ISACA®

San Francisco Chapter

The ATT&CK Matrix

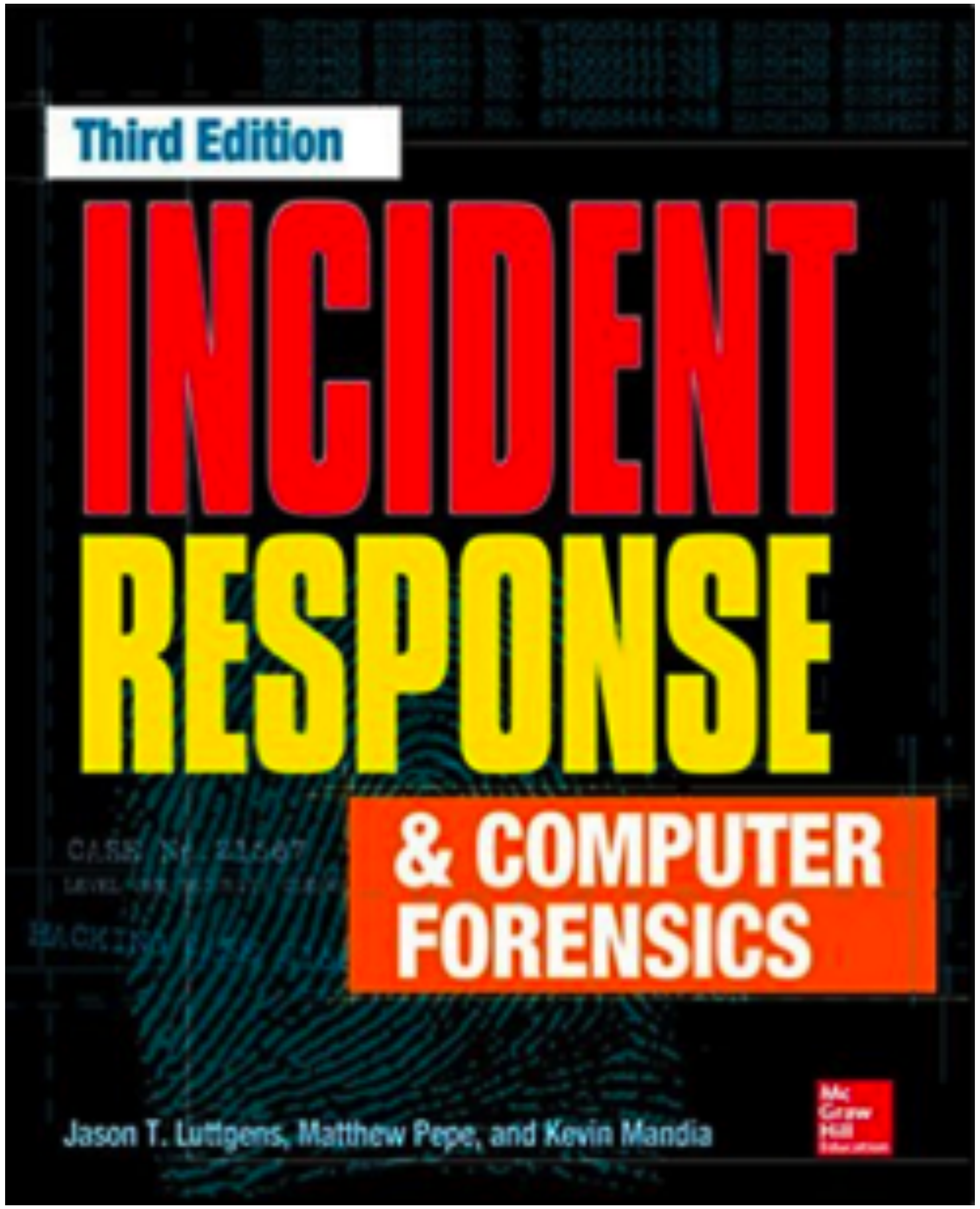
Sam Bowne
Oct 26, 2020

Who

- Sam Bowne
- Twitter: **@sambowne**
- Instructor, City College San Francisco
- Founder, Infosec Decoded, Inc.
- All slides, lecture videos, projects, etc. free at
  - **samsclass.info**
- All classes free online worldwide

CNIT 152: Incident Response

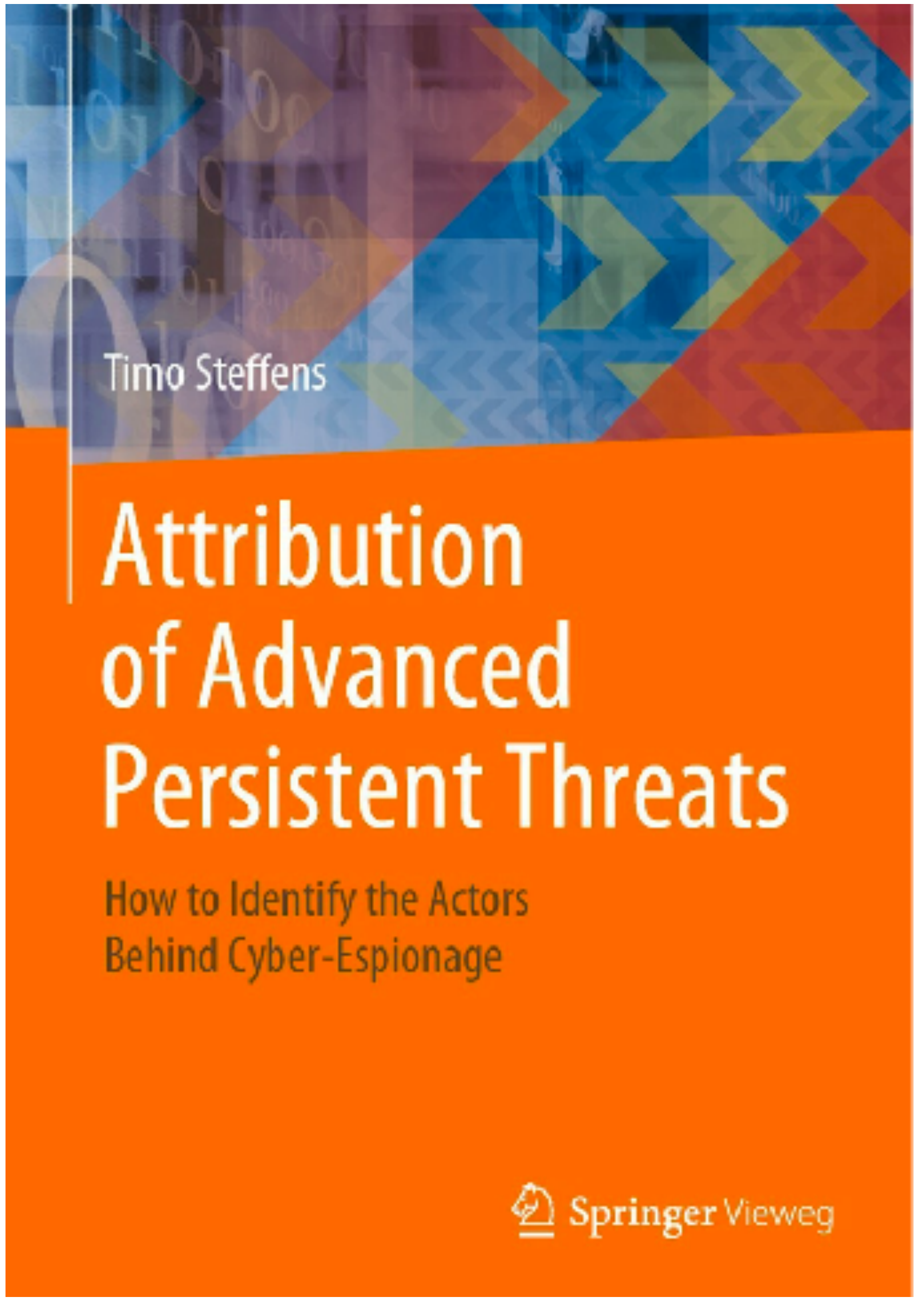
Fall 2020 Sam Bowne



Third Edition

INCIDENT RESPONSE & COMPUTER FORENSICS

Jason T. Luttgens, Matthew Pepe, and Kevin Mandia



Timo Steffens

Attribution of Advanced Persistent Threats

How to Identify the Actors Behind Cyber-Espionage

Springer Vieweg

ATT&CK Matrix

Reference: ATT&CK Matrix v7 for Enterprise

ATT 1: ATT&CK Tactics	10
ATT 2: ATT&CK Techniques for Tactics 1-3	10
ATT 3: ATT&CK Techniques for Tactics 4-6	10
ATT 4: ATT&CK Techniques for Tactics 7-9	10
ATT 5: ATT&CK Techniques for Tactics 10-12	10
ATT 6: ATT&CK Groups	10
ATT 7: ATT&CK Navigator	10
ATT 100: Caldera	25+
ATT 101: Caldera Operation	15

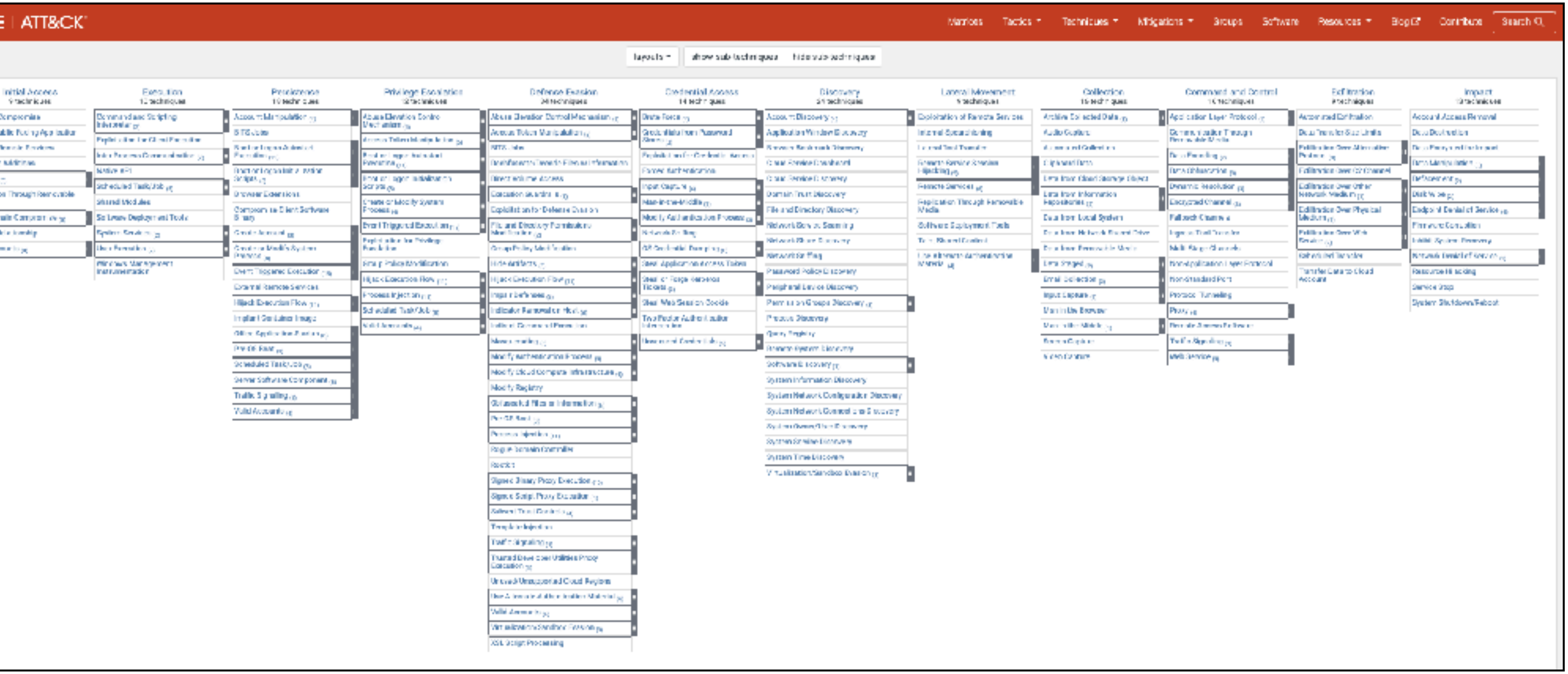
ATT&CK

- A framework to address four issues
  - **Adversary behaviors**: tactics and techniques
  - **Lifecycle models** better than the Cyber Kill Chain
  - **Applicability to real environments**
  - **Common taxonomy**

Tactics and Techniques

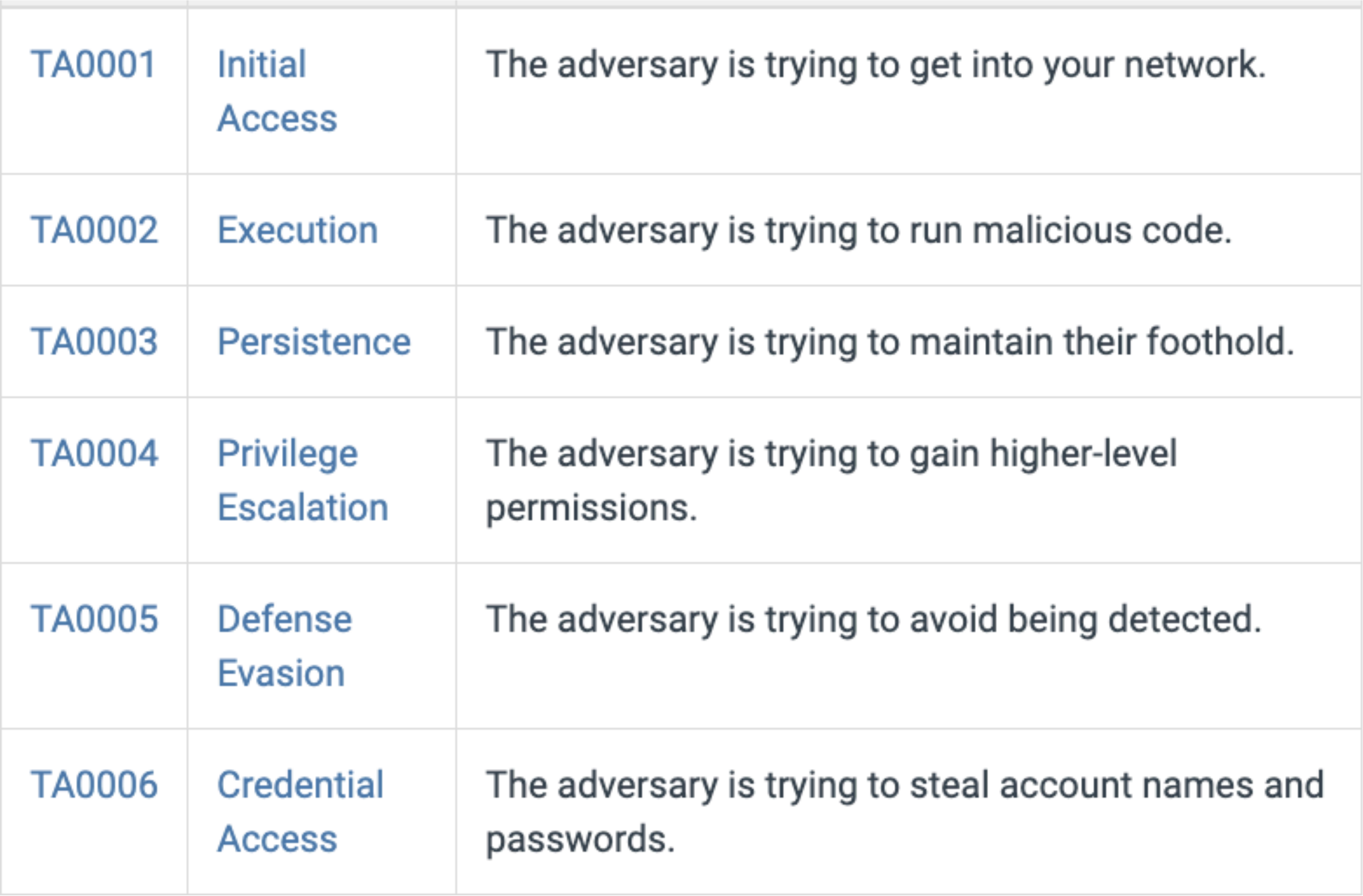
- Tactics
  - Adversary objective: the "why"
- Techniques
  - The "how"

The ATT&CK Matrix



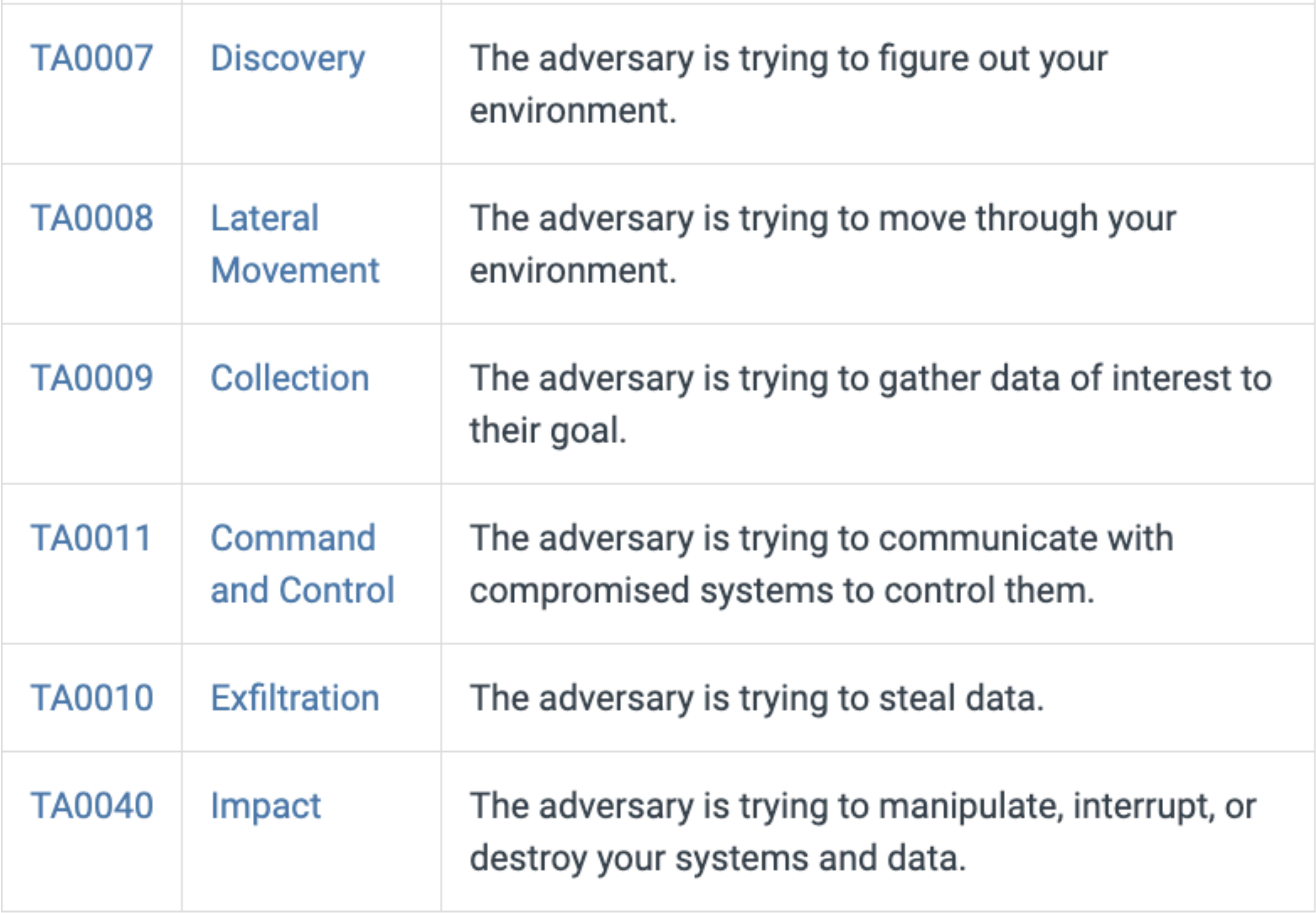
itial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
9 techniques	10 techniques	18 techniques	12 techniques	34 techniques	14 techniques	24 techniques	9 techniques	16 techniques	16 techniques	9 techniques	13 techniques
Compromise	Command and Scripting Interpreter	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Brute Force	Account Discovery	Exploitation of Remote Services	Archive Collected Data	Application Layer Protocol	Automated Exfiltration	Account Access Removal
blic-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Credentials from Password Stores	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
emote Services	Inter-Process Communication	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
Additions	Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Service Session Hijacking	Clipboard Data	Data Obfuscation	Exfiltration Over C2 Channel	Data Manipulation
g	Scheduled Task/Job	Browser Extensions	Create or Modify System Process	Direct Volume Access	Input Capture	Cloud Service Discovery	Remote Services	Data from Cloud Storage Object	Dynamic Resolution	Exfiltration Over Other Network Medium	Defacement
on Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution	Execution Guardrails	Man-in-the-Middle	Domain Trust Discovery	Replication Through Removable Media	Data from Information Repositories	Encrypted Channel	Exfiltration Over Physical Medium	Disk Wipe
ain Compromise	Software Deployment Tools	Create Account	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Modify Authentication Process	File and Directory Discovery	Software Deployment Tools	Data from Local System	Fallback Channels	Exfiltration Over Web Service	Endpoint Denial of Service
Relationship	System Services	Create or Modify System Process	Group Policy Modification	File and Directory Permissions Modification	Network Sniffing	Network Service Scanning	Taint Shared Content	Data from Network Shared Drive	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
counts	User Execution	Event Triggered Execution	Hijack Execution Flow	Group Policy Modification	OS Credential Dumping	Network Share Discovery	Use Alternate Authentication Material	Data from Removable Media	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
	Windows Management Instrumentation	External Remote Services	Process Injection	Hide Artifacts	Steal Application Access Token	Network Sniffing		Data Staged	Non-Application Layer Protocol		Network Denial of Service
		Hijack Execution Flow	Scheduled Task/Job	Hijack Execution Flow	Steal or Forge Kerberos Tickets	Password Policy Discovery		Email Collection	Non-Standard Port		Resource Hijacking
		Implant Container Image	Valid Accounts	Impair Defenses	Steal Web Session Cookie	Peripheral Device Discovery		Input Capture	Protocol Tunneling		Service Stop
		Office Application Startup		Indicator Removal on Host	Two-Factor Authentication Interception	Permission Groups Discovery		Man in the Browser	Proxy		System Shutdown/Reboot
		Pre-OS Boot		Indirect Command Execution	Unsecured Credentials	Process Discovery		Man-in-the-Middle	Remote Access Software		
		Scheduled Task/Job		Masquerading		Query Registry		Screen Capture	Traffic Signaling		
		Server Software Component		Modify Authentication Process		Remote System Discovery		Video Capture	Web Service		
		Traffic Signaling		Modify Cloud Compute Infrastructure		Software Discovery					
		Valid Accounts		Modify Registry		System Information Discovery					
				Obfuscated Files or Information		System Network Configuration Discovery					
				Pre-OS Boot		System Network Connections Discovery					
				Process Injection		System Owner/User Discovery					
				Rogue Domain Controller		System Service Discovery					
				Rootkit		System Time Discovery					
				Signed Binary Proxy Execution		Virtualization/Sandbox Evasion					
				Signed Script Proxy Execution							
				Subvert Trust Controls							
				Template Injection							
				Traffic Signaling							
				Trusted Developer Utilities Proxy Execution							
				Unused/Unsupported Cloud Regions							
				Use Alternate Authentication Material							
				Valid Accounts							
				Virtualization/Sandbox Evasion							
				XSL Script Processing							

Tactics



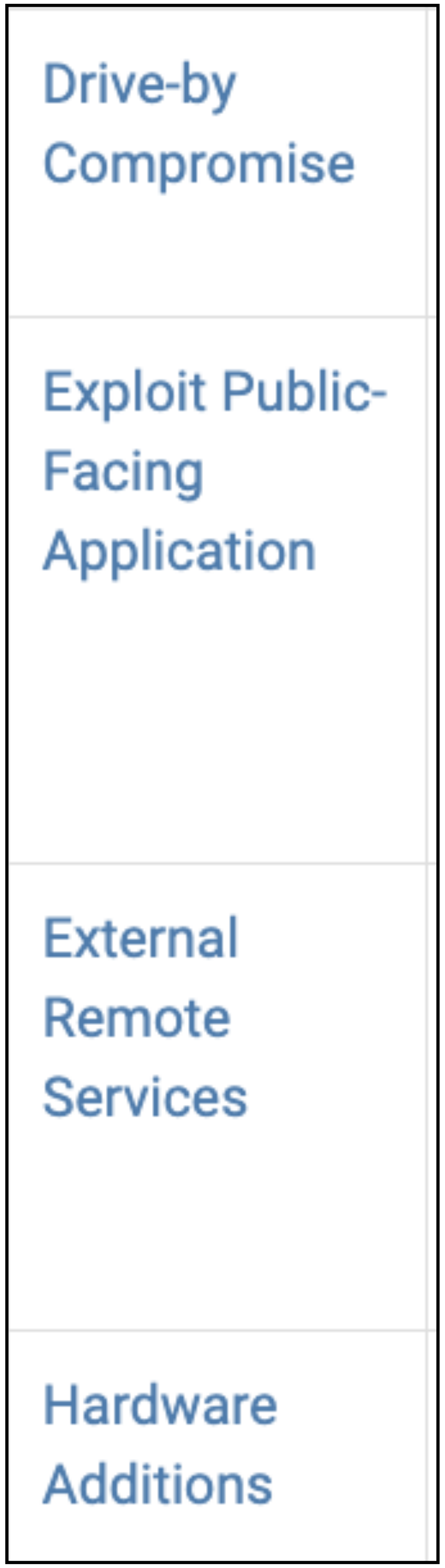
TA0001	Initial Access	The adversary is trying to get into your network.
TA0002	Execution	The adversary is trying to run malicious code.
TA0003	Persistence	The adversary is trying to maintain their foothold.
TA0004	Privilege Escalation	The adversary is trying to gain higher-level permissions.
TA0005	Defense Evasion	The adversary is trying to avoid being detected.
TA0006	Credential Access	The adversary is trying to steal account names and passwords.

Tactics



TA0007	Discovery	The adversary is trying to figure out your environment.
TA0008	Lateral Movement	The adversary is trying to move through your environment.
TA0009	Collection	The adversary is trying to gather data of interest to their goal.
TA0011	Command and Control	The adversary is trying to communicate with compromised systems to control them.
TA0010	Exfiltration	The adversary is trying to steal data.
TA0040	Impact	The adversary is trying to manipulate, interrupt, or destroy your systems and data.

Techniques

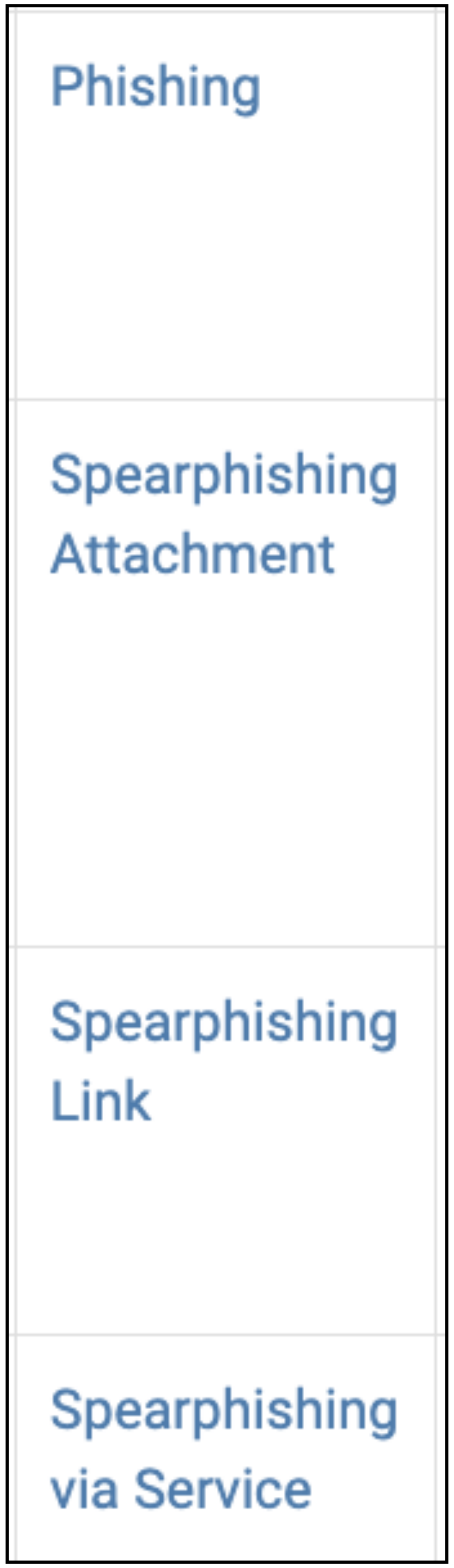


Drive-by Compromise

Exploit Public-Facing Application

External Remote Services

Hardware Additions

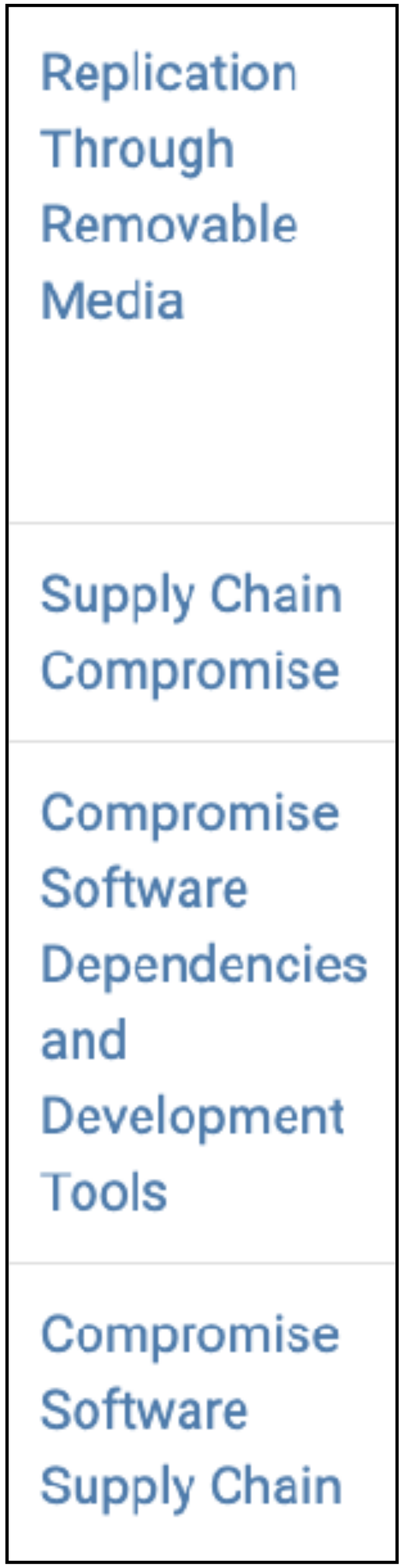


Phishing

Spearphishing Attachment

Spearphishing Link

Spearphishing via Service



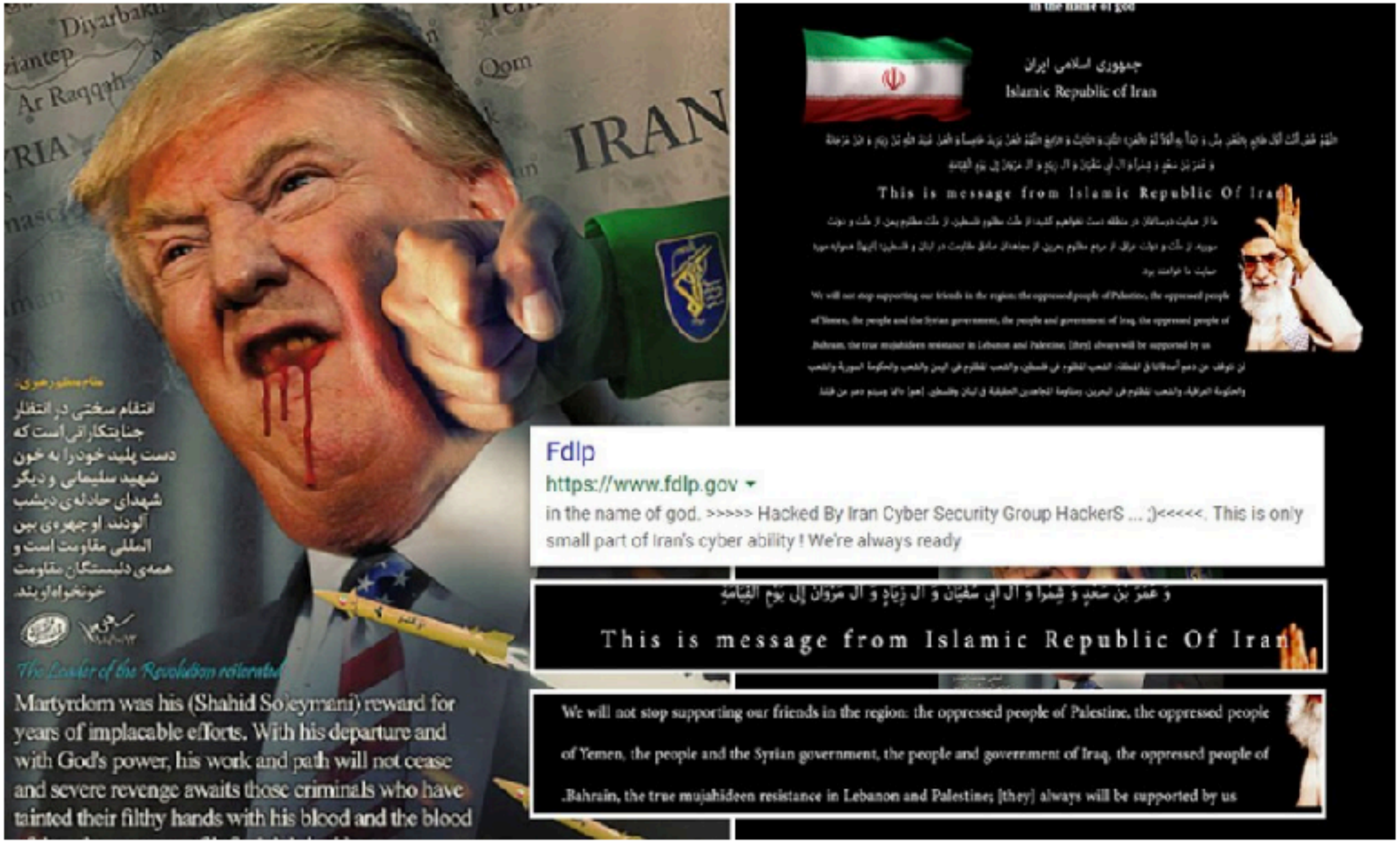
Replication Through Removable Media

Supply Chain Compromise

Compromise Software Dependencies and Development Tools

Compromise Software Supply Chain

Iran



انتقام سختی در انتظار
جنایتکارانی است که
دست پلید خود را به خون
شهید سلیمانی و دیگر
شهدای حادثه‌ی دیشب
آلودند او چهره‌ی بین
المللی مقاومت است و
همه‌ی دلبستگان مقاومت
خونخواه اویند.

The Leader of the Revolution reiterated

Martyrdom was his (Shahid Soleymani) reward for years of implacable efforts. With his departure and with God's power, his work and path will not cease and severe revenge awaits those criminals who have tainted their filthy hands with his blood and the blood

in the name of god

جمهوری اسلامی ایران
Islamic Republic of Iran

This is message from Islamic Republic Of Iran

We will not stop supporting our friends in the region: the oppressed people of Palestine, the oppressed people of Yemen, the people and the Syrian government, the people and government of Iraq, the oppressed people of Bahrain, the true mujahideen resistance in Lebanon and Palestine; [they] always will be supported by us

Fdlp
https://www.fdlp.gov ▾
in the name of god. >>>>> Hacked By Iran Cyber Security Group HackerS ... ;)<<<<<. This is only small part of Iran's cyber ability ! We're always ready

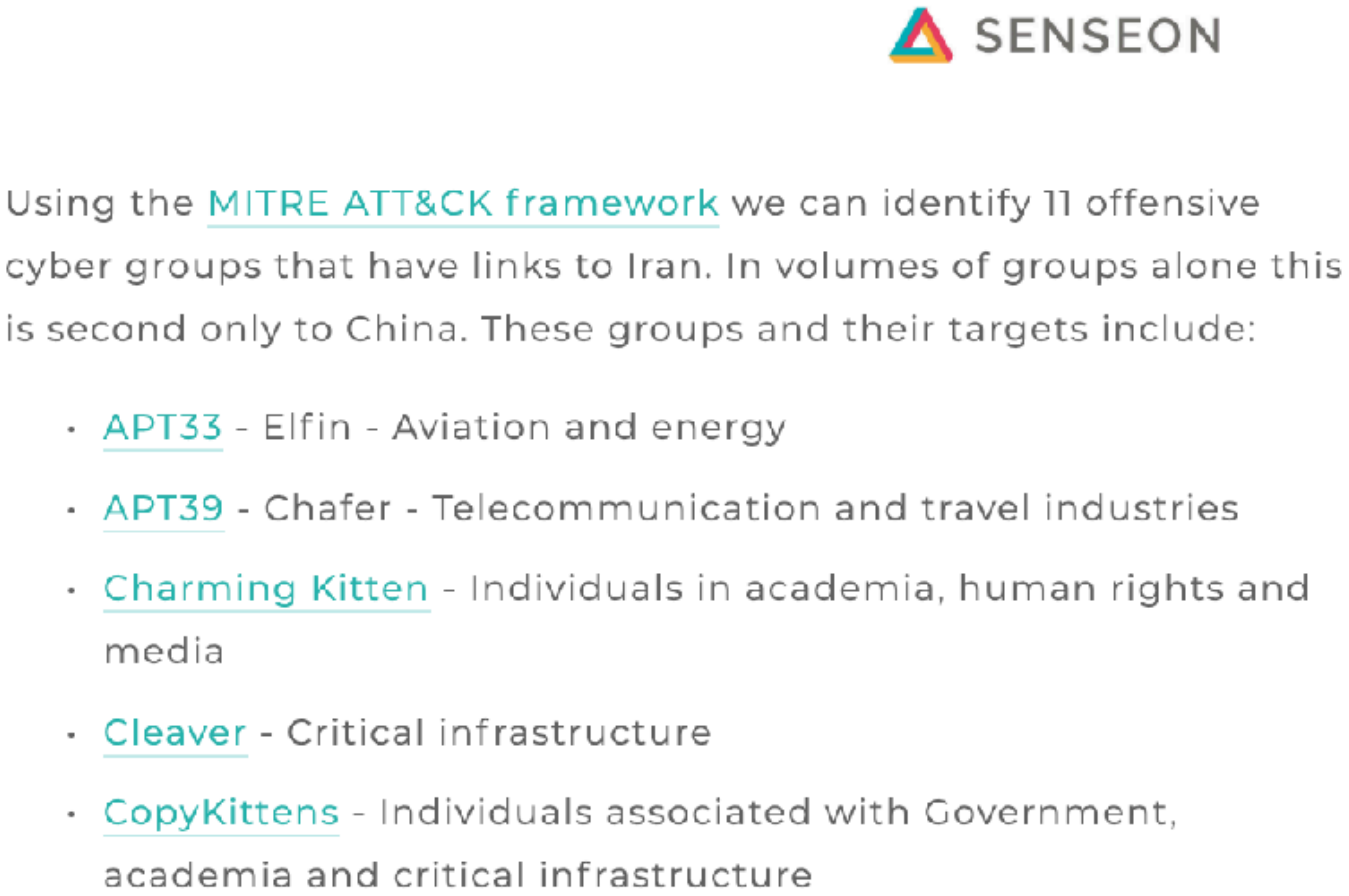
وَ عُمَرَ بْنَ سَعْدٍ وَ شِمْراً وَ آلَ أَبِي سُفْيَانَ وَ آلَ زِيَادٍ وَ آلَ مَرْوَانَ إِلَى يَوْمِ الْقِيَامَةِ

This is message from Islamic Republic Of Iran

We will not stop supporting our friends in the region: the oppressed people of Palestine, the oppressed people of Yemen, the people and the Syrian government, the people and government of Iraq, the oppressed people of .Bahrain, the true mujahideen resistance in Lebanon and Palestine; [they] always will be supported by us

A website operated by the U.S. government hacked by a group claiming to represent the government of Iran

Iran’s cyber capabilities

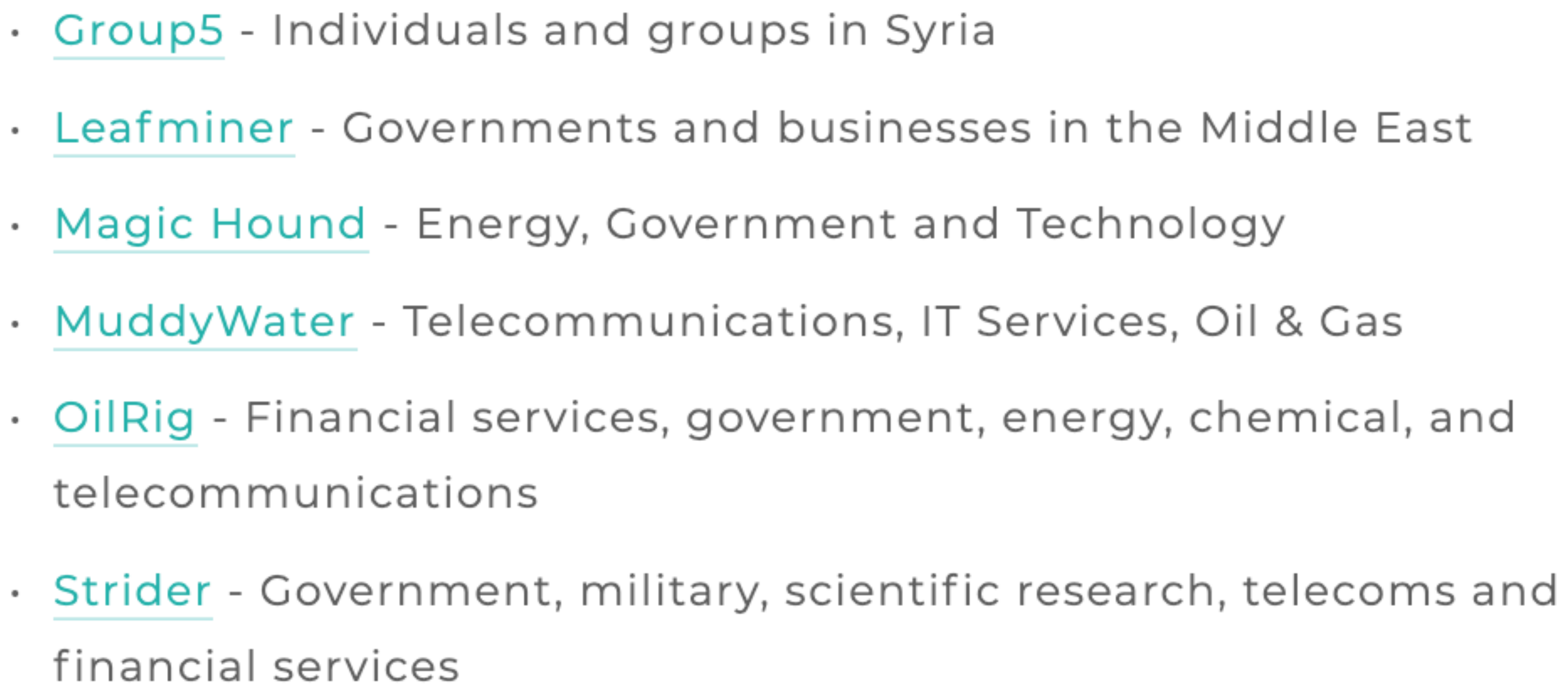


SENSEON

Using the MITRE ATT&CK framework we can identify 11 offensive cyber groups that have links to Iran. In volumes of groups alone this is second only to China. These groups and their targets include:

- APT33 - Elfin - Aviation and energy
- APT39 - Chafer - Telecommunication and travel industries
- Charming Kitten - Individuals in academia, human rights and media
- Cleaver - Critical infrastructure
- CopyKittens - Individuals associated with Government, academia and critical infrastructure

Iran's Attack Groups



- Group5 - Individuals and groups in Syria
- Leafminer - Governments and businesses in the Middle East
- Magic Hound - Energy, Government and Technology
- MuddyWater - Telecommunications, IT Services, Oil & Gas
- OilRig - Financial services, government, energy, chemical, and telecommunications
- Strider - Government, military, scientific research, telecoms and financial services

Iran and Russia obtained U.S. voter registration data in effort to influence election, national security officials say

PUBLISHED WED, OCT 21 2020•7:20 PM EDT | UPDATED THU, OCT 22 2020•7:53 AM EDT

VIDEO 04:31

FBI press conference on foreign interference in U.S. election

FEDERAL BUREAU OF INVESTIGATION
FIDELITY
BRAVERY
BREAKING NEWS
JOHN RATCLIFFE
DIRECTOR OF NATIONAL INTELLIGENCE
CNBC

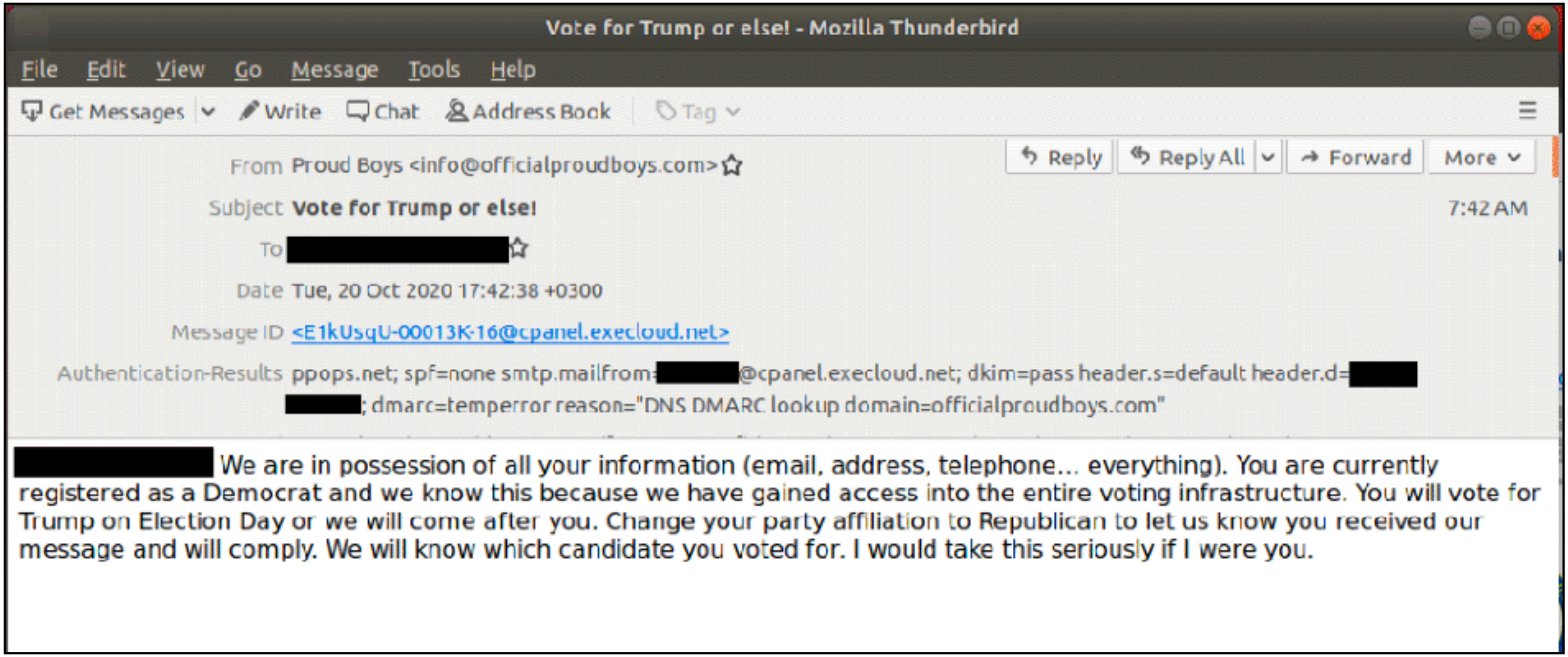
Offensive Actions

- Iran and Russia obtained information about American voter registrations

- Trying to influence the public about the upcoming U.S. presidential election

- Iran has been sending “spoofed emails designed to intimidate voters, incite social unrest and damage President” Donald Trump

- Iran is distributing other content to include a video that implies that individuals could cast fraudulent ballots even from overseas,



From Proud Boys <info@officialproudboys.com>

Subject **Vote for Trump or else!**

7:42 AM

To [redacted]

Date Tue, 20 Oct 2020 17:42:38 +0300

Message ID <E1kUsqU-00013K-16@cpanel.execloud.net>

Authentication-Results ppops.net; spf=none smtp.mailfrom=[redacted]@cpanel.execloud.net; dkim=pass header.s=default header.d=[redacted]; dmarc=temperror reason="DNS DMARC lookup domain=officialproudboys.com"

[redacted] We are in possession of all your information (email, address, telephone... everything). You are currently registered as a Democrat and we know this because we have gained access into the entire voting infrastructure. You will vote for Trump on Election Day or we will come after you. Change your party affiliation to Republican to let us know you received our message and will comply. We will know which candidate you voted for. I would take this seriously if I were you.

Mandiant

- John Hultquist, Senior Director of Analysis, Mandiant Threat Intelligence:
  - "Iranian information operations date back at least eight years and they have grown beyond **fake news sites** and social network activity to elaborate tactics, such as **impersonating journalists** to solicit video interviews and placing op-eds. They have even **impersonated American politicians**"
  - "The information operations we have seen from Iran to date have been about **amplifying pro-Iranian messages** and pushing a desired narrative out into the world that's anti-Saudi or ant-Israeli or pro-JCPOA"
  - "This is different. This is **deliberate interference in our democracy** and it crosses a major red line. I think the Intel community scored a win here against Iran today"

Attempts to Blur

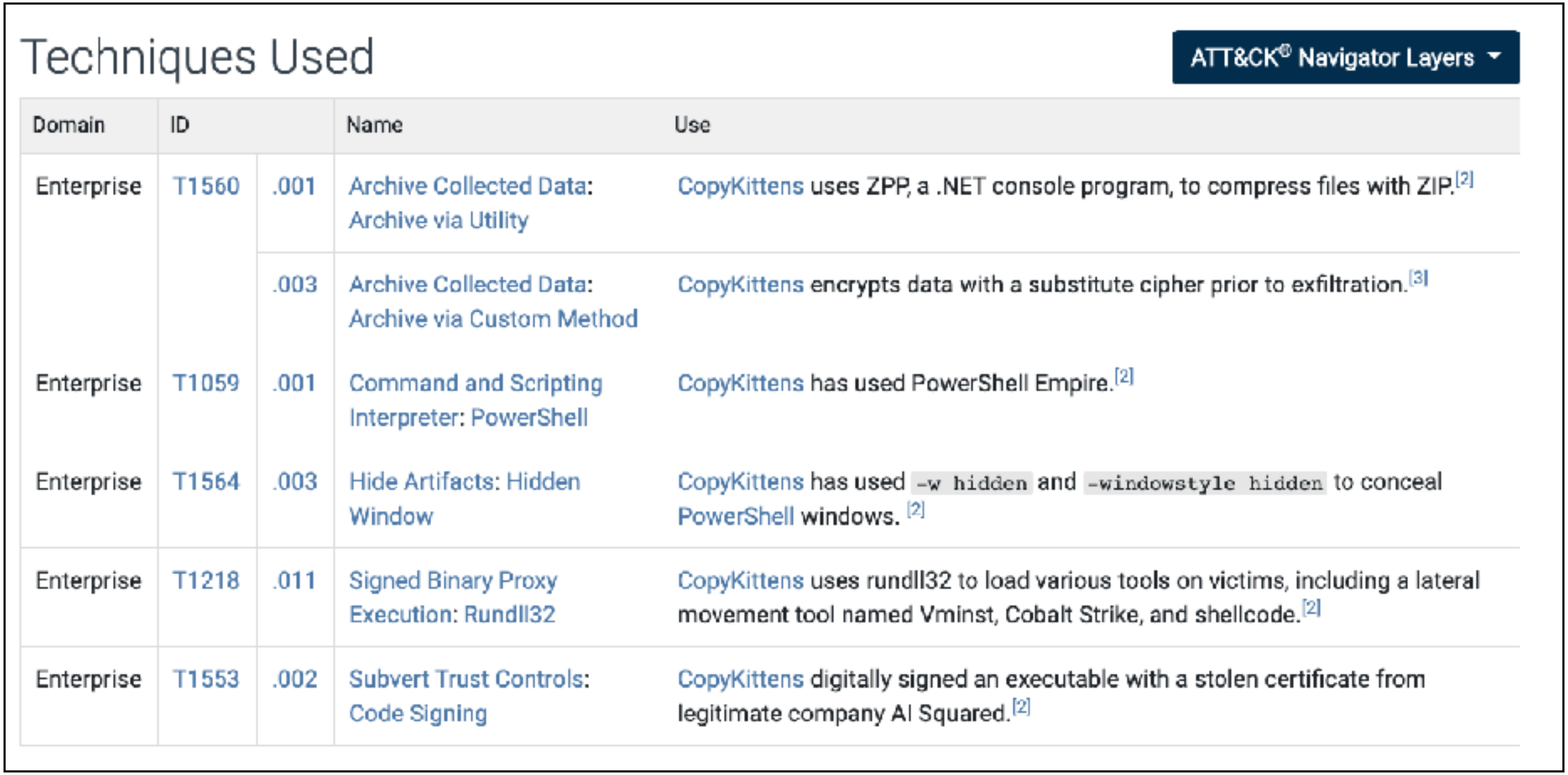
- Despite attempts to blur aspects of the video to hide their identity, the hackers were unable to obfuscate all of the incriminating information, the sources said.

- The video showed the hackers' computer screen as they typed in commands and pretended to hack a voter registration system. Investigators noticed snippets of revealing computer code, including file paths, file names and an internet protocol (IP) address.

- Security analysts found that the IP address, hosted through an online service called Worldstream, traced back to previous Iranian hacking activity, the sources said.

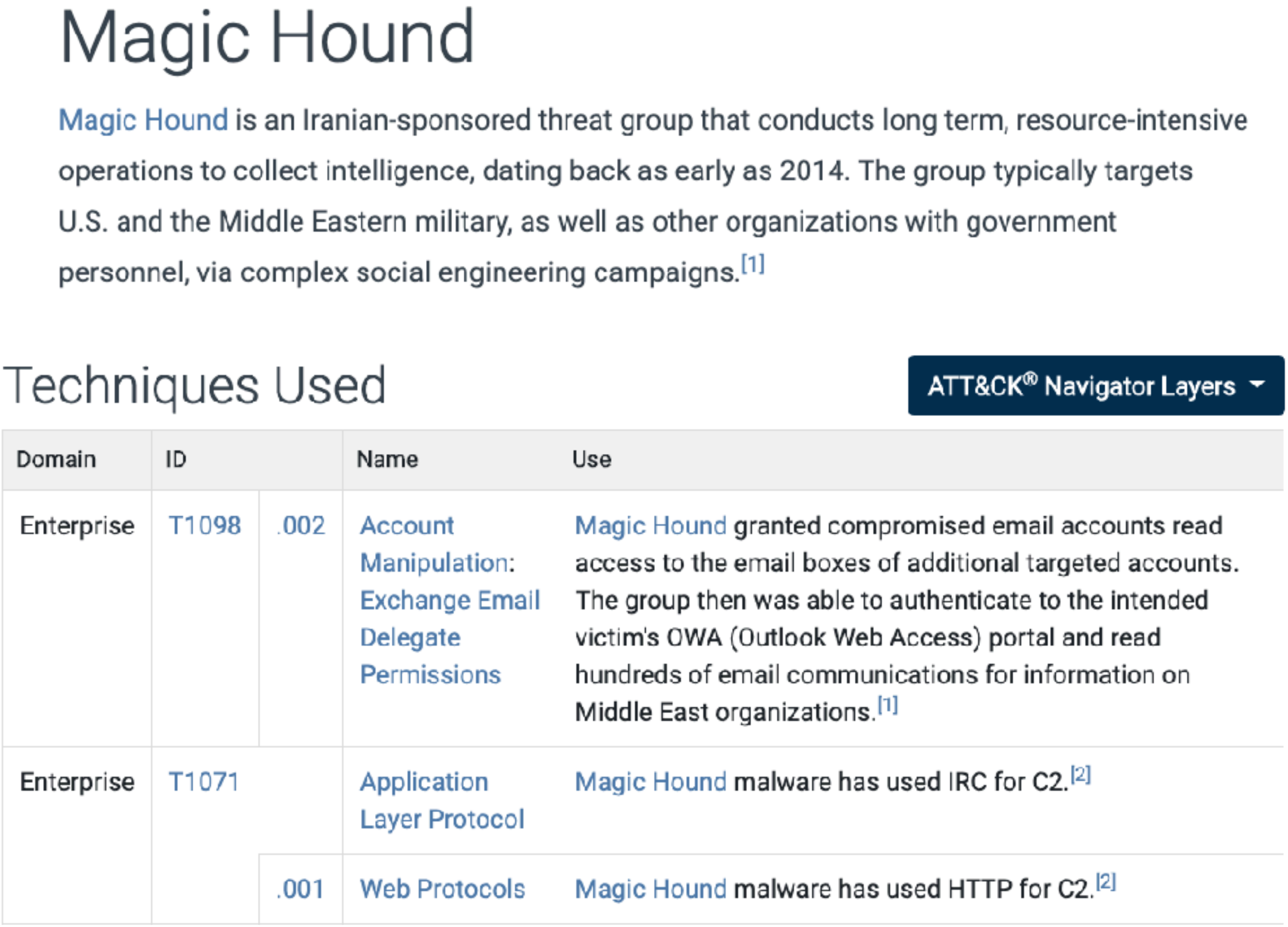
CopyKittens

CopyKittens is an Iranian cyber espionage group that has been operating since at least 2013. It has targeted countries including Israel, Saudi Arabia, Turkey, the U.S., Jordan, and Germany. The group is responsible for the campaign known as Operation Wilted Tulip. [1] [2] [3]



Techniques Used

Domain	ID		Name	Use
Enterprise	T1560	.001	Archive Collected Data: Archive via Utility	CopyKittens uses ZPP, a .NET console program, to compress files with ZIP.[2]
		.003	Archive Collected Data: Archive via Custom Method	CopyKittens encrypts data with a substitute cipher prior to exfiltration.[3]
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	CopyKittens has used PowerShell Empire.[2]
Enterprise	T1564	.003	Hide Artifacts: Hidden Window	CopyKittens has used `-w hidden` and `-windowstyle hidden` to conceal PowerShell windows. [2]
Enterprise	T1218	.011	Signed Binary Proxy Execution: Rundll32	CopyKittens uses rundll32 to load various tools on victims, including a lateral movement tool named Vminst, Cobalt Strike, and shellcode.[2]
Enterprise	T1553	.002	Subvert Trust Controls: Code Signing	CopyKittens digitally signed an executable with a stolen certificate from legitimate company AI Squared.[2]

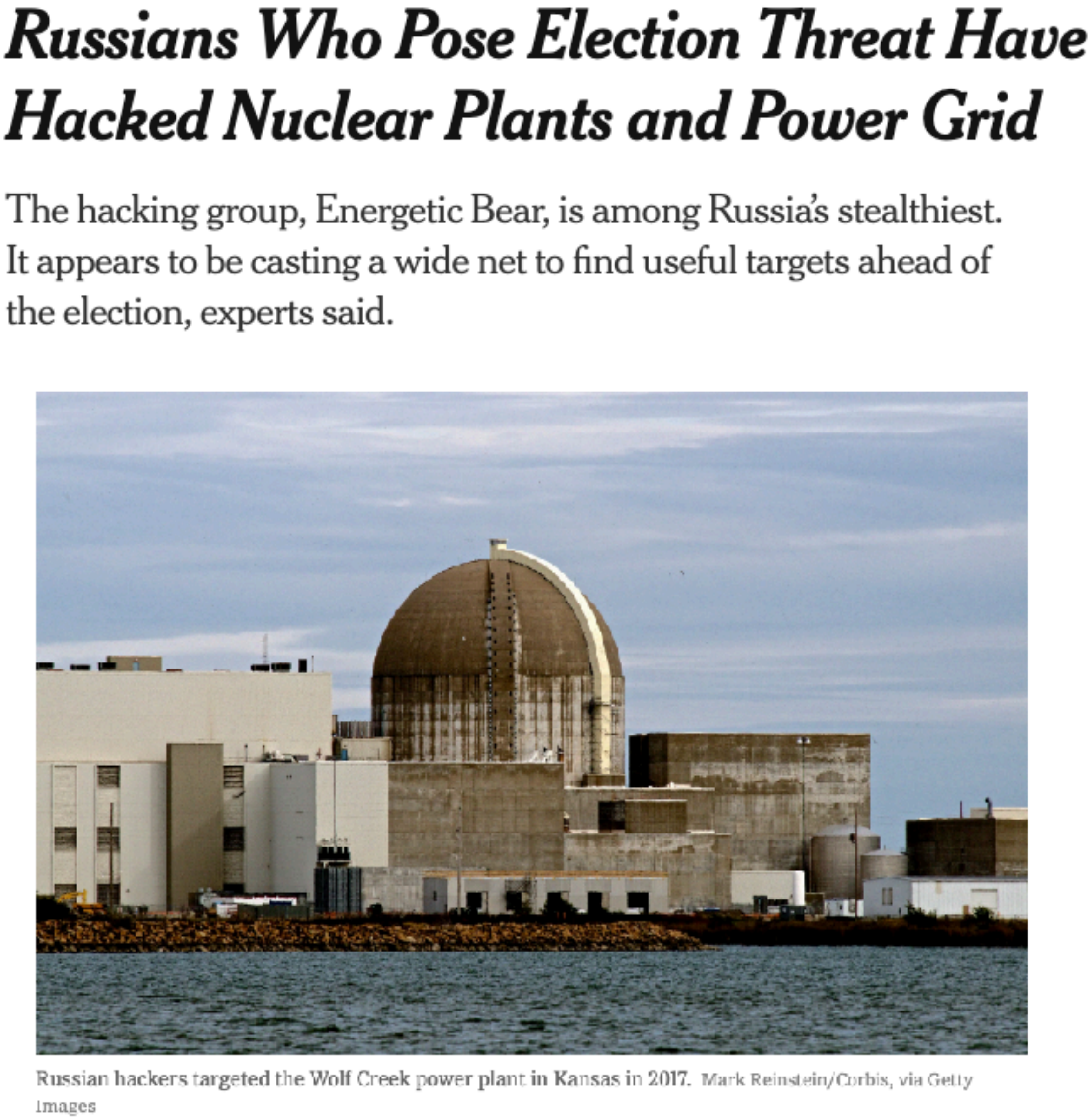


Magic Hound

Magic Hound is an Iranian-sponsored threat group that conducts long term, resource-intensive operations to collect intelligence, dating back as early as 2014. The group typically targets U.S. and the Middle Eastern military, as well as other organizations with government personnel, via complex social engineering campaigns.[1]

Techniques Used

Domain	ID		Name	Use
Enterprise	T1098	.002	Account Manipulation: Exchange Email Delegate Permissions	Magic Hound granted compromised email accounts read access to the email boxes of additional targeted accounts. The group then was able to authenticate to the intended victim's OWA (Outlook Web Access) portal and read hundreds of email communications for information on Middle East organizations.[1]
Enterprise	T1071		Application Layer Protocol	Magic Hound malware has used IRC for C2.[2]
		.001	Web Protocols	Magic Hound malware has used HTTP for C2.[2]



Russians Who Pose Election Threat Have Hacked Nuclear Plants and Power Grid

The hacking group, Energetic Bear, is among Russia's stealthiest. It appears to be casting a wide net to find useful targets ahead of the election, experts said.

Russian hackers targeted the Wolf Creek power plant in Kansas in 2017. Mark Reinstein/Corbis, via Getty Images

- But it has in the past five years breached the power grid, water treatment facilities and even nuclear power plants, including one in Kansas.

- It also hacked into Wi-Fi systems at San Francisco International Airport and at least two other West Coast airports in March in an apparent bid to find one unidentified traveler

- The group has thus far stopped short of sabotage, but appears to be preparing for some future attack. The hackings so unnerved officials that starting in 2018, the United States Cyber Command, the arm of the Pentagon that conducts offensive cyberattacks, hit back with retaliatory strikes on the Russian grid.

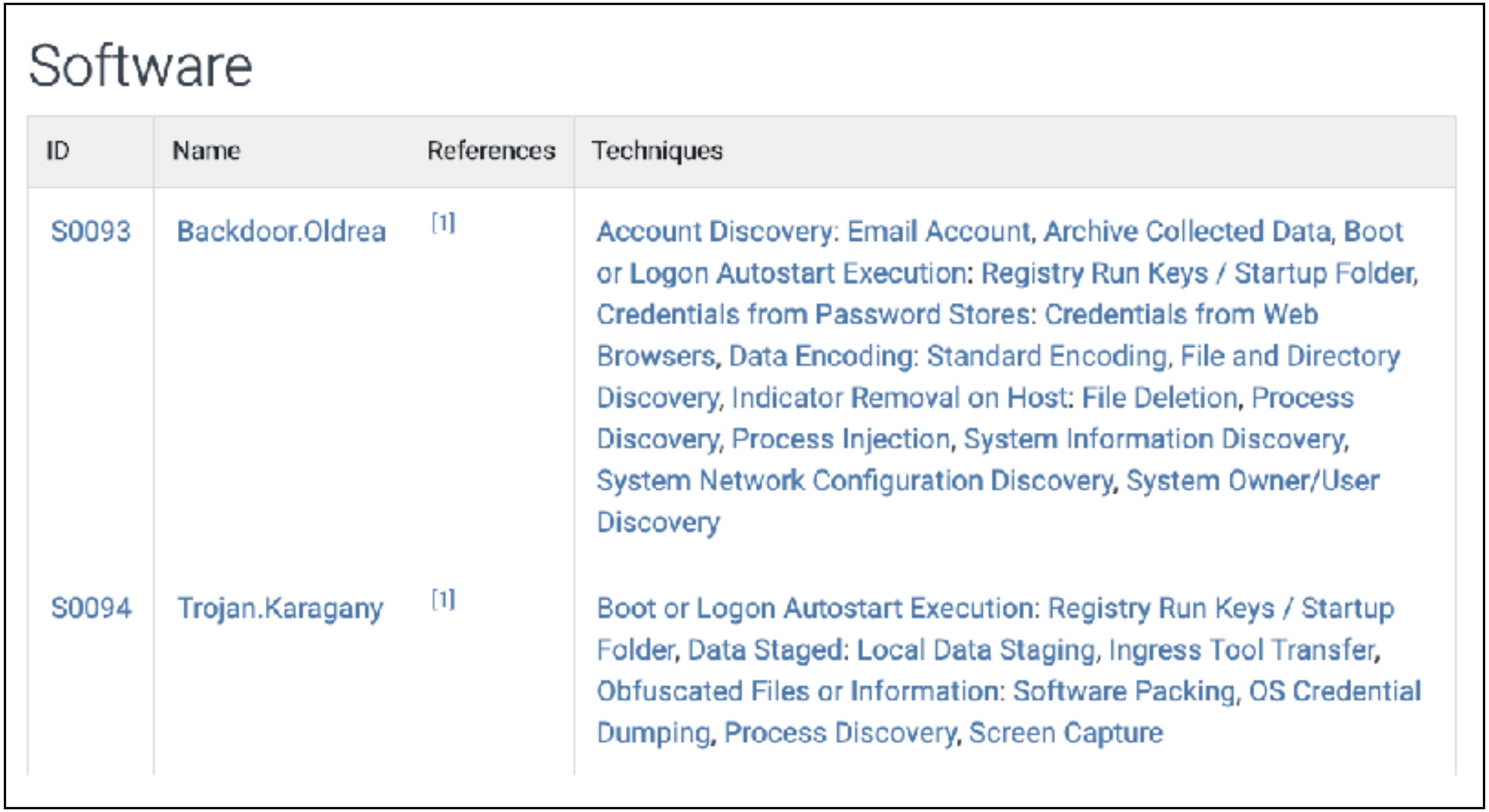
- Officials at San Francisco International Airport discovered Russia’s state hackers had breached the online system that airport employees and travelers used to gain access to the airport’s Wi-Fi. The hackers injected code into two Wi-Fi portals that stole visitors’ user names, cracked their passwords and infected their laptops.

- The attack began on March 17 and continued for nearly two weeks until it was shut down. By then, officials at two other airports discovered their Wi-Fi portals had also been compromised. Researchers would not name the other victims, citing nondisclosure agreements, but said they were on the West Coast.

-

Dragonfly

Dragonfly is a cyber espionage group that has been active since at least 2011. They initially targeted defense and aviation companies but shifted to focus on the energy sector in early 2013. They have also targeted companies related to industrial control systems. [1]



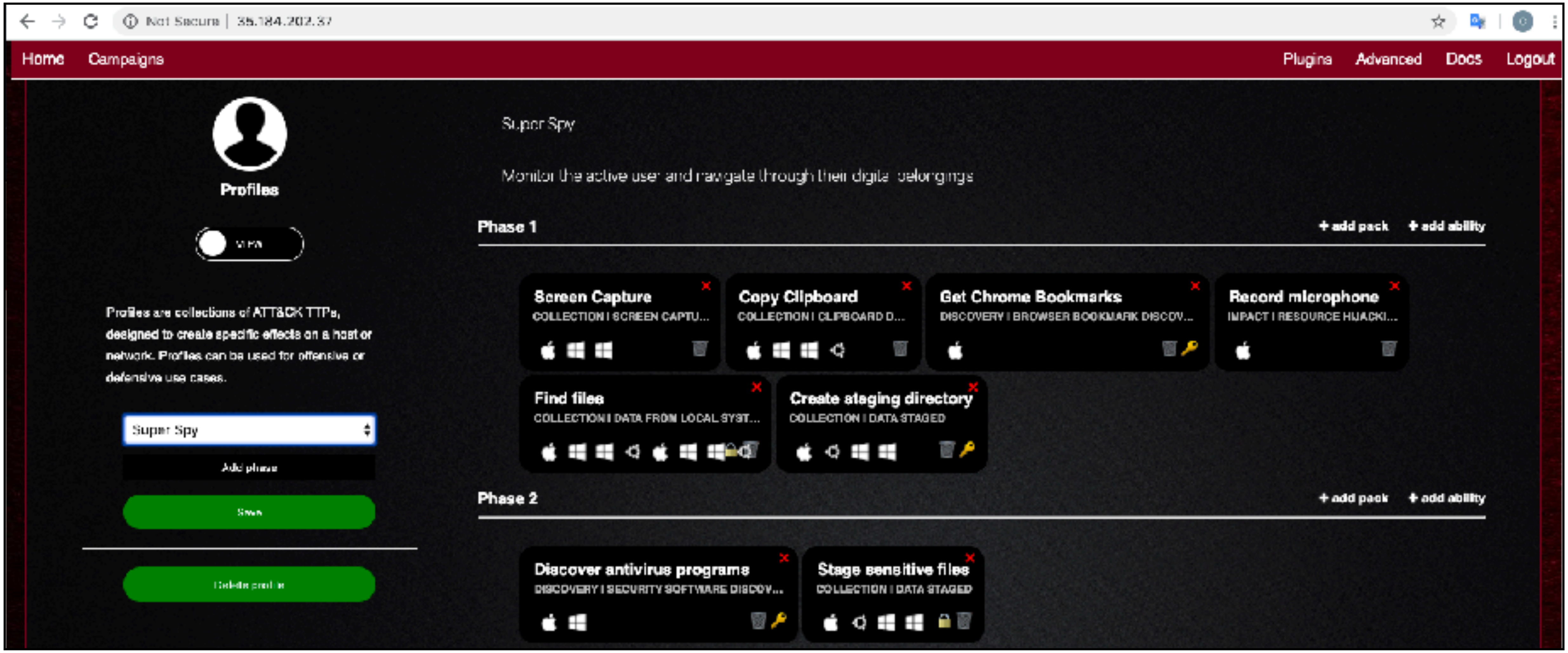
Software

ID	Name	References	Techniques
S0093	Backdoor.Oldrea	[1]	Account Discovery: Email Account, Archive Collected Data, Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Credentials from Password Stores: Credentials from Web Browsers, Data Encoding: Standard Encoding, File and Directory Discovery, Indicator Removal on Host: File Deletion, Process Discovery, Process Injection, System Information Discovery, System Network Configuration Discovery, System Owner/User Discovery
S0094	Trojan.Karagany	[1]	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Data Staged: Local Data Staging, Ingress Tool Transfer, Obfuscated Files or Information: Software Packing, OS Credential Dumping, Process Discovery, Screen Capture

ATT&CK Navigator

- Compares Groups
- https://mitre-attack.github.io/attack-navigator/enterprise/

Caldera
Adversary Emulator



Profiles are collections of ATT&CK TTPs, designed to create specific effects on a host or network. Profiles can be used for offensive or defensive use cases.

Super Spy

Super Spy

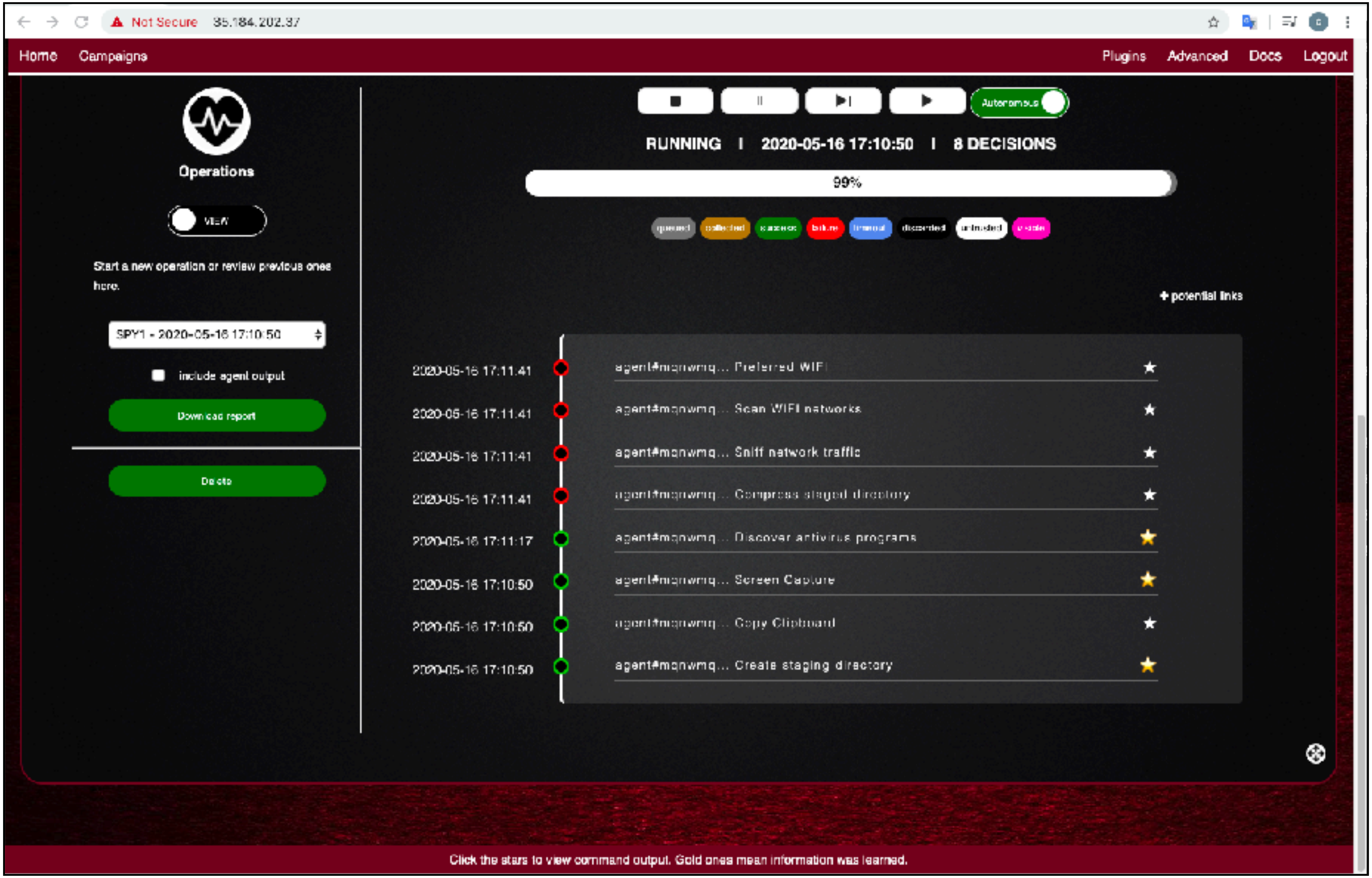
Monitor the active user and navigate through their digital belongings

Phase 1

- Screen Capture — COLLECTION | SCREEN CAPTU...
- Copy Clipboard — COLLECTION | CLIPBOARD D...
- Get Chrome Bookmarks — DISCOVERY | BROWSER BOOKMARK DISCOV...
- Record microphone — IMPACT | RESOURCE HIJACKI...
- Find files — COLLECTION | DATA FROM LOCAL SYST...
- Create staging directory — COLLECTION | DATA STAGED

Phase 2

- Discover antivirus programs — DISCOVERY | SECURITY SOFTWARE DISCOV...
- Stage sensitive files — COLLECTION | DATA STAGED



Start a new operation or review previous ones here.

SPY1 - 2020-05-16 17:10:50

□ include agent output

RUNNING | 2020-05-16 17:10:50 | 8 DECISIONS

2020-05-16 17:11:41 agent#mqnwmq... Preferred WIFI ★

2020-05-16 17:11:41 agent#mqnwmq... Scan WIFI networks ★

2020-05-16 17:11:41 agent#mqnwmq... Sniff network traffic ★

2020-05-16 17:11:41 agent#mqnwmq... Compress staged directory ★

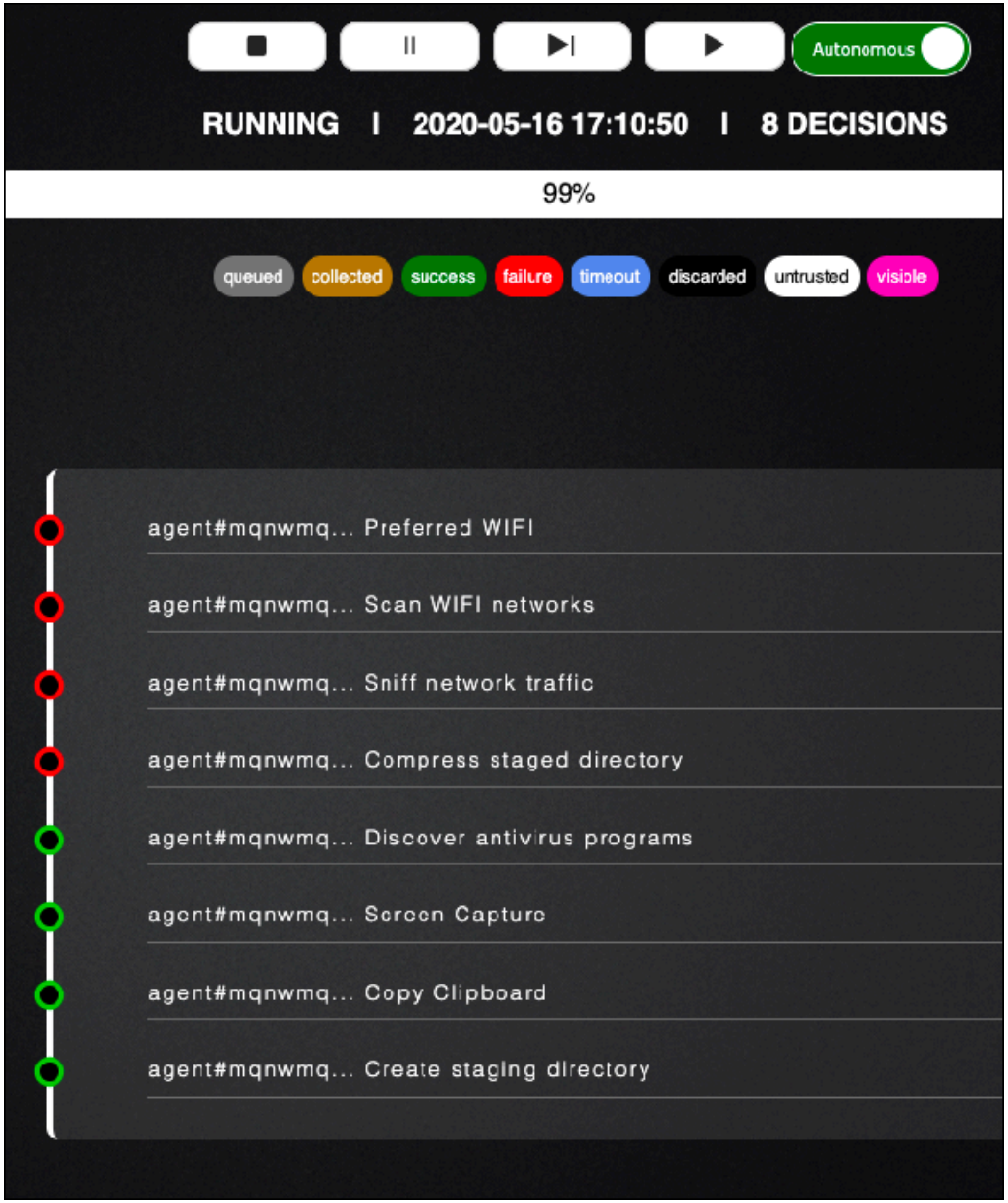
2020-05-16 17:11:17 agent#mqnwmq... Discover antivirus programs ★

2020-05-16 17:10:50 agent#mqnwmq... Screen Capture ★

2020-05-16 17:10:50 agent#mqnwmq... Copy Clipboard ★

2020-05-16 17:10:50 agent#mqnwmq... Create staging directory ★

Click the stars to view command output. Gold ones mean information was learned.



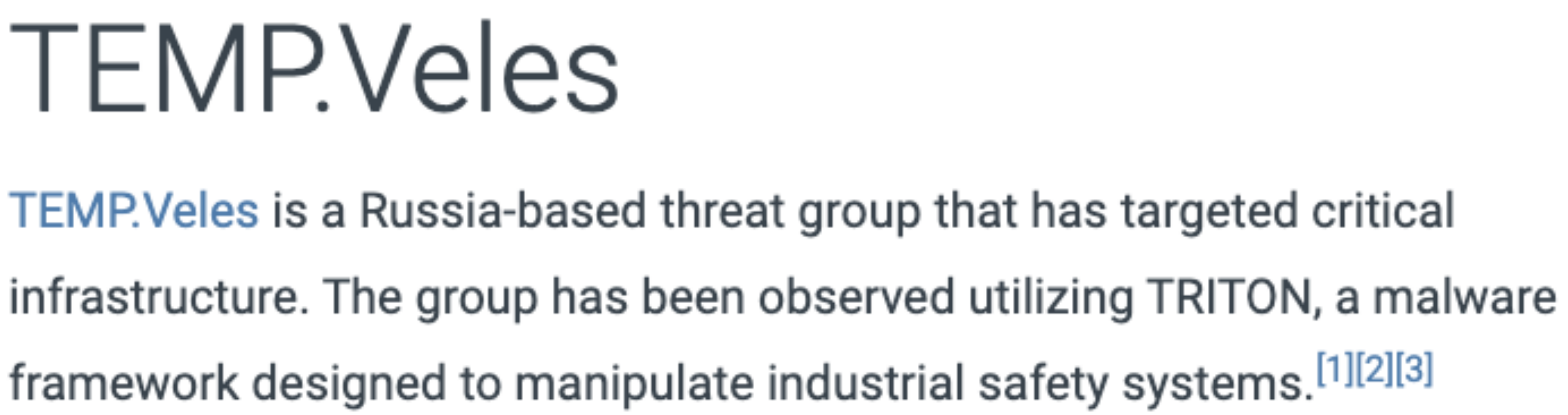
RUNNING I 2020-05-16 17:10:50 I 8 DECISIONS

99%

```
agent#mqnwmq... Preferred WIFI
agent#mqnwmq... Scan WIFI networks
agent#mqnwmq... Sniff network traffic
agent#mqnwmq... Compress staged directory
agent#mqnwmq... Discover antivirus programs
agent#mqnwmq... Screen Capture
agent#mqnwmq... Copy Clipboard
agent#mqnwmq... Create staging directory
```

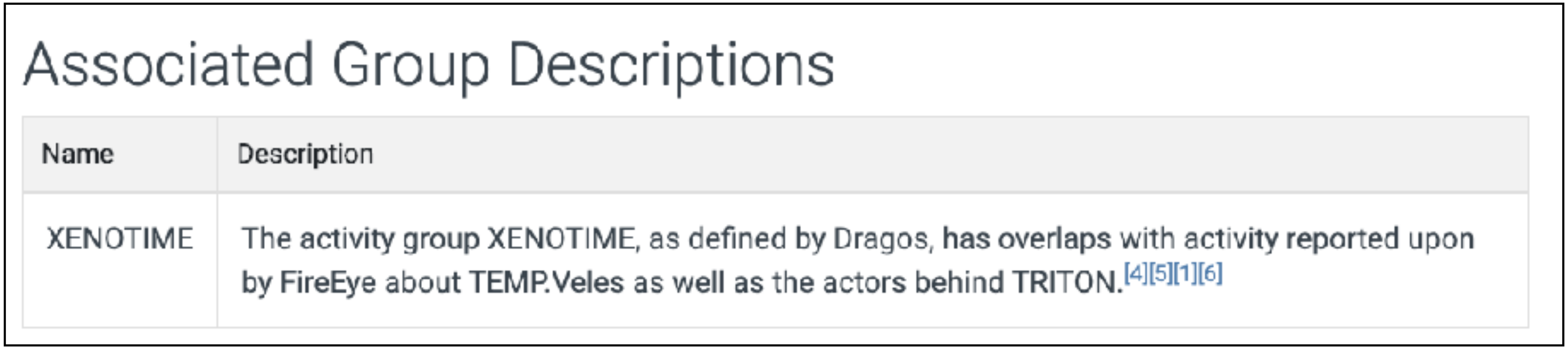
Hack of Saudi Petrochemical Plant Was Coordinated From Russian Institute

The cyberattack on a Saudi petrochemical plant was the first known attempt to manipulate an emergency-shutdown system, which is designed to avoid disaster and protect human lives. Christophe Viseux for The New York Times



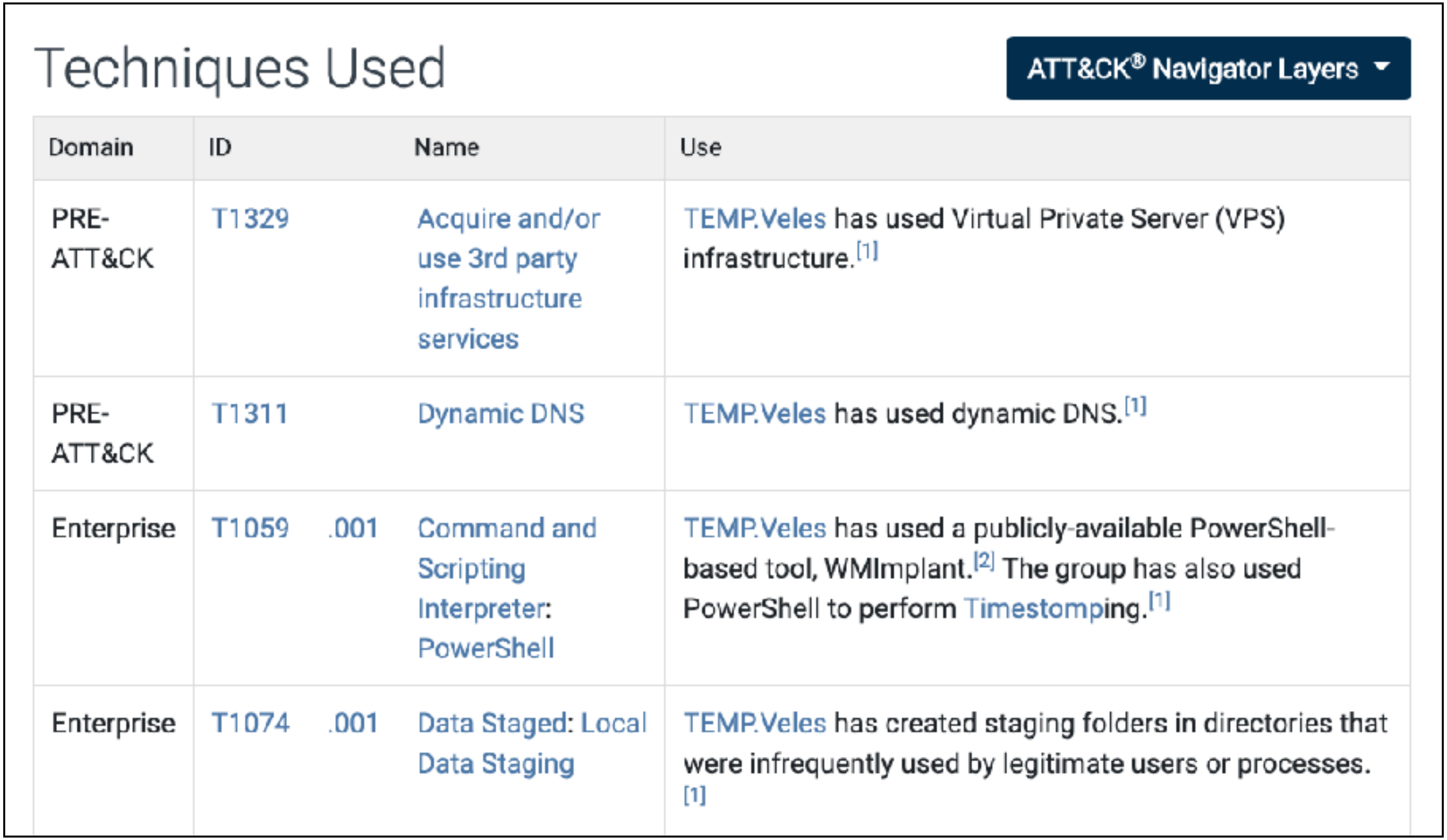
TEMP.Veles

TEMP.Veles is a Russia-based threat group that has targeted critical infrastructure. The group has been observed utilizing TRITON, a malware framework designed to manipulate industrial safety systems.[1][2][3]



Associated Group Descriptions

Name	Description
XENOTIME	The activity group XENOTIME, as defined by Dragos, has overlaps with activity reported upon by FireEye about TEMP.Veles as well as the actors behind TRITON.[4][5][1][6]



Techniques Used

Domain	ID		Name	Use
PRE-ATT&CK	T1329		Acquire and/or use 3rd party infrastructure services	TEMP.Veles has used Virtual Private Server (VPS) infrastructure.[1]
PRE-ATT&CK	T1311		Dynamic DNS	TEMP.Veles has used dynamic DNS.[1]
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	TEMP.Veles has used a publicly-available PowerShell-based tool, WMImplant.[2] The group has also used PowerShell to perform Timestomping.[1]
Enterprise	T1074	.001	Data Staged: Local Data Staging	TEMP.Veles has created staging folders in directories that were infrequently used by legitimate users or processes.[1]

References

- https://attack.mitre.org/matrices/enterprise/
- https://www.senseon.io/blog/mapping-iranian-cyber-attacks-to-the-mitre-attack-framework
- https://www.cnbc.com/2020/10/21/fbi-to-make-an-announcement-on-a-major-election-security-issue.html
- https://www.zdnet.com/article/us-blames-iran-for-spoofed-proud-boys-emails-threatening-democrat-voters/
- https://www.reuters.com/article/us-usa-election-cyber-iran-exclusive/exclusive-dumb-mistake-exposed-iranian-hand-behind-fake-proud-boys-u-s-election-emails-sources-idUSKBN2772YL
- https://www.nytimes.com/2020/10/23/us/politics/energetic-bear-russian-hackers.html
- https://www.nytimes.com/2018/10/23/us/politics/russian-hackers-saudi-chemical-plant.html
- https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html
-