Using MITRE ATT&CK for better communication

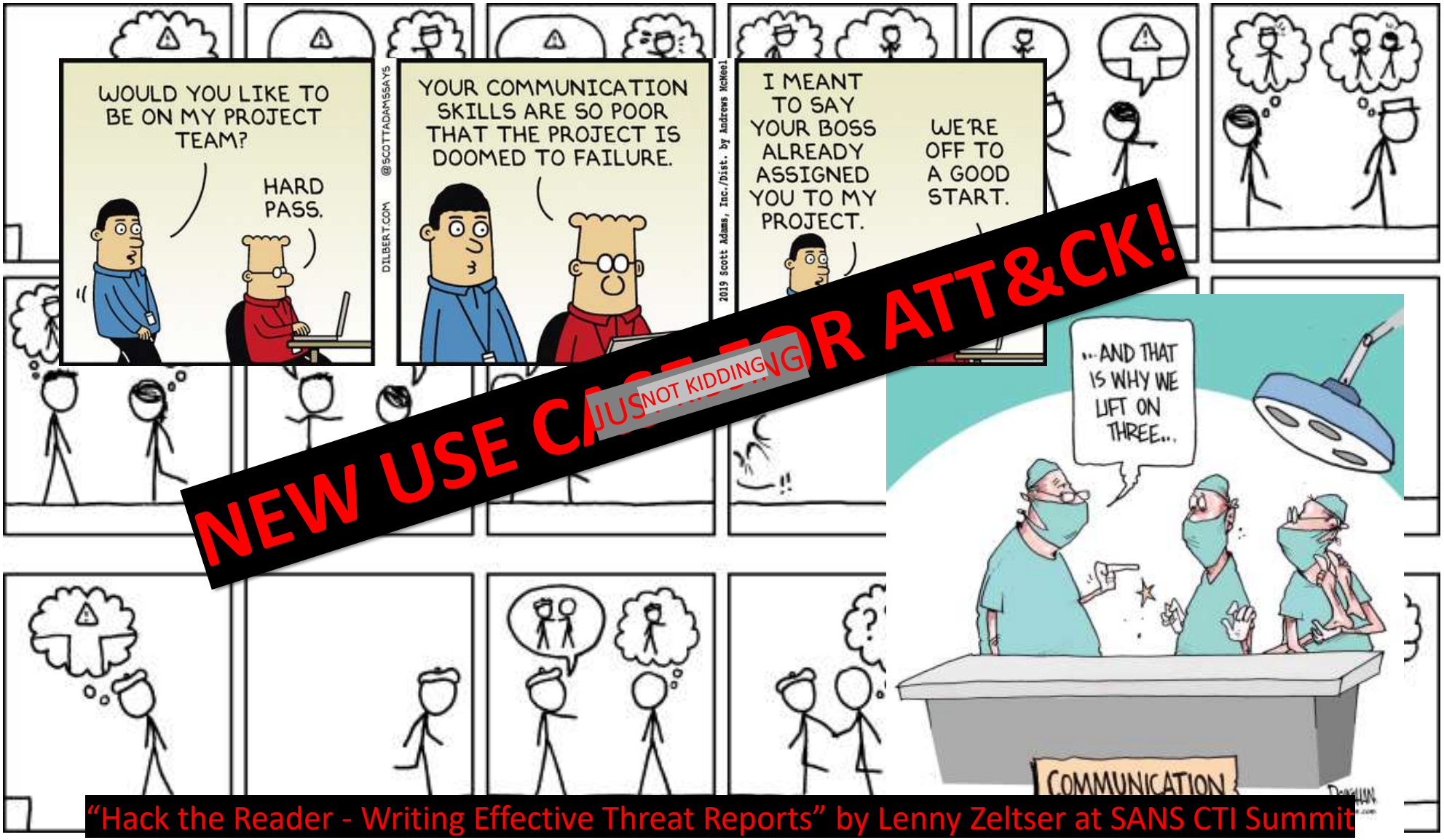
Philip Winther

user@attack:~$ whoami

- Cyber Security Analyst
- SARS-CoV-2 (COVID19) negative
- Purveyor of fine UTF-8 art

It really doesn't matter

¯_(ツ)_/¯



"Hack the Reader - Writing Effective Threat Reports" by Lenny Zeltser at SANS CTI Summit

New use case for ATT&CK?

- ATT&CK library as reference work
- ATT&CK words/concepts as standard phrasing
- Easy to read, concise, procedural stories that are understandable by laypeople, powered by ATT&CK

Case 1 – initial access stories

Client: ”… it was a phishing attack that used a fake Google Chrome update to trick the user.”

After some meetings and clarifications:
Client: ”About the attack vector – it was not a phishing attempt that caused the attack. The user searched on Google with specific keywords. One of the websites they visited was compromised. When they visited the website a prompt blocking them from viewing the website asked them to update Google Chrome to view the website.

User visits hxxps://$DOMAIN{dot}$TLD/$KEYWORDS/
file:///C:/Chrome.zip
User interacts with Google.com searching for “$KEYWORDS””

What we communicated:
”The story for Initial Access[1] is:
A user ($FULLNAME <$EMAILACCOUNT>) makes a query on google.com for “$KEYWORDS". A website $NAME visits through this query is "https://$DOMAIN[.]$TLD/$KEYWORDS/". This website prompts $NAME to upgrade their Google Chrome browser to view the content. The file "C:\Chrome.zip" is downloaded and executed on $NAME's computer.

This is categorized as a Drive-By Compromise[2] technique, and we estimate that it is unlikely to be a targeted attack, due to the unpredictable nature of user interaction in this situation.”

TACTICS

Enterprise
- Reconnaissance
- Resource Development
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration
- Impact

Mobile

Home > Tactics > Enterprise > Initial Access

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.

ID: TA0001
Created: 17 October 2018
Last Modified: 19 July 2019

Version Permalink

Techniques

Techniques: 9

ID	Name	Description
T1189	Drive-by Compromise	Adversaries may gain access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is typically targeted for exploitation, but adversaries may also use compromised websites for non-exploitation behavior such as acquiring Application Access Token.
T1190	Exploit Public-Facing Application	Adversaries may attempt to take advantage of a weakness in an Internet-facing computer or program using software, data, or commands in order to cause unintended or unanticipated behavior. The weakness in the system can be a bug, a glitch, or a design vulnerability. These applications are often websites, but can include databases (like SQL), standard services (like SMB or SSH), network device administration and management protocols (like SNMP and Smart Install), and any other applications with Internet accessible open sockets, such as web servers and related services. Depending on the flaw being exploited this may include Exploitation for Defense Evasion.
T1133	External Remote Services	Adversaries may leverage external-facing remote services to initially access and/or persist within a network. Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential authentication for these services. Services such as Windows Remote Management can also be used externally.
T1200	Hardware Additions	Adversaries may introduce computer accessories, computers, or networking hardware into a system or network that can be used as a vector to gain access. While public references of usage by APT groups are scarce, many penetration testers leverage hardware additions for initial access. Commercial and open source products are leveraged with capabilities such as passive network tapping , man-in-the middle encryption breaking , keystroke injection , kernel memory reading via DMA , adding new wireless access to an existing network , and others.

Drive-by Compromise

Adversaries may gain access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is typically targeted for exploitation, but adversaries may also use compromised websites for non-exploitation behavior such as acquiring Application Access Token.

Multiple ways of delivering exploit code to a browser exist, including:

- A legitimate website is compromised where adversaries have injected some form of malicious code such as JavaScript, iFrames, and cross-site scripting.
- Malicious ads are paid for and served through legitimate ad providers.
- Built-in web application interfaces are leveraged for the insertion of any other kind of object that can be used to display web content or contain a script that executes on the visiting client (e.g. forum posts, comments, and other user controllable web content).

Often the website used by an adversary is one visited by a specific community, such as government, a particular industry, or region, where the goal is to compromise a specific user or set of users based on a shared interest. This kind of targeted attack is referred to a strategic web compromise or watering hole attack. There are several known examples of this occurring.[1]

Typical drive-by compromise process:

1. A user visits a website that is used to host the adversary controlled content.
2. Scripts automatically execute, typically searching versions of the browser and plugins for a potentially vulnerable version.
   - The user may be required to assist in this process by enabling scripting or active website components and ignoring warning dialog boxes.
3. Upon finding a vulnerable version, exploit code is delivered to the browser.
4. If exploitation is successful, then it will give the adversary code execution on the user's system unless other protections are in place.
   - In some cases a second visit to the website after the initial scan is required before exploit code is delivered.

Unlike Exploit Public-Facing Application, the focus of this technique is to exploit software on a client endpoint upon visiting a website. This will commonly give an adversary access to systems on the internal network instead of external systems that may be in a DMZ.

ID: T1189

Sub-techniques: No sub-techniques

Tactic: Initial Access

Platforms: Linux, SaaS, Windows, macOS

Permissions Required: User

Data Sources: Application Log: Application Log Content, File: File Creation, Network Traffic: Network Connection Creation, Network Traffic: Network Traffic Content, Process: Process Creation

Contributors: Jeff Sakowicz, Microsoft Identity Developer Platform Services (IDPM Services); Saisha Agrawal, Microsoft Threat Intelligent Center (MSTIC)

Version: 1.2

Created: 18 April 2018

Last Modified: 29 March 2020

Version Permalink

Case 2 – categorizing attacks and talking about threat environments

Initial version: ”In the collection period, research has uncovered a great deal of information regarding attacks of different calibers and with different targets, and the attack on $CLIENT is assessed to fit relatively well into this overall threat environment.”

Version 2.0: “In the collection period, research has uncovered a great deal of information regarding attacks of different calibers and with different targets, for example an attack on Solarwind using a mix of off-the-shelf components, such as the Cobalt Strike tool, and custom made malware such as SUNBURST, and an attack on Microsoft Exchange deploying a new critical vulnerability. The attack on $CLIENT is assessed to fit relatively well into this overall threat environment.”

And with a little help from ATT&CK:
”Cyber threat intelligence research has found a great deal of information regarding cyber-attacks of different calibers and with different targets, e.g., the SolarWinds supply chain compromise[1] targeting a wide variety of large private and public organizations. The attack on $CLIENT is assessed to fit relatively well into this overall threat environment, where large organizations and institutions are indirectly targeted for financial or intellectual gain by nation state threat actors, such as Lazarus Group[2], or criminal organizations, such as FIN7[3].”

Supply Chain Compromise

Sub-techniques (3)

Adversaries may manipulate products or product delivery mechanisms prior to receipt by a final consumer for the purpose of data or system compromise.

Supply chain compromise can take place at any stage of the supply chain including:

- Manipulation of development tools
- Manipulation of a development environment
- Manipulation of source code repositories (public or private)
- Manipulation of source code in open-source dependencies
- Manipulation of software update/distribution mechanisms
- Compromised/infected system images (multiple cases of removable media infected at the factory) [1] [2]
- Replacement of legitimate software with modified versions
- Sales of modified/counterfeit products to legitimate distributors
- Shipment interdiction

While supply chain compromise can impact any component of hardware or software, attackers looking to gain execution have often focused on malicious additions to legitimate software in software distribution or update channels. [3] [4] [5] Targeting may be specific to a desired victim set [6] or malicious software may be distributed to a broad set of consumers but only move on to additional tactics on specific victims. [3] [5] Popular open source projects that are used as dependencies in many applications may also be targeted as a means to add malicious code to users of the dependency. [7]

ID: T1195
Sub-techniques: T1195.001, T1195.002, T1195.003
Tactic: Initial Access
Platforms: Linux, Windows, macOS
CAPEC ID: CAPEC-437, CAPEC-438, CAPEC-439
Contributors: Veeral Patel
Version: 1.2
Created: 18 April 2018
Last Modified: 06 January 2021

Version Permalink

Mitigations

ID	Mitigation	Description

GROUPS

Overview
admin@338
Ajax Security Team
APT-C-36
APT1
APT12
APT16
APT17
APT18
APT19
APT28
APT29
APT3
APT30
APT32
APT33
APT37
APT38
APT39
APT41

Lazarus Group

Lazarus Group is a threat group that has been attributed to the North Korean government.[1] The group has been active since at least 2009 and was reportedly responsible for the November 2014 destructive wiper attack against Sony Pictures Entertainment as part of a campaign named Operation Blockbuster by Novetta. Malware used by Lazarus Group correlates to other reported campaigns, including Operation Flame, Operation 1Mission, Operation Troy, DarkSeoul, and Ten Days of Rain.[2] In late 2017, Lazarus Group used KillDisk, a disk-wiping tool, in an attack against an online casino based in Central America.[3]

North Korean group definitions are known to have significant overlap, and the name Lazarus Group is known to encompass a broad range of activity. Some organizations use the name Lazarus Group to refer to any activity attributed to North Korea.[1] Some organizations track North Korean clusters or groups such as Bluenoroff,[4] APT37, and APT38 separately, while other organizations may track some activity associated with those group names by the name Lazarus Group.

ID: G0032

Associated Groups: HIDDEN COBRA, Guardians of Peace, ZINC, NICKEL ACADEMY

Version: 1.5

Created: 31 May 2017

Last Modified: 18 March 2021

Version Permalink

Associated Group Descriptions

Name	Description
HIDDEN COBRA	The U.S. Government refers to malicious cyber activity by the North Korean government as HIDDEN COBRA.[1][5]
Guardians of Peace	[1]
ZINC	[6]
NICKEL ACADEMY	[7]

Techniques Used

ATT&CK® Navigator Layers

GROUPS

Overview
admin@338
Ajax Security Team
APT-C-36
APT1
APT12
APT16
APT17
APT18
APT19
APT28
APT29
APT3
APT30
APT32
APT33
APT37
APT38
APT39
APT41
Axiom

FIN7

FIN7 is a financially-motivated threat group that has primarily targeted the U.S. retail, restaurant, and hospitality sectors since mid-2015. They often use point-of-sale malware. A portion of FIN7 was run out of a front company called Combi Security. FIN7 is sometimes referred to as Carbanak Group, but these appear to be two groups using the same Carbanak malware and are therefore tracked separately. [1] [2] [3] [4]

ID: G0046
Version: 1.5
Created: 31 May 2017
Last Modified: 22 October 2020

Version Permalink

Techniques Used

ATT&CK® Navigator Layers

Domain	ID		Name	Use
Enterprise	T1071	.004	Application Layer Protocol: DNS	FIN7 has performed C2 using DNS via A, OPT, and TXT records.[4]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	FIN7 malware has created Registry Run and RunOnce keys to establish persistence, and has also added items to the Startup folder.[2][4]
Enterprise	T1059		Command and Scripting Interpreter	FIN7 used SQL scripts to help perform tasks on the victim's machine.[4][5][4]
		.001	PowerShell	FIN7 used a PowerShell script to launch shellcode that retrieved an additional payload.[7][4]
		.003	Windows Command Shell	FIN7 used the command prompt to launch commands on the victim's machine.[4][5]
		.005	Visual Basic	FIN7 used VBS scripts to help perform tasks on the victim's machine.[4][5]
		.007	JavaScript	FIN7 used JavaScript scripts to help perform tasks on the victim's machine.[4][5][4]
Enterprise	T1543	.003	Create or Modify System Process: Windows Service	FIN7 created new Windows services and added them to the startup directories for persistence.[4]

Challenges!

- ATT&CK does not cover everything
- Context is important
- ATT&CK is not designed for our consumers
- Loss of information is important to avoid

What about undiscovered APTs?

TTPs come and go in the metagame

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.

Trivial mitigations might block techniques – e.g. NAT

Find this hash on Deep Visibility

Hitting the right amount of context is key!

Copy Details Download Threat File

Agent Policy

Behavioral AI

pe Dynamic

Generic.Heuristic

N/A

[redacted]

[redacted]

[redacted]

[redacted]

THREAT INDICATORS (7) NOTES

Ransomware

Deletes shadow copy.
MITRE : Impact [T1490]

Reconnaissance

Suspicious WMI query was identified.
MITRE : Execution [T1047]
MITRE : Discovery [T1518.001]

Injection

A library owned by one process was loaded to other process.
MITRE : Defense Evasion [T1574.001]
MITRE : Privilege Escalation [T1574.001]
MITRE : Persistence [T1574.001]

Exploitation

Shellcode execution from Powershell was detected.
MITRE : Execution [T1059.001][T1106]

Shellcode execution was detected.
MITRE : Execution [T1106]

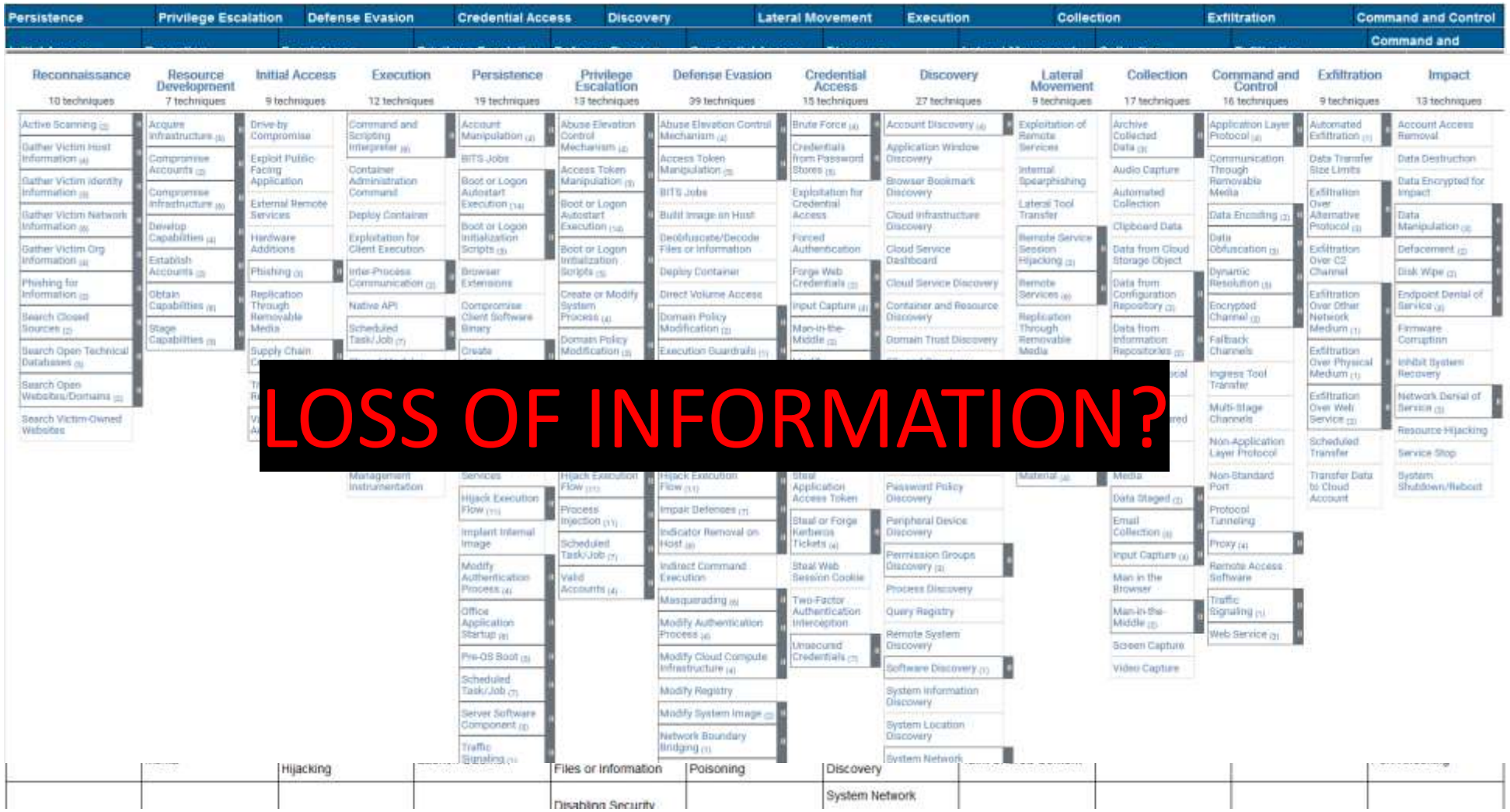
Evasion

Application added firewall rules to allow network traffic.
MITRE : Exfiltration [T1041]
MITRE : Defense Evasion [T1562.004]

Infostealer

Blocked read access to LSASS.
MITRE : Credential Access [T1003]

The view from the perspective of a large portion of our consumers:


Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Execution
Collection
Exfiltration
Command and Control
Reconnaissance
10 techniques
Resource Development
7 techniques
Initial Access
9 techniques
Execution
12 techniques
Persistence
19 techniques
Privilege Escalation
13 techniques
Defense Evasion
39 techniques
Credential Access
15 techniques
Discovery
27 techniques
Lateral Movement
9 techniques
Collection
17 techniques
Command and Control
16 techniques
Exfiltration
9 techniques
Impact
13 techniques
LOSS OF INFORMATION?

Conclusion!

What our clients like:

- Using MITRE ATT&CK library as reference work
- Streamlined wording/phrasing
- Easy to read stories with optional further reading

Hopefully, this will start a discourse that will improve ATT&CK in this use case for posterity.

Questions?

pw@certaintelligence.com
@analyzing:matrix.org