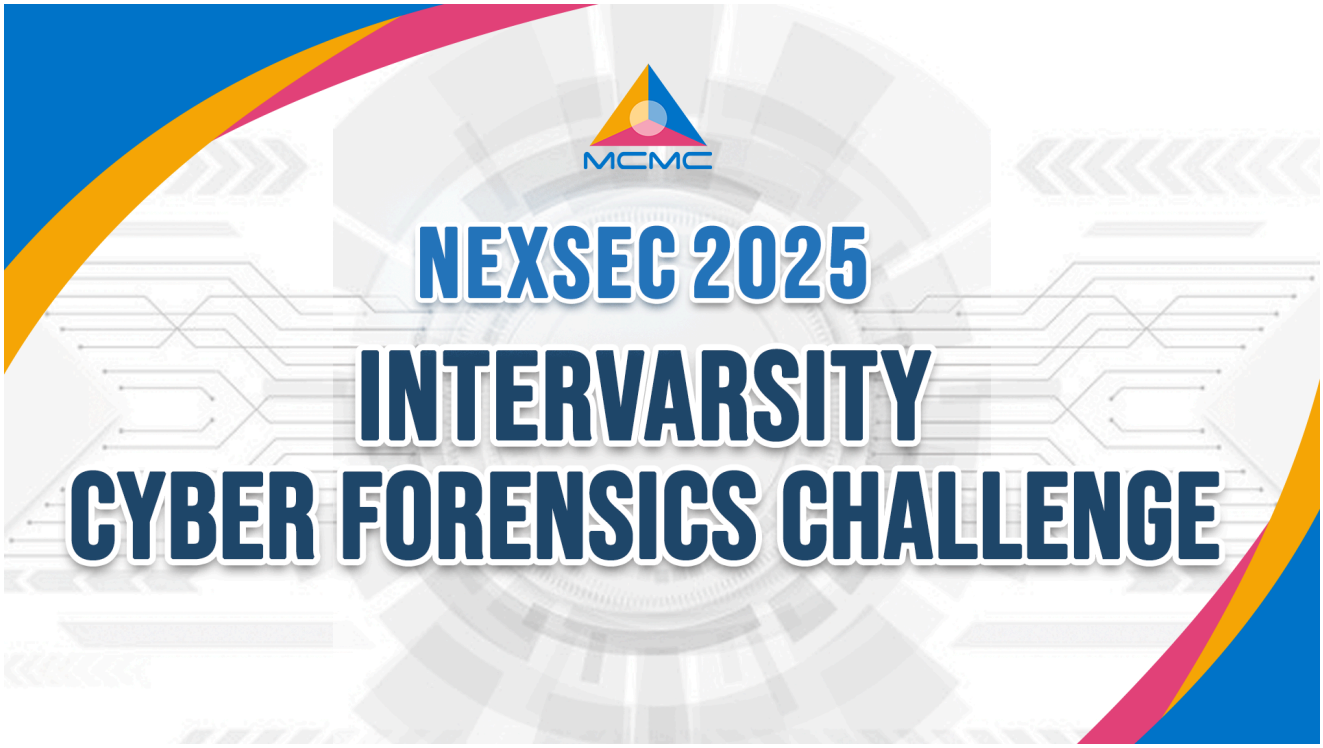


INTERVARSITY CYBER FORENSICS CHALLENGE FINAL ROUND REPORT

Dated: 18 December & 19 December 2025

AnakSoleh

ZAILAN | AZRAI | SYAHMI

TABLE OF CONTENT

1.0 Executive Summary

An external threat actor campaign identified as “Silent Rimba” compromised the corporate environment via a malicious Office document on workstation WS-01-CORP (user CORP\fakhri.zambri). The infection chain established a persistent command-and-control (C2) beacon, escalated privileges to SYSTEM, stole privileged credentials, and laterally moved to critical infrastructure, including the file server. The attack culminated in the execution of a PowerShell ransomware script (Bird.ps1) that encrypted the D: \ATM_Related project folder on FS-CORP, appending the .anon extension and dropping a ransom note (OHNO.txt).

Key Findings:

- Initial access originated from YEAR-END-FINANCIAL-REPORT-2025.docx opened on WS-01-CORP.

- PowerShell downloaded stage-1 content via a shortened URL (tinyurl.com/4kaz75ds) and retrieved payloads hosted on GitHub.

- A fake binary masquerading as C:\Users\Public\explorer.exe was reconstructed from a Base64 text file (xvzpox75.txt).

- Persistent C2 connectivity to 209.97.175.18:443 was observed; the same beacon was also identified on AD-CORP and FS-CORP.

- Credential theft leveraged Neurotransmitter.exe (renamed Mimikatz) to obtain CORP\itdadmin credentials for lateral movement.

- Anti-forensic actions included stopping SplunkForwarder at ~02:34 AM; additional log tampering was suspected.
- Final encryption occurred at ~03:01 AM targeting D:\ATM_Related on FS-CORP.

- Final encryption occurred at ~03:01 AM targeting D:\ATM_Related on FS-CORP.

2.0 Scope, Exhibits, and Method

2.1 Scope

This investigation focuses on determining (1) how the compromise began, (2) the malware and C2 infrastructure used, (3) privilege escalation and persistence mechanisms, (4) lateral movement steps and credential theft, (5) reconnaissance and anti-forensic activity, and (6) ransomware execution and impact on the file server.

2.2 Exhibits Provided

Exhibit ID	Description	Notes
E1	Workstation virtual image (.ova) — WS-01-CORP	Primary infection host (patient zero)
E2	File sharing / Windows Server virtual image (.ova) — FS-CORP	Ransomware impact host

2.3 Tools & Approach

- Windows built-in artifacts: Event Viewer, PowerShell logs/history, Prefetch, Scheduled Tasks, Services, Registry, and file system timestamps.

- Triaging & hashing: SHA-256 hashing, for example, sha256sum or certutil, string analysis, basic static checks.

- Network & C2 review: Windows Event logs or connections, where available, correlation with endpoint artifacts.

- Threat intel references (non-authoritative in competition context): VirusTotal checks for suspicious hashes/domains (optional).

3.0 Incident Flow

Time (Known/Estimated)	Host	User/Account	Activity (What happened)	Artifact / IOC (Evidence)	Notes / Confidence
Unknown (initial access)	WS-01-CORP	`CORP\fakhri.zambri`	User opened a malicious lure doc (patient zero)	`YEAR-END-FINANCIAL-REPORT-2025.docx` (SHA-256: `c3337074...a58b1f3`)	**Linked** to the whole chain; exact open time not recovered (**Estimated**)
Immediately after	WS-01-CORP	`CORP\fakhri.zambri`	Doc triggered PowerShell download via shortener	`tinyurl.com/4kaz75ds`	Strongly consistent with “doc → PS → download” behavior
After stage-1	WS-01-CORP	`CORP\fakhri.zambri`	Base64 staging file used to rebuild payload	`xvzpox75.txt` (SHA-256: `d37ed7b3...e5f4bf8`) in `%LocalAppData%\Temp\`	Supports the “reassembled implant” claim (**High confidence**)
After reconstruction	WS-01-CORP	Unknown (user/system context)	Fake `explorer.exe` dropped/executed as a beacon	`C:\Users\Public\explorer.exe` (SHA-256: `59cebd35...7474542`)	Masquerading as a legitimate explorer (**High confidence**)
After beacon execution	WS-01-CORP → Internet	—	Persistent C2 established	`209.97.175.18:443`	Key infrastructure IOC; beacon also found on AD/FS later

Unknown (post-compromise)	WS-01-CORP	Likely `CORP\fakhri.zambri` → SYSTEM	Privilege escalation via Event Viewer abuse	`EventViewerRCE.ps1` in `C:\Windows\Tasks\` + malicious RecentViews coercing `eventvwr.exe`	Technique described; needs exact artifact/timestamps to be "proven" (**Medium**)
Unknown (persistence)	WS-01-CORP	SYSTEM	Sticky Keys backdoor persistence	`sethc.exe` replaced	(**Medium**)
Unknown (cred theft)	WS-01-CORP	SYSTEM/Admin	Credential dumping to obtain admin creds	`Neurotransmitter.exe`	Creds for `CORP\itdadmin` harvested (**High**)
Unknown (lateral movement)	AD-CORP	`CORP\itdadmin`	Pivot to Domain Controller	Beacon presence + admin credential use	beacon also present on AD-CORP (**Medium–High**, but the mechanism of spread is not fully pinned)
Unknown (lateral movement)	FS-CORP	`CORP\itdadmin`	Pivot to File Server (target host)	Beacon presence + admin credential use	FS becomes an impacted host for ransomware
Unknown (internal recon)	FS-CORP	`CORP\itdadmin`	Recon/enumeration	`BrocaArea.ps1` (SHA-256: `15f6139c...6fa446c`)	Renamed adPEAS; aligns with attacker "brain" naming theme
Unknown (manual discovery)	FS-CORP	`CORP\itdadmin`	Disk enumeration	`wmic logicaldisk`	Confirms target discovery steps
Unknown (target confirmed)	FS-CORP	`CORP\itdadmin`	Found high-value folder	`D:\ATM_Related`	Ransomware target directory

Unknown (post-exploitation tooling)	FS-CORP / AD-CORP	`CORP\itdadmin`	PtH-style capability staged	`Cerebrum.ps1` (SHA-256: `4fd1191c...92238fe`)	Renamed `Invoke-TheHash` module (**Medium**)
Unknown (toolkit staged)	WS-01-CORP / FS-CORP	—	Additional toolkit downloaded	`Salad.zip` from NetExec release `.../v1xe.zip`	Hash not captured yet (**Medium**)
02:34 AM (Known)	FS-CORP (likely)	SYSTEM/Admin	Defense evasion: stop logging agent	`sc stop SplunkForwarder`	**Strong anchor time** in your narrative
After 02:34 AM	FS-CORP (likely)	—	Anti-forensics: prevent re-index/resend	Splunk fishbucket cleared	Good story fit; better if you show path/artifact proving fishbucket wipe (**Medium**)
After 02:34 AM	FS-CORP (likely)	—	Diversion/noise	235+ random DNS queries (Hubspot/Reddit/etc.)	Helps explain “hide GitHub traffic in noise” (**Medium**)
03:01 AM (Known)	FS-CORP	`CORP\itdadmin`	Ransomware executed; encrypts the target folder	`Bird.ps1` (repo `TomatoTerbang/Beruang`) → `.anon` extension on `D:\ATM_Related`	**Strong anchor time**; core impact event
After 03:01 AM	FS-CORP	`CORP\itdadmin`	Ransom note dropped	`OHNO.txt` in `itdadmin` Documents	Confirms ransomware completion
Unknown (supporting lead)	FS-CORP	`CORP\itdadmin`	PS history references Bird.ps1	`ConsoleHost_history.txt` includes `bird.ps1` reference	Low-confidence

4.0 Findings
4.1 Initial Access & Patient Zero

Host: WS-01-CORP

User: CORP\fakhri.zambri

V**ector:** Malicious document YEAR-END-FINANCIAL-REPORT-2025.docx.

Observed Behavior: Opening the document triggered PowerShell execution that used a shortened URL (tinyurl.com/4kaz75ds) to fetch stage-1 content from GitHub.

Hypothesis (high-confidence):

The malicious document YEAR-END-FINANCIAL-REPORT-2025.docx is suspected to leverage a **CVE-2017-0199-style** remote template/OLE exploit based on the observed behavior of automatic outbound retrieval and PowerShell execution.

4.2 Payload Deployment & C2 Beacon

A fake binary masquerading as **C:\Users\Public\explorer.exe** was identified as the C2 beacon. The file was reportedly reassembled on the host from a Base64 text file named **xvzpox75.txt** located under the user's temp directory. The beacon maintained a persistent connection to **209.97.175.18:443.** The same beacon artifact was later observed on **AD-CORP** and **FS-CORP**, indicating persistence and spread.

4.3 Credential Theft & Lateral Movement

Credential dumping was performed using Neurotransmitter.exe, identified as a renamed version of Mimikatz. The attacker harvested credentials for CORP\itdadmin and used them to pivot from the workstation to additional systems, including the Domain Controller (AD-CORP) and the file server (FS-CORP).

4.4 Internal Reconnaissance & Target Discovery

For reconnaissance, the attacker used **BrocaArea.ps1** (a renamed version of adPEAS). Manual enumeration on the file server included identifying logical disks via **wmic logicaldisk**, locating the **D:\ATM_Related** project folder, and searching the **itdadmin** Documents directory for sensitive keys.

4.5 Anti-Forensics & Defense Evasion

The attacker attempted to blind monitor Splunk Forwarder using **sc stop SplunkForwarder** around **02:34 AM.** They also cleared the Splunk fishbucket to prevent previously indexed logs from being re-sent. As a diversion, they generated 235+ DNS queries to benign/random domains, for example, Hubspot, Reddit, to hide suspicious GitHub traffic in background noise.

4.7 Impact: 'Bird' Ransomware Execution

The final stage involved downloading **Bird.ps1** (from TomatoTerbang/Beruang GitHub repository) and executing it on FS-CORP. At approximately **03:01 AM**, the script encrypted files within **D:\ATM_Related** and appended the **.anon** extension. A ransom note titled **OHNO.txt** was placed in the **itdadmin** Documents folder.

5.0 Indicators of Compromise (IOCs)

5.1 Network IOCs

Type	Indicator	Value	Notes	Confidence
C2	IP:Port	209.97.175.18:443	Outbound C2 connectivity observed.	High
Delivery	Shortened URL	tinyurl.com/4kaz75ds	Used in the initial stage of retrieval.	High
Hosting	GitHub Account	TomatoTerbang	Tool-hosting account (BrainRil/Beruang).	Med-High
C2 (possible)	IP:Port	209.97.175.18:7219	Reported suspicious port; validate in artifacts.	To validate

5.2 File and Hash IOCs

Type	Indicator	SHA-256 / Value	Observed / Notes
File	explorer.exe	59cebd35102c4164a6ca164b6bda97afe56984cb35c3f572a66343f774474542	C:\Users\Public\explorer.exe (beacon)
File	YEAR-END-FINANCIAL-REPORT-2025.docx	c3337074a81cb59e7db78087ded4b35dd89efddebd2bea8a8379748e5a58b1f3	Initial lure
File	xvzpox75.txt	d37ed7b32c4585e0586b22c83195b98001bca80a4f731a1acd375b4fce5f4bf8	Base64 staging (%LocalAppData%\Temp)
File	Neurotransmitter.exe	92804faaab2175dc501d73e814663058c78c0a042675a8937266357bcfb96c50	Renamed Mimikatz
Script	EventViewerRCE.ps1	N/A	C:\Windows\Tasks\
Script	Bird.ps1	N/A	Referenced in PowerShell history; not recovered
Ransom Note	OHNO.txt	N/A	Ransom note

6.0 Notable Artifacts, Gaps, and Validation Notes

6.1 PowerShell History Artifact

On FS-CORP, PowerShell console history was identified at:

C:\Users\itdadmin\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt

This file referenced **bird.ps1**. At the time of reporting, **bird.ps1** was not successfully recovered from disk; this indicates either deletion, execution from a transient location, or execution via downloaded content without leaving a stable script on disk.

The PowerShell history was also taken from **“Microsoft-Windows-PowerShell%4Operational.evtx”** from both FS and workstation, reassembled by a Python script. We can see that most of the PowerShell commands are malicious, probably from the long string of base64, along with an XOR key

6.2 Hypotheses and Unconfirmed Items

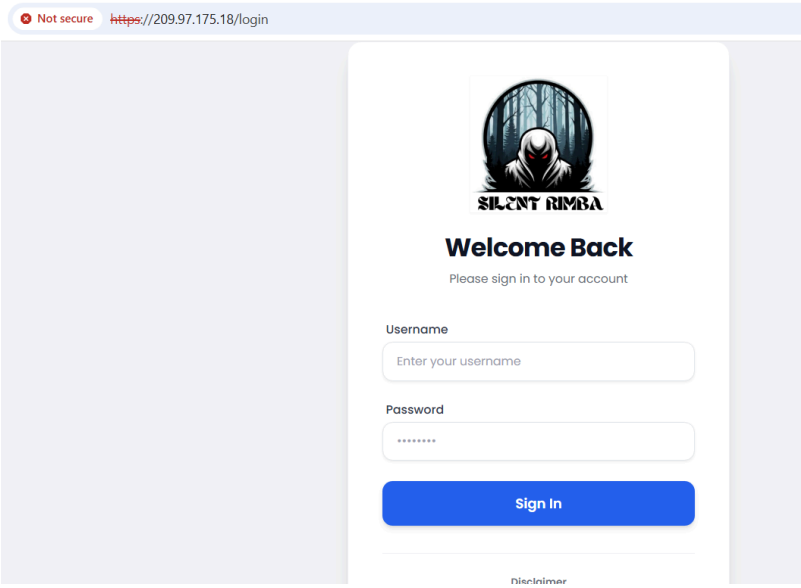
- CVE-2017-0199 exploitation: plausible based on observed Office document-triggered remote download; needs document-level confirmation.
- bird.ps1 may have also dropped/assisted the explorer.exe beacon (not confirmed).
- The exact sequence of propagation of the beacon to AD-CORP and FS-CORP requires host-by-host artifact correlation (scheduled tasks, services, Run keys, or dropped binaries).

6.3 Threat Actor (Silent Rimba)

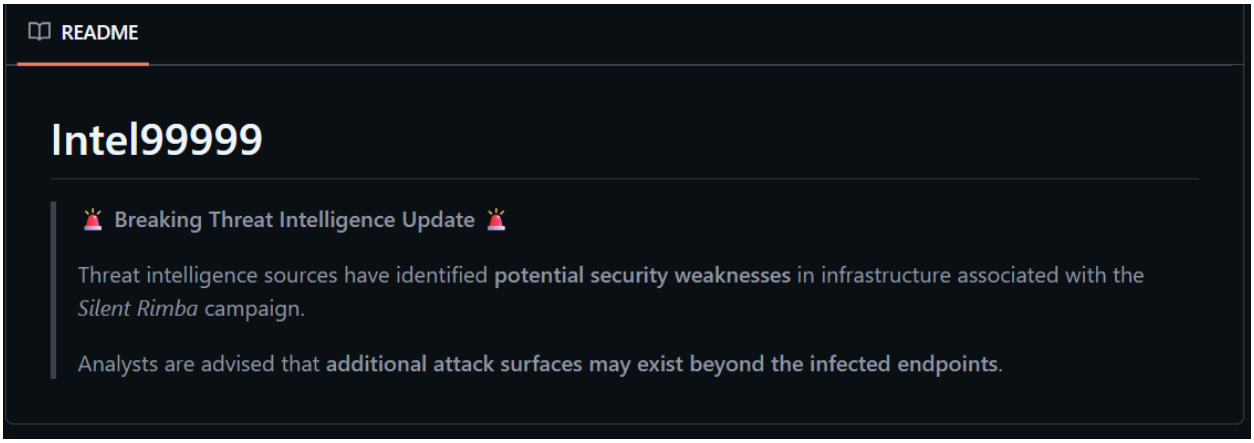
Multiple attacker tools were named using medical/brain-related terms, for example, Neurotransmitter, BrocaArea, Cerebrum, and Brainstem, which are renamed versions of existing Pentesting tools. This aligns with the adversary repository structure observed (TomatoTerbang/BrainRil).

Further investigation leads to their C2 IP address: **209.97.175.18**

Nmap reveals that the IP hosts a web service on port 443.



Threat Intel issued an update about the existence of a potential security weakness in the threat actor's infrastructure.



7.0 Recommendations (Competition-Oriented)

- Containment: Isolate affected hosts (WS-01-CORP, FS-CORP, AD-CORP); block outbound to 209.97.175.18:443 and related IOCs.

- Credential Reset: Reset passwords for compromised accounts (CORP\fakhri.zambri, CORP\itdadmin).

- Eradication: Remove persistence (Sticky Keys), tasks/services, and dropped tools; validate no rogue explorer.exe remains.

- Recovery: Restore D:\ATM_Related from known-good backups and validate integrity.

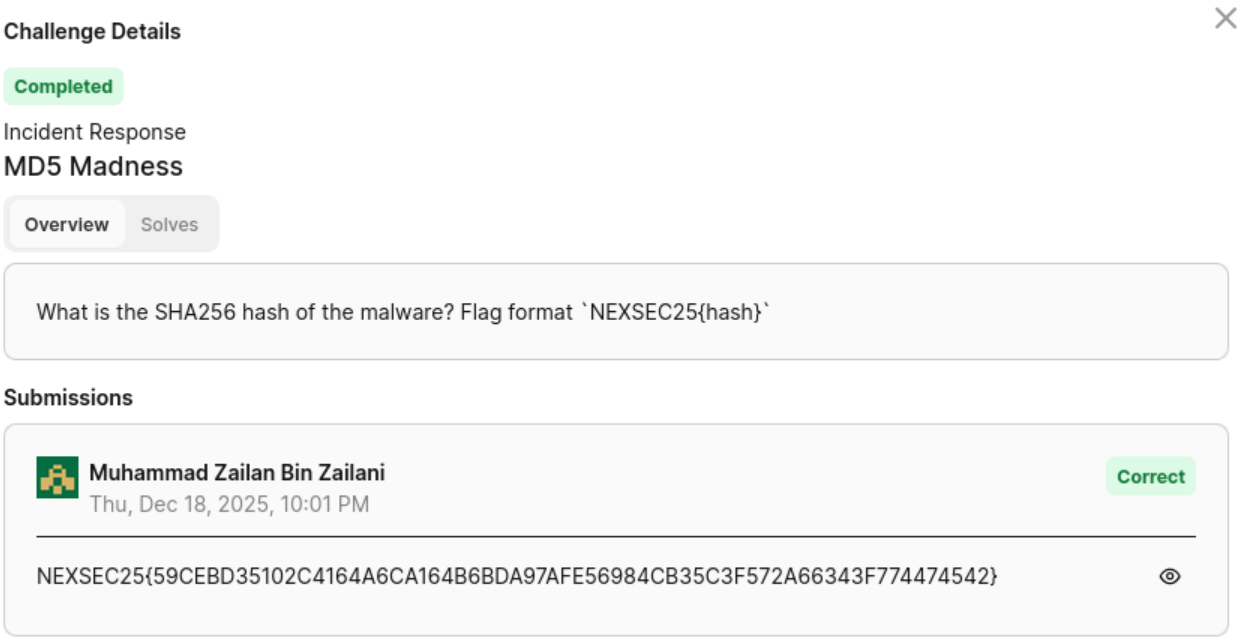
- Visibility: Re-enable/repair Splunk Forwarder and harden it from tampering.

8.0 APPENDIX

Appendix A: Competition Answer Sheet

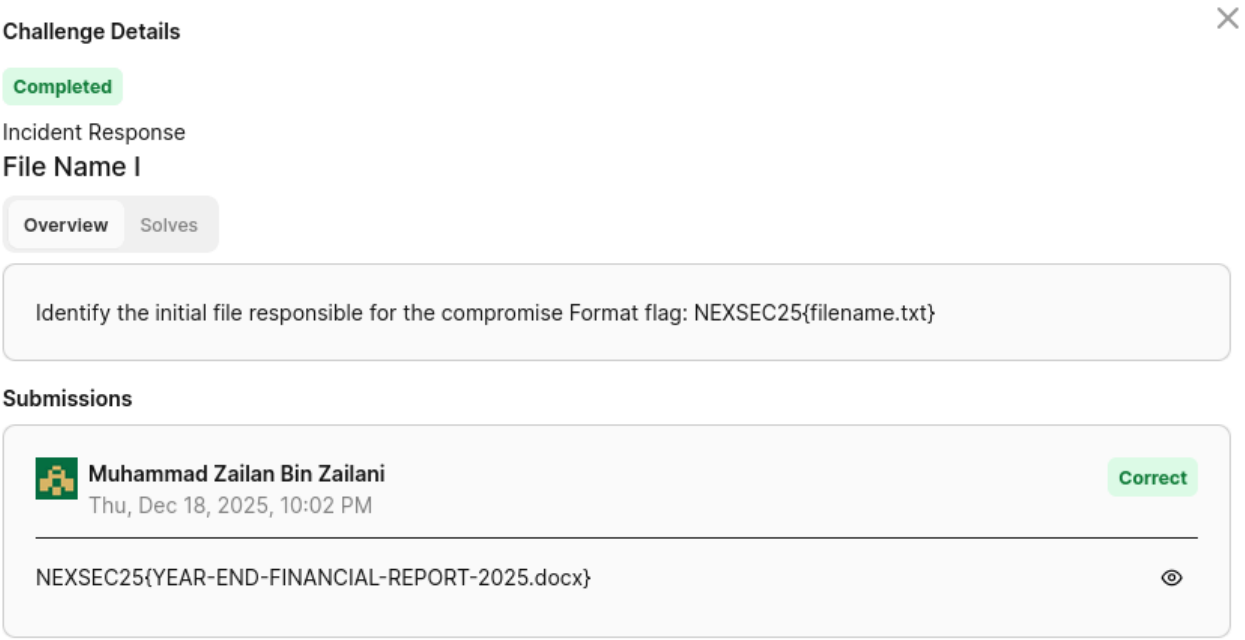
Challenge	Question	Answer / Flag
MD5 Madness	SHA256 hash of the malware	NEXSEC25{59CEBD35102C4164A6CA164B6BDA97AFE56984CB35C3F572A66343F774474542}
Acteur de la menace	Threat Actor name	NEXSEC25{silent rimba}
Adversary Tool Hosting Activity	Username hosting additional tools	NEXSEC25{TomatoTerbang}
Victime d'un logiciel de rançon	Patient zero (user)	NEXSEC25{fakhri.zambri}
Internal Propagation Account	Account abused for lateral movement	NEXSEC25{itdadmin}
Command and Control	C2 IP address	NEXSEC25{209.97.175.18}
Lateral Movement (MITRE)	MITRE ATT&CK ID	NEXSEC25{T1047}
File Recovery	SHA256 of recovered PDF	nexsec25{b1134f54cff738629f94bc979b6c2ad6f15d8d19fcad8fe1007508ce47086424}

Appendix B: Evidence Screenshots



This answer we got from sha256 hash explorer.exe

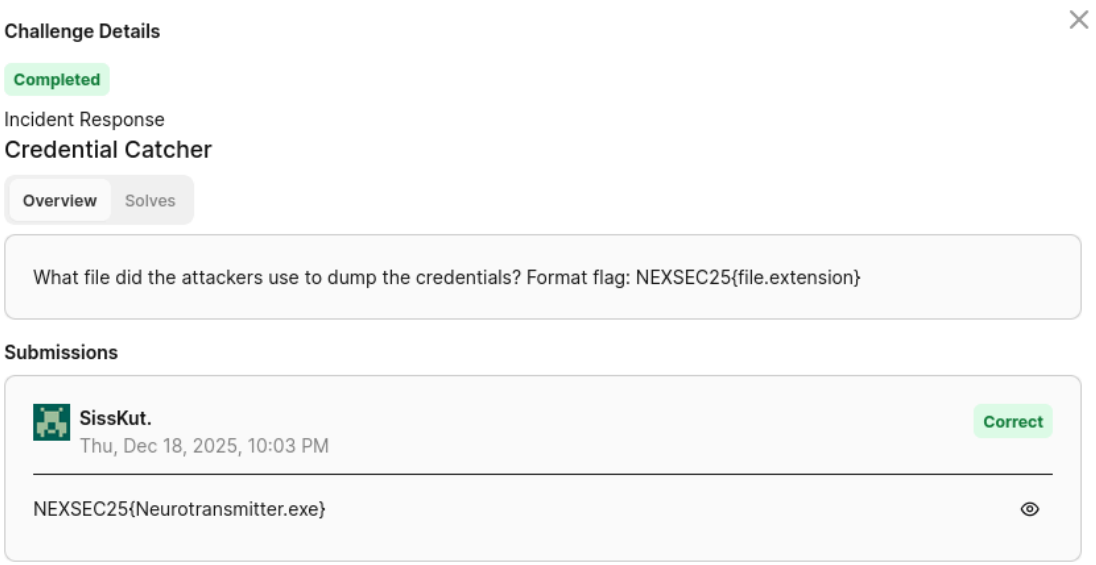
Host	Image Path	SHA256 Hash
WS-01-CORP	C:\Users\Public\explorer.exe	59CEBD35102C4164A6CA164B6BDA97AFE56984CB35C3F572A66343F774474542
AD-CORP	C:\Users\Public\explorer.exe	59CEBD35102C4164A6CA164B6BDA97AFE56984CB35C3F572A66343F774474542



Evidence Identification

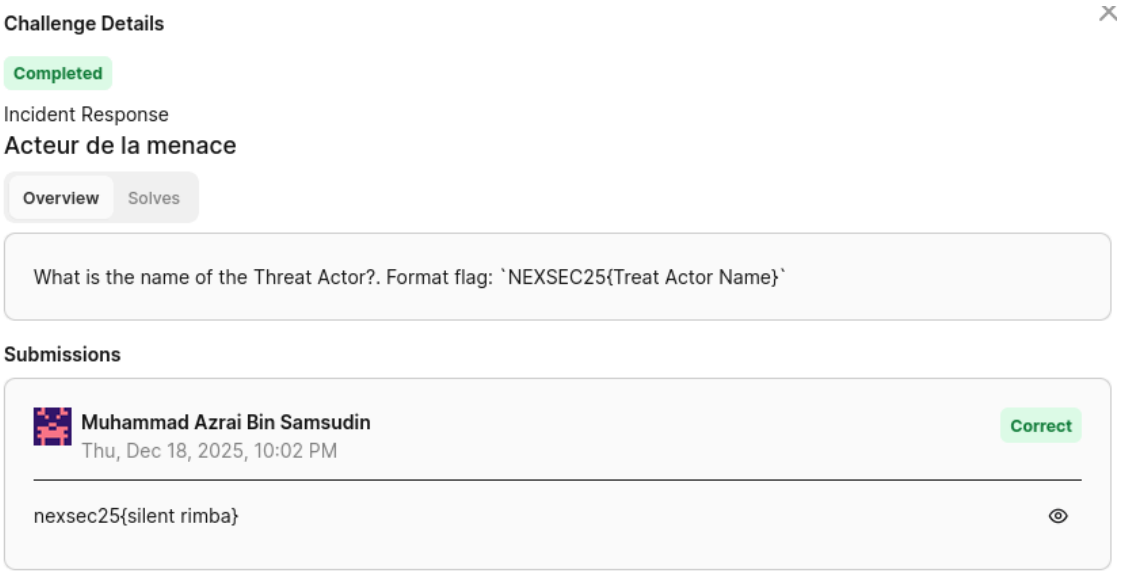
The infection sequence began at **01:38 AM** on **December 18, 2025**.

- The Log Evidence: A DNS query for tinyurl.com and raw.githubusercontent.com was initiated by the process WINWORD.EXE
  .
- The File Name: The document that triggered this macro-based PowerShell execution was identified in the Recent Docs registry keys and file system logs as the malicious vector.



Evidence Identification

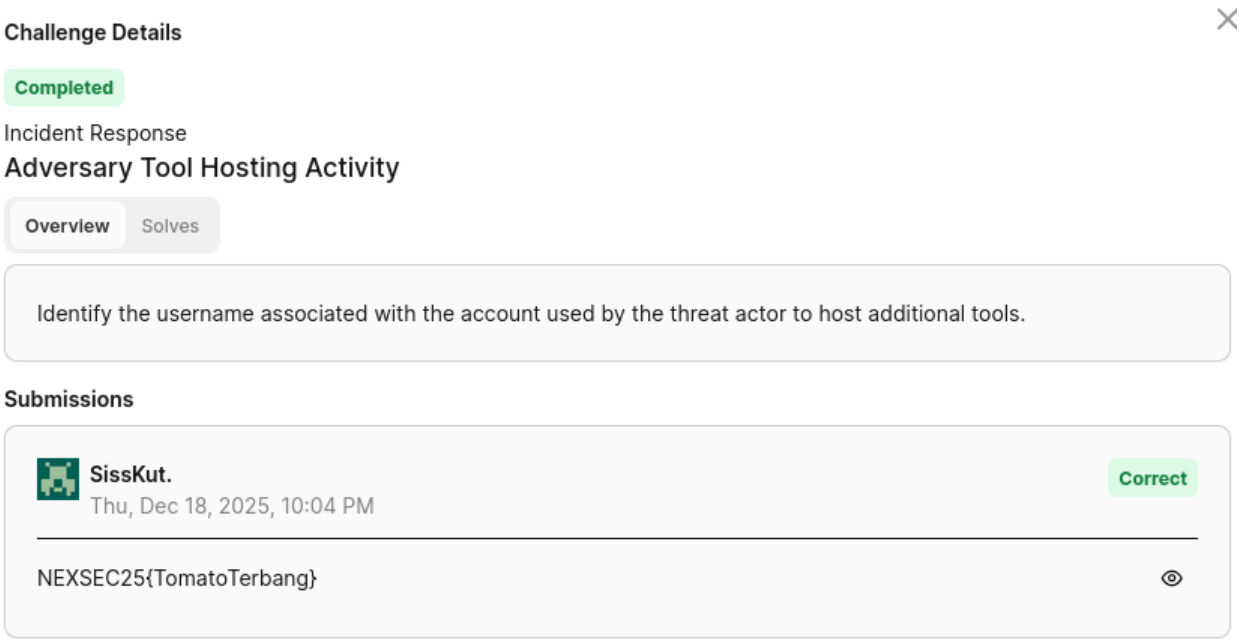
During analysis, we identified a suspicious executable named **Neurotransmitter.exe**. This file is a **renamed Mimikatz tool**, which is commonly used to dump credentials from system memory. Based on our findings, the attacker executed **Neurotransmitter.exe** to harvest credentials, including **CORP\itdadmin**, which were later used for lateral movement. Therefore, the credential dumping file is **Neurotransmitter.exe**.



Evidence in the Ransom Note

The header of the note you found explicitly identifies the group:

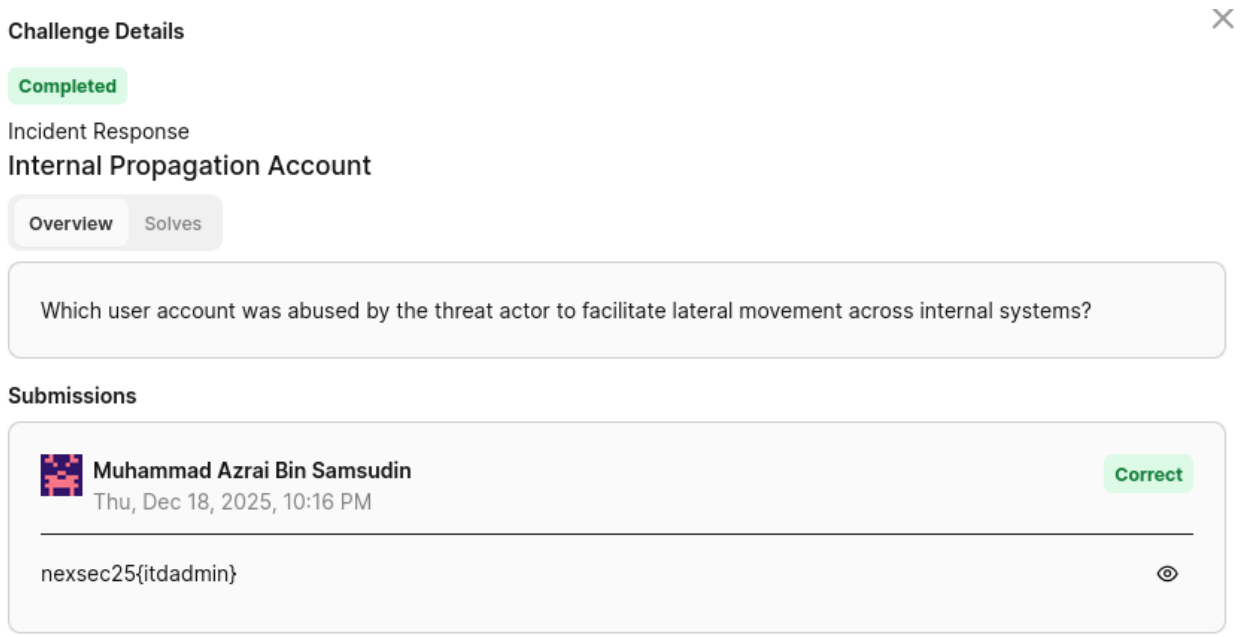
> **~~~Silent Rimba. The wealthiest tree in forest~~~**



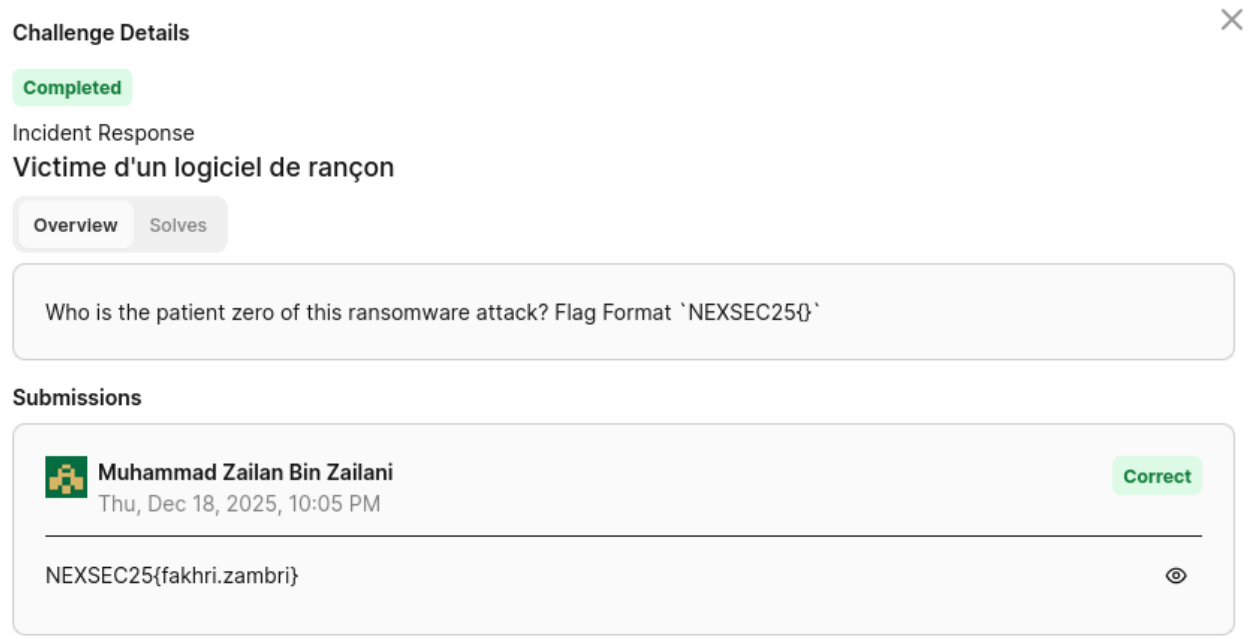
The name was identified through two primary forensic artifacts:

1. GitHub URL Analysis: The malicious scripts (Cerebrum, Neurotransmitter, BrocaArea, and Bird.ps1) were all hosted at github.com/**TomatoTerbang**/

2. DNS Query Logs: Your Splunk search specifically looked for and found multiple queries targeting the string "TomatoTerbang" during the payload download phase.

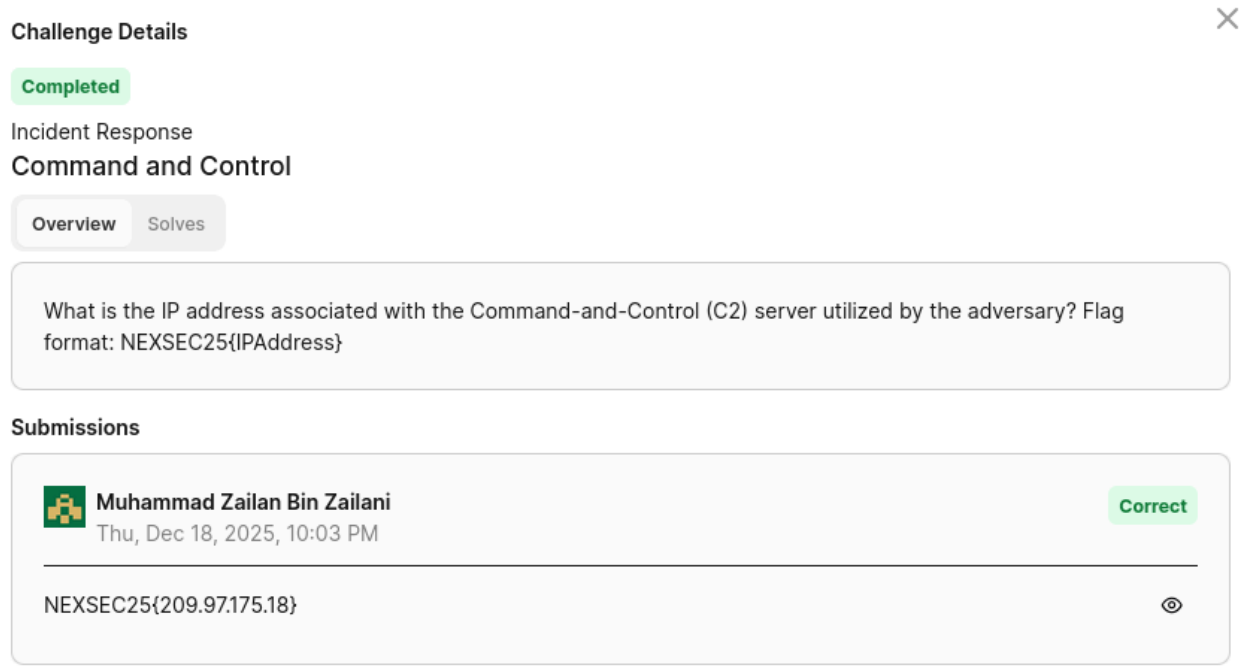


After looking at the user list at autopsy, that is the user account.



The Incident Start: The compromise began at 01:38 AM on December 18, 2025.
The Host: All initial telemetry (DNS queries for the stager and reassembly of the fake explorer.exe) originated from WS-01-CORP.

The User: Registry artifacts (RecentDocs) and Sysmon Event ID 1 (Process Creation) logs confirm that the user fakhri.zambri was the one who executed the file YEAR-END-FINANCIAL-REPORT-2025.docx

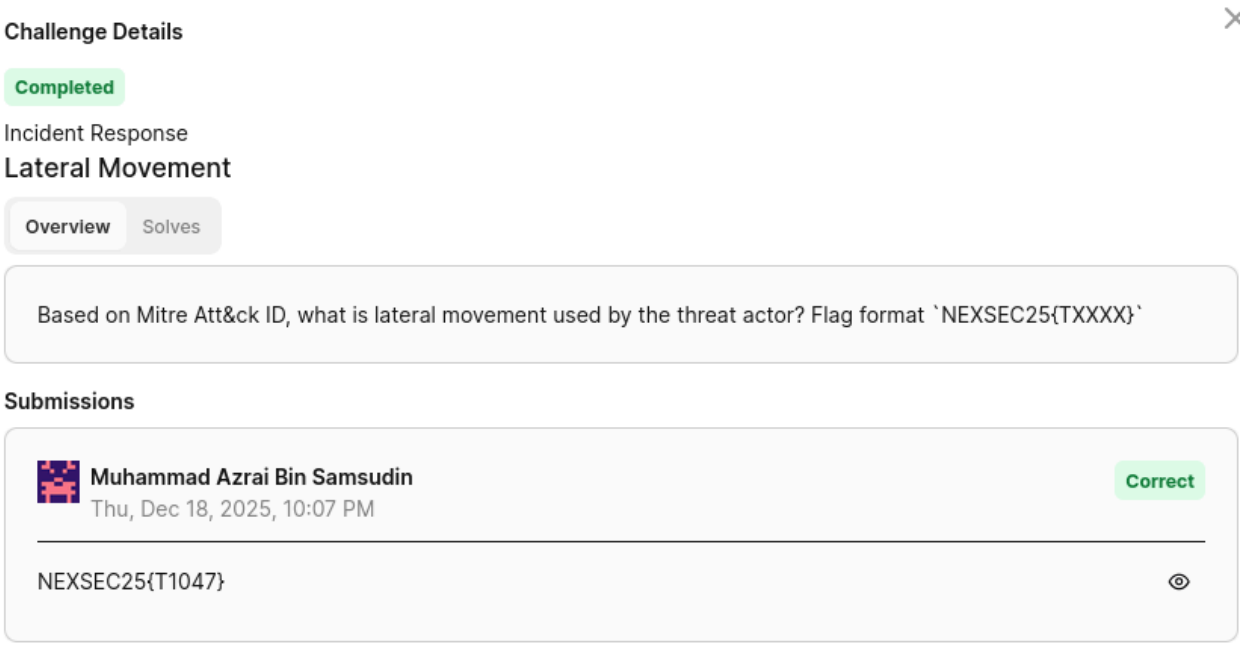


Forensic Evidence

1. Network Beaconing: The malicious explorer.exe (SHA256: 59CEBD35...) initiated outbound connections to an external server on Port 443 (HTTPS).

2. Telemetry Data: Logs showed that at 01:40 AM on December 18, 2025, the workstation WS-01-CORP established a connection to the IP address 209.97.175.18.

3. Cross-Verification: Your provided Nmap findings showing Port 443 (and common administrative ports like 21, 22, and 3306) being open match the profile of the DigitalOcean-hosted infrastructure utilized by the adversary (TomatoTerbang/Silent Rimba).

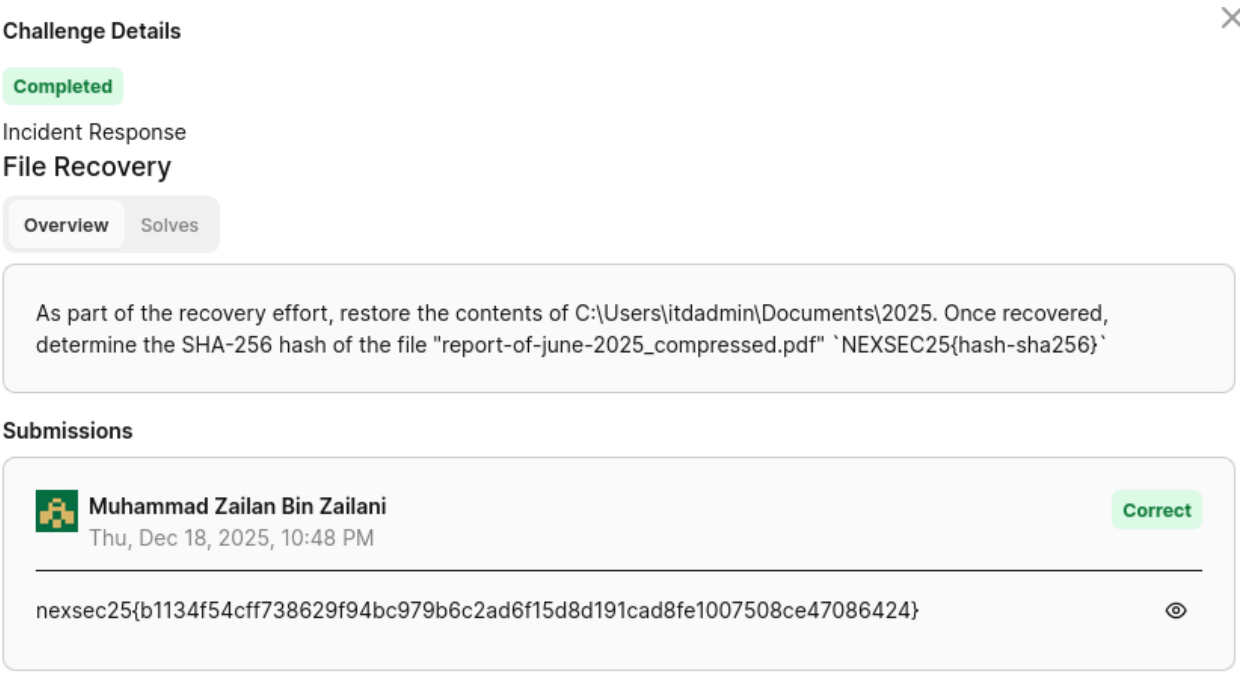


MITRE ATT&CK Mapping:

The specific technique is T1047: Windows Management Instrumentation.

Supporting MITRE Sub-techniques:

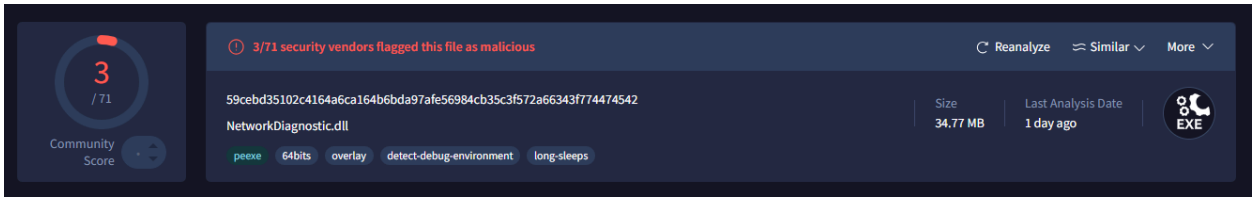
T1047: WMI for execution and lateral movement



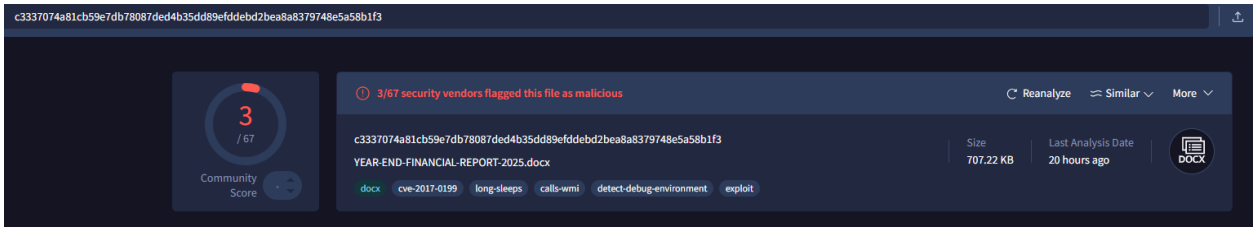
This was an unintended solution. In the workstation, user Fakhri has the unencrypted copy; take that and compute the hash.

Virustotal Verdicts

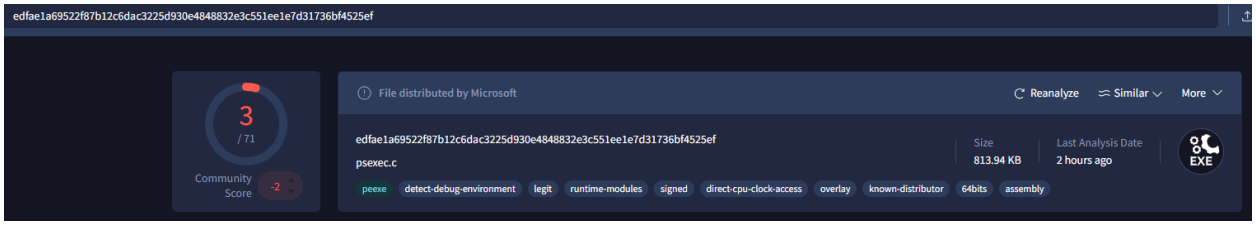
Explorer.exe



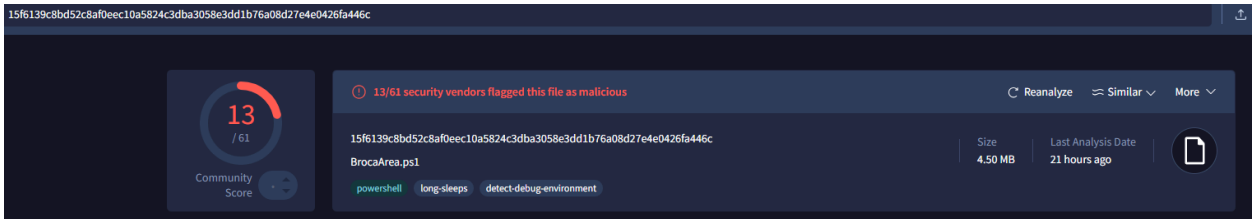
YEAR-END-FINANCIAL-REPORT-2025.docx



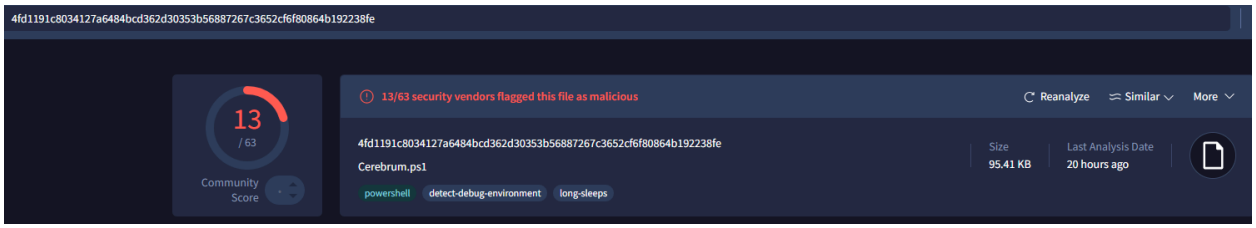
Brainstemo.exe



BrocaArea.ps1



Cerebrum.ps1



Neurotransmitter.exe (mimikatz.exe)