Author: Jack Fitzgerald

Official Incident Report

Date: Mar, 14, 2024, 05:23 PM

Event ID: 238

Rule Name: SOC153 - Suspicious Powershell Script Executed

Table of Contents

Alert Details

Severity: Medium

Type: Malware

Hostname: Tony

Ip Address: 172.16.17.206

File Name: payload_1.ps1

File Path: C:\Users\LetsDefend\Downloads\payload_1.ps1

File Hash: db8be06ba6d2d3595dd0c86654a48cfc4c0c5408fdd3f4e1eaf342ac7a2479d0

Trigger Reason: Suspicious Powershell Script Executed

AV/EDR Action: Detected

Based on the information provided in the alert, it appears that a **suspicious PowerShell script** has been executed on a LetsDefend host machine. The alert is triggered by rule SOC153 - Suspicious Powershell Script Executed.

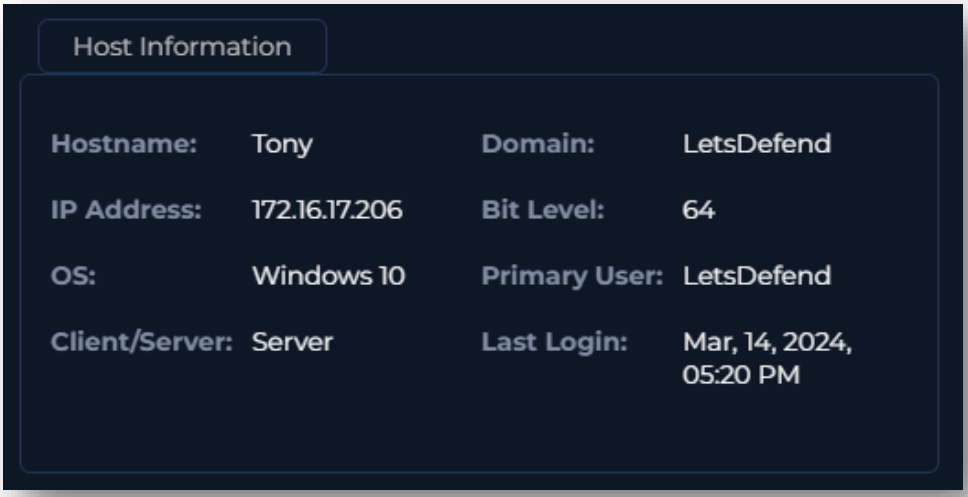
Overall, it appears that the alert may be **suspicious**, and further investigation is needed to identify the extent of the alert and determine if any necessary actions are required to remediate the situation.

Detection

Verify

As a security analyst, one of the first steps we take to verify the alert and determine whether it is a **false positive** or a **true positive** incident is to analyse the alert details.

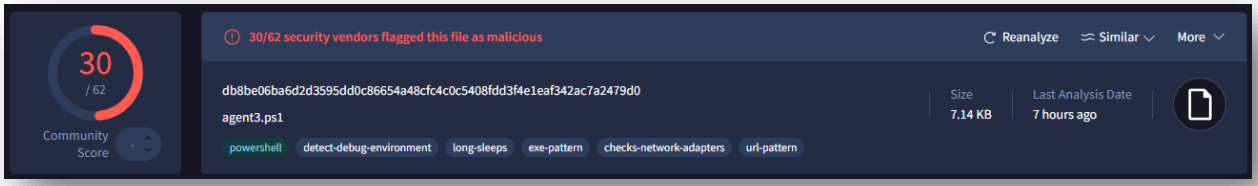
We have identified that the ‘payload.ps1’ PowerShell script was executed in the Downloads folder by the LetsDefend user on the Tony server machine. This indicates that the script was downloaded from another source to the server at some point prior to the alert.



Analysis

Now that we have identified the information in the alert, we can start the analysis by first investigating the SHA256 file hash.

https://www.virustotal.com/gui/file/db8be06ba6d2d3595dd0c86654a48cfc4c0c5408fdd3f4e1eaf342ac7a2479d0



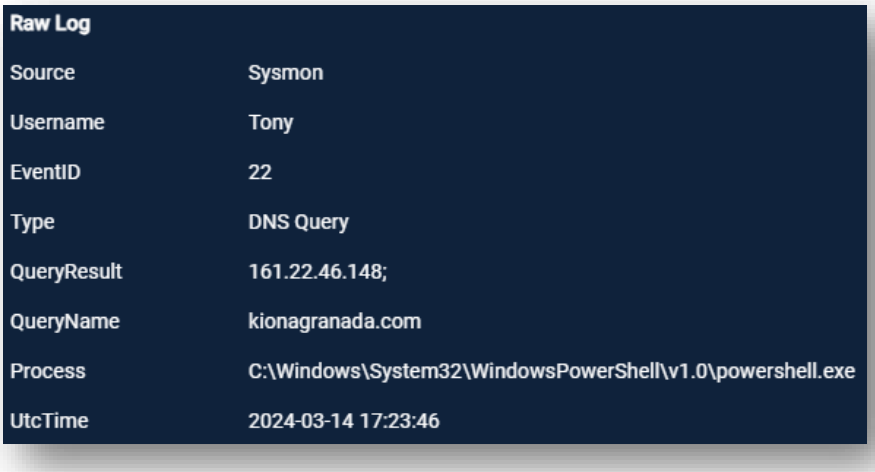
Important Information:

- Filename: payload_1.ps1
- Alias: agent3.ps1
- MD5: e971b4ed257b0c60287e63c5d533eace
- Contacted Domain: kionagranada.com
- Contacted URL: https://kionagranada.com/upload/beauty.exe
- Contacted IP: 161.22.46.148

Next, we will investigate Log Management.

We found 13 events (before Mar, 15, 2024, 11:36 PM UTC) coming from the Source Address for the Tony server machine.

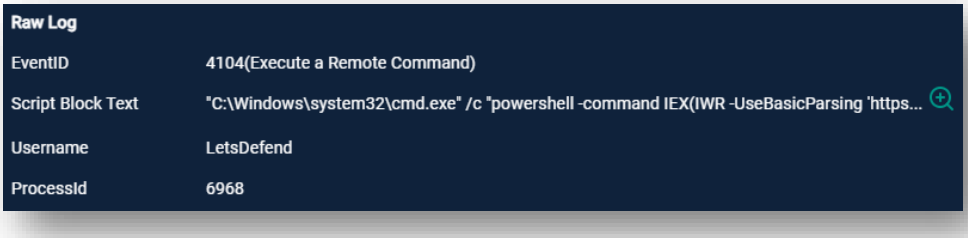
The first log we will analyse is a **DNS resolution** for malicious infrastructure.



In this log, PowerShell resolves the domain 'kionagranada.com' and its corresponding IP 161.22.46.148. Both pieces of information were found as **indicators of malicious activity** in the earlier analyses of the malicious file hash.

This confirms that the script execution attempted an outbound connection to a **C2 server**. This correlates directly with the **IWR** download command.

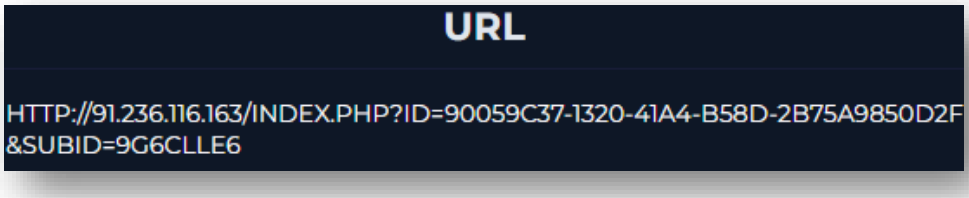
The next log shows a remote command being executed on the server, to perform the initial malicious PowerShell download, via LOLBin abuse.



This script block uses cmd.exe to launch PowerShell, which runs the command **IEX** (Invoke-Expression) to execute another command **IWR** (Invoke-WebRequest) directly in memory. This is an example of **fileless execution** performed to download 'sd2.ps1' from URL 'https://kionagranada.com/upload/'.

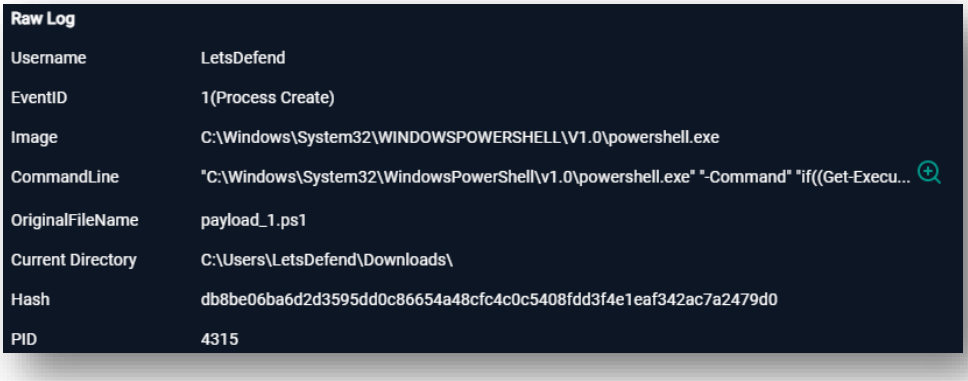
This URL was identified previously via the malicious file hash analyzed earlier, indicating malicious activity.

The next log shows a follow-on C2 tracking request.

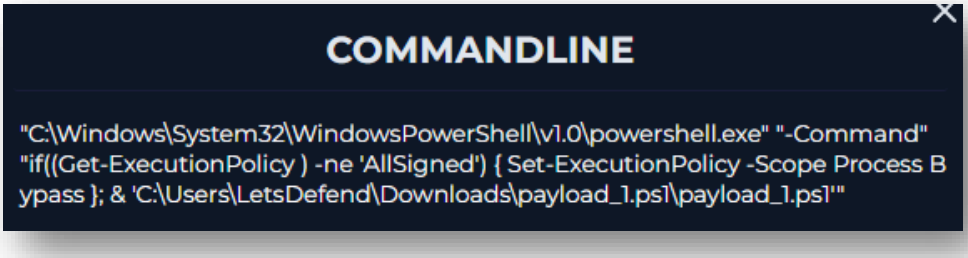


This is a beacon-style URL that uses a direct IP-based HTTP request to 91.236.116.163. The Unique ID strongly suggests victim trafficking used to register infection or receive next-stage commands.

The next log shows execution policy bypass and the payload execution.



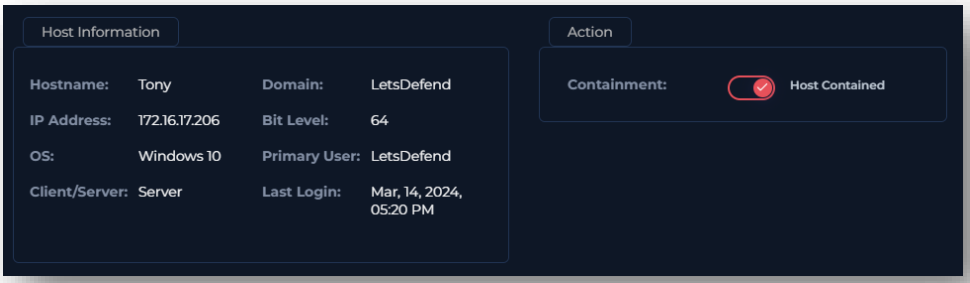
Raw Log	
Username	LetsDefend
EventID	1(Process Create)
Image	C:\Windows\System32\WINDOWSPOWERSHELL\V1.0\powershell.exe
CommandLine	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" "-Command" "if((Get-Execu...
OriginalFileName	payload_1.ps1
Current Directory	C:\Users\LetsDefend\Downloads\
Hash	db8be06ba6d2d3595dd0c86654a48cfc4c0c5408fdd3f4e1eaf342ac7a2479d0
PID	4315



The ExecutionPolicy is **explicitly bypassed** and executed payload_1.ps1 from the disk. This suggests that the previously identified sd2.ps1 likely dropped/staged payload_1.ps1, resulting in **second-stage payload execution**.

Containment

Based on the information gathered during the investigation, it is highly likely that the system has been compromised. Immediate isolation of the system from the network is required.



Summary

The incident involves a compromised system named **Tony** with an IP address of **172.16.17.206**. The alert was triggered by the execution of a suspicious PowerShell script, based on the rule SOC153 - Suspicious Powershell Script Executed.

After investigating the Logs and the Endpoint that was affected, we identified the alert was valid and malicious. This was evidenced by a **multi-stage PowerShell attack via fileless execution** from 'https://kionagranada.com/upload/sd2.ps1' to download a second-stage payload 'payload_1.ps1'.

This was followed by a **unique identifier being beaconed out by the system**, and an **execution policy bypass** to ensure script execution of 'payload_1.ps1'.

Based on the findings of the incident, immediate action needs to be taken to isolate the compromised system, and the event was identified as a **True Positive**.

Lessons Learned

- The power and flexibility of PowerShell, which make it useful for system administrators, is also leveraged by attackers to run obfuscated, fileless malware that can evade traditional security tools

- Use of Invoke-Expression (IEX) or Invoke-WebRequest to download and execute code from remote sources can be indicators of compromise

- Attackers frequently use PowerShell for living-off-the-land techniques, leveraging legitimate tools for malicious purposes like data exfiltration, credential dumping, and persistence

Remediation Actions

- Isolate the affected system from the network immediately to prevent further malicious activity, such as lateral movement or communication with command-and-control (C2) servers

Appendix

MITRE ATT&CK

MITRE Tactics	MITRE Techniques
Execution	T1059.001 - Command and Scripting Interpreter: PowerShell
Defense Evasion	T1562 - Impair Defenses
Command and Control	T1071.001 - Application Layer Protocol: Web Protocols
Command and Control	T1105 – Ingress Tool Transfer

Artifacts

Value	Comment	Type
https://kionagranada.com/upload/	Hosts malicious PowerShell scripts	URL Address
161.22.46.148	C2 Server	IP Address
91.236.116.163	Potential beacon for victim trafficking	IP Address
e971b4ed257b0c60287e63c5d533eace	payload_1.ps1	MD5 Hash

LetsDefend Playbook

LetsDefend Event ID: 238