EuskalHack Security Congress IX

Insiders ?


ANOMALY DETECTION
Detecting unusual network patterns. Machine learning analysis.
FORENSIC ANALYSIS
Post-incident review. Tracing attacker footprints.
SYSTEM INTEGRITY COMPROMISE
Rootkit insertion. System file modifications.
IS IT AN INSIDE JOB?
LACK OF VISIBILITY?
Missing pieces? Hidden pathways?
TOO MUCH COMPLEXITY?
Tangled systems? Overwhelming dependencies?
IDENTITY ISSUES?
Impersonation? Unauthorized access?
OR
IS IT...
AN APT?
Targeted, persistent, state-sponsored. Advanced techniques & exfiltration.
A SCRIPT KIDDIE?
Automated tools, low skill. Simple exploits, mass scanning.
AN OPPORTUNISTIC ATTACK?
vulnerability found
Exploiting a specific vulnerability. Broad sweep, fast impact.

Who am I?

Ruben Castillo

Unit 42 Director for Southern Europe - Palo Alto Networks

20 years of experience in Cyber Security.

- MSIT - CMU
- BS - Electronic Engineering
- Security Certs

Running
Exploring new cities on foot

Cycling
Mountain Biking enthusiast

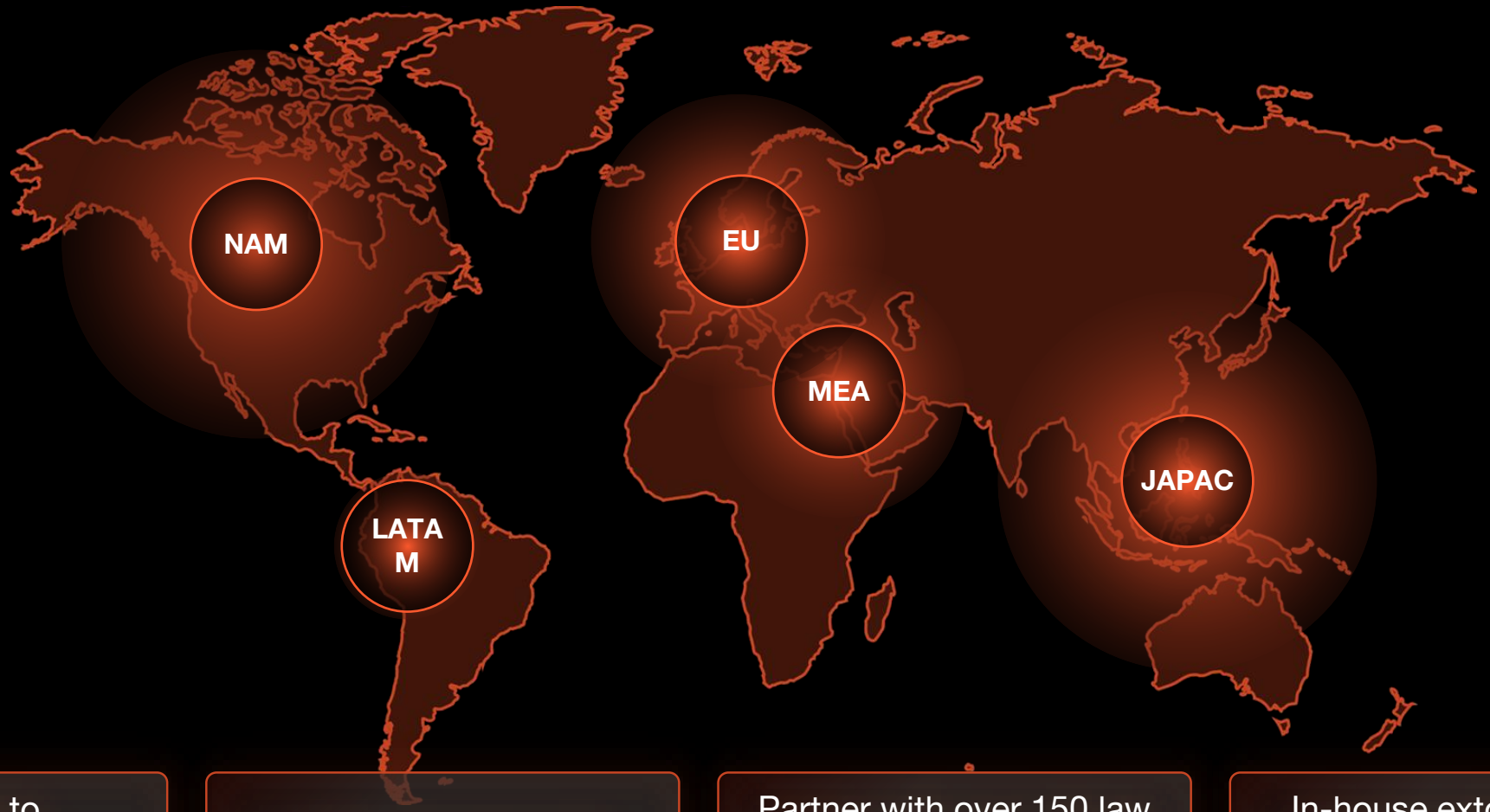
Family
3 Kids + 2 Dogs

Location
Defending our Digital World from Asturias

Cybersecurity
Passion for defense

A Global Team of 500+ Cybersecurity Experts

Expertise in threat intel, incident response, proactive services and managed detection & response



Responded to some of the largest breaches in history

1,000+ Engagements per year

Partner with over 150 law firms and 70 insurance carriers

In-house extortion and ransomware negotiations team

paloalto NETWORKS | UNIT 42

paloalto NETWORKS | UNIT 42

Global Incident Response Report 2026

Release date: 2026-02

Four major trends that will shape the threat landscape for 2026

1

AI has become a force multiplier for threat actors

2

Identity has become the most reliable path to attacker success

3

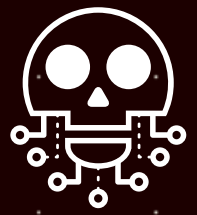
Software supply chain risk has expanded beyond vulnerable code to the misuse of trusted connectivity

4

Nation-state actors are adapting stealth and persistence tactics to modern enterprise operating environments

TREND 1

AI is Now Operational



AI is no longer a concept; it is an

attack accelerator

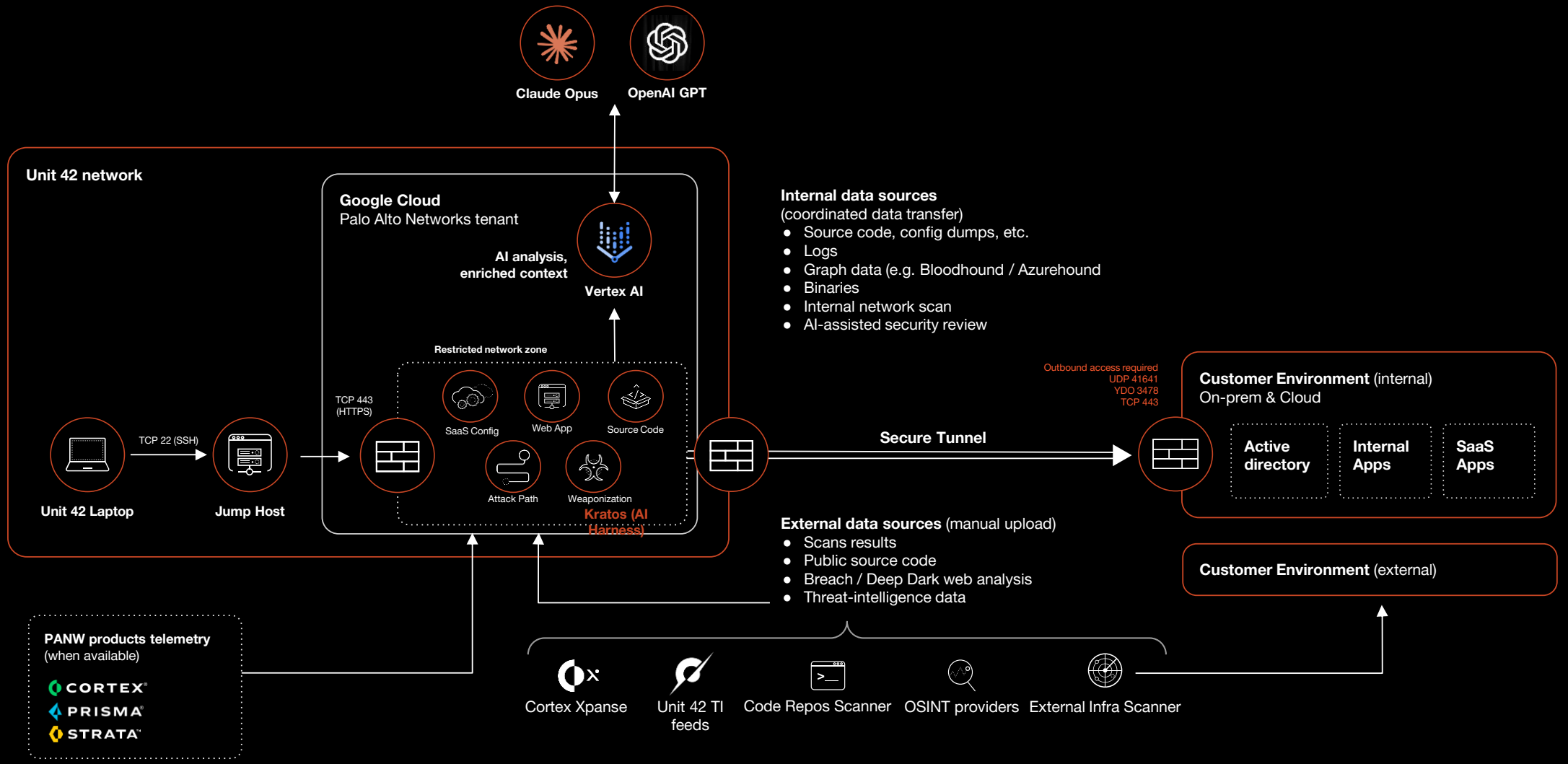
Why this matters

- Automation increased attack speed and consistency
- Skill barriers are reduced for complex operations
- AI improved execution efficacy changing intent

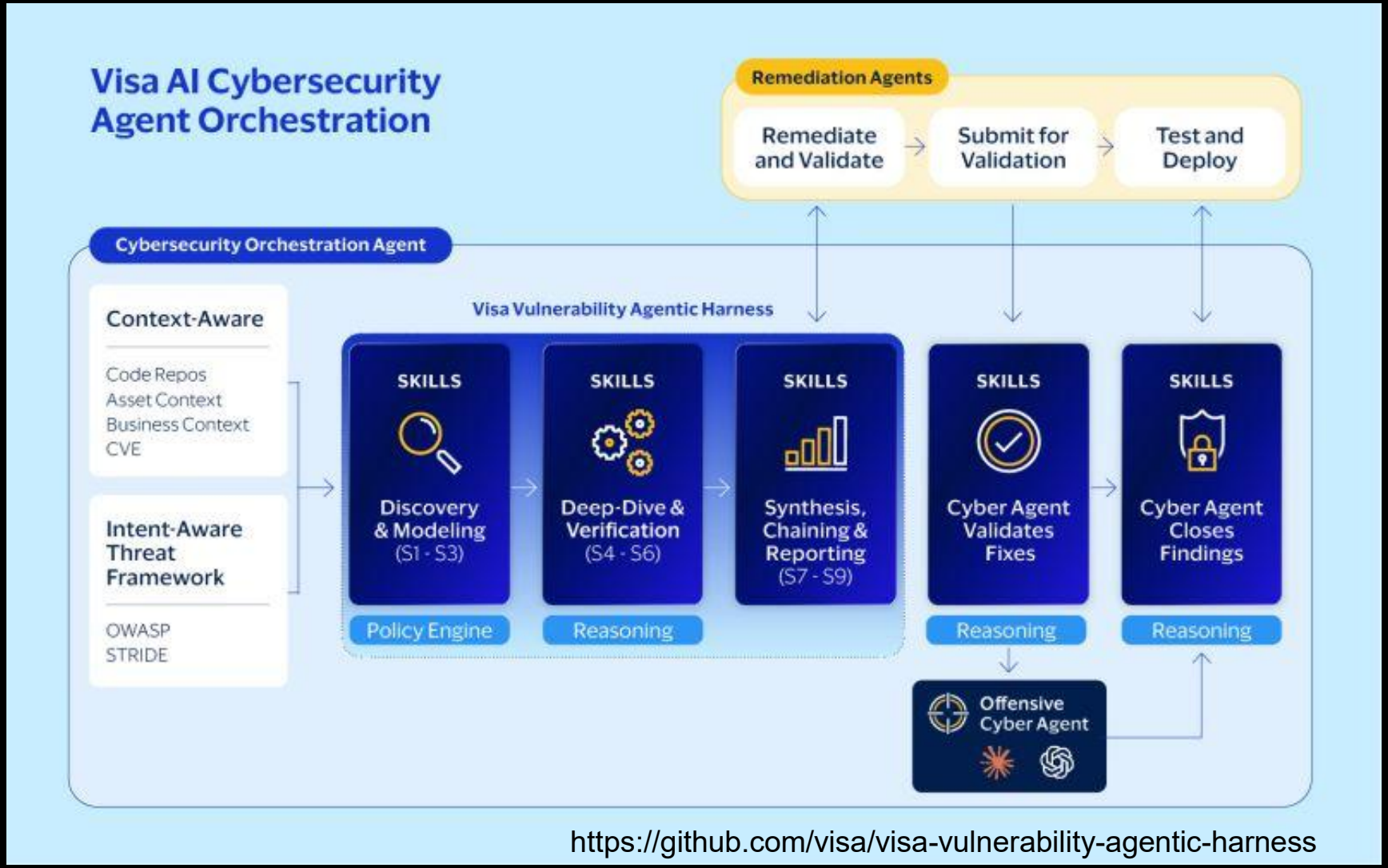
Recommendation

Apply automation defensively to match attacker speed and efficiency.

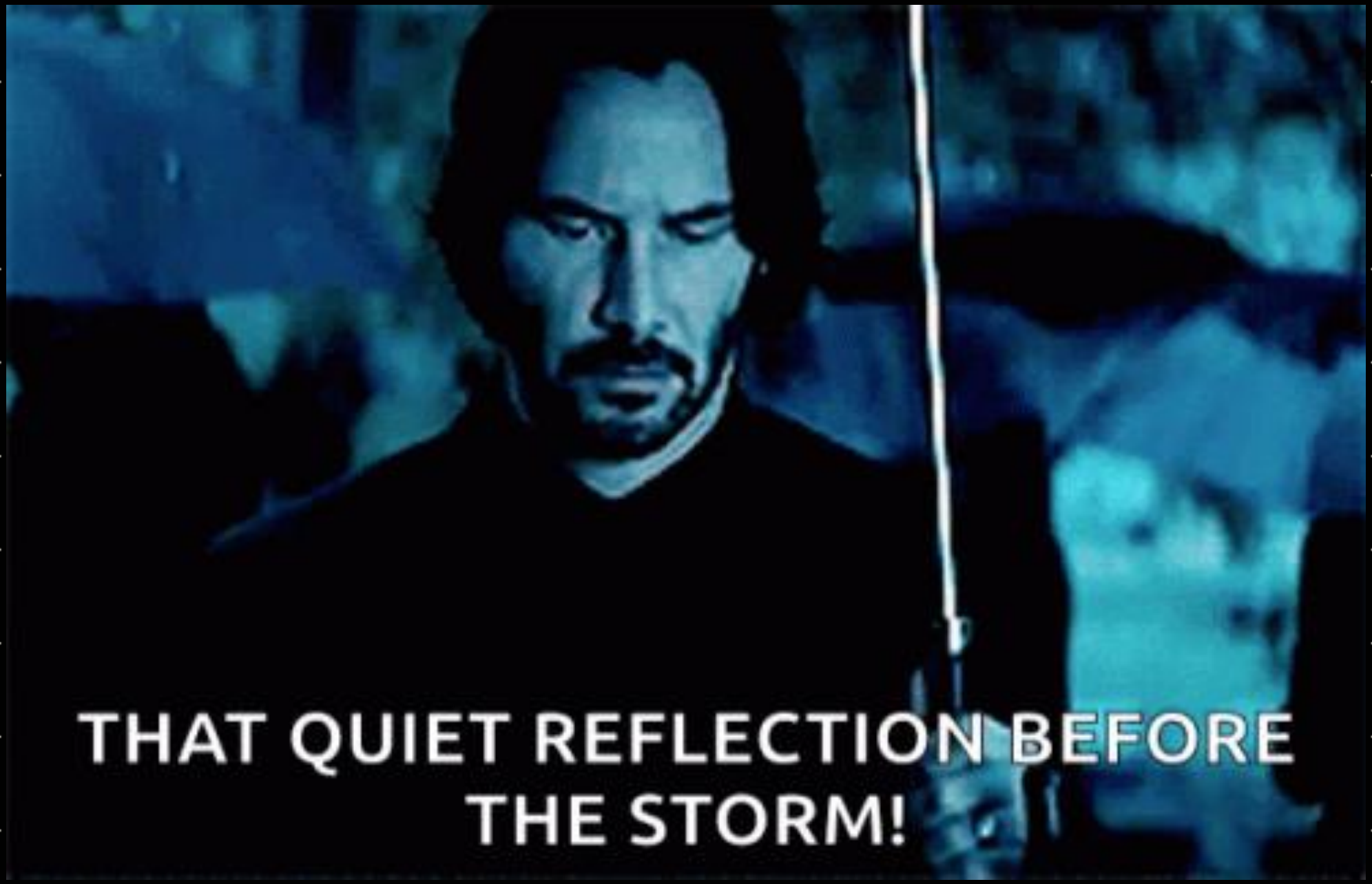
Unit 42 AI Harness High-Level Network Diagram



Models and tools are maturing and published in open source



https://github.com/visa/visa-vulnerability-agentic-harness



Risks with Secrets

Reference: https://trufflesecurity.com/blog/google-api-keys-werent-secrets-but-then-gemini-changed-the-rules

Policy trufflesecurity.com/blog/google-api-...

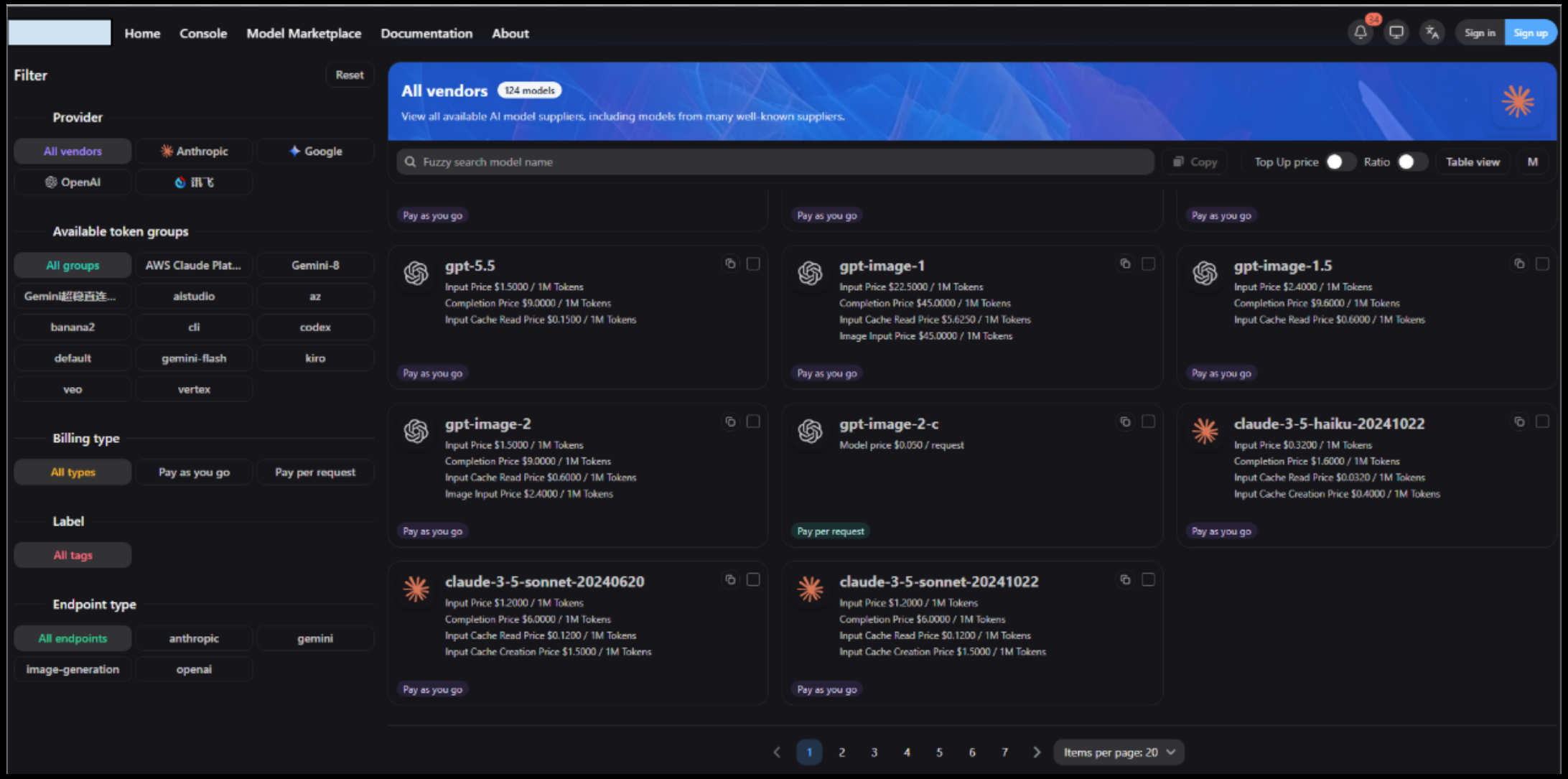
THE DIG

Google API Keys Weren't Secrets. But then Gemini Changed the Rules.

JOE LEON
FEBRUARY 25, 2026

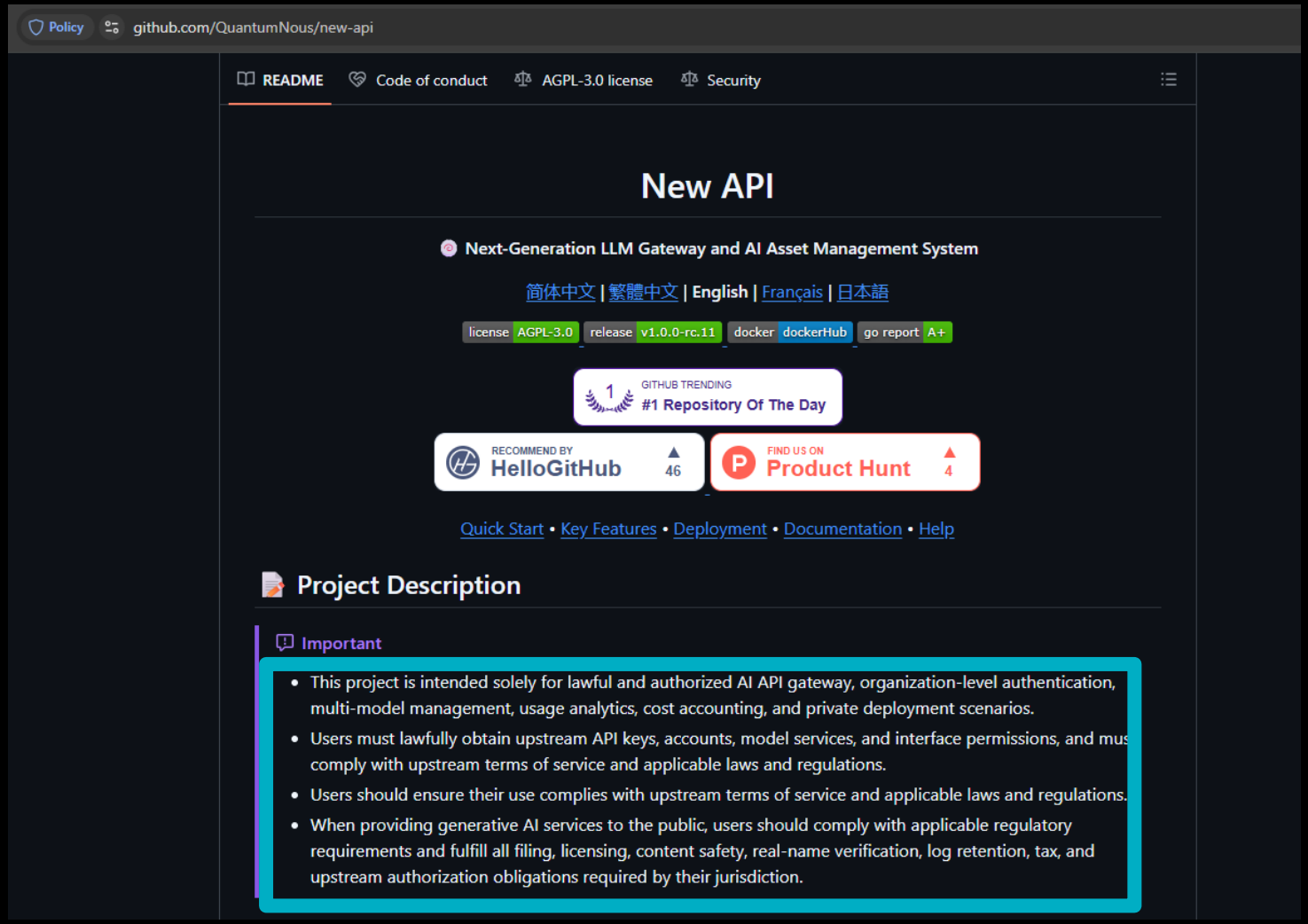
tl;dr Google spent over a decade telling developers that Google API keys (like those used in Maps, Firebase, etc.) are not secrets. But that's no longer true: Gemini accepts the same keys to access your private data. We scanned millions of websites and found nearly 3,000 Google API keys, originally deployed for public services like Google Maps, that now also authenticate to Gemini even though they were never intended for it. With a valid key, an attacker can access uploaded files, cached data, and charge LLM-usage to your account. Even Google themselves had old public API keys, which they thought were non-sensitive, that we could use to access Google's internal Gemini.

What are we seeing now



An Underground AI Economy Explained: https://x.com/HarshalsinghCN/status/2056626175959826692?s=20

How they work?

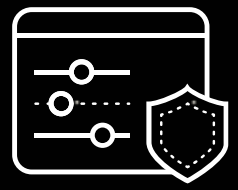


https://github.com/QuantumNous/new-api

Over Attacks Are Preventable, and Security is Solvable

of breaches were enabled by preventable gaps in visibility and inconsistently applied controls.

90%



Why this matters

- Most incidents did not rely on novel or advanced exploits
- Existing controls were often deployed unevenly
- Gaps became more damaging as attack speed increased

Recommendation

Prioritize closing visibility and enforcement gaps before adding new tools.

Attackers Succeed Because of Three Critical Gaps

Complexity

Missing context delays detection

87% data across multiple disconnected sources

Visibility

Inconsistency creates the path of least resistance

90% involved misconfigurations or security coverage gaps

Identity

Excessive trust leads to lateral movement

89% saw identity play a material role in the attack success

From the previous case…. Attackers Succeed Because of Three Critical Gaps

Visibility

- Test environment not integrated with corporate security.
- No centralized governance for extensions, packages, local LLMs, and non-binary tools.

Complexity

- Need to monitor X number of environments in X number of dashboards.

Identity

- Missing Workload Identity Federation (WIF) for Ephemeral Access.
- Insufficient account limits risking resource overconsumption.

New inbound

assignment_late**Resource Management**

Good afternoon Ruben, and happy friday. We have a new inbound, we need your support.

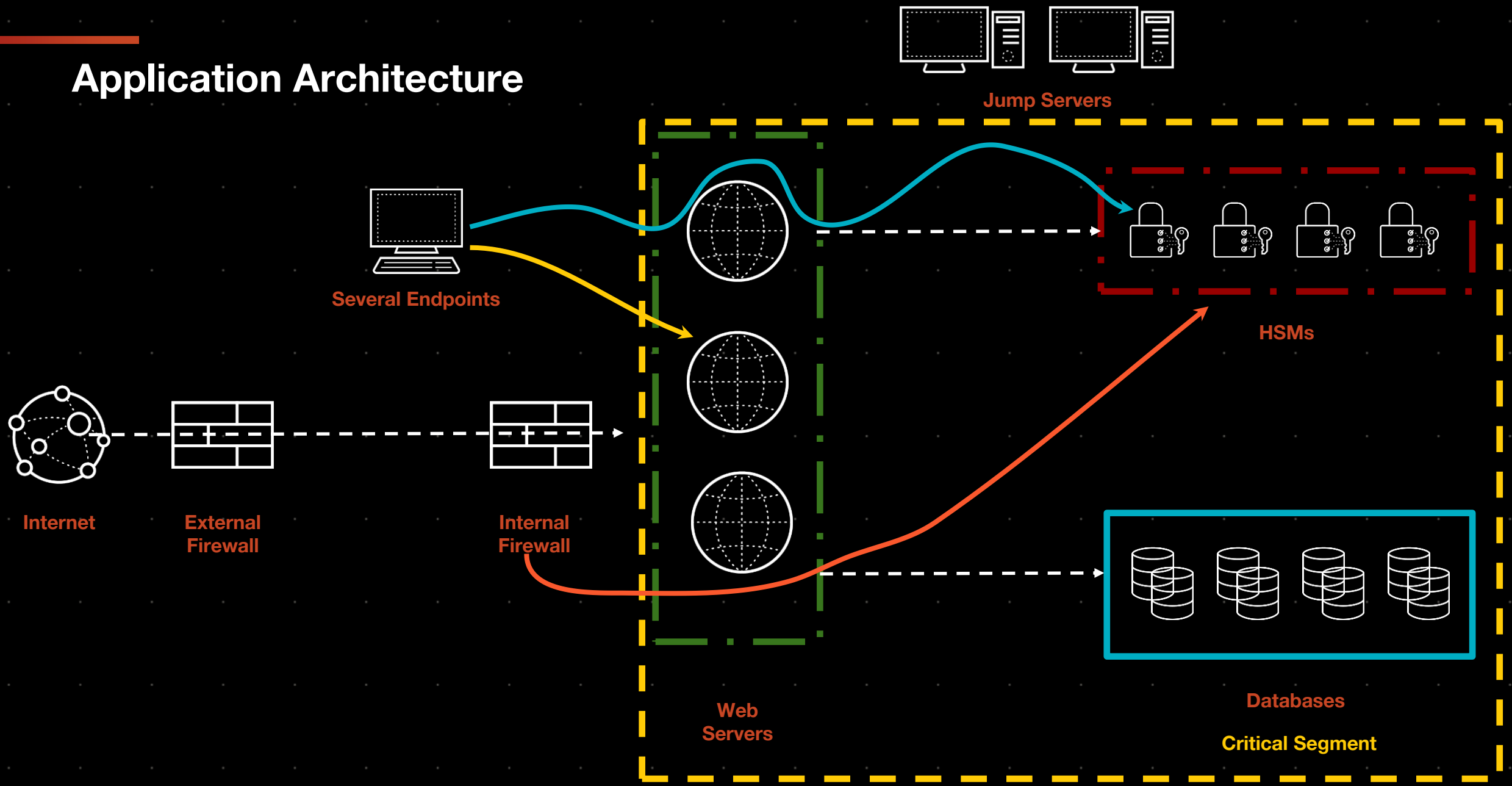
Internal Control Bypass

Evidence Analyzed

- Network traffic
- Web Application Traffic
- Database extractions
- Triage data

- Firewall Rules
- Forensic Images
- Reverse Engineering
- Threat hunting the whole environment

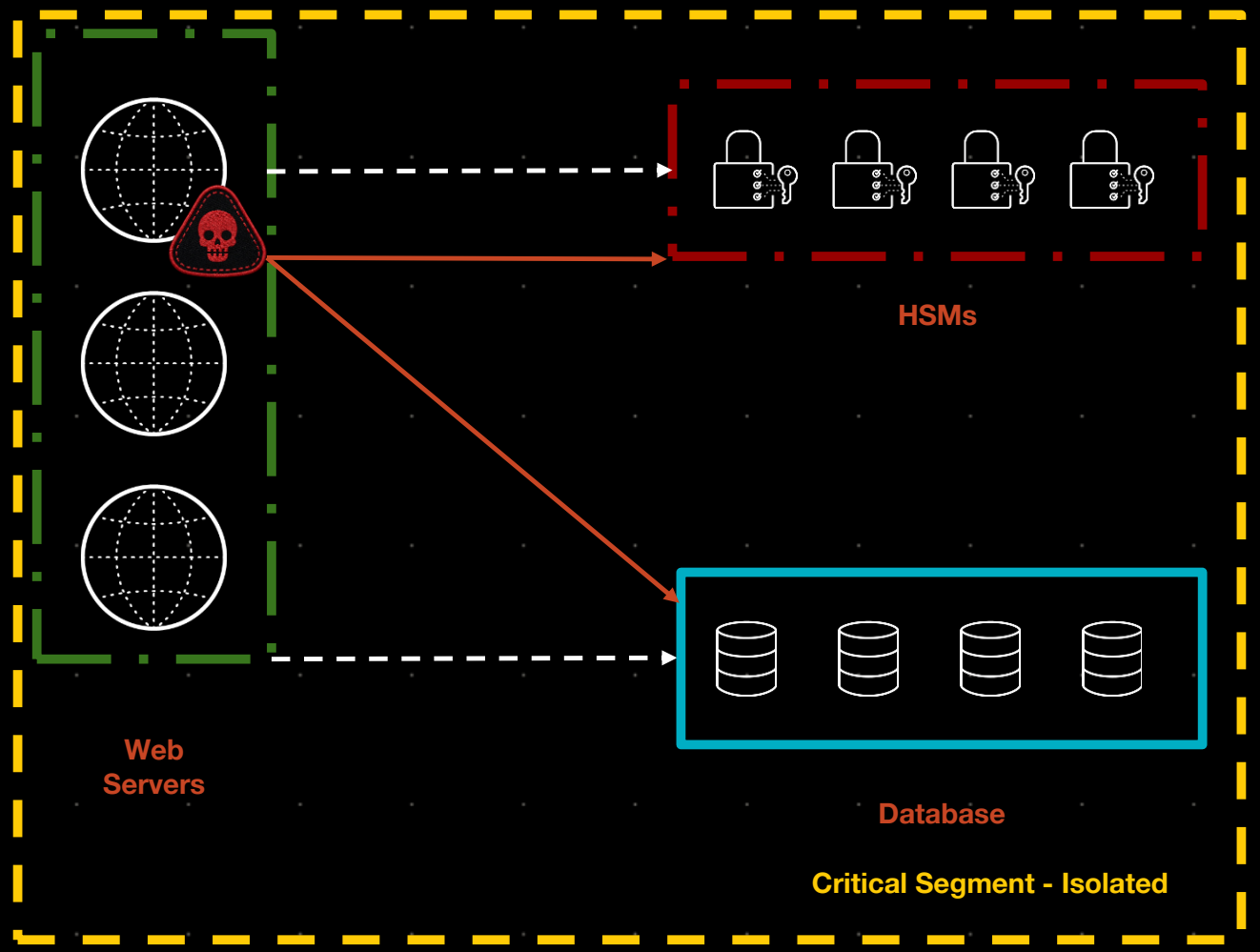
Application Architecture



Findings

Capabilities

- **Malicious Tool build using GraalVM**
- **Bypass Business Logic**
  - Interact directly with databases and HSMs
- **Anti forensics / security measures**



Anti Forensic/Security Measures

Evasion & Persistence

Timestomping

Alters file timestamps to deceive forensic analysis and bypass detection.

Encryption

Used to protect malicious payloads and obfuscate command and control traffic.

Masquerading

Matches legitimate file names or locations to blend into system directories.

System Process Manipulation

Creates or modifies Windows Services to ensure persistence and higher privileges.

Forensic Evidence

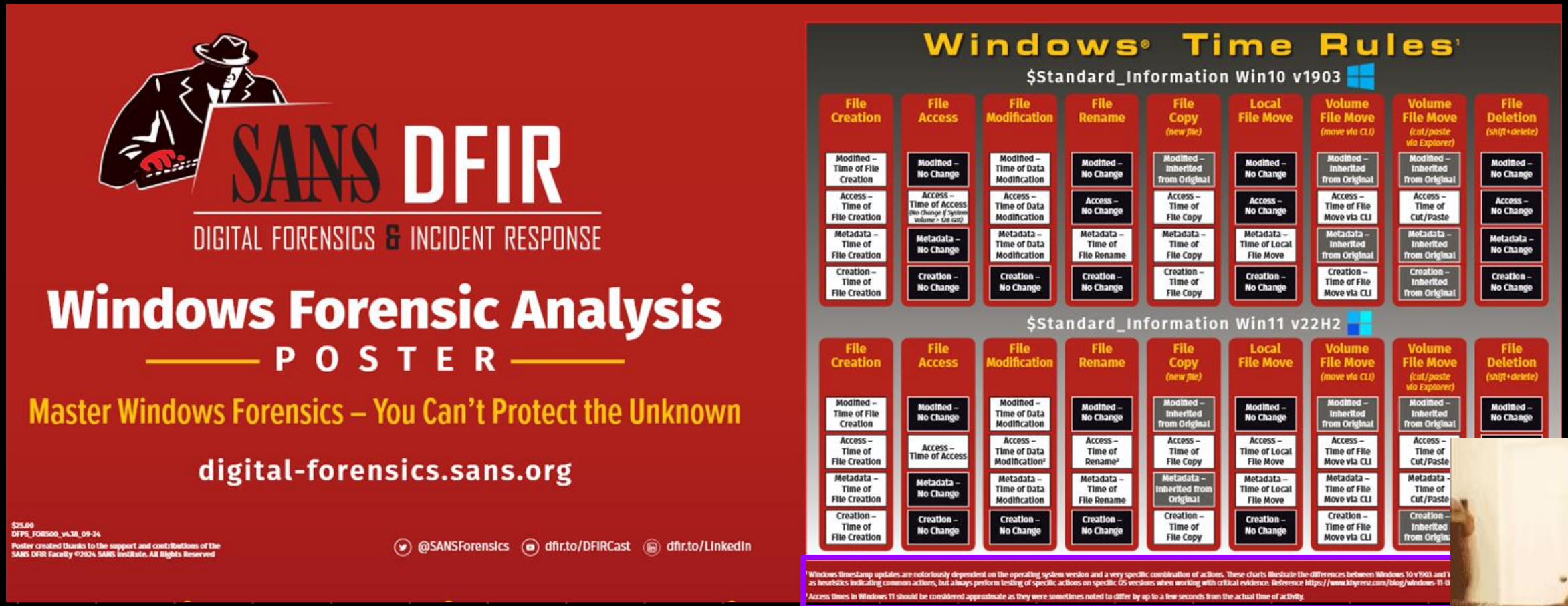
Timestomping Detected

Full path	Created	Created²
\Windows\System32	[redacted]	[redacted]
\Windows\System32\gs-LR		
\Windows\System32\gs-LR[redacted]ll	2011-09-12 14:22:15.888 +0	04-26 11:21:48.730 +0
\Windows\System32\gs-LR[redacted]dll	2017-11-17 04:30:39.530 +0	04-26 09:05:12.115 +0
\Windows\System32\gs-LR[redacted]dll	2005-07-10 02:05:41.577 +0	04-26 16:54:23.902 +0
\Windows\System32\gs-LR[redacted]dll	2012-06-08 20:29:51.656 +0	04-26 07:12:01.045 +0
\Windows\System32\gs-LR[redacted]dll	2005-03-19 20:47:50.526 +0	04-26 14:30:55.678 +0
\Windows\System32\gs-LR[redacted]dll	2010-07-11 07:36:08.647 +0	04-26 10:19:44.201 +0
\Windows\System32\gs-LR[redacted]dll	2011-08-02 21:34:30.443 +0	04-26 22:01:33.890 +0
\Windows\System32\gs-LR[redacted]dll	2010-12-19 20:30:55.989 +0	04-26 05:40:07.123 +0
\Windows\System32\gs-LR[redacted]dll	2014-06-09 20:29:28.703 +0	04-26 13:15:22.951 +0
\Windows\System32\gs-LR[redacted]dll	2014-06-17 08:45:46.156 +0	04-26 20:55:10.009 +0
\Windows\System32\gs-LR[redacted]dll	2025-06-20 03:00:01.234 +0	04-26 11:00:03.456 +0
\Windows\System32\gs-LR[redacted]dll	2011-03-17 09:25:16.244 +0	04-26 01:25:39.111 +0
\Windows\System32\gs-LR[redacted]dll	2005-06-26 06:14:26.492 +0	04-26 18:03:50.770 +0
\Windows\System32\gs-LR[redacted]dll	2011-01-21 22:08:38.755 +0	04-26 23:44:00.001 +0
\Windows\System32\gs-LR[redacted]dll	2008-05-07 22:20:57.106 +0	04-26 08:31:16.822 +0
\Windows\System32\gs-LR[redacted]dll	2005-01-13 14:24:43.714 +0	04-26 04:10:49.555 +0
\Windows\System32\gs-LR[redacted]dll	2009-04-13 08:51:23.027 +0	04-26 19:20:00.670 +0
\Windows\System32\gs-LR[redacted]dll	2013-06-09 01:07:38.448 +0	04-26 15:10:11.234 +0
\Windows\System32\gs-LR[redacted]dll	2014-08-26 21:02:55.196 +0	04-26 12:50:58.333 +0
\Windows\System32\gs-LR[redacted]dll	2007-10-15 08:58:36.210 +0	04-26 21:12:44.120 +0
\Windows\System32\gs-LR[redacted]dll	2009-09-12 08:28:36.365 +0	04-26 17:01:05.671 +0
\Windows\System32\gs-LR[redacted]dll	2011-09-02 12:17:47.304 +0	04-26 06:14:27.888 +0
\Windows\System32\gs-LR[redacted]dll	2011-06-09 23:08:01.644 +0	04-26 14:48:33.102 +0
\Windows\System32\gs-LR[redacted]dll	2017-03-23 11:04:09.261 +0	04-26 09:22:15.999 +0
\Windows\System32\gs-LR[redacted]dll	2012-02-10 02:54:34.449 +0	04-26 22:33:55.000 +0
\Windows\System32\gs-LR[redacted]dll	2015-01-06 11:33:11.339 +0	04-26 10:59:01.002 +0
\Windows\System32\gs-LR[redacted]dll	2016-11-24 03:03:42.769 +0	04-26 05:07:07.707 +0
\Windows\System32\gs-LR[redacted]dll	2008-01-01 23:59:59.999 +0	01-01 23:59:59.999 +0

"Language Resource Folder"

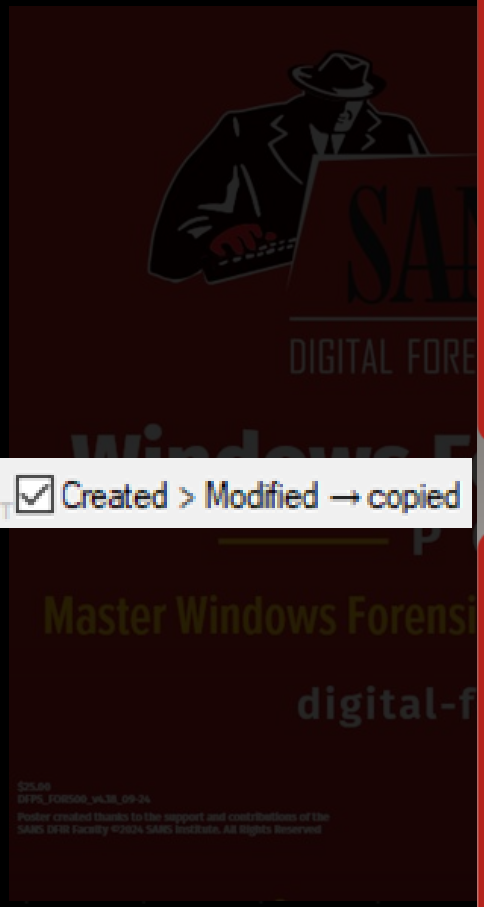
Timestomping

Timestomping



Timestomping

Timestomp



Created > Modified → copied

$Standard_Information Win10 v1903

File Creation	File Access	File Modification	File Rename	File Copy (new file)	Local File Move	Volume File Move (move via CLI)	Volume File Move (cut/paste via Explorer)	File Deletion (shift+delete)
Modified – Time of File Creation	Modified – No Change	Modified – Time of Data Modification	Modified – No Change	Modified – Inherited from Original	Modified – No Change	Modified – Inherited from Original	Modified – Inherited from Original	Modified – No Change
Access – Time of File Creation	Access – Time of Access (No Change if System Volume > 128 GiB)	Access – Time of Data Modification	Access – No Change	Access – Time of File Copy	Access – No Change	Access – Time of File Move via CLI	Access – Time of Cut/Paste	Access – No Change
Metadata – Time of File Creation	Metadata – No Change	Metadata – Time of Data Modification	Metadata – Time of File Rename	Metadata – Time of File Copy	Metadata – Time of Local File Move	Metadata – Inherited from Original	Metadata – Inherited from Original	Metadata – No Change
Creation – Time of File Creation	Creation – No Change	Creation – No Change	Creation – No Change	Creation – Time of File Copy	Creation – No Change	Creation – Time of File Move via CLI	Creation – Inherited from Original	Creation – No Change

$Standard_Information Win11 v22H2

File Creation	File Access	File Modification	File Rename	File Copy (new file)	Local File Move	Volume File Move (move via CLI)	Volume File Move (cut/paste via Explorer)	File Deletion (shift+delete)
Modified – Time of File Creation	Modified – No Change	Modified – Time of Data Modification	Modified – No Change	Modified – Inherited from Original	Modified – No Change	Modified – Inherited from Original	Modified – Inherited from Original	Modified – No Change
Access – Time of File Creation	Access – Time of Access	Access – Time of Data Modification[2]	Access – Time of Rename[2]	Access – Time of File Copy	Access – Time of Local File Move	Access – Time of File Move via CLI	Access – Time of Cut/Paste	Access – No Change
Metadata – Time of File Creation	Metadata – No Change	Metadata – Time of Data Modification	Metadata – Time of File Rename	Metadata – Inherited from Original	Metadata – Time of Local File Move	Metadata – Time of File Move via CLI	Metadata – Time of Cut/Paste	Metadata – No Change
Creation – Time of File Creation	Creation – No Change	Creation – No Change	Creation – No Change	Creation – Time of File Copy	Creation – No Change	Creation – Time of File Move via CLI	Creation – Inherited from Original	Creation – No Change

Persistence & Privilege Escalation

Service Identity

Service Name

Network Application Support

Binary: NetTrackSvc.exe

Masquerading as a Network Binary → in reality NSSM service wrapper.

Operational Goals

- **Persistence:** Established via a deceptive Windows Service.
- **Privilege Escalation:** Service execution typically grants SYSTEM-level access.
- **Deception:** Blends in with legitimate network management utilities.

Description Analysis

Legitimate Source: "Application Information"

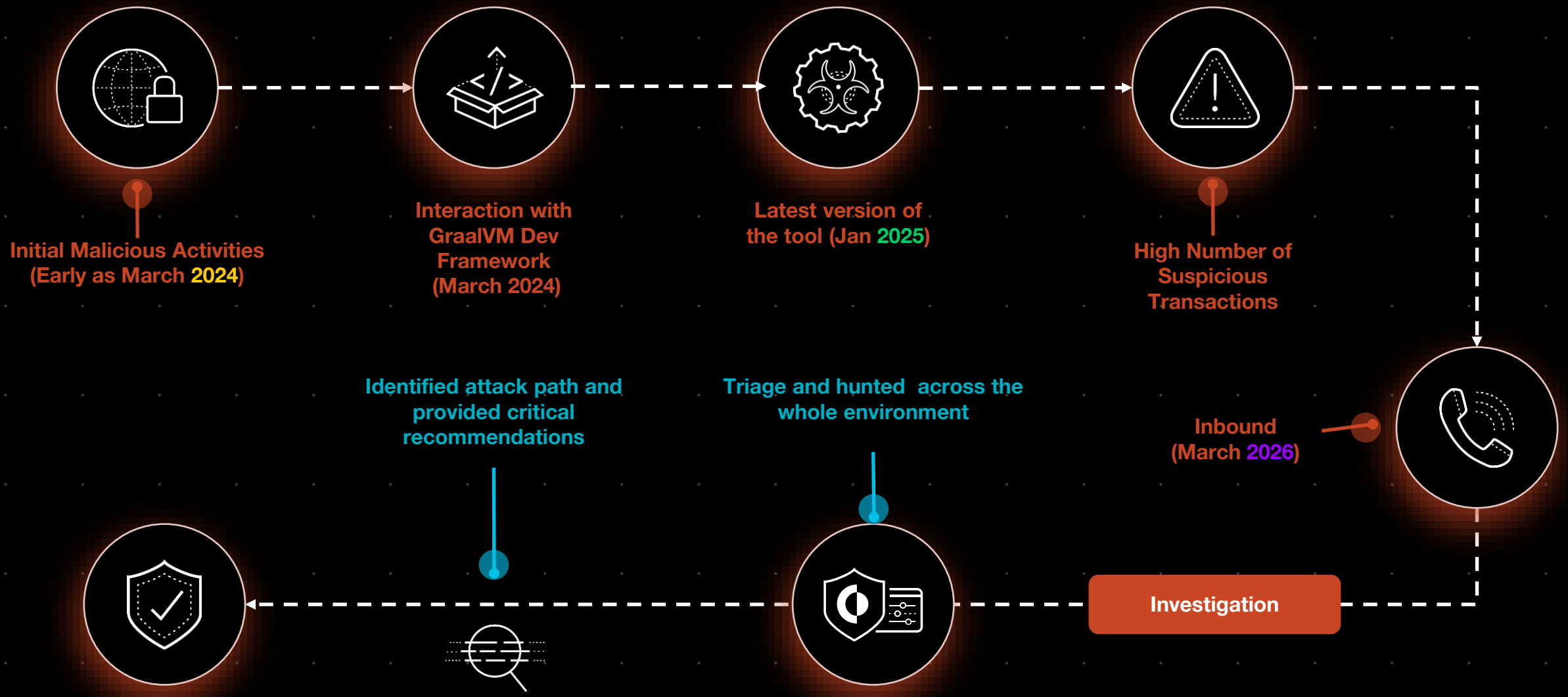
"Facilitates the execution of interactive applications with additional administrative privileges. If this service is stopped, users will be unable to launch applications with the additional administrative privileges they may require to perform preferred user tasks"

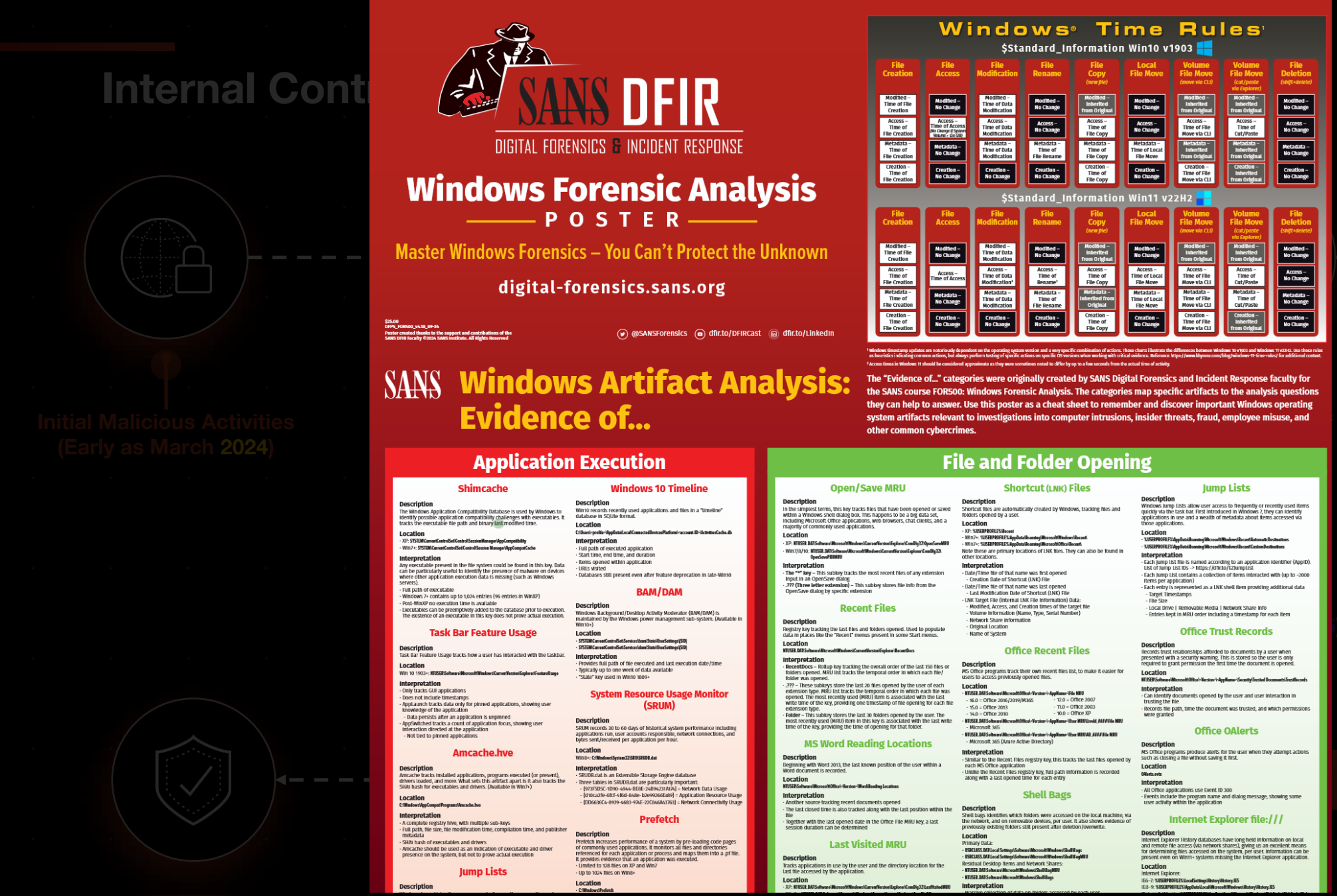
Malicious Modification

"Facilitates the execution of interactive applications with additional network tracking configurations. If this service is stopped, users will be unable to launch applications with the additional administrative privileges they may require to perform preferred user tasks."

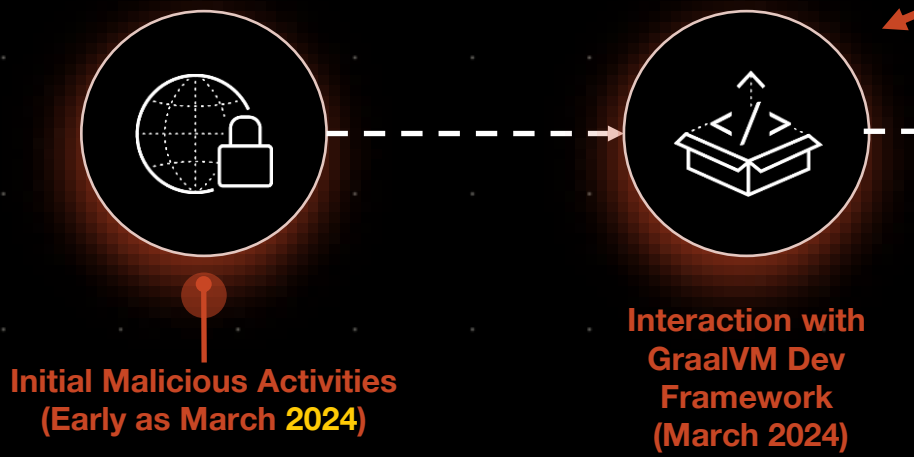
Detection Note: The attacker kept parts of the legitimate description, only altering the functional purpose to match their "Network System" masquerade.

Internal Control Bypass

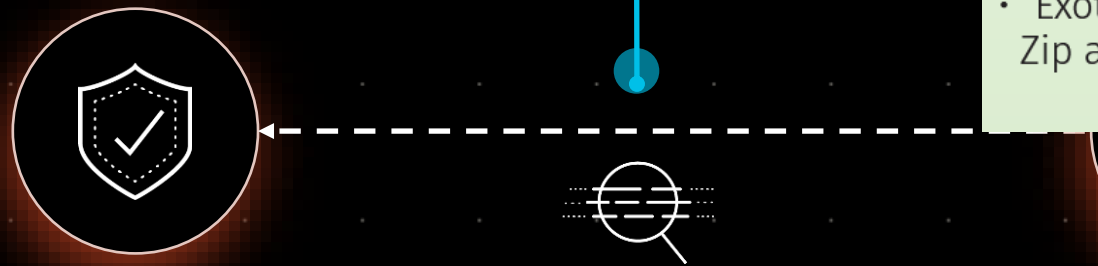



SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE
Windows Forensic Analysis
POSTER
Master Windows Forensics – You Can't Protect the Unknown
digital-forensics.sans.org
@SANSForensics
dfir.to/DFIRCast
dfir.to/LinkedIn
SANS Windows Artifact Analysis: Evidence of...
Windows® Time Rules[1]
$Standard_Information Win10 v1903
$Standard_Information Win11 v22H2
The "Evidence of..." categories were originally created by SANS Digital Forensics and Incident Response faculty for the SANS course FOR500: Windows Forensic Analysis. The categories map specific artifacts to the analysis questions they can help to answer. Use this poster as a cheat sheet to remember and discover important Windows operating system artifacts relevant to investigations into computer intrusions, insider threats, fraud, employee misuse, and other common cybercrimes.
Application Execution
Shimcache
Windows 10 Timeline
BAM/DAM
Task Bar Feature Usage
System Resource Usage Monitor (SRUM)
Amcache.hve
Prefetch
Jump Lists
File and Folder Opening
Open/Save MRU
Shortcut (LNK) Files
Jump Lists
Recent Files
Office Recent Files
Office Trust Records
MS Word Reading Locations
Shell Bags
Office OAlerts
Last Visited MRU
Internet Explorer file:///

Internal Control Bypass



Identified attack path and provided critical recommendations



Shell Bags

Description

Shell bags identifies which folders were accessed on the local machine, via the network, and on removable devices, per user. It also shows evidence of previously existing folders still present after deletion/overwrite.

Location

Primary Data:

- **USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\Bags**
- **USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\BagMRU**

Residual Desktop Items and Network Shares:

- **NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU**
- **NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags**

Interpretation

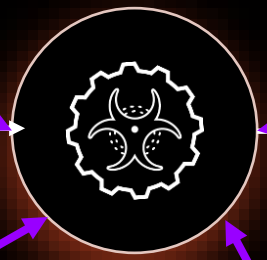
- Massive collection of data on folders accessed by each user
- Folder file system timestamps are archived in addition to first and last interaction times
- “Exotic” items recorded like mobile device info, control panel access, and Zip archive access

Last Visited MRU

Description
Tracks applications in use by the user and the directory location for the last file accessed by the application.

Location
- XP: **NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU**
- Win7+: **NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU**

Interpretation
We get two important pieces of information from this key: applications executed by the user and the last place in the file system that those applications interacted with. Interesting and hidden directories are often identified via this registry key.



Latest version of the tool (Jan 2025)

Jump Lists

Description
Windows Jump Lists allow user access to frequently or recently used items quickly via the task bar. First introduced in Windows 7, they can identify applications in use and a wealth of metadata about items accessed via those applications.

Location
- **%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations**
- **%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations**

Interpretation
- Each jump list file is named according to an application identifier (AppID). List of Jump List IDs -> https://dfir.to/EZJumpList
- Each Jump List contains a collection of items interacted with (up to ~2000 items per application)
- Each entry is represented as a LNK shell item providing additional data
  - Target Timestamps
  - File Size
  - Local Drive | Removable Media | Network Share Info
  - Entries kept in MRU order including a timestamp for each item

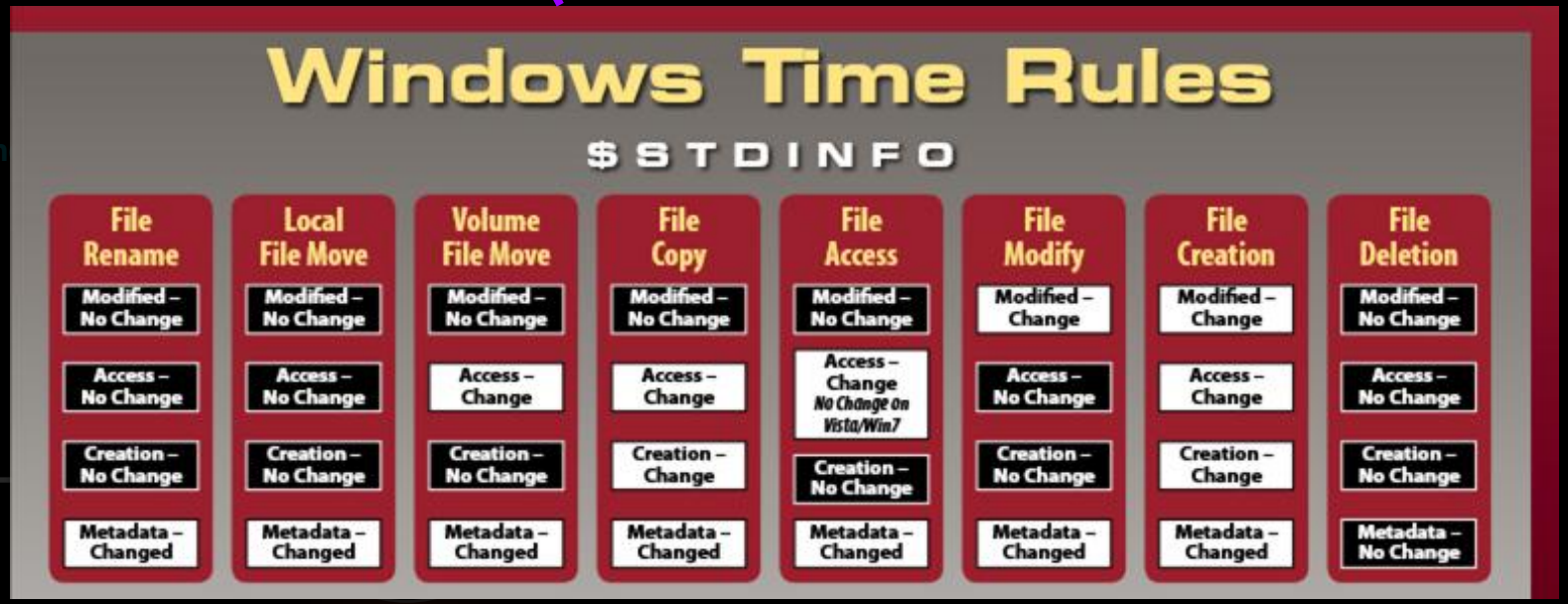
Shortcut (LNK) Files

Description
Shortcut files are automatically created by Windows, tracking files and folders opened by a user.

Location
- XP: **%USERPROFILE%\Recent**
- Win7+: **%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent**
- Win7+: **%USERPROFILE%\AppData\Roaming\Microsoft\Office\Recent**

Note these are primary locations of LNK files. They can also be found in other locations.

Interpretation
- Date/Time file of that name was first opened
  - Creation Date of Shortcut (LNK) File
- Date/Time file of that name was last opened
  - Last Modification Date of Shortcut (LNK) File
- LNK Target File (Internal LNK File Information) Data:
  - Modified, Access, and Creation times of the target file
  - Volume Information (Name, Type, Serial Number)
  - Network Share information
  - Original Location
  - Name of System



Attackers Succeed Because of Three Critical Gaps

Visibility

- Lack of behavioral rules to detect connections from unauthorized systems or processes.

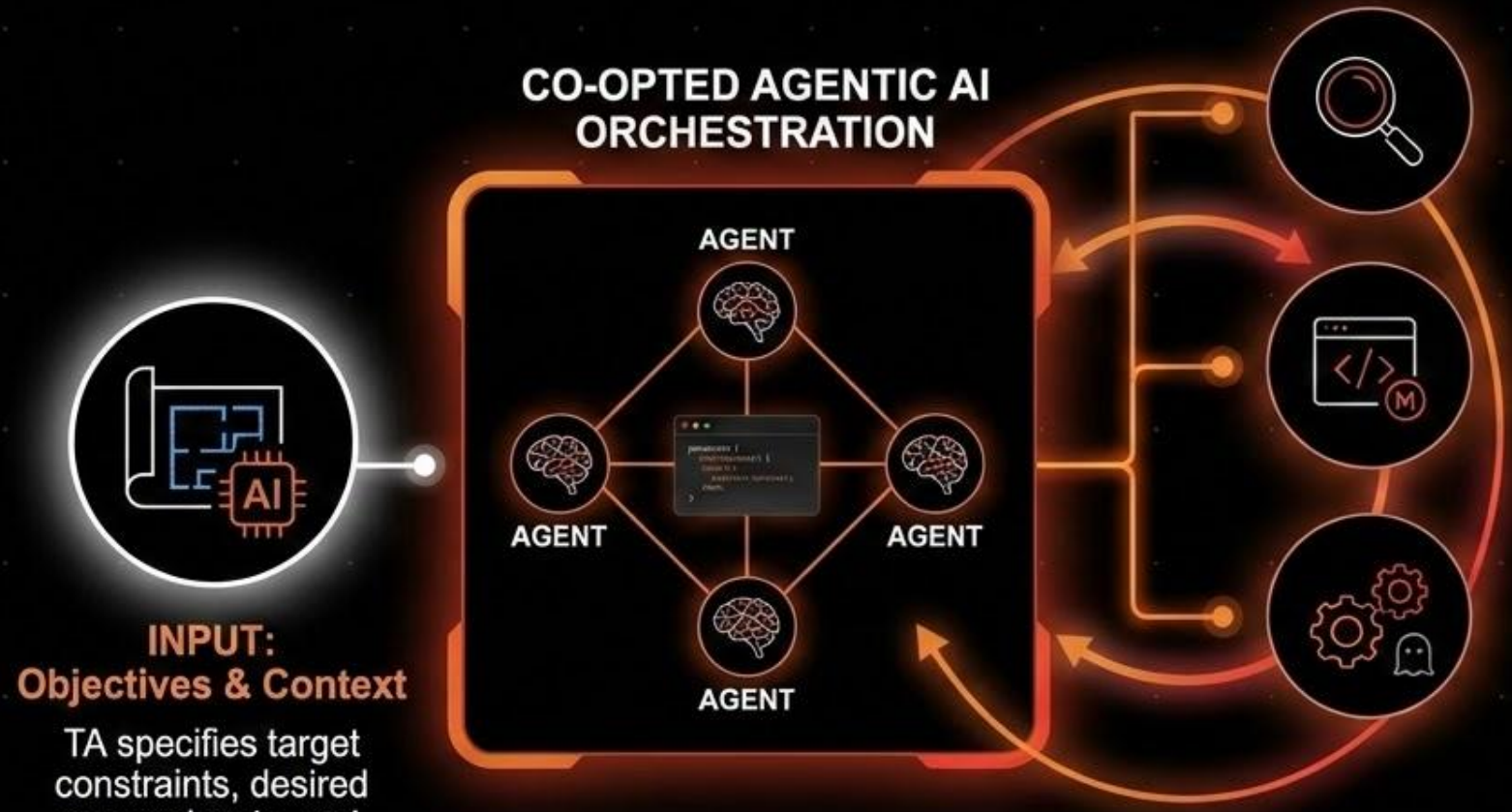
Complexity

- Critical application ecosystems relied on unhardened, End-of-Life operating systems cluttered with diagnostic utilities, providing a pre-installed adversary toolkit.
- Network segmentation allowed connections from insecure zones.

Identity

- Access controls lacked regular lifecycle audits and continuous validation, allowing administrative accounts to operate without MFA or session recording.

Automated Exploitation Lifecycle: Agentic AI as Developer



INPUT: Objectives & Context

TA specifies target constraints, desired access levels, and specific control points for logic manipulation.

Vulnerability Research & Recon

Analyzes target system architectures and potential weaknesses.

Custom Code Generation

Compiles obfuscated exploits and target-specific payloads.

Evasion & Persistence Tuning

Optimizes malware for invisible dwell and logic control bypass.

OUTPUT: Custom Malware Package

OUTPUT: Custom Malware Package

Polymorphic software ready for deployment with embedded persistence and logic bypass capabilities.

New inbound

assignment_late**Resource Management**

Good morning Ruben! Welcome back from your PTO! New inbound, can you support it?

Case File: The Dream Job

Industry
Telco

Region
EMEA

Threat Actor
APT

Type
Network Instrussion

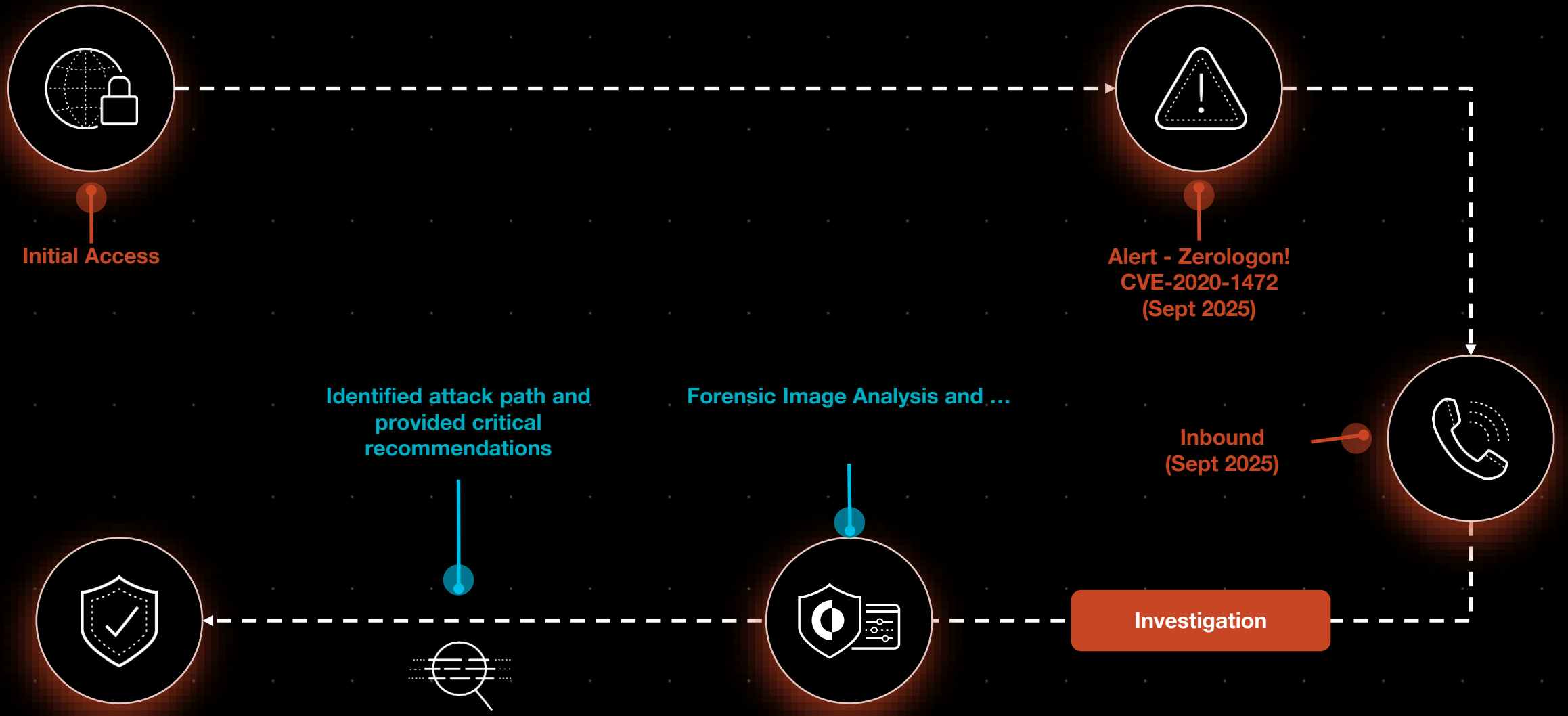
Tactics

- Spear phishing
- Discovery
- Persistence
- Data Exfiltration

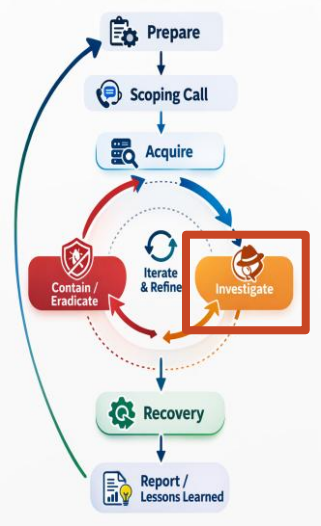
#whoami

Toño Díaz

The Dream Job



Browsing artifacts

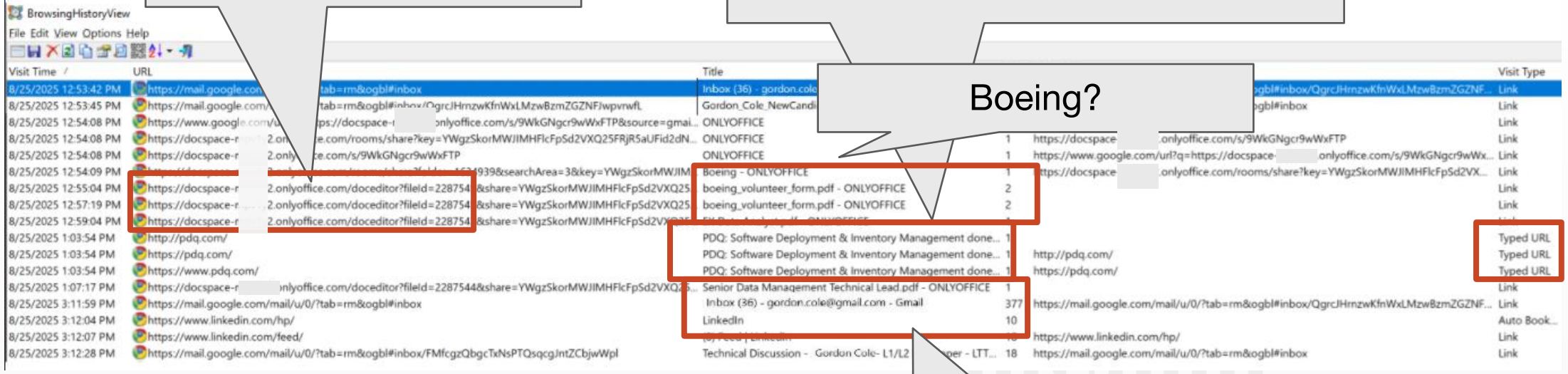


Let’s check browsing. Tool Nirsoft

Onlyoffice space?

PDQ downloaded.Typed URL! why?

Boeing?



PDF of a role description, personal Gmail, LinkedIn..

Tools:

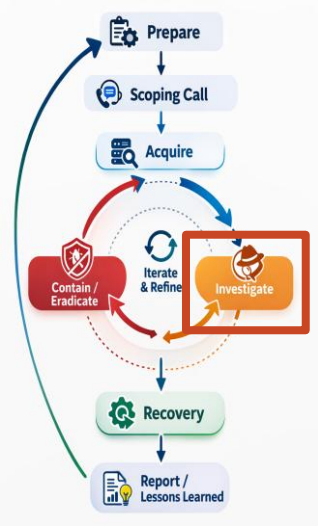
BrowsingHistoryView

SQLite

Tips:

Consider containment actions

Browsing artifacts



Let's check browsing. Tool Nirsoft

CV

LinkedIn chat

Gmail conversation: GordonCole New Candidate

BrowsingHistoryView

File Edit View Options Help

Visit Time	URL	Title	Vis...	Visited From	Visit Type
12:27:53 PM	https://www.linkedin.com/hp/	LinkedIn	10		Auto Book...
12:27:56 PM	https://www.linkedin.com/feed/		18	https://www.linkedin.com/hp/	Link
12:27:59 PM	https://www.linkedin.com/messaging/thread/2-ZGE0MmQ1ZjAtMDk2Y00N2NhLThlYzEtMTdkYmFiMWQ0NGM1...	(7) Messaging | LinkedIn			Link
12:28:14 PM	file:///C:/Users/gordon/Downloads/Resume%20 -%20Gordon(1).pdf				
12:28:34 PM	file:///C:/Users/gordon/Downloads/Resume%20 -%20Gordon(1).pdf				
12:28:41 PM	https://mail.google.com/mail/u/0/?tab=rm&ogbl#inbox	Inbox (36) - gordon.cole@gmail.com - Gmail			Link
12:28:46 PM	https://mail.google.com/mail/u/0/?tab=rm&ogbl#sent	Sent Mail - gordon.cole@gmail.com - Gmail			Link
12:28:49 PM	https://mail.google.com/mail/u/0/?tab=rm&ogbl#sent/QgrcJHrnzwKfnWxLMzwBzmZGZNFJwpvrwfL	Gordon_Cole_NewCandidate - gordon.cole@gmai			Link
12:29:29 PM	https://mail.google.com/mail/u/0/?tab=rm&ogbl#sent	Sent Mail - gordon.cole@gmail.com - Gmail			Link
12:29:33 PM	https://mail.google.com/mail/u/0/?tab=rm&ogbl#sent/QgrcJHrnzwKfnWxLMzwBzmZGZNFJwpvrwfL	Gordon_Cole_NewCandidate - gordon.cole@gmai			Link
12:31:20 PM	https://mail.google.com/mail/u/0/?tab=rm&ogbl#inbox	Inbox (36) - gordon.cole@gmail.com - Gmail			Link
12:31:21 PM	https://mail.google.com/mail/u/0/?tab=rm&ogbl#sent	Sent Mail - gordon.cole@gmail.com - Gmail			Link
12:31:38 PM	https://mail.google.com/mail/u/0/?tab=rm&ogbl#sent/QgrcJHrnzwKfnWxLMzwBzmZGZNFJwpvrwfL	Gordon_Cole_NewCandidate - gordon.cole@gmail.com - Gmail	3	https://mail.google.com/mail/u/0/?tab=rm&ogbl#sent	Link
12:32:11 PM	https://mail.google.com/mail/u/0/?tab=rm&ogbl#sent	Sent Mail - gordon.cole@gmail.com - Gmail	13	https://mail.google.com/mail/u/0/?tab=rm&ogbl#sent/QgrcJHrnzwKfnWxLMzwBzmZGZNFJ...	Link
12:32:15 PM	https://mail.google.com/mail/u/0/?tab=rm&ogbl#inbox	Inbox (36) - gordon.cole@gmail.com - Gmail	377	https://mail.google.com/mail/u/0/?tab=rm&ogbl#sent	Link
12:32:19 PM	https://mail.google.com/mail/u/0/?tab=rm&ogbl#inbox/QgrcJHrnzwKfnWxLMzwBzmZGZNFJwpvrwfL	Gordon_Cole_NewCandidate - gordon.cole@gmail.com - Gmail	10	https://mail.google.com/mail/u/0/?tab=rm&ogbl#inbox	Link
12:32:23 PM	https://mail.google.com/mail/u/0/?tab=rm&ogbl#inbox	Gordon_Cole_NewCandidate - gordon.cole@gmail.com - Gmail	377	https://mail.google.com/mail/u/0/?tab=rm&ogbl#inbox/QgrcJHrnzwKfnWxLMzwBzmZGZNF...	Link
12:33:35 PM	https://www.linkedin.com/hp/	LinkedIn	10		Auto Book...
12:33:37 PM	https://www.linkedin.com/feed/	(8) Feed | LinkedIn	18	https://www.linkedin.com/hp/	Link
12:34:47 PM	https://mail.google.com/mail/?tab=rm&authuser=0&ogbl	Inbox (36) - gordon.cole@gmail.com - Gmail	165		Link
12:34:47 PM	https://mail.google.com/mail/u/0/?tab=rm&authuser=0&ogbl	mail.google.com	165	https://mail.google.com/mail/?tab=rm&authuser=0&ogbl	Link
12:34:47 PM	https://mail.google.com/mail/u/0/?tab=rm&ogbl	Inbox (36) - gordon.cole@gmail.com - Gmail	165	https://mail.google.com/mail/u/0/?tab=rm&authuser=0&ogbl	Link
12:34:49 PM	https://mail.google.com/mail/u/0/?tab=rm&ogbl#inbox	Inbox (36) - gordon.cole@gmail.com - Gmail	377	https://mail.google.com/mail/u/0/?tab=rm&ogbl	Link
12:35:42 PM	https://www.google.com/search?q=test+projects+in+boweing&rlz=1C1GCEA_en&oq=test+projects+in+bowe...	test projects in boweing - Google Search	1		Generated
12:35:50 PM	https://www.google.com/search?q=test+projects+in+boeing&sca_esv=e7c1514da748dd1c&rlz=1C1GCEA_en...	test projects in boeing - Google Search	1	https://www.google.com/search?q=test+projects+in+boweing&rlz=1C1GCEA_en&oq=test+...	Form Submi
12:39:44 PM	https://mail.google.com/mail/u/0/?tab=rm&ogbl#inbox/QgrcJHrnzwKfnWxLMzwBzmZGZNFJwpvrwfL	Gordon_Cole_NewCandidate - gordon.cole@gmail.com - Gmail	10	https://mail.google.com/mail/u/0/?tab=rm&ogbl#inbox	Link
12:40:17 PM	https://docspace onlyoffice.com/rooms/shared/1634892/filter?folder=1634892	ONLYOFFICE	2	https://www.google.com/url?q=https://docspace- onlyoffice.com/rooms/shared/163...	Link

Tools:

BrowsingHistoryView

SQLite

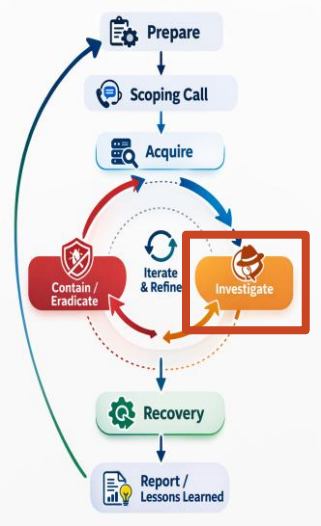
Tips:

Consider containment actions

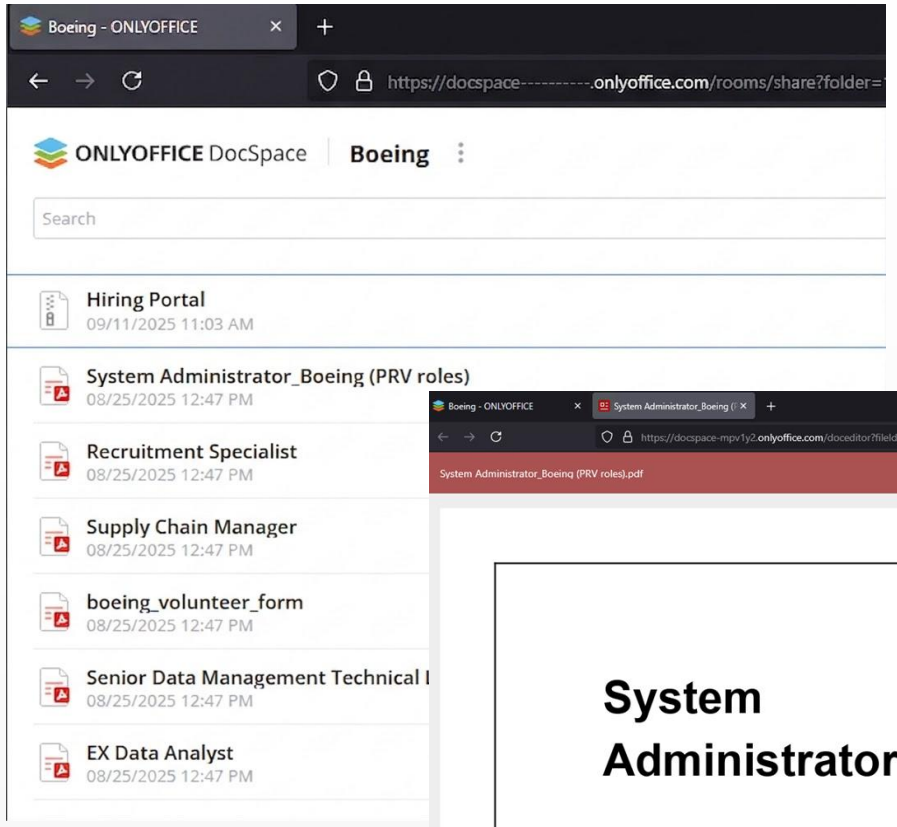
In the interview: Gordon confirmed he had a chat in LinkedIn with recruiter, allegedly from Boeing

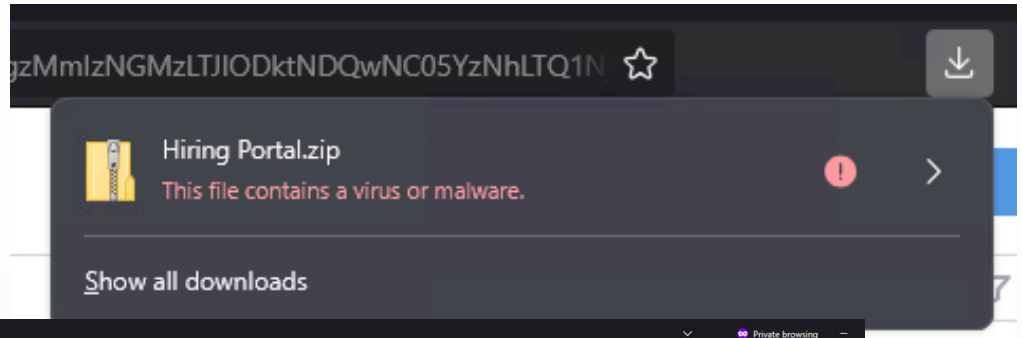
First access to OnlyOffice storage

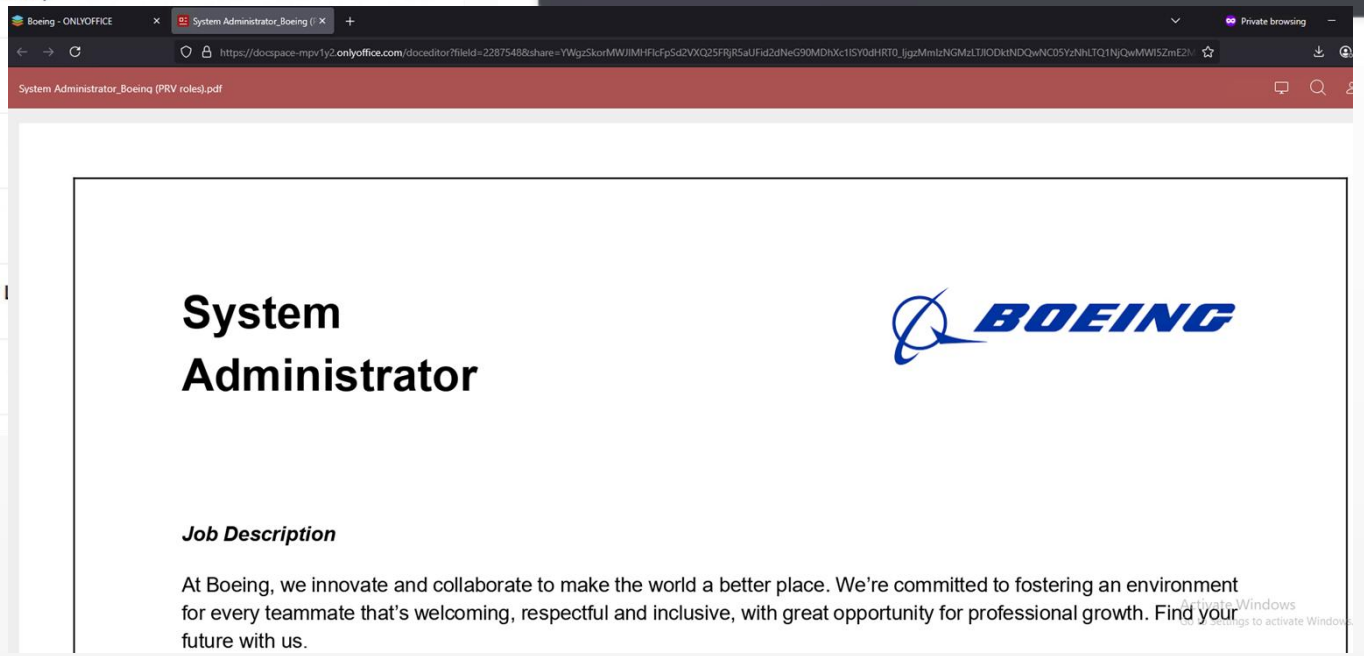
Browsing artifacts



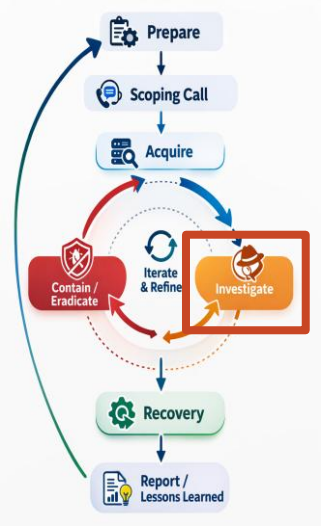
What is in ths docspace?



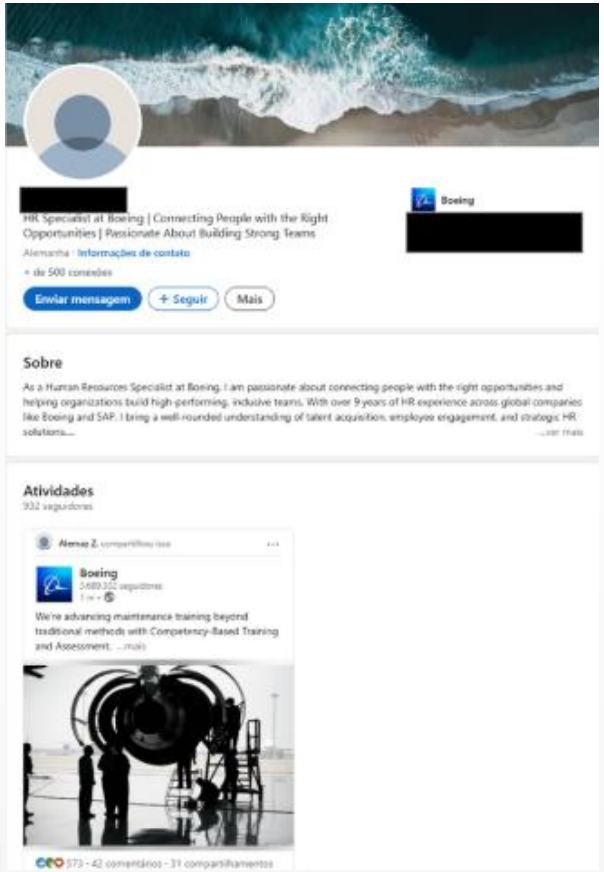




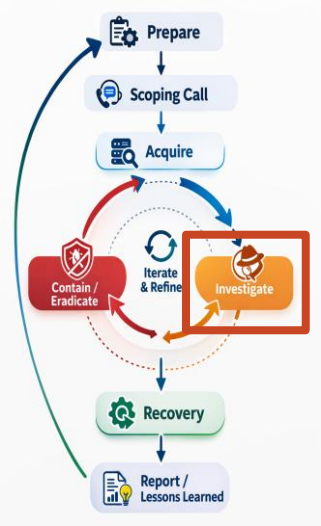
Browsing artifacts

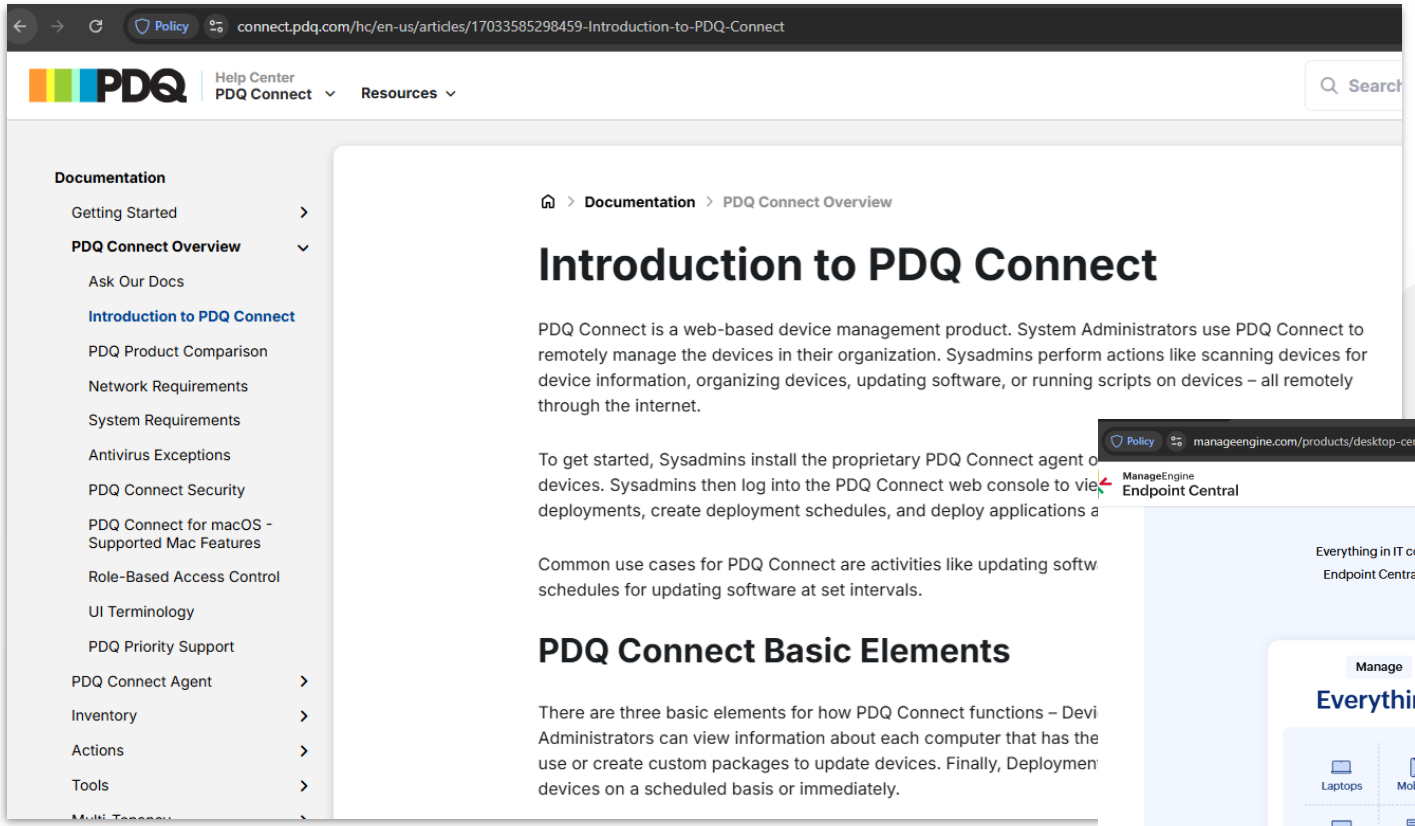


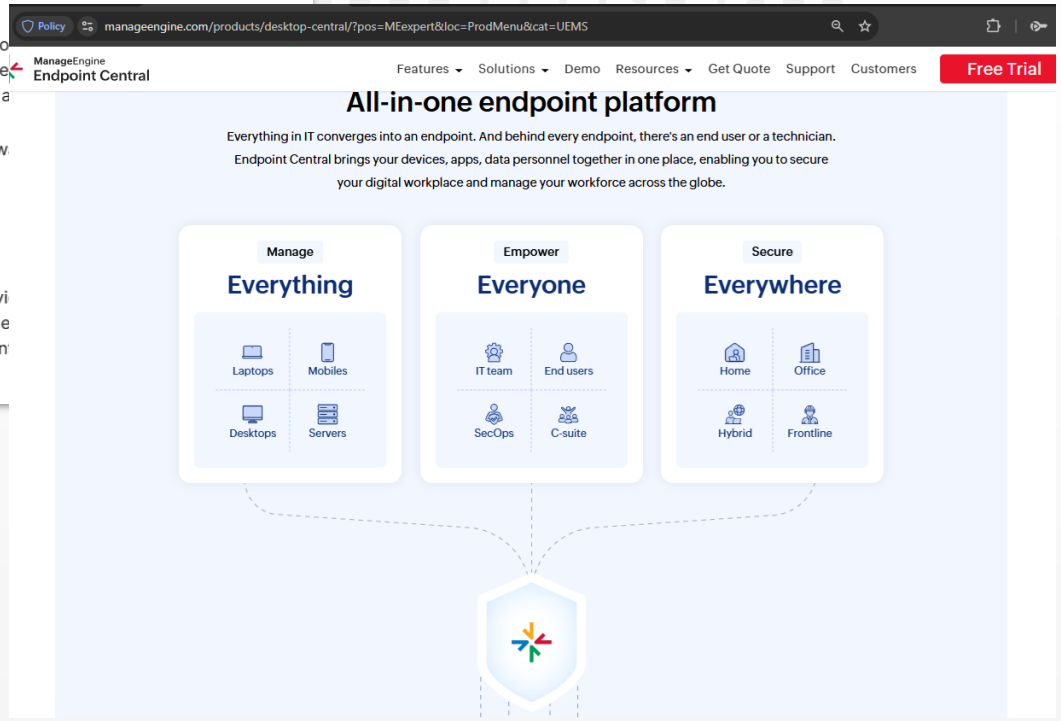
We confirm that TA replicate actual Boeing recruiters



Legit Remote Access Tools







Artifacts:

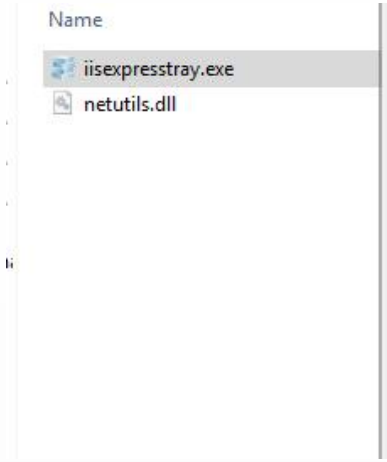
MFT Parser

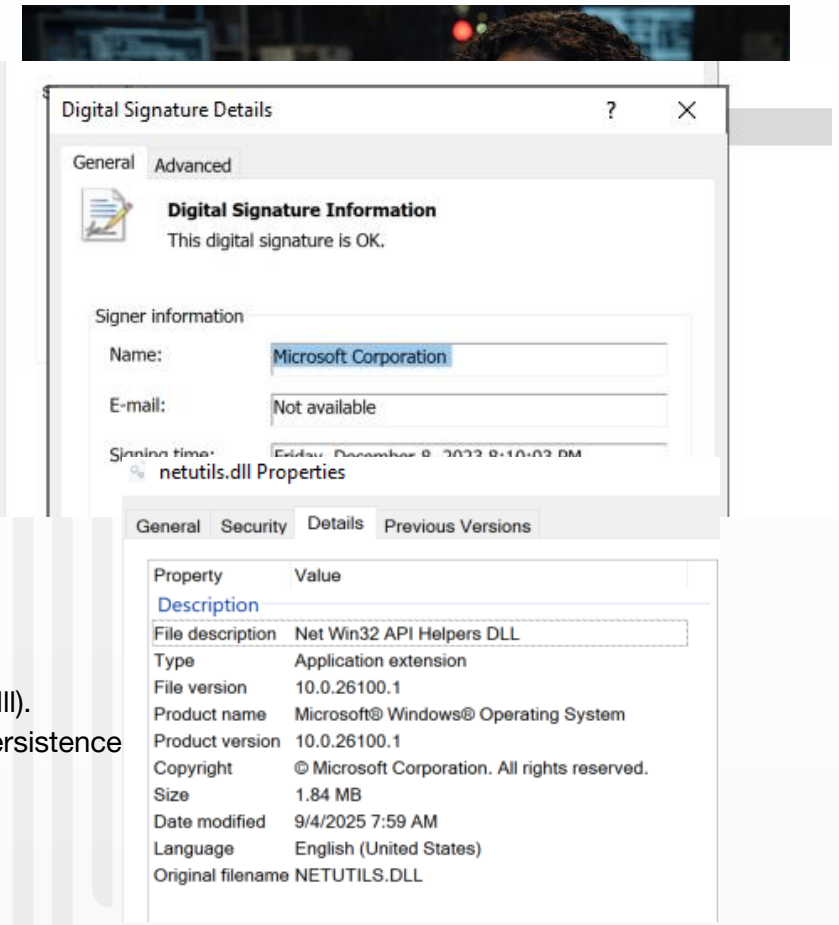
Registry

EVTx

netutils.dll malware analysis

REM colleagues reach us, they have finished netutils.dll analysis:





1. Benign Executable: iisexpresstray.exe

- **Legitimate "IIS Express System Tray" program**, digitally signed by Microsoft.
- Found in paths like C:/Program Files/Microsoft/MDOP MBAM/iisexpress/ and
- C:/Users/gordon.cole/AppData/Local/Microsoft/InstallService/.
- Acts as the **benign host** for the malicious DLL, leveraging trust.

2. MINIBUS Backdoor: netutils.dll

- **Malicious DLL identified as a MINIBIKE/MINIBUS backdoor** by MRE team analysis.
- Found alongside iisexpresstray.exe (e.g., C:/Users/gordon.cole/AppData/Local/Microsoft/InstallService/netutils.dll).
- Provides **full backdoor functionality**: file exfiltration, command execution, system information collection, and persistence

3. Search Order Hijacking (SOH)

- **Key execution method**: iisexpresstray.exe attempts to load a legitimate netutils.dll.
- Attackers exploit the DLL search order, causing the **malicious netutils.dll to be loaded instead**.
- This TTP is consistent with Screening Serpens' known methods for initial payload execution.

4. Fake Outlook Logon Page

- **Post-exploitation action** by the MINIBIKE backdoor.
- The backdoor is designed to **"Prompt Outlook creds"** (as per MRE team findings).
- This is a social engineering tactic to **steal user credentials** by presenting a fraudulent login interface.

```
START[  gordoncole DammGoodCoffee@42 ]END
START[    ]END
START[    ]END
START[    ]END
START[    ]END
START[    ]END
```

C:\Users\Public\NTUSER2.dat

Agent Serpens

Agent Serpens is a suspected nation-state threat actor attributed to **Iran**. Active since **2013**.

Tactics & Custom Tools

Sophisticated social engineering and adaptive tactics.

- **Backdoors:** SnailResin, SlugResin, Sponsor.
- **Harvesting:** GCollection, DWP.

Mobile & Open Source

Surveillance via **PINEFLOWER** Android malware.

Augments capabilities with open-source tools:

- Mimikatz, Chisel, Plink
- Abuses PowerShell (AnvilEcho, TAMECAT)

Motivation(s): Espionage

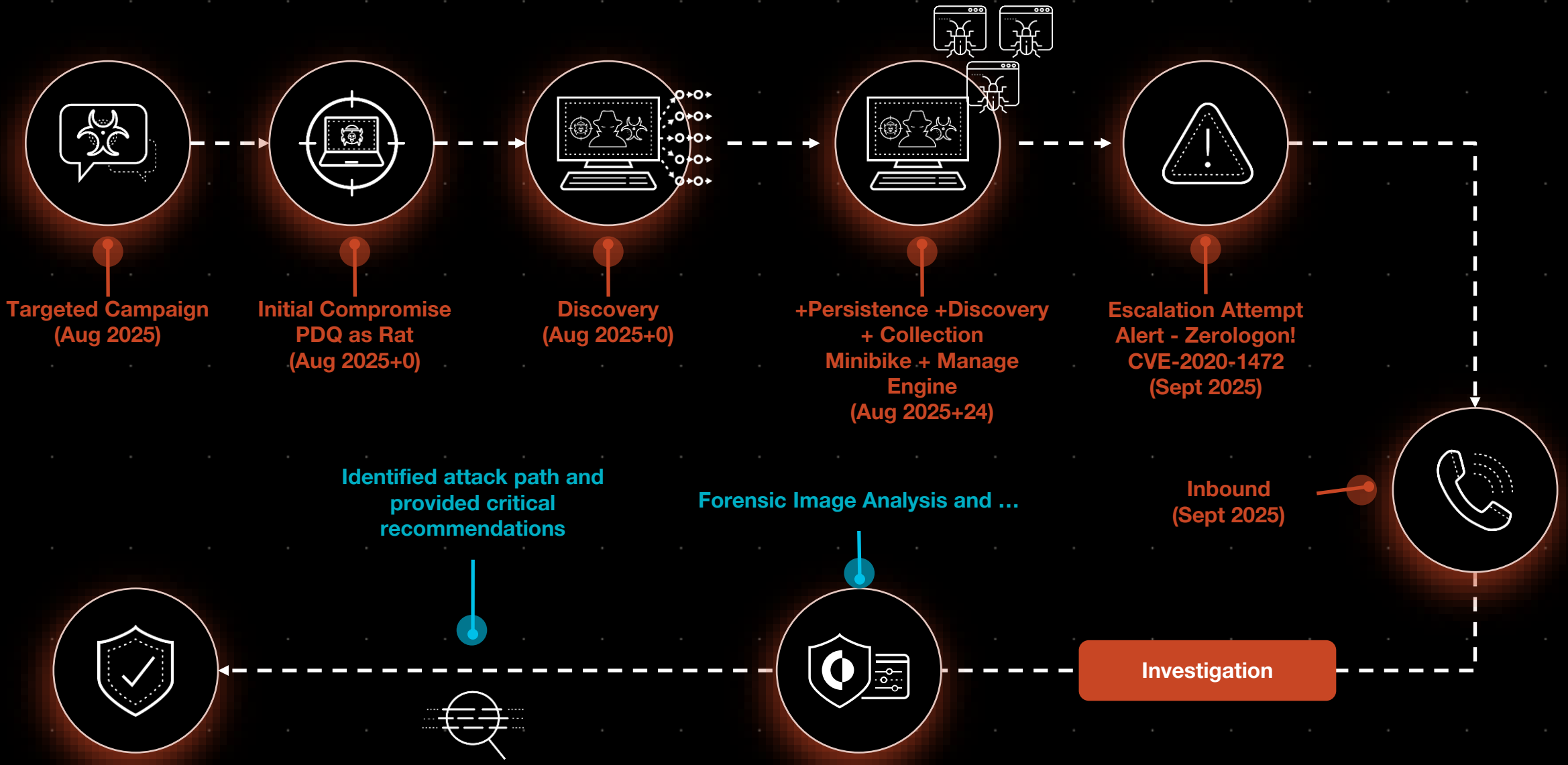
Aliases

APT35 | G0059 | ITG18 | TA453 | DIREFATE | GROUP 83 | DAMSELFLY | NEWSCASTER | PHOSPHORUS | GREYCATFISH | MAGIC HOUND | PHOSPHOROUS | SAFFRON ROSE | IRIDIUM GROUP | YELLOW GARUDA | MINT SANDSTORM | CHARMING KITTEN | COBALT ILLUSION | BALLISTIC BOBCAT | WHITE PHOSPHOROUS

Targeted Industries

COLLEGE/UNIVERSITY | HIGHER EDUCATION | HEALTHCARE | HIGH TECHNOLOGY | MEDIA & ENTERTAINMENT | PHARMA & LIFE SCIENCES | FEDERAL GOVERNMENT | FINANCIAL SERVICES | MANUFACTURING | EDUCATION | PHARMACEUTICAL PREPARATIONS | PROFESSIONAL & LEGAL SERVICES | TELECOMMUNICATIONS | COLLEGES AND UNIVERSITIES, NSK | NONCOMMERCIAL RESEARCH ORGANIZATIONS | AUTOMOTIVE | CIVIL ENGINEERING

The Dream Job



Attackers Succeed Because of Three Critical Gaps

Visibility

- Lack of alerts due to the lack of application allowlisting.
- Therefore, SOC did not have visibility to identify remote access tools being deployed creating a 24-day dwell time.

Complexity

- Lack of application allowlisting allowed unapproved remote management utilities to execute.

Identity

- Administrative identities lacked behavioral baselines or continuous step-up authentication, enabling compromised accounts to silently execute deep system reconnaissance and high-privilege registry dumps.

Insiders ?

¡MUCHAS GRACIAS!

ESKERRIK ASKO!