temporarily unavailable or unusable.

- You must protect against certain types of DoS threats simply to improve system availability and reliability

Elevation of privilege

- An unprivileged user gains privileged access and thereby has sufficient access to compromise or destroy the entire system.

- Elevation of privilege threats include those situations in which an attacker has effectively penetrated all system defenses and become part of the trusted system itself, a dangerous situation indeed

Spoofing

Tampering

Repudiation

Information Disclosure

Denial of Service

Elevation of privilege

Confidentiality

Integrity

Availability

Security models

- Why models?
- Microsoft STRIDE
- Attack trees
- Cyber kill chain
- MITRE ATT&CK

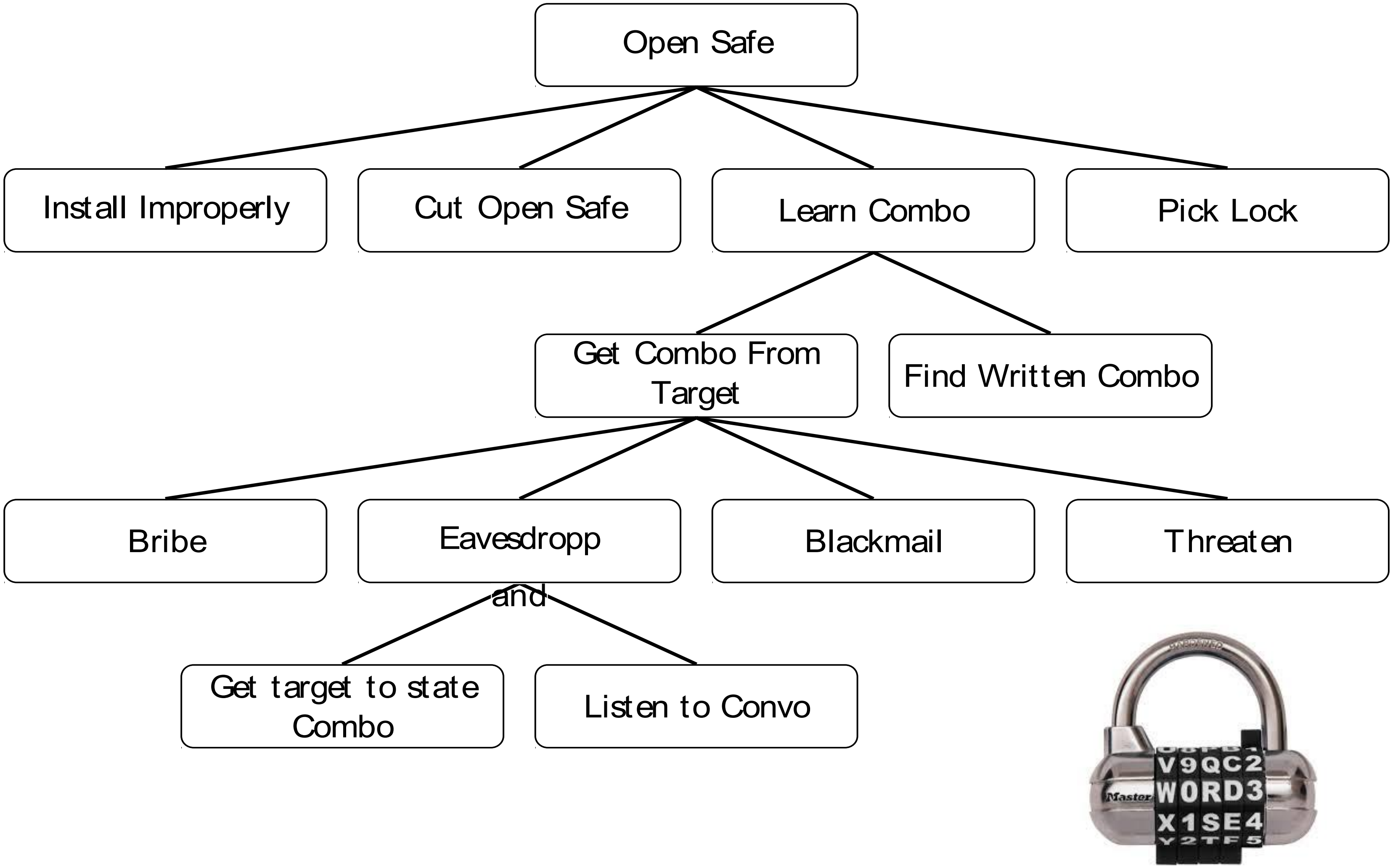
Attack Trees

- We need to model threats against computer systems.
- What are the different ways in which a system can be attacked?
- If we can understand this, we can design proper countermeasures.
- Attack trees are a way to methodically describe the security of a system.
- Attack trees have both AND and OR nodes:

  OR: Alternatives to achieving a goal.
  AND: Different steps toward achieving a goal.

  Each node is a subgoal. Child nodes are ways to achieve that subgoal.

Attack Trees — Example I — Open a Safe



Open Safe

Install Improperly

Cut Open Safe

Learn Combo

Pick Lock

Get Combo From Target

Find Written Combo

Bribe

Eavesdropp

Blackmail

Threaten

and

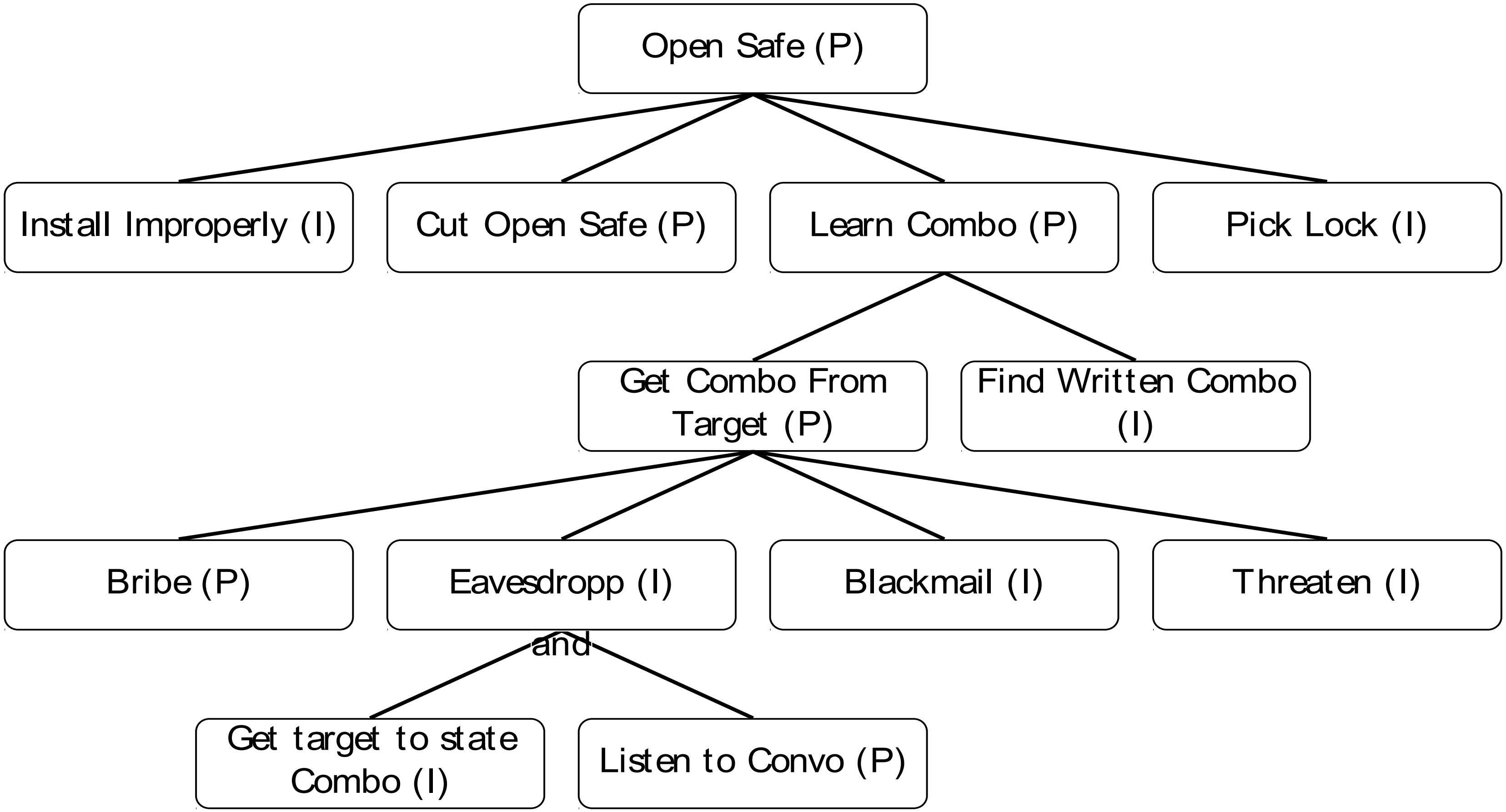
Get target to state Combo

Listen to Convo

Attack Trees — Example I — Open a Safe

- Examine the safe/ safe owner/ attacker's abilities/ etc. and assign values to the nodes:
  - P = Possible
  - I = Impossible
- The value of an OR node is possible if any of its children are possible.
- The value of an AND node is possible if all children are possible.
- A path of P:s from a leaf to the root is a possible attack!
- Once you know the possible attacks, you can think of ways to defend against them!

Attack Trees — Example I — Open a Safe



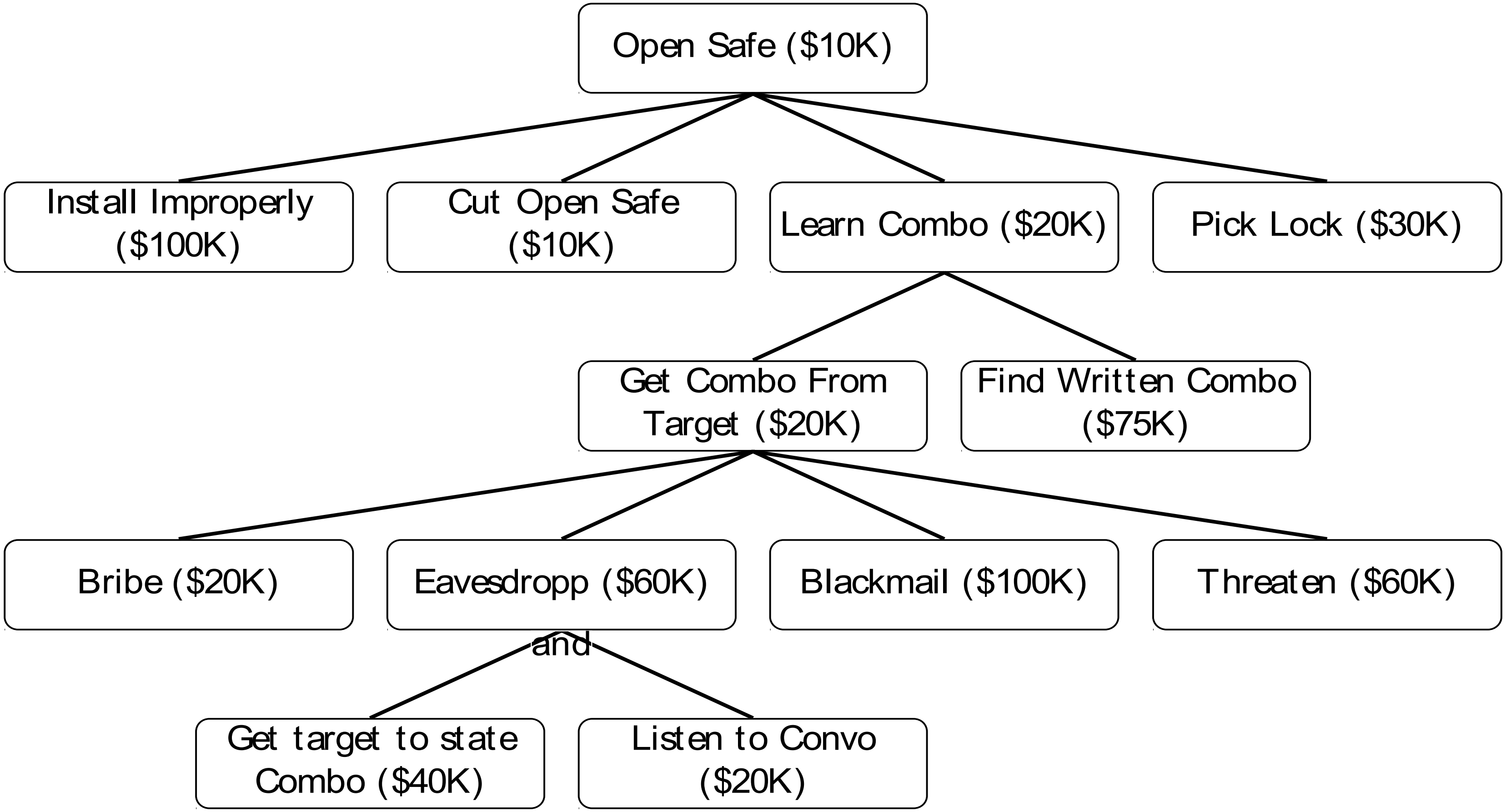
Attack Trees — Example I — Open a Safe

- We can be more specfic and model the cost of an attack.
- Costs propagate up the tree:

  OR nodes: take the min of the children.

  AND nodes: take the sum the children.

Attack Trees — Example I — Open a Safe

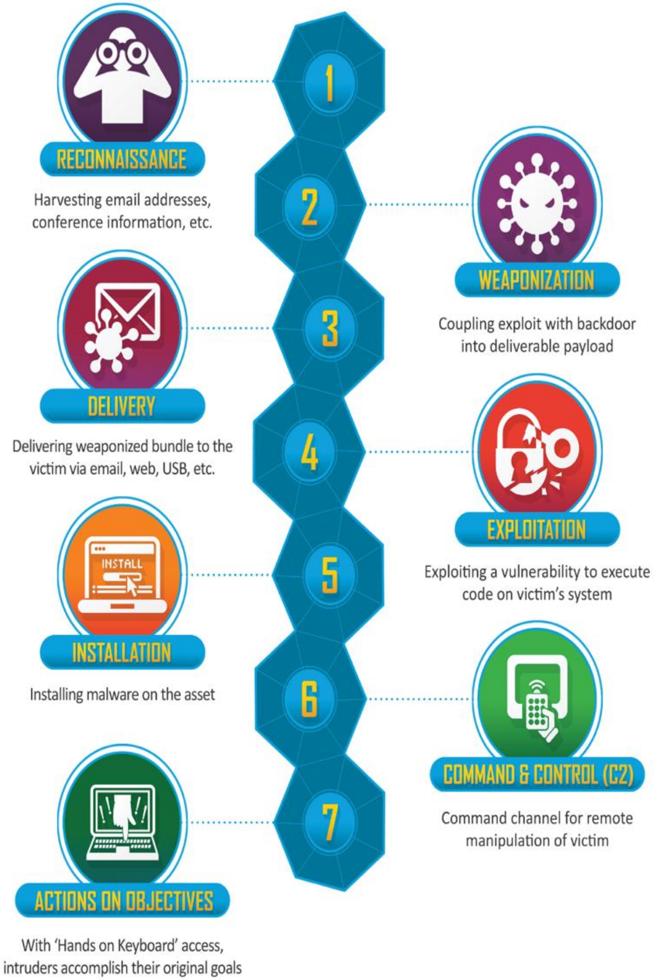


Security models

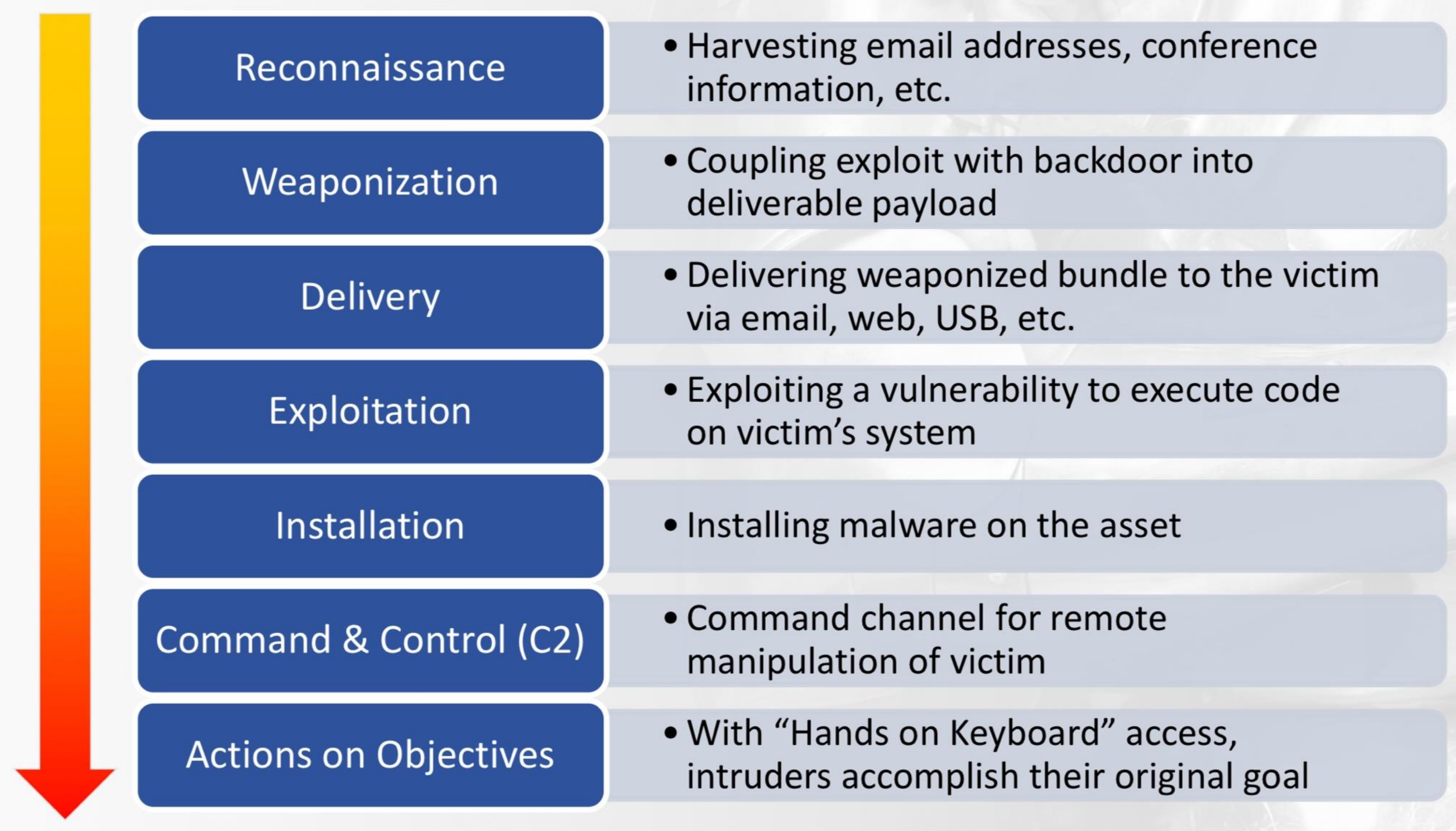
- Why models?
- Microsoft STRIDE
- Attack trees
- Cyber kill chain
- MITRE ATT&CK

What is cyber kill chain?

- **Developed by Lockheed Martin**
- **Industry-accepted methodology for understanding how an attacker conducts activities to compromise the security of an enterprise network**
- **It includes seven steps.**
- **Used to analyze high-profile security incidents**
  - Target data breach


1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

Cyber kill chain



Reconnaissance

- Harvesting email addresses, conference information, etc.

Weaponization

- Coupling exploit with backdoor into deliverable payload

Delivery

- Delivering weaponized bundle to the victim via email, web, USB, etc.

Exploitation

- Exploiting a vulnerability to execute code on victim's system

Installation

- Installing malware on the asset

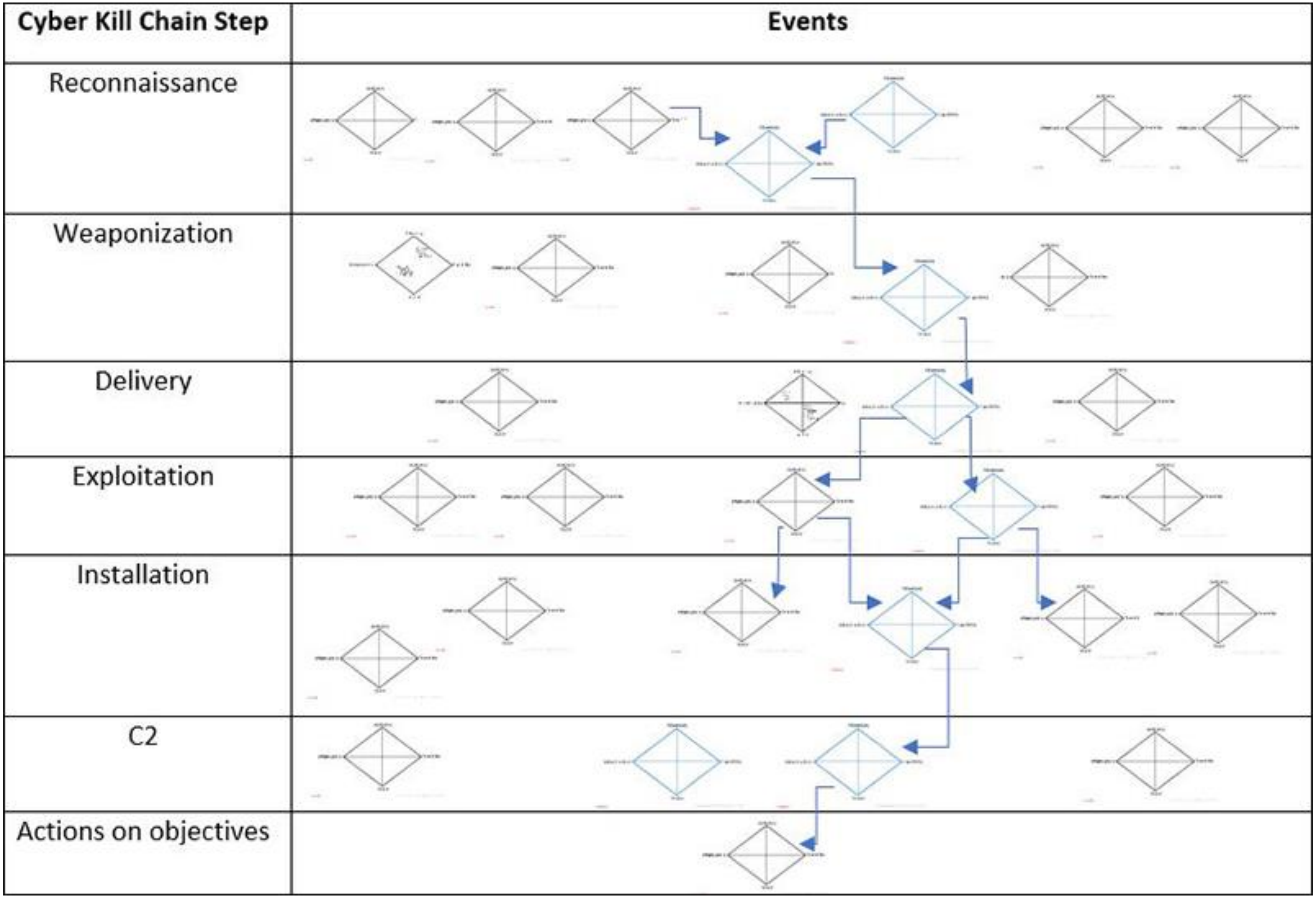
Command & Control (C2)

- Command channel for remote manipulation of victim

Actions on Objectives

- With "Hands on Keyboard" access, intruders accomplish their original goal

Activity-attack graph



Cyber Kill Chain Step	Events
Reconnaissance	
Weaponization	
Delivery	
Exploitation	
Installation	
C2	
Actions on objectives	

ShadowHammer attack

- Operation discovered in 2018 by Kaspersky
- More than a million computer users affected worldwide
- The adversary was able to compromise a computer vendor’s software update tool and modified it into a trojan downloader.
- The attackers had hardcoded a list of MAC addresses in the trojanized samples and this list was used to identify the actual intended targets of this massive operation.
- For the vast majority of infected systems, the trojanized tool remained dormant.
- The ShadowHammer operation is a form of supply chain attack, where the adversary attacks the supplier and uses them to gain access to the target.

Attack analysis

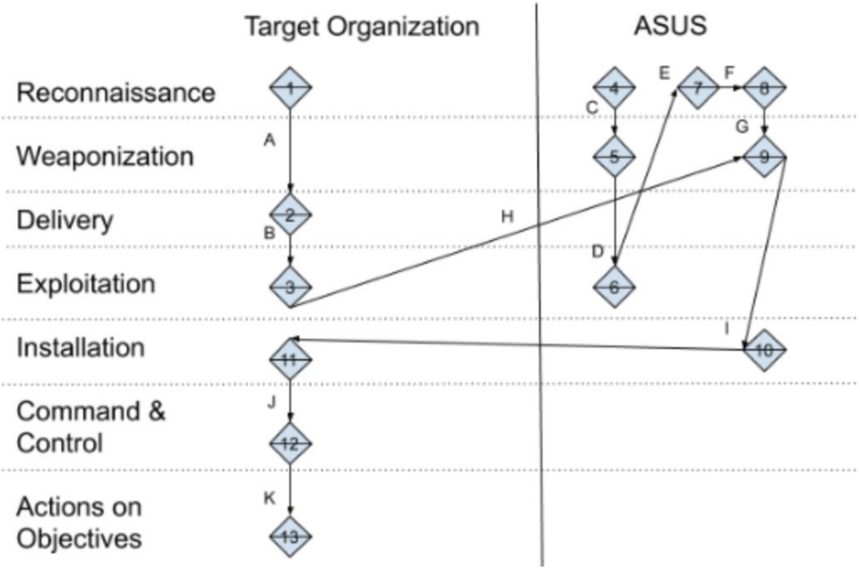
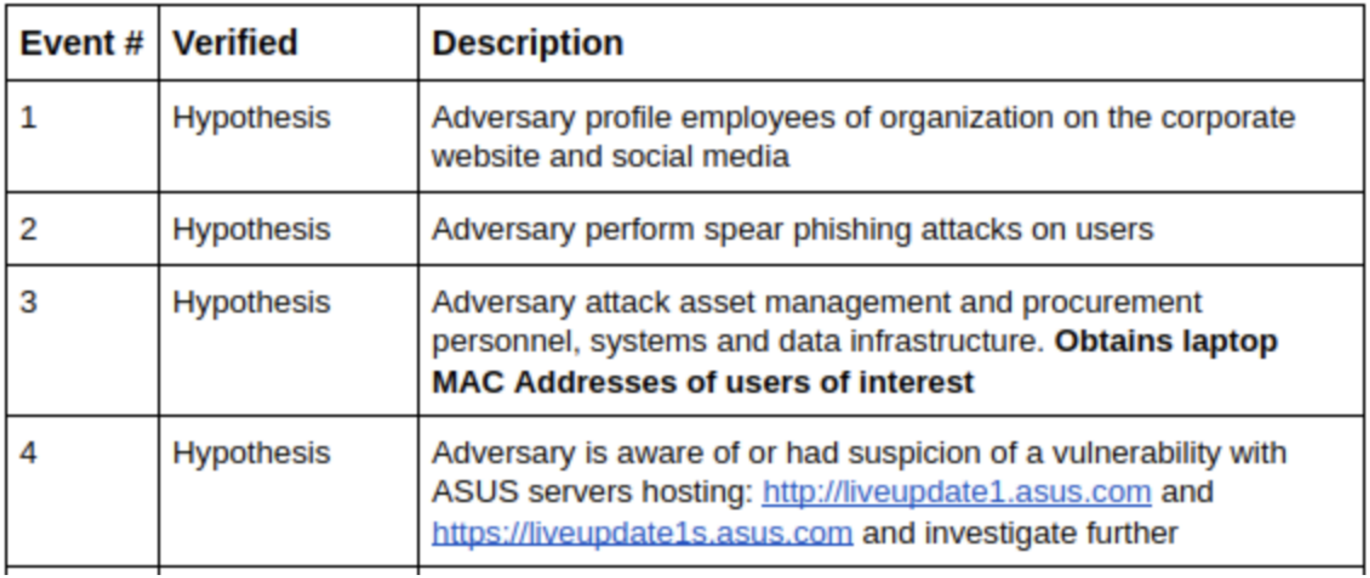


Diagram 1: Diamond Model - Activity-Attack Graph



Event #	Verified	Description
1	Hypothesis	Adversary profile employees of organization on the corporate website and social media
2	Hypothesis	Adversary perform spear phishing attacks on users
3	Hypothesis	Adversary attack asset management and procurement personnel, systems and data infrastructure. **Obtains laptop MAC Addresses of users of interest**
4	Hypothesis	Adversary is aware of or had suspicion of a vulnerability with ASUS servers hosting: http://liveupdate1.asus.com and https://liveupdate1s.asus.com and investigate further

Attack analysis

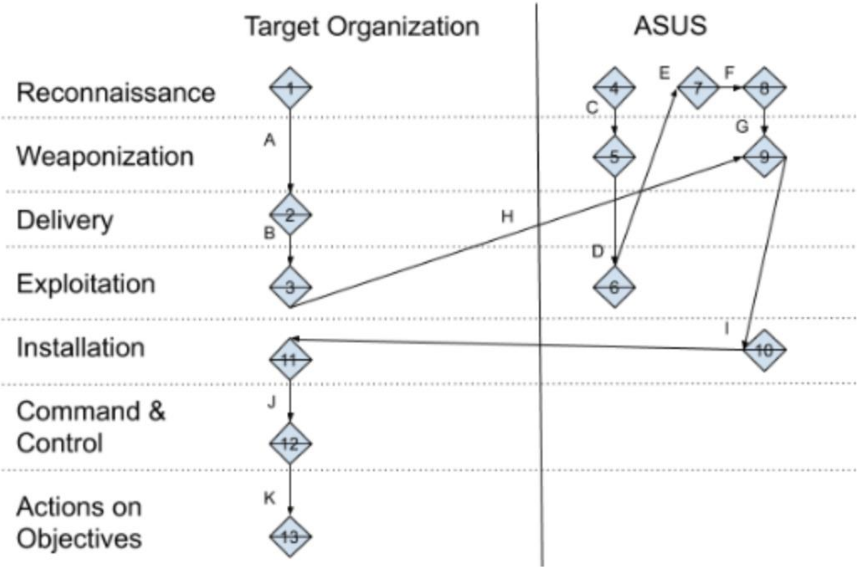
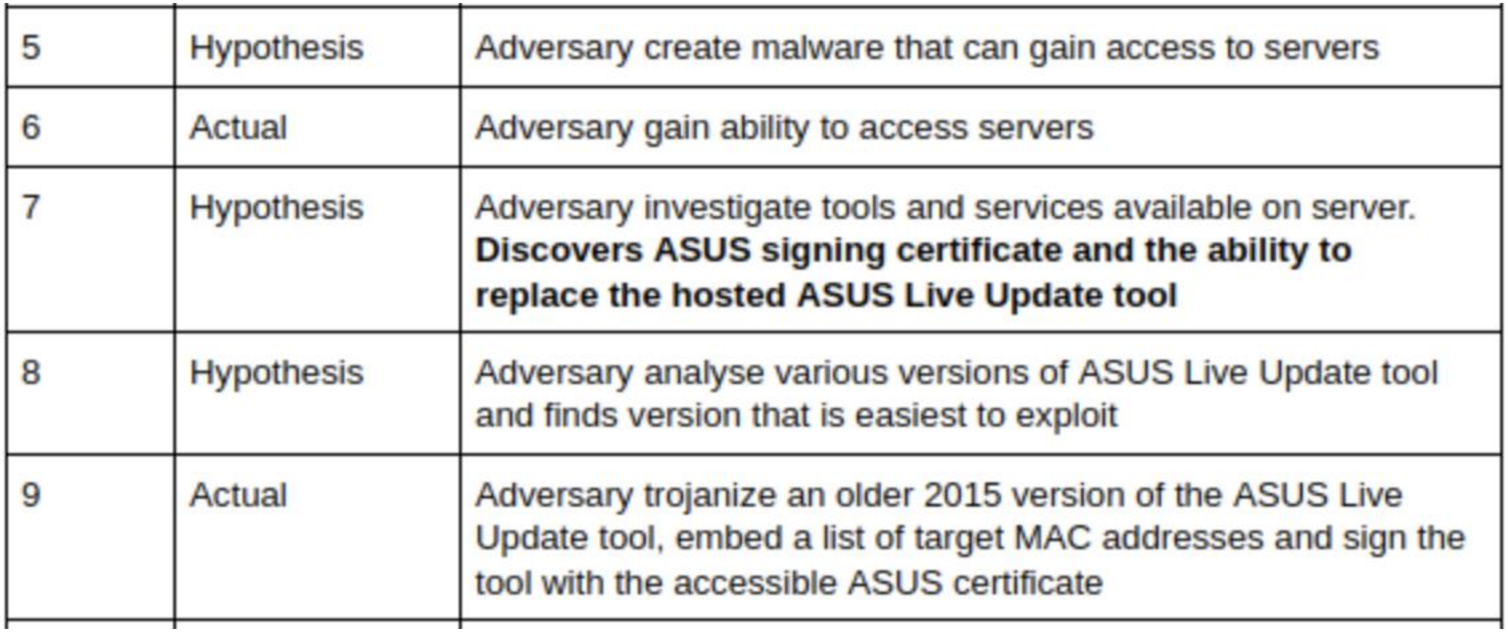


Diagram 1: Diamond Model - Activity-Attack Graph



5	Hypothesis	Adversary create malware that can gain access to servers
6	Actual	Adversary gain ability to access servers
7	Hypothesis	Adversary investigate tools and services available on server. **Discovers ASUS signing certificate and the ability to replace the hosted ASUS Live Update tool**
8	Hypothesis	Adversary analyse various versions of ASUS Live Update tool and finds version that is easiest to exploit
9	Actual	Adversary trojanize an older 2015 version of the ASUS Live Update tool, embed a list of target MAC addresses and sign the tool with the accessible ASUS certificate

Attack analysis

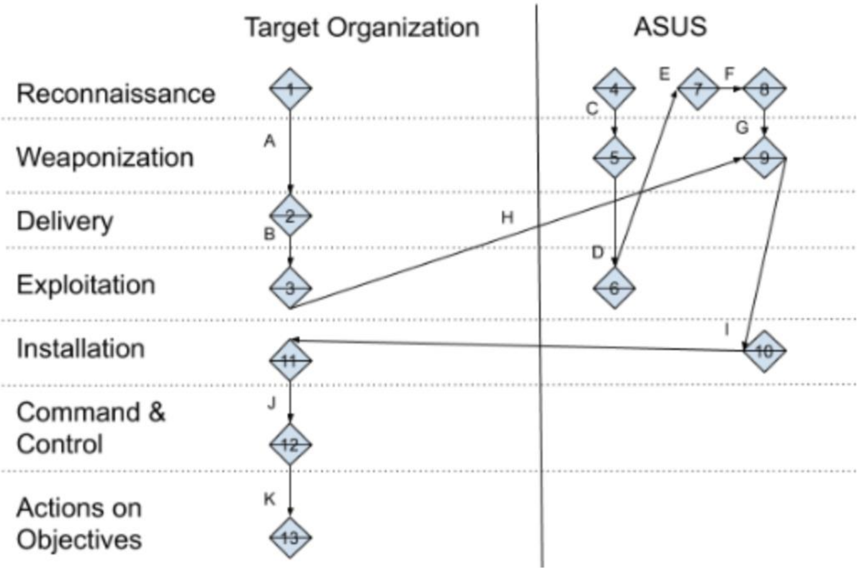
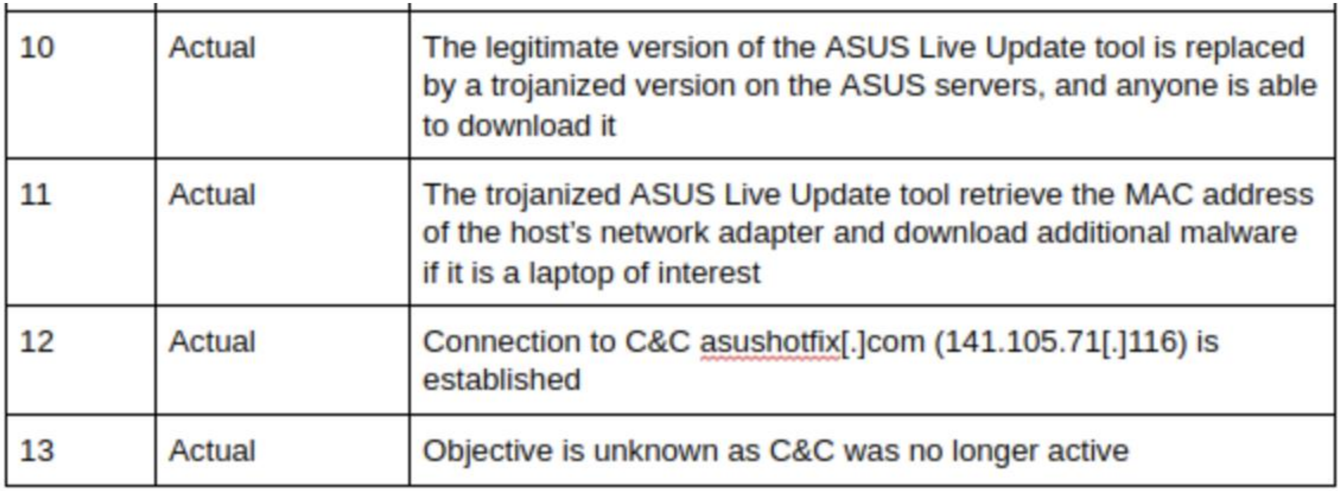


Diagram 1: Diamond Model - Activity-Attack Graph



10	Actual	The legitimate version of the ASUS Live Update tool is replaced by a trojanized version on the ASUS servers, and anyone is able to download it
11	Actual	The trojanized ASUS Live Update tool retrieve the MAC address of the host's network adapter and download additional malware if it is a laptop of interest
12	Actual	Connection to C&C asushotfix[.]com (141.105.71[.]116) is established
13	Actual	Objective is unknown as C&C was no longer active

Table 1: Activity Thread Event Descriptions

Security models

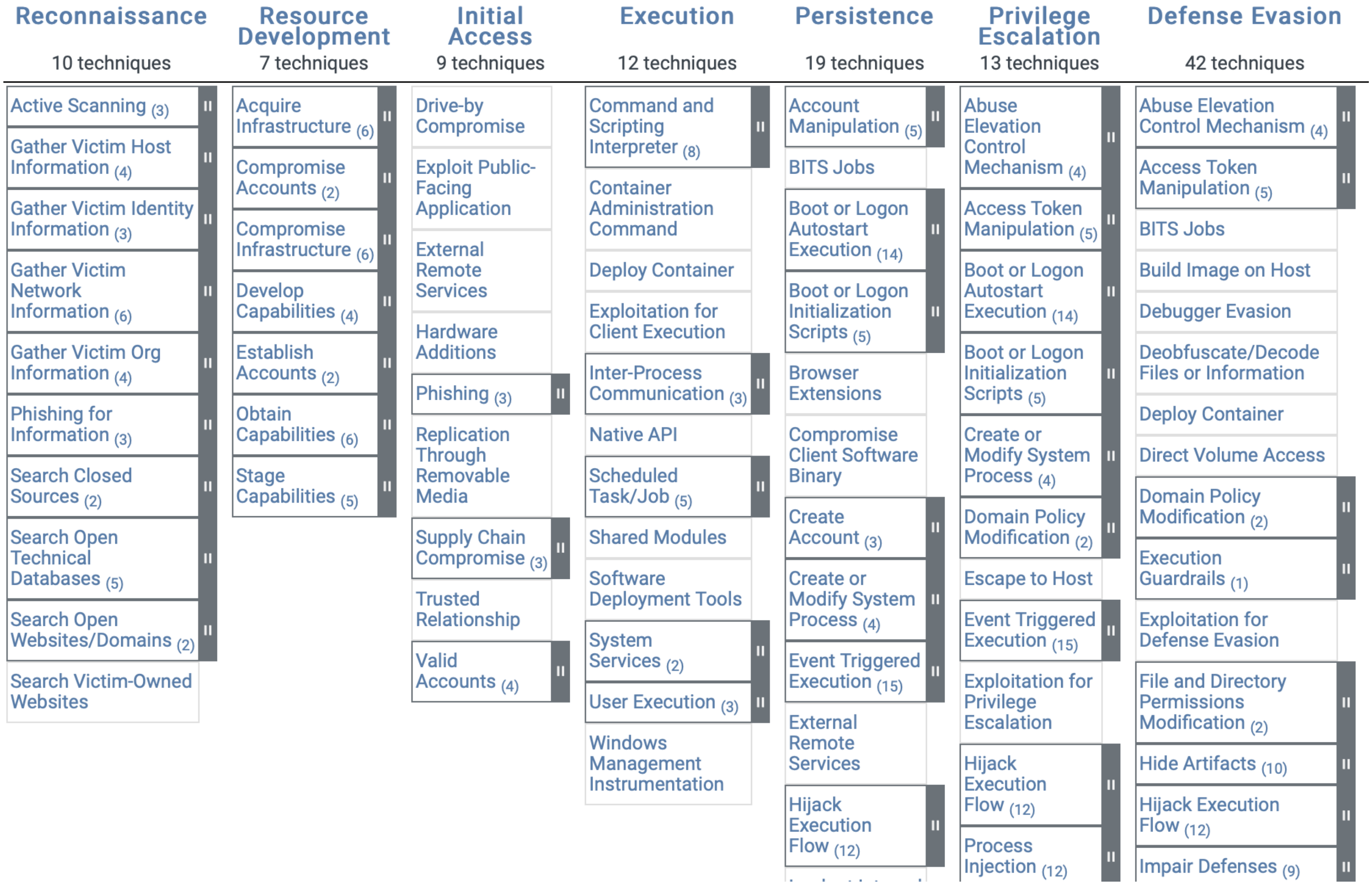
- Why models?
- Microsoft STRIDE
- Attack trees
- Cyber kill chain
- MITRE ATT&CK

MITRE ATT&CK

- MITRE ATT&CK is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.

- The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

Matrix (Enterprise)



Reconnaissance
10 techniques

- Active Scanning (3)
- Gather Victim Host Information (4)
- Gather Victim Identity Information (3)
- Gather Victim Network Information (6)
- Gather Victim Org Information (4)
- Phishing for Information (3)
- Search Closed Sources (2)
- Search Open Technical Databases (5)
- Search Open Websites/Domains (2)
- Search Victim-Owned Websites

Resource Development
7 techniques

- Acquire Infrastructure (6)
- Compromise Accounts (2)
- Compromise Infrastructure (6)
- Develop Capabilities (4)
- Establish Accounts (2)
- Obtain Capabilities (6)
- Stage Capabilities (5)

Initial Access
9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (3)
- Replication Through Removable Media
- Supply Chain Compromise (3)
- Trusted Relationship
- Valid Accounts (4)

Execution
12 techniques

- Command and Scripting Interpreter (8)
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (3)
- Native API
- Scheduled Task/Job (5)
- Shared Modules
- Software Deployment Tools
- System Services (2)
- User Execution (3)
- Windows Management Instrumentation

Persistence
19 techniques

- Account Manipulation (5)
- BITS Jobs
- Boot or Logon Autostart Execution (14)
- Boot or Logon Initialization Scripts (5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (3)
- Create or Modify System Process (4)
- Event Triggered Execution (15)
- External Remote Services
- Hijack Execution Flow (12)

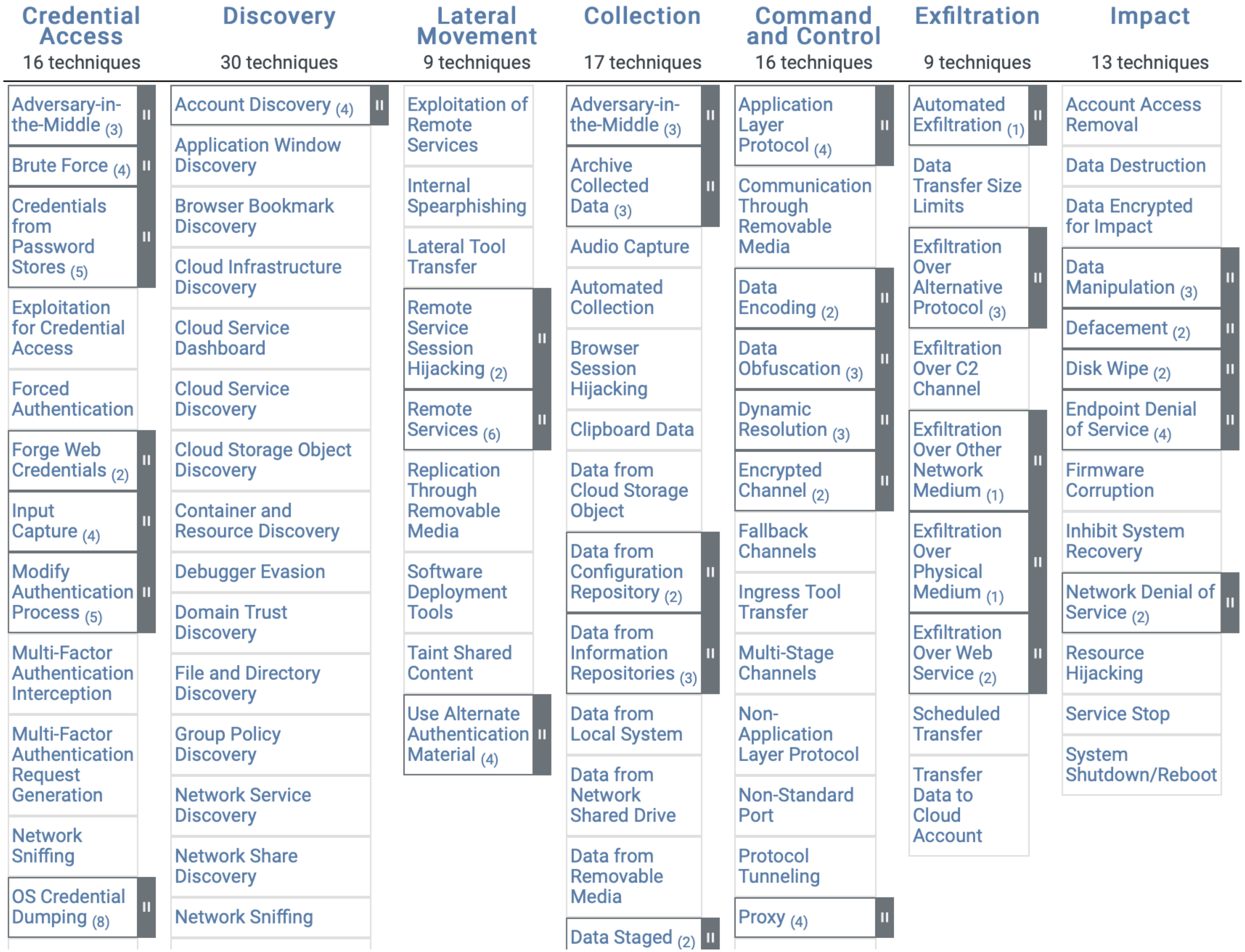
Privilege Escalation
13 techniques

- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- Boot or Logon Autostart Execution (14)
- Boot or Logon Initialization Scripts (5)
- Create or Modify System Process (4)
- Domain Policy Modification (2)
- Escape to Host
- Event Triggered Execution (15)
- Exploitation for Privilege Escalation
- Hijack Execution Flow (12)
- Process Injection (12)

Defense Evasion
42 techniques

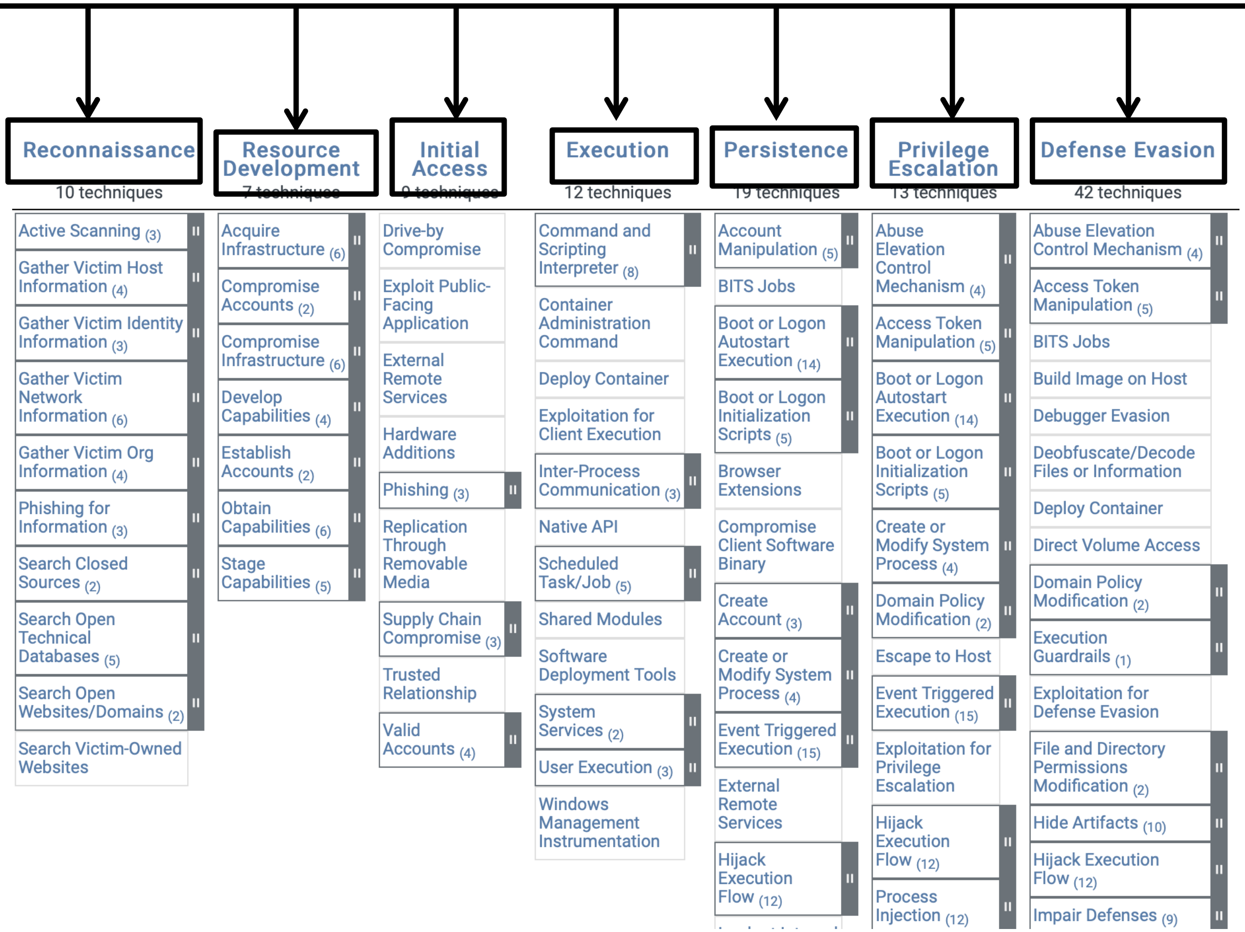
- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification (2)
- Execution Guardrails (1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (2)
- Hide Artifacts (10)
- Hijack Execution Flow (12)
- Impair Defenses (9)

Matrix (Enterprise) – Cont’d



Credential Access 16 techniques	Discovery 30 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Credentials from Password Stores (5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Forced Authentication	Cloud Service Dashboard	Remote Services (6)	Browser Session Hijacking	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage Object	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Modify Authentication Process (5)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Multi-Factor Authentication Request Generation	Domain Trust Discovery		Data from Local System	Non-Application Layer Protocol		Network Denial of Service (2)
Network Sniffing	File and Directory Discovery		Data from Network Shared Drive	Non-Standard Port		Resource Hijacking
OS Credential Dumping (8)	Group Policy Discovery		Data from Removable Media	Protocol Tunneling		Service Stop
	Network Service Discovery		Data Staged (2)	Proxy (4)		System Shutdown/Reboot
	Network Share Discovery					
	Network Sniffing					

Tactics represent the "why" of an ATT&CK technique or sub-technique. It is the adversary's tactical goal: the reason for performing an action. For example, an adversary may want to achieve credential access.



Reconnaissance
10 techniques

- Active Scanning (3)
- Gather Victim Host Information (4)
- Gather Victim Identity Information (3)
- Gather Victim Network Information (6)
- Gather Victim Org Information (4)
- Phishing for Information (3)
- Search Closed Sources (2)
- Search Open Technical Databases (5)
- Search Open Websites/Domains (2)
- Search Victim-Owned Websites

Resource Development
7 techniques

- Acquire Infrastructure (6)
- Compromise Accounts (2)
- Compromise Infrastructure (6)
- Develop Capabilities (4)
- Establish Accounts (2)
- Obtain Capabilities (6)
- Stage Capabilities (5)

Initial Access
9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (3)
- Replication Through Removable Media
- Supply Chain Compromise (3)
- Trusted Relationship
- Valid Accounts (4)

Execution
12 techniques

- Command and Scripting Interpreter (8)
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (3)
- Native API
- Scheduled Task/Job (5)
- Shared Modules
- Software Deployment Tools
- System Services (2)
- User Execution (3)
- Windows Management Instrumentation

Persistence
19 techniques

- Account Manipulation (5)
- BITS Jobs
- Boot or Logon Autostart Execution (14)
- Boot or Logon Initialization Scripts (5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (3)
- Create or Modify System Process (4)
- Event Triggered Execution (15)
- External Remote Services
- Hijack Execution Flow (12)

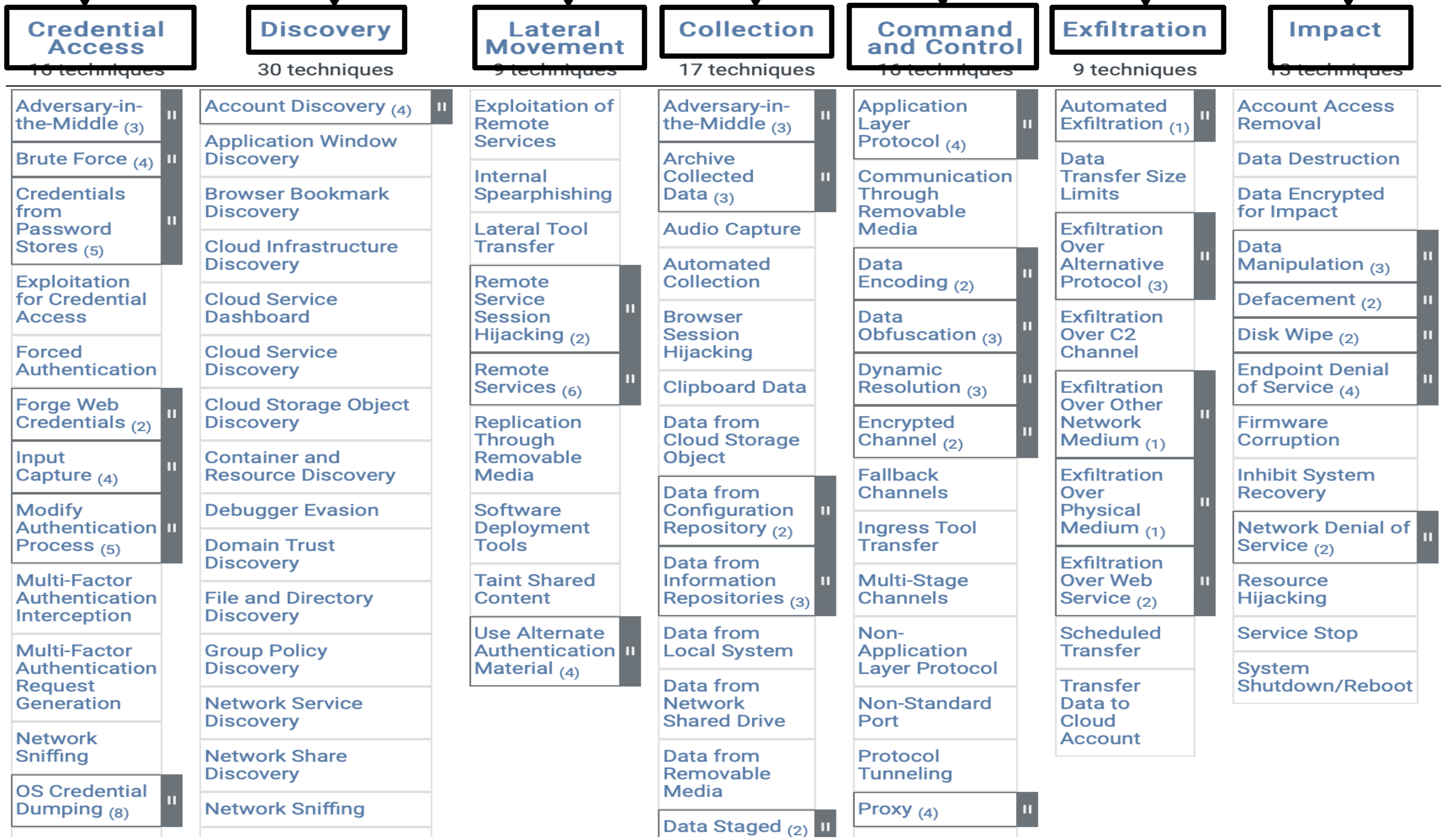
Privilege Escalation
13 techniques

- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- Boot or Logon Autostart Execution (14)
- Boot or Logon Initialization Scripts (5)
- Create or Modify System Process (4)
- Domain Policy Modification (2)
- Escape to Host
- Event Triggered Execution (15)
- Exploitation for Privilege Escalation
- Hijack Execution Flow (12)
- Process Injection (12)

Defense Evasion
42 techniques

- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification (2)
- Execution Guardrails (1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (2)
- Hide Artifacts (10)
- Hijack Execution Flow (12)
- Impair Defenses (9)

Tactics represent the "why" of an ATT&CK technique or sub-technique. It is the adversary's tactical goal: the reason for performing an action. For example, an adversary may want to achieve credential access.



Credential Access
16 techniques

- Adversary-in-the-Middle (3)
- Brute Force (4)
- Credentials from Password Stores (5)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (2)
- Input Capture (4)
- Modify Authentication Process (5)
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- Network Sniffing
- OS Credential Dumping (8)

Discovery
30 techniques

- Account Discovery (4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Network Service Discovery
- Network Share Discovery
- Network Sniffing

Lateral Movement
9 techniques

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (2)
- Remote Services (6)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (4)

Collection
17 techniques

- Adversary-in-the-Middle (3)
- Archive Collected Data (3)
- Audio Capture
- Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Cloud Storage Object
- Data from Configuration Repository (2)
- Data from Information Repositories (3)
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (2)

Command and Control
16 techniques

- Application Layer Protocol (4)
- Communication Through Removable Media
- Data Encoding (2)
- Data Obfuscation (3)
- Dynamic Resolution (3)
- Encrypted Channel (2)
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy (4)

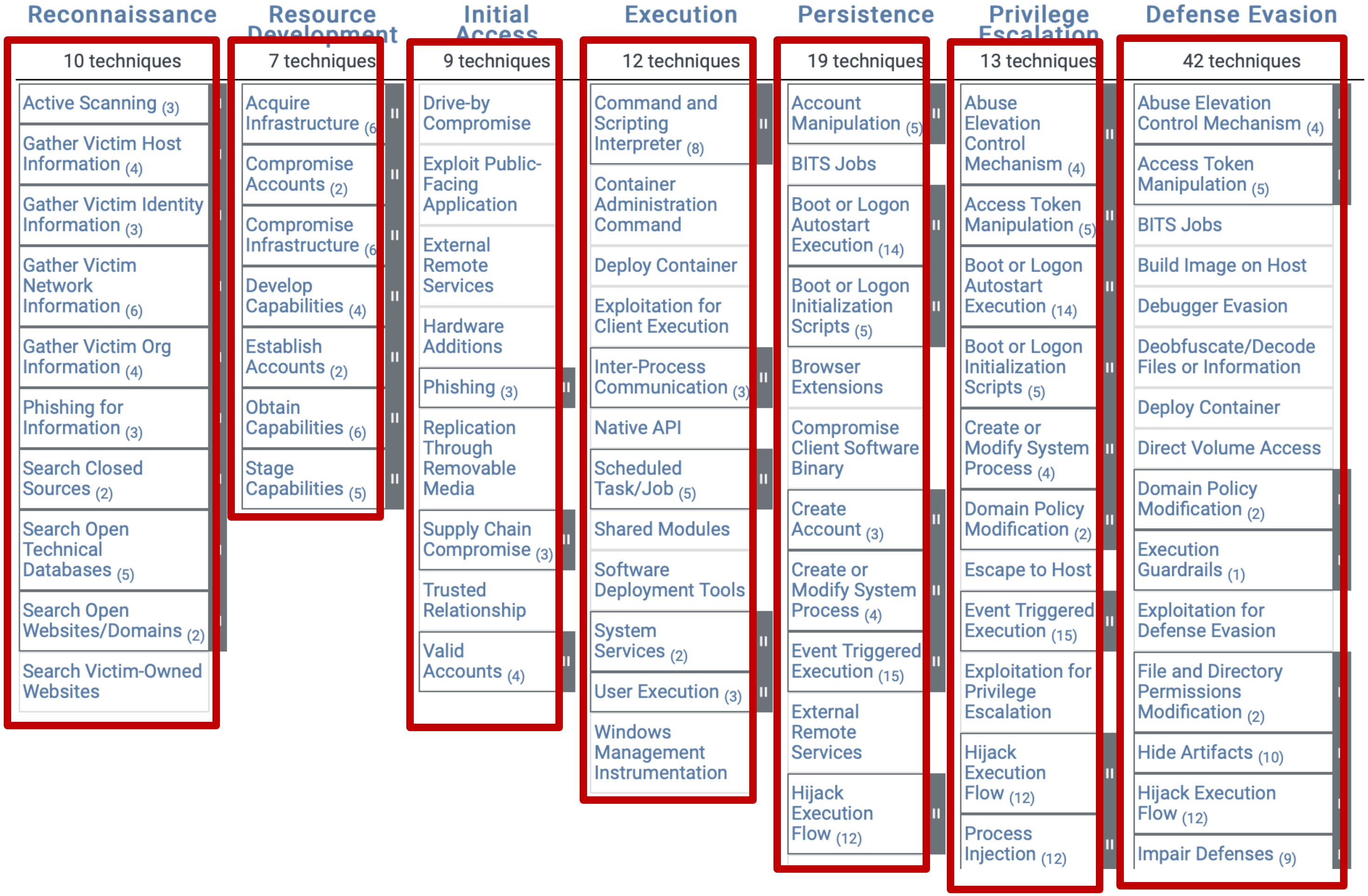
Exfiltration
9 techniques

- Automated Exfiltration (1)
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (1)
- Exfiltration Over Physical Medium (1)
- Exfiltration Over Web Service (2)
- Scheduled Transfer
- Transfer Data to Cloud Account

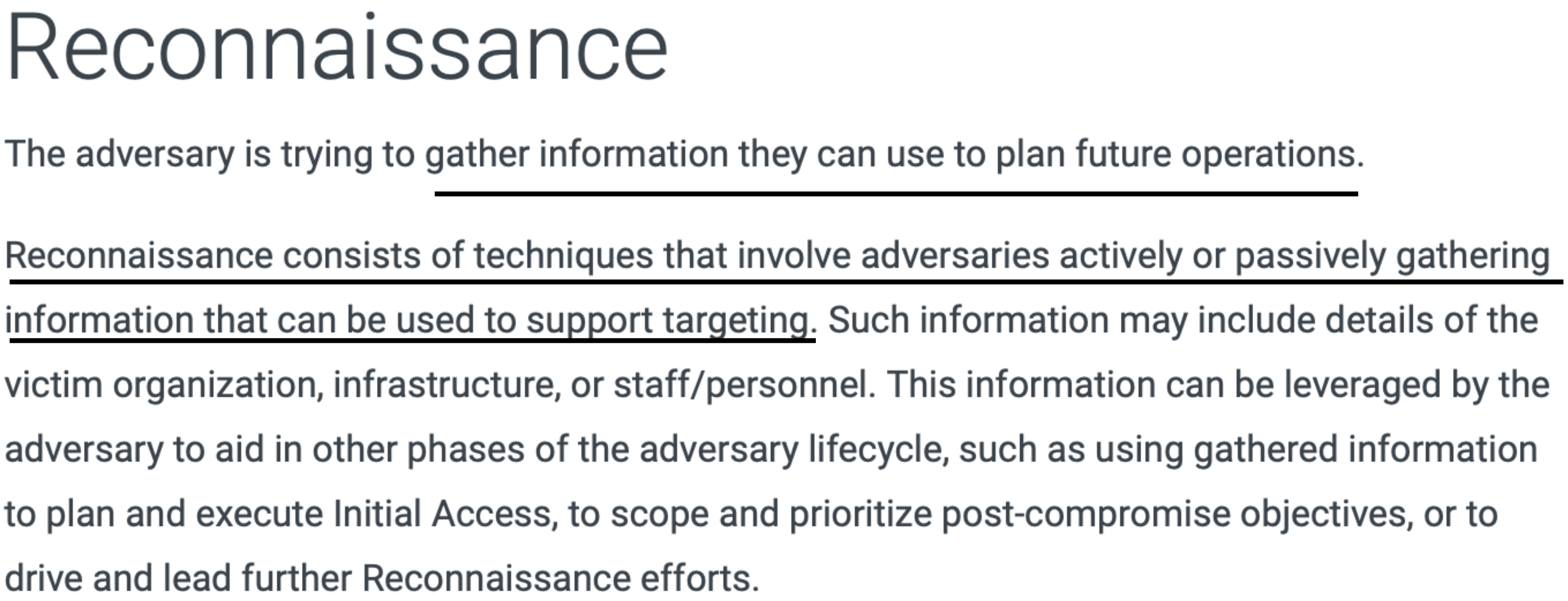
Impact
13 techniques

- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation (3)
- Defacement (2)
- Disk Wipe (2)
- Endpoint Denial of Service (4)
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service (2)
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

Techniques represent 'how' an adversary achieves a tactical goal by performing an action. For example, an adversary may dump credentials to achieve credential access.



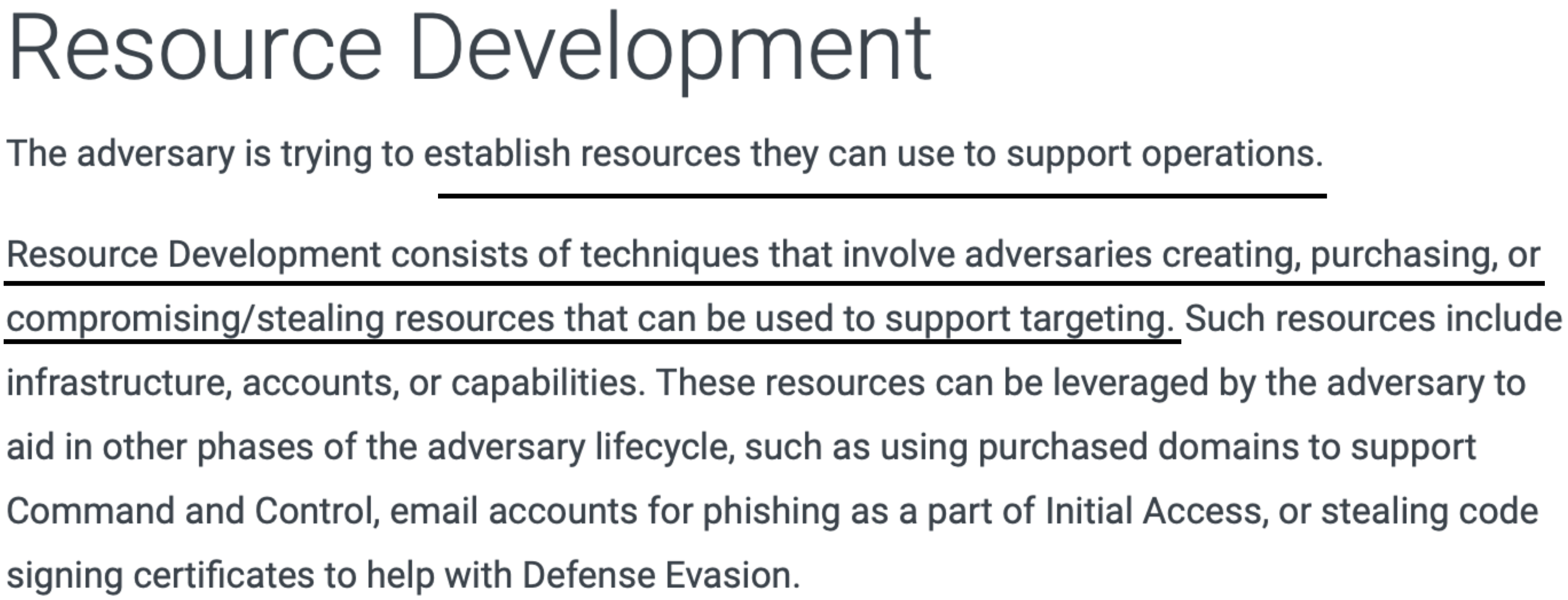
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion
10 techniques	7 techniques	9 techniques	12 techniques	19 techniques	13 techniques	42 techniques
Active Scanning (3)	Acquire Infrastructure (6	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (5)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)
Gather Victim Identity Information (3)	Compromise Infrastructure (6	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	BITS Jobs
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (3)	Browser Extensions	Create or Modify System Process (4)	Debugger Evasion
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Deobfuscate/Decode Files or Information
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create Account (3)	Escape to Host	Deploy Container
Search Open Technical Databases (5)		Trusted Relationship	Shared Modules	Create or Modify System Process (4)	Event Triggered Execution (15)	Direct Volume Access
Search Open Websites/Domains (2)		Valid Accounts (4)	Software Deployment Tools	Event Triggered Execution (15)	Exploitation for Privilege Escalation	Domain Policy Modification (2)
Search Victim-Owned Websites			System Services (2)	External Remote Services	Hijack Execution Flow (12)	Execution Guardrails (1)
			User Execution (3)	Hijack Execution Flow (12)	Process Injection (12)	Exploitation for Defense Evasion
			Windows Management Instrumentation			File and Directory Permissions Modification (2)
						Hide Artifacts (10)
						Hijack Execution Flow (12)
						Impair Defenses (9)



Reconnaissance

The adversary is trying to gather information they can use to plan future operations.

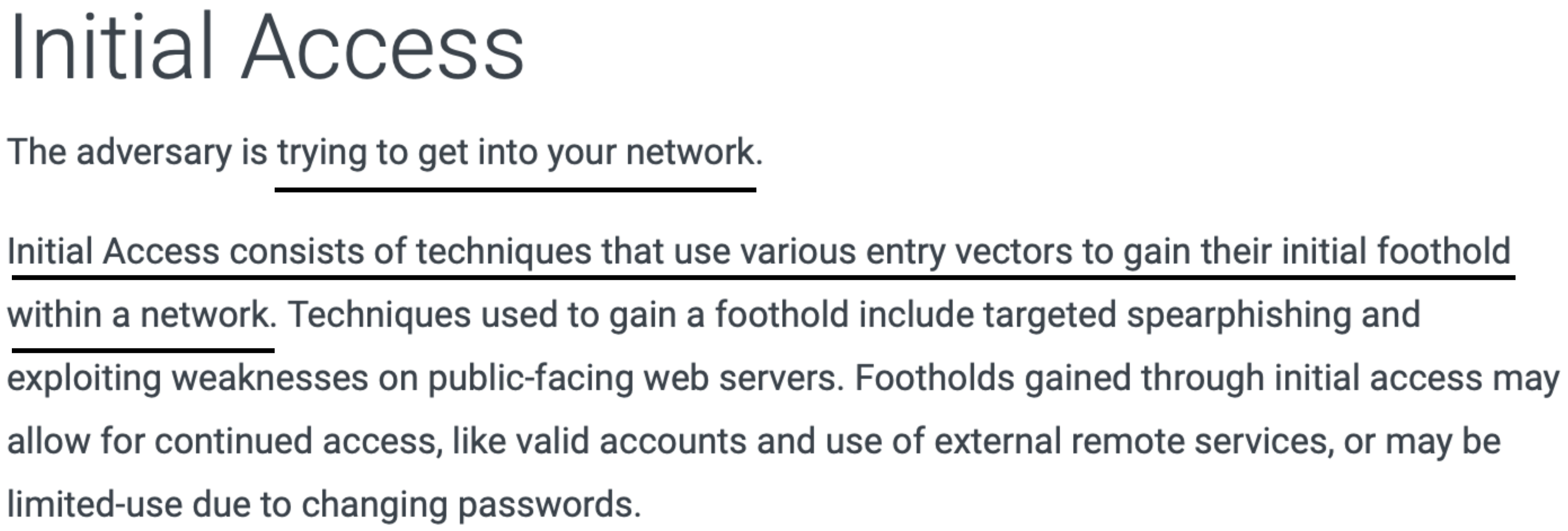
Reconnaissance consists of techniques that involve adversaries actively or passively gathering information that can be used to support targeting. Such information may include details of the victim organization, infrastructure, or staff/personnel. This information can be leveraged by the adversary to aid in other phases of the adversary lifecycle, such as using gathered information to plan and execute Initial Access, to scope and prioritize post-compromise objectives, or to drive and lead further Reconnaissance efforts.



Resource Development

The adversary is trying to establish resources they can use to support operations.

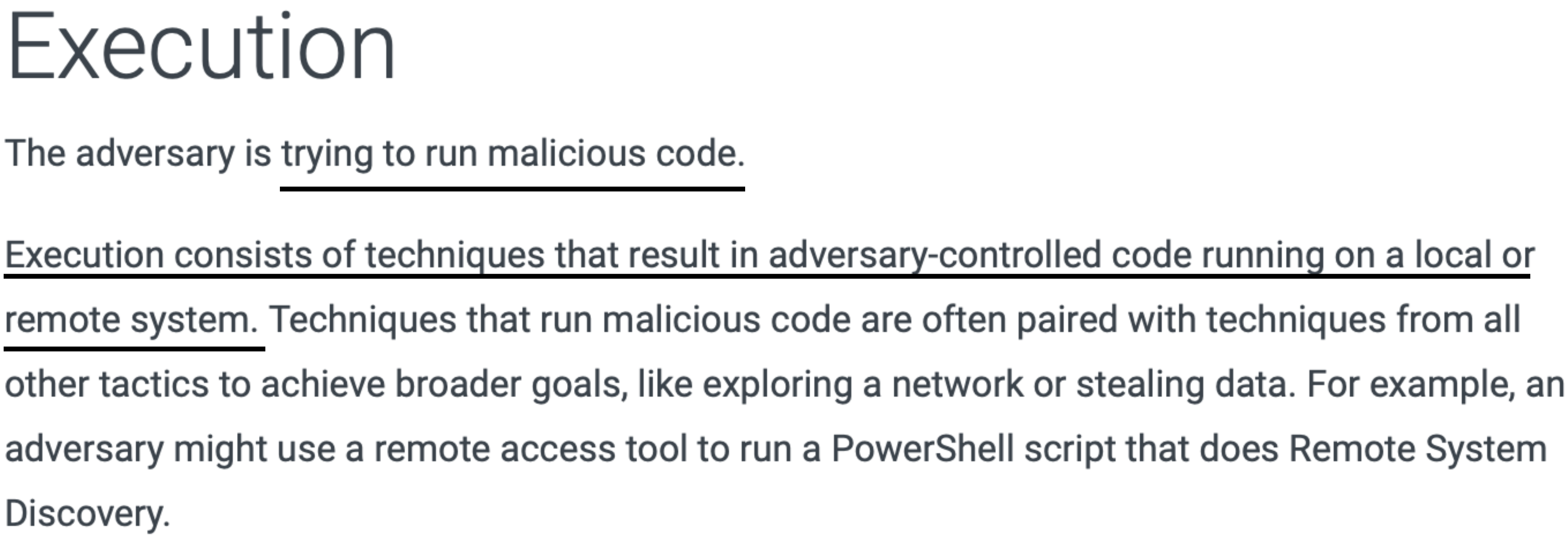
Resource Development consists of techniques that involve adversaries creating, purchasing, or compromising/stealing resources that can be used to support targeting. Such resources include infrastructure, accounts, or capabilities. These resources can be leveraged by the adversary to aid in other phases of the adversary lifecycle, such as using purchased domains to support Command and Control, email accounts for phishing as a part of Initial Access, or stealing code signing certificates to help with Defense Evasion.



Initial Access

The adversary is trying to get into your network.

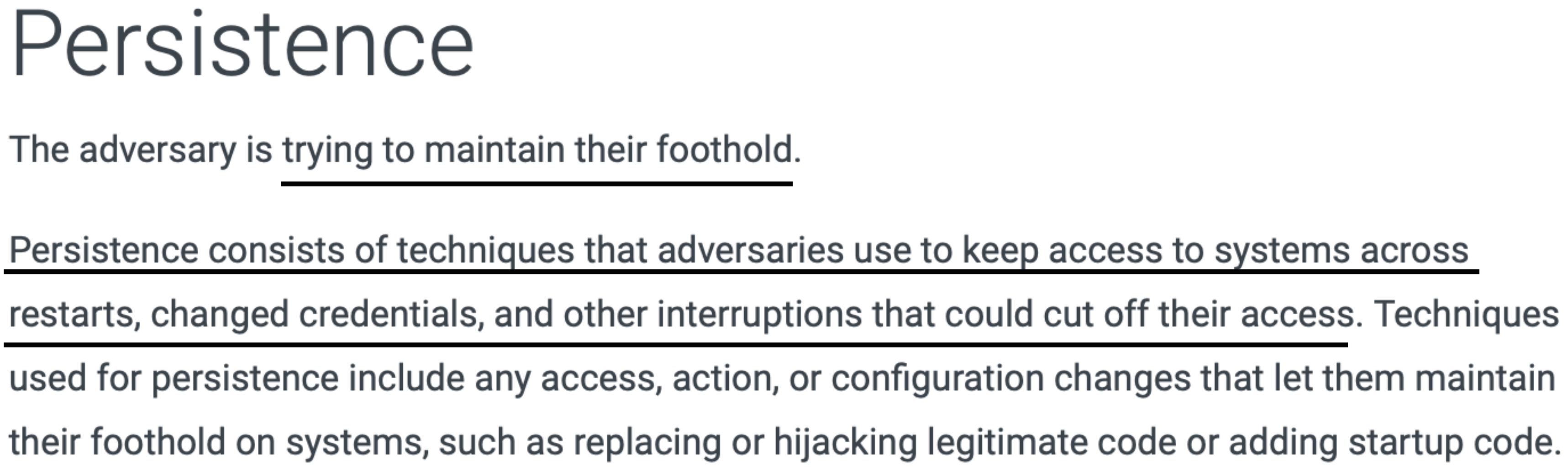
Initial Access consists of techniques that use various entry vectors to gain their initial foothold within a network. Techniques used to gain a foothold include targeted spearphishing and exploiting weaknesses on public-facing web servers. Footholds gained through initial access may allow for continued access, like valid accounts and use of external remote services, or may be limited-use due to changing passwords.



Execution

The adversary is trying to run malicious code.

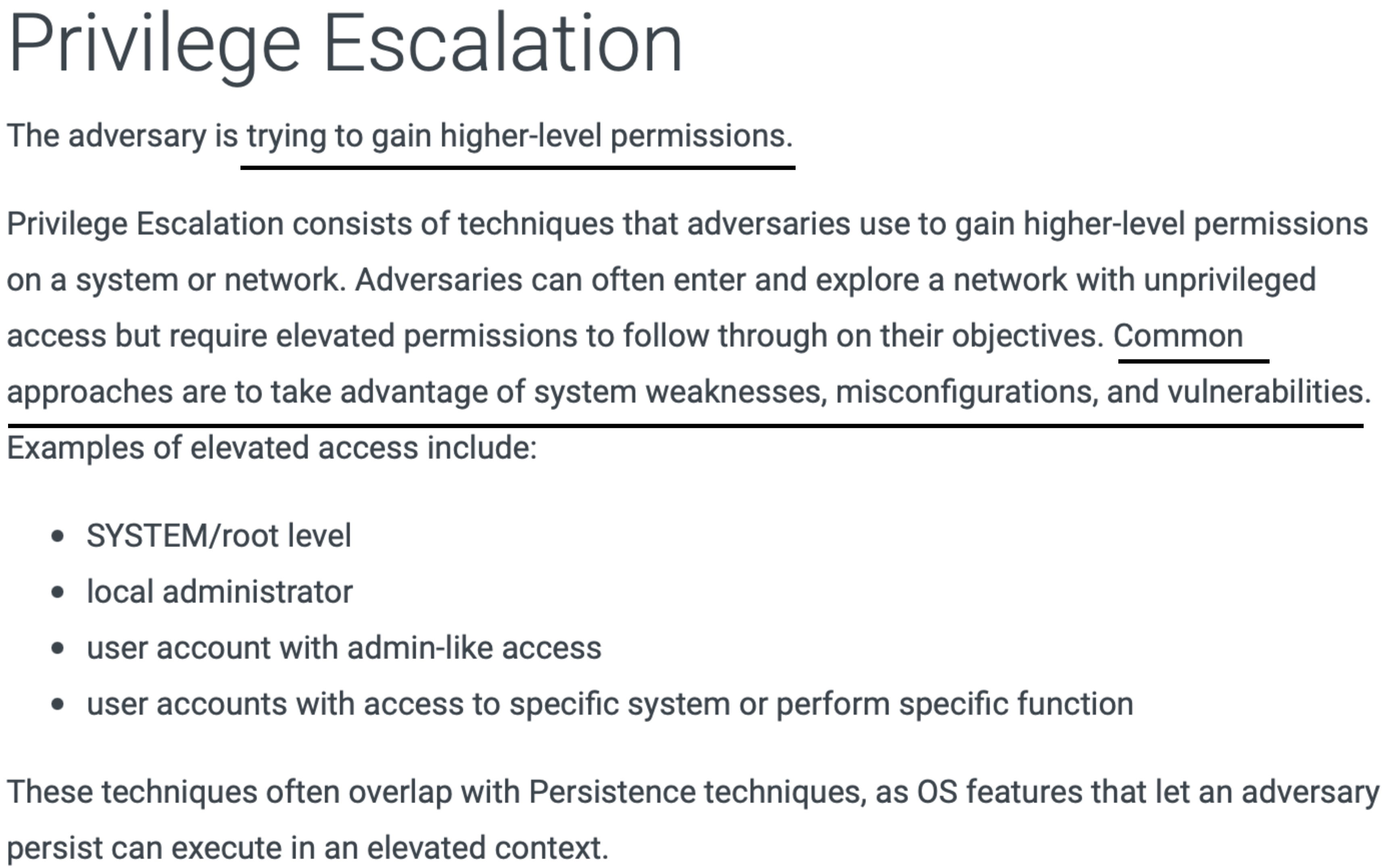
Execution consists of techniques that result in adversary-controlled code running on a local or remote system. Techniques that run malicious code are often paired with techniques from all other tactics to achieve broader goals, like exploring a network or stealing data. For example, an adversary might use a remote access tool to run a PowerShell script that does Remote System Discovery.



Persistence

The adversary is trying to maintain their foothold.

Persistence consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access. Techniques used for persistence include any access, action, or configuration changes that let them maintain their foothold on systems, such as replacing or hijacking legitimate code or adding startup code.



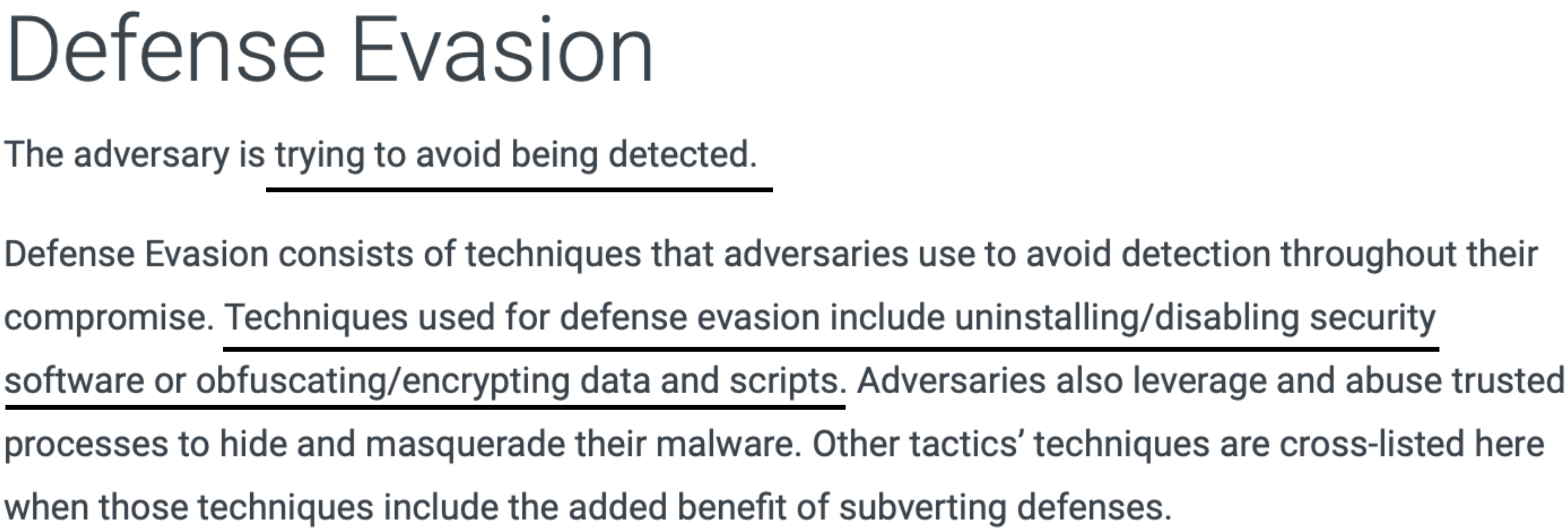
Privilege Escalation

The adversary is trying to gain higher-level permissions.

Privilege Escalation consists of techniques that adversaries use to gain higher-level permissions on a system or network. Adversaries can often enter and explore a network with unprivileged access but require elevated permissions to follow through on their objectives. Common approaches are to take advantage of system weaknesses, misconfigurations, and vulnerabilities. Examples of elevated access include:

- SYSTEM/root level
- local administrator
- user account with admin-like access
- user accounts with access to specific system or perform specific function

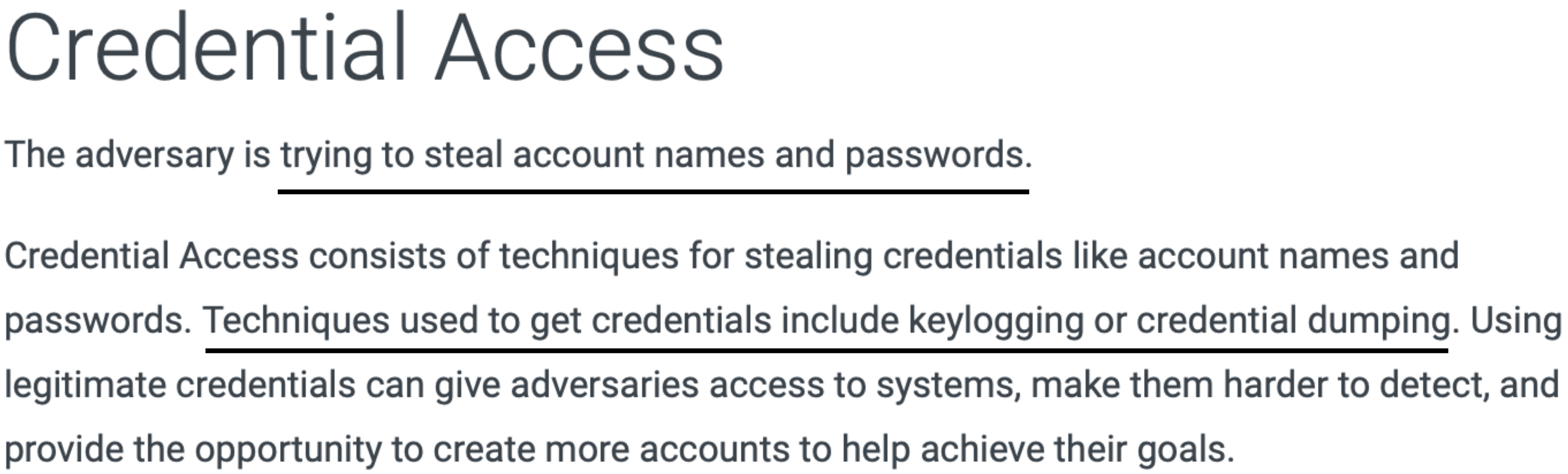
These techniques often overlap with Persistence techniques, as OS features that let an adversary persist can execute in an elevated context.



Defense Evasion

The adversary is trying to avoid being detected.

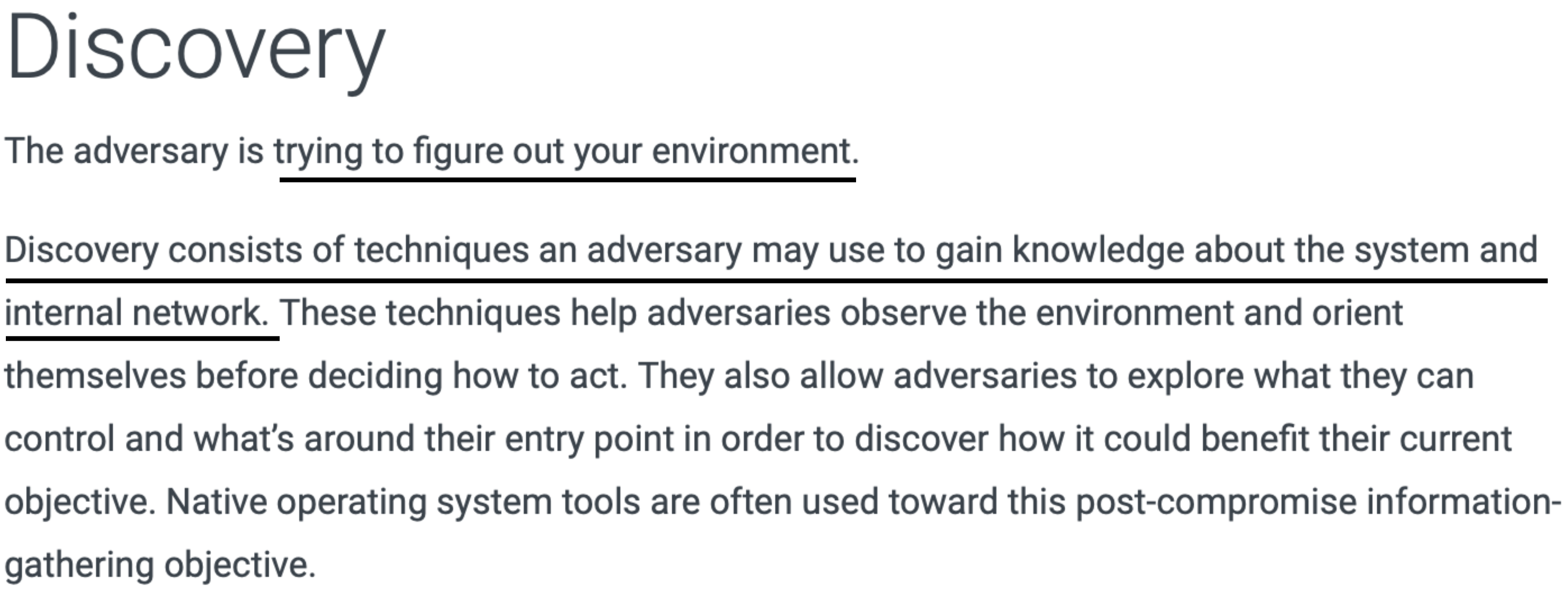
Defense Evasion consists of techniques that adversaries use to avoid detection throughout their compromise. Techniques used for defense evasion include uninstalling/disabling security software or obfuscating/encrypting data and scripts. Adversaries also leverage and abuse trusted processes to hide and masquerade their malware. Other tactics’ techniques are cross-listed here when those techniques include the added benefit of subverting defenses.



Credential Access

The adversary is trying to steal account names and passwords.

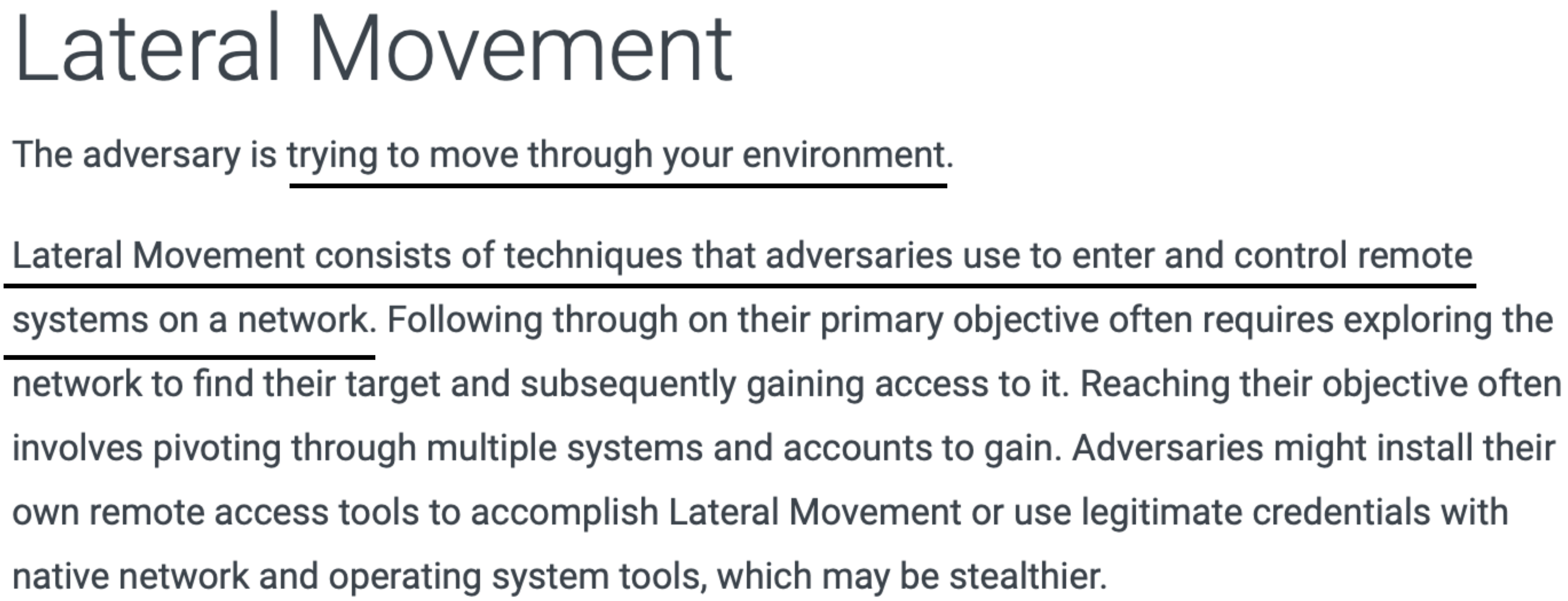
Credential Access consists of techniques for stealing credentials like account names and passwords. Techniques used to get credentials include keylogging or credential dumping. Using legitimate credentials can give adversaries access to systems, make them harder to detect, and provide the opportunity to create more accounts to help achieve their goals.



Discovery

The adversary is trying to figure out your environment.

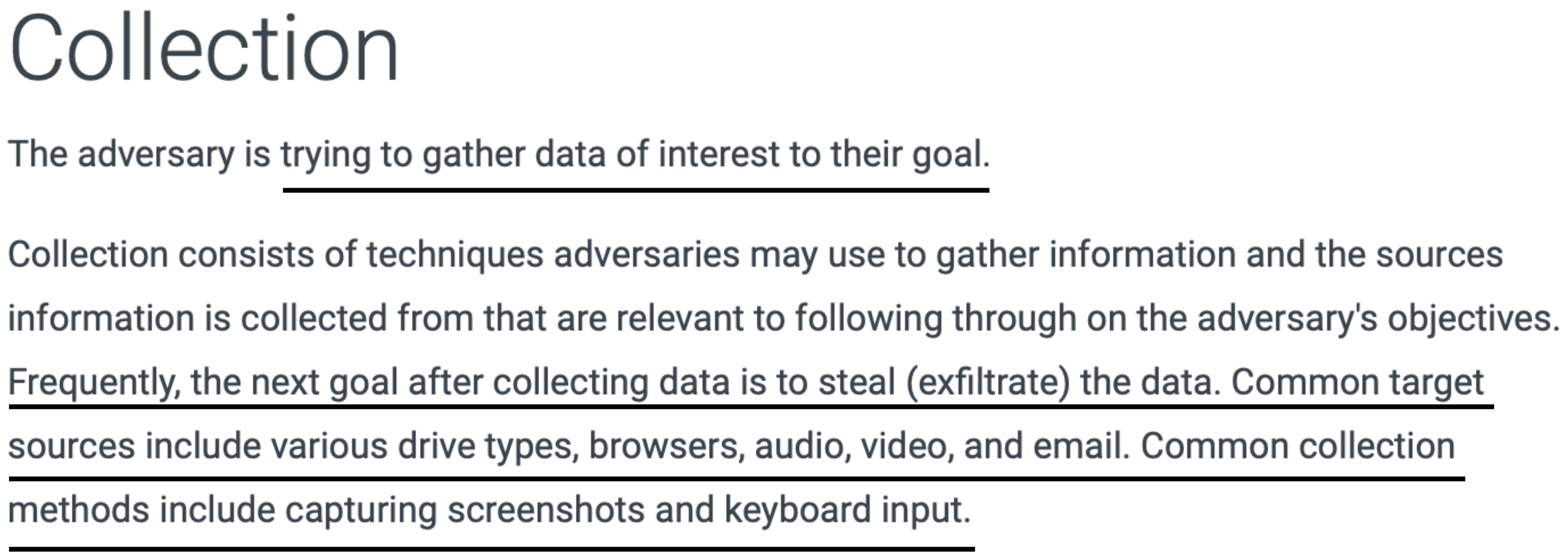
Discovery consists of techniques an adversary may use to gain knowledge about the system and internal network. These techniques help adversaries observe the environment and orient themselves before deciding how to act. They also allow adversaries to explore what they can control and what's around their entry point in order to discover how it could benefit their current objective. Native operating system tools are often used toward this post-compromise information-gathering objective.



Lateral Movement

The adversary is trying to move through your environment.

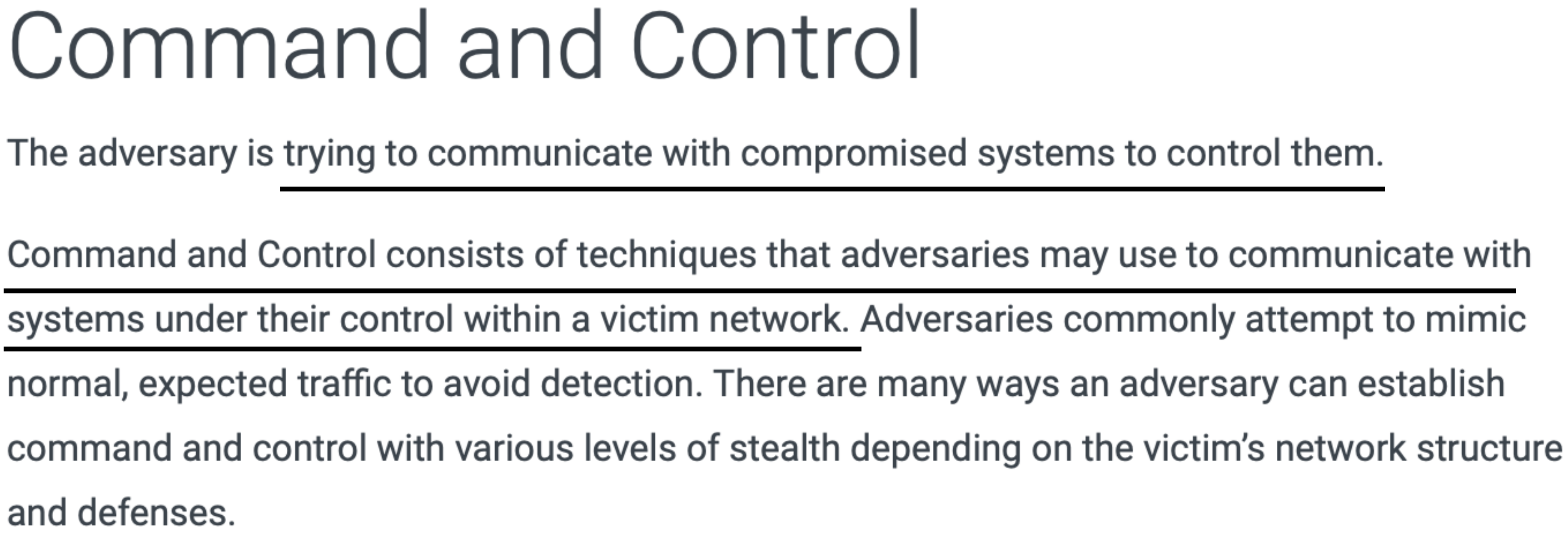
Lateral Movement consists of techniques that adversaries use to enter and control remote systems on a network. Following through on their primary objective often requires exploring the network to find their target and subsequently gaining access to it. Reaching their objective often involves pivoting through multiple systems and accounts to gain. Adversaries might install their own remote access tools to accomplish Lateral Movement or use legitimate credentials with native network and operating system tools, which may be stealthier.



Collection

The adversary is trying to gather data of interest to their goal.

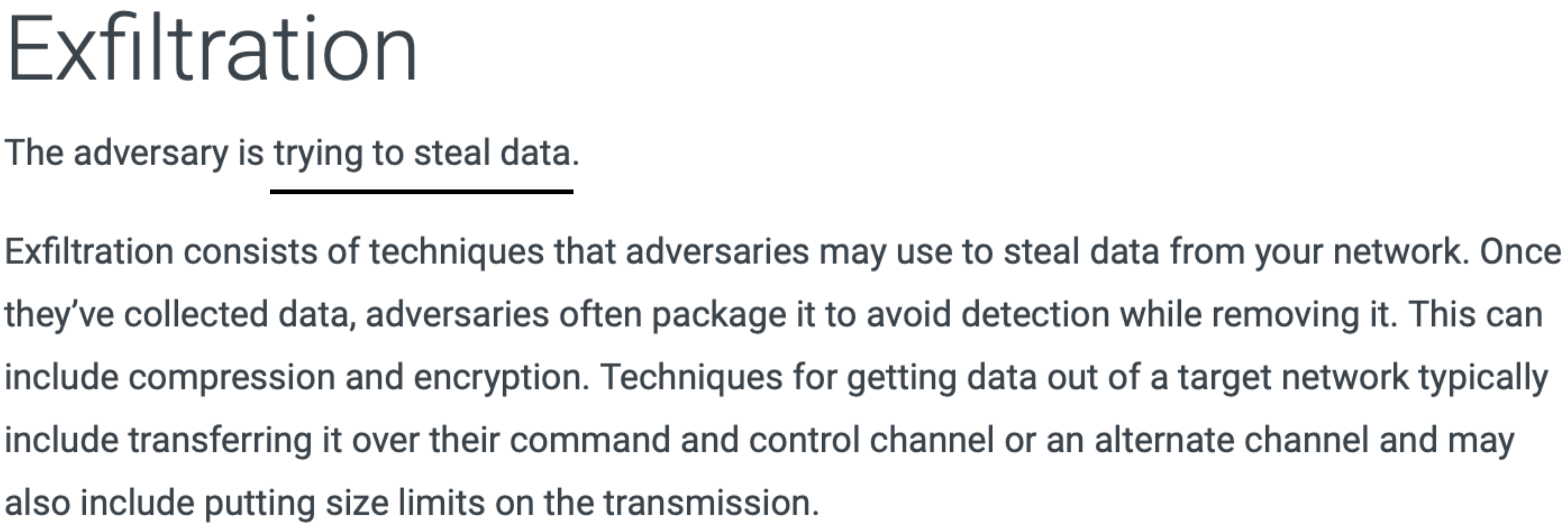
Collection consists of techniques adversaries may use to gather information and the sources information is collected from that are relevant to following through on the adversary's objectives. Frequently, the next goal after collecting data is to steal (exfiltrate) the data. Common target sources include various drive types, browsers, audio, video, and email. Common collection methods include capturing screenshots and keyboard input.



Command and Control

The adversary is trying to communicate with compromised systems to control them.

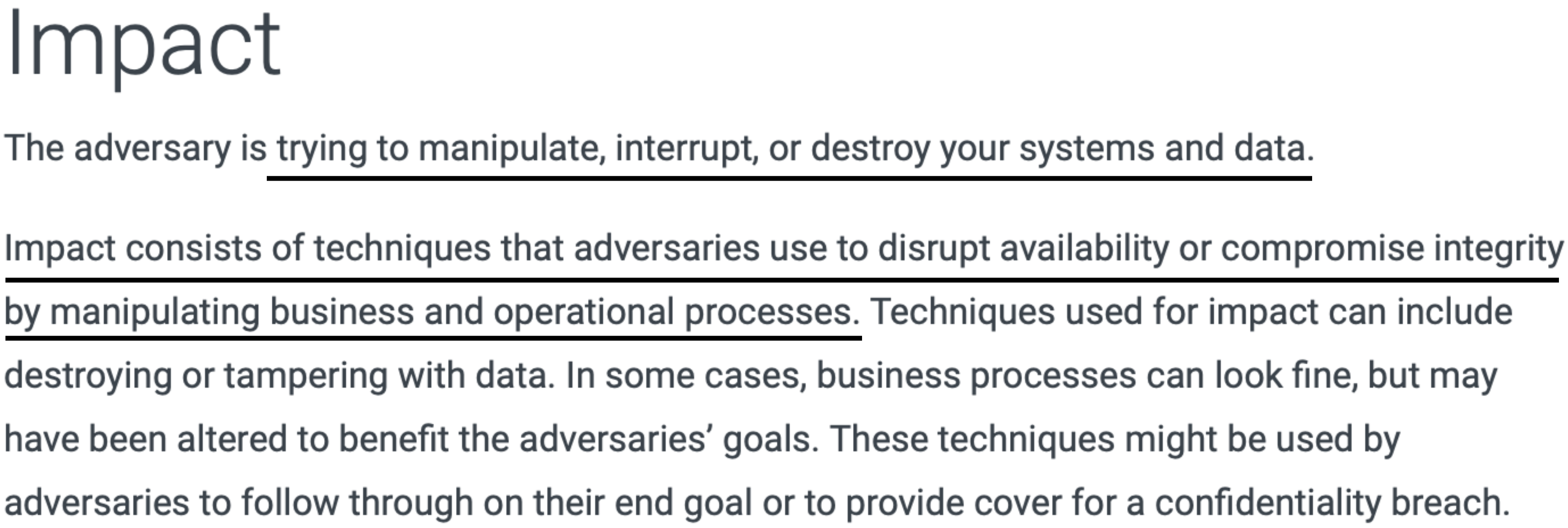
Command and Control consists of techniques that adversaries may use to communicate with systems under their control within a victim network. Adversaries commonly attempt to mimic normal, expected traffic to avoid detection. There are many ways an adversary can establish command and control with various levels of stealth depending on the victim's network structure and defenses.



Exfiltration

The adversary is trying to steal data.

Exfiltration consists of techniques that adversaries may use to steal data from your network. Once they've collected data, adversaries often package it to avoid detection while removing it. This can include compression and encryption. Techniques for getting data out of a target network typically include transferring it over their command and control channel or an alternate channel and may also include putting size limits on the transmission.



Impact

The adversary is trying to manipulate, interrupt, or destroy your systems and data.

Impact consists of techniques that adversaries use to disrupt availability or compromise integrity by manipulating business and operational processes. Techniques used for impact can include destroying or tampering with data. In some cases, business processes can look fine, but may have been altered to benefit the adversaries' goals. These techniques might be used by adversaries to follow through on their end goal or to provide cover for a confidentiality breach.

Mitigations

- **Mitigation represent security concepts and classes of technologies that can be used to prevent a technique or sub-technique from being successfully executed.**

https://attack.mitre.org/mitigations/enterprise/

End of Lecture 2