PRIVATE AND CONFIDENTIAL

Prepared For :

CORP .BHD

DIGITAL FORENSIC **REPORT**

TABLE OF CONTENT

1. DOCUMENT VERIFICATION

Name of Document	**:**	**MCMC CTF FINAL ROUND**
Exhibit Reference	**:**	**-**
Produced Date	**:**	**19/12/2025**
Prepared By	**:**	**Team InsyaAllahFinal**

RAZLAN BIN RAMLI

ABDUL HAZIQ BIN SUJIF

MOHAMAD AIMAN BIN HASAN

2. EXHIBIT INFORMATION

EXHIBIT REFERENCE	:	**-**
FORENSIC EXAMINER	:	**RAZLAN BIN RAMLI** **ABDUL HAZIQ BIN SUJIF** **MOHAMAD AIMAN BIN HASAN**
CONTACT NUMBER	:	**011-12340485**
DATE OF EXHIBIT	:	**19/10/2025 @ 1200HRS**
ACCEPTANCE	:	
RELEASED BY	:	
RECEIVED BY	:	
LOCATION	:	**MCMC CCOE, CYBERJAYA**

3. TECHNICAL REPORT PURPOSE

The purpose of this report is to document the forensic analysis of a targeted ransomware attack against the corporate network. It identifies the threat actor, details the technical methodology of the breach, establishes a timeline of compromise, and provides remediation strategies to prevent future occurrences.

4. EXECUTIVE SUMMARY

Incident Overview: On December 18, 2025, a financially motivated threat actor, identified as **SILENT RIMBA**, compromised the corporate network using a custom toolkit named **BrainRil**. The attack followed a standard kill chain: initial access via phishing, lateral movement via credential theft, and a final impact involving data exfiltration and mass encryption.

Key Findings

Patient Zero : User Fakhri Zambri was the initial entry point after executing a malicious document.

Exfiltration : Sensitive data from the ATM_Release folder was stolen and sent to the C2 domain echonine.org.

Impact : A total of 849 files were encrypted with the .anon extension using AES-256-CBC.

Anti-Forensics: The attacker used "Slack Stomping" on 849 files to prevent disk carving and stopped the Splunk Forwarder service to hide activity

5. EXAMINATION OBJECTIVE(S)

5.1 To identify the initial entry vector and lateral movement techniques.
5.2 To analyze the malware and its cryptographic functions
5.3 To verify persistence mechanisms and Command & Control (C2) infrastructure.
5.4 To determine the timeline of data exfiltration and encryption.

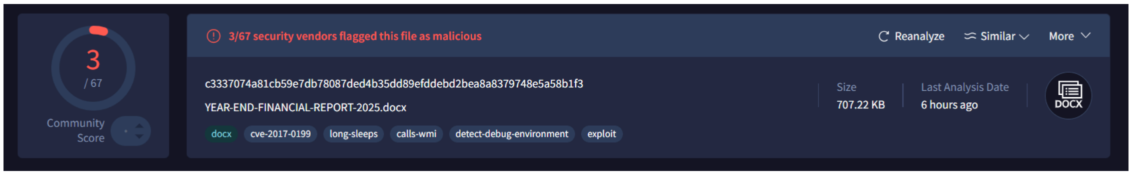
6. EQUIPMENT AND SOFTWARE USED

6.1 Autopsy 4.22.1
6.2 Splunk Enterprise
6.3 VirusTotal
.4 CyberChef

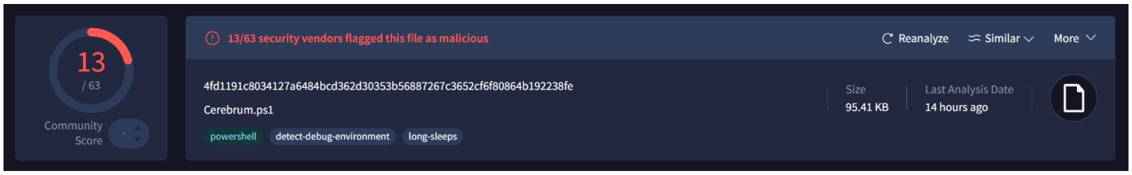
7. EXAMINATION RESULTS

The result of the examination is based on the details in Section 9

8. IOCs

Analysis Result			
 3 / 67 Community Score 3/67 security vendors flagged this file as malicious Reanalyze Similar More c3337074a81cb59e7db78087ded4b35dd89efddebd2bea8a8379748e5a58b1f3 YEAR-END-FINANCIAL-REPORT-2025.docx docx cve-2017-0199 long-sleeps calls-wmi detect-debug-environment exploit Size 707.22 KB Last Analysis Date 6 hours ago DOCX			
General Information			
Filename	YEAR-END-FINANCIAL-REPORT-2025.docx	**Date Created**	2025-12-18 01:37:00
Format	MS Word Document	**Date Modified**	2025-12-18 01:37:36
File Size	707.22 KB	**Date Accessed**	2025-12-18 01:41:12
Hash (Sha-1)	501ed53276a1ac3f0736faee86cff28ed11e628a		
Hash (Sha-256)	c3337074a81cb59e7db78087ded4b35dd89efddebd2bea8a8379748e5a58b1f3		
Hash (MD5)	2412b095ddd77acf9f12fb9f27a3b45f		
File Information			
Path	/img_workstation-disk1.vmdk/vol_vol6/Users/fakhri.zambri/Documents/YEAR-END-FINANCIAL-REPORT-2025.docx		
Function	Initial dropper/phishing payload		
Parent PID	4112 (WINWORD.EXE)		
Summary	This file contains an obfuscated macro that executes a PowerShell command to download the BrainRil toolkit from GitHub.		

Analysis Result



13/63 security vendors flagged this file as malicious

4fd1191c8034127a6484bcd362d30353b56887267c3652cf6f80864b192238fe

Cerebrum.ps1

powershell detect-debug-environment long-sleeps

Size 95.41 KB

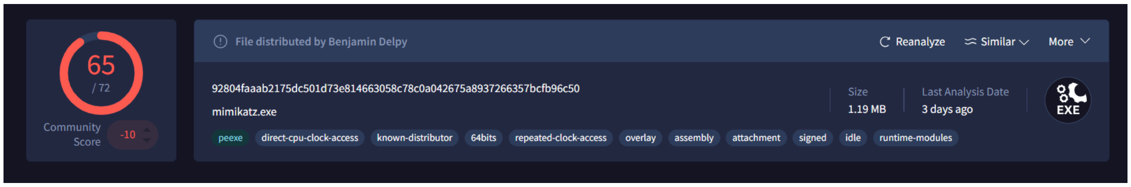
Last Analysis Date 14 hours ago

General Information

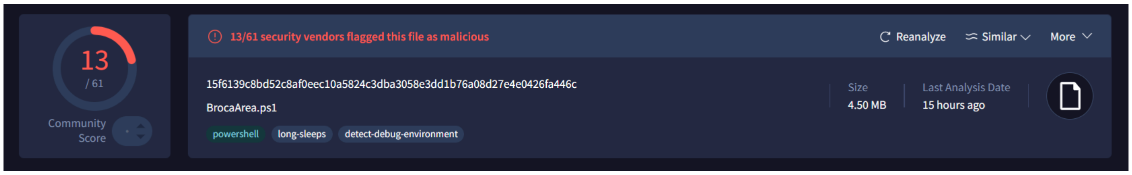
Filename	Cerebrum.ps1	**Date Created**	2025-12-18 02:22:28
Format	Powershell Script	**Date Modified**	2025-12-18 02:22:29
File Size	95.41 KB	**Date Accessed**	2025-12-18 02:22:51
Hash (Sha-1)	c355f457f76dc8ff44f5837641785756b13c44e5		
Hash (Sha-256)	4fd1191c8034127a6484bcd362d30353b56887267c3652cf6f80864b192238fe		
Hash (MD5)	621383cb58c85c414a3c1e791a2c06a2		

File Information

Path	/img_workstation-disk1.vmdk/vol_vol6/Windows/Temp/Celebrum.ps1
Function	UAC Bypass / Pass-the-Hash (PtH)
MITRE	T1548.002, T1550.002
Summary	A critical component of the BrainRil toolkit. It performs a UAC bypass to gain High Integrity permissions and contains the Invoke-LargeBrain function, which facilitates Pass-the-Hash (PtH) attacks via WMI

Analysis Result			
 65 / 72 Community Score -10 File distributed by Benjamin Delpy Reanalyze Similar More 92804faaab2175dc501d73e814663058c78c0a042675a8937266357bcfb96c50 mimikatz.exe Size 1.19 MB Last Analysis Date 3 days ago EXE peexe direct-cpu-clock-access known-distributor 64bits repeated-clock-access overlay assembly attachment signed idle runtime-modules			
General Information			
Filename	Neurotransmitter.exe	**Date Created**	2025-12-18 02:19:35
Format	Neurotransmitter.exe	**Date Modified**	2025-12-18 02:19:35
File Size	1.19 MB	**Date Accessed**	2025-12-18 02:20:04
Hash (Sha-1)	d1f7832035c3e8a73cc78afd28cfd7f4cece6d20		
Hash (Sha-256)	92804faaab2175dc501d73e814663058c78c0a042675a8937266357bcfb96c50		
Hash (MD5)	e930b05efe23891d19bc354a4209be3e		
File Information			
Path	/img_workstation-disk1.vmdk/vol_vol6/Windows/Temp/Neurotransmitter.exe		
Function	Credential Dumping (LSASS/SAM)		
MITRE	T1003.001 (LSASS Memory)		
Summary	A renamed version of Mimikatz. It was used to dump the NTLM hash for the itdadmin account from the LSASS process, providing the necessary credentials for lateral movement across the domain.		

Analysis Result



13/61 security vendors flagged this file as malicious

15f6139c8bd52c8af0eec10a5824c3dba3058e3dd1b76a08d27e4e0426fa446c

BrocaArea.ps1

powershell long-sleeps detect-debug-environment

Size 4.50 MB

Last Analysis Date 15 hours ago

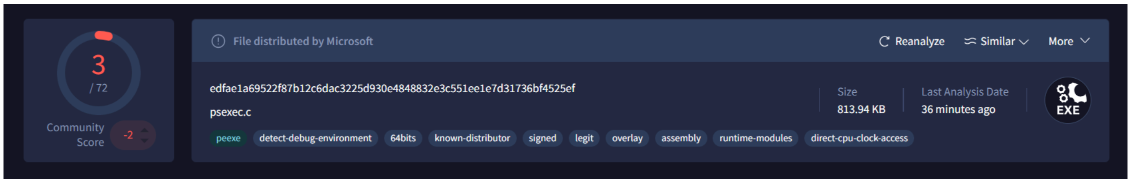
General Information

Filename	BrocaArea.ps1	**Date Created**	2025-12-18 02:16:38
Format	Powershell Script	**Date Modified**	2025-12-18 02:16:41
File Size	4.50 MB	**Date Accessed**	2025-12-18 02:17:00
Hash (Sha-1)	25fbee2493d7111b68bb7b8414c1f6299ccbe86c		
Hash (Sha-256)	15f6139c8bd52c8af0eec10a5824c3dba3058e3dd1b76a08d27e4e0426fa446c		
Hash (MD5)	8182a667355dce657514b279e43da9f7		

File Information

Path	/img_workstation-disk1.vmdk/vol_vol6/Windows/Temp/BrocaArea.ps1
Function	Active Directory Enumeration
Component	PowerView & BloodHound Ingestors
Summary	Used for full-scale domain reconnaissance. It mapped the shortest attack path to the FS-CORP FileShare by identifying vulnerable GPOs and accounts with DCSync rights.

Analysis Result



edfae1a69522f87b12c6dac3225d930e4848832e3c551ee1e7d31736bf4525ef

psexec.c

Size: 813.94 KB

Last Analysis Date: 36 minutes ago

peexe · detect-debug-environment · 64bits · known-distributor · signed · legit · overlay · assembly · runtime-modules · direct-cpu-clock-access

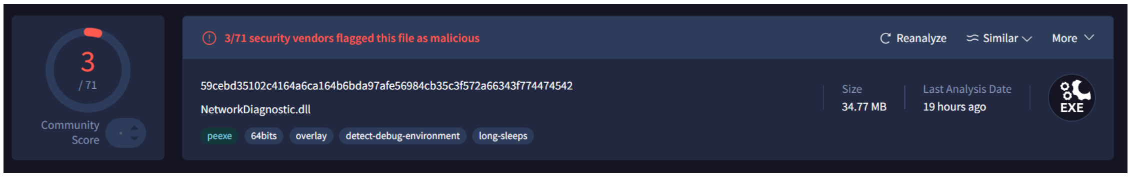
General Information

Filename	Brainstemo.exe	**Date Created**	2025-12-18 02:20:13
Format	PE32+ Executable	**Date Modified**	2025-12-18 02:20:13
File Size	813.94 KB	**Date Accessed**	2025-12-18 02:20:13
Hash (Sha-1)	0098c79e1404b4399bf0e686d88dbf052269a302		
Hash (Sha-256)	edfae1a69522f87b12c6dac3225d930e4848832e3c551ee1e7d31736bf4525ef		
Hash (MD5)	db89ec570e6281934a5c5fcf7f4c8967		

File Information

Path	/img_workstation-disk1.vmdk/vol_vol6/Windows/Temp/Brainstemo.exe
Function	Lateral Movement / Remote Execution
MITRE	T1047, T1569.002
Summary	A renamed version of PsExec. The attacker used this tool to execute the final ransomware payload on FS-CORP with SYSTEM-level privileges after gaining credentials via PtH.

Analysis Result



3 / 71

3/71 security vendors flagged this file as malicious

59cebd35102c4164a6ca164b6bda97afe56984cb35c3f572a66343f774474542

NetworkDiagnostic.dll

peexe 64bits overlay detect-debug-environment long-sleeps

Size 34.77 MB

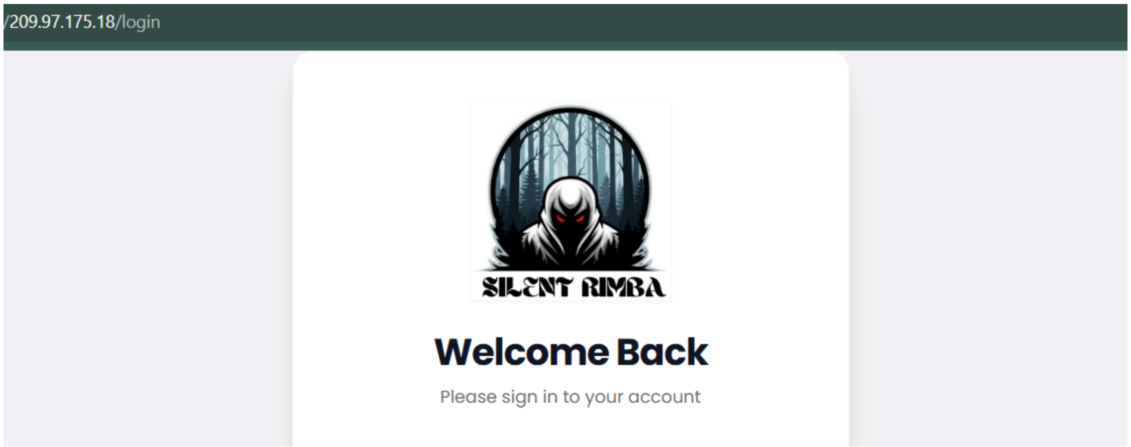
Last Analysis Date 19 hours ago

General Information

Filename	Explorer.exe	**Date Created**	2025-12-18 02:31:54
Format	PE32+ executable	**Date Modified**	2025-12-18 02:39:24
File Size	34.77 MB	**Date Accessed**	2025-12-18 02:39:24
Hash (Sha-1)	1632eaa14c3b7fe678c534a46eafb32d814944ca		
Hash (Sha-256)	59cebd35102c4164a6ca164b6bda97afe56984cb35c3f572a66343f774474542		
Hash (MD5)	78f54036cc749baaf0b0f9216d458d19		

File Information

Path	/img_FS-disk1.vmdk/vol_vol7/Users/Public/explorer.exe
Function	Silent Rimba Ransomware / Stealer
Parent PID	7600 (0x1db0)
Summary	The primary payload. It exfiltrated the ATM_Release data to echonine.org (C2), encrypted files using AES-256-CBC and performed Slack Stomping on 849 files to prevent disk carving as an anti-forensic technique.

Analysis Result			
 /209.97.175.18/login SILENT RIMBA Welcome Back Please sign in to your account			
General Information			
Filename	209.97.175.18	**Date Created**	-
Format	C2 Server	**Date Modified**	-
File Size	-	**Date Accessed**	-
Hash (Sha-1)	-		
Hash (Sha-256)	-		
Hash (MD5)	-		
File Information			
Path	-		
Function	Serve as the host to receive stolen data		
Parent PID	-		
Summary	C2 domain used by the attacker to store keys and stolen data. Can be found inside pcapng.		

9. CHRONOLOGICAL EVENTS TIMELINE

Date/Time	Attack Phase	Event Description	Forensic Evidence Source
18/12/2025 01:38:07	Initial Access	**WINWORD.EXE** is launched. The user (Fakhri Zamri) opens the malicious phishing document.	Splunk (PID 11216)
18/12/2025 01:39:21	Payload Delivery	Word spawns PowerShell to reconstruct the **ransomware** payload.	Splunk (Event ID 1)
18/12/2025 01:39:21	De-obfuscation	PowerShell reads a Base64 string from a temp file (xvzpox75.txt) and writes the binary to **C:\Users\Public\explorer.exe.**	Splunk (CommandLine)
18/12/2025 01:39:34	Toolkit Download	PowerShell executes a second command using Invoke-WebRequest to download the **BrainRil toolkit** via a shortened URL (tinyurl.com/4kaz75ds).	Splunk (CommandLine)
18/12/2025 02:31:57	Execution	The reconstructed explorer.exe payload is activated on the **FS-CORP** server.	Splunk (Sysmon ID 7)
18/12/2025 02:34:05	Defense Evasion	The Splunk Forwarder service is stopped to **hide** the mass encryption activity.	Splunk Metrics
18/12/2025 03:01:13	Final Impact	Mass encryption of **849** files concludes; project files renamed to .anon.	$UsnJrnl / MFT

9.0.1 Table shows the chronological event

10. CONCLUSION AND FURTHER ACTION(S)

Based on the forensic examination of FS-CORP and WS-01-CORP, the following conclusions have been reached regarding the security breach on 18 December 2025:

10.1 Conclusion

The investigation confirms that the breach was targeted by a financially motivated threat actor, the initial defences were bypassed through social engineering (phishing) and the actors utilized legitimate administrative tools (renamed to evade detection) for lateral movement. The successful exfiltration of project data and the destruction of file headers through slack stomping indicate a high level of technical proficiency by the actor.

10.2 Further action

To remediate the current incident and prevent recurrence, the following are recommended:

- **Network Containment**

  Immediately block traffic echonine.org and download source at the perimeter firewall.

- **System Remediation**

  Reimage the compromised host WS-01-CORP and FS-CORP, as the attacker utilizes persistence mechanisms and anti-forensic techniques that make data carving difficult. Restore encrypted data from offline backups created prior to 18 December 2025.

- **Policy Hardening**

  1) Disable execution macros in Microsoft Office document via Group Policy, as this was the initial entry vector.
  2) Restrict the usage of an administrative tools like PowerShell and PsExec to authorized personnel only to prevent the execution scripts like Cerebrum.ps1 and Brainstemo.exe

11.BIBLIOGRAPHY

[1] Alexander Sturz (2025), *adPEAS - Automated Active Directory Enumeration*,https://github.com/61106960/adPEAS

[2] Benjamin Delpy (2025), *Mimikatz - Credential Extraction Tool*, https://github.com/gentilkiwi/mimikatz

[3] Kevin Robertson (2025), *Invoke-TheHash - PowerShell Pass-the-Hash*, https://github.com/Kevin-Robertson/Invoke-TheHash

[4] Microsoft Support (2025), *Antimalware Scan Interface (AMSI) Functions*, https://learn.microsoft.com/en-us/windows/win32/amsi/antimalware-scan-interface-functions

[5] Splunk Documentation (2025), *Monitor service status and disruptions*,https://docs.splunk.com/Documentation

[6] Sleuth Kit (2025), *Autopsy User Documentation - Timeline Analysis*,https://sleuthkit.org/autopsy/docs/user-docs/4.19.3/timeline_page.html