CustomerName

Incident Report

Prepared by: Rapid7 Managed Detection and Response

Rapid7 Contact Information

Please direct any additional questions or concerns to your Customer Advisor via the Insight Platform: 'https://insight.rapid7.com/login'.

If you require immediate assistance, please call the emergency hotline to speak with an MDR representative.

Region	24/7 Hotline Number
United States (US)	+1 844-777-7637
European Union (EU)	+44 800-088-5859
Singapore (SG)	+65 800-852-3321
Australia (AU)	+61-2-4734-7032

Table of Contents:

Executive Summary

On June 26th, Rapid7's Managed Detection and Response (MDR) notified CustomerName regarding the execution of a suspicious PowerShell command via the Windows Run dialog box. Rapid7 initiated incident response services to identify the extent of the compromise within the CustomerName environment. Rapid7 determined that a total of one asset and one account were in scope for the investigation.

Rapid7 classified this incident with Medium severity.

Incident Synopsis

Rapid7 determined that the CustomerName environment was initially compromised on 2025-06-26 at 16:30:36 UTC when the user account 'useraccount' executed a suspicious PowerShell command via the Windows Run dialog box on asset 'ASSETNAME'.

Rapid7 determined that the PowerShell command was designed to download and execute a payload from the URL ***hXXps[://]myinetverif[.]cloud/Z7M[.]dof***. Rapid7 navigated to the suspicious URL and observed that it hosted an obfuscated PowerShell script ***Z7M.dof*** at the time of the investigation.

Rapid7 successfully acquired the PowerShell script ***Z7M.dof*** from external infrastructure, executed it in a controlled environment and observed that it would create a folder named ***eliqykz*** under the user's *\AppData\Roaming* directory. Additionally, it would extract multiple embedded files including ***client32.exe***, a NetSupport Remote Access Trojan (RAT) and its dependencies from ***Z7M.dof*** and add them to the folder ***eliqykz***. Rapid7 additionally observed that a Windows shortcut file (LNK) ***zDMpryHgOkZ*** for ***client32.exe*** would be added to the user's *\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup* directory. This is intended to establish persistence as the LNK file ***zDMpryHgOkZ*** will execute ***client32.exe*** whenever the user logs in to the system.

Rapid7 observed that ***Z7M.dof*** was additionally designed to use the Windows Command Prompt (*cmd.exe*) to first launch the Windows Program Compatibility Assistant (*pcalua.exe*), and use it to execute ***client32.exe*** from the path ***C:\Users\username\AppData\Roaming\eliqykz***. Attackers often abuse *pcalua.exe* as a Living Off the Land Binary (LOLBin) to execute malicious payloads.

Rapid7 observed that ***client32.exe*** was designed to establish connections with the Command and Control (C2) domains ***deepholeintheworld[.]com*** and ***THANKYOUMYKIO[.]COM***. Rapid7 reviewed the DNS, Web Proxy, and Sysmon network connection logs and observed connection attempts to the C2 domains and to the IP address ***83.222.190[.]174***, which was observed to be hosting the C2 domains at the time of the investigation.

Rapid7 observed that ***client32.exe*** later spawned the process ***remcmdstub.exe*** from the path ***C:\Users\username\AppData\Roaming\eliqykz*** and used it to spawn *cmd.exe*. Then a

PowerShell process (powershell.exe) was used to execute a command to download the malicious MSI file ***WTXBSLLD.msi*** from the URL ***hXXps[://]cloudverifsecure[.]com/IALMKAFJ.msi***, save it in the user's Temp folder, use the legitimate Windows installer 'msiexec.exe' to install the payload on the asset, and then delete the downloaded MSI file ***WTXBSLLD.msi***.

Rapid7 acquired ***WTXBSLLD.msi*** from external infrastructure and observed that upon execution the file would leverage 'msiexec.exe' to install it in the following locations on the asset:

- C:\Users\<useraccount>\AppData\Local\Temp\{674CF26D-4CA8-387B-A7D0-8DF0943A5205}\
- C:\ProgramData\localwriter_Mujv2\

Rapid7 observed that the folders would contain the binary ***CacheData.exe*** alongside multiple suspicious files and that upon execution, ***CacheData.exe*** would spawn the process ***FluxBr128.exe*** from the ***C:\Users\username*** folder and leverage the following malicious files to inject it with malicious code:

- ***mfc110u.dll***, a malicious DLL used to sideload the ***CacheData.exe*** process with malicious code.
- ***Maidreart.nvu***, file which exhibits characteristics consistent with the *IDAT Loader* family of malware and used to inject *SecTop RAT* into ***FluxBr128.exe***.

Rapid7 additionally observed that a LNK file ***Readerexplore_idn*** for ***CacheData.exe*** would be added to the user's *\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup* folder. This is intended to establish persistence as the LNK file ***Readerexplore_idn*** will execute ***CacheData.exe*** whenever the user logs in to the system.

Rapid7 determined that the process ***FluxBr128.exe*** would attempt to make connections to the IP addresses ***185.125.50[.]72*** and ***91.92.46[.]47***, and the domains ***ninicoin[.]io*** and ***defibit[.]io***.

Rapid7 reviewed the available Sysmon registry event logs and observed that the malicious PowerShell command was present within the user's ***RunMRU*** registry key, confirming that the user executed the PowerShell command via the Windows Run dialog box.

Upon review of the process start event logs, Rapid7 observed that the user was using the Google Chrome browser prior to running the PowerShell command. Rapid7 acquired the user's Google Chrome browser history to determine the URL of the webpage hosting the Fake CAPTCHA lure but observed that there was no data present around the time of the suspicious activity.

Rapid7 reviewed the available Virus and Third Party alert logs and did not observe any remedial actions taken on this activity at the time of the investigation.

The Tactics, Techniques, and Procedures (TTPs) that Rapid7 identified in the investigation were consistent with the Bunny Loader[1] family of malware. Rapid7 determined that the incident was

[1] https://www.rapid7.com/globalassets/docs/managedservices/malware-research-bunny_loader.html

the result of an opportunistic Bunny Loader infection and not the result of a targeted attack against the CustomerName environment.

Recommended Actions

Remediation Actions

- **Rebuild Affected Systems from a Known-Good Baseline Image**
  - Rebuild systems from a known-good baseline image to counter undetected threats.
  - Manually removing malware or scanning with an updated antivirus solution may not fully restore the integrity of the system.
- **Change Passwords for Affected Accounts**
  - Change the affected account passwords as soon as possible to prevent a threat actor from leveraging the credentials to access services.
  - Instruct users to not just change one character of a password, such as changing ***Example1!*** to ***Example2!*** and to follow the NIST guidelines for the 'memorized secret' password policy[2]. A threat actor who has captured past credentials could be more successful in guessing credentials changed by only one character.
  - InsightConnect could be used to perform these actions, which can be accessed through the 'Take Action' button in the *Investigations* section.
- **Block Malicious Domains**
  - Block the identified malicious domains at all appropriate network filtering devices, such as firewalls, web proxies, and DNS servers.
- **Block Malicious IP Addresses**
  - Block the identified malicious IP addresses at all appropriate network filtering devices, such as firewalls, web proxies, routers, and switches.
- **Rebuild the Affected User's Roaming Profile**
  - When enabled, User Roaming Profiles are stored remotely, as opposed to directly on their computer. This allows for settings and information associated with the user to sync with any device across the network that they log into. Threat actors use the Roaming Profile of a user account to store malicious files for staging and persistence.
  - If an infected asset is re-imaged from a known good baseline, but the user's Roaming Profile was not rebuilt as well, the malicious files stored in the Roaming Profile will persist, leaving the infection un-remediated.

Corrective Actions

- **User Awareness Training**
  - Implement phishing-based training for users identified as opening unknown attachments or clicking unknown links. Train users on how to forward suspicious links or emails to information security for analysis.

[2] https://pages.nist.gov/800-63-3/sp800-63-3.html

    - Rapid7 recommends providing user awareness training at regular intervals to all users in the environment.
- **Block Archive Files at the Web Proxy**
    - Block archive files (e.g. ***.zip***, ***.rar***) at the web proxy and only allow archive files to be downloaded from whitelisted sites serving business purposes.
    - Many commodity malware families package malicious executable files or scripts within archive files as a method of initial access. Packaging malware within archive files can prevent browser and asset-based antivirus solutions from identifying and taking action on suspicious files.
- **Block or Warn on Uncategorized Sites at the Web Proxy**
    - Block or warn on uncategorized sites at the web proxy. Aside from blocking uncategorized sites, certain web proxies will display a warning page, but allow the user to continue by clicking a link in the warning page. This will stop drive-by exploits and malware from being able to download further payloads from the Internet, as most malware will not be able to interact with the web proxy warning page.
- **Disable the Windows Run Dialog Box**
    - Rapid7 recommends disabling the Windows Run dialog box (Win + R) on devices in the environment. This can be accomplished through Group Policy or the Windows Registry.

Appendix A: Alert Summary

Time to Respond

Event Time	2025-06-26 16:31:17 UTC
Alert Time	2025-06-26 16:31:17 UTC
Acknowledge Time	2025-06-26 16:33:00 UTC

Alert time and time to begin investigation

Associated Alerts

Alert Name	IDR Investigation URL
Attacker Tool - PowerShell -noni -ep -nop Flags	https://us2.idr.insight.rapid7.com/op/16FF306704678B#/investigations/4d4918-ad74-bccdd
Attacker Technique - Remote Payload Execution via Run Utility (shell32.dll)	
Suspicious Process - Download & Execution Of Payload Via Powershell	
Suspicious Process - Malicious Hash On Asset	

Investigation IDs from IDR

Appendix B: Incident Severity, Category, Type

Rapid7 classified this incident with Medium severity.

Rapid7 determines the severity of an incident based on a number of factors, including:

- **Intent**: Whether the threat appears to be targeted or opportunistic/automated, and the likely objectives of the attack
- **Scope**: The number and criticality of systems and users impacted
- **Ongoing Activity**: Whether the incident appears to have been fully contained/no longer active, or whether the attacker remains active within the environment
- **Impact**: The criticality of in-scope assets or users, evidence of data exfiltration, etc.

Incident Severity	Incident Definition	Example Incident(s)
Low	A non-targeted, low-impact threat involving a small number of systems or users which is already contained by existing security controls.	A non-targeted phishing attack with evidence that the recipient(s) provided credentials.
Medium	A non-targeted, low-impact threat impacting a small number of systems or users, but requiring additional actions from you to fully contain and eradicate the threat.	Malware delivered via a non-targeted phishing attack that is only partially blocked on an endpoint.
High	A high risk or high impact threat, often impacting a large number of systems or users and ongoing attacker activity.	Unauthorized interactive network access with evidence of reconnaissance, privilege escalation, lateral movement, data exfiltration, or other signs of a late-stage compromise being observed.

Severity levels and Incident Types

Compromise Category	Compromise Type
Malicious Code	Virus

Incident Category and Type

Appendix C: Affected Assets and Accounts

Hostname	Disposition
HOSTNAME	Compromised

Affected Hosts

Account	Notes
USERNAME	User account that executed the suspicious PowerShell command via the Windows Run Dialog Box.

Affected Accounts

Appendix D: Indicators of Compromise

File

File Name	File Path	SHA256	Notes
Z7M.dof	-	952E3B9DB51BE60E58C5ED32D123C21123EBAE34B2F9FB549E814A0EBAC51234	PowerShell script hosted at the domain ***myinetverif[.]cloud,*** designed to install and execute ***client32.exe*** and its dependencies.
client32.exe	C:\Users\username\AppData\Roaming\eliqykz\	97123456b12315901324dd5d4b764e8712345b1bd87179552f249062ee26128	NetSupport RAT configured to reach out to ***deepholeintheworld[.]com*** and ***THANKYOUMYKIO[.]COM***.
WTXBSLLD.msi	C:\Users\ACME~1\AppData\Local\Temp\	e48a123456bafb123471ca77c72e15be99d1d62b941ddd1ff50f33b1234bcb8c2	MSI file hosted at the domain ***cloudverifsecure[.]com***, used to install malware.
CacheData.exe	C:\Users\ACME~1\AppData\Local\Temp\{123CF26D-3CA8-123B-A5D0-8DF1234A1234}\ C:\ProgramData\localwriter_Mujv2\	c2a1236f3775e641218ce24189e795acbac3562d7b2f0f27a4e08f12345678c1	Binary that would spawn ***FluxBr128.exe***.
mfc110u.dll	C:\Users\ACME~1\AppData\Local\Temp\{674CF26D-3CA8-123B-A5D0-8DF0123A1234}\ C:\ProgramData\localwriter_Mujv2\	a1e5df12345b0d8f9ab381a42a12312379a49e12345454f2a0e6b4d2ae12346d	DLL used to sideload malicious code into ***CacheData.exe***.

Maidreart.nvu	C:\Users\ACME~1\AppData\Local\Temp\{674CF123-3CA8-487B-A5D0-8DF0593A1234}\ C:\ProgramData\localwriter_Mujv2\	65f49f3ab123a6ebeba9daf0d165acad1f6d9e16a123c25e4acaa77fe0d12345	File consistent with *IDAT loader*, used to inject *SecTop RAT* into ***FluxBr128.exe***.
FluxBr128.exe	C:\Users\username\	f3fa12345b0512e7065f9b3b1233f8d7840213edb47a92bdfc32ba12342251d1	Binary injected with malicious code.
-	-	9612341f71c2bcd93ddbf26fd30b92c06d0fc810404ef6cb62bbc67709a7902f	.NET executable extracted from the ***FluxBr128.exe*** process, consistent with *SecTop RAT.*

File Based Indicators of Compromise

Network

Network Based Indicator	Notes
hXXps[://]myinetverif[.]cloud/Z7M[.]dof	URL present in the initial PowerShell command.
deepholeintheworld[.]com THANKYOUMYKIO[.]COM	C2 domains leveraged by ***client32.exe***, present in the *client32.ini* file.
83.222.190[.]174	IP address at which the domains ***deepholeintheworld[.]com*** and ***THANKYOUMYKIO[.]COM*** were hosted on.
hXXps[://]cloudverifsecure.com/IALMKAFJ[.]msi	URL at which the malicious MSI file ***WTXBSLLD.msi*** was hosted on.
bsc-dataseed1.ninicoin[.]io bsc-dataseed2.ninicoin[.]io bsc-dataseed2.ninicoin[.]io bsc-dataseed4.ninicoin[.]io	Domains that the ***FluxBr128.exe*** process would attempt to make a connection with.
bsc-dataseed1.defibit[.]io bsc-dataseed2.defibit[.]io bsc-dataseed3.defibit[.]io bsc-dataseed4.defibit[.]io	

185.125.50[.]72	IP address previously associated with *SecTopRAT*, and that the ***FluxBr128.exe*** process would attempt to make a connection with.
91.92.46[.]47	IP that the ***FluxBr128.exe*** process would attempt to make a connection with.

Network Based Indicators of Compromise