



EuskalHack Security Congress IX





Insiders ?





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

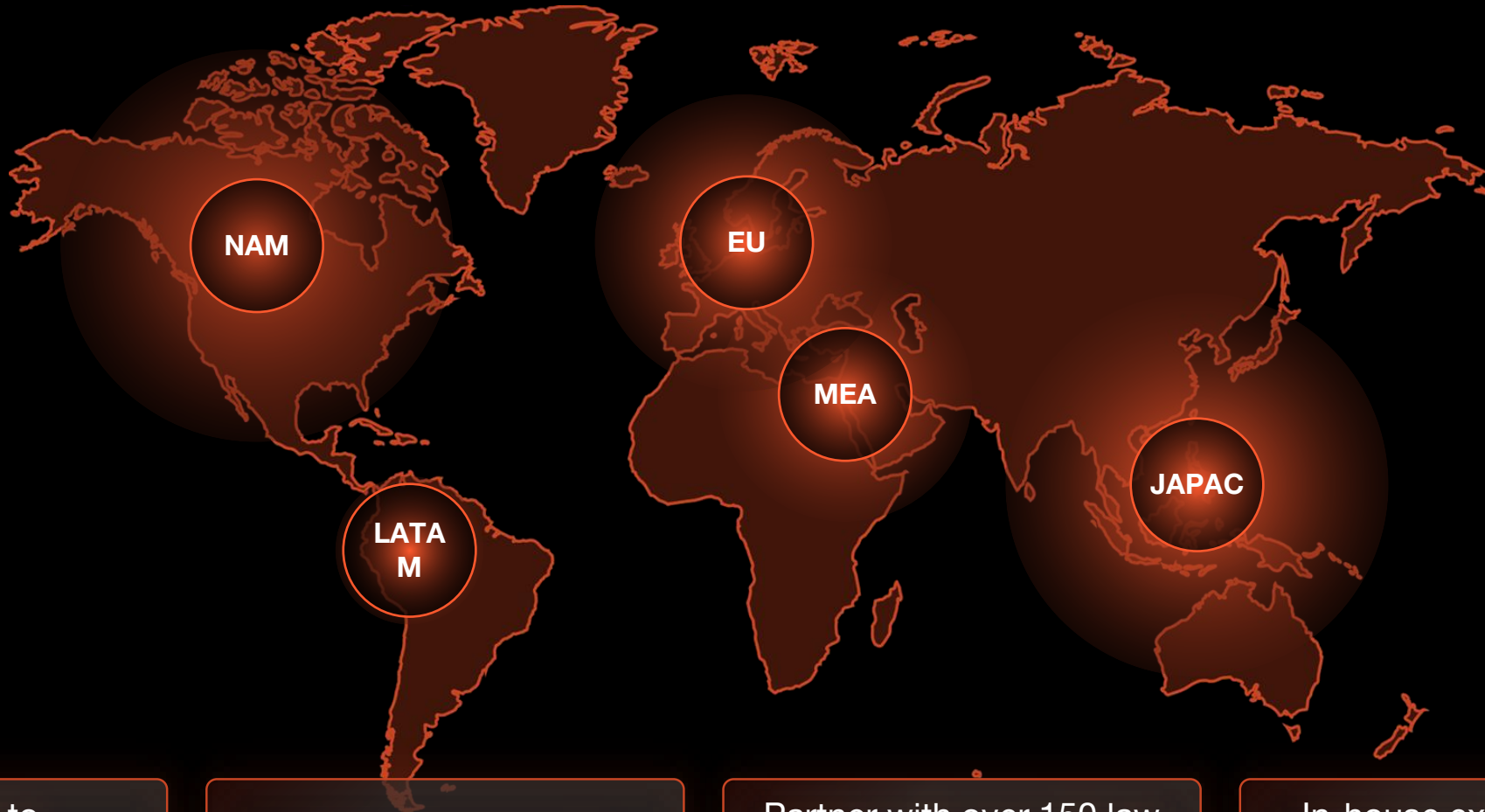


Cybersecurity

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

Global Incident Response Report 2026

CASE ID: CL-STA-0043

SYSTEM.
REFLECTION.METHODINFO

METHODINFO

=

ASSEMBLY.GETTYPES()
[0].GETMETHOD("RUN");

|||||

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



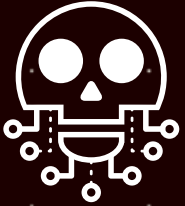
4

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

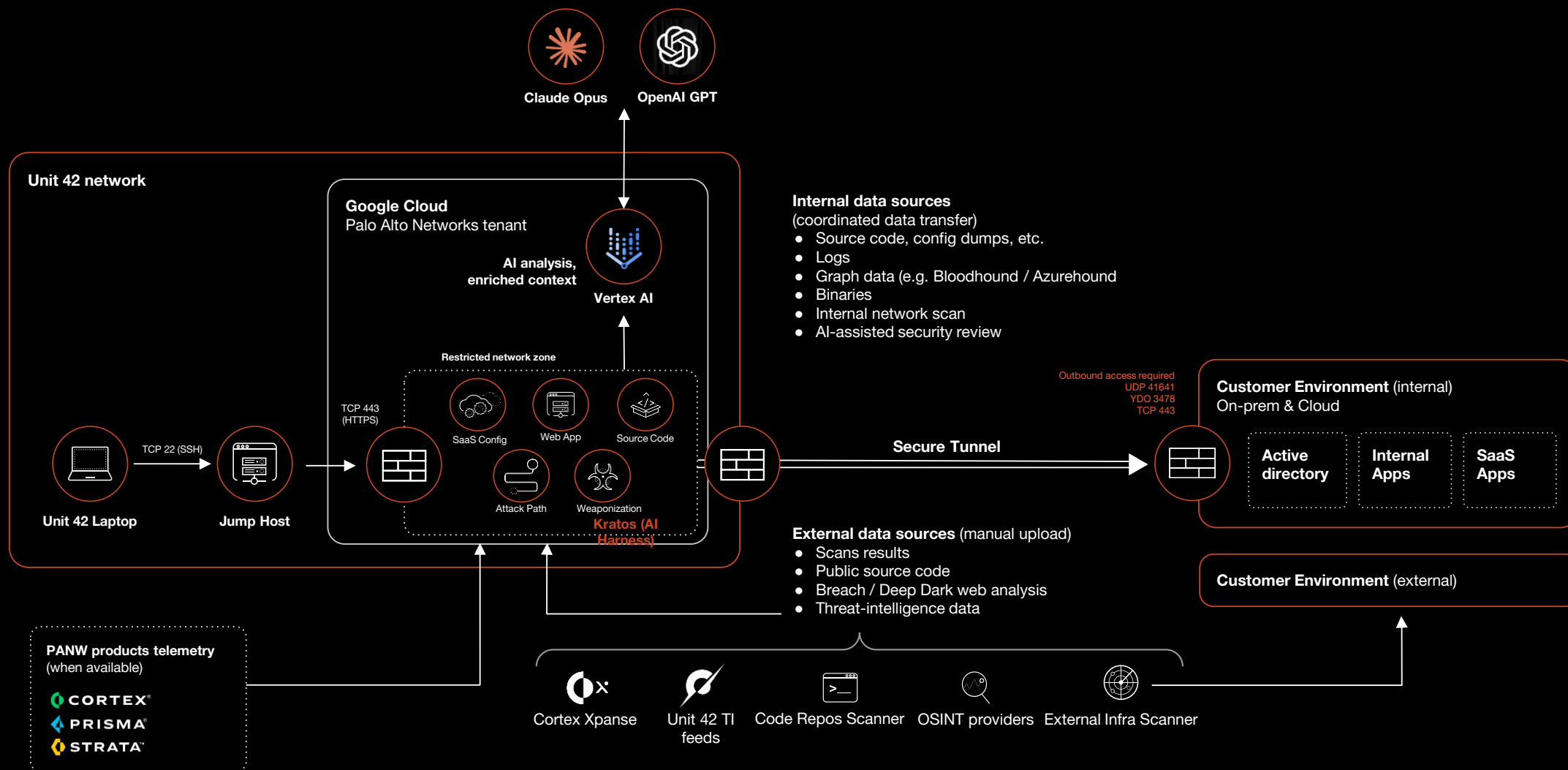
- Automation increased attack speed and consistency
- Skill barriers are reduced for complex operations.
- AI improved execution efficacy changing intent

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





Risks with Secrets



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

THE DIG

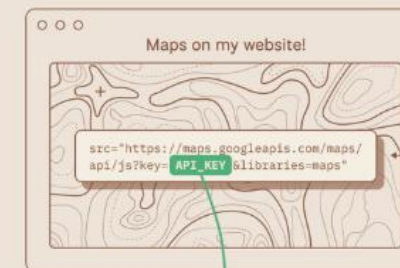
Google API Keys Weren't Secrets. But then Gemini Changed the Rules.

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.

Simpler times

It was 2019, remember Hot Girl Summer?



"not a secret"

Used as a project identifier,
totally cool for client code

Today

After you enabled Gemini on your project



"please don't notice me"

The same key today can access
sensitive Gemini endpoints

What are we seeing now

Home

Console

Model Marketplace

Documentation

About

Filter

Reset

Provider

All vendors

Anthropic

Google

OpenAI

讯飞

Available token groups

All groups

AWS Claude Plat...

Gemini-8

Gemini超稳直连...

aistudio

az

banana2

cli

codex

default

gemini-flash

kiro

veo

vertex

Billing type

All types

Pay as you go

Pay per request

Label

All tags

Endpoint type

All endpoints

anthropic

gemini

image-generation

openai

All vendors124 models

View all available AI model suppliers, including models from many well-known suppliers.

Fuzzy search model name

Copy

Top Up price

Ratio

Table view

M

Pay as you go

gpt-5.5

Input Price \$1.5000 / 1M Tokens

Completion Price \$9.0000 / 1M Tokens

Input Cache Read Price \$0.1500 / 1M Tokens

Pay as you go

gpt-image-1

Input Price \$22.5000 / 1M Tokens

Completion Price \$45.0000 / 1M Tokens

Input Cache Read Price \$5.6250 / 1M Tokens

Image Input Price \$45.0000 / 1M Tokens

Pay as you go

gpt-image-1.5

Input Price \$2.4000 / 1M Tokens

Completion Price \$9.6000 / 1M Tokens

Input Cache Read Price \$0.6000 / 1M Tokens

Pay as you go

gpt-image-2

Input Price \$1.5000 / 1M Tokens

Completion Price \$9.0000 / 1M Tokens

Input Cache Read Price \$0.6000 / 1M Tokens

Image Input Price \$2.4000 / 1M Tokens

Pay as you go

gpt-image-2-c

Model price \$0.050 / request

Pay per request

claude-3-5-haiku-20241022

Input Price \$0.3200 / 1M Tokens

Completion Price \$1.6000 / 1M Tokens

Input Cache Read Price \$0.0320 / 1M Tokens

Input Cache Creation Price \$0.4000 / 1M Tokens

Pay as you go

claude-3-5-sonnet-20240620

Input Price \$1.2000 / 1M Tokens

Completion Price \$6.0000 / 1M Tokens

Input Cache Read Price \$0.1200 / 1M Tokens

Input Cache Creation Price \$1.5000 / 1M Tokens

Pay as you go

claude-3-5-sonnet-20241022

Input Price \$1.2000 / 1M Tokens

Completion Price \$6.0000 / 1M Tokens

Input Cache Read Price \$0.1200 / 1M Tokens

Input Cache Creation Price \$1.5000 / 1M Tokens

Pay as you go

<

1

2

3

4

5

6

7

>

Items per page: 20

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

How they work?

Policy github.com/QuantumNous/new-api

README Code of conduct AGPL-3.0 license Security

New API

Next-Generation LLM Gateway and AI Asset Management System

[简体中文](#) | [繁體中文](#) | [English](#) | [Français](#) | [日本語](#)

license [AGPL-3.0](#) release [v1.0.0-rc.11](#) docker [dockerHub](#) go report [A+](#)

1 GITHUB TRENDING
#1 Repository Of The Day

RECOMMEND BY **HelloGitHub** 46

FIND US ON **Product Hunt** 4

[Quick Start](#) • [Key Features](#) • [Deployment](#) • [Documentation](#) • [Help](#)

Project Description

Important

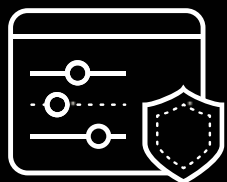
- This project is intended solely for lawful and authorized AI API gateway, organization-level authentication, multi-model management, usage analytics, cost accounting, and private deployment scenarios.
- Users must lawfully obtain upstream API keys, accounts, model services, and interface permissions, and must comply with upstream terms of service and applicable laws and regulations.
- Users should ensure their use complies with upstream terms of service and applicable laws and regulations.
- When providing generative AI services to the public, users should comply with applicable regulatory requirements and fulfill all filing, licensing, content safety, real-name verification, log retention, tax, and upstream authorization obligations required by their jurisdiction.

<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

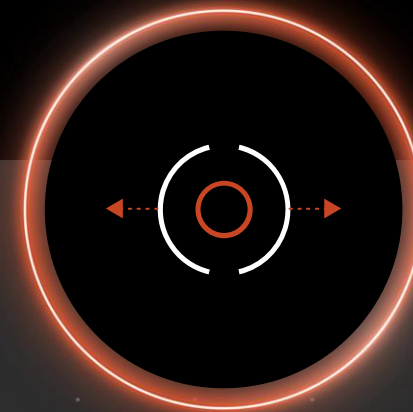
87% data across
multiple disconnected sources



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.

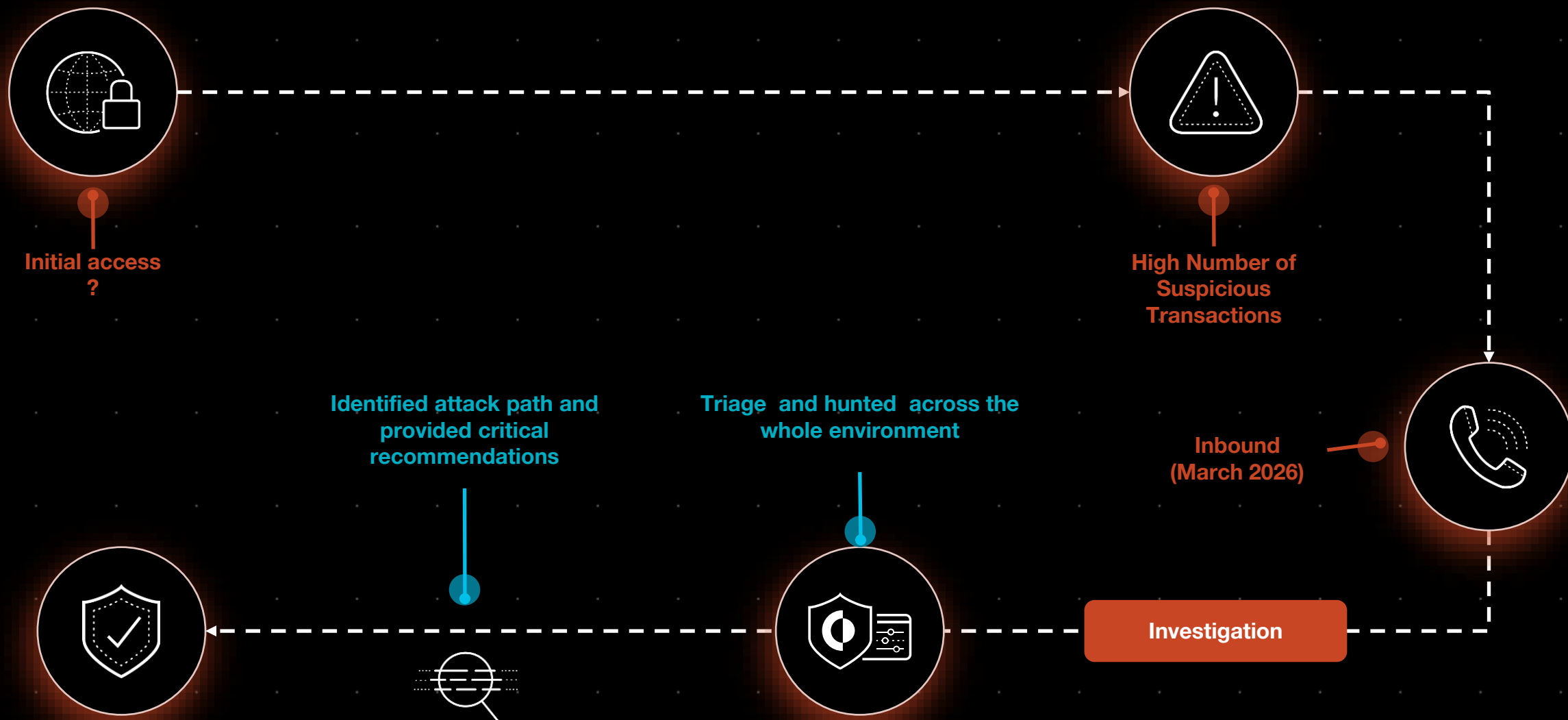
New inbound



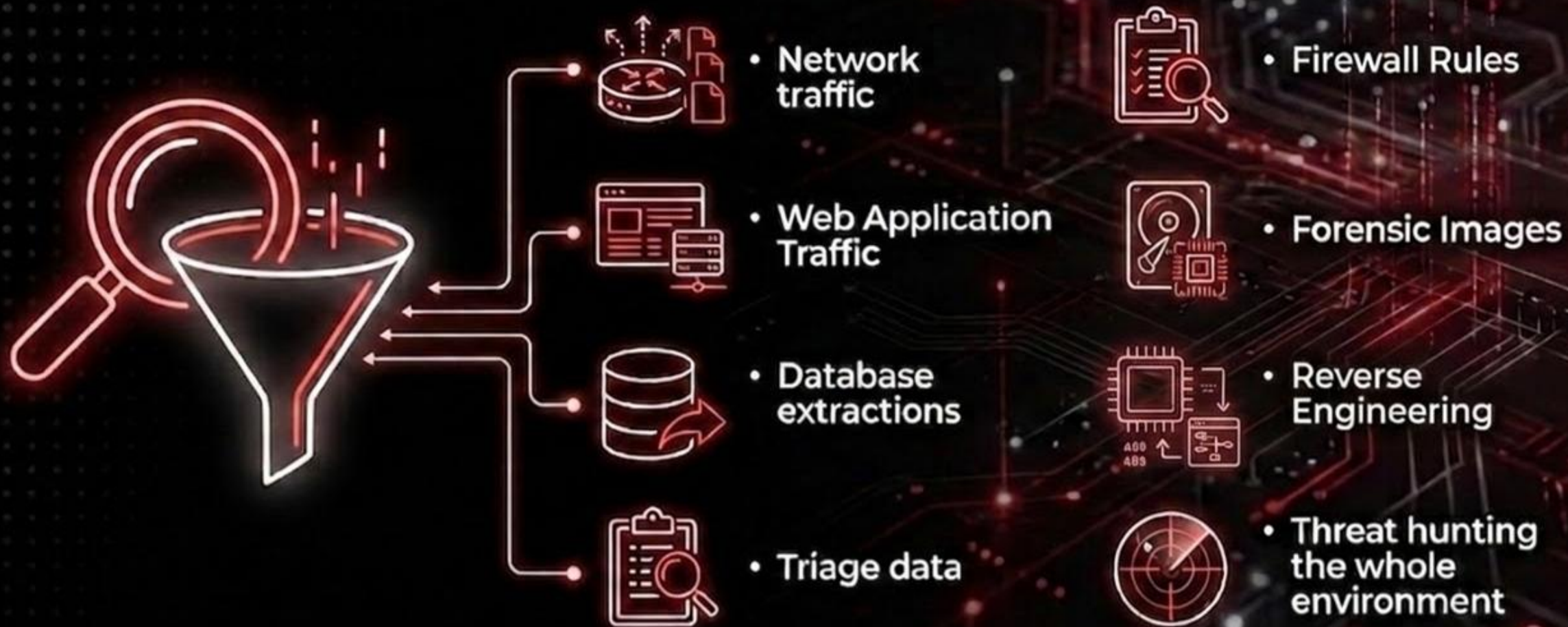
assignment_lateResource Management

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

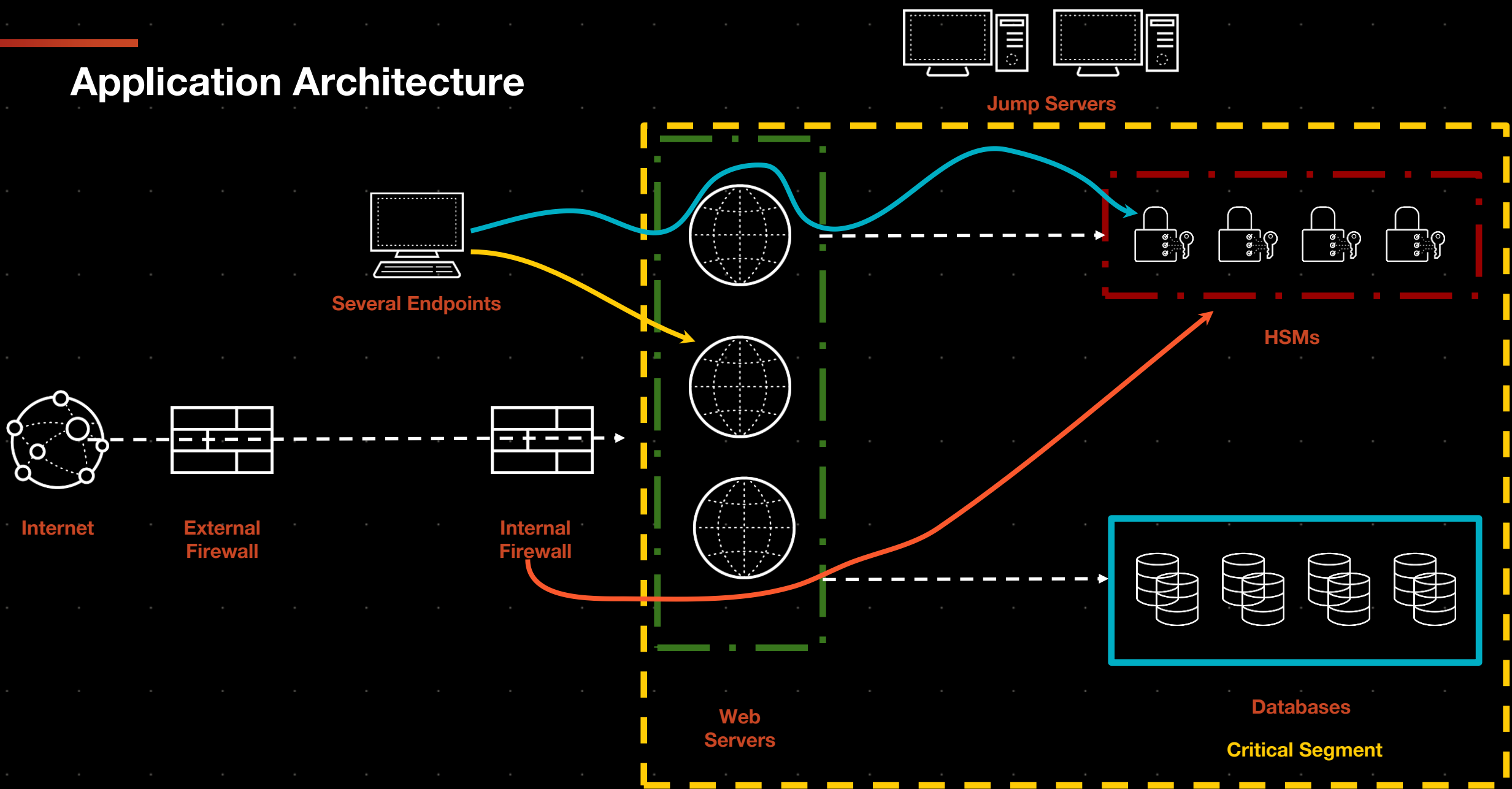
Internal Control Bypass



Evidence Analyzed



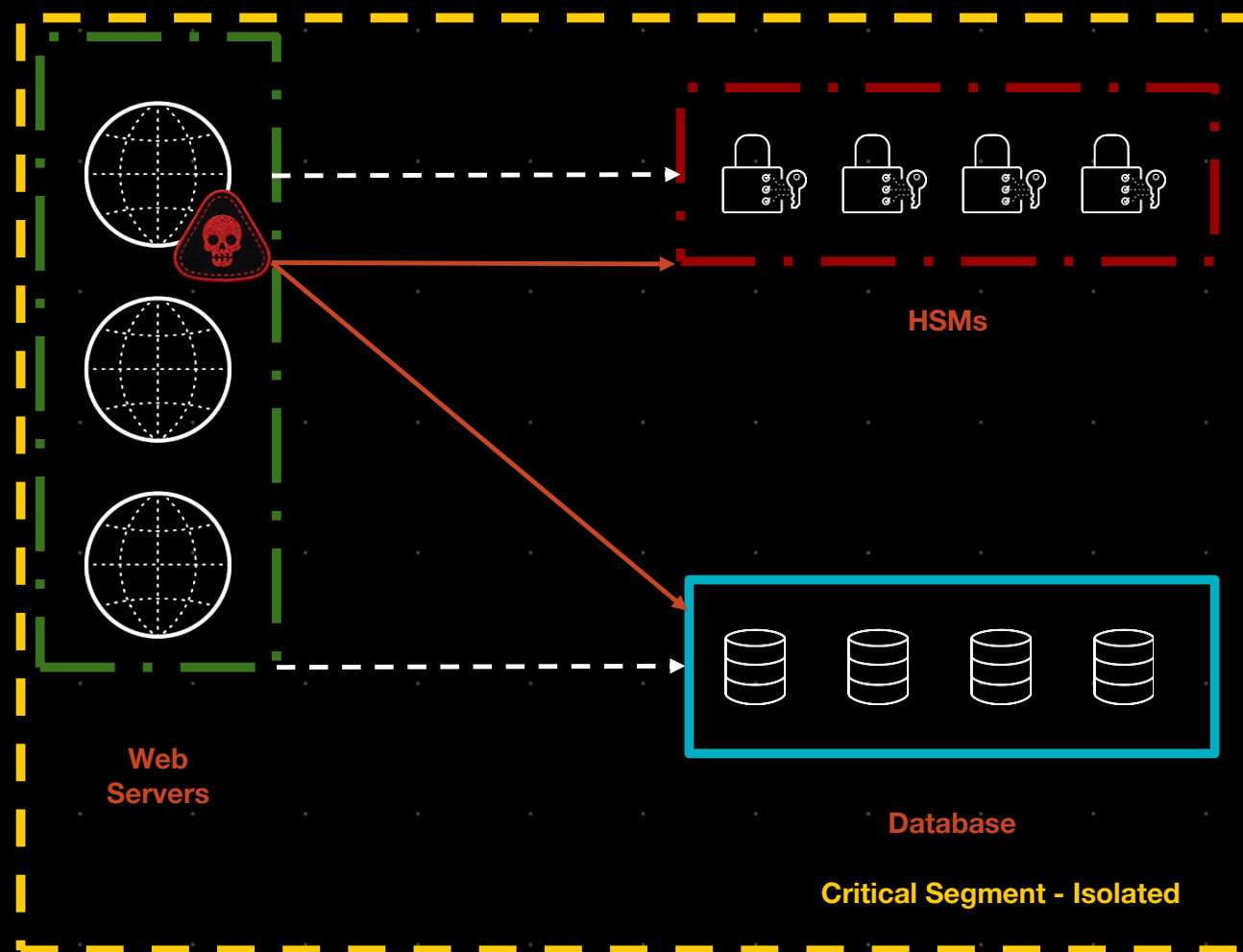
Application Architecture



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

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

Timestomping Detected

"Language Resource Folder"

Timestamping



Digital Forensics and Incident Response

P O S T E R

FALL 2012 - 22ND EDITION

<http://computer-forensics.sans.org>

Windows Time Rules

\$STDIINFO

File Rename	Local File Move	Volume File Move	File Copy	File Access	File Modify	File Creation	File Deletion
Modified - No Change	Modified - No Change	Modified - No Change	Modified - No Change	Modified - No Change	Modified - Change	Modified - Change	Modified - No Change
Access - No Change	Access - No Change	Access - Change	Access - Change	Access - Change No Change on Vista/Win7	Access - No Change	Access - Change	Access - No Change
Creation - No Change	Creation - No Change	Creation - No Change	Creation - Change	Creation - No Change	Creation - No Change	Creation - Change	Creation - No Change
Metadata - Changed	Metadata - Changed	Metadata - Changed	Metadata - Changed	Metadata - Changed	Metadata - Changed	Metadata - Changed	Metadata - No Change

\$FILENAME

File Rename	Local File Move	Volume File Move	File Copy	File Access	File Modify	File Creation	File Deletion
Modified - No Change	Modified - Change	Modified - Change	Modified - Change	Modified - No Change	Modified - No Change	Modified - Change	Modified - No Change
Access - No Change	Access - No Change	Access - Change	Access - Change	Access - No Change	Access - No Change	Access - Change	Access - No Change
Creation - No Change	Creation - No Change	Creation - Change	Creation - Change	Creation - No Change	Creation - No Change	Creation - Change	Creation - No Change
Metadata - No Change	Metadata - Changed	Metadata - Changed	Metadata - Changed	Metadata - No Change	Metadata - No Change	Metadata - Changed	Metadata - No Change

©2012 SANS – Created by Rob Lee and the SANS DFIR Faculty

Timestomping



SANS DFIR

DIGITAL FORENSICS & INCIDENT RESPONSE

Windows Forensic Analysis

POSTER

Master Windows Forensics – You Can't Protect the Unknown

digital-forensics.sans.org

\$25.00
DFIR_F0R5506_v4.3A_09-24

Poster created thanks to the support and contributions of the
SANS DFIR Faculty ©2024 SANS Institute. All Rights Reserved

[@SANSForensics](#) [dfir.to/DFIRCast](#) [dfir.to/LinkedIn](#)

Windows® Time Rules¹

\$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 = C:) (C:) (C:)	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

¹ Windows timestamp updates are notoriously dependent on the operating system version and a very specific combination of actions. These charts illustrate the differences between Windows 10 v1903 and 11 as heuristics indicating common actions, but always perform testing of specific actions on specific OS versions when working with critical evidence. Reference <https://www.kitware.com/blog/windows-11-t1-t2>

² Access times in Windows 11 should be considered approximate as they were sometimes noted to differ by up to a few seconds from the actual time of activity.

SANS DFIR Faculty ©2024 SANS Institute. All Rights Reserved



Timestomping



Windows® Time Rules ¹								
\$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 (for Change & System Volume > 100 GB)	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 – Time of Data Modification	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

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

¹ Windows timestamp updates are notoriously dependent on the operating system version and a very specific combination of actions. These charts illustrate the differences between Windows 10 v1903 and Windows 11 v22H2. Use these rules as heuristics indicating common actions, but always perform testing of specific actions on specific OS versions when working with critical evidence. Reference <https://www.khyrenz.com/blog/windows-11-time-rules/> for additional context.

² Access times in Windows 11 should be considered approximate as they were sometimes noted to differ by up to a few seconds from the actual time of activity.

Master Windows Forensics – You Can't Protect the Unknown
digital-forensics.sans.org

S25L44
DFIR_100000_v4.38_09-24
Power content thanks to the support and contributions of the
SANS DFIR Faculty Windows SANS Institute. All Rights Reserved

@SANSForensics dfir.to/DFIRCast dfir.to/LinkedIn

SANS DFIR Faculty ©2024 SANS Institute. All Rights Reserved

Timestomp



☒ Created > Modified → copied

SANS DFIR Faculty
©2024 SANS
Institute. All Rights
Reserved

\$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"*

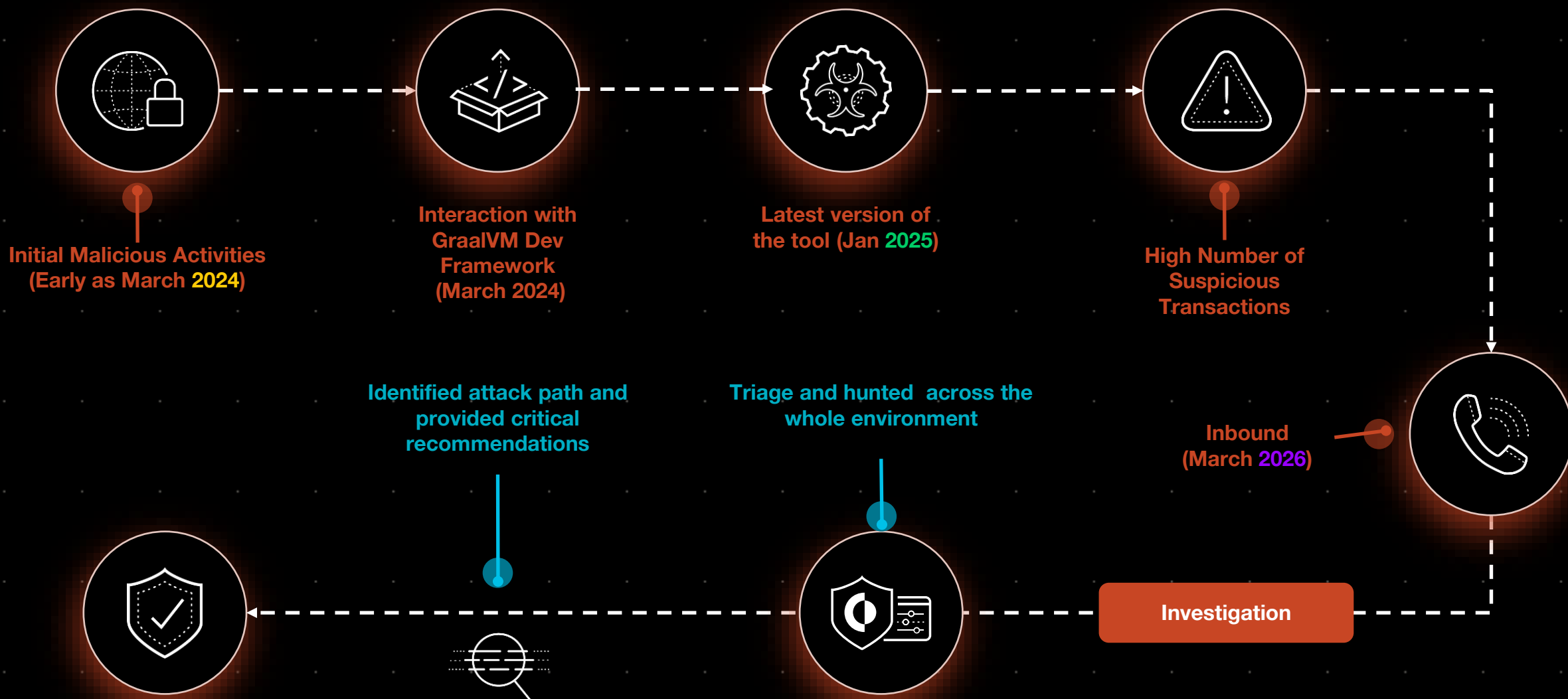
Malicious Modification

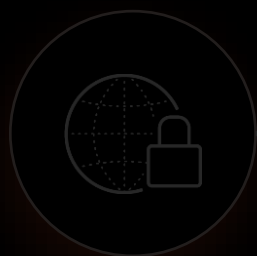
*"Facilitates the execution of interactive applications with additional **network tracking configurations**. If this service is stopped, users will be unable to launch applications with the additional administrative privileges they may require to perform preferred user tasks."*

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



Internal Control Bypass





Initial Malicious Activities
(Early as March 2024)



SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE

Windows Forensic Analysis POSTER

Master Windows Forensics – You Can't Protect the Unknown

digital-forensics.sans.org

SANS
SANS FOR500 v4.18.09-24
Poster created thanks to the support and contributions of the
SANS DFIR Faculty & SANS Institute. All rights reserved.

@SANSForensics dfirto/DFIRCast dfirto/LinkedIn

SANS Windows Artifact Analysis: Evidence of...

Application Execution

Shimcache

Description

The Windows Application Compatibility Database is used by Windows to identify possible application compatibility challenges with executable. It tracks the executable file path and binary¹ modified time.

Location

- XP: SYSTEM32\winlogon\ShimCache\ShimCache.dat

- Win7: SYSTEM32\winlogon\ShimCache\ShimCache.dat

Interpretation

Any executable present in the file system could be found in this key. Data can be particularly useful to identify the presence of malware on drives where other application execution data is missing (such as Windows servers).

- Full path of executable
- Windows 7+ contains up to 128 entries (64 entries in Windows 7)
- Most Windows 7+ no execution time is available
- Executables can be preemptively added to the database prior to execution. The existence of an executable in this key does not prove actual execution.

Task Bar Feature Usage

Description

Task Bar Feature Usage tracks how a user has interacted with the taskbar.

Location

Win 10: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\TaskBarFeatureUsage

Interpretation

- Only tracks GUI applications
- Does not include timestamps
- Application tracks data only for pinned applications, showing user knowledge of the application
- Data persists after an application is unpinned
- Application tracks a count of application focus, showing user interaction directed at the application
- Not tied to pinned applications

Amcache.hve

Description

Amcache tracks installed applications, programs executed (or present), drivers loaded, and more. What sets this artifact apart is it also tracks the SHA1 hash for executables and drivers. (Available in Windows 7)

Location

C:\Windows\System32\amcache.hve

Interpretation

- A complete registry hive, with multiple sub-keys
- Full path, file size, file modification time, compilation time, and publisher metadata
- SHA1 hash of executables and drivers
- Amcache should be used as an indication of executable and driver presence on the system, but not to prove actual execution

Jump Lists

Description

Windows 10 Timeline

Description

Windows 10 Timeline tracks activities that have been performed by users in a "timeline" database in SQLite format.

Location

C:\Users\%user%\AppData\Local\Microsoft\Windows\CurrentVersion\Timeline\Timeline.dat

Interpretation

- Full path of executed application
- Start time, end time, and duration
- Items opened within application
- URLs visited
- Databases still present even after feature deprecation in late Windows 10

BAM/DAM

Description

Windows Background/Foreground Activity Moderator (BAM/DAM) is maintained by the Windows power management sub-system. (Available in Windows 7)

Location

SYSTEM32\winlogon\ShimCache\ShimCache.dat

Interpretation

- Provides full path of file executed and last execution date/time
- Typically up to one week of data available
- "Safe" key used in Windows 10

System Resource Usage Monitor (SRUM)

Description

SRUM records 30 to 60 days of historical system performance including applications run, user accounts, network connections, and bytes sent/received per application per hour.

Location

Win7: C:\Windows\System32\SRUM\SRUM.dat

Interpretation

- SRUM.dat is an accessible Storage Engine database
- Three tables in SRUM.dat are particularly important:
 - SRUM.sys: System-wide data
 - SRUM.sys: System-wide data
 - SRUM.sys: System-wide data
- Network Connectivity Usage

Prefetch

Description

Prefetch increases performance of a system by pre-loading code pages of commonly used applications. It monitors all files and directories referenced for each application in process and maps them into a pif file. It provides evidence that an application was executed.

- Limited to 128 files on XP and Win7
- Up to 1024 files on Windows 8

Location

C:\Windows\Prefetch

Windows® Time Rules¹

\$Standard_Information Win10 v1903

File Creation	File Access	File Modification	File Rename	File Copy (new file)	Local File Move	Volume File Move (source via CLI)	Volume File Move (target 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 from Time of File Creation)	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 - No Change	Metadata - Inherited from Original	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 (source via CLI)	Volume File Move (target 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 Modification¹	Access - No Change²	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

¹ Windows filesystem updates are notoriously dependent on the operating system version and a very specific combination of actions. These charts illustrate the differences between Windows 10 v1903 and Windows 11 v22H2. Use these rules as heuristics indicating common actions, but always perform testing of specific actions on specific OS versions when working with critical evidence. Reference <https://www.sans.org/whitepapers/windows-11-time-rules/> for additional context.

² Access times in Windows 11 should be considered approximate as they were sometimes noted to differ by up to a few seconds from the actual time of activity.

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.

File and Folder Opening

Open/Save MRU

Description

In the simplest terms, this key tracks files that have been opened or saved within a Windows shell dialog box. This happens to be a big data set, including Microsoft Office applications, web browsers, chat clients, and a majority of commonly used applications.

Location

- XP: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Recent\OpenSaveMRU

- Win7: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Recent\OpenSaveMRU

Interpretation

- The "MRU" - This subkey tracks the most recent files of any extension input in an Open/Save dialog
- ??? (Three letter extension) - This subkey stores the info from the Open/Save dialog by specific extension

Recent Files

Description

Registry key tracking the last files and folders opened. Used to populate data in places like the "Recent" menu present in some Start menus.

Location

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Recent\Files

Interpretation

- RecentFiles - Rollup key tracking the overall order of the last 150 files or folders opened. MRU list tracks the temporal order in which each file/folder was opened.
- ??? - These subkeys store the last 20 files opened by the user of each extension type. MRU list tracks the temporal order in which each file/folder was opened. MRU list tracks the temporal order in which each file/folder was opened.
- Folder - This subkey stores the last 30 folders opened by the user. The most recently used (MRU) item in this key is associated with the last write time of the key, providing one timestamp of file opening for each extension type.

MS Word Reading Locations

Description

Beginning with Word 2013, the last known position of the user when a Word document is recorded.

Location

HKEY_CURRENT_USER\Software\Microsoft\Office\Word\ReadingLocations

Interpretation

- Another source tracking recent documents opened
- The last closed time is also tracked along with the last position within the file
- Together with the last opened date in the Office File MRU key, a last session duration can be determined

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: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Recent\LastVisitedMRU

Shortcut (.LNK) Files

Description

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

Location

- XP: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Recent\OpenSaveMRU

- Win7: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Recent\OpenSaveMRU

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

Interpretation

- Data/Time file of that name was first opened
- Creation Date of Shortcut (.LNK) File
- Data/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

Office Recent Files

Description

MS Office programs track their own recent files list, to make it easier for users to access previously opened files.

Location

- HKEY_CURRENT_USER\Software\Microsoft\Office\Word\Recent\Files

- Word 2003: Office 2003\Word\Recent\Files

- Word 2007: Office 2007\Word\Recent\Files

- Word 2010: Office 2010\Word\Recent\Files

- Word 2013: Office 2013\Word\Recent\Files

- Word 2016: Office 2016\Word\Recent\Files

- Word 2019: Office 2019\Word\Recent\Files

- Word 2021: Office 2021\Word\Recent\Files

- Word 2022: Office 2022\Word\Recent\Files

- Word 2023: Office 2023\Word\Recent\Files

- Word 2024: Office 2024\Word\Recent\Files

- Word 2025: Office 2025\Word\Recent\Files

- Word 2026: Office 2026\Word\Recent\Files

- Word 2027: Office 2027\Word\Recent\Files

- Word 2028: Office 2028\Word\Recent\Files

- Word 2029: Office 2029\Word\Recent\Files

- Word 2030: Office 2030\Word\Recent\Files

- Word 2031: Office 2031\Word\Recent\Files

- Word 2032: Office 2032\Word\Recent\Files

- Word 2033: Office 2033\Word\Recent\Files

- Word 2034: Office 2034\Word\Recent\Files

- Word 2035: Office 2035\Word\Recent\Files

- Word 2036: Office 2036\Word\Recent\Files

- Word 2037: Office 2037\Word\Recent\Files

- Word 2038: Office 2038\Word\Recent\Files

- Word 2039: Office 2039\Word\Recent\Files

- Word 2040: Office 2040\Word\Recent\Files

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

- XP: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Recent\OpenSaveMRU

- Win7: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Recent\OpenSaveMRU

Interpretation

- Each jump list file is named according to an application identifier (AppID). List of jump list IDs -> <https://officeapps.com/jump-list-ids/>
- 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
 - Icons kept in MRU order including a timestamp for each item

Office Trust Records

Description

Records trust relationships afforded to documents by a user when presented with a security warning. This is stored so the user is only required to grant permission the first time the document is opened.

Location

HKEY_CURRENT_USER\Software\Microsoft\Office\Word\Recent\Files

Interpretation

- Can identify documents opened by the user and user interaction in trusting the file
- Records the path, time the document was trusted, and which permissions were granted

Office OAlerts

Description

MS Office programs produce alerts for the user when they attempt actions such as closing a file without saving it first.

Location

HKEY_CURRENT_USER\Software\Microsoft\Office\Word\Recent\Files

Interpretation

- All Office applications use Event ID 300
- Events include the program name, and dialog message, showing some user activity within the application

Internet Explorer file:///

Description

Internet Explorer History databases have long held information on local and remote file access (via network shares), giving us an excellent means for determining files accessed on the system, per user information can be present even on Windows systems missing the Internet Explorer application.

Location

Internet Explorer: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\History\History

IE8 -> HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\History\History

IE9 -> HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\History\History

IE10 -> HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\History\History

IE11 -> HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\History\History

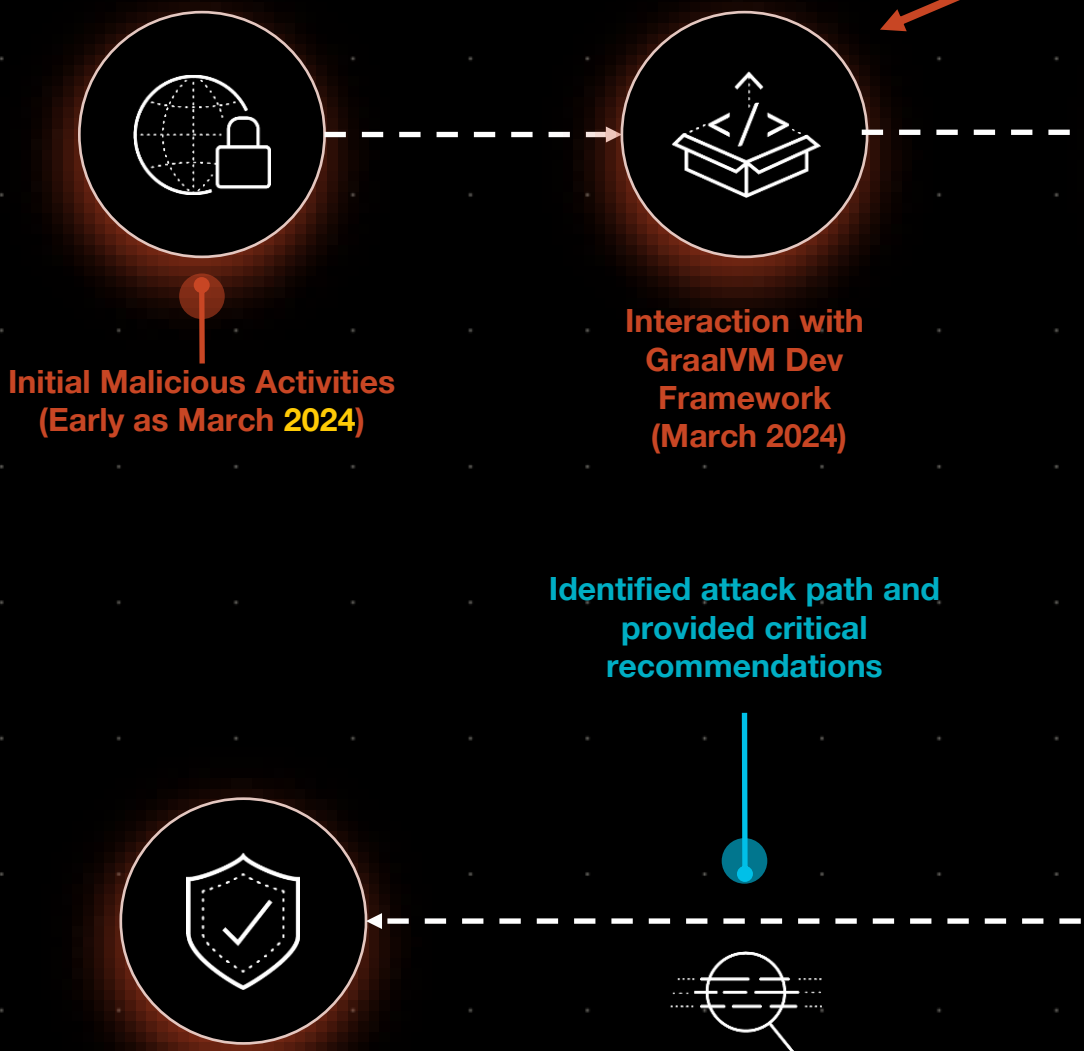
IE12 -> HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\History\History

IE13 -> HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\History\History

IE14 -> HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\History\History

IE15 -> HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\History\History

Internal Control Bypass



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

Investigation

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\LastVisitedPidIMRU`

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.

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

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

Windows Time Rules

\$STDINFO

File Rename	Local File Move	Volume File Move	File Copy	File Access	File Modify	File Creation	File Deletion
Modified – No Change	Modified – No Change	Modified – No Change	Modified – No Change	Modified – No Change	Modified – Change	Modified – Change	Modified – No Change
Access – No Change	Access – No Change	Access – Change	Access – Change	Access – Change No Change on Vista/Win7	Access – No Change	Access – Change	Access – No Change
Creation – No Change	Creation – No Change	Creation – No Change	Creation – Change	Creation – No Change	Creation – No Change	Creation – Change	Creation – No Change
Metadata – Changed	Metadata – Changed	Metadata – Changed	Metadata – Changed	Metadata – Changed	Metadata – Changed	Metadata – Changed	Metadata – No Change

Attackers Succeed Because of Three Critical Gaps



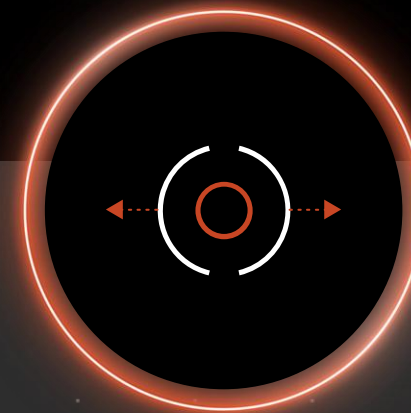
Visibility

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



Complexity

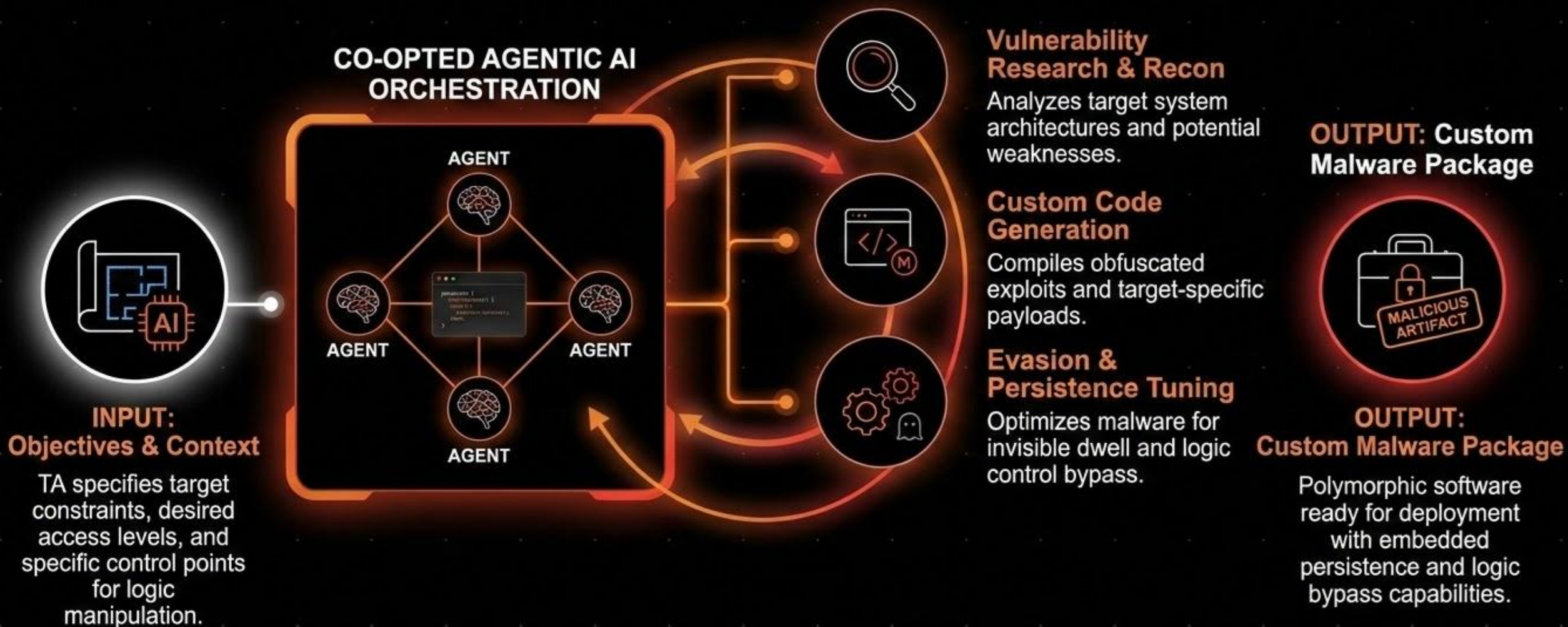
- Critical application ecosystems relied on unhardened, End-of-Life operating systems cluttered with diagnostic utilities, providing a pre-installed adversary toolkit.
- **Network segmentation** allowed connections from insecure zones.



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



New inbound



assignment_lateResource e 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 Intrusion

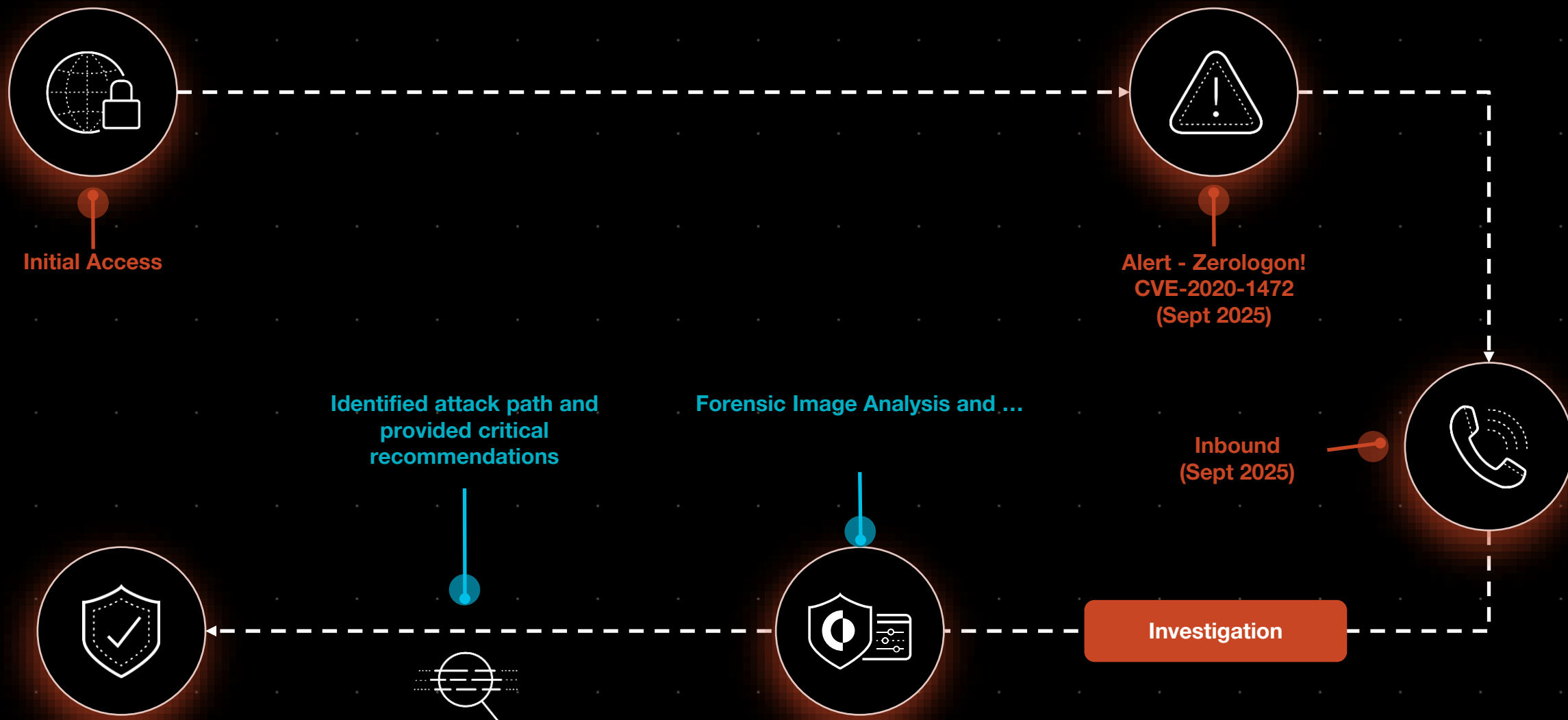
Tactics

- Spear phishing
- Discovery
- Persistence
- Data Exfiltration



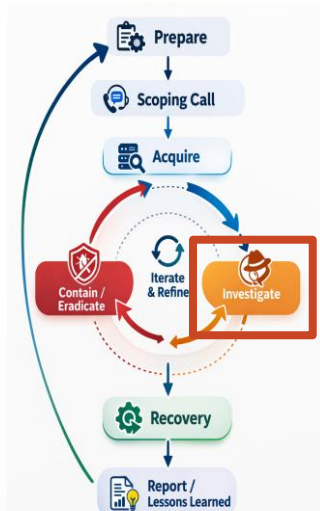
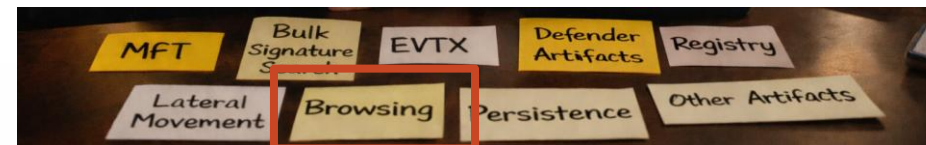
Toño Díaz

The Dream Job



Browsing artifacts

Let's check browsing. Tool Nirsoft



Onlyoffice space?

PDQ downloaded. Typed URL!
why?

Boeing?

Visit Time	URL	Title	Visit Type
8/25/2025 12:53:42 PM	https://mail.google.com/mail/u/0/?tab=rm&ogbl#inbox	Inbox (36) - gordon.cole	Link
8/25/2025 12:53:45 PM	https://mail.google.com/mail/u/0/?tab=rm&ogbl#inbox/QgrcJHmzwKfnWxLMzwBzmZGZNFjwpvwl	Gordon_Cole_NewCandi	Link
8/25/2025 12:54:08 PM	https://www.google.com/url?q=https://docspace-...onlyoffice.com/s/9WkGNgr9wWxFTP&source=gmail&context=menu	ONLYOFFICE	Link
8/25/2025 12:54:08 PM	https://docspace-...onlyoffice.com/s/9WkGNgr9wWxFTP	ONLYOFFICE	Link
8/25/2025 12:54:08 PM	https://docspace-...onlyoffice.com/s/9WkGNgr9wWxFTP	ONLYOFFICE	Link
8/25/2025 12:54:09 PM	https://docspace-...onlyoffice.com/doceditor?fileId=228754&share=YWgzSkorMWJIMHFicFpSd2VXQ25FRjR5aUfid2dn...	Boeing - ONLYOFFICE	Link
8/25/2025 12:55:04 PM	https://docspace-...onlyoffice.com/doceditor?fileId=228754&share=YWgzSkorMWJIMHFicFpSd2VXQ25FRjR5aUfid2dn...	boeing_volunteer_form.pdf - ONLYOFFICE	Link
8/25/2025 12:57:19 PM	https://docspace-...onlyoffice.com/doceditor?fileId=228754&share=YWgzSkorMWJIMHFicFpSd2VXQ25FRjR5aUfid2dn...	boeing_volunteer_form.pdf - ONLYOFFICE	Link
8/25/2025 12:59:04 PM	https://docspace-...onlyoffice.com/doceditor?fileId=228754&share=YWgzSkorMWJIMHFicFpSd2VXQ25FRjR5aUfid2dn...	boeing_volunteer_form.pdf - ONLYOFFICE	Link
8/25/2025 1:03:54 PM	http://pdq.com/	PDQ: Software Deployment & Inventory Management done...	Link
8/25/2025 1:03:54 PM	https://pdq.com/	PDQ: Software Deployment & Inventory Management done...	Link
8/25/2025 1:03:54 PM	https://www.pdq.com/	PDQ: Software Deployment & Inventory Management done...	Link
8/25/2025 1:07:17 PM	https://docspace-...onlyoffice.com/doceditor?fileId=2287544&share=YWgzSkorMWJIMHFicFpSd2VXQ25FRjR5aUfid2dn...	Senior Data Management Technical Lead.pdf - ONLYOFFICE	Link
8/25/2025 3:11:59 PM	https://mail.google.com/mail/u/0/?tab=rm&ogbl#inbox	Inbox (36) - gordon.cole@gmail.com - Gmail	Link
8/25/2025 3:12:04 PM	https://www.linkedin.com/hp/	LinkedIn	Auto Book...
8/25/2025 3:12:07 PM	https://www.linkedin.com/feed/	LinkedIn	Link
8/25/2025 3:12:28 PM	https://mail.google.com/mail/u/0/?tab=rm&ogbl#inbox/FMfcgZQbgcTxNsPTQsqcgIntZCbjwWpl	Technical Discussion - Gordon Cole- L1/L2	Link

Typed URL
Typed URL
Typed URL

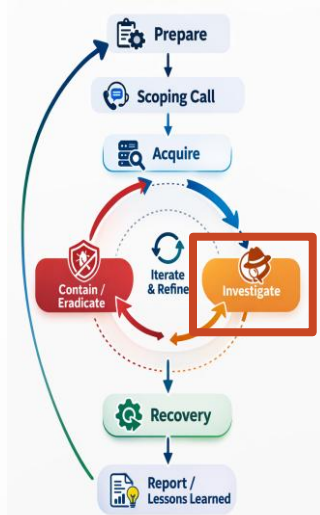
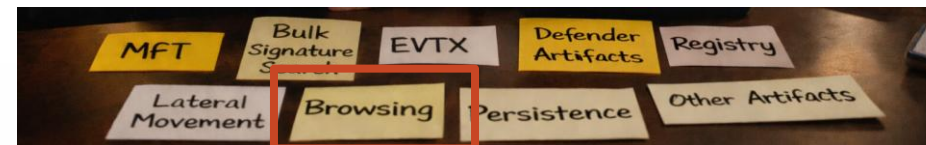
PDF of a role description,
personal Gmail, LinkedIn..

Tools:
BrowsingHistoryView
SQLite

Tips:
Consider containment actions

Browsing artifacts

Let's check browsing. Tool Nirsoft



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/	LinkedIn	18	https://www.linkedin.com/hp/	Link
12:27:59 PM	https://www.linkedin.com/messaging/thread/2-ZGE0MmQ17A+MDk2Y00N2NhLThYzEtMTdkYmFIMWQ0NGM1...	(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			CMWCwBn...
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/QgrcJHrnzWkfnWxLMzwBzmZGZNFJwprwfl	Gordon_Cole_NewCandidate - gordon.cole@gmail.com - Gmail			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/QgrcJHrnzWkfnWxLMzwBzmZGZNFJwprwfl	Gordon_Cole_NewCandidate - gordon.cole@gmail.com - Gmail			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/QgrcJHrnzWkfnWxLMzwBzmZGZNFJwprwfl	Gordon_Cole_NewCandidate - gordon.cole@gmail.com - Gmail			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#inbox	Link
12:32:15 PM	https://mail.google.com/mail/u/0/?tab=rm&ogbl#inbox	Inbox (36) - gordon.cole@gmail.com - Gmail	3	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/QgrcJHrnzWkfnWxLMzwBzmZGZNFJwprwfl	Sent Mail - gordon.cole@gmail.com - Gmail	13	https://mail.google.com/mail/u/0/?tab=rm&ogbl#sent/QgrcJHrnzWkfnWxLMzwBzmZGZNFJ...	Link
12:32:23 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
12:33:35 PM	https://www.linkedin.com/hp/	Gordon_Cole_NewCandidate - gordon.cole@gmail.com - Gmail	10	https://mail.google.com/mail/u/0/?tab=rm&ogbl#inbox	Link
12:33:37 PM	https://www.linkedin.com/feed/	LinkedIn	10	https://mail.google.com/mail/u/0/?tab=rm&ogbl#inbox/QgrcJHrnzWkfnWxLMzwBzmZGZNF...	Auto Book...
12:34:47 PM	https://mail.google.com/mail/?tab=rm&authuser=0&ogbl	(8) Feed LinkedIn	18	https://www.linkedin.com/hp/	Link
12:34:47 PM	https://mail.google.com/mail/u/0/?tab=rm&authuser=0&ogbl	Inbox (36) - gordon.cole@gmail.com - Gmail	165	https://www.linkedin.com/hp/	Link
12:34:47 PM	https://mail.google.com/mail/u/0/?tab=rm&ogbl	mail.google.com	165	https://mail.google.com/mail/?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	165	https://mail.google.com/mail/u/0/?tab=rm&authuser=0&ogbl	Link
12:35:42 PM	https://www.google.com/search?q=test+projects+in+boweing&rlz=1C1GCEA_en&oq=test+projects+in+bowe...	Inbox (36) - gordon.cole@gmail.com - Gmail	377	https://mail.google.com/mail/u/0/?tab=rm&ogbl	Link
12:35:50 PM	https://www.google.com/search?q=test+projects+in+boweing&sca_esv=e7c1514da748dd1c&rlz=1C1GCEA_en...	test projects in boweing - Google Search	1		Generated
12:39:44 PM	https://mail.google.com/mail/u/0/?tab=rm&ogbl#inbox/QgrcJHrnzWkfnWxLMzwBzmZGZNFJwprwfl	test projects in boweing - Google Search	1	https://www.google.com/search?q=test+projects+in+boweing&rlz=1C1GCEA_en&oq=test+...	Form Submi
12:40:17 PM	https://docspace-...onlyoffice.com/rooms/shared/1634892/filter?folder=1634892	Gordon_Cole_NewCandidate - gordon.cole@gmail.com - Gmail	10	https://mail.google.com/mail/u/0/?tab=rm&ogbl#inbox	Link
		ONLYOFFICE	2	https://www.google.com/url?q=https://docspace-...onlyoffice.com/rooms/shared/163...	Link

CV

LinkedIn chat

Gmail conversation:
GordonCole New
Candidate

First access to
OnlyOffice
storage

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

Tools:

BrowsingHistoryView

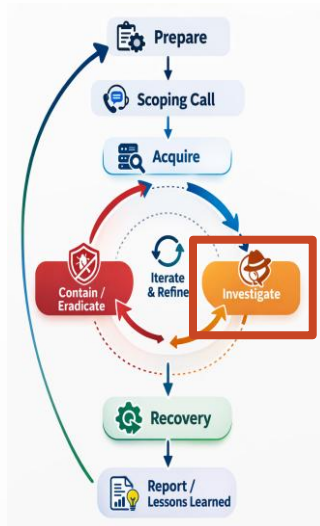
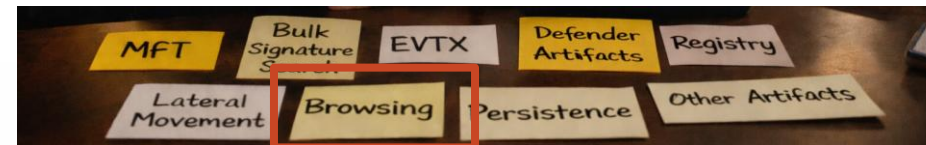
SQLite

Tips:

Consider containment action

Browsing artifacts

What is in this docspace?



Boeing - ONLYOFFICE

ONLYOFFICE DocSpace Boeing

Hiring Portal
09/11/2025 11:03 AM

System Administrator_Boeing (PRV roles)
08/25/2025 12:47 PM

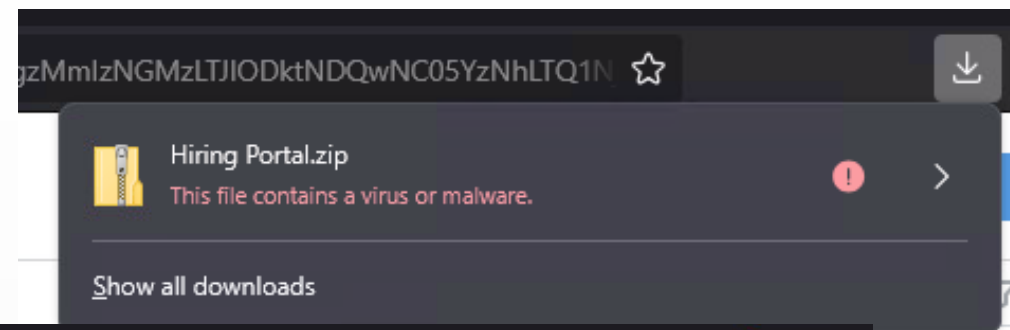
Recruitment Specialist
08/25/2025 12:47 PM

Supply Chain Manager
08/25/2025 12:47 PM

boeing_volunteer_form
08/25/2025 12:47 PM

Senior Data Management Technical I
08/25/2025 12:47 PM

EX Data Analyst
08/25/2025 12:47 PM



Boeing - ONLYOFFICE

System Administrator_Boeing (PRV roles).pdf

System Administrator

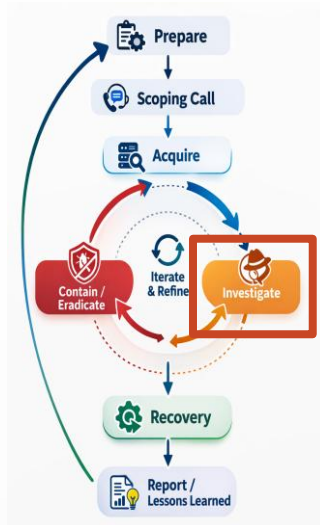
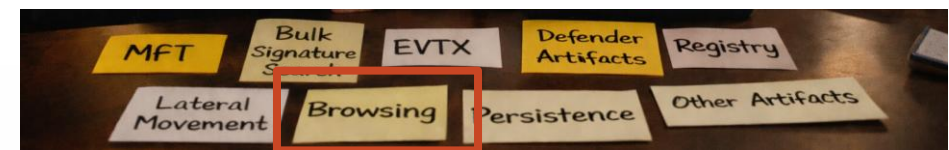
Job Description

At Boeing, we innovate and collaborate to make the world a better place. We're committed to fostering an environment for every teammate that's welcoming, respectful and inclusive, with great opportunity for professional growth. Find your future with us.



Browsing artifacts

We confirm that TA replicate actual Boeing recruiters



BOEING

YOUR RECRUITMENT CONTACTS AT BOEING GERMANY

	Human Resources Manager @outlook.com	Leads the HR team at Boeing Germany with a focus on talent development, strategic workforce planning, and leadership support. As Human Resources Manager, he plays a key role in shaping the recruitment vision, ensuring that hiring practices align with both global Boeing standards and local compliance requirements. His leadership drives efficiency, integrity, and innovation within the HR function.
	Talent Acquisition Specialist @outlook.com	is responsible for identifying, sourcing, and engaging top talent for Boeing globally. With a keen eye for potential and a strong grasp of the aerospace industry's evolving demands, he manages the full recruitment cycle—from job postings and candidate outreach to interviews and offers. Daniel's commitment to excellence ensures that each hire meets Boeing's high standards.
	Senior HR Specialist @outlook.com	brings extensive experience in human resources, specializing in strategic recruitment initiatives and cross-functional team coordination. As a Senior HR Specialist at Boeing Germany, he collaborates closely with business units to align talent acquisition strategies with company goals. His deep understanding of HR policies, labor laws, and organizational culture helps create a seamless and professional recruitment experience.
	Recruitment Coordinator @outlook.com	supports Boeing Germany's recruitment operations by managing scheduling, candidate communications, and administrative logistics throughout the hiring process. His organized and detail-oriented approach ensures that both candidates and internal stakeholders receive timely, accurate, and professional support. David plays a crucial behind-the-scenes role in delivering a positive candidate experience.
	Human Resources Specialist @outlook.com	plays a vital role in supporting Boeing Germany's recruitment operations with a strong focus on compliance, documentation, and candidate experience. With attention to detail and a passion for people, she ensures every step of the hiring process runs smoothly, from application tracking to onboarding support. Her proactive approach helps maintain HR operational excellence across teams.

Boeing is an equal opportunity employer. All applicants are considered equally.

HR Specialist at Boeing | Connecting People with the Right Opportunities | Passionate About Building Strong Teams

Alexandra | Informações de contato

+ de 500 conexões

[Enviar mensagem](#) [+ Seguir](#) [Mais](#)

Sobre

As a Human Resources Specialist at Boeing, I am passionate about connecting people with the right opportunities and helping organizations build high-performing, inclusive teams. With over 9 years of HR experience across global companies like Boeing and SAP, I bring a well-rounded understanding of talent acquisition, employee engagement, and strategic HR solutions...

Atividades

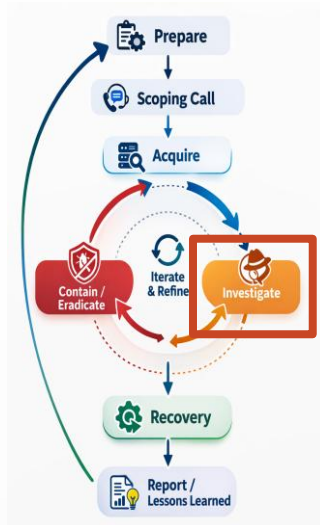
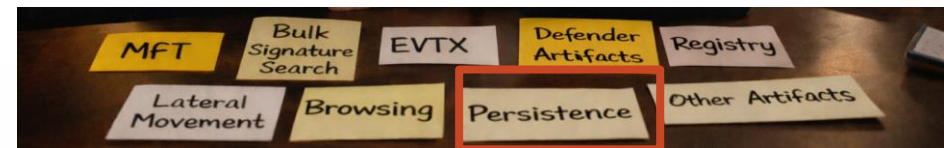
932 seguidores

Boeing
2689,332 seguidores
17 de 18

We're advancing maintenance training beyond traditional methods with Competency-Based Training and Assessment. ...mais

570 · 42 comentários · 31 compartilhamentos

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

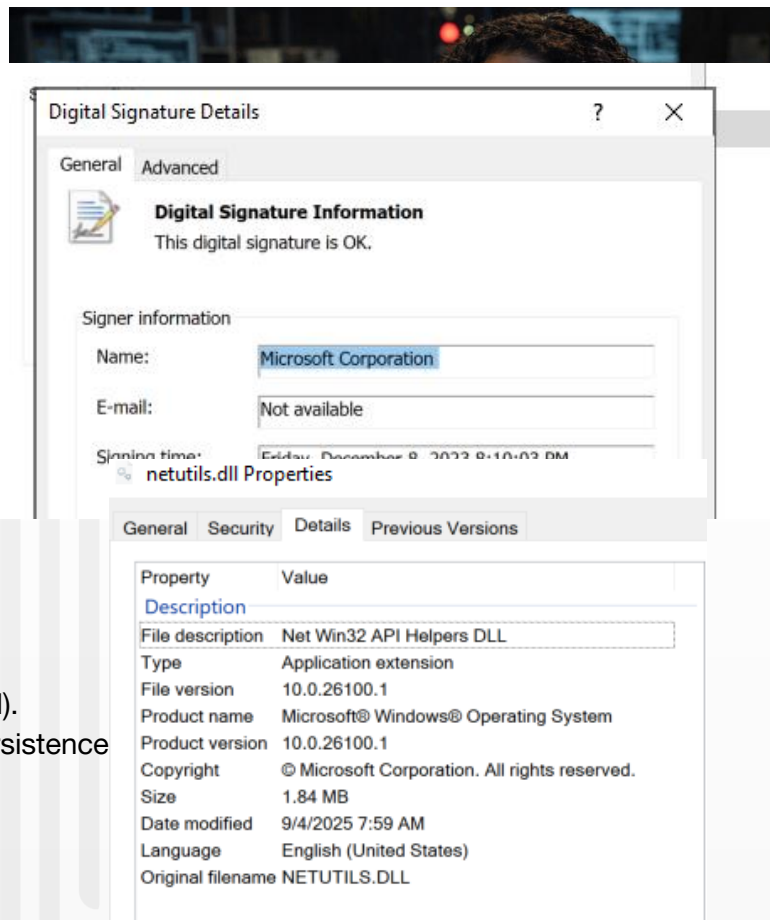
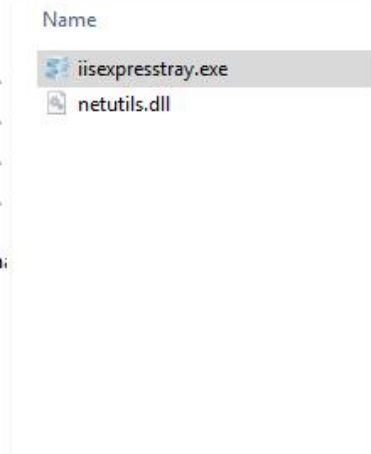
3. Search Order Hijacking (SOH)

- **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.

C:\Users\Public\NTUSER2.dat



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

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

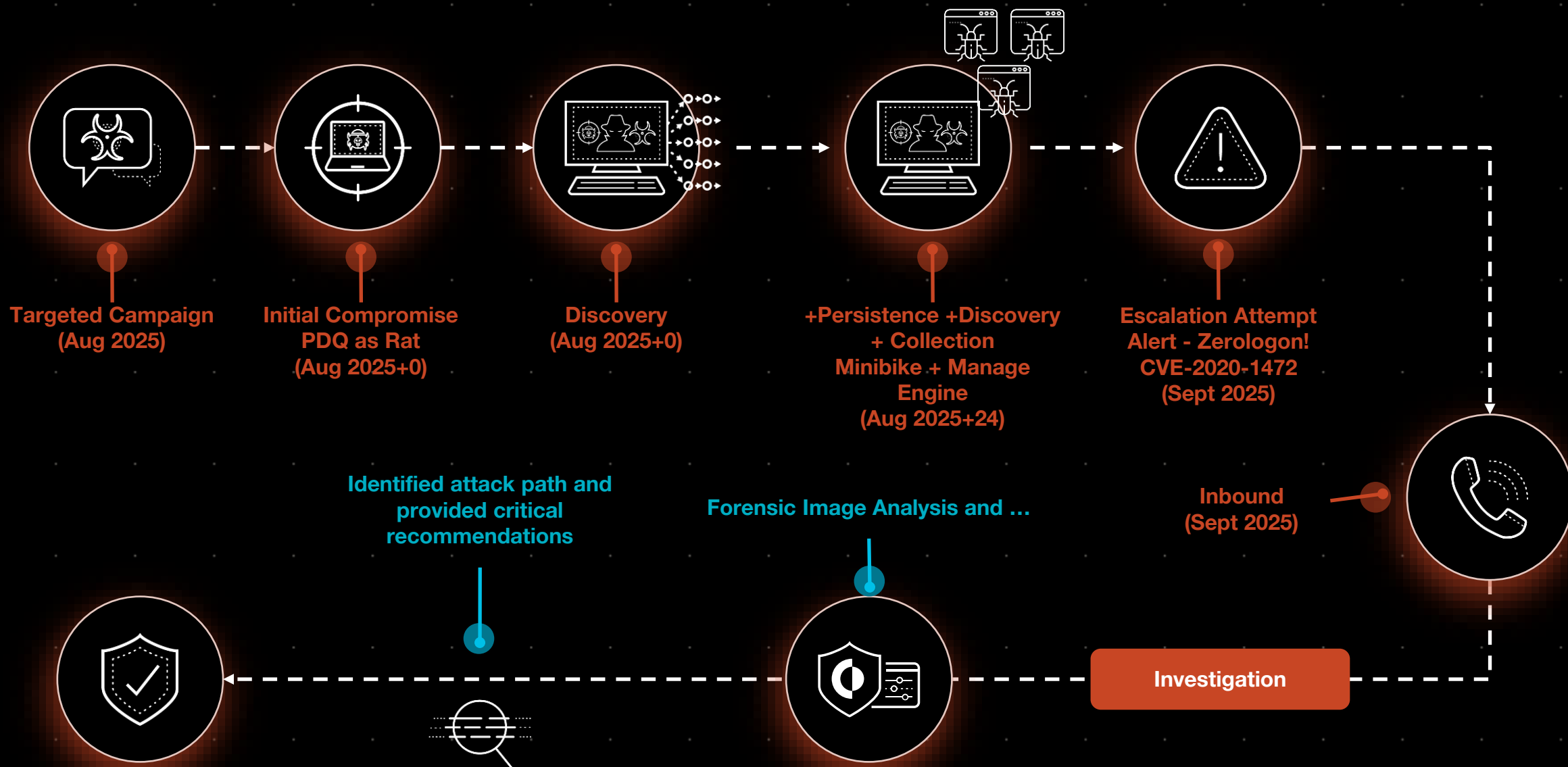
Aliases

APT35 G0059 ITG18 TA453 DIREFATE
GROUP 83 DAMSELFY NEWSCASTER PHOSPHORUS
GREYCATFISH MAGIC HOUND PHOSPHOROUS
SAFFRON ROSE IRIIDIUM 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



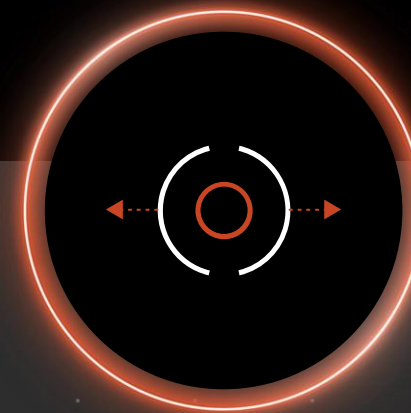
Visibility

- 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!

