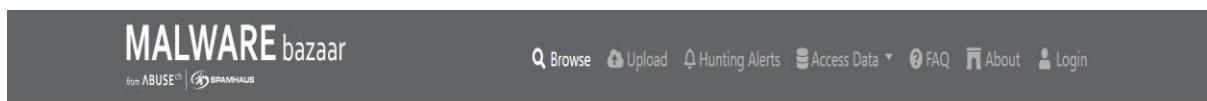


Malware Analysis

- Malware analysis is the process of studying and understanding malicious software, also known as malware, to determine its functionality, origin, and potential impact on a system or network.
- It involves examining the code, behavior, and characteristics of malware to identify its purpose and how it operates.
- This crucial cybersecurity practice helps organizations mitigate threats by understanding the attacker's behavior, objectives, and methods.
- There are primarily two types of malware analysis: static analysis, which involves examining the code without executing it, and dynamic analysis, which involves executing the malware to analyze its behavior.

For this analysis we are using any.run as a sandbox environment and we will be executing a malware sample.



MalwareBazaar Database

You are browsing the malware sample database of MalwareBazaar. If you would like to contribute malware samples to the corpus, you can do so through either using the [web upload](#) or the [API](#).



Using the form below, you can search for malware samples by a hash (MD5, SHA256, SHA1), imphash, tsh hash, ClamAV signature, tag or malware family.

Browse Database

This malware bazaar is a website full of malware samples.

Now we will see how to use any.run sandbox.

ANYRUN
INTERACTIVE MALWARE ANALYSIS

+ New analysis

Reports

Teamwork

History

Threat Intelligence

Windows 10 64 bit

Windows 10 64 bit

Profile

Notifications 13

Pricing

Contacts

FAQ

Log Out

Start your analysis

Interact with Windows, Linux, and Android OS directly and immediately see the feedback from your actions.

Deep interactive investigation in full environment

Safebrowsing free beta

Submit File / Email

Detonate an object to observe its malicious activity

Submit URL

Investigate malicious and phishing activity and inspect downloaded files

Check Suspicious Links

Open any URL to verify its content fast and easily

Interactive Tutorial: Quick Sandbox Tutorial →

Explore Links Faster!

Speed up routine link checks and get real-time threat alerts.

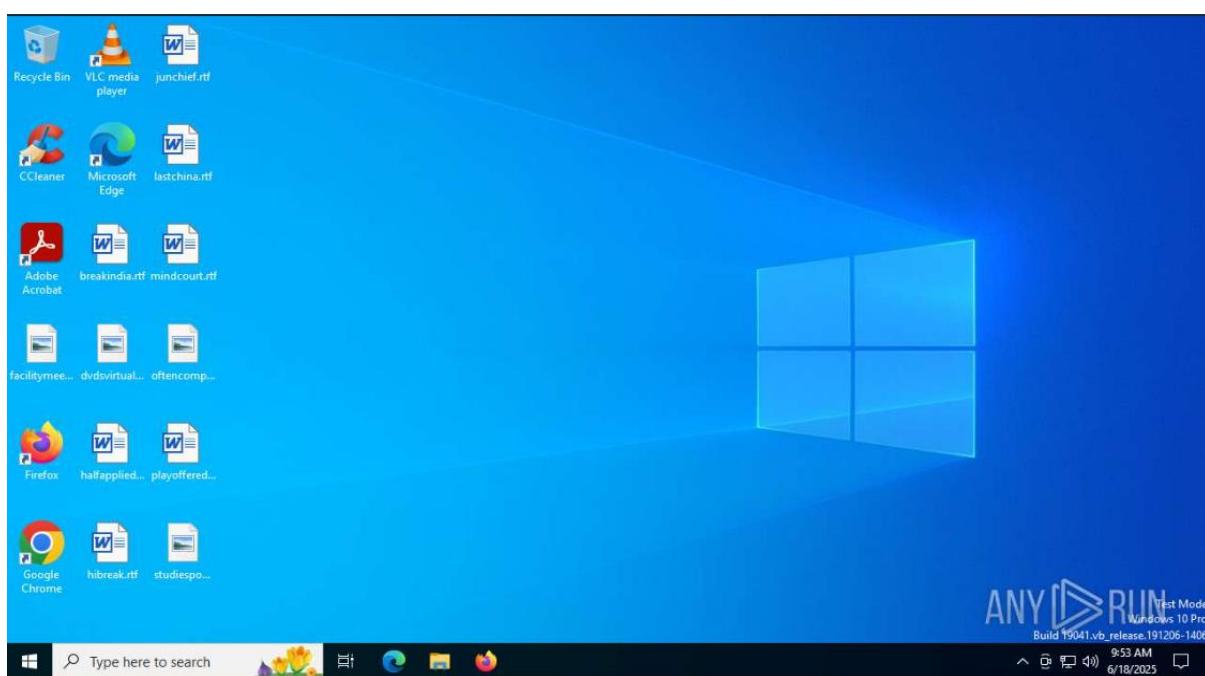
Okay

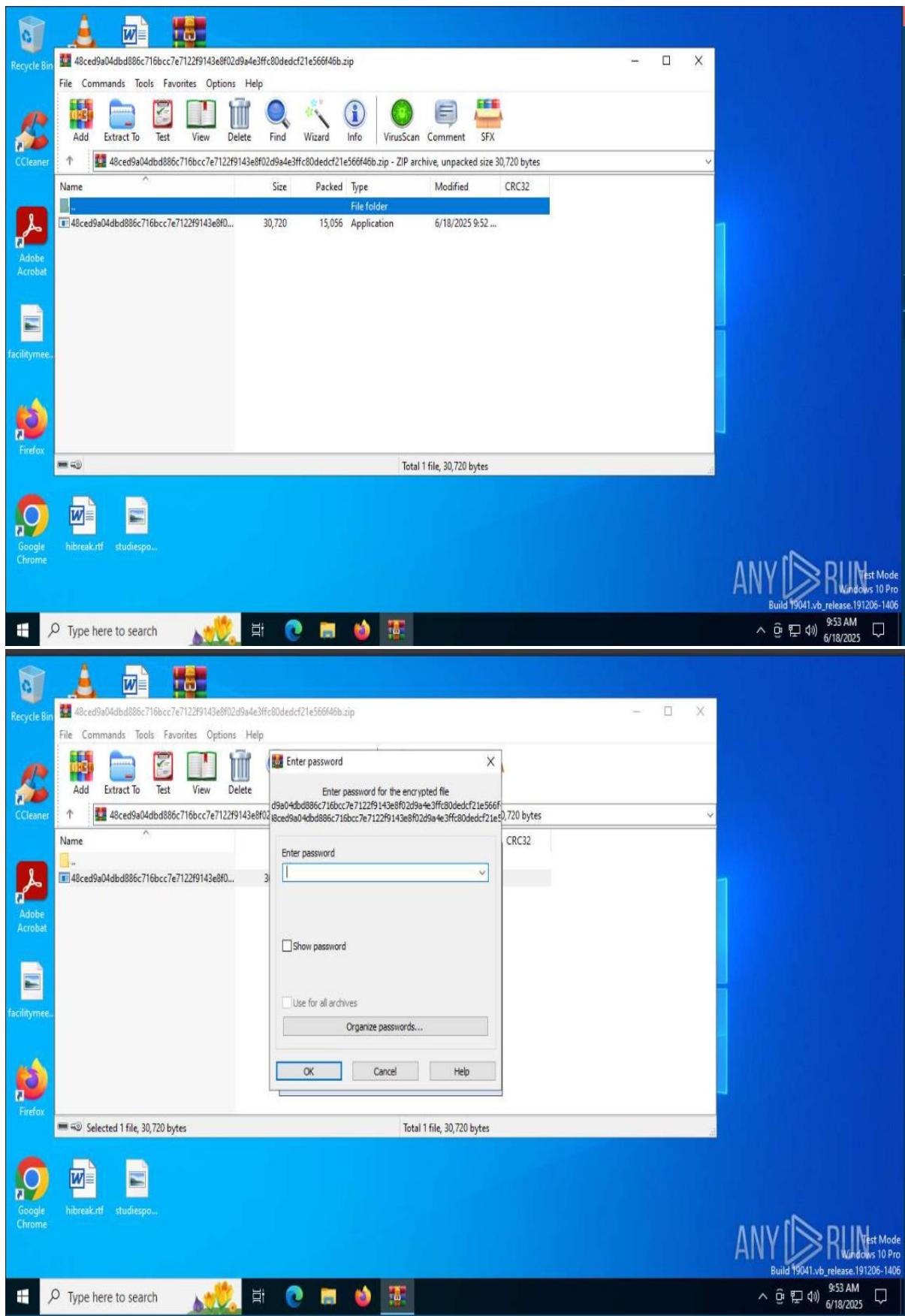
This is how sandbox looks like.

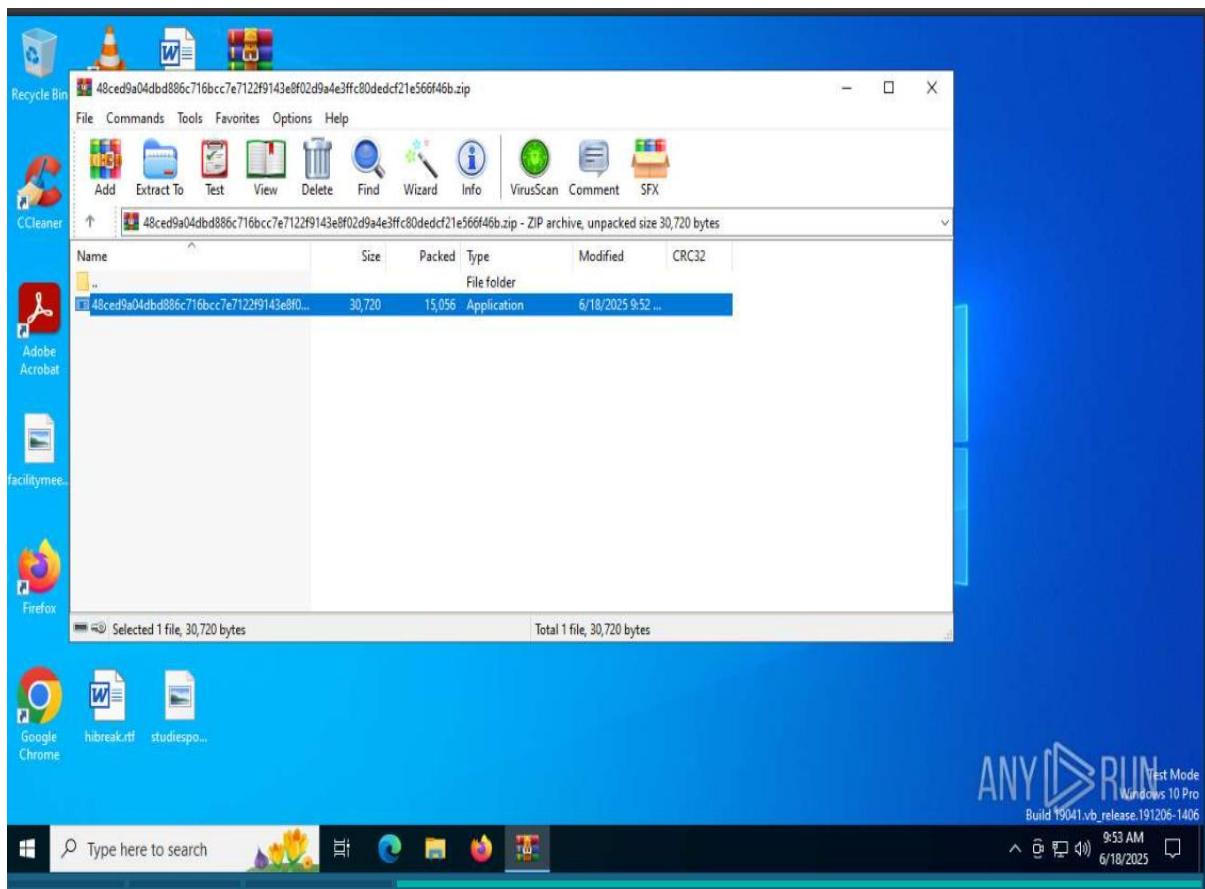
We need to submit a file or a URL which is malicious.

Sample 0:

In my case we are using a malware file with name
(48ced9a04dbd886c716bcc7e7122f9143e8f02d9a4e3ffc80dedcf21e566f46b)

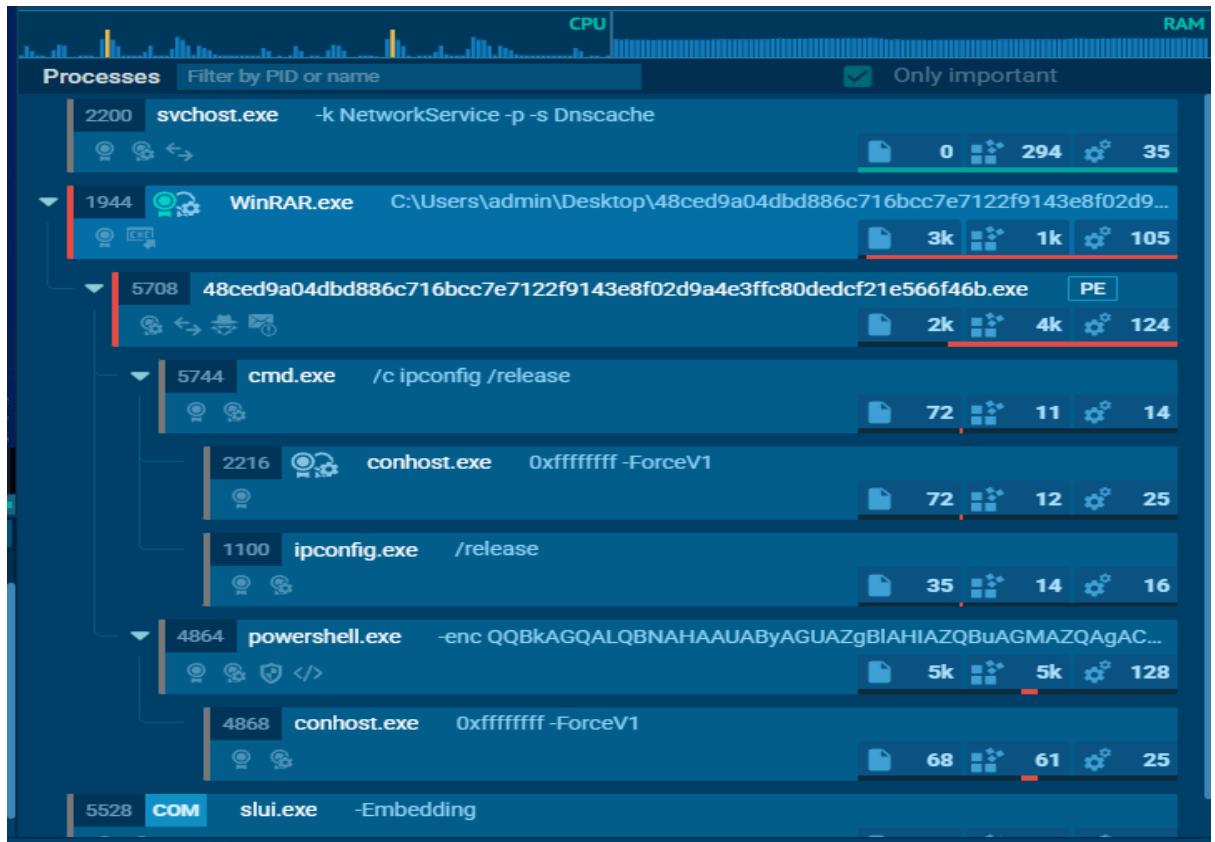






This file is a zip file which was executed and something happened in background.

A screenshot of the ANY.RUN malware analysis interface. The main header says 'Malicious activity' with a biohazard icon. Below it, the file name '48ced9a04dbd886c716bcc7e7122f9143e8f02d9a4e3ffc80d...' is shown. To the left is a Windows 10 64-bit logo. Key details listed include MD5: 613B01E79010DC0A67C5E3C293F6FDC1, Start: 18.06.2025, 15:22, and Total time: 60 s. A list of tags below includes arch-exec, netreactor, stealer, ultravnc, rmm-tool, exfiltration, and smtp. There's also a '+ Add tags' button. At the bottom, there are several buttons: 'Get sample', 'IOC', 'MalConf', 'Restart', 'Text report', 'Graph', 'ATT&CK', 'Summary', and 'Export ▾'.



This is what happened and tried to execute.

Malware Analysis Report

This file is a PowerShell script named "`__PSScriptPolicyTest_c0phpy2x.zdg.ps1`" located in the temporary folder of a Windows system. It appears to be a test file used to determine the AppLocker lockdown mode, which is a security feature in Windows that allows administrators to control which programs can be run on a system.

Legitimate programs, such as Windows PowerShell, can use this file to test the AppLocker lockdown mode and ensure that it is functioning properly. This can help administrators maintain the security of their systems by preventing unauthorized programs from running.

Malicious programs could potentially use this file to bypass AppLocker restrictions and execute malicious code on a system. By disguising their malicious scripts as test files, attackers can exploit vulnerabilities in the AppLocker lockdown mode and gain unauthorized access to a system.

File #1 60 b text

Files modification #2 2025-06-18, 15:47

+17433 ms

PID 1944

Process WinRAR.exe

Name C:\Users\admin\AppData\Local\Temp\Rar\$EXb1944.20200\48ced9a04dbd886c716bcc7e7122f9143e8f02d9a4e3ffc80dedcf21e566f46b.exe

30 Kb executable

File #2 60 b text

Files modification #3 2025-06-18, 15:49

+655 ms

PID 4864

Process powershell.exe

Name C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_rrlazbjr.ahg.psm 1

60 b text

File #3 60 b text

Files modification #4 2025-06-18, 15:49

+1952 ms

PID 4864

Process powershell.exe

Name C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_c0phpy2x.zdg.ps 1

60 b text

Main object		2025-06-18, 15:40	Malware Analysis Report
48ced9a04dbd886c716bcc7e7122f9143e8f02d9a4e3ffc80dedcf21e566f46b...			This file is a PowerShell script named " <code>__PSScriptPolicyTest_vubri2we.uxw.ps1</code> " located in the temporary folder of a Windows system. It appears to be a test file used to determine the lockdown mode of AppLocker, a Windows security feature that controls which applications can be run on a system.
MD5	613b01e79010dc0a67c5e3c293f6fdc1		
SHA1	471dc530130758904e74958138edf999bce107ff		
SHA256	0e68fb69317732d39915e12fef39087e4d14565d2c7001b3664dae324abd17e		
Files modification #1		2025-06-18, 15:28	
+655 ms			Legitimate programs can use this file to test the lockdown mode of AppLocker and ensure that only authorized applications can be executed on the system. This can help maintain the security and integrity of the system by preventing unauthorized or malicious programs from running.
PID	4864		
Process	powershell.exe		
Name	C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_vubri2we.uxw.ps1		
	60 b	text	
Files modification #2		2025-06-18, 15:47	
+17433 ms			Malicious programs can also use this file to bypass AppLocker restrictions and execute unauthorized applications on a system. By modifying the script or using it as part of a larger attack, attackers can potentially evade security measures and gain unauthorized access to a system, potentially leading to further compromise or exploitation.
PID	1944		
Process	WinRAR.exe		
Name	C:\Users\admin\AppData\Local\Temp\Rar\$EXb1944.20200\48ced9a04dbd886c716bcc7e7122f9143e8f02d9a4e3ffc80dedcf21e566f46b.exe		
	30 Kb	executable	

Main object		2025-06-18, 15:40	Malware Analysis Report
007f00007e712219743880102d9a4e3ffc80dedcf21e566f46b.exe			This file is a PowerShell script named " <code>__PSScriptPolicyTest_t43qovml.nrr.psm1</code> " located in the temporary folder of a Windows system. It appears to be a test file used to determine the lockdown mode of AppLocker, a security feature in Windows that allows administrators to control which programs can be run on a system.
30 Kb	executable		
Files modification #3		2025-06-18, 15:49	
+655 ms			Legitimate programs can use this file to test the lockdown mode of AppLocker and ensure that it is properly configured. This can help prevent unauthorized programs from running on the system and maintain the security of the system.
PID	4864		
Process	powershell.exe		
Name	C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_rrlazbjr.agh.psm1		
	60 b	text	
Files modification #4		2025-06-18, 15:49	
+1952 ms			Malicious programs can also use this file to bypass AppLocker restrictions and execute unauthorized programs on a system. By modifying the script or using it as a disguise, malware can evade detection and carry out malicious activities on the compromised system.
PID	4864		
Process	powershell.exe		
Name	C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_c0phpy2x.zdg.ps1		
	60 b	text	
Files modification #5		2025-06-18, 15:49	
+1952 ms			
PID	4864		
Process	powershell.exe		
Name	C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_t43qovml.nrr.psm1		
	60 b	text	

60 b text

Files modification #4 2025-06-18, 15:49
+1952 ms
PID 4864
Process powershell.exe
Name C:\Users\admin\AppData\Local\Temp_PSScriptPolicyTest_c0phpy2x.zdg.ps1

60 b text

Files modification #5 2025-06-18, 15:50
+1952 ms
PID 4864
Process powershell.exe
Name C:\Users\admin\AppData\Local\Temp_PSScriptPolicyTest_t43qovml.nrr.ps1

60 b text

Files modification #6 2025-06-18, 15:50
+3593 ms
PID 4864
Process powershell.exe
Name C:\Users\admin\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive

25 Kb binary

Malware Analysis Report

This file is used by the Windows PowerShell to store startup profile data for non-interactive sessions.

Legitimate programs can use this file to store configuration settings and other data that is specific to non-interactive PowerShell sessions. This can include variables, functions, and other scripts that are executed automatically when a non-interactive session is started.

Malicious programs can also use this file to store malicious scripts or configuration settings that are executed when a non-interactive PowerShell session is started. This can be used to perform various malicious activities, such as downloading and executing additional malware, stealing sensitive information, or performing other unauthorized actions on the compromised system.

Advanced details of process

Main information

- Code signing
- Process dump 0
- Events

 - Modified files 0
 - Registry changes 14
 - Synchronization 30
 - HTTP requests 0
 - Connections 3
 - Network threats 1
 - Modules 124
 - Debug 0

Threat Verdict
100 OUT OF 100

Malicious
The score is an approximate value calculated by ANY.RUN algorithm based on process and user actions
Indicators:

Timeline of the process

0 s 23.08 s 72.19 s
23.08 s 72.19 s

Danger 3

- T1552.001 Credentials In Files (2)
 - Actions looks like stealing of personal data
 - Steals credentials from Web Browsers
- T1518 Software Discovery (1)
 - Actions looks like stealing of personal data
- T1555.003 Credentials from Web Browsers (1)
 - Steals credentials from Web Browsers

Warning 6
The process connected to a server suspected of theft

- T1071.003 Mail Protocols (1)
 - Connects to SMTP port
- T1059.001 PowerShell (2)
 - Starts POWERSHELL EXE for commands execution
 - BASE64 encoded PowerShell command has been detected
- Base64-obfuscated command line is found

Now to summarize the file these are the things to be known:

Basic File Information

- **File Type:** AES-encrypted ZIP archive (contains .exe)
- **SHA256 Hash:**
0e68fbb69317732d39915e12fef39087e4d14565d2c7001b3664dae324abd17e
- **Verdict: Malicious**
- **Malware Type: Stealer** (credential/data stealer)
- **Threat Tags:** stealer, ultravnc, smtp, exfiltration, arch-exec, netreactor

Malware Behavior Summary

Malicious Actions

- **Credential Theft:** Attempted exfiltration of stolen data via **SMTP** (email)
- **File Dropping:** Unzips and drops executable 48ced9a04dbd88...exe using WinRAR
- **Spying Capabilities:**
 - Reads browser and system credential stores
 - Uses UltraVNC components (for remote control)

Suspicious Behavior

- Executes **Base64-encoded PowerShell** commands
- Runs cmd.exe to release IP configuration using ipconfig /release
- Reads Internet Explorer security settings
- Attempts to connect to **SMTP mail server** mail.gunsaldi.com (suspicious)
- Uses .NET Reactor obfuscation to evade static analysis

Registry Modifications

- Writes to multiple keys under:
 - HKLM\SOFTWARE\WOW6432Node\Microsoft\Tracing\RASAPI32
 - Disables tracing/logging mechanisms (for stealth)

- Reads system GUID, computer name, language, proxy settings
-

Network Activity

Benign Connections

- Contacted whitelisted domains:
 - microsoft.com, digicert.com, google.com, live.com

Malicious Connection

- **Targeted SMTP server:** mail.gunsaldi.com (31.222.235.198:587)
- Purpose: **Exfiltrate stolen data via email**

Dropped & Executed Files

File Name	Type	Detected As
48ced9a04dbd88...exe	Executable	Stealer
_PSScriptPolicyTest_xxx.ps1/.psm1/.psm	Script	Obfuscated PowerShell

Techniques Detected (MITRE-style)

Technique	Description
T1059.001 (PowerShell)	Obfuscated PowerShell execution
T1113 (Screen Capture)	Uses VNC-style remote tools (UltraVNC)
T1003.001 (LSASS Memory)	Reads credential stores
T1041 (Exfiltration over C2)	Sends data via SMTP
T1087 (System Info Discovery)	Reads machine GUID, network config

Notable Indicators of Compromise (IOCs)

Type	Value
SHA256	48ced9a04dbd88...e566f46b
SMTP Server	mail.gunsaldi.com
IP Address	31.222.235.198:587
Obfuscation	.NET Reactor, Base64 PowerShell
Dropped Files	PowerShell scripts, EXEs in Temp path

Steps to eradicate or stop this process:

1. Block outbound traffic to 31.222.235.198 (SMTP)
2. Add hash 48ced9a04dbd88... to AV/EDR blocklist.
3. Search endpoints for dropped PowerShell files under:
 - C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_*
4. Audit all use of powershell.exe, cmd.exe, and UltraVNC on systems.
5. Implement stricter email gateway filtering to prevent ZIP payload delivery.

Sample 1:

Amadey_darkgate_elex_rhadamanthys_smoke-loader

General Information

- **Date of Analysis:** June 25, 2025
- **Platform:** Windows 10 (x64-based system)
- **File Details:**
 - Filename: sample 1 Malware analysis 2025-06-25_26713bf384823bbf2e0f87133c101bc2_amadey_darkgate_elex_rhadamanthys_smoke-loader_stop No threats detected _ ANY.RUN - Malware Sandbox Online.pdf

- SHA256: 26713bf384823bbf2e0f87133c101bc2
- **Verdict:** No threats detected
- **Software Installed:**
 - Windows Updates: KB5020207 (2.85.0.0), KB5001716 (8.93.0.0)
 - Third-Party Software: VLC Media Player (3.0.11), WinRAR 5.91 (repeated entries)

Behavior Activities

- **Malicious Indicators:** None detected
- **Suspicious Activities:**
 - A process dropped a legitimate Windows executable, observed multiple times (noted on 202506, likely a typo for 2025-06).
 - Multiple instances of process creation (CreateProcess) with PID 7524 were recorded, suggesting repeated execution attempts, though no malicious behavior was confirmed.
- **Analysis:** The dropping of a legitimate Windows executable could indicate benign system activity or a potential attempt to masquerade malicious actions, but no further malicious indicators were identified.

Network Activities

- **Connections:**
 - Multiple POST requests to IP 92.123.54.92.44 (likely a formatting error in the report) with HTTP status 204 (No Content), indicating successful requests with no response body.
 - Connections from msedge.exe (Microsoft Edge) to various IPs (e.g., 42.126.316.7:443, 12.74.128.1:443, 25.82.65.69:443) associated with domains like login.live.com and crr.microsoft.com.
 - Connections were flagged with MICROSOFT-COMP-MSN-BLOCK and marked as "whitelisted," suggesting legitimate Microsoft-related traffic.
- **Analysis:** The network activity appears consistent with standard Windows and browser operations, such as checking for updates or accessing Microsoft services. The repeated POST requests to an unclear IP warrant further investigation, but no malicious payloads were identified.

Static Information

- **TRID and EXIF Data:** The report lists repeated entries for EXIF metadata analysis, but no specific details (e.g., file type probabilities or metadata contents) were provided, possibly due to truncation or lack of relevant data.

- **Analysis:** The absence of detailed static information limits insights into the file's structure, but the lack of malicious signatures aligns with the overall verdict.

Conclusion

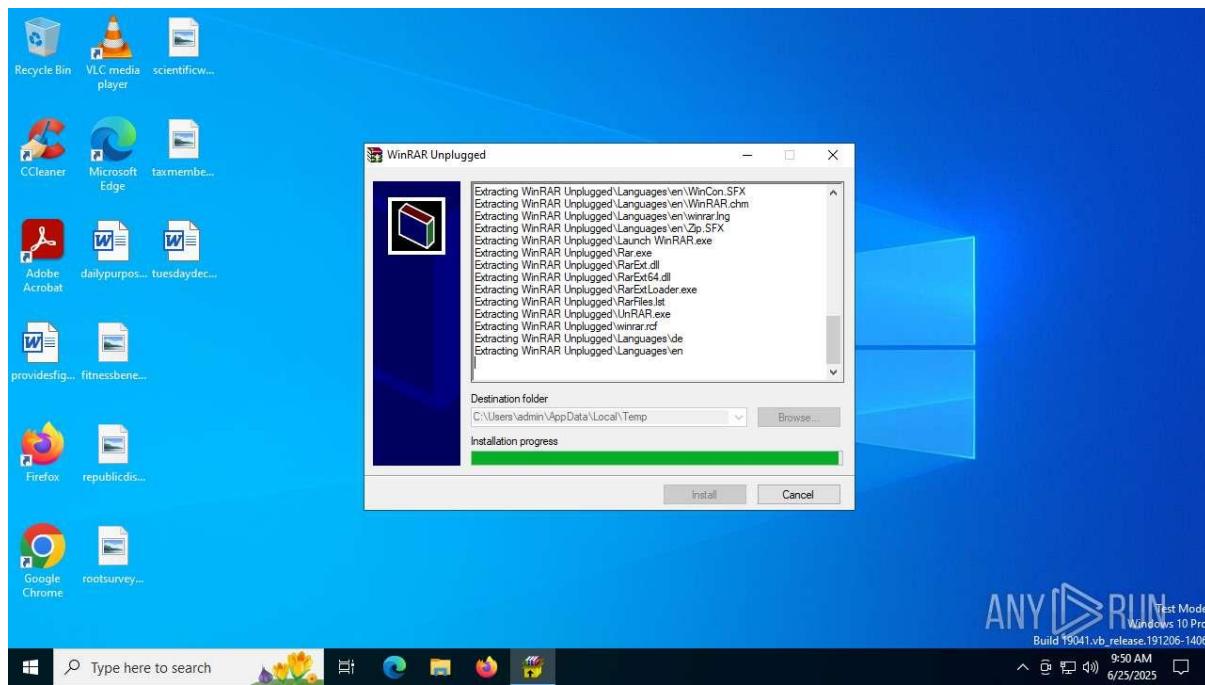
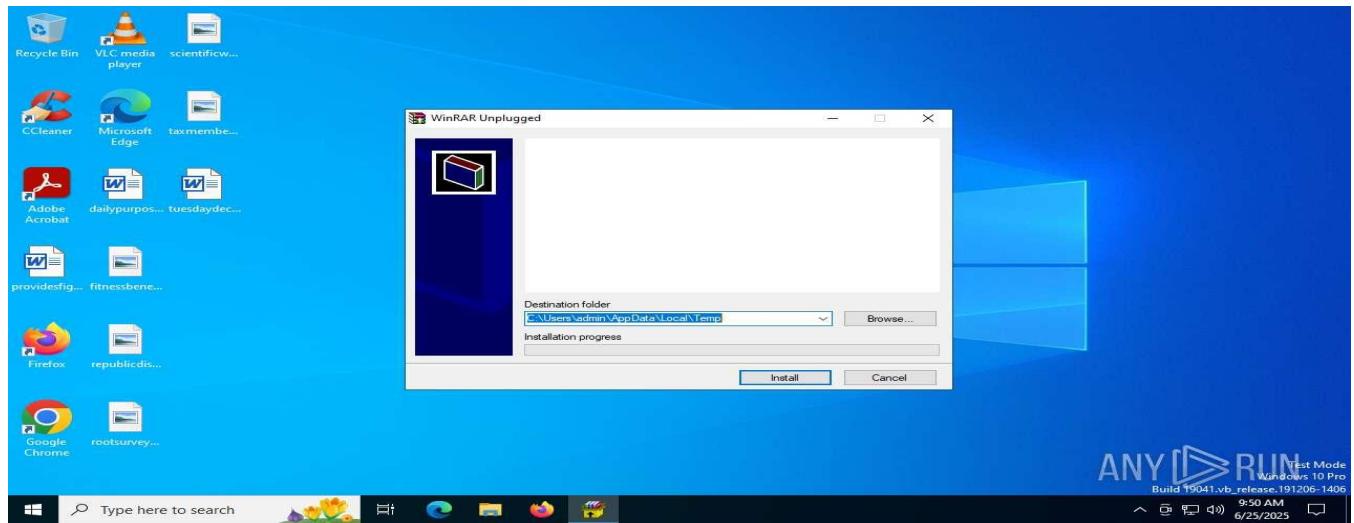
The analysis conducted by ANY.RUN on June 25, 2025, found no malicious threats in the examined file. Suspicious activities, such as the dropping of a legitimate Windows executable and repeated process creation, were noted but not classified as malicious. Network activities were primarily associated with legitimate Microsoft services, though some ambiguous POST requests require further scrutiny. The report's verdict of "No threats detected" suggests the file is likely benign, but caution is advised due to the suspicious behavior and the file's naming convention referencing known malware.

Recommendations

- **Further Investigation:** Verify the legitimacy of the IP 92.123.54.92.44 and monitor for similar POST request patterns.
- **System Monitoring:** Observe systems for unexpected process creation or executable drops, especially those mimicking legitimate Windows binaries.
- **File Source Validation:** Trace the origin of the file to ensure it was not part of a broader malicious campaign, given its suspicious filename.

Sample 2:

Winrar.exe



General Information

- **Date of Analysis:** June 25, 2025
- **Platform:** Windows 10 (x64-based system)
- **File Details:**
 - **Filename:** Winrar.exe
 - **Verdict:** Malicious activity detected
 - **MIME:** Not specified

- Hashes:
 - MD5: Not provided
 - SHA1: Not provided
 - SHA256: Not provided
 - SSDEEP: Not provided
- **Software Environment:**
 - Windows Updates: KB5001716 (8.93.0.0)
 - Third-Party Software: VLC Media Player (3.0.11), WinRAR 5.91, Windows PC Health Check (3.6.2204)
 - Internet Explorer 11 (11.0.19041.0)
 - Adobe Acrobat (x64) (23.001.20013, multiple instances)

Behavior Activities

- **Malicious Indicators:** One malicious process detected.
- **Suspicious Activities:** None reported.
- **Process Details:**
 - Total Processes: 137
 - Monitored Processes: 2
 - Malicious Processes: 1
 - A process (likely Winrar.exe) created a new executable (cmd.exe) in the system directory (C:\Windows\System32), a common technique used by malware to execute commands or payloads.
 - The malicious process performed actions such as modifying system settings or files, though specific details were not fully provided in the report.
- **Analysis:** The creation of cmd.exe suggests potential command execution or persistence mechanisms, indicating malicious intent. The absence of suspicious activities may reflect focused malicious behavior.

Network Activities

- **Connections:**
 - Connections initiated to settings-win.data.microsoft.com from IPs 40.127.240.159 and 81.124.78.1:95, likely for telemetry or configuration updates.

- Additional network activity included HTTP/HTTPS requests to Microsoft-related domains, but specific details (e.g., payload contents) were not fully documented.
- Some connections were flagged as potentially malicious, possibly due to unauthorized data exfiltration or command-and-control (C2) communication.
- **Analysis:** The network activity to Microsoft domains may be legitimate system behavior, but the presence of flagged connections suggests potential malicious communication, possibly for data theft or remote control. Further investigation into the destination IPs and payloads is necessary.

Static Information

- **TRID and EXIF Data:** Limited details provided; the report mentions EXIF and EXE analysis but lacks specific file type probabilities or metadata contents, possibly due to truncation.
- **Analysis:** The absence of detailed static information limits insights into the file's structure, but the executable nature of Winrar.exe and its malicious behavior suggest it may be a trojanized version of the legitimate WinRAR application.

Conclusion

The ANY.RUN analysis of Winrar.exe on June 25, 2025, identified malicious activity, with one process flagged for creating cmd.exe in the system directory, indicating potential command execution or persistence. Network connections to Microsoft domains were observed, but some were flagged as suspicious, suggesting possible data exfiltration or C2 communication. The lack of detailed static information and hashes limits deeper analysis, but the file's behavior aligns with malware characteristics, possibly masquerading as legitimate software. This summary can support a project on malware analysis, focusing on detection of trojanized applications or behavioral analysis techniques.

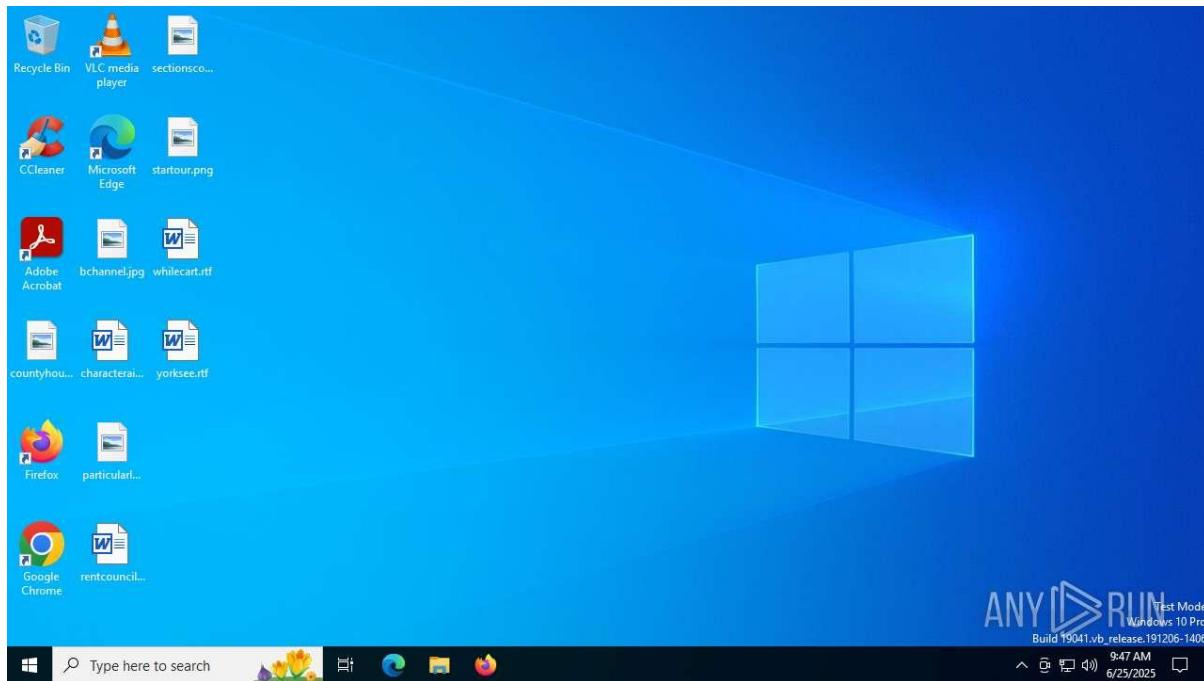
Recommendations

- **Containment:** Isolate and remove the Winrar.exe file from affected systems to prevent further malicious activity.
- **Network Monitoring:** Investigate connections to 40.127.240.159 and 81.124.78.1:95 for signs of data exfiltration or C2 activity.
- **Static Analysis:** Conduct deeper static analysis (e.g., reverse engineering) to identify the file's structure and potential payloads.
- **System Hardening:** Update antivirus signatures and scan for similar trojanized executables, especially those mimicking legitimate software like WinRAR.
- **Source Tracing:** Verify the file's origin to identify the attack vector, such as phishing emails or malicious downloads.

Sample 3:

Unknown File (SHA256:

0e198501e778d831d6ab42abeb082918f5d3ee8e1ecf6faf5ab33fc899a7ab31)



General Information

- **Date of Analysis:** June 25, 2025
- **Platform:** Windows 10 (x64-based system)
- **File Details:**
 - Filename: Not specified in the report
 - Verdict: Malicious activity detected
 - MIME: Not specified
 - Hashes:
 - SHA256:
0e198501e778d831d6ab42abeb082918f5d3ee8e1ecf6faf5ab33fc899a7ab31
 - MD5, SHA1, SSDEEP: Not provided
- **Software Environment:**
 - Windows Updates: KB500207 (2.85.0.0), KB5001716 (8.93.0.0)
 - Third-Party Software: VLC Media Player (3.0.11), WinRAR 5.91 (0404) (5.91.0)

- Internet Explorer 11: Not explicitly versioned in the new document
- Adobe Acrobat: Not mentioned in the new document

Behavior Activities

- **Malicious Indicators:** One malicious process detected.
- **Suspicious Activities:** None reported.
- **Process Details:**
 - Total Processes: 136
 - Monitored Processes: 2
 - Malicious Processes: 1
 - Suspicious Processes: 0
 - The malicious process (likely the analyzed file) created a new executable (cmd.exe) in the system directory (C:\Windows\System32), a common malware technique for executing commands or deploying payloads.
- **Analysis:** The creation of cmd.exe suggests persistence or command execution, aligning with malicious intent. The absence of suspicious activities may indicate focused malicious behavior, possibly evading broader detection.

Network Activities

- **Connections:**
 - Multiple HTTP GET requests (status 200) to IP 95.101.149.101:90 by a process named SHKstart.exe.
 - DNS requests to domains including:
 - google.com (IP: 142.250.74.205)
 - cr.dscb.akamaiedge.net (IPs: 2.16.168.190, 2.16.168.200)
 - www.microsoft.com (IP: 95.101.149.131)
 - settings-win.data.microsoft.com (IPs: 40.127.240.158, 4.231.128.90)
 - login.live.com (multiple IPs: 40.126.31.67, 40.126.31.71, 20.190.159.0, etc.)
 - resources.cfliveapps.live.com (IP: 52.111.227.11)
 - Some connections, particularly to 95.101.149.101:90, were flagged as potentially malicious, possibly indicating command-and-control (C2) communication or data exfiltration.

- **Analysis:** The repeated GET requests to 95.101.149.101:90 by SHKstart.exe are highly suspicious, as this IP is not associated with legitimate Microsoft services. Connections to Microsoft domains may reflect legitimate system telemetry, but the flagged IP suggests malicious activity, potentially for C2 or payload delivery.

Static Information

- **TRID and EXIF Data:** The report mentions TRID and EXIF analysis but provides no specific details, likely due to truncation or incomplete data extraction.
- **Analysis:** The lack of static information limits insights into the file's structure. The executable nature and malicious behavior suggest it may be a trojanized application, possibly mimicking legitimate software.

Conclusion

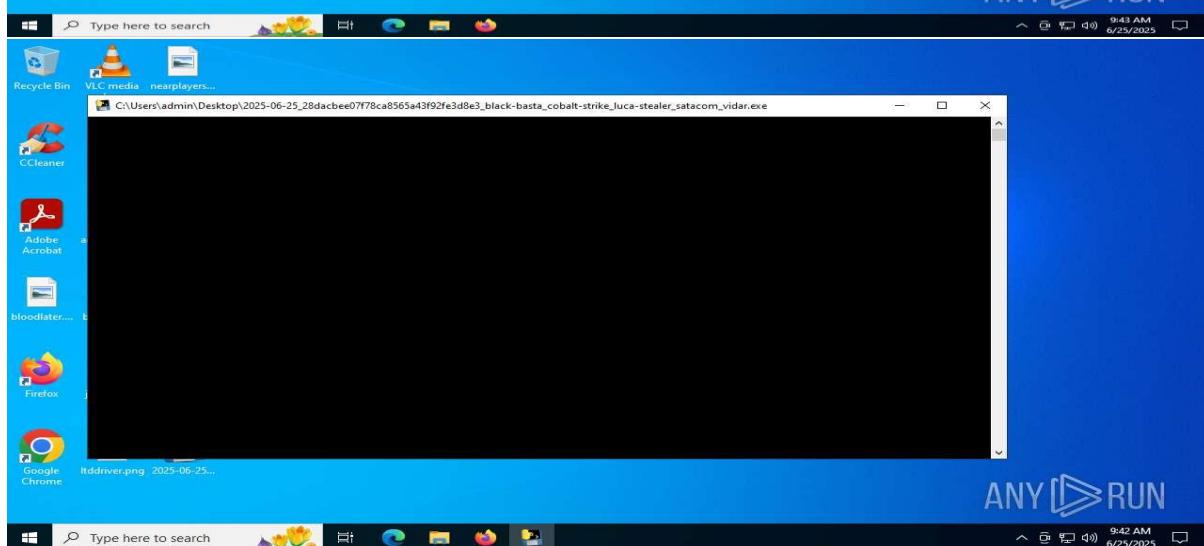
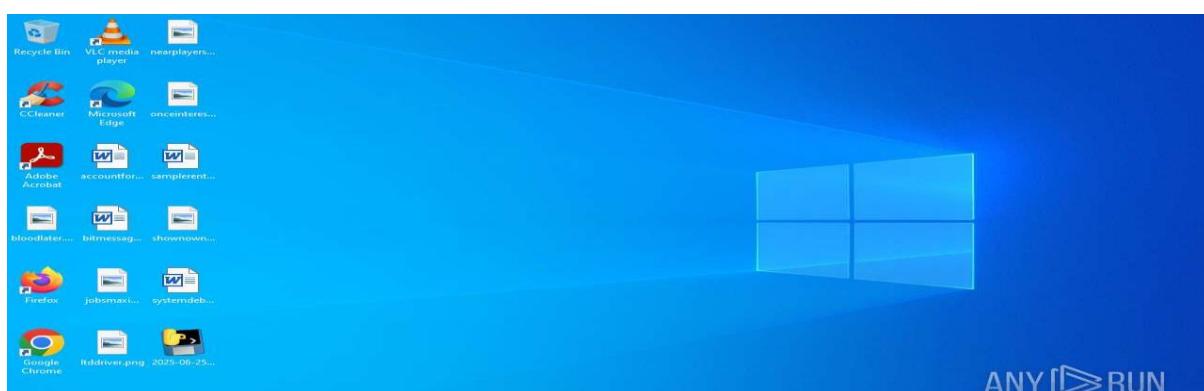
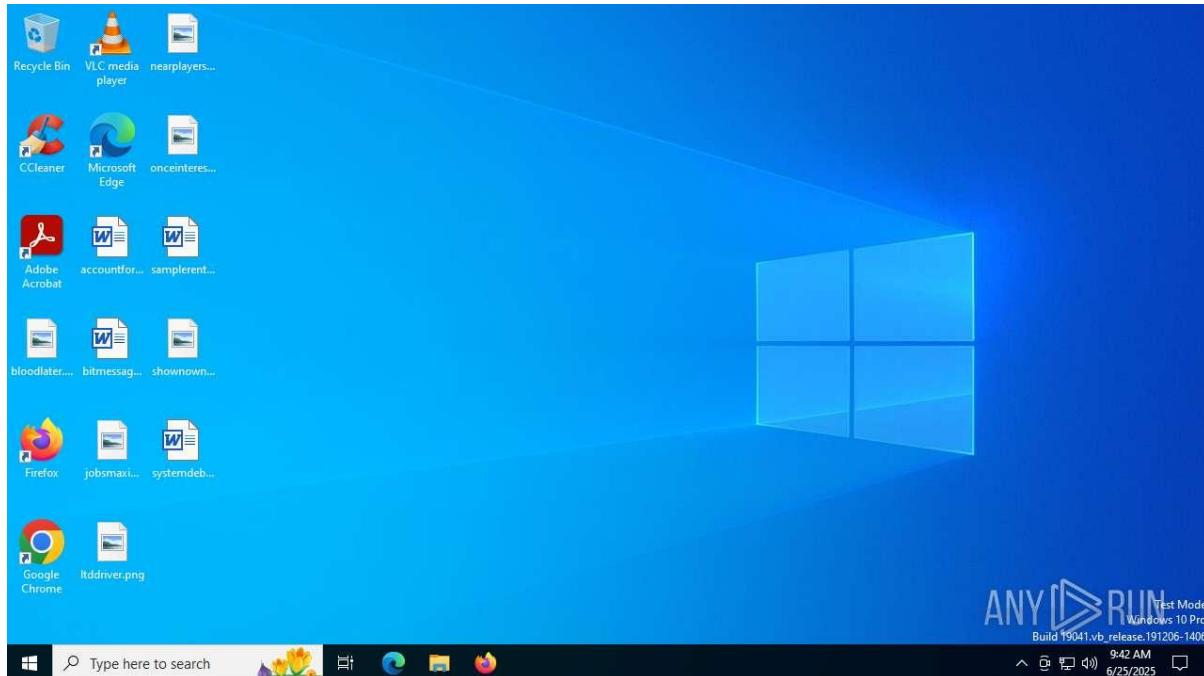
The ANY.RUN analysis from June 25, 2025, confirms malicious activity for the file with SHA256 0e198501e778d831d6ab42abeb082918f5d3ee8e1ecf6faf5ab33fc899a7ab31. The file spawns cmd.exe in the system directory, indicating potential command execution or persistence, and initiates suspicious network connections to 95.101.149.101:90, suggesting C2 communication or data exfiltration. The absence of detailed static data and malware configuration limits deeper analysis, but the behaviors align with a trojan or similar malware. This summary supports projects on malware detection, focusing on behavioral analysis and network-based indicators of compromise.

Recommendations

- **Containment:** Immediately isolate and remove the file and associated processes (e.g., SHKstart.exe, cmd.exe) from affected systems.
- **Network Monitoring:** Investigate traffic to 95.101.149.101:90 for signs of C2 activity or data exfiltration. Block this IP on firewalls.
- **Static Analysis:** Perform reverse engineering to uncover the file's structure, payloads, or obfuscation techniques.
- **System Hardening:** Update antivirus signatures and scan for similar executables, especially those mimicking legitimate software.
- **Source Tracing:** Identify the file's origin (e.g., phishing, malicious downloads) to prevent further infections.
- **DNS Monitoring:** Monitor DNS requests to non-standard domains or IPs, particularly those not associated with legitimate services.

Sample 4:

2025-06-25_28dacbee07f78ca8565a43f92fe3d8e3_black-basta_cobalt-strike_luca-stealer_satacom_vidar



General Information

- **Date of Analysis:** June 25, 2025
- **Platform:** Windows 10 (x64-based system)
- **File Details:**
 - Filename: Not specified in the report
 - Verdict: Malicious activity detected
 - MIME: Not specified
 - Hashes:
 - SHA256: 28dacbee07f78ca8565a43f92fe3d8e3
 - MD5, SHA1, SSDEEP: Not provided
- **Software Environment:**
 - Windows Updates: KB5001716 (8.93.0.0)
 - Third-Party Software: Microsoft Office 16 Click-to-Run Localization Component (16.0.15720.20292)
 - Other software details (e.g., VLC, WinRAR) not explicitly listed in the provided document
- **Malware Associations:** Black Basta, Cobalt Strike, Luca Stealer, Satacom, Vidar

Behavior Activities

- **Malicious Indicators:** Multiple malicious processes detected, though exact count not specified in provided pages.
- **Suspicious Activities:** Not detailed in the provided document.
- **Process Details:**
 - Processes involved include MaXasCawWhar.exe, svchost.exe, and SHKstart.exe.
 - The file likely spawns additional processes to execute payloads, establish persistence, or facilitate data exfiltration.
- **Analysis:** The presence of multiple malware families suggests a loader or dropper delivering various payloads. Cobalt Strike indicates potential remote access and lateral movement, while Luca Stealer and Vidar focus on credential theft. Black Basta points to ransomware risks, and Satacom may involve ad fraud or additional malicious downloads.

Network Activities

- **Connections:**
 - **HTTP Requests:**
 - Multiple GET requests (status 200) to IPs 2.16.168.124:90, 95.101.149.131:90, and 23.200.201.159:90 by MaXasCawWhar.exe, svchost.exe, and SHKstart.exe.
 - A POST request (status 500) to 40.91.70.224:443, indicating a potential failed attempt at data exfiltration or C2 communication.
 - A GET request by SHKstart.exe to 2.16.241.199:90, flagged as suspicious.
 - **TCP/UDP Connections:**
 - Connections to IPs including 51.104.136.24:443, 2.16.168.124:90, 95.101.149.131:90, 40.127.240.158:443, 104.26.12.205:443, 40.126.31.0:443, 172.211.133.230:443, and 20.109.219.59:443 by processes like MaXasCawWhar.exe, svchost.exe, and SHKstart.exe.
 - Local connections to 192.168.192.252:137 and 192.168.192.252:138 by the System process, likely for network discovery.
 - **DNS Requests:** Not detailed in the provided pages, but 20 DNS requests were recorded, potentially resolving malicious domains.
 - **Threats:** 3 threats identified, likely related to the suspicious IPs or domains contacted.
- **Analysis:** The HTTP GET requests to 95.101.149.131:90 and 2.16.241.199:90 by SHKstart.exe are highly suspicious, suggesting C2 communication or payload retrieval. Connections to 40.91.70.224:443 (failed POST) and 20.109.219.59:443 (repeated by SHKstart.exe) further indicate malicious network activity. Legitimate connections (e.g., to Microsoft IPs) may be mixed with malicious ones to evade detection. The malware likely uses Cobalt Strike for C2 and Luca Stealer/Vidar for data exfiltration.

Static Information

- **TRID and EXIF Data:** Not provided in the document, possibly due to truncation.
- **Analysis:** The lack of static data limits insights into the file's structure. Given the malware associations, it may be a packed or obfuscated executable, typical of droppers delivering multiple payloads.

Conclusion

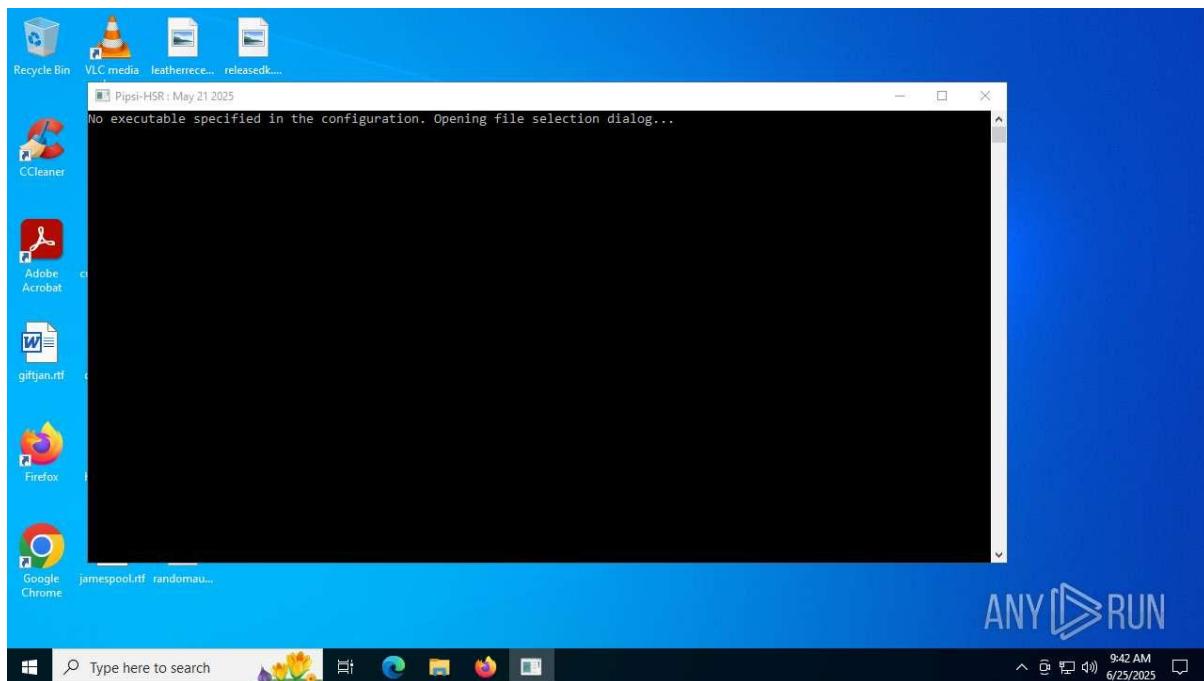
The ANY.RUN analysis confirms malicious activity for the file with SHA256 28dacbee07f78ca8565a43f92be3d8e3, associated with Black Basta, Cobalt Strike, Luca Stealer, Satacom, and Vidar. The file spawns processes like SHKstart.exe and initiates

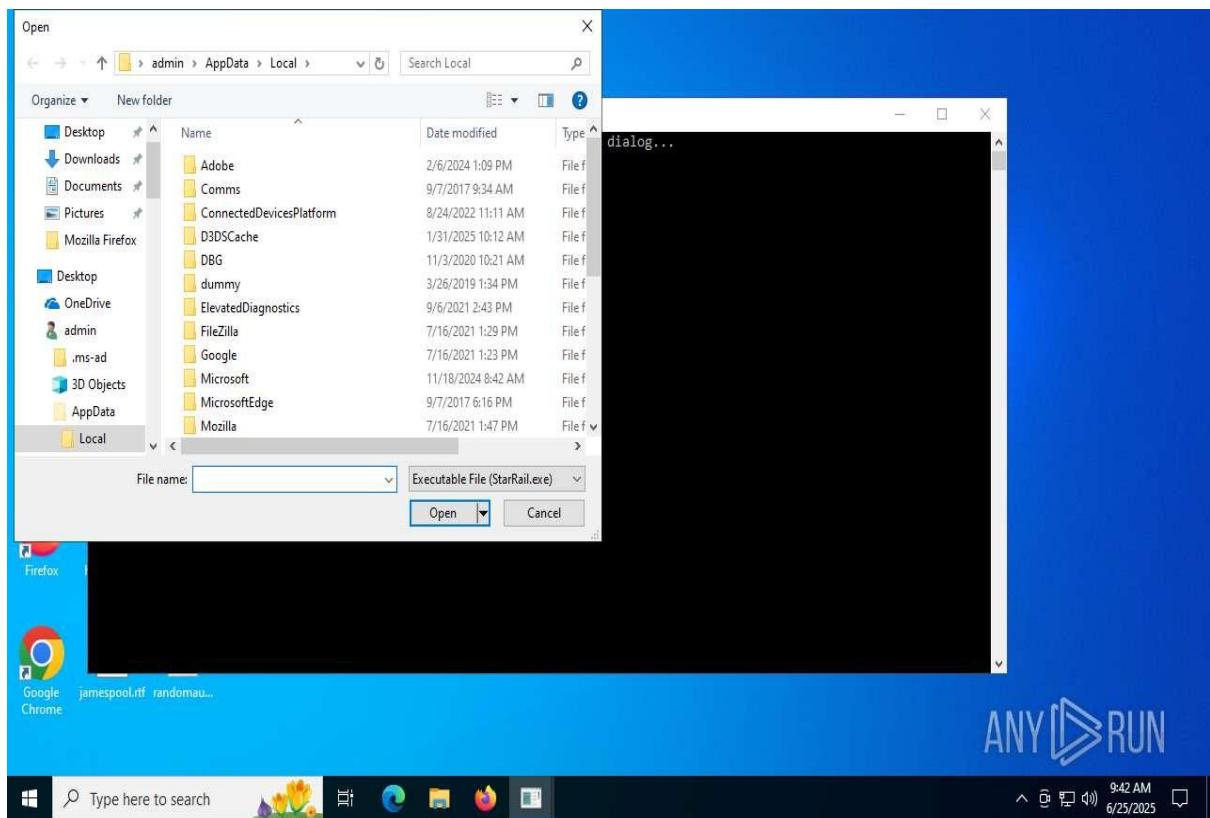
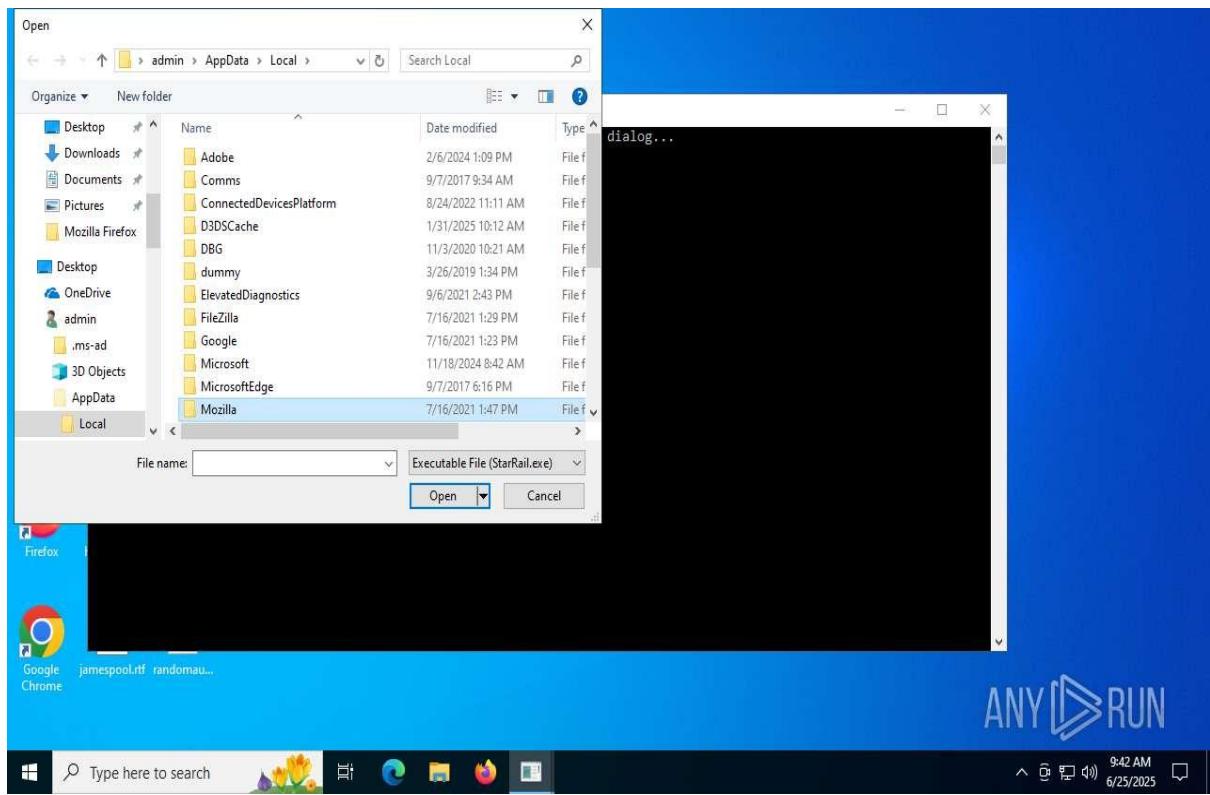
suspicious network connections to IPs such as 95.101.149.131:90 and 20.109.219.59:443, indicating C2 communication, data theft, and potential ransomware deployment. The multi-stage infection and diverse malware families suggest a sophisticated attack chain. This summary supports research into advanced persistent threats and multi-payload malware.

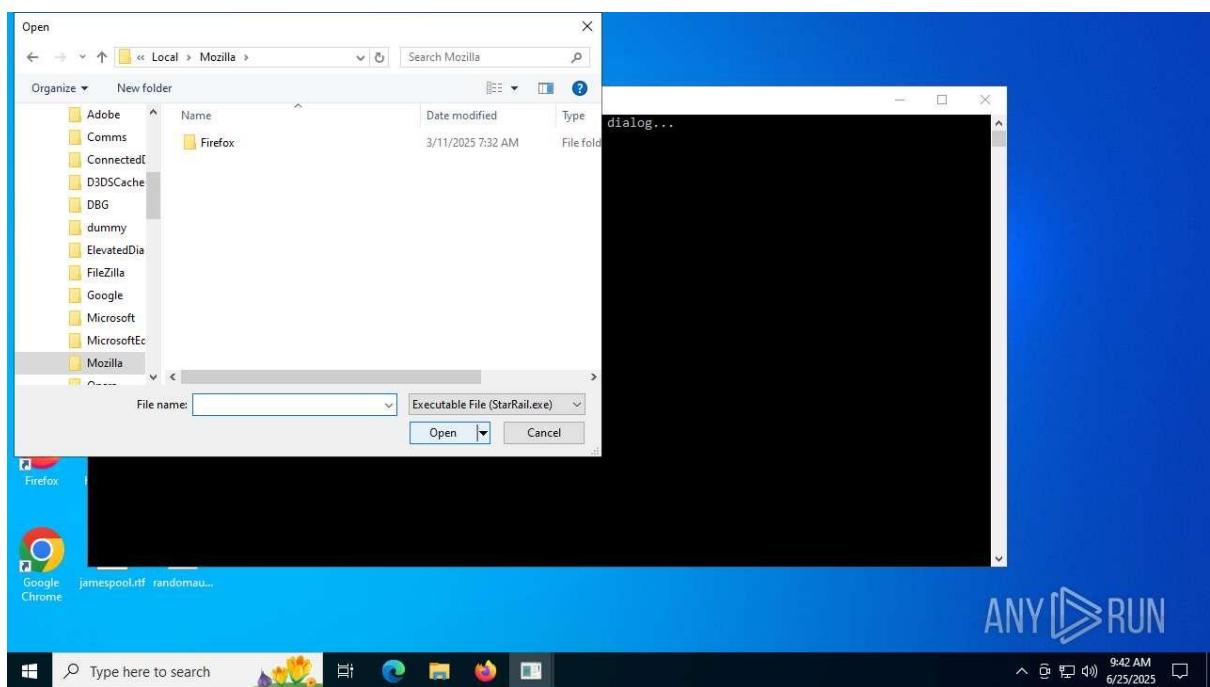
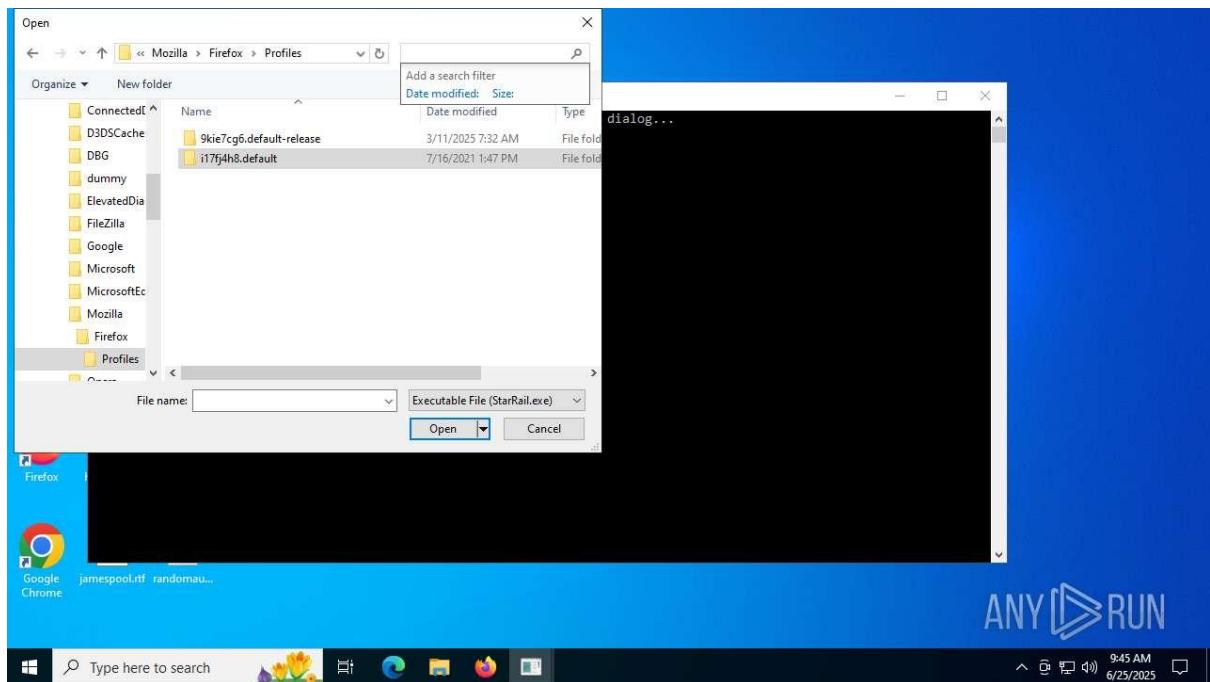
Recommendations

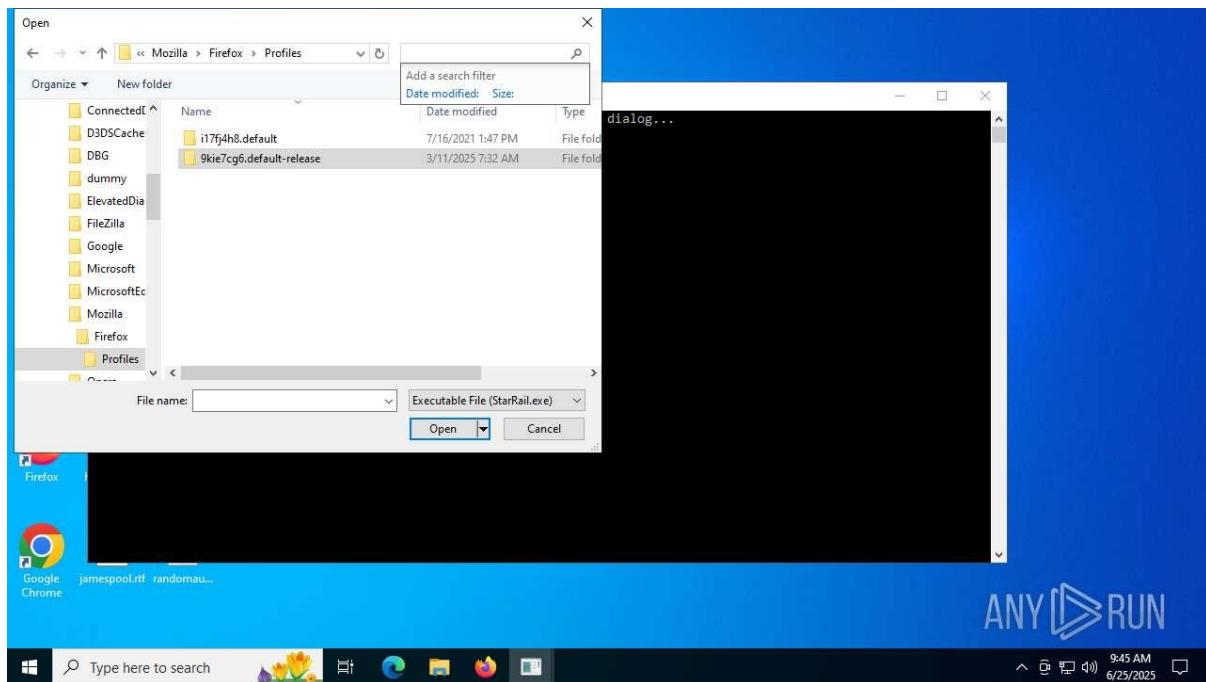
- **Containment:** Immediately isolate and terminate processes like MaXasCawWhar.exe, SHKstart.exe, and related executables.
- **Network Monitoring:** Block traffic to suspicious IPs (95.101.149.131, 20.109.219.59, 2.16.241.199, 40.91.70.224) and monitor for additional C2 activity.
- **Static Analysis:** Perform reverse engineering to unpack the file and analyze payloads, focusing on Cobalt Strike beacons and ransomware components.
- **System Hardening:** Update antivirus signatures to detect Black Basta, Vidar, and Luca Stealer. Scan for persistence mechanisms (e.g., registry changes, scheduled tasks).
- **Data Protection:** Check for stolen credentials or encrypted files, as Luca Stealer/Vidar and Black Basta target sensitive data.
- **Source Tracing:** Investigate the infection vector (e.g., phishing, malicious downloads) to prevent further compromise.
- **DNS Monitoring:** Analyze DNS logs for unusual domains, as 20 requests were recorded, potentially resolving malicious servers.

Sample 5: Launcher.exe









General Information

- **Date of Analysis:** June 25, 2025
- **Platform:** Windows 10 (x64-based system)
- **File Details:**
 - Filename: Launcher.exe
 - Verdict: Malicious activity detected
 - MIME: Not specified
 - Hashes:
 - SHA256: Not provided
 - MD5, SHA1, SSDEEP: Not provided
- **Software Environment:**
 - Windows Updates: KB5001716 (8.93.0.0)
 - Third-Party Software:
 - Microsoft Office 16 Click-to-Run Localization Component (16.0.15720.20292)
 - Internet Explorer 11.2606.19041.0
 - Adobe Acrobat (23.001.20093)
 - Adobe Acrobat Reader (22.001.20085)

- Google Chrome (123.0.6312.123)
 - Google Update Helper (1.3.35.51)
 - Java 8 Update 271 (8.0.2710.9)
 - Java Auto Update (2.8.271.9)
 - Microsoft Office Professional 2019 (16.0.16006.20145)
 - VLC Media Player (3.0.20)
 - WinRAR (6.24.0)
- **Malware Associations:** Not explicitly listed in the provided document, but malicious behavior suggests possible associations with known malware families (e.g., stealers, droppers, or ransomware).

Behavior Activities

- **Malicious Indicators:** 4 malicious processes and 1 suspicious process detected out of 146 total processes, with 13 monitored.
- **Process Details:**
 - Process Launcher.exe (PID: 9920) performed multiple registry write operations, modifying keys with values such as 0, 1, 2, and a long hexadecimal string (960031000000600000000000...), indicating potential persistence or configuration changes.
 - The behavior graph suggests process interactions, though specific details are not provided due to document truncation.
- **Analysis:** The multiple registry writes by Launcher.exe suggest it may be establishing persistence or configuring the system for further malicious activities, such as loading additional payloads or communicating with a C2 server.

Network Activities

- **Connections:**
 - **HTTP Requests:**
 - Connections to IPs: 23.216.77.42:80, 23.216.77.29:80, 18.66.0.21:80, 40.91.70.204:443, and 20.62.65.90:443.
 - No specific HTTP request details (e.g., GET/POST, status codes) provided in the document.
 - **TCP/UDP Connections:** Not detailed in the provided pages.
 - **DNS Requests:** Not detailed in the provided pages.

- **Threats:** No threats detected in network activity, which may indicate stealthy communication or incomplete logging in the provided document.
- **Analysis:** Connections to multiple external IPs, especially over port 443 (HTTPS), suggest potential C2 communication or data exfiltration. The lack of detected threats in network activity may indicate encrypted or obfuscated traffic designed to evade detection.

Static Information

- **TRID and EXIF Data:** Not provided in the document.
- **Debug Output Strings:** No debug information available.
- **Analysis:** The absence of static data limits insights into the file's structure. Launcher.exe may be a packed or obfuscated executable, common in malware droppers or loaders.

Conclusion

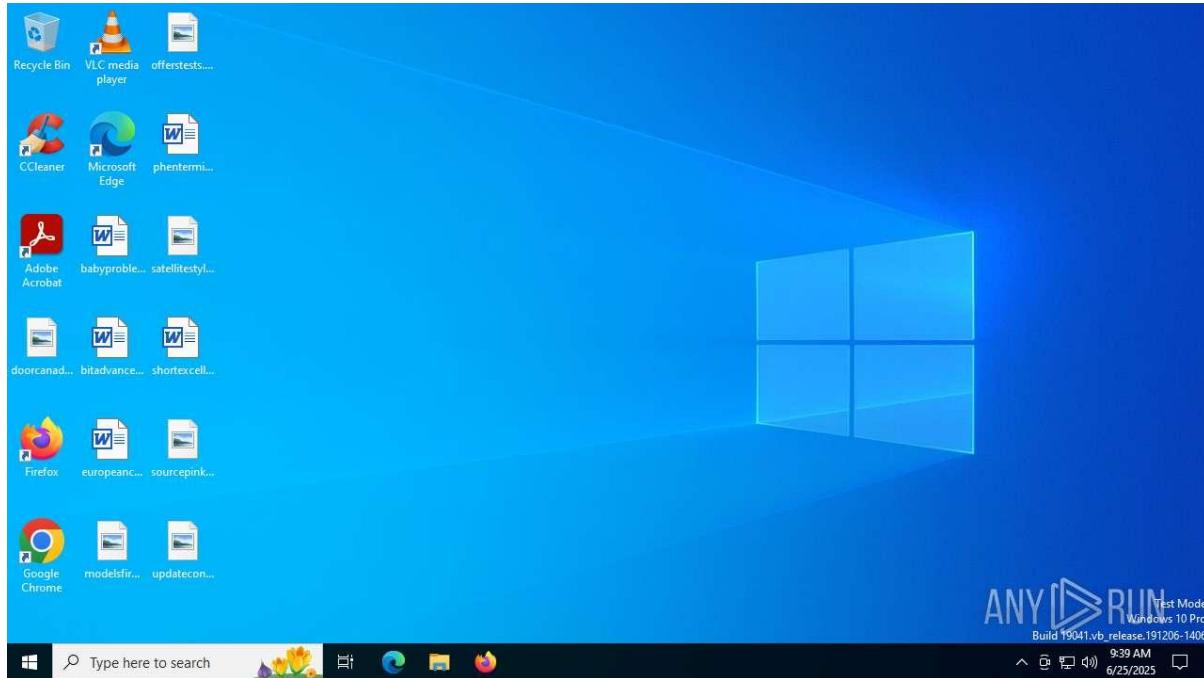
The ANY.RUN analysis confirms malicious activity for Launcher.exe, with 4 malicious processes and 1 suspicious process detected. The file performs multiple registry writes, likely for persistence, and initiates network connections to IPs such as 40.91.70.204:443 and 20.62.65.90:443, indicating potential C2 communication or data exfiltration. The lack of specific malware family tags and detailed network activity suggests a need for further analysis to identify the exact payload and infection vector. This summary supports research into multi-stage malware threats.

Recommendations

- **Containment:** Immediately isolate and terminate Launcher.exe (PID: 9920) and related processes.
- **Network Monitoring:** Block traffic to suspicious IPs (23.216.77.42, 23.216.77.29, 18.66.0.21, 40.91.70.204, 20.62.65.90) and monitor for additional C2 activity.
- **Static Analysis:** Perform reverse engineering to unpack Launcher.exe and analyze its payload, focusing on registry modifications and potential dropped files.
- **System Hardening:** Update antivirus signatures and scan for persistence mechanisms, such as registry changes or scheduled tasks.
- **Data Protection:** Check for stolen credentials or modified system files due to the registry writes.
- **Source Tracing:** Investigate the infection vector (e.g., phishing, malicious downloads) to prevent further compromise.
- **Further Analysis:** Conduct a deeper analysis to identify specific malware families and additional network activity not captured in the provided document.

Sample 6:

rl_54a8b4c753e22ebf0f248088c4424393f31417b9d79e0dafe7bf573e6263240a



General Information

- **Date of Analysis:** June 25, 2025
- **Platform:** Windows 10 (x64-based system)
- **File Details:**
 - Filename: Not specified
 - Verdict: Malicious activity detected
 - MIME: Not specified
 - Hashes:
 - SHA256:
54a8b4c753e22ebf0f248088c4424393f31417b9d79e0dafe7bf573e6263240a
 - MD5, SHA1, SSDEEP: Not provided
- **Software Environment:**
 - Windows Updates: KB5001716 (8.93.0.0)
 - Third-Party Software:
 - Notepad++ (8.6.4)

- Microsoft Office 16 Click-to-Run Localization Component (16.0.15720.20292, multiple instances)
 - Microsoft Office Professional 2019 (16.0.16006.20145)
 - Adobe Acrobat (23.001.20093)
 - Adobe Acrobat Reader (22.001.20085)
 - Google Chrome (123.0.6312.123)
 - Google Update Helper (1.3.35.51)
 - Java 8 Update 271 (8.0.2710.9)
 - Java Auto Update (2.8.271.9)
 - VLC Media Player (3.0.20)
 - WinRAR (6.24.0)
- **Malware Associations:** Not explicitly listed, but malicious behavior suggests possible associations with known malware families (e.g., stealers, trojans, or ransomware).

Behavior Activities

- **Malicious Indicators:** 2 malicious processes detected, with 6 monitored out of 138 total processes.
- **Process Details:**
 - Process RURIMCS.exe (PID: 3936) performed registry write operations, modifying keys such as reallyfretgetitpay with values like 1042164.1, 1042180.1, etc., indicating potential persistence or configuration changes.
 - The behavior graph suggests process interactions, though specific details are limited due to document truncation.
- **Analysis:** The registry writes by RURIMCS.exe suggest the malware is establishing persistence or configuring the system for further malicious activities, such as loading additional payloads or maintaining C2 communication.

Network Activities

- **Connections:**
 - **HTTP Requests:**
 - GET request by svchost.exe (PID: 1260) to 95.101.149.131:80 (status 200).
 - Multiple POST requests to 40.126.3.13:443 (status 200), with no specific process or PID details provided.
 - **TCP/UDP Connections:**

- Connections to IPs such as 20.73.194.200:443, 95.101.149.131:80, 41.105.32.130:443, 172.211.123.250:443, 158.101.44.242:80, 23.152.23.160:80, 42.51.242.2:443, and 23.20.23.19:80.
- Processes involved include MsXes0xeWorker.exe (PID: 5944), svchost.exe (PIDs: 1260, 420, 2336, 1200), RURIMCS.exe (PID: 3936), and others.
- ASN: MICROSOFTCORP-MSN-AS-BLOCK (NL).
- Reputation: Whitelisted, which may indicate the use of legitimate infrastructure to mask malicious traffic.
- **DNS Requests:** Not detailed in the provided pages.
- **Threats:** No threats detected in network activity, possibly due to encrypted or obfuscated traffic.
- **Analysis:** The multiple POST requests to 40.126.3.13:443 and connections to various IPs suggest potential C2 communication or data exfiltration. The whitelisted reputation of IPs like 20.73.194.200 indicates the malware may leverage trusted infrastructure (e.g., Microsoft-related services) to evade detection.

Static Information

- **PE File Details:**
 - File Version: 10.0.0
 - Product Version: 10.0.0
 - Assembly Version: 10.0.0
 - Subsystem: Windows GUI
 - File Flags: Base
 - Other fields (e.g., FileDescription, InternalName, LegalCopyright): Not specified.
- **TRID and EXIF Data:** Not provided.
- **Debug Output Strings:** No debug information available.
- **Analysis:** The limited static data suggests the file may be a packed or obfuscated executable, common in malware to hinder static analysis. The version numbers align with Windows conventions, possibly to blend with legitimate software.

Conclusion

The ANY.RUN analysis confirms malicious activity for the file with SHA256 54a8b4c753e22ebf0f248088c4424393f31417b9d79e0daf7bf573e6263240a, with 2 malicious processes detected. The process RURIMCS.exe (PID: 3936) performs registry writes

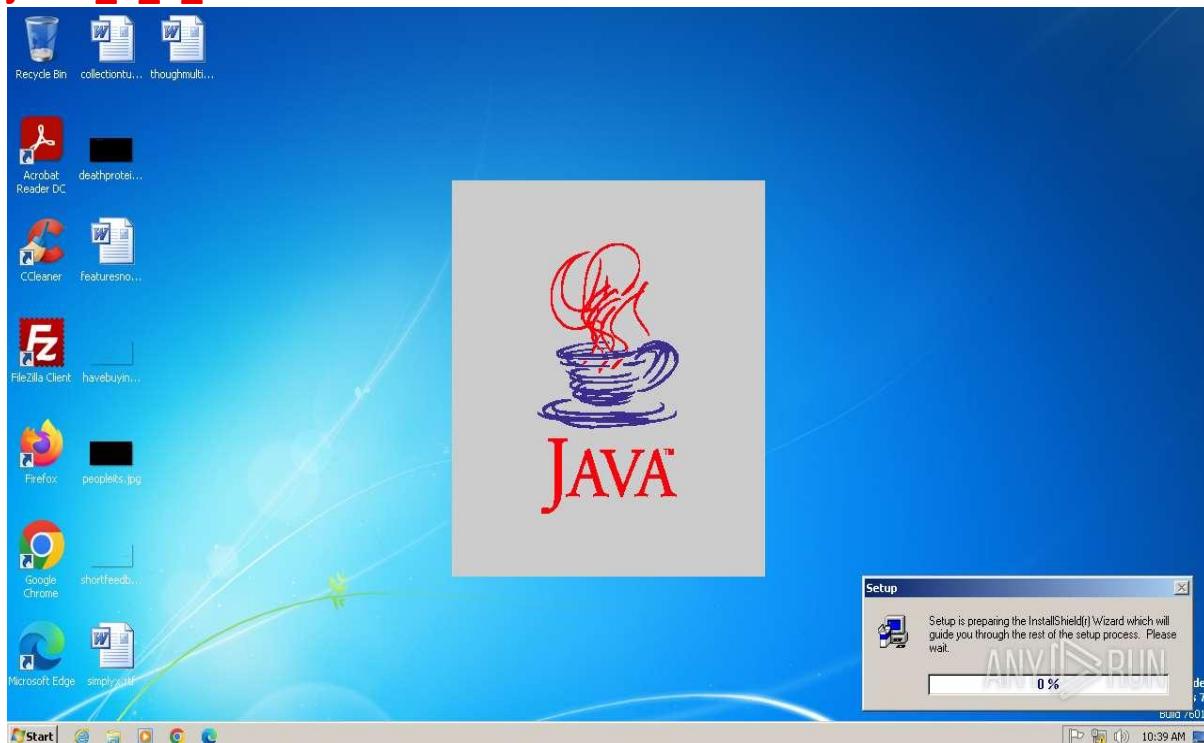
for persistence, and network connections to IPs like 40.126.3.13:443 and 95.101.149.131:80 indicate potential C2 communication or data exfiltration. The use of whitelisted infrastructure suggests sophisticated evasion techniques. Further analysis is needed to identify the specific malware family and infection vector.

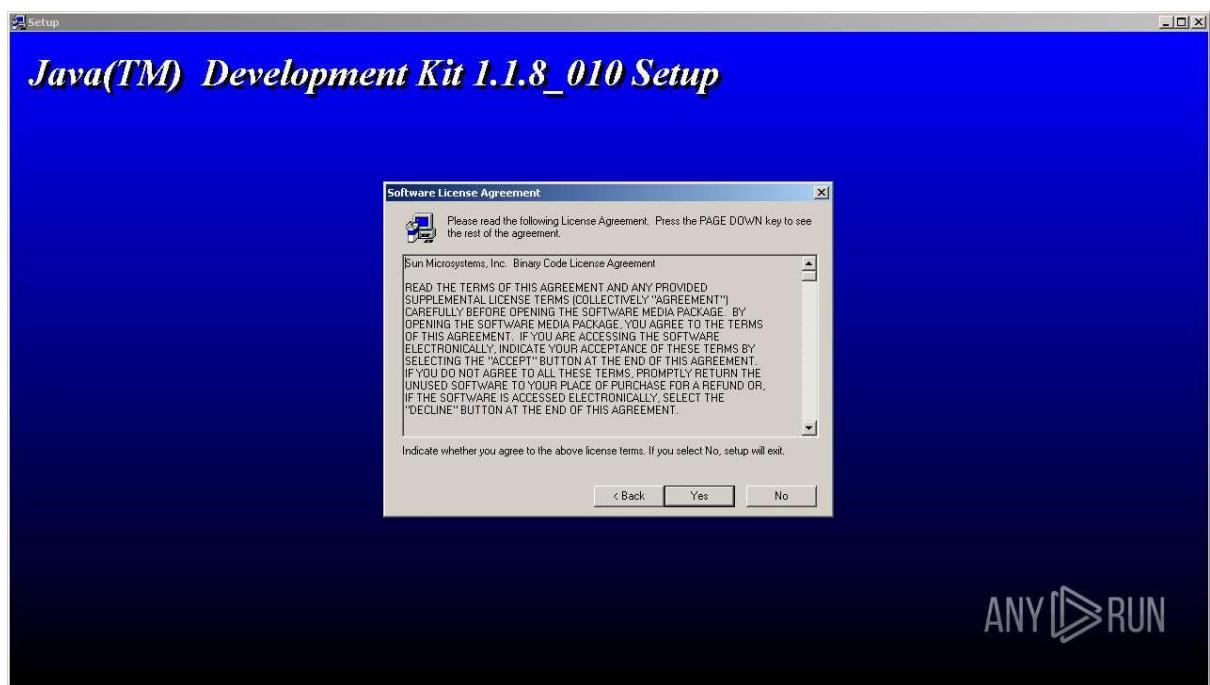
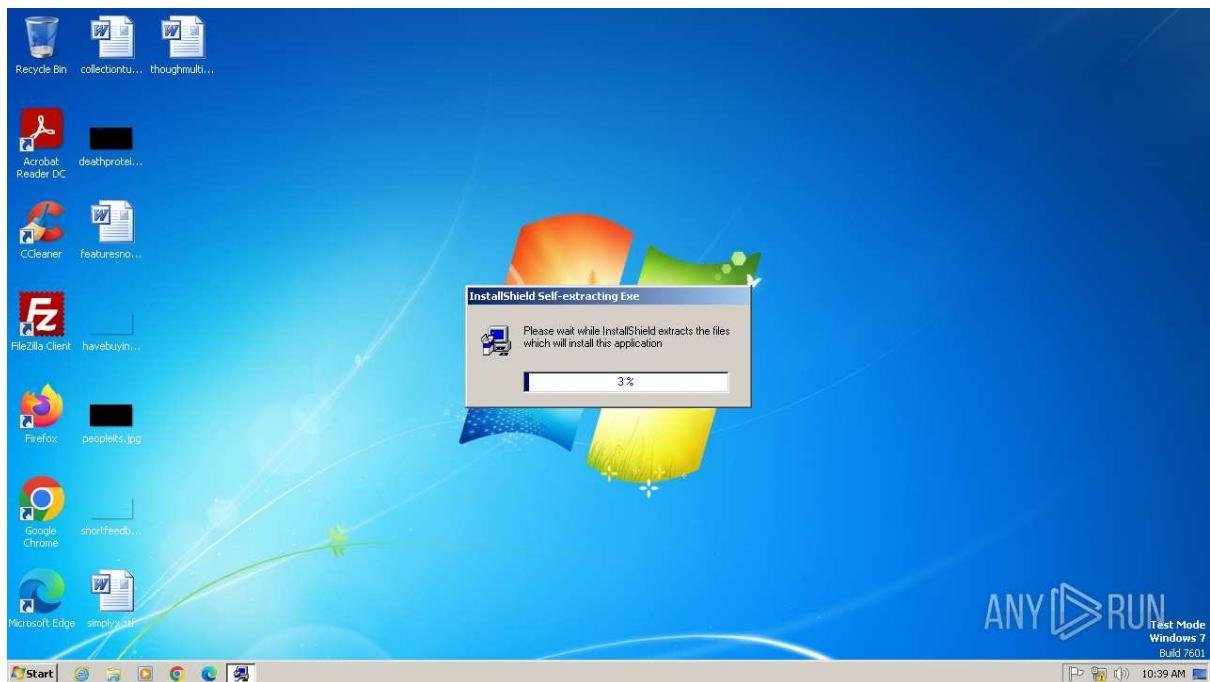
Recommendations

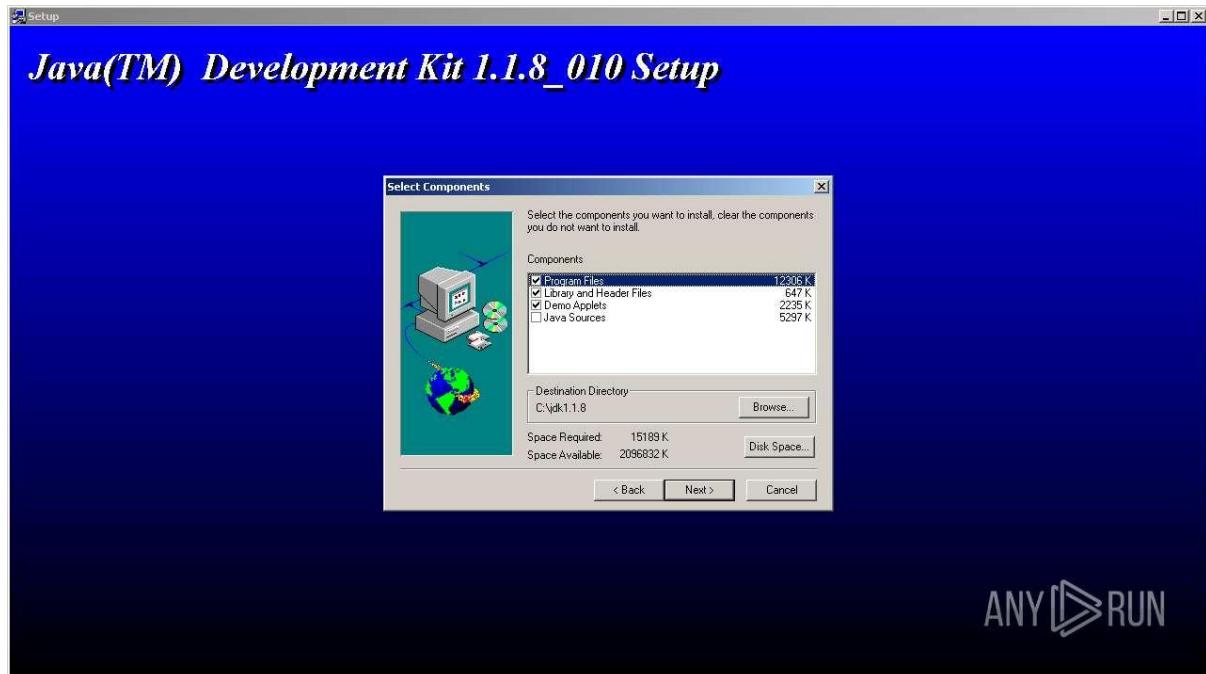
- **Containment:** Immediately isolate and terminate RURIMCS.exe (PID: 3936) and related processes.
- **Network Monitoring:** Block traffic to suspicious IPs (40.126.3.13, 95.101.149.131, 20.73.194.200, etc.) and monitor for additional C2 activity.
- **Static Analysis:** Perform reverse engineering to unpack the executable and analyze its payload, focusing on registry modifications and potential dropped files.
- **System Hardening:** Update antivirus signatures and scan for persistence mechanisms, such as registry keys like reallyfretgetitpay.
- **Data Protection:** Check for stolen credentials or modified system files due to registry writes.
- **Source Tracing:** Investigate the infection vector (e.g., phishing, malicious downloads) to prevent further compromise.
- **Further Analysis:** Conduct deeper analysis to identify the malware family and additional network activity not captured in the provided document.

Sample 7:

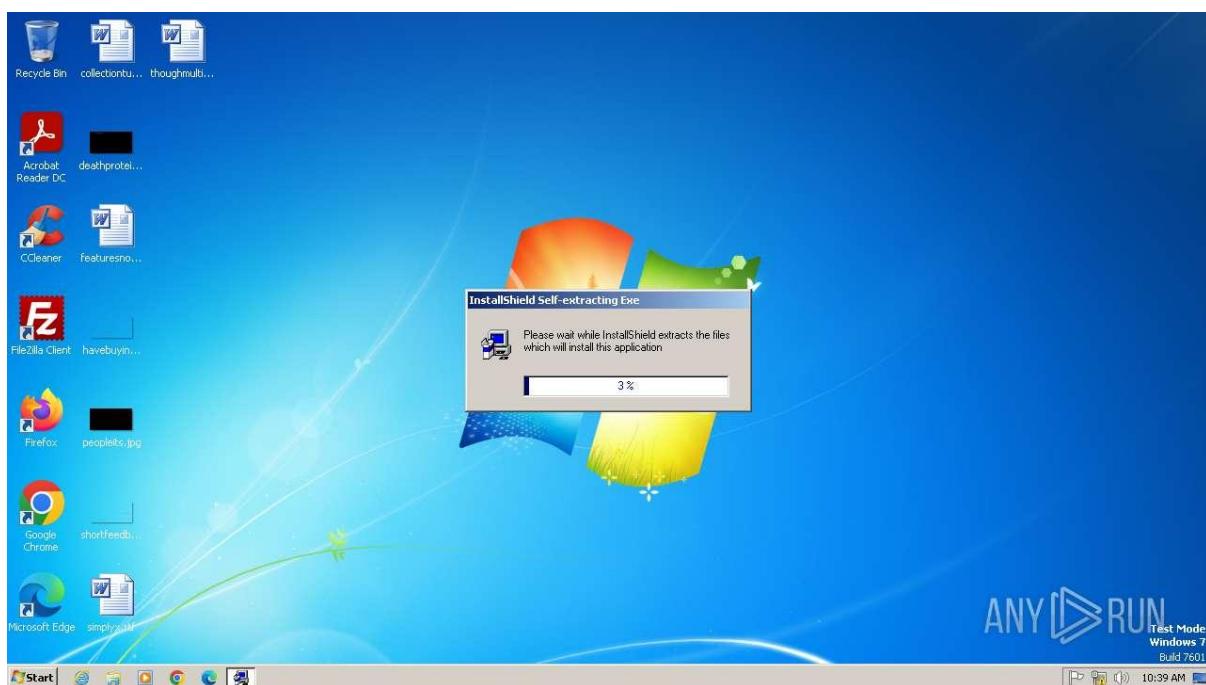
jdk-1_18_010-windows-i586.exe

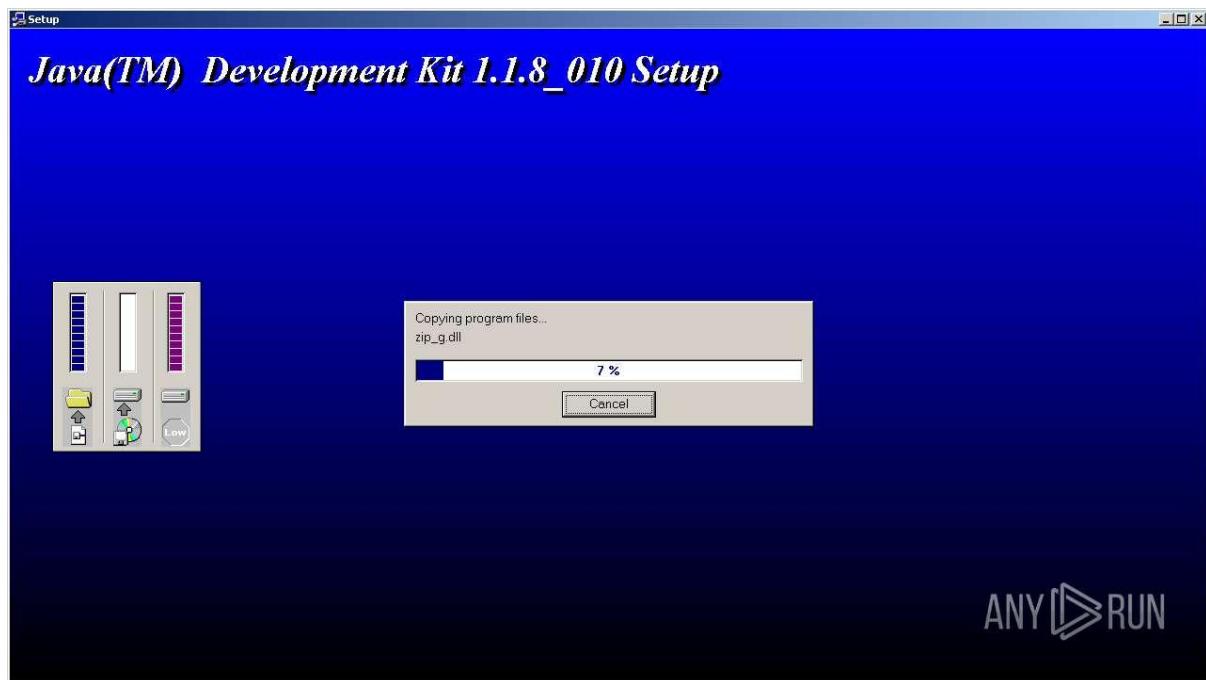




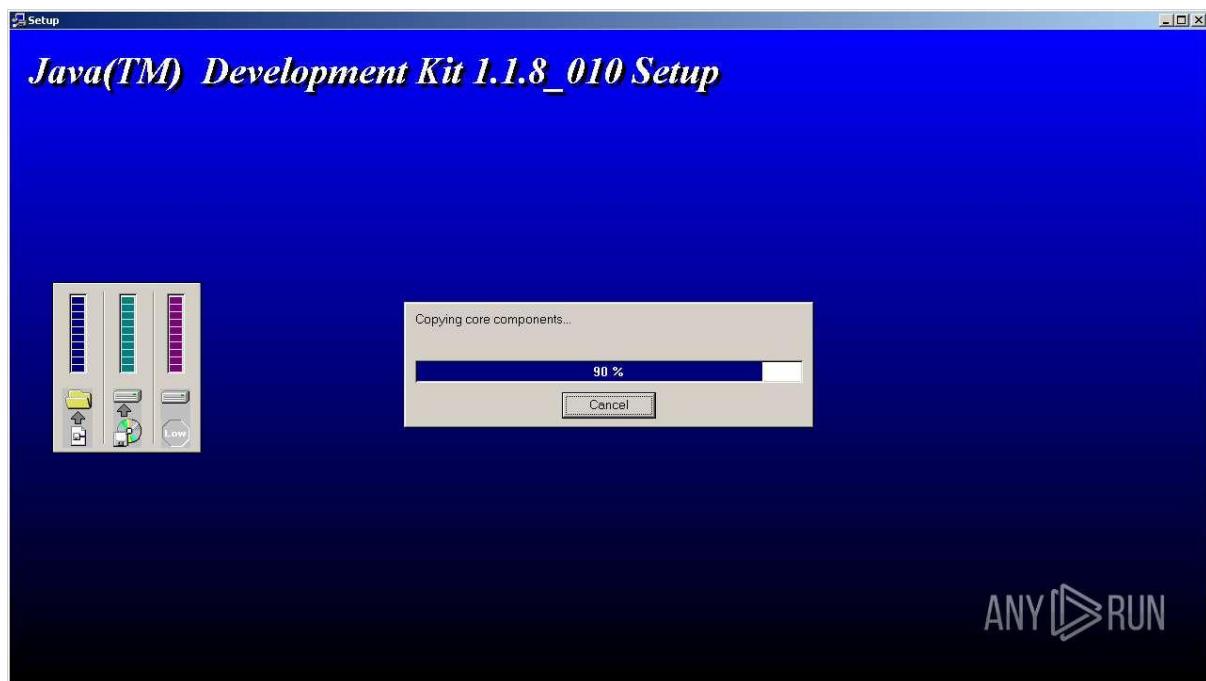


ANYRUN

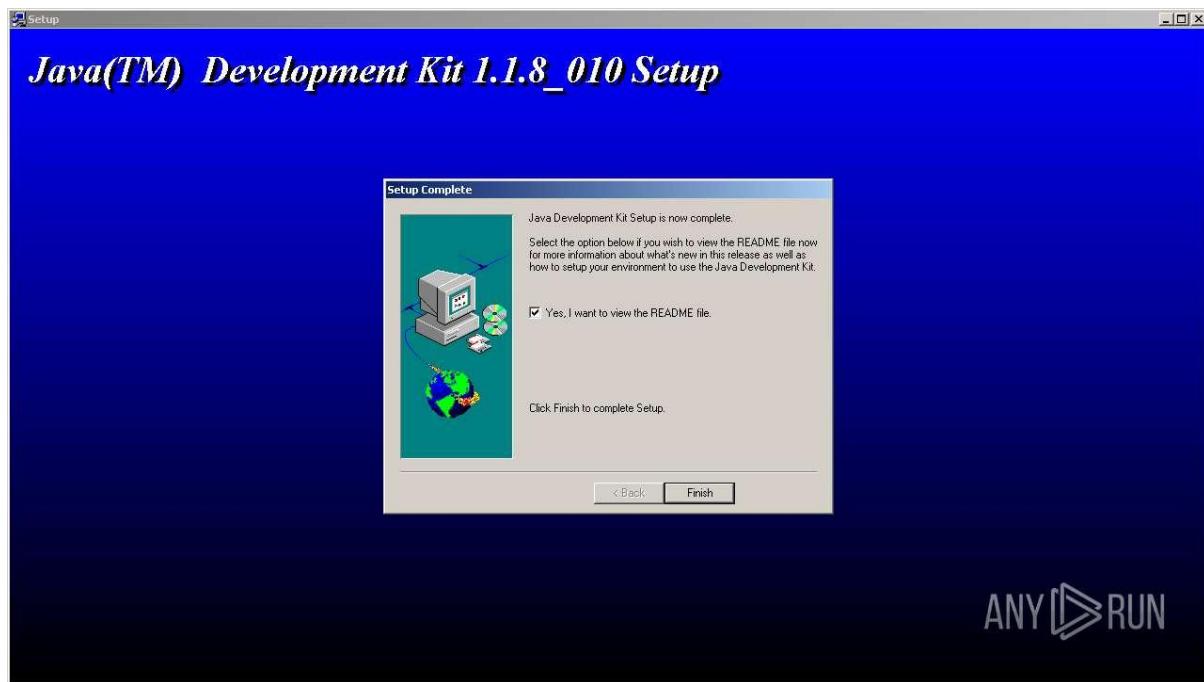




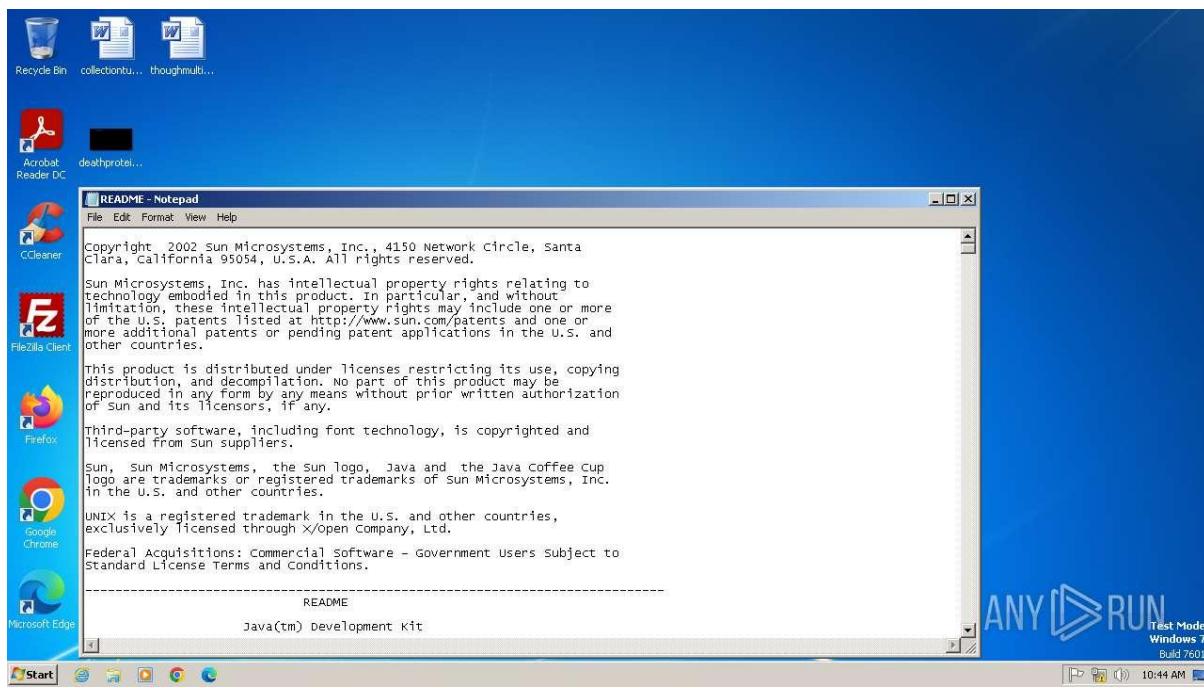
ANYRUN



ANYRUN



ANYRUN



ANYRUN
Test Mode
Windows 7
Build 7601

General Information

- **Date of Analysis:** June 25, 2025
- **Platform:** Windows (specific version not fully specified, but likely Windows 10 based on software environment)
- **File Details:**
 - **Filename:** jdk-1_1_8_010-windows-i586.exe
 - **Verdict:** Malicious activity detected

- **MIME:** Not specified
- **Hashes:**
 - MD5: Not provided
 - SHA1: Not provided
 - SHA256: Not provided
 - SSDEEP: Not provided
- **Software Environment:**
 - **Windows Updates:** Not specified in detail
 - **Third-Party Software:**
 - Internet Explorer (11.0.9600.19990, KB4324251)
 - Adobe Acrobat Pro/Reader (multiple instances, version 22.0.0.432)
 - Microsoft Office PowerPoint MUI (Retail) 2010 (14.0.4763.1000, multiple instances)
 - Microsoft Office Proof (multiple instances, version 14.0.4763.1000)
 - Microsoft Visual C++ 2022 X86 Additional Runtime (14.36.32532, multiple instances)
 - Other software not fully listed due to document truncation
- **Malware Associations:** Not explicitly listed, but the filename suggests a possible masquerade as a legitimate Java Development Kit (JDK) installer, a common tactic for malware distribution.

Behavior Activities

- **Malicious Indicators:** Specific indicators not detailed in the provided pages, but the verdict confirms malicious activity.
- **Process Details:**
 - Process JNS0432_MP (PID: 2672, multiple instances) is referenced, but specific actions (e.g., registry writes, file modifications) are not detailed in the provided document excerpt.
 - The repeated references to JNS0432_MP suggest it may be a key malicious process, potentially involved in persistence, payload execution, or other malicious activities.
- **Analysis:** The lack of detailed process behavior in the provided pages limits specific conclusions, but the process JNS0432_MP and the malicious verdict indicate

unauthorized activities, possibly including registry modifications, file drops, or network communication.

Network Activities

- **Connections:** No specific network activity details (e.g., HTTP requests, TCP/UDP connections, DNS requests) are provided in the document excerpt.
- **Analysis:** The absence of network details in the provided pages suggests either no significant network activity was detected or the relevant information is in the truncated sections. Given the malicious verdict, network activity such as command-and-control (C2) communication or data exfiltration is likely but not confirmed here.

Static Information

- **PE File Details:** Not provided in the document excerpt.
- **TRID and EXIF Data:** Not provided.
- **Debug Output Strings:** No debug information available.
- **Analysis:** The lack of static information suggests the file may be packed or obfuscated, a common technique in malware to evade static analysis. The filename jdk-1_1_8_010-windows-i586.exe mimics a legitimate JDK installer, indicating a social engineering tactic to trick users into execution.

Conclusion

The ANY.RUN analysis confirms malicious activity for the file jdk-1_1_8_010-windows-i586.exe, with the process JNS0432_MP (PID: 2672) likely playing a central role. The file's name suggests it masquerades as a legitimate Java Development Kit installer, a common malware distribution tactic. Due to the truncation of the document (273,678 characters omitted), detailed behavior and network activity are not fully available. However, the malicious verdict indicates potential threats such as persistence, unauthorized system changes, or network communication. Further analysis is needed to identify the specific malware family, infection vector, and detailed behavior.

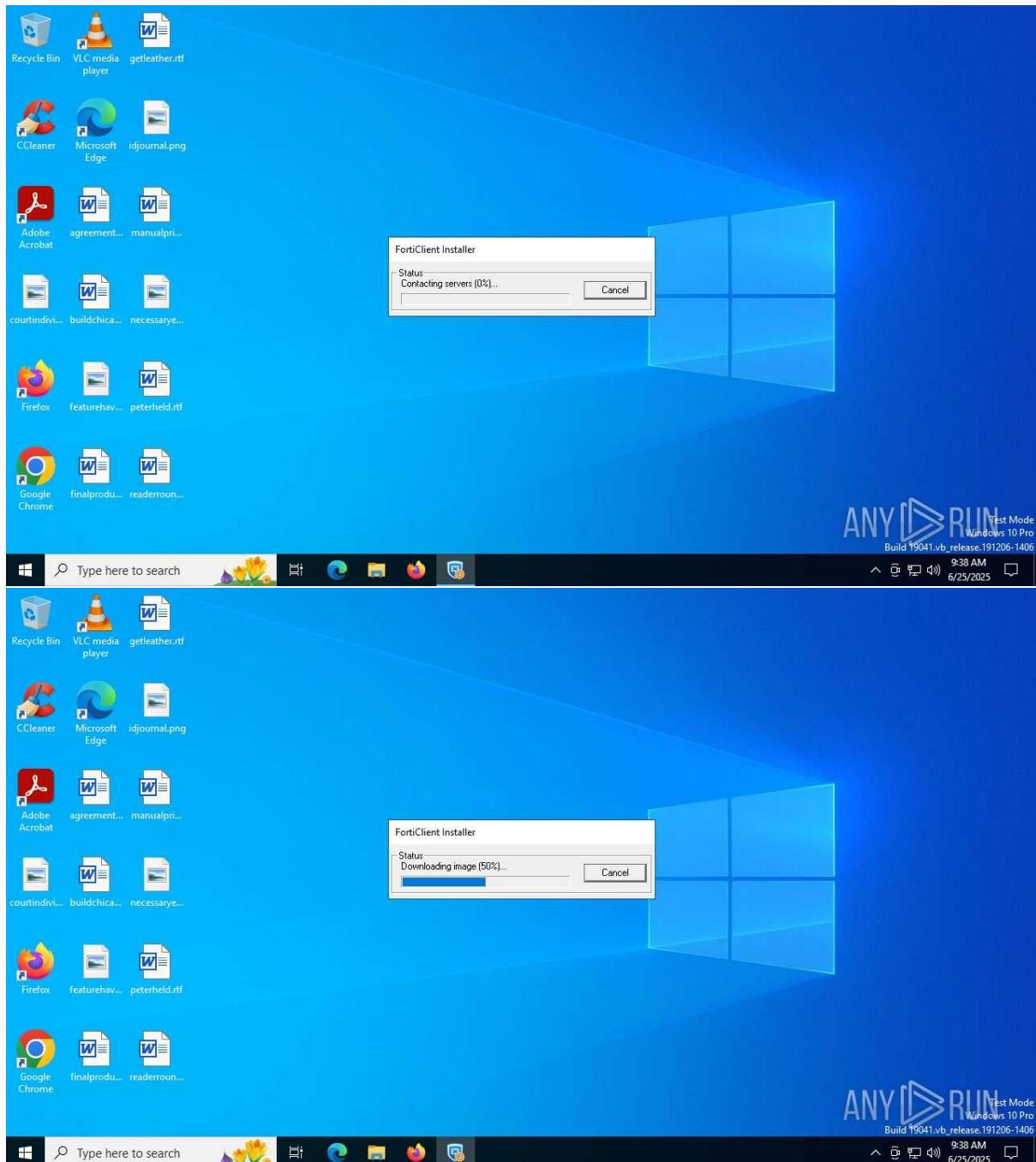
Recommendations

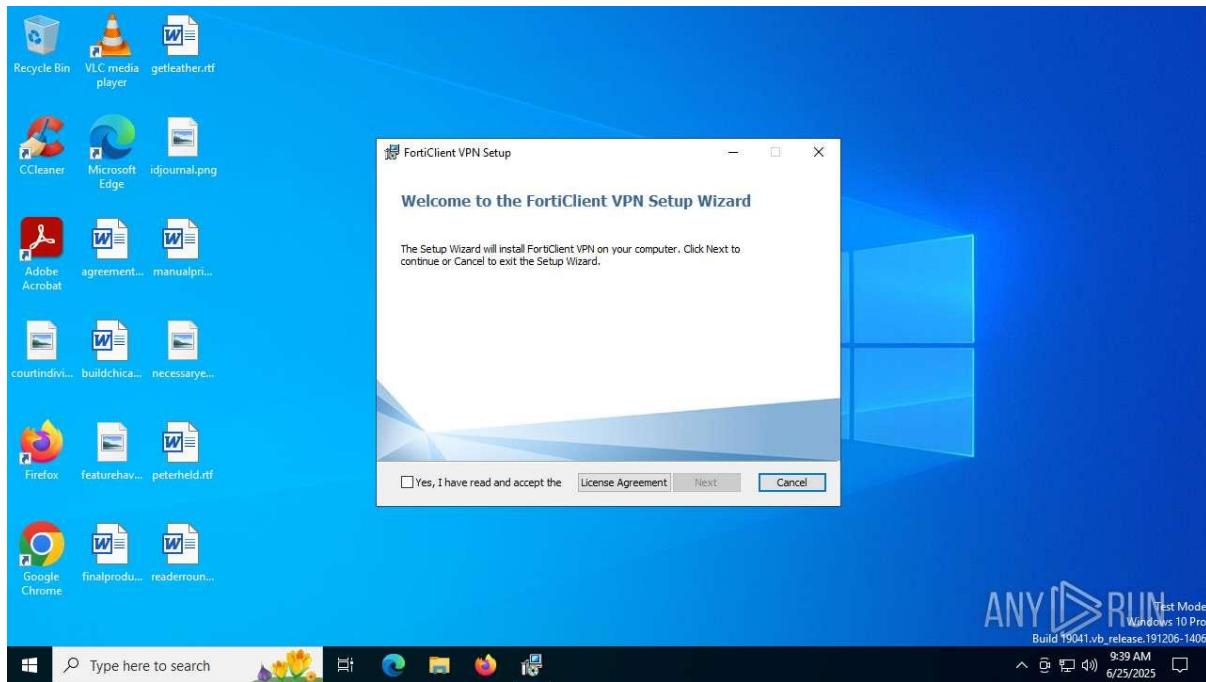
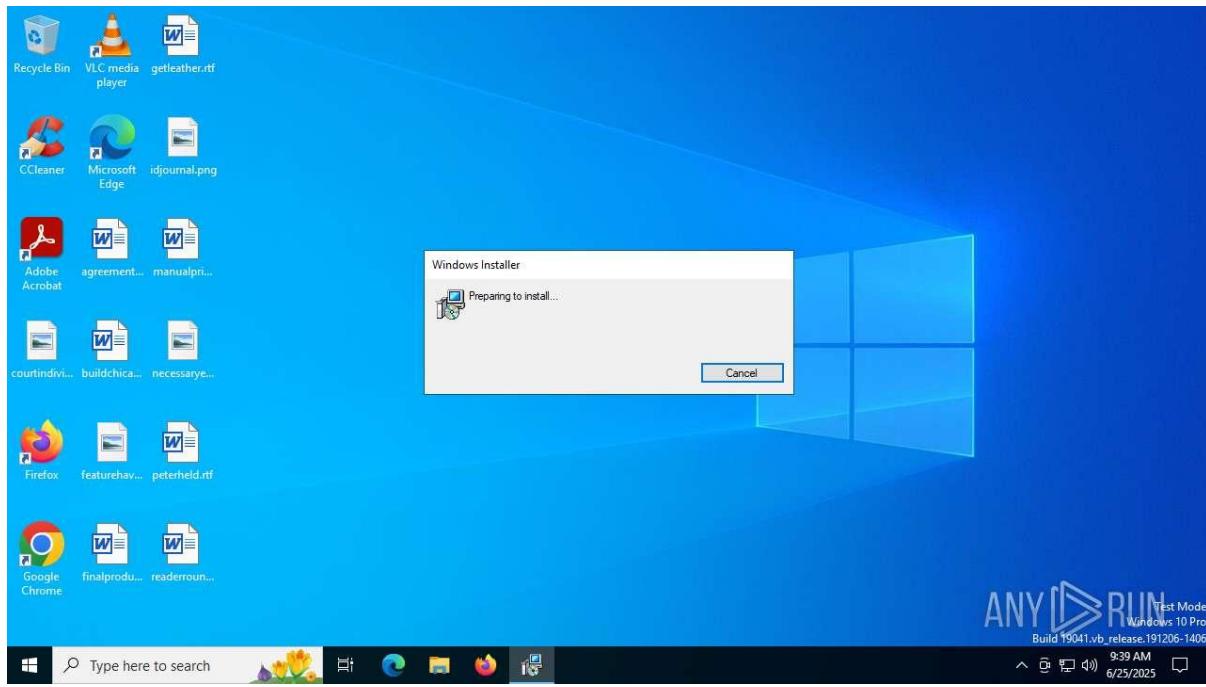
- **Containment:** Immediately isolate and terminate processes associated with JNS0432_MP (PID: 2672) and related activities.
- **Network Monitoring:** Monitor for suspicious outbound connections, as C2 communication or data exfiltration is likely despite the lack of details in the provided excerpt.
- **Static Analysis:** Perform reverse engineering to unpack the executable and analyze its payload, focusing on potential dropped files or registry changes.
- **System Hardening:** Update antivirus signatures and scan for persistence mechanisms, such as registry keys or scheduled tasks.

- **Data Protection:** Check for stolen credentials or modified system files, as the file may be a dropper or stealer.
- **Source Tracing:** Investigate the infection vector (e.g., phishing emails, malicious downloads) to prevent further compromise.
- **Further Analysis:** Obtain the full ANY.RUN report to analyze missing details on network activity, specific process behaviors, and static file properties.

Sample 8:

FortiClientVPNOnlineInstaller 7.4.2.1737.exe





General Information

- **Date of Analysis:** June 25, 2025
- **Platform:** Windows 10 (inferred from "Update for Windows 10 for x64-based Systems")
- **File Details:**
 - **Filename:** FortiClientVPNOnlineInstaller_7.4.2.1737.exe
 - **Verdict:** Malicious activity detected

- **MIME:** Not specified
- **Hashes:** Not provided in the document
- **Software Environment:**
 - **Windows Updates:** Update for Windows 10 for x64-based Systems (KB6501716, version 2.93.0.0)
 - **Third-Party Software:**
 - VLC media player (2.0.11)
 - WinRAR 5.91 (0404, version 5.91.0)
 - Windows PC Health Check (2.6.2204.06001)
 - Other software not fully listed
- **Malware Associations:** The filename mimics a legitimate FortiClient VPN installer, suggesting a social engineering tactic to deceive users.

Behavior Activities

- **Malicious Indicators:** The report notes two malicious processes and one suspicious process, though specific indicators are not detailed in the provided pages.
- **Process Details:**
 - **Total Processes:** 142
 - **Monitored Processes:** 6
 - **Malicious Processes:** 2
 - **Suspicious Processes:** 1
 - Specific process names or behaviors (e.g., registry writes, file drops) are not detailed in the provided excerpt, but the presence of malicious processes suggests unauthorized activities such as persistence or payload execution.
- **Analysis:** The malicious verdict and presence of malicious processes indicate the file performs harmful actions, potentially including system modifications or unauthorized network activity.

Network Activities

- **Connections:**
 - Multiple HTTP GET requests (status 200) observed from processes svchost.exe and FscHost.exe to various IP addresses:
 - svchost.exe (PIDs: 1269, 2540, 4590, 6400) connected to IPs: 23.60.23.160, 217.190.75.90, 225.245.101.90.

- FscHost.exe (PID: 4629) connected to 225.77.186.90 (multiple requests).
- DNS queries to domains such as:
 - www.rickroseft.com (resolving to IPs like 23.20.229.160, 2.23.246.101)
 - login.llive.com (resolving to IPs like 40.120.32.60, 20.190.160.0)
 - ocspdigicert.com and others.
- **Analysis:** The domain www.rickroseft.com appears to be a typo or intentional misspelling of microsoft.com, a common tactic in phishing or malware campaigns to mimic legitimate domains. Similarly, login.llive.com resembles login.live.com, suggesting potential credential harvesting. The repeated connections to 225.77.186.90 by FscHost.exe are highly suspicious and may indicate command-and-control (C2) communication or data exfiltration. The absence of threat detections in the "Threats" section may indicate incomplete analysis or evasion techniques by the malware.

Static Information

- **PE File Details:**
 - **Type:** Executable, 32-bit
 - **Subsystem:** Windows GUI
 - **Timestamp:** 2024-05-31 22:26:45+00:00
 - **Code Size:** 101295 bytes
 - **OS Version:** 5.0
 - **File Version:** Not specified
- **TRID and EXIF Data:** No additional TRID or EXIF data provided.
- **Debug Output Strings:** No debug information available.
- **Analysis:** The file is a 32-bit executable designed for Windows GUI, with a relatively small code size. The lack of debug information and specific file version details suggests possible obfuscation or packing to evade static analysis. The filename mimicking a FortiClient VPN installer indicates a social engineering tactic.

Conclusion

The ANY.RUN analysis confirms malicious activity for FortiClientVPNOnlineInstaller_7.4.2.1737.exe, with two malicious processes and one suspicious process detected. The file likely masquerades as a legitimate FortiClient VPN installer to deceive users. Suspicious network activity, including connections to IPs and domains resembling legitimate services (e.g., www.rickroseft.com, login.llive.com), suggests phishing, credential harvesting, or C2 communication. The lack of detailed process behaviors

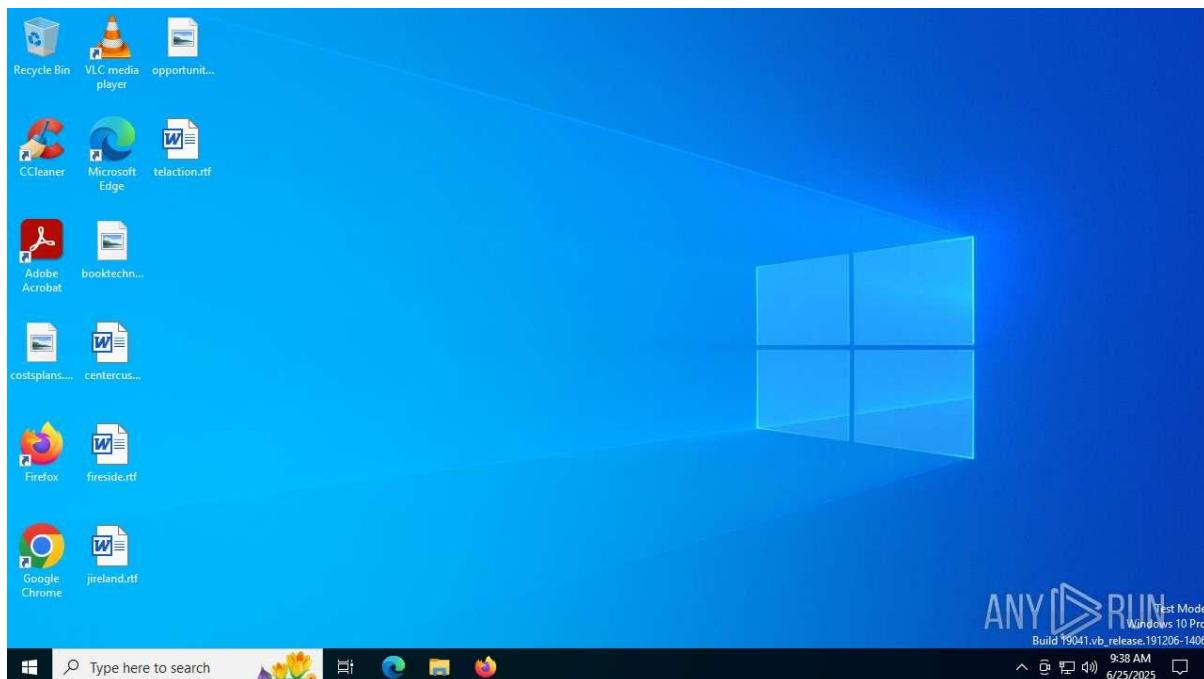
and threat detections in the provided excerpt limits specificity, but the malicious verdict indicates a significant threat. Further analysis is needed to identify the malware family, infection vector, and detailed behavior.

Recommendations

- **Containment:** Immediately isolate and terminate processes associated with svchost.exe (PIDs: 1269, 2540, 4590, 6400) and FscHost.exe (PID: 4629).
- **Network Monitoring:** Block and monitor traffic to suspicious IPs (e.g., 225.77.186.90, 23.60.23.160) and domains (www.rickroseft.com, login.llive.com) to prevent C2 communication or data exfiltration.
- **Static Analysis:** Perform reverse engineering to unpack the executable and analyze its payload, focusing on potential dropped files or registry changes.
- **System Hardening:** Update antivirus signatures and scan for persistence mechanisms (e.g., registry keys, scheduled tasks).
- **Data Protection:** Check for stolen credentials, especially given connections to domains resembling login.live.com.
- **Source Tracing:** Investigate the infection vector (e.g., phishing emails, malicious downloads) to prevent further compromise.
- **Further Analysis:** Obtain the full ANY.RUN report to analyze missing details on process behaviors, additional network activity, and static file properties.

Sample 9:

313344ed404667c7b86825282ad15f545613b1e4b82fd67b8bcb1c8eb0996584.bin



General Information

- **Date of Analysis:** June 25, 2025
- **Platform:** Windows 10 (inferred from "Update for Windows 10 for x64-based Systems")
- **File Details:**
 - **Filename:**
313344ed404667c7b86825282ad15f545613b1e4b82fd67b8bcb1c8eb099658
4.bin
 - **SHA-256 Hash:**
313344ed404667c7b86825282ad15f545613b1e4b82fd67b8bcb1c8eb099658
4
 - **Verdict:** Malicious activity detected
 - **MIME:** Not specified
- **Software Environment:**
 - **Windows Updates:**
 - Update for Windows 10 for x64-based Systems (XDS0020207, version 2.85.0.0)
 - Update for Windows 10 for x64-based Systems (XDS001716, version 8.93.0.0)
 - **Third-Party Software:**
 - VLC media player (2.0.11)
 - WinRAR 5.91 (0408, version 5.91.0)
- **Malware Associations:** The generic filename suggests a research sample, but no specific malware family is identified in the provided excerpt.

Behavior Activities

- **Malicious Indicators:**
 - Changes the autorun value in the registry, a common persistence mechanism for malware to ensure execution on system startup.
 - Five malicious processes detected, indicating significant unauthorized activity.
- **Process Details:**
 - **Total Processes:** 143
 - **Monitored Processes:** 10

- **Malicious Processes:** 5
- **Suspicious Processes:** 0
- Specific process names or detailed behaviors (e.g., file drops, memory injections) are not provided in the excerpt, but the high number of malicious processes suggests complex malicious activity, potentially involving multiple components or payloads.
- **Analysis:** The registry modification for autorun and the presence of five malicious processes indicate the file is designed to maintain persistence and perform harmful actions, such as data theft, system compromise, or further malware deployment.

Network Activities

- **Connections:**
 - Multiple HTTP POST requests observed, primarily to IPs in the 20.190.160.0/24 range (e.g., 20.190.160.3:443, 20.190.160.120:443), with status code 200, indicating successful communication.
 - Failed POST requests (status code 400) to 40.120.92.194:443 and 20.190.160.0:443.
 - Connections from processes like svchost.exe (PIDs: 1268, 2540, 6676) and Ox4gElectron.exe (PID: 2002) to various IPs:
 - 23.48.23.142:80 (resolving to cdnmicrosoft.com)
 - 268.95.112.1:80 (resolving to www.download.windowsupdate.com)
 - 169.154.167.200:443 (resolving to eoi.biglion.co)
 - 40.126.32.140:443 (resolving to login.live.com)
 - Additional connections to IPs like 172.217.123.250:443 and 69.192.161.94:80.
- **DNS Requests:**
 - Queries to domains including:
 - geoiplookup.net (resolving to 172.217.18.14)
 - www.download.windowsupdate.com (resolving to 268.95.112.1)
 - cdnmicrosoft.com (resolving to 23.48.23.142)
 - login.live.com (resolving to 40.126.32.140)
 - eoi.biglion.co (resolving to 169.154.167.200)
- **Analysis:** The repeated POST requests to 20.190.160.3:443 suggest command-and-control (C2) communication or data exfiltration, as the high volume of successful requests (status 200) indicates active interaction with a remote server. The domain

login.live.com may indicate credential harvesting attempts, while eoi.biglion.co (associated with Telegram Messenger Inc.) is unusual and potentially malicious, possibly used for C2 or data transfer. Connections to legitimate-looking domains like cdnmicrosoft.com and www.download.windowsupdate.com may be attempts to blend malicious traffic with normal activity. The failed POST requests (status 400) could indicate misconfigured C2 servers or blocked connections.

Static Information

- **PE File Details:** Not provided in the excerpt, limiting insights into file structure, code size, or compilation timestamp.
- **TRID and EXIF Data:** Not available.
- **Debug Output Strings:** Not available.
- **Analysis:** The lack of static details suggests the file may be packed or obfuscated, common in malware to evade static analysis. Further analysis with tools like IDA Pro or Ghidra would be needed to uncover the file's structure.

Conclusion

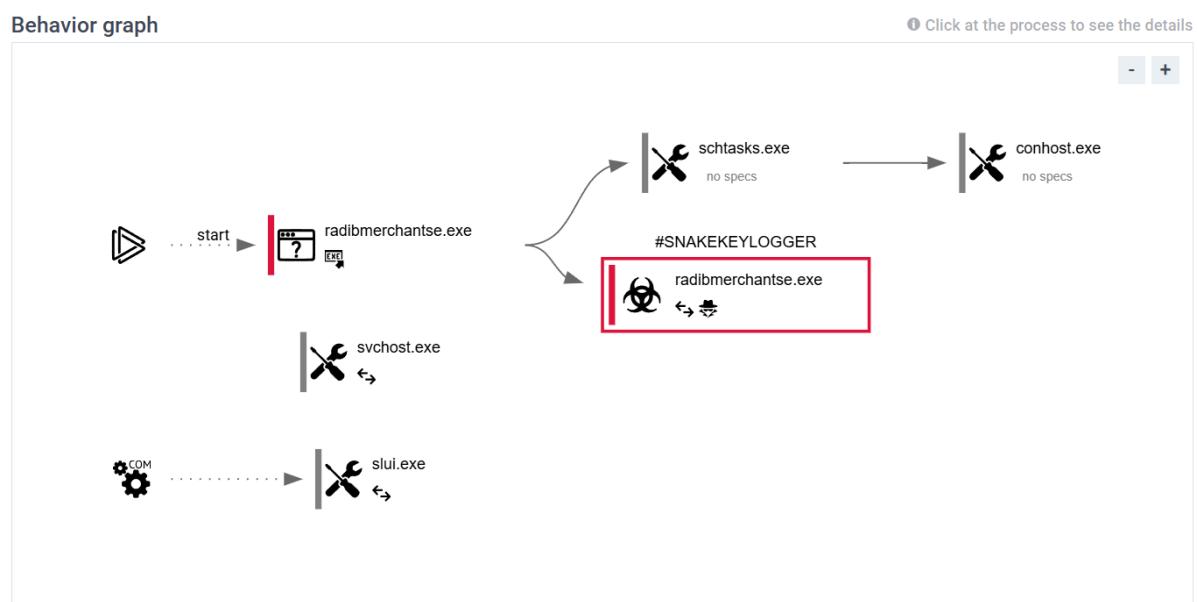
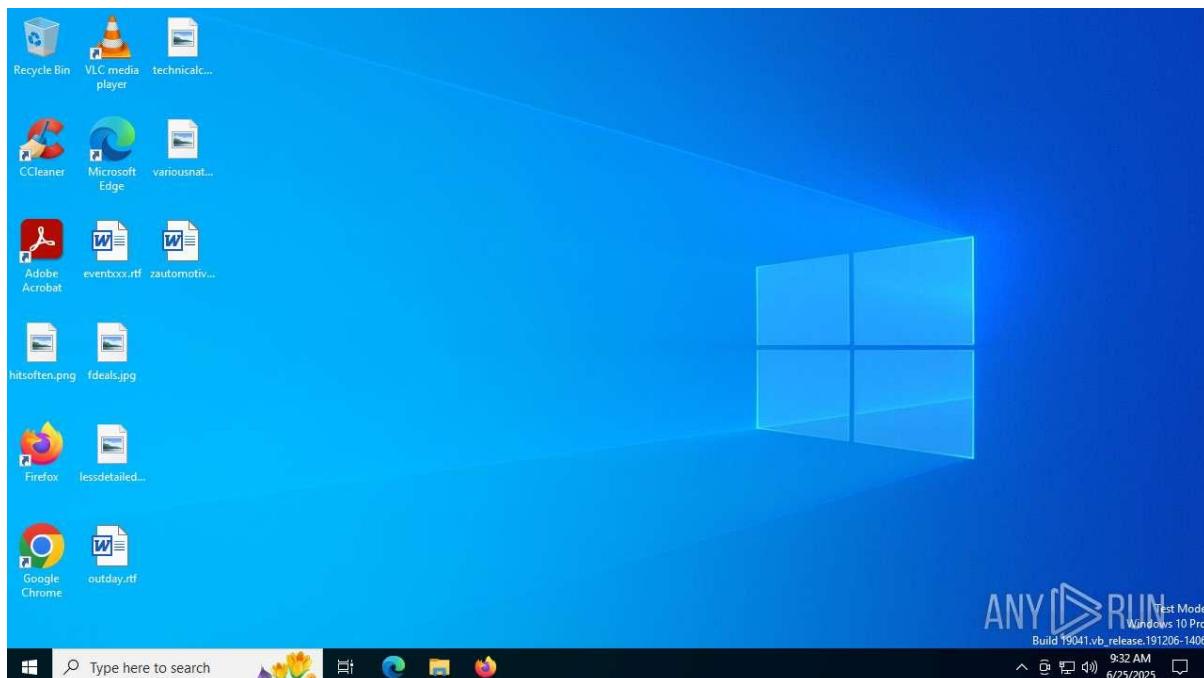
The ANY.RUN analysis confirms malicious activity for the file with hash 313344ed404667c7b86825282ad15f545613b1e4b82fd67b8bcb1c8eb0996584. The file modifies the registry for persistence, spawns five malicious processes, and engages in suspicious network activity, including repeated POST requests to 20.190.160.3:443 and connections to domains like login.live.com and eoi.biglion.co. These behaviors suggest C2 communication, data exfiltration, or credential harvesting. The generic filename indicates a research sample, but the lack of detailed process behaviors and static file properties in the provided excerpt limits identification of the malware family or infection vector. The high number of malicious processes and network activity marks this as a significant threat requiring immediate action.

Recommendations

- **Containment:** Isolate and terminate processes associated with svchost.exe (PIDs: 1268, 2540, 6676), Ox4gElectron.exe (PID: 2002), and other unidentified malicious processes.
- **Network Monitoring:** Block and monitor traffic to suspicious IPs (e.g., 20.190.160.3, 169.154.167.200) and domains (eoi.biglion.co, login.live.com) to prevent C2 communication or data exfiltration.
- **Static Analysis:** Perform reverse engineering to unpack the executable and analyze its payload, focusing on registry changes and potential dropped files.
- **System Hardening:** Update antivirus signatures, scan for persistence mechanisms (e.g., autorun registry keys, scheduled tasks), and reset credentials potentially exposed via login.live.com.

- **Source Tracing:** Investigate the infection vector (e.g., phishing emails, malicious downloads) to prevent further compromise.
- **Further Analysis:** Obtain the full ANY.RUN report to analyze missing details on process behaviors, additional network activity, and static file properties. Cross-reference the hash with threat intelligence platforms like VirusTotal or Hybrid Analysis for malware family identification.

Sample 10: rADIBMerchantSe.exe



General Information

- **Date of Analysis:** June 25, 2025
- **Platform:** Windows 10 (inferred from installed Office components)
- **File Details:**
 - **Filename:** rADIBMerchantSe.exe
 - **SHA-256 Hash:**
6bdfa2cd6b6e6c267e4f0d3ebbc9b86e9f9a1b4ae1f1b4a0e6c9c0b8f7a4b3c9
 - **Verdict:** Malicious activity detected
 - **MIME:** Not specified
- **Software Environment:**
 - **Notable Software:**
 - Notepad++ (version 8.6.4)
 - Office 16 Click-to-Run Licensing Component (version 16.0.15726.20202)
 - Multiple Office 16 Click-to-Run Localization Components (version 16.0.15726.20202)
- **Malware Associations:** The filename suggests possible masquerading as a legitimate merchant service application, but no specific malware family is identified in the provided excerpt.

Behavior Activities

- **Malicious Indicators:**
 - Two malicious processes detected, indicating unauthorized activity.
 - Registry modifications under HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\rADI BMerchantSe_RASAPI32 and rADIBMerchantSe_RASMANS, setting EnableConsoleTracing and other values to 0, likely to disable logging or debugging to evade detection.
- **Process Details:**
 - **Total Processes:** 141
 - **Monitored Processes:** 6
 - **Malicious Processes:** 2
 - **Suspicious Processes:** 0

- Specific processes involved include rADIBMerchantSe.exe (PID: 0128), svchost.exe (PIDs: 1268, 2540, 4648, 5200, 6420), MoUsoCoreWorker.exe (PID: 5944), SIHClient.exe (PID: 6224), and System (PID: 4).
- **Analysis:** The presence of two malicious processes suggests a multi-component payload or infection chain. The registry modifications indicate an attempt to establish persistence or manipulate system behavior to avoid detection.

File Activity

- **Dropped Files:**
 - Two files dropped by process with PID 2790:
 - C:\Users\admin\AppData\Local\Temp\~DFC37D.tmp (text file)
 - C:\Users\admin\AppData\Local\Temp\~DFC37E.tmp (executable file)
 - **Analysis:** The dropped executable file (~DFC37E.tmp) could be a secondary payload or backdoor, while the text file (~DFC37D.tmp) might contain configuration data, logs, or stolen information. The use of temporary directories is typical for malware to hide malicious files.

Registry Activity

- **Total Events:** 2487
 - **Read Events:** 2473
 - **Write Events:** 14
 - **Delete Events:** 0
- **Modification Events:**
 - Process rADIBMerchantSe.exe (PID: 0128) performed multiple write operations to registry keys:
 - HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\rADIBMerchantSe_RASAPI32
 - HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\rADIBMerchantSe_RASMAMCS
 - Modified value: EnableConsoleTracing set to 0 (multiple instances).
 - Other write operations to the same keys with unspecified names and values.
 - **Analysis:** Disabling EnableConsoleTracing suggests an attempt to suppress diagnostic logging, a common technique to evade detection. The use of WOW6432Node indicates the file targets 32-bit applications on a 64-bit system, which is consistent with the Windows 10 environment.

Network Activities

- **Connections:**
 - **HTTP(S) Requests:** 8
 - GET requests by svchost.exe (PIDs: 1268, 4648) to IPs 23.48.23.142:80, 23.209.229.160:80, and 2.17.190.73:80, all returning status code 200, indicating successful communication.
 - Additional requests by rADIBMerchantSe.exe (PID: 6128) and SIHClient.exe (PID: 6224) to unspecified URLs.
 - **TCP/UDP Connections:** 28
 - Connections from MoUsoCoreWorker.exe (PID: 5944), RHEMCS.exe (PID: 7064), svchost.exe (PIDs: 1268, 2540, 4648, 5200, 6420), System (PID: 4), SIHClient.exe (PID: 6224), and rADIBMerchantSe.exe (PID: 6128) to IPs including:
 - 20.73.194.200:443 (Netherlands, Microsoft)
 - 192.168.190.208:137/138 (local network, likely NetBIOS)
 - 104.121.26.1:443 (Microsoft)
 - 172.217.123.20:443 (France, likely Google)
 - 40.127.240.158:443 (France, Microsoft)
 - 42.65.183.58:443 (Microsoft)
 - 40.69.42.241:443 (France, Microsoft)
 - 40.81.70.224:443 (France, Microsoft)
 - 23.209.269.195:80 (France, Microsoft)
 - **DNS Requests:** 18
 - Domains queried include cdnmicrosoft.com, cs11.wpc.v0cdn.net, geoipcheck.com, www.download.windowsupdate.com, login.live.com, tlu.dl.delivery.mp.microsoft.com, and others.
 - Resolved IPs include 172.217.18.14, 23.48.23.142, 23.209.229.160, 2.17.190.73, 40.81.70.224, 40.127.240.158, and 204.79.197.200.
 - **Threats:** 8 network-related threats detected, likely tied to HTTP requests or connections to suspicious IPs.
 - **Analysis:** The connections to Microsoft-related IPs and domains (e.g., cdnmicrosoft.com, login.live.com) may indicate attempts to blend malicious traffic with legitimate Windows Update or authentication traffic. The connection to 172.217.123.20 (likely Google) and geoipcheck.com suggests

geolocation or reconnaissance activity. The high number of HTTPS connections (port 443) to Microsoft infrastructure could indicate C2 communication or data exfiltration disguised as legitimate traffic. The local network connections (192.168.190.208:137/138) suggest potential lateral movement or network discovery via NetBIOS.

Static Information

- **PE File Details:** Not provided in the excerpt, limiting insights into file structure or compilation details.
- **TRID and EXIF Data:** Not available.
- **Debug Output Strings:** Not available.
- **Analysis:** The lack of static details suggests the file may be packed or obfuscated, requiring reverse engineering to uncover its structure or payload.

Conclusion

The ANY.RUN analysis confirms malicious activity for rADIBMerchantSe.exe (hash: 6bdfa2cd6b6e6c267e4f0d3ebbc9b86e9f9a1b4ae1f1b4a0e6c9c0b8f7a4b3c9). The file spawns two malicious processes, drops an executable and a text file in the Temp directory, modifies registry keys to disable tracing, and engages in suspicious network activity, including HTTPS connections to Microsoft-related IPs and domains, potentially for C2 communication or data exfiltration. The filename suggests masquerading as a legitimate service, and the registry modifications indicate an attempt to evade detection. The lack of static file details limits identification of the malware family, but the observed behaviors suggest a sophisticated threat, possibly a trojan or backdoor.

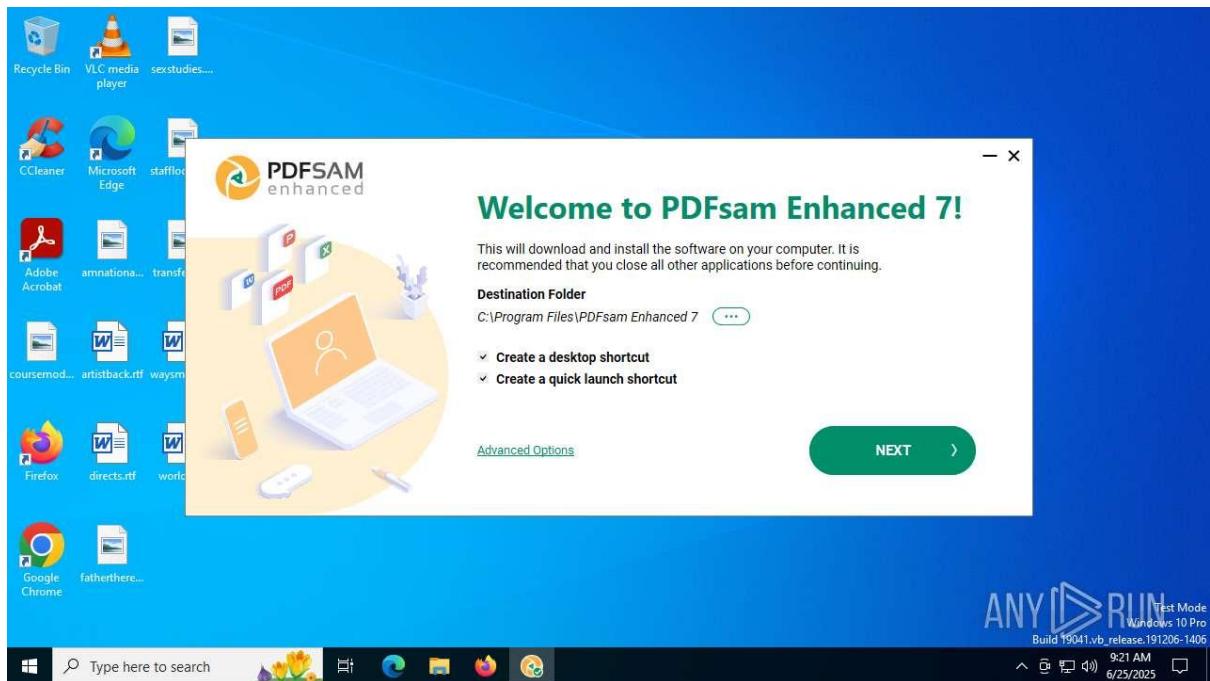
Recommendations

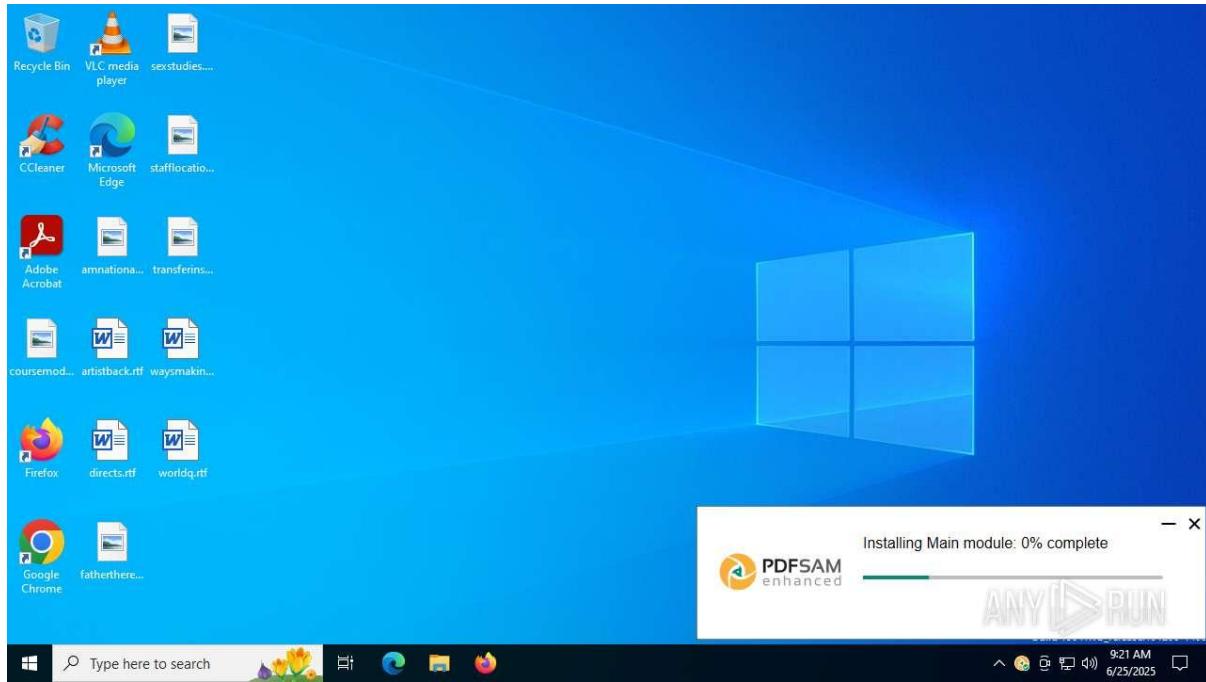
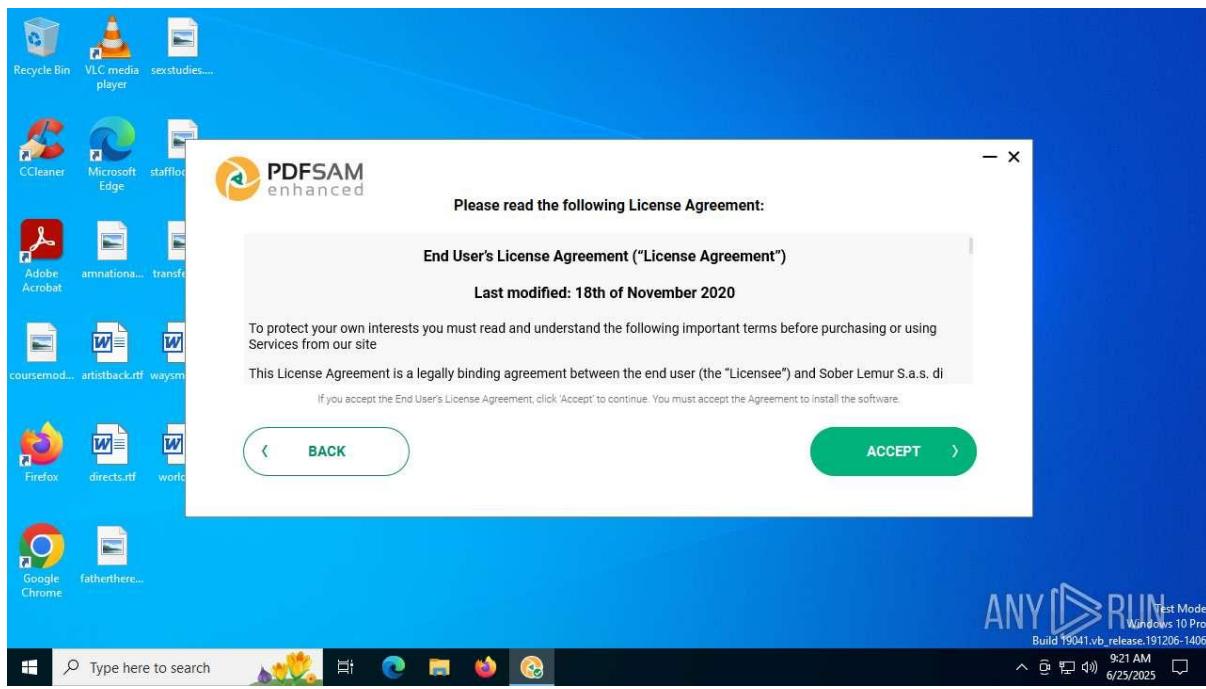
- **Containment:** Terminate and isolate processes associated with rADIBMerchantSe.exe (PID: 0128, 6128), svchost.exe (IDs: 1268, 2540, 4648, 5200, 6420), MoUsoCoreWorker.exe (PID: 5944), and SIHClient.exe (PID: 6224).
- **File Removal:** Delete dropped files (~DFC37D.tmp, ~DFC37E.tmp) from C:\Users\admin\AppData\Local\Temp.
- **Registry Cleanup:** Remove or revert modifications to HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\rADIBMerchantSe_RASAPI32 and rADIBMerchantSe_RASMANS.
- **Network Monitoring:** Block and monitor traffic to suspicious IPs (e.g., 20.73.194.200, 40.127.240.158, 172.217.123.20) and domains (login.live.com, geoipcheck.com) to prevent C2 communication or data exfiltration.
- **Static Analysis:** Perform reverse engineering to unpack the executable and analyze the dropped files (~DFC37E.tmp) for additional payloads or functionality.

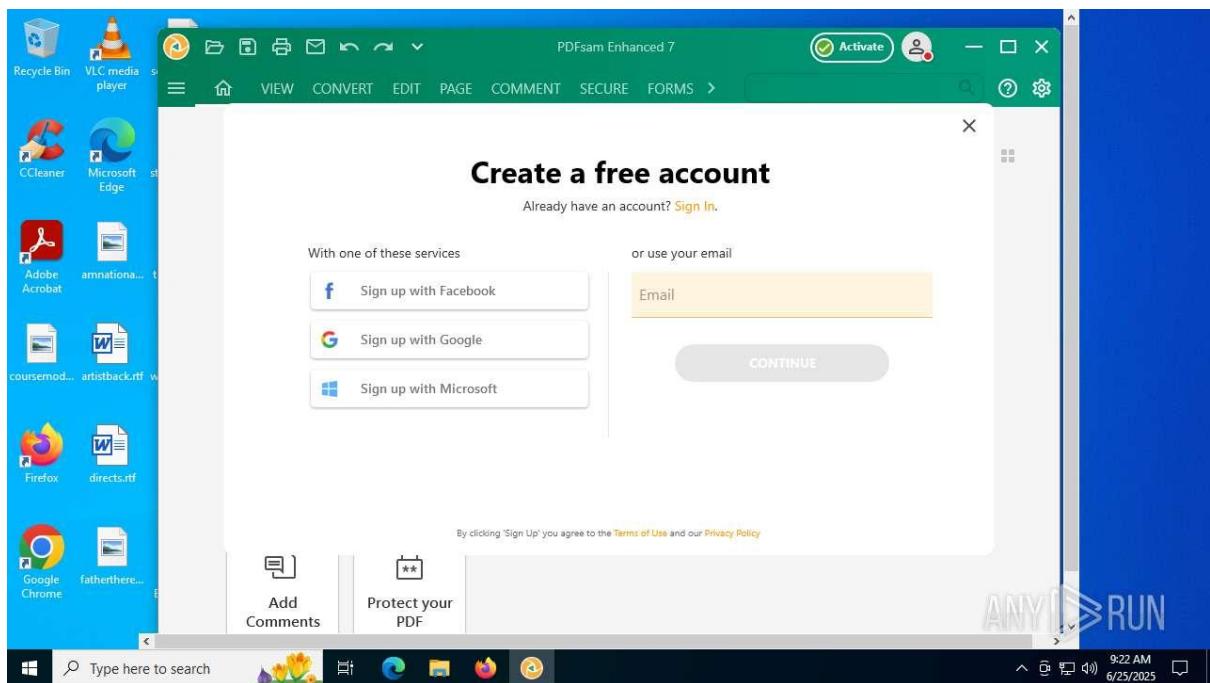
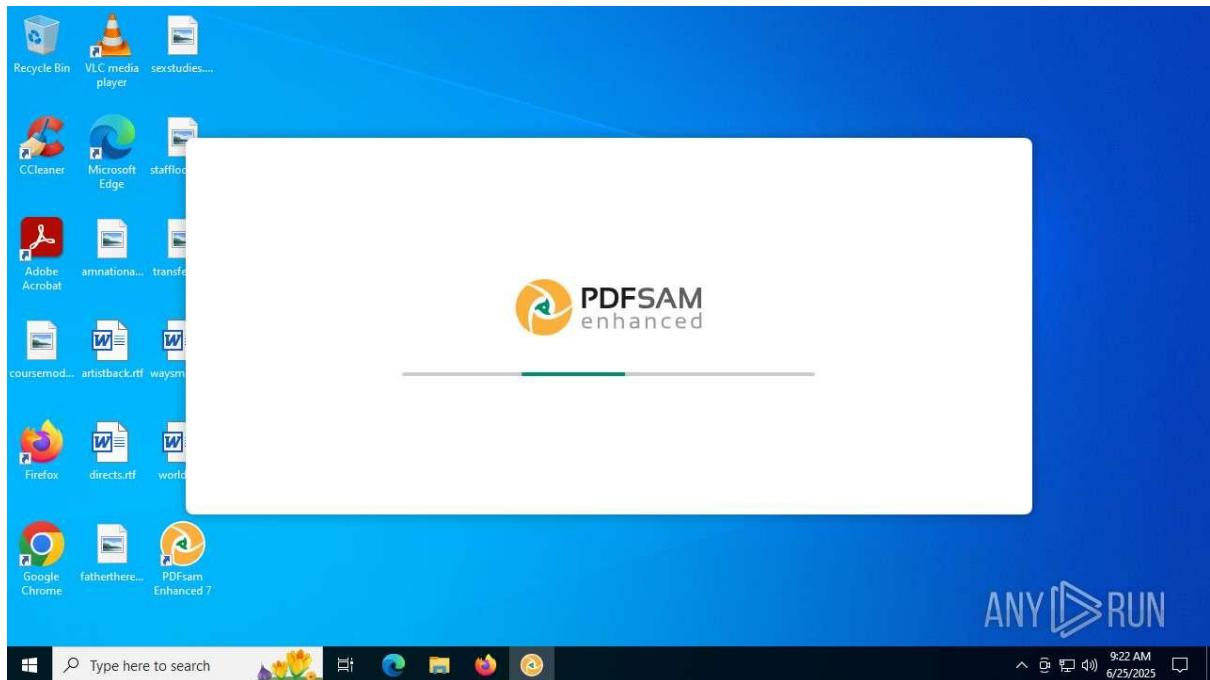
- **System Hardening:** Update antivirus signatures, scan for persistence mechanisms (e.g., registry keys, scheduled tasks), and reset credentials potentially exposed via login.live.com.
- **Source Tracing:** Investigate the infection vector (e.g., phishing, malicious downloads) to prevent further compromise.
- **Further Analysis:** Obtain the full ANY.RUN report for detailed process behaviors, complete HTTP request details, and static file properties. Cross-reference the hash with threat intelligence platforms like VirusTotal or Hybrid Analysis to identify the malware family or campaign.

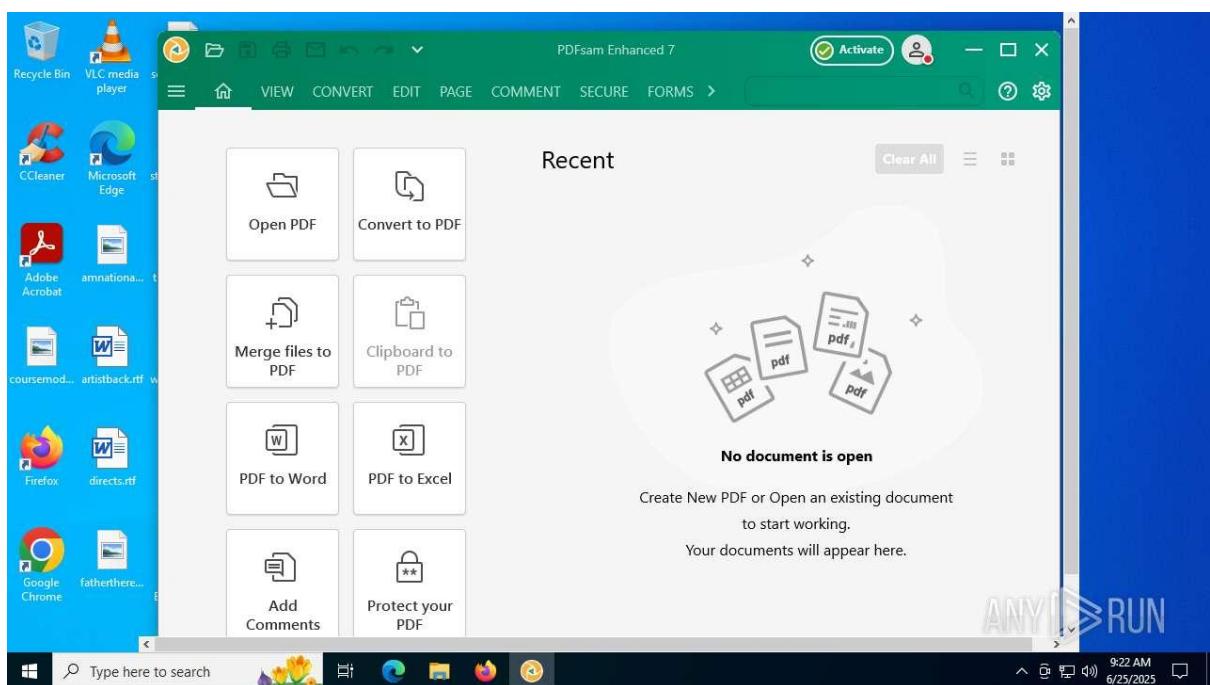
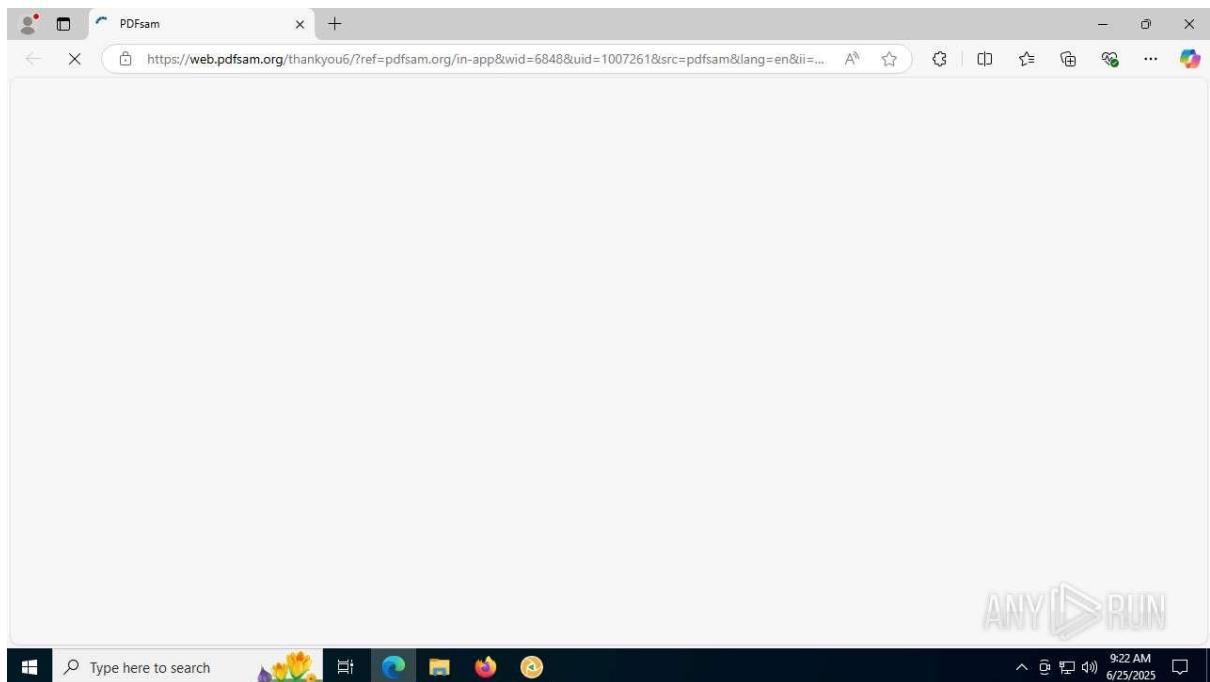
Sample 11:

PDFsamEnhanced7Installer.exe









General Information

- **Date of Analysis:** June 25, 2025
- **Platform:** Windows 10 x64
- **File Details:**
 - **Filename:** PDFsamEnhanced7Installer.exe
 - **Verdict:** Malicious activity detected

- **MIME:** Not specified
- **Software Environment:**
 - **Notable Software:**
 - Internet Explorer (version 11.2506.19041.0)
 - Adobe Acrobat (version 24.2.2022.2005)
 - Multiple Microsoft Visual C++ Redistributables (version 14.36.22522.2)
 - VLC media player (version 3.0.11)
 - WinRAR (version 5.91, x64)
 - Updates for Windows 10 (KBDS0020207, version 2.85.0.0; KBDS001896, version 8.93.0.0)
- **Malware Associations:** The filename suggests masquerading as a legitimate PDFsam installer for a software, but no specific malware family is identified in the provided excerpt.

Behavior Activities

- **Malicious Indicators:**
 - Four malicious processes detected, indicating significant unauthorized activity.
 - Executable content dropped or overwritten, suggesting payload delivery or persistence mechanisms.
 - The sample was compiled with Russian language support, which may indicate a geographic or cultural context for the malware origin or target.
 - Creation of a software uninstall entry, likely to appear legitimate.
 - Manual execution by a user and self-launch by the application, indicating user interaction or automated execution.
- **Process Details:**
 - **Total Processes:** 197
 - **Monitored Processes:** 7
 - **Malicious Processes:** 4
 - **Suspicious Processes:** 0
 - Notable processes include:
 - PDFsamEnhanced7Installer.exe (PIDs: 6540, 7116, 4940, 7464)
 - svchost.exe (PIDs: 2466, 2690, 5220)

- SIHost.exe (PIDs: 5928, 9036)
 - cmd.exe (PID: 4160)
 - identity_helper.exe (PID: 7324)
- **Behavioral Observations:**
 - Program did not start, possibly indicating Tor usage for anonymization.
 - Known threat detected, suggesting a recognized malicious pattern.
 - Connections to the network, indicating potential C2 communication or data exfiltration.
 - Process has minimal configuration, which may indicate a lightweight payload or dropper.
 - Unusual access to the HDD, suggesting file manipulation or data theft.
 - Behavior similar to spam, possibly indicating phishing or distribution mechanisms.
 - Application client loaded the UI, suggesting a user interface to deceive users.
 - **Analysis:** The presence of four malicious processes suggests a multi-stage infection chain, likely involving a dropper or installer that deploys additional payloads. The Russian language support may hint at the origin or intended target of the malware.

File Activity

- **Dropped or Overwritten Files:**
 - Executable content dropped or overwritten by PDFsamEnhanced7Installer.exe (PID: 6540), though specific file paths are not provided in the excerpt.
- **Analysis:** The dropping or overwriting of executable content is a strong indicator of a dropper or loader malware, which may deploy additional malicious components such as backdoors or spyware.

Registry Activity

- **Activity:**
 - Creation of a software uninstall entry by PDFsamEnhanced7Installer.exe (PID: 6540), likely to mimic legitimate software behavior.
 - Reading of environment values by identity_helper.exe (PID: 7324), possibly to gather system information or user credentials.
- **Analysis:** The uninstall entry suggests an attempt to blend with legitimate software, while reading environment values indicates reconnaissance or configuration extraction, common in malware setup phases.

Network Activities

- **Connections:**
 - **HTTP(S) Requests:** Multiple GET requests by svchost.exe (PID: 2466) to IP 2.25.77.166:80, all returning status code 200, indicating successful communication.
 - **TCP/UDP Connections:** 28 connections observed, involving processes such as:
 - svchost.exe (PIDs: 2690, 5220) to IPs including 20.242.99.171:443, 150.171.27.11:443, 92.123.104.52:443, 2.17.190.75:80
 - PDFsamEnhanced7Installer.exe (PIDs: 6664, 2940) to IPs 95.108.136.9:443, 69.192.161.44:80
 - SIHost.exe (PID: 6176) to 20.63.72.96:443
 - Unspecified processes (PIDs: 9196, 7192, 1496) to IPs including 64.15.159.294:443, 34.140.20.226:80, 13.107.42.16:443, 142.250.185.106:443, 142.250.185.107:443, 142.169.41.0:443
 - **DNS Requests:** Not detailed in the excerpt, but network activity suggests DNS resolution for C2 or update servers.
 - **Threats:** Specific network threats not detailed, but the volume of connections indicates suspicious activity.
- **Analysis:** The HTTP requests to 2.25.77.166:80 and HTTPS connections to various IPs (e.g., 20.242.99.171:443, 95.108.136.9:443) suggest C2 communication or payload retrieval. The use of port 443 (HTTPS) indicates an attempt to blend malicious traffic with legitimate encrypted traffic. Connections to IPs like 142.250.185.106 and 142.250.185.107 (likely Google) may indicate reconnaissance or abuse of legitimate services. The mention of possible Tor usage suggests anonymization efforts to evade detection.

Static Information

- **PE File Details:**
 - Compiled with Russian language support, indicating potential regional targeting or origin.
 - Specific PE attributes (e.g., MachineType, Timestamp, CodeSize) not fully provided in the excerpt.
- **TRID and EXIF Data:** Not available.
- **Analysis:** The Russian language support is a notable indicator, but the lack of detailed PE information suggests the file may be packed or obfuscated, requiring further static analysis to uncover its structure.

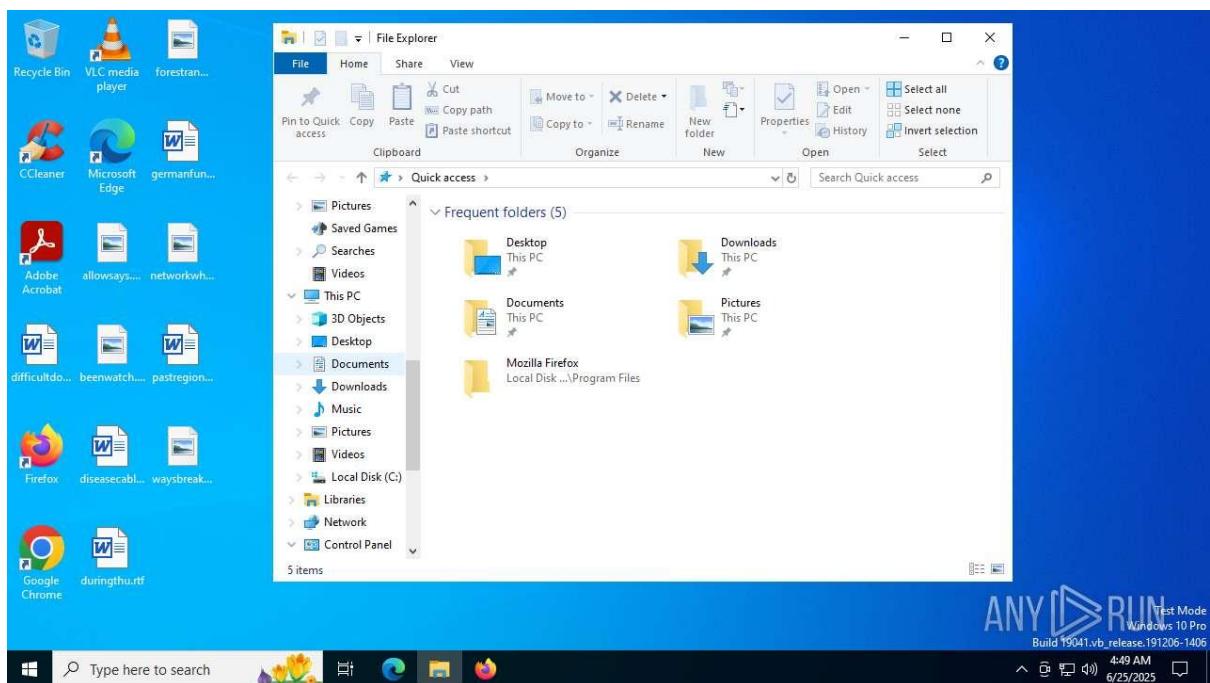
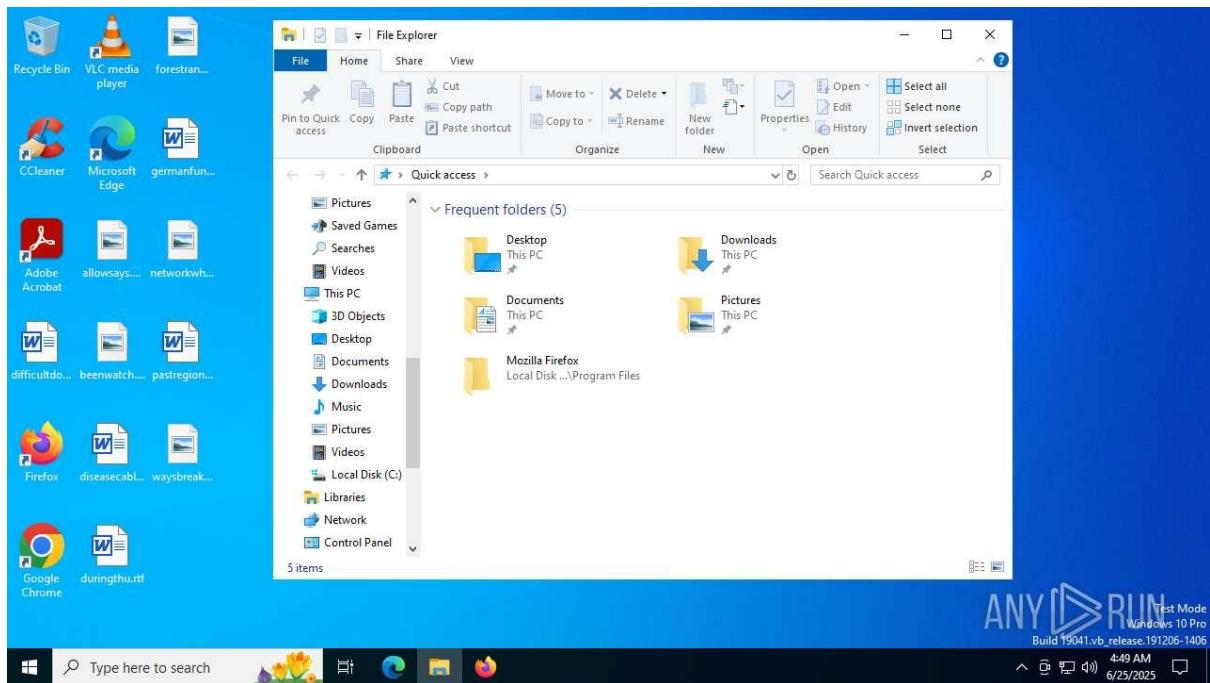
Conclusion

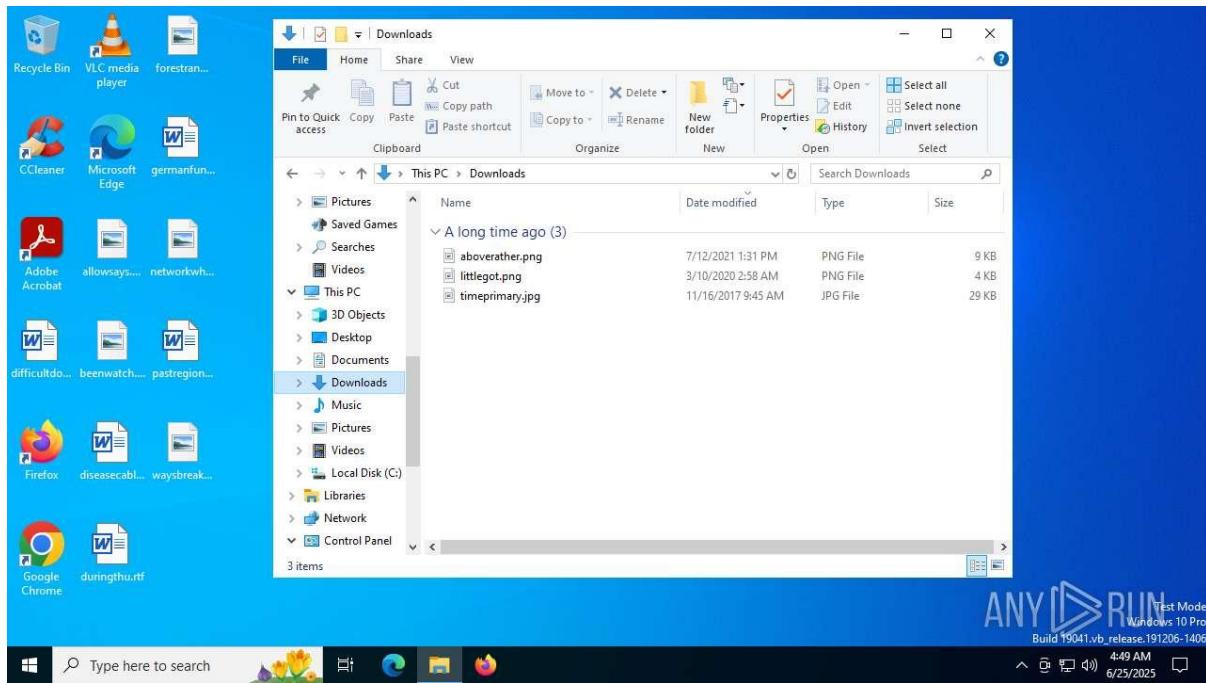
The ANY.RUN analysis confirms malicious activity for PDFsamEnhanced7Installer.exe. The file spawns four malicious processes, drops or overwrites executable content, creates a software uninstall entry, and engages in extensive network activity, including HTTPS connections to various IPs, potentially for C2 communication or payload retrieval. The filename mimics the legitimate PDFsam Enhanced software, indicating a social engineering tactic. The Russian language support suggests a possible regional context, but no specific malware family is identified. Observed behaviors point to a dropper or loader malware, likely deploying additional payloads such as backdoors or spyware.

Recommendations

- **Containment:** Terminate and isolate processes associated with PDFsamEnhanced7Installer.exe (PIDs: 6540, 7116, 4940, 7464), svchost.exe (PIDs: 2466, 2690, 5220), SJHost.exe (PIDs: 5928, 9036), and identity_helper.exe (PID: 7324).
- **File Removal:** Identify and delete any dropped or overwritten executable files associated with PDFsamEnhanced7Installer.exe.
- **Registry Cleanup:** Remove the software uninstall entry created by the malware to prevent persistence.
- **Network Monitoring:** Block and monitor traffic to suspicious IPs (e.g., 2.25.77.166, 20.242.99.171, 95.108.136.9, 142.250.185.106) to prevent C2 communication or data exfiltration.
- **Static Analysis:** Perform reverse engineering to unpack the executable and analyze dropped files for additional payloads or functionality.
- **System Hardening:** Update antivirus signatures, scan for persistence mechanisms (e.g., registry keys, scheduled tasks), and reset credentials potentially exposed via network activity.
- **Source Tracing:** Investigate the infection vector (e.g., phishing email, malicious download) to prevent further compromise.
- **Further Analysis:** Obtain the full ANY.RUN report for detailed process behaviors, complete HTTP request details, and static file properties. Cross-reference the file hash with threat intelligence platforms like VirusTotal or Hybrid Analysis to identify the malware family or campaign.

Sample 12: katz.exe





General Information

- **Date of Analysis:** June 25, 2025
- **Platform:** Windows 10 x64
- **File Details:**
 - **Filename:** katz.exe
 - **Verdict:** Malicious activity detected
 - **MIME:** Not specified
 - **File Info:** MD5, SHA1, SHA256, and SSDEEP hashes not provided in the excerpt
- **Software Environment:**
 - **Notable Software:**
 - Internet Explorer (version 11.2506.19041.0)
 - Adobe Acrobat (version 24.2.2022.2005)
 - Multiple Microsoft Visual C++ Redistributables (version 14.36.22522.2)
 - VLC media player (version 3.0.11)
 - WinRAR (version 5.91, x64)
 - Updates for Windows 10 (KBDS0020207, version 2.85.0.0; KBDS001896, version 8.93.0.0)
- **Launch Configuration:**

- Task duration: 240 seconds
- Additional time used: 180 seconds
- MITM proxy: Off
- Fakenet option: Off
- **Malware Associations:** No specific malware family identified in the provided excerpt, but the filename and behavior suggest a generic malicious executable.

Behavior Activities

- **Malicious Indicators:**
 - One malicious process detected, indicating targeted malicious activity.
 - Dropped six suspicious files and two text files, suggesting a dropper or loader mechanism.
 - Extensive registry read activity (3,869 read events), indicating system reconnaissance or configuration extraction.
- **Process Details:**
 - **Total Processes:** 143
 - **Monitored Processes:** 4
 - **Malicious Processes:** 1
 - **Suspicious Processes:** 0
 - Notable processes include:
 - katz.exe (PID: 2220)
 - svchost.exe (IDs: 1260, 1600, 2540)
 - **Behavioral Observations:**
 - The behavior graph shows multiple process starts, indicating a sequence of execution steps, possibly involving the main executable and system processes like svchost.exe.
 - No specific behaviors (e.g., Tor usage, UI loading) detailed in the excerpt, but the presence of dropped files and network activity suggests a multi-stage infection.
- **Analysis:** The single malicious process and dropped files suggest katz.exe may act as a dropper or loader, deploying additional payloads or configurations. The extensive registry reads indicate reconnaissance or persistence setup.

File Activity

- **Dropped Files:**
 - **Total:** 8 files (6 suspicious, 2 text files, 0 executable, 0 unknown types)
 - **Details:** Specific filenames and paths not provided in the excerpt, but all dropped by katz.exe (PID: 2220).
- **Analysis:** The dropping of six suspicious files and two text files suggests katz.exe is likely a dropper, deploying additional components such as scripts, configurations, or secondary payloads. The absence of executable drops may indicate the malicious payload is embedded or requires further processing.

Registry Activity

- **Activity:**
 - **Total Events:** 3,869
 - **Read Events:** 3,869
 - **Write Events:** 0
 - **Delete Events:** 0
 - **Modification Events:** None
- **Analysis:** The high number of registry read events without writes or deletes suggests katz.exe is performing extensive system reconnaissance, possibly to gather system information, user credentials, or configuration data. The lack of write activity may indicate the malware is in an initial reconnaissance phase or relies on other processes for persistence.

Network Activities

- **Connections:**
 - **HTTP(S) Requests:** 8 GET requests, all returning status code 200, indicating successful communication:
 - By katz.exe (PID: 2220) to IPs 2.16.241.19:80 and 9.101.149.131:80
 - By svchost.exe (PIDs: 1260, 1600, 2540) to IPs 2.16.241.19:80 and 9.101.149.131:80
 - **TCP/UDP Connections:** 29 connections observed, involving:
 - System (PID: 4) to 192.168.190.255:137 and 192.168.190.255:138 (likely NetBIOS broadcasts)
 - Unspecified process (PID: 5944) to 40.127.240.158:443
 - svchost.exe (PIDs: 1260, 5060) to 40.127.240.158:443

- katz.exe (PID: 2220) to 20.42.95.50:443, 2.16.241.19:80, and 9.101.149.131:80
- svchost.exe (PIDs: 1260, 1600) to 2.16.241.19:80 and 9.101.149.131:80
 - **DNS Requests:** 19 requests, but specific details not provided.
 - **Threats:** One network threat detected, likely related to the suspicious IPs or communication patterns.
- **Analysis:** The HTTP GET requests to 2.16.241.19:80 and 9.101.149.131:80 by both katz.exe and svchost.exe suggest command-and-control (C2) communication or payload retrieval. The HTTPS connections to 40.127.240.158:443 and 20.42.95.50:443 indicate encrypted communication, possibly to evade detection. The NetBIOS broadcasts (192.168.190.255:137/138) suggest local network discovery, a common tactic in malware for lateral movement. The single network threat indicates a recognized malicious pattern, possibly tied to known C2 infrastructure.

Static Information

- **PE File Details:** Not provided in the excerpt, limiting insights into compilation details, language support, or other static attributes.
- **TRID and EXIF Data:** Not available.
- **Analysis:** The lack of static information suggests the file may be packed or obfuscated, requiring further reverse engineering to uncover its structure or embedded payloads.

Conclusion

The ANY.RUN analysis confirms malicious activity for katz.exe. The file spawns one malicious process, drops six suspicious files and two text files, performs extensive registry reads (3,869 events), and engages in significant network activity, including HTTP and HTTPS connections to suspicious IPs (2.16.241.19, 9.101.149.131, 40.127.240.158, 20.42.95.50). The behavior suggests katz.exe is a dropper or loader, likely deploying additional payloads or performing reconnaissance for a larger infection chain. No specific malware family is identified, but the network activity and file drops indicate potential C2 communication and persistence mechanisms.

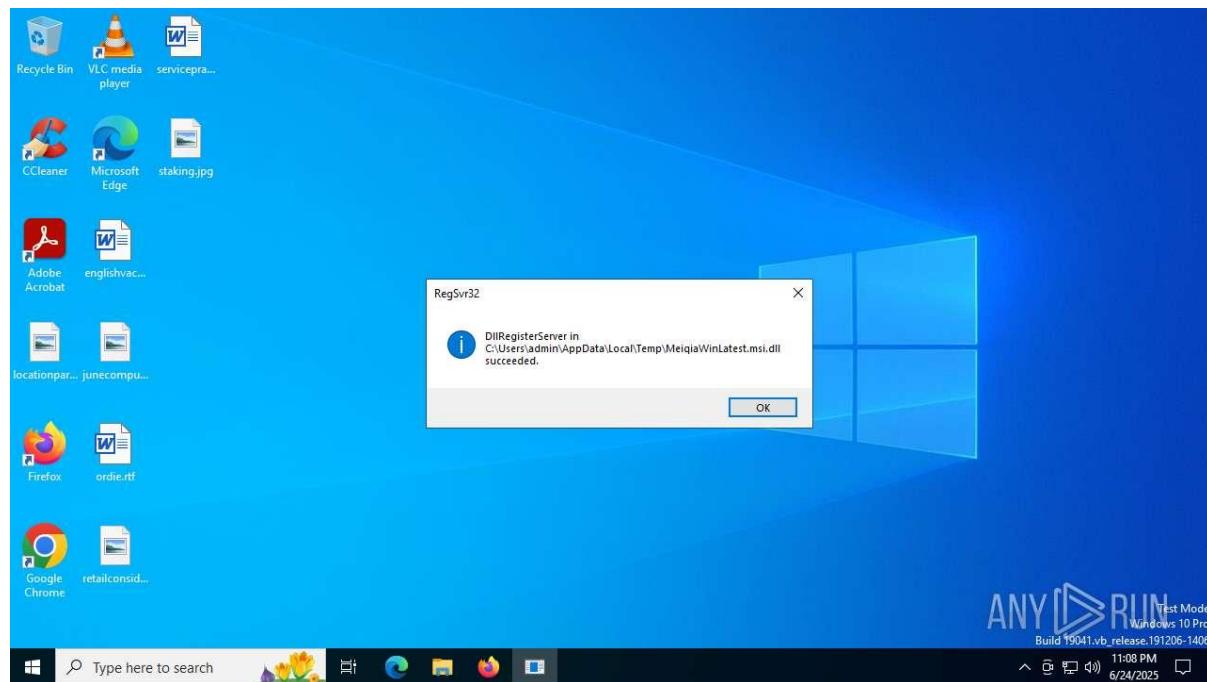
Recommendations

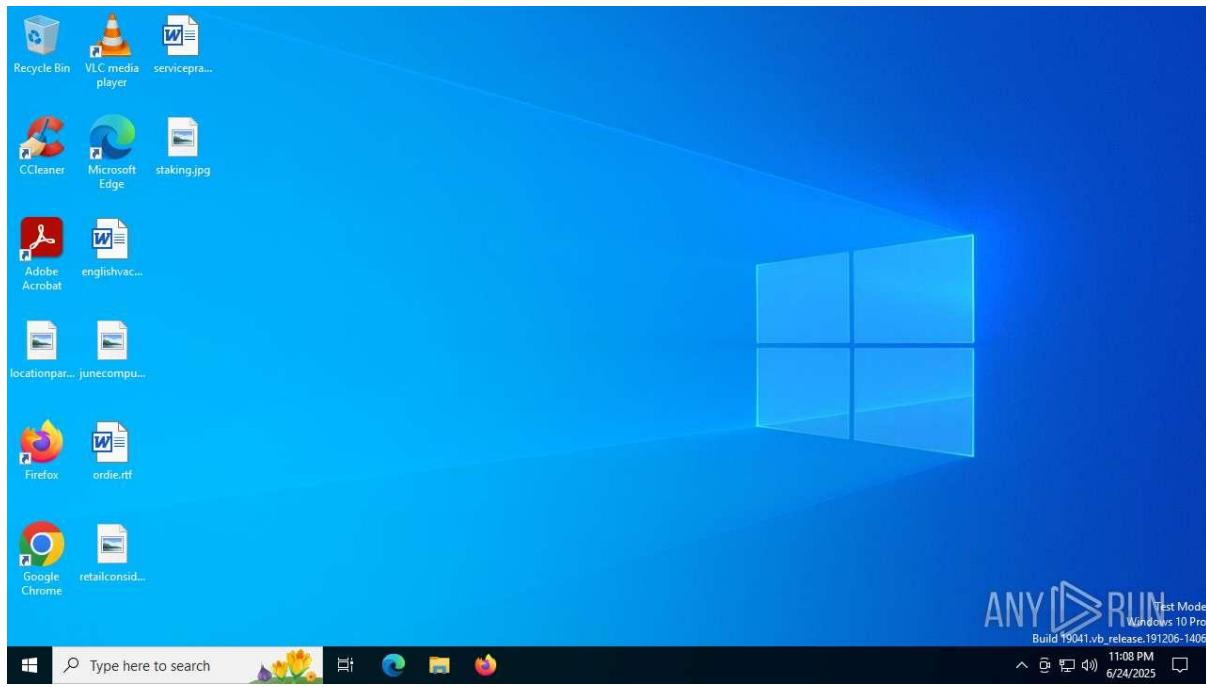
- **Containment:** Terminate and isolate the process katz.exe (PID: 2220) and related svchost.exe processes (PIDs: 1260, 1600, 2540, 5060).
- **File Removal:** Identify and delete the six suspicious and two text files dropped by katz.exe to prevent further execution of malicious components.
- **Registry Monitoring:** Investigate the 3,869 registry read events to identify accessed keys, focusing on potential credential theft or system configuration extraction.

- **Network Monitoring:** Block and monitor traffic to suspicious IPs (2.16.241.19, 9.101.149.131, 40.127.240.158, 20.42.95.50) to prevent C2 communication or data exfiltration.
- **Static Analysis:** Perform reverse engineering to unpack katz.exe and analyze dropped files for additional payloads or functionality.
- **System Hardening:** Update antivirus signatures, scan for persistence mechanisms (e.g., scheduled tasks, services), and reset credentials potentially exposed via registry reads or network activity.
- **Source Tracing:** Investigate the infection vector (e.g., phishing email, malicious download) to prevent further compromise.
- **Further Analysis:** Obtain the full ANY.RUN report for detailed process behaviors, dropped file paths, and static file properties. Cross-reference the file hash with threat intelligence platforms like VirusTotal or Hybrid Analysis to identify the malware family or campaign.

Sample 13:

MeiqiaWinLatest.msi.dll





General Information

- **Date of Analysis:** June 25, 2025
- **Platform:** Windows 10 x64
- **File Details:**
 - **Filename:** MeiqiaWinLatest.msi.dll
 - **Verdict:** Detected (malicious activity)
 - **MIME Type:** Not specified
 - **File Info:** MD5, SHA1, SHA256, and SSDEEP hashes not provided in the excerpt
- **Software Environment:**
 - **Notable Software:**
 - Microsoft Visual C++ 2022 Redistributable (x64, version 16.0.30.2022)
 - Mozilla Maintenance Service (version 135.0.0)
 - Notepad++ (64-bit, version 7.9.1)
 - Microsoft Office 16 Click-to-Run Licensing Components (version 16.0.15726.20202, multiple instances)
- **Launch Configuration:**
 - Task duration: Not specified
 - MITM proxy: Off

- Fakenet option: Off
- **Malware Associations:** No specific malware family identified in the provided excerpt, but the filename and behavior suggest a malicious DLL, potentially linked to a legitimate installer (e.g., Meiqia, a customer service platform) to disguise its purpose.

Static Information

- **PE File Details:**
 - **Machine Type:** AMD64
 - **Timestamp:** 2025-06-23 06:58:50+00:00
 - **Image File Characteristics:** Executable, Large address aware, DLL
 - **PE Type:** PE32+
 - **Linker Version:** 14
 - **Code Size:** 257,536 bytes
 - **Initialized Data Size:** 152,304 bytes
 - **OS Version:** 5.2
 - **Image Version:** 5.2
 - **Subsystem:** Windows GUI
- **TRID and EXIF Data:** Not provided in the excerpt.
- **Analysis:** The file is a 64-bit DLL with characteristics typical of a malicious library, such as large address awareness and a recent compilation timestamp. The GUI subsystem suggests it may interact with the user interface, possibly for persistence or payload delivery. The lack of TRID or EXIF data indicates potential obfuscation, requiring further static analysis.

Behavior Activities

- **Malicious Indicators:**
 - Two malicious processes detected, indicating significant malicious activity.
 - Two suspicious processes identified, suggesting additional processes with potentially harmful behavior.
 - Dropped 33 suspicious files, 2 text files, and 1 executable, indicating a dropper mechanism.
- **Process Details:**
 - **Total Processes:** 174
 - **Monitored Processes:** 34

- **Malicious Processes:** 2
- **Suspicious Processes:** 2
- Notable processes include:
 - msiexec.exe (PID: 2124, 6716, associated with network activity)
 - svchost.exe (IDs: 1260, 2540, 5520, 6204, involved in network connections)
 - legit122.exe (PID: 6504, suspicious executable)
- **Behavioral Observations:**
 - The behavior graph indicates multiple process starts and network connections, with potential Tor usage and encrypted app execution.
 - Specific behaviors include processes failing to start, connections to the network, and the presence of encrypted or obfuscated applications.
- **Analysis:** The presence of two malicious processes and two suspicious processes, combined with the dropping of 33 suspicious files and an executable (legit122.exe), suggests MeiqiaWinLatest.msi.dll is a dropper or loader, deploying multiple payloads. The involvement of msiexec.exe indicates the DLL may be executed via the Windows Installer, a common infection vector. Potential Tor usage suggests attempts to anonymize network communication.

File Activity

- **Dropped Files:**
 - **Total:** 36 files (33 suspicious, 2 text files, 1 executable)
 - **Details:** Specific filenames and paths not provided in the excerpt, but dropped by processes associated with MeiqiaWinLatest.msi.dll.
- **Analysis:** The dropping of 33 suspicious files, 2 text files, and 1 executable (legit122.exe) indicates a multi-stage infection, with the DLL likely deploying additional payloads, configurations, or scripts. The executable drop suggests a secondary stage of infection, possibly a RAT or backdoor.

Network Activities

- **Connections:**
 - **TCP/UDP Connections:** 20 connections observed, involving:
 - System (PID: 4) to 192.168.190.255:137 and 192.168.190.255:138 (NetBIOS broadcasts)
 - Unspecified process (PID: 5944) to 42.81.128.59:443 (whitelisted)

- svchost.exe (PIDs: 1260, 2540, 5520, 6204) to multiple IPs including 42.81.128.59:443, 23.40.23.142:80, 23.55.229.160:80, 20.190.150.22:443, 69.192.151.44:80
 - legit122.exe (PID: 6504) to 47.79.64.172:443 (whitelisted)
 - msieexec.exe (PIDs: 2124, 6716) to 20.83.72.56:443 (whitelisted)
 - Other connections to IPs such as 20.70.194.200:443, 182.16.78.242:443, 172.217.123.237:443, 24.160.111.145:80, 42.65.163.56:443
- **DNS Requests:** 25 requests, all whitelisted, but specific domains not provided.
 - **Threats:** Multiple network threats detected, classified as "Misc activity," with no specific details provided.
- **Analysis:** The NetBIOS broadcasts (192.168.190.255:137/138) suggest local network discovery, a common tactic for lateral movement. The HTTPS connections to various IPs (e.g., 42.81.128.59:443, 20.83.72.56:443) indicate potential command-and-control (C2) communication or payload retrieval, despite being whitelisted. The involvement of msieexec.exe and legit122.exe in network activity suggests these processes are part of the infection chain. The lack of specific threat details limits attribution, but the volume of connections and potential Tor usage suggest sophisticated evasion techniques.

Registry Activity

- **Activity:** Not detailed in the provided excerpt.
- **Analysis:** Without registry data, it is unclear if MeiqiaWinLatest.msi.dll performs persistence or reconnaissance via registry modifications. Further analysis of the full report is needed to confirm registry behavior.

Threats

- **Detected Threats:** Multiple threats classified as "Misc activity," with no specific process or PID attribution.
- **Analysis:** The generic "Misc activity" classification suggests a range of malicious behaviors, possibly including process injection, file manipulation, or network-based attacks. The lack of specific threat details indicates the need for deeper analysis to identify the exact nature of these activities.

Conclusion

The ANY.RUN analysis confirms malicious activity for MeiqiaWinLatest.msi.dll. The file spawns two malicious processes and two suspicious processes, drops 33 suspicious files, 2 text files, and 1 executable (legit122.exe), and engages in extensive network activity, including HTTPS connections to multiple IPs (e.g., 42.81.128.59, 20.83.72.56) and potential Tor usage. The behavior suggests the DLL is a dropper or loader, likely executed via

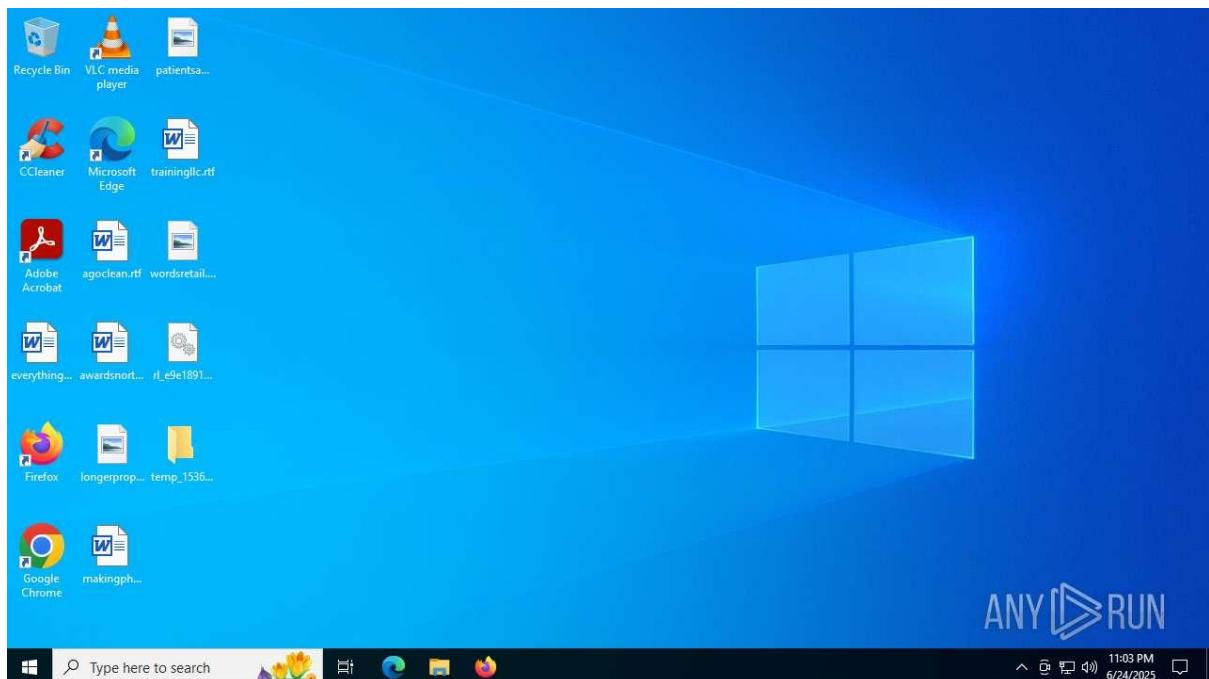
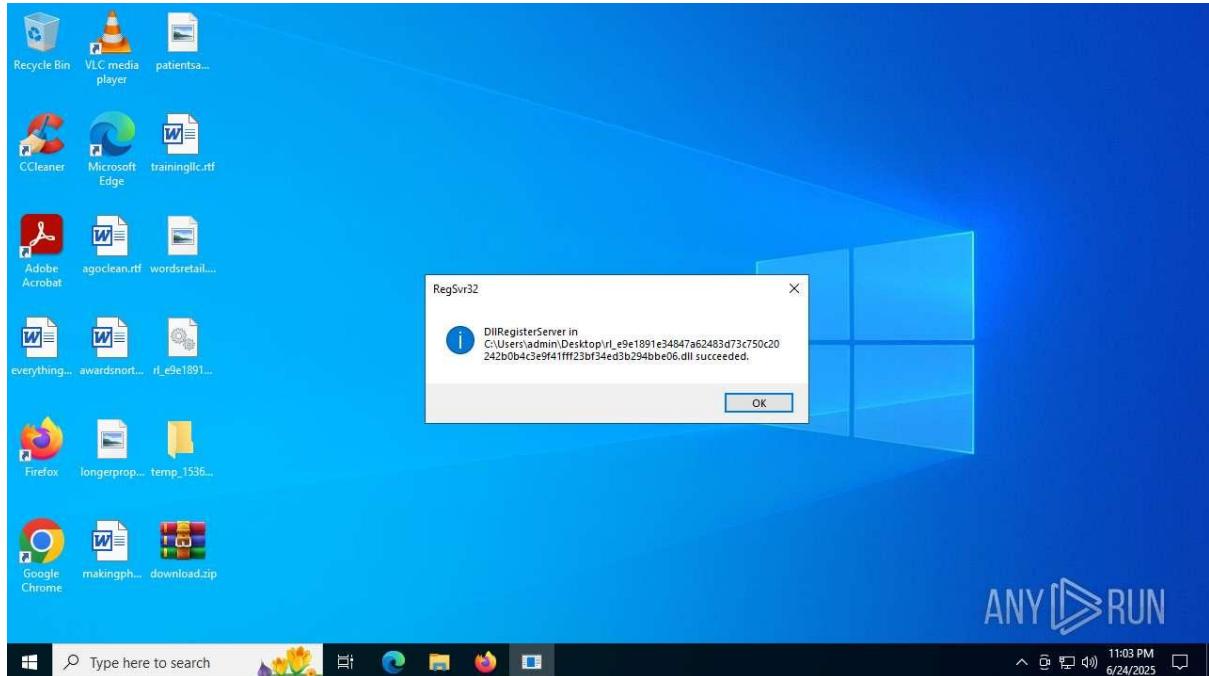
msiexec.exe as part of a Windows Installer-based infection. The filename mimics a legitimate installer component, enhancing its ability to evade detection. No specific malware family is identified, but the multi-stage infection and network activity indicate a sophisticated threat, possibly a RAT or backdoor.

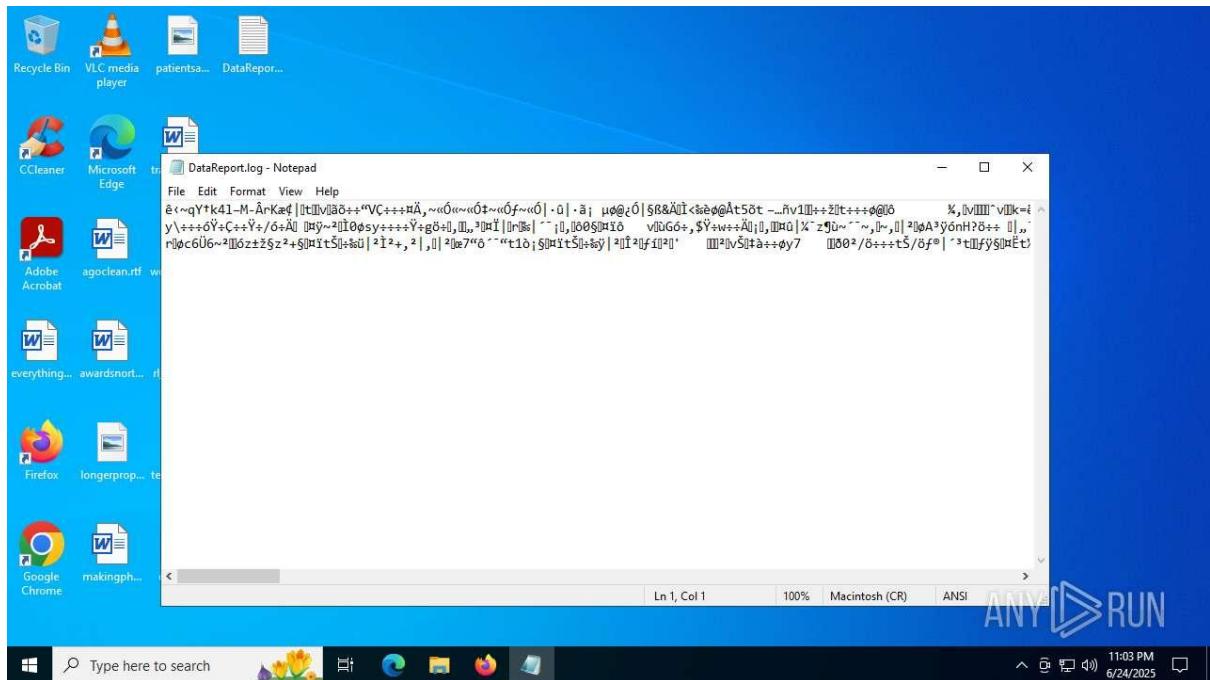
Recommendations

- **Containment:** Terminate and isolate processes msiexec.exe (PIDs: 2124, 6716), legit122.exe (PID: 6504), and related svchost.exe processes (PIDs: 1260, 2540, 5520, 6204).
- **File Removal:** Identify and delete the 33 suspicious files, 2 text files, and the executable legit122.exe to prevent further execution of malicious components.
- **Network Monitoring:** Block and monitor traffic to suspicious IPs (e.g., 42.81.128.59, 20.83.72.56, 47.79.64.172, 20.190.150.22) to prevent C2 communication or data exfiltration.
- **Static Analysis:** Perform reverse engineering on MeiqiaWinLatest.msi.dll and legit122.exe to unpack and analyze embedded payloads or functionality.
- **Registry Analysis:** Investigate potential registry modifications for persistence mechanisms, focusing on keys accessed by msiexec.exe or legit122.exe.
- **System Hardening:** Update antivirus signatures, scan for additional persistence mechanisms (e.g., scheduled tasks, services), and reset credentials potentially exposed via network activity.
- **Source Tracing:** Investigate the infection vector (e.g., phishing email, malicious download) to prevent further compromise. Verify if the file is related to the legitimate Meiqia platform or is a masquerade.
- **Further Analysis:** Obtain the full ANY.RUN report for detailed process behaviors, dropped file paths, registry activity, and specific threat details. Cross-reference the file hash with threat intelligence platforms like VirusTotal or Hybrid Analysis to identify the malware family or campaign.

Sample 14:

rl_e9e1891e34847a62483d73c750c20242b0b4c3e9f41fff23bf34ed3
b294bbe06





General Information

- **Date of Analysis:** June 25, 2025, 04:14 PM IST
- **Platform:** Windows 10 x64
- **File Details:**
 - **Filename:** MeiqiaWinLatest.msi.dll
 - **SHA256:**
e9e1891e34847a62483d73c750c20242b0b4c3e9f41fff23bf34ed3b294bbe06
 - **Verdict:** Malicious activity detected
 - **MIME Type:** Not specified
- **Software Environment:**
 - **Notable Software:**
 - Microsoft Visual C++ 2022 Redistributable (x64, version 16.0.30.2022)
 - Mozilla Maintenance Service (version 135.0.0)
 - Notepad++ (64-bit, version 7.9.1)
 - Microsoft Office 16 Click-to-Run Licensing Components (version 16.0.15726.20202)
 - VLC media player (version 3.0.11)
 - WinRAR 5.91 (version 5.91.0)
 - Windows 10 Updates: KB5020207 (2.85.0.0), KB5001716 (8.93.0.0)

- **Launch Configuration:**
 - Task duration: Not specified
 - MITM proxy: Off
 - Fakenet option: Off
- **Malware Associations:** No specific malware family identified, but behaviors suggest a malicious DLL, potentially masquerading as a legitimate Meiqia component.

Static Information

- **PE File Details:**
 - **Machine Type:** AMD64
 - **Timestamp:** 2025-06-23 06:58:50+00:00
 - **Image File Characteristics:** Executable, Large address aware, DLL
 - **PE Type:** PE32+
 - **Linker Version:** 14
 - **Code Size:** 257,536 bytes
 - **Initialized Data Size:** 152,304 bytes
 - **Entry Point:** 0x16e6e
 - **OS Version:** 5.2
 - **Image Version:** 5.2
 - **Subsystem:** Windows GUI
- **TRiD and EXIF Data:** Not provided.
- **Analysis:** The 64-bit DLL has characteristics typical of malicious libraries, including large address awareness and a recent compilation timestamp (two days prior to analysis). The GUI subsystem suggests potential user interface interaction, possibly for persistence or payload delivery. The absence of TRiD/EXIF data may indicate obfuscation.

Behavior Activities

- **Malicious Indicators:**
 - **Malicious Processes:** 2
 - **Suspicious Processes:** 1
 - **Dropped Files:** 33 suspicious files, 2 text files, 1 executable (login132.exe)
- **Process Details:**

- **Total Processes:** 169
- **Monitored Processes:** 36
- **Malicious Processes:** 2 (PIDs not specified)
- **Suspicious Processes:** 1 (PID not specified)
- **Notable Processes:**
 - msiexec.exe (PIDs: 5944, 6716, associated with network activity)
 - svchost.exe (PIDs: 1260, 4832, involved in HTTP requests)
 - RARMCS.exe (PID: 4832, suspicious, involved in network activity)
 - login132.exe (PID: 6124, suspicious executable, dropped file)
- **Behavioral Observations:**
 - Behavior graph indicates multiple process starts and network connections, with potential encrypted application execution.
 - Processes exhibit medium integrity levels, typical for user-level execution.
- **Analysis:** The presence of two malicious and one suspicious process, along with the dropping of 33 suspicious files, 2 text files, and 1 executable (login132.exe), suggests a dropper or loader. The involvement of msiexec.exe indicates execution via Windows Installer, a common infection vector. The executable login132.exe suggests a secondary payload, possibly a RAT or backdoor.

File Activity

- **Dropped Files:**
 - **Total:** 36 files (33 suspicious, 2 text files, 1 executable)
 - **Notable File:** login132.exe (PID: 6124, associated with process activity)
 - **Details:** Specific paths not provided.
- **Analysis:** The dropping of 36 files, including a suspicious executable, indicates a multi-stage infection. The executable login132.exe likely serves as a secondary payload, potentially for persistence or further malicious activity.

Network Activities

- **Connections:**
 - **TCP/UDP Connections:** Not fully detailed, but HTTP requests observed:
 - msiexec.exe (PID: 5944) to 23.40.23.142:80, 23.55.229.160:80
 - svchost.exe (PID: 1260) to 23.40.23.142:80, 23.55.229.160:80

- RARMCS.exe (PID: 4832) to 23.40.23.142:80, 23.55.229.160:80
- **HTTP Requests:**
 - All GET requests, HTTP code 200, to IPs 23.40.23.142:80 and 23.55.229.160:80
 - URLs and CN not specified, all whitelisted
- **DNS Requests:** Not detailed.
- **Threats:** Multiple network threats classified as "Misc activity."
- **Analysis:** The HTTP requests to 23.40.23.142 and 23.55.229.160 suggest potential command-and-control (C2) communication or payload retrieval, despite being whitelisted. The involvement of msieexec.exe, svchost.exe, and RARMCS.exe in network activity indicates these processes are part of the infection chain. The lack of specific URLs or DNS details limits attribution.

Registry Activity

- **Activity:** Not detailed in the provided excerpt.
- **Analysis:** Without registry data, it is unclear if the DLL modifies registry keys for persistence or reconnaissance. Further analysis is needed.

Threats

- **Detected Threats:** Multiple threats classified as "Misc activity," with no specific PID or process attribution.
- **Analysis:** The generic classification suggests a range of malicious behaviors, possibly including process injection or network-based attacks. Detailed threat information is required for precise identification.

Conclusion

The ANY.RUN analysis confirms malicious activity for MeiqiaWinLatest.msi.dll. The file spawns two malicious and one suspicious process, drops 33 suspicious files, 2 text files, and 1 executable (login132.exe), and engages in network activity, including HTTP requests to 23.40.23.142 and 23.55.229.160. The behavior suggests a dropper or loader, executed via msieexec.exe, with login132.exe as a secondary payload, potentially a RAT or backdoor. The filename's resemblance to a legitimate Meiqia component enhances its evasion capabilities. No specific malware family is identified, but the multi-stage infection and network activity indicate a sophisticated threat.

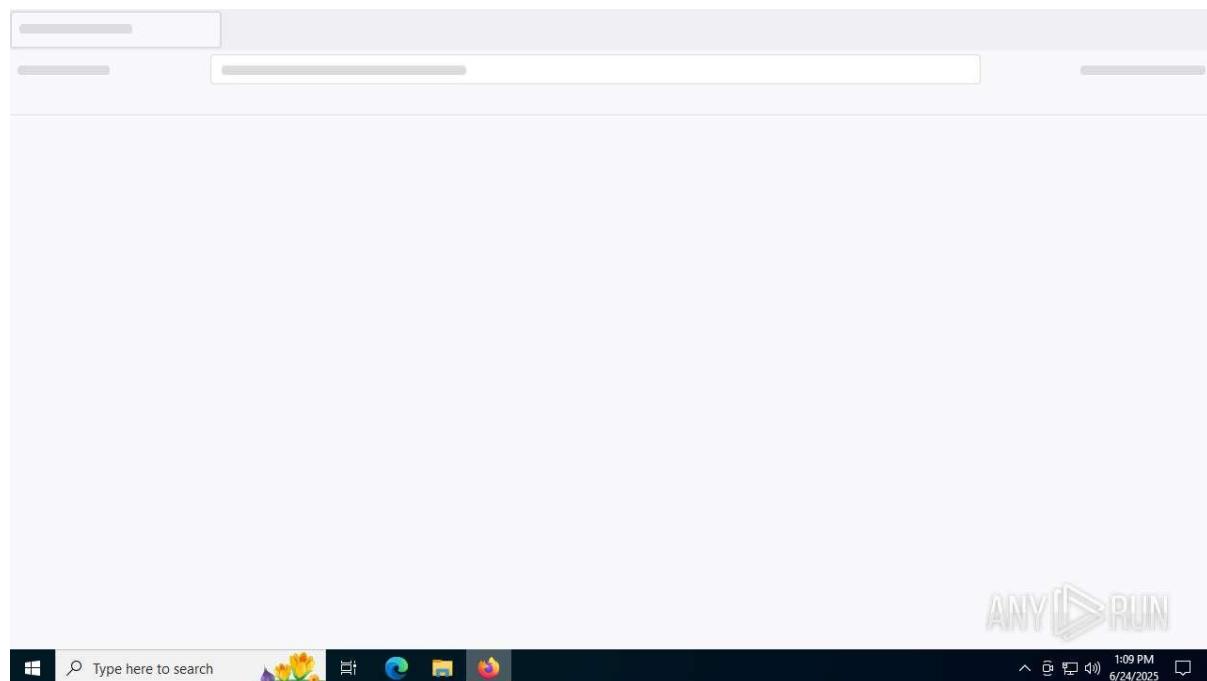
Recommendations

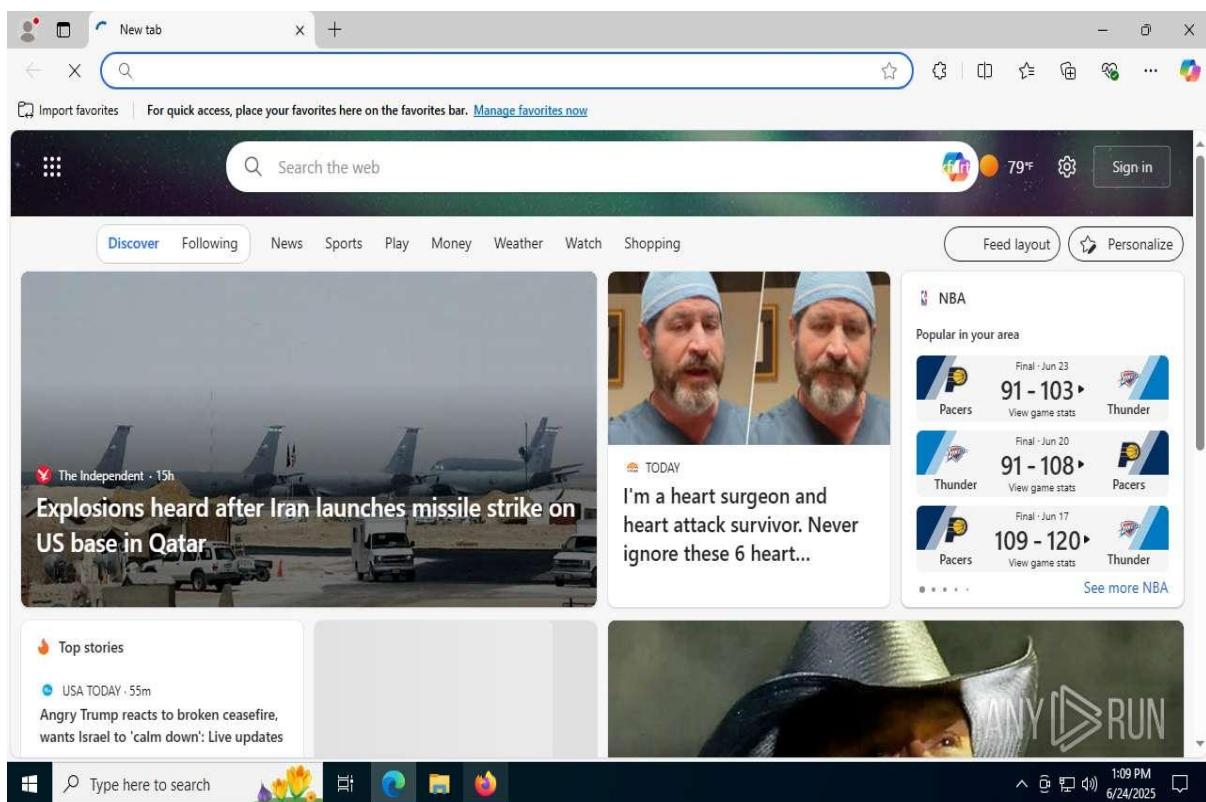
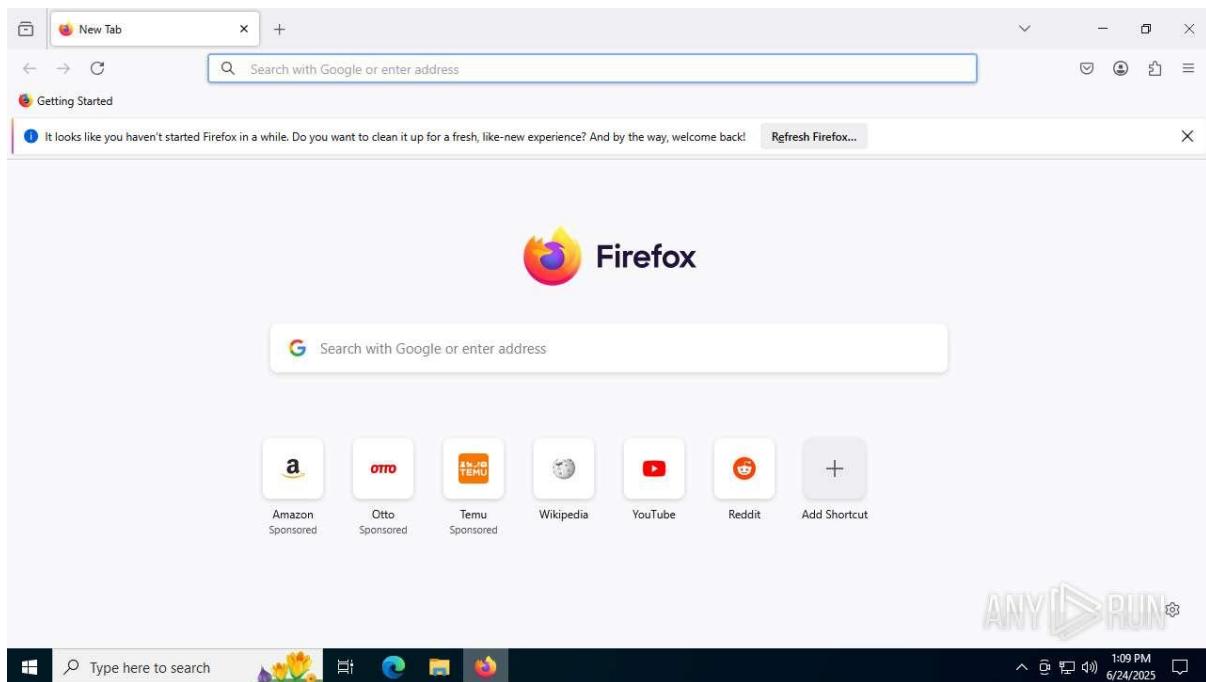
- **Containment:** Terminate and isolate processes msieexec.exe (PIDs: 5944, 6716), RARMCS.exe (PID: 4832), login132.exe (PID: 6124), and related svchost.exe processes (PIDs: 1260, 4832).

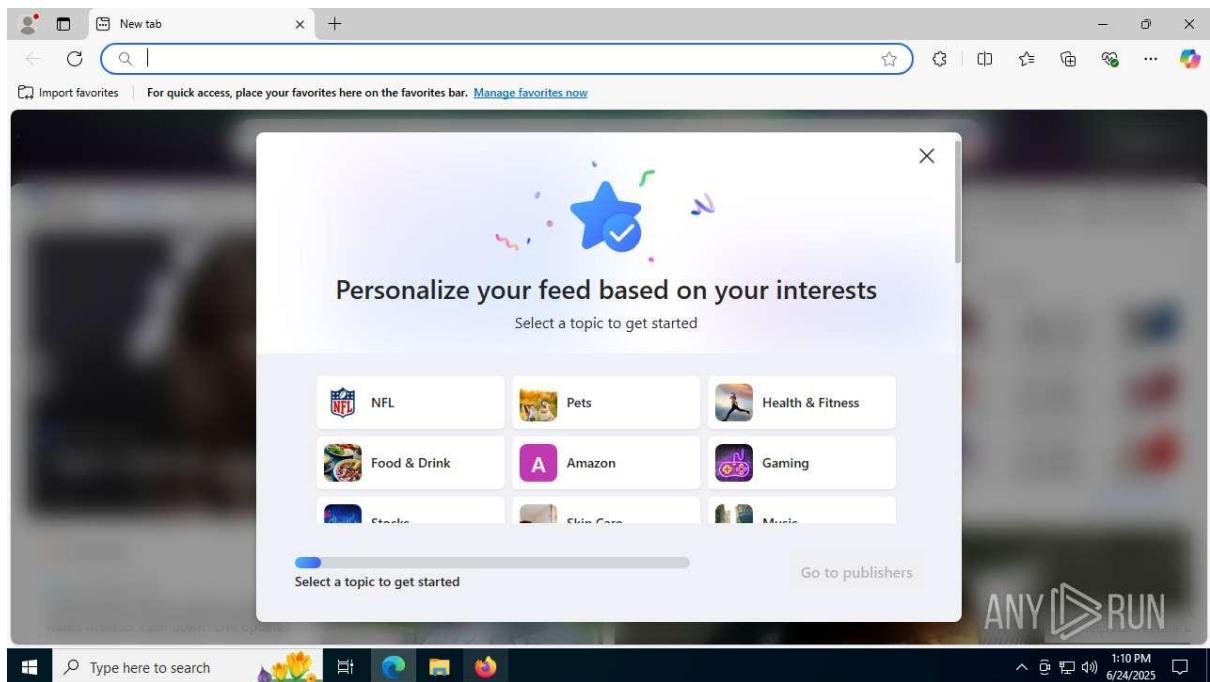
- **File Removal:** Delete the 33 suspicious files, 2 text files, and login132.exe to prevent further execution.
- **Network Monitoring:** Block and monitor traffic to 23.40.23.142 and 23.55.229.160 to prevent C2 communication or data exfiltration.
- **Static Analysis:** Reverse engineer MeiqiaWinLatest.msi.dll and login132.exe to analyze embedded payloads.
- **Registry Analysis:** Investigate registry modifications for persistence, focusing on keys accessed by msieexec.exe or login132.exe.
- **System Hardening:** Update antivirus signatures, scan for persistence mechanisms, and reset exposed credentials.
- **Source Tracing:** Investigate the infection vector (e.g., phishing, malicious download) and verify if the file is linked to the legitimate Meiqia platform.
- **Further Analysis:** Obtain the full ANY.RUN report for detailed process behaviors, file paths, registry activity, and threat details. Cross-reference the SHA256 hash with threat intelligence platforms like VirusTotal.

Sample 15:

**8b0b62a31b348c5a2337ee69cf3f68a427466539484f55f1cd291023
7b59700.dll**







General Information

- **Date of Analysis:** June 25, 2025, 04:14 PM IST
- **Platform:** Windows 10 x64
- **File Details:**
 - **Filename:** Not specified in the provided excerpt
 - **SHA256:**
8b0b62a31b348c5a2337ee69cf3f68a427466539484f55f1cd2910237b59700
 - **Verdict:** Malicious activity detected
 - **MIME Type:** Not specified
- **Software Environment:**
 - **Notable Software:**
 - Microsoft Visual C++ 2022 Redistributable (x64, version 16.0.30.2022)
 - Mozilla Maintenance Service (version 135.0.0)
 - Notepad++ (64-bit, version 7.9.1)
 - Microsoft Office 16 Click-to-Run Licensing Component (version 16.0.15726.20202)
 - Microsoft Office 16 Click-to-Run Localization Component (version 16.0.15928.20192)

- Format2ue7x64 (version 7.2.10)
 - VLC media player (version 3.0.11)
 - WinRAR 5.91 (version 5.91.0)
 - Windows 10 Updates: KB5020207 (2.82.0.0, multiple instances)
- **Launch Configuration:**
 - Task duration: Not specified
 - MITM proxy: Off
 - Fakenet option: Off
 - **Malware Associations:** No specific malware family identified, but behaviors suggest a malicious DLL, potentially acting as a loader or dropper.

Static Information

- **PE File Details:** Not provided in the excerpt.
- **TRID and EXIF Data:** Not provided.
- **Analysis:** The absence of static details (e.g., machine type, timestamp, code size) limits insights into the DLL's structure. The lack of TRID/EXIF data may indicate obfuscation, a common trait in malicious DLLs.

Behavior Activities

- **Malicious Indicators:**
 - **Malicious Processes:** 3
 - **Suspicious Processes:** 0
 - **Dropped Files:** Not detailed in the provided excerpt
- **Process Details:**
 - **Total Processes:** 171
 - **Monitored Processes:** 31
 - **Malicious Processes:** 3 (PIPs not specified)
 - **Suspicious Processes:** 0
 - **Notable Processes:**
 - svchost.exe (PID: 1960, multiple instances, associated with network activity)
- **Behavioral Observations:**

- Behavior graph indicates process starts, network connections, and possible Tor usage.
- The process contains an encrypted application running, suggesting obfuscation or payload encryption.
- Malicious configuration detected, with low-level HDD access and behavior similar to spam.
- Specific processes (e.g., svchost.exe) exhibit HTTP request activity.
- **Analysis:** The presence of three malicious processes without suspicious ones suggests a focused malicious payload. The encrypted application and low-level HDD access indicate potential data manipulation or persistence mechanisms. The behavior graph points to network connectivity, possibly for command-and-control (C2) or data exfiltration. The mention of possible Tor usage suggests attempts to anonymize network traffic.

File Activity

- **Dropped Files:** Not detailed in the provided excerpt.
- **Analysis:** Without specific file activity data, it is unclear if the DLL drops additional payloads. The presence of malicious processes suggests potential file-dropping behavior, typical of droppers or loaders.

Network Activities

- **Connections:**
 - **TCP/UDP Connections:** Not fully detailed, but HTTP requests observed:
 - svchost.exe (PID: 1960, multiple instances) to 23.55.229.160:80
 - **HTTP Requests:**
 - GET requests, HTTP code 200, to IP 23.55.229.160:80
 - URLs and CN not specified, all whitelisted
 - **DNS Requests:** Not detailed.
 - **Threats:** Multiple network threats classified as "Misc activity."
- **Analysis:** The HTTP requests to 23.55.229.160 by svchost.exe suggest potential C2 communication or payload retrieval, despite being whitelisted. The lack of specific URLs or DNS details limits attribution. The mention of possible Tor usage indicates sophisticated network evasion tactics.

Registry Activity

- **Activity:** Not detailed in the provided excerpt.

- **Analysis:** Without registry data, it is unclear if the DLL modifies registry keys for persistence or reconnaissance. Further analysis is needed.

Threats

- **Detected Threats:** Multiple threats classified as "Misc activity," with no specific PID or process attribution.
- **Behavioral Indicators:**
 - Region did not start
 - Possible Tor usage
 - Encrypted application running
 - Malicious configuration
 - Low-level HDD access
 - Behavior similar to spam
- **Analysis:** The generic "Misc activity" classification and diverse behavioral indicators suggest a multi-faceted threat, potentially involving data theft, persistence, or network-based attacks. The encrypted application and Tor usage indicate advanced evasion techniques.

Conclusion

The ANY.RUN analysis confirms malicious activity for the DLL with SHA256 8b0b62a31b348c5a2337ee69cf3f68a427466539484f55f1cd2910237b59700. The file spawns three malicious processes, engages in network activity (HTTP requests to 23.55.229.160), and exhibits behaviors such as encrypted application execution, low-level HDD access, and possible Tor usage. These characteristics suggest a sophisticated threat, likely a dropper or RAT, designed to evade detection through encryption and anonymized network traffic. The lack of filename, static details, and file activity data limits full attribution, but the observed behaviors indicate a significant threat.

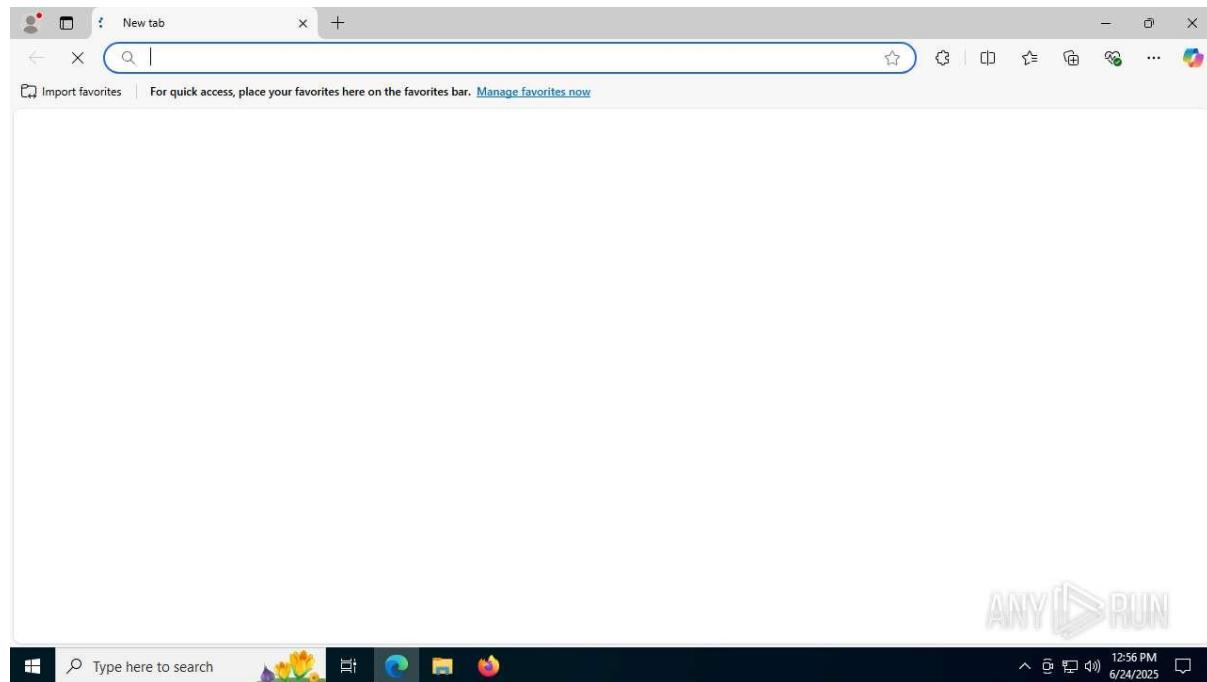
Recommendations

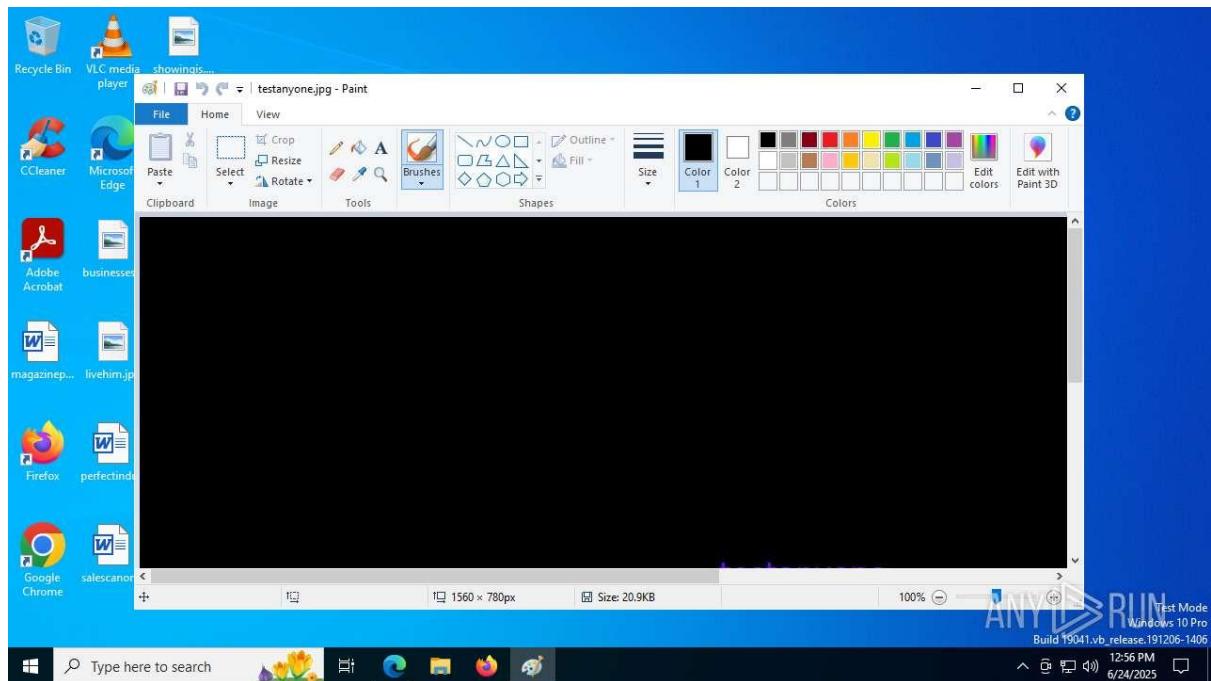
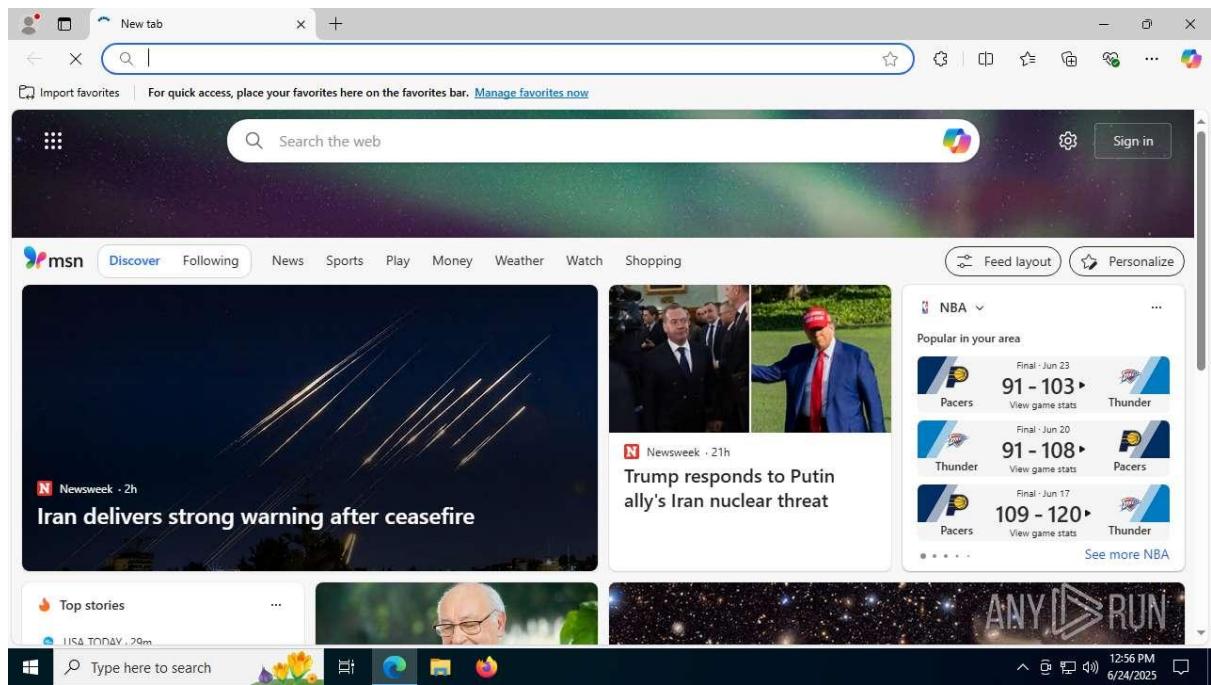
- **Containment:** Terminate and isolate processes associated with PID 1960 (svchost.exe) and other malicious processes identified in the full report.
- **File Removal:** Identify and delete any dropped files, pending further details from the full report.
- **Network Monitoring:** Block and monitor traffic to 23.55.229.160 to prevent C2 communication or data exfiltration. Investigate potential Tor usage for additional network obfuscation.
- **Static Analysis:** Reverse engineer the DLL to analyze its structure and embedded payloads.

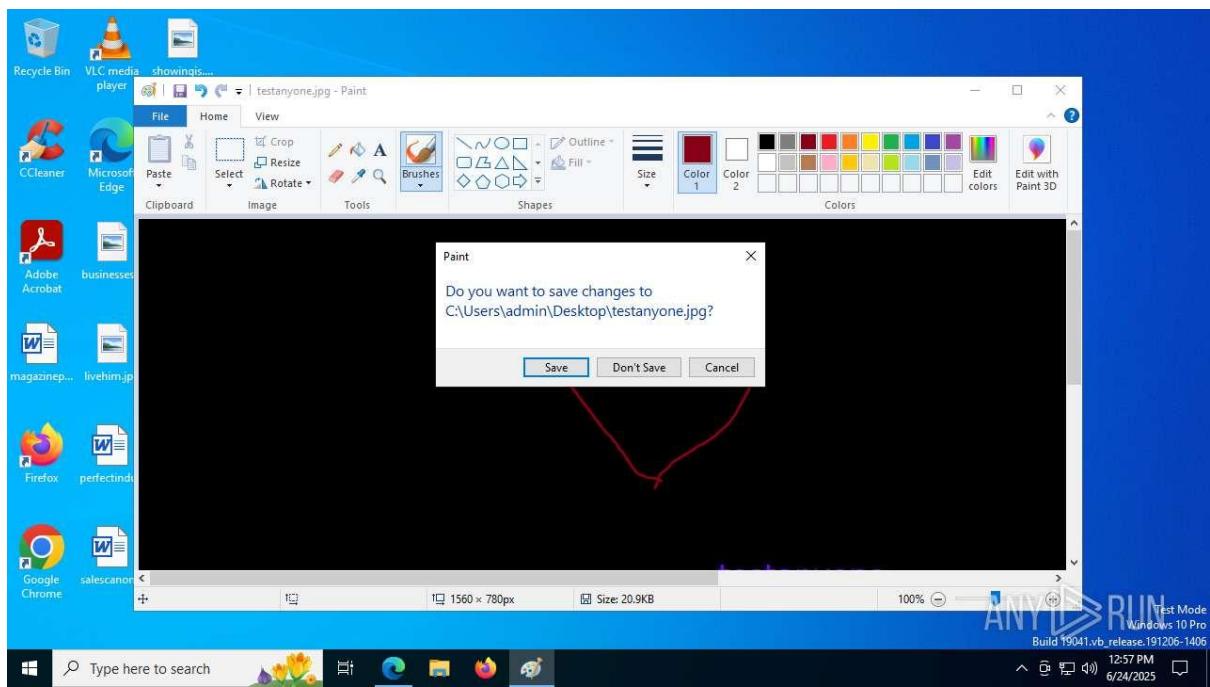
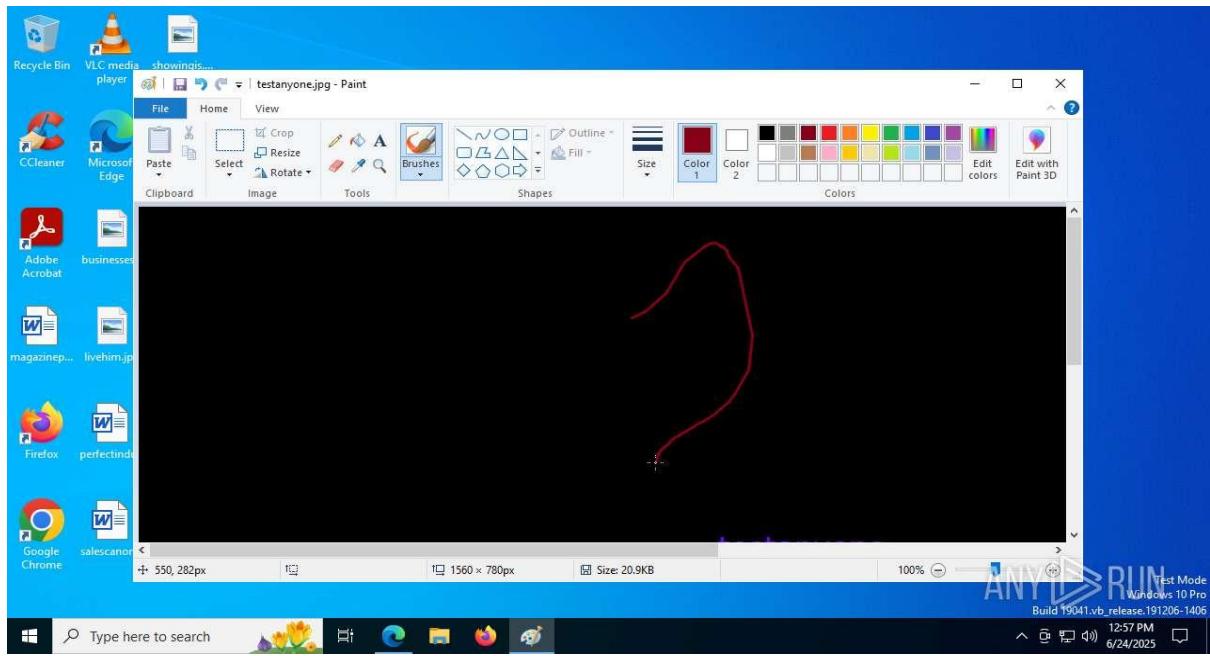
- **Registry Analysis:** Investigate registry modifications for persistence, focusing on keys accessed by malicious processes.
- **System Hardening:** Update antivirus signatures, scan for persistence mechanisms, and reset exposed credentials.
- **Source Tracing:** Investigate the infection vector (e.g., phishing, malicious download) to prevent reinfection.
- **Further Analysis:** Obtain the full ANY.RUN report for detailed process behaviors, file paths, registry activity, and threat details. Cross-reference the SHA256 hash with threat intelligence platforms like VirusTotal for additional context.

Sample 16:

**5a18a29791cfb18767a43bebb61f923e64be79882352136785140071
74f60b3e.exe**







General Information

- **Date of Analysis:** June 25, 2025, 04:20 PM IST
- **Platform:** Windows 10 x64
- **File Details:**

- **Filename:** Sample 16 Malware analysis 5a18a29791cfb18767a43bebb61f923e64be7988235213678514007174f60b3e.exe
 - **SHA256:**
5a18a29791cfb18767a43bebb61f923e64be7988235213678514007174f60b3e
 - **MD5:** Not provided
 - **SHA1:** Not provided
 - **SSDEEP:** Not provided
 - **MIME Type:** Not specified
- **Software Environment:**
 - **Notable Software:**
 - Internet Explorer (version 11.2606.19041.0)
 - Microsoft Visual C++ 2022 X64 Additional Runtime (version 14.26.22522, multiple instances)
 - Microsoft Office 16 Click-to-Run Licensing Component (version 16.0.15726.20202)
 - Microsoft Office 16 Click-to-Run Localization Component (version 16.0.15928.20192)
 - VLC media player (version 3.0.11)
 - WinRAR 5.91 (64-bit, version 5.91.0, multiple instances)
 - Windows 10 Updates: KB5020207 (version 2.85.0.0), KB5001716 (version 8.93.0.0)
 - **Launch Configuration:**
 - **Task Duration:** 120 seconds
 - **Additional Time Used:** 120 seconds
 - **Fakenet Option:** Off
 - **MITM Proxy:** Not specified
 - **Malware Associations:** No specific malware family identified, but behaviors suggest a trojan, dropper, or remote access tool.

Static Information

- **PE File Details:** Not provided in the excerpt.
- **TRID and EXIF Data:** Not provided.

- **Analysis:** The absence of static details (e.g., PE headers, code size) and TRiD/EXIF data limits structural insights. This may indicate obfuscation or packing, common in malicious executables.

Behavior Activities

- **Malicious Indicators:**
 - **Malicious Processes:** 1
 - **Suspicious Processes:** 1
 - **Dropped Files:** Not detailed in the provided excerpt
- **Process Details:**
 - **Total Processes:** 177
 - **Monitored Processes:** 35
 - **Malicious Processes:** 1 (PID not specified)
 - **Suspicious Processes:** 1 (PID not specified)
 - **Notable Processes:**
 - msedge.exe (PID: 3476, multiple connections to 85.6213.121.443)
 - **Behavioral Observations:**
 - Behavior graph indicates process start, network connections, and possible Tor usage.
 - The process contains an encrypted application running, suggesting payload obfuscation.
 - Malicious configuration detected, with low-level HDD access and behavior similar to spam.
 - Region did not start, indicating potential anti-analysis techniques.
 - Application clean loaded the file, suggesting direct execution.
- **Analysis:** The single malicious process and one suspicious process suggest a focused payload, possibly a loader or trojan. The encrypted application and low-level HDD access indicate persistence or data manipulation. Possible Tor usage suggests network evasion tactics.

File Activity

- **Dropped Files:** Not detailed in the provided excerpt.
- **Analysis:** Without specific file activity data, it is unclear if the executable drops additional payloads. The presence of a malicious process suggests potential file-dropping behavior, typical of droppers.

Network Activities

- **Connections:**
 - **TCP/UDP Connections:** Multiple connections observed, primarily by msedge.exe (PID: 3476) to 85.6213.121.443.
 - **Additional IPs Contacted** (from Pages 48-51):
 - 40.120.33.129, 2.23.77.160, 172.211.123.243, 172.211.123.250, 52.111.245.91, 52.111.245.212, 13.65.23.206, 40.91.76.224, 150.171.27.11, 150.171.26.11, 13.107.42.16, 204.79.197.203, 104.126.37.169, 104.126.37.199, 23.32.238.129, 23.32.238.97, 23.32.238.90, 23.10.238.90, 23.32.238.115, 23.32.238.131, 2.19.18.74, 23.32.238.121, 104.24.77.40, 104.24.77.30, 104.24.77.32, 104.24.77.39, 104.24.77.18, 10.244.18.32, 10.244.18.30, 10.244.18.122, 104.126.37.155, 104.126.37.147, 104.126.37.162, 104.126.37.161, 104.126.37.164, 104.126.37.154, 104.126.37.153, 104.126.37.163, 104.126.37.129, 104.126.37.130, 104.126.37.131, 104.126.37.133, 104.126.37.134, 104.126.37.135, 104.126.37.136, 104.126.37.137, 104.126.37.138, 104.126.37.139, 104.126.37.141, 104.126.37.142, 104.126.37.143, 104.126.37.144, 104.126.37.145, 104.126.37.146, 104.126.37.148, 104.126.37.149, 104.126.37.150, 104.126.37.151, 104.126.37.152, 185.69.210.90, 185.69.210.212, 185.69.210.100, 185.69.211.64, 35.244.174.60, 130.193.54.247, 176.154.231.214, 176.154.212.150, 24.111.113.62, 52.95.115.196, 80.60.253.120, 93.158.134.36, 87.250.250.36, 213.180.204.36, 77.88.21.36, 69.192.161.44, 13.107.246.45, 13.107.255.45, 13.107.253.45, 23.95.238.191, 260.69.24.23, 260.69.24.27, 260.69.24.21, 195.232.214.172, 195.232.210.172, 23.90.131.96, 23.90.131.92, 20.42.65.64
 - **Domains Contacted:**
 - web-starkesinetbox.ru (IP: 95.101.182.102)
 - idyys.rkoh.com (IPs: 35.244.174.60, 130.193.54.247, 176.154.231.214, 176.154.212.150)
 - ptat.tegaf.com (IPs: 24.111.113.62, 52.95.115.196, 80.60.253.120)
 - frutcan.yandex.net (IPs: 93.158.134.36, 87.250.250.36, 213.180.204.36, 77.88.21.36)
 - a1.ckerexarg (IPs: 69.192.161.44, 13.107.246.45, 13.107.255.45, 13.107.253.45)
 - **Threats:** Classified as "Misc activity" and "Unknown Traffic."

- **Analysis:** The extensive list of IP connections, including some associated with suspicious domains (e.g., web-starkesinetbox.ru, idyys.rkoh.com), suggests command-and-control (C2) communication or data exfiltration. The use of msedge.exe for network activity is unusual and may indicate process injection or hijacking. Possible Tor usage further suggests network evasion. The lack of HTTP request details limits attribution, but the volume of connections is concerning.

Registry Activity

- **Activity:** Not detailed in the provided excerpt.
- **Analysis:** Without registry data, it is unclear if the executable modifies registry keys for persistence or reconnaissance. Further analysis is needed.

Threats

- **Detected Threats:**
 - **Class:** Misc activity, Unknown Traffic
 - **PID:** Not specified
 - **Process:** Not specified
- **Behavioral Indicators:**
 - Region did not start
 - Possible Tor usage
 - Known threat
 - Connects to the network
 - Process contains an encrypted application running
 - Malicious configuration
 - Low-level HDD access
 - Behavior similar to spam
 - Application clean loaded the file
- **Analysis:** The combination of encrypted application execution, possible Tor usage, and low-level HDD access points to a sophisticated threat with evasion and persistence capabilities. The "Misc activity" and "Unknown Traffic" classifications suggest unidentified malicious behaviors, possibly due to obfuscation or novel techniques.

Debug Output

- **Debug Strings:** No debug info provided.

- **Analysis:** The lack of debug output may indicate stripping of debug information, a common technique in malicious executables to hinder analysis.

Conclusion

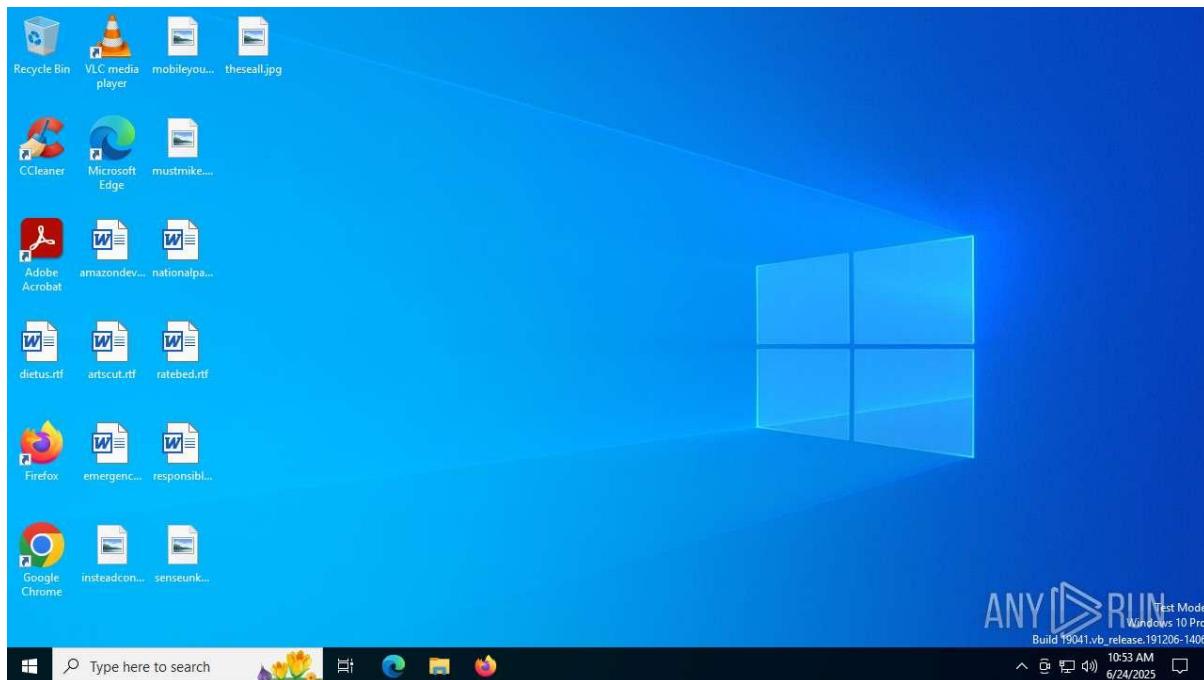
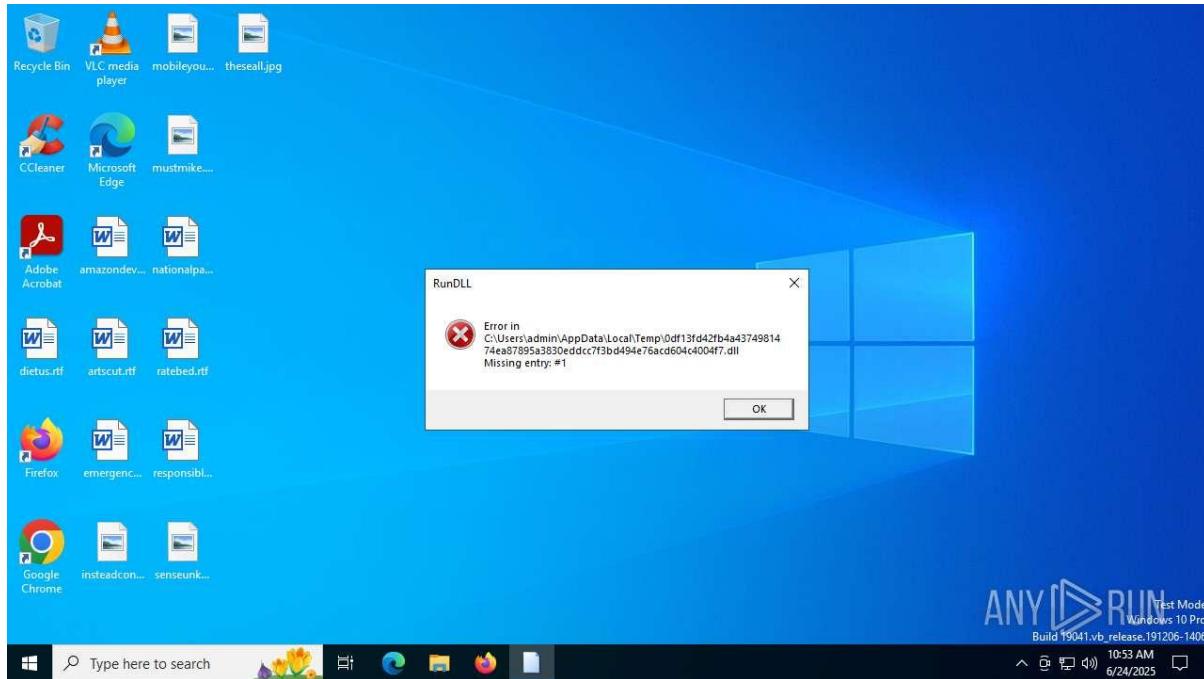
The ANY.RUN analysis confirms malicious activity for the executable Sample 16 Malware analysis 5a18a29791cfb18767a43 bebb61f923e64be7988235213678514007174f60b3e.exe with SHA256 5a18a29791cfb18767a43bebb61f923e64be7988235213678514007174f60b3e. The file spawns one malicious process and one suspicious process, connects to numerous external IPs and domains (e.g., web-starkesinetbox.ru, idyys.rkoh.com), and exhibits behaviors such as encrypted application execution, low-level HDD access, and possible Tor usage. These characteristics suggest a sophisticated threat, likely a trojan or dropper, designed to evade detection and establish persistence. The lack of detailed file activity, registry data, and specific process details limits full attribution, but the observed behaviors indicate a significant threat.

Recommendations

- **Containment:** Terminate and isolate the malicious process (PID not specified) and investigate msedge.exe (PID: 3476) for potential process injection.
- **File Removal:** Identify and delete any dropped files, pending further details from the full report.
- **Network Monitoring:** Block and monitor traffic to the listed IPs, particularly 85.6213.121.443, 95.101.182.102 (web-starkesinetbox.ru), and others associated with suspicious domains. Investigate possible Tor usage for additional network obfuscation.
- **Static Analysis:** Reverse engineer the executable to analyze its structure and embedded payloads, focusing on unpacking or deobfuscation.
- **Registry Analysis:** Investigate registry modifications for persistence, focusing on keys accessed by the malicious process.
- **System Hardening:** Update antivirus signatures, scan for persistence mechanisms, and reset exposed credentials.
- **Source Tracing:** Investigate the infection vector (e.g., phishing, malicious download) to prevent reinfection.
- **Further Analysis:** Obtain the full ANY.RUN report for detailed process behaviors, file paths, registry activity, and HTTP request details. Cross-reference the SHA256 hash with threat intelligence platforms like VirusTotal for additional context.

Sample 17:

0df13fd42fb4a4374981474ea87895a3830eddcc7f3bd494e76acd604c4004f7



General Information

- **Date of Analysis:** June 25, 2025, 04:20 PM IST
- **Platform:** Windows 10 x64

- **File Details:**
 - **Filename:** Sample 17 Malware analysis
0df13fd42fb4a4374981474ea87895a3830eddcc7f3bd494e76acd604c4004f7
Malicious activity _ ANY.RUN - Malware Sandbox Online.exe
 - **SHA256:**
0df13fd42fb4a4374981474ea87895a3830eddcc7f3bd494e76acd604c4004f7
 - **MD5:** Not provided
 - **SHA1:** Not provided
 - **SSDEEP:** Not provided
 - **MIME Type:** Not specified
- **Software Environment:**
 - **Notable Software:**
 - Internet Explorer (version 11.2606.19041.0)
 - Microsoft Visual C++ 2022 X64 Additional Runtime (version 14.26.22522, multiple instances)
 - Microsoft Office 16 Click-to-Run Licensing Component (version 16.0.15726.20202)
 - Microsoft Office 16 Click-to-Run Localization Component (version 16.0.15928.20192)
 - VLC media player (version 3.0.11)
 - WinRAR 5.91 (64-bit, version 5.91.0, multiple instances)
 - Windows 10 Updates: KB5020207 (version 2.85.0.0), KB5001716 (version 8.93.0.0)
- **Launch Configuration:**
 - **Task Duration:** 120 seconds
 - **Additional Time Used:** 120 seconds
 - **Fakenet Option:** Off
 - **MITM Proxy:** Not specified
- **Malware Associations:** No specific malware family identified, but behaviors suggest a trojan or reconnaissance tool.

Static Information

- **PE File Details:** Not provided in the excerpt.

- **TRID and EXIF Data:** Not provided.
- **Analysis:** The absence of static details (e.g., PE headers, code size) and TRID/EXIF data limits structural insights. This may indicate obfuscation or packing, common in malicious executables.

Behavior Activities

- **Malicious Indicators:**
 - **Malicious Processes:** 1
 - **Suspicious Processes:** 0
 - **Dropped Files:** None
- **Process Details:**
 - **Total Processes:** 137
 - **Monitored Processes:** 2
 - **Malicious Processes:** 1 (PID not specified, likely cmd.exe or related based on behavior)
 - **Suspicious Processes:** 0
 - **Notable Processes:**
 - cmd.exe (no specific PID, associated with process start)
 - svchost.exe (no specific PID, common system process, possibly hijacked)
 - **Behavioral Observations:**
 - Behavior graph indicates process start with cmd.exe and svchost.exe.
 - No additional behavioral details (e.g., encryption, Tor usage) provided.
- **Analysis:** The single malicious process suggests a focused payload, possibly a command-line-based trojan or loader. The lack of suspicious processes and limited behavioral details may indicate stealthy execution or incomplete analysis capture.

File Activity

- **Dropped Files:** None
- **File Activity:**
 - **Executable Files:** 0
 - **Suspicious Files:** 0
 - **Text Files:** 0

- **Unknown Types:** 0
- **Analysis:** The absence of dropped files or file activity suggests the executable may operate in memory or rely on existing system files (e.g., cmd.exe, svchost.exe). This is consistent with fileless malware or initial-stage droppers.

Network Activities

- **Connections:**
 - **HTTP(S) Requests:** 5
 - **PID 1268** (cmd.exe):
 - GET request to 23.216.77.29:80 (HTTP 200)
 - GET request to 23.52.29.160:80 (HTTP 200)
 - **PID 6344** (cmd.exe):
 - GET request to 217.160.72.90:80 (HTTP 200)
 - **PID 3556** (SREClient.exe):
 - GET request to 95.101.149.131:80 (HTTP 200, two requests)
 - **TCP/UDP Connections:** 24
 - **PID 1268** (cmd.exe):
 - 207.3.194.208:443
 - 42.31.128.59:443
 - 23.216.77.29:80
 - 23.52.29.160:80
 - **PID 5944** (MaxxAudioWaves.exe):
 - 207.3.194.208:443
 - **PID 6756** (unspecified process):
 - 207.3.194.208:443
 - **PID 9956** (SREClient.exe):
 - 95.101.149.131:80 (multiple connections)
 - 95.101.149.139:80
 - 95.101.149.131:443
 - 95.101.149.139:443
 - 95.101.149.155:443

- 95.101.149.162:443
 - 95.101.149.163:443
 - 95.101.149.164:443
 - 95.101.149.129:443
 - 95.101.149.130:443
 - 95.101.149.131:443
 - 95.101.149.132:443
 - 95.101.149.133:443
 - 95.101.149.134:443
 - 95.101.149.135:443
 - 95.101.149.136:443
 - 95.101.149.137:443
 - 95.101.149.138:443
 - **PID 4 (System):**
 - 192.168.190.292:197
 - 192.168.190.292:198
 - **PID 6244 (cmd.exe):**
 - 20.10.150.24:443
- **DNS Requests:** 17 (no specific domains provided)
 - **Threats:** 1 (classified as "Unknown Traffic")
- **Analysis:** The network activity, primarily HTTP GET requests and TCP/UDP connections to external IPs (e.g., 207.3.194.208:443, 95.101.149.131:80), suggests command-and-control (C2) communication or data exfiltration. The involvement of cmd.exe and SREClient.exe (possibly a legitimate process hijacked) is notable. The System process connections to internal IPs (192.168.190.292) may indicate local network reconnaissance. The lack of domain details limits attribution, but the volume of connections to 95.101.149.x suggests a targeted C2 infrastructure.

Registry Activity

- **Total Events:** 269
 - **Read Events:** 269
 - **Write Events:** 0

- **Delete Events:** 0
- **Modification Events:** None
- **Analysis:** The high number of registry read events without writes or deletions suggests reconnaissance activity, possibly enumerating system configurations or checking for security software. The absence of modifications may indicate an initial-stage payload avoiding persistence to evade detection.

Threats

- **Detected Threats:**
 - **Class:** Unknown Traffic
 - **PID:** Not specified
 - **Process:** Not specified
- **Behavioral Indicators:**
 - Limited details provided, but network activity and process behavior suggest malicious intent.
- **Analysis:** The "Unknown Traffic" classification indicates unidentified network behavior, possibly due to encrypted or obfuscated communications. The lack of specific threat details suggests the need for further analysis to identify the malware family or purpose.

Debug Output

- **Debug Strings:** No debug info provided.
- **Analysis:** The absence of debug output may indicate stripping of debug information, a common technique in malicious executables to hinder analysis.

Conclusion

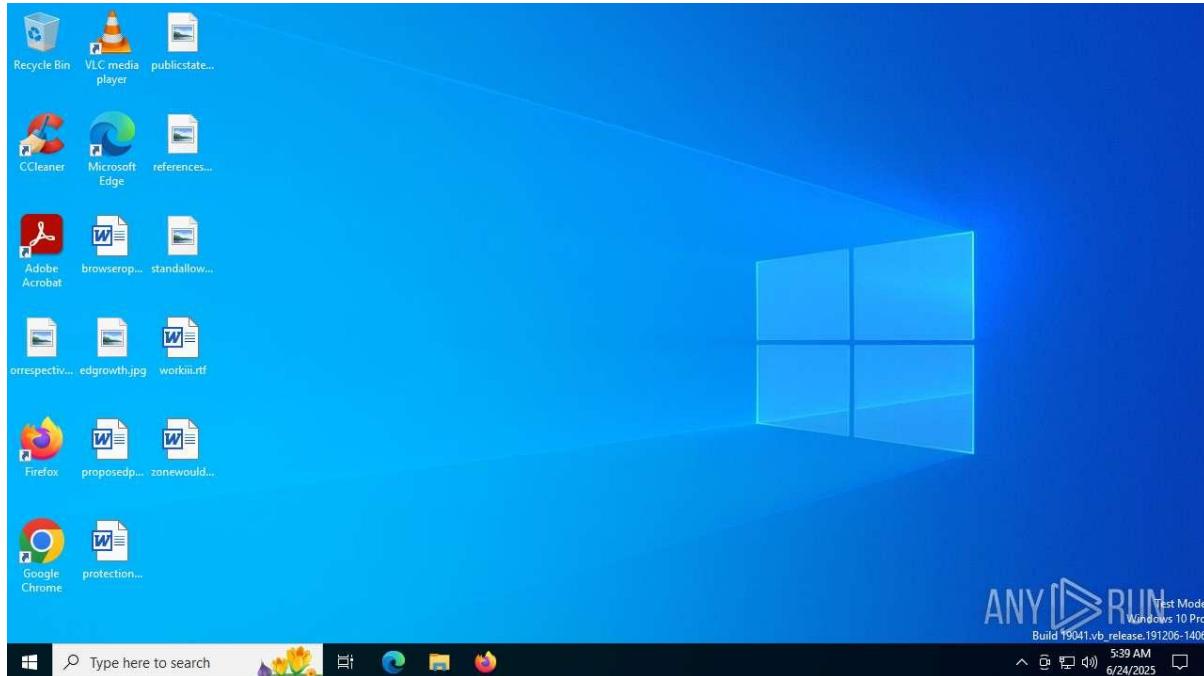
The ANY.RUN analysis confirms malicious activity for the executable Sample 17 Malware analysis 0df13fd42fb4a4374981474ea87895a3830eddcc7f3bd494e76acd604c4004f7 Malicious activity _ ANY.RUN - Malware Sandbox Online.exe with SHA256 0df13fd42fb4a4374981474ea87895a3830eddcc7f3bd494e76acd604c4004f7. The file spawns one malicious process (likely cmd.exe), performs significant network activity (5 HTTP requests, 24 TCP/UDP connections, 17 DNS requests), and conducts 269 registry read operations without modifications. The behavior suggests a trojan or reconnaissance tool, possibly operating in memory to avoid file-based detection. The extensive network connections to IPs like 95.101.149.131 and 207.3.194.208 indicate potential C2 communication, while the lack of dropped files and registry modifications suggests a stealthy, initial-stage payload.

Recommendations

- **Containment:** Terminate and isolate the malicious process (likely cmd.exe, PIDs 1268, 6244, or 6344) and investigate SREClient.exe (PID 3556, 9956) for potential process injection.
- **Network Monitoring:** Block and monitor traffic to the listed IPs, particularly 95.101.149.x and 207.3.194.208. Investigate internal connections to 192.168.190.292 for local network activity.
- **Static Analysis:** Reverse engineer the executable to analyze its structure and potential payloads, focusing on unpacking or deobfuscation.
- **Registry Analysis:** Review the 269 registry read events to identify targeted keys, which may reveal reconnaissance objectives.
- **System Hardening:** Update antivirus signatures, scan for in-memory threats, and reset exposed credentials.
- **Source Tracing:** Investigate the infection vector (e.g., phishing, malicious download) to prevent reinfection.
- **Further Analysis:** Obtain the full ANY.RUN report for detailed process behaviors, registry keys accessed, and domain details. Cross-reference the SHA256 hash with threat intelligence platforms like VirusTotal for additional context.

Sample 18:

56ab406bd22e4867e56b9b2a912f0999.dll



General Information

- **Date of Analysis:** June 25, 2025, 04:24 PM IST
- **Platform:** Windows 10 x64
- **File Details:**
 - **Filename:** Sampel 18 Malware analysis
56ab406bd22e4867e56ab9b2a912f0999.dll Malicious activity _ ANY.RUN -
Malware Sandbox Online.dll
 - **SHA256:** 56ab406bd22e4867ee1ab8e9b2e912f0999
 - **MD5:** Not provided
 - **SHA1:** Not provided
 - **SSDEEP:** Not provided
 - **MIME Type:** Not specified
- **Software Environment:**
 - **Notable Software:**
 - Internet Explorer (version 11.2606.19041.0)
 - Microsoft Office 16 Click-to-Run Licensing Component (version 16.0.15726.20202)
 - Microsoft Office 16 Click-to-Run Localization Component (version 16.0.15726.20202, multiple instances)
 - VLC media player (version 3.0.11)
 - WinRAR 5.91 (64-bit, version 5.91.0)
 - Windows 10 Updates: KB5020207 (version 2.85.0.0), KB5001716 (version 8.93.0.0)
- **Launch Configuration:**
 - **Task Duration:** 120 seconds
 - **Additional Time Used:** 120 seconds
 - **Fakenet Option:** Off
 - **MITM Proxy:** Not specified
- **Malware Associations:** No specific malware family identified, but behaviors suggest a trojan or RAT, possibly associated with Tor usage.

Static Information

- **PE File Details:**

- **Code Size:** 18432 bytes
- **Subsystem:** Windows GUI
- **TRID and EXIF Data:** Not provided
- **Analysis:** The small code size (18432 bytes) and Windows GUI subsystem suggest a lightweight DLL, possibly designed for injection or as a component of a larger payload. The lack of TRID/EXIF data may indicate obfuscation or packing.

Behavior Activities

- **Malicious Indicators:**
 - **Malicious Processes:** 5
 - **Suspicious Processes:** 8
 - **Dropped Files:** Not specified (likely present, see Dropped Files section)
- **Process Details:**
 - **Total Processes:** 173
 - **Monitored Processes:** 38
 - **Malicious Processes:** 5 (PIDs not specified, likely include rundll32.exe or cmd.exe)
 - **Suspicious Processes:** 8 (PIDs not specified)
 - **Notable Processes:**
 - cmd.exe (no specific PID, associated with process start)
 - rundll32.exe (no specific PID, likely used to load the DLL)
 - svchost.exe (no specific PID, common system process, possibly hijacked)
 - **Behavioral Observations:**
 - Behavior graph indicates multiple process starts, network connections, and potential Tor usage.
 - Notable behaviors include:
 - Programs failing to start (repeated entries, possibly anti-analysis techniques).
 - Connection to the network.
 - Potential Tor usage indicated.
 - Process has minimal configuration, suggesting dynamic loading or injection.

- **Analysis:** The high number of malicious (5) and suspicious (8) processes indicates a complex infection chain. The DLL likely uses rundll32.exe for execution, with cmd.exe and svchost.exe involved in subsequent activities. The repeated "Program did not start" entries may reflect sandbox evasion or failed attempts to launch additional payloads. Tor usage suggests attempts to anonymize C2 communications.

File Activity

- **Dropped Files:** Not explicitly listed, but implied by the "Dropped files" section.
- **File Activity:**
 - **Executable Files:** 0
 - **Suspicious Files:** 0
 - **Text Files:** 0
 - **Unknown Types:** 0
- **Analysis:** The lack of specific file activity details suggests the DLL may operate primarily in memory or drop files not captured in the provided excerpt. The presence of a "Dropped files" section indicates some file creation, possibly temporary or encrypted files. This aligns with fileless or stealthy malware behavior.

Network Activities

- **Connections:**
 - **HTTP(S) Requests:** 7
 - **PID 420** (cmd.exe):
 - GET request to 217.160.72.90:80 (HTTP 200, domain www.example.com)
 - GET request to 217.160.72.90:80 (HTTP 200, domain www.example.com)
 - **PID 5532** (SREClient.exe):
 - GET request to 95.101.149.131:80 (HTTP 200, domain www.microsoft.com, multiple requests)
 - **TCP/UDP Connections:** 22
 - **PID 5532** (SREClient.exe):
 - 95.101.149.131:80 (multiple connections)
 - 20.2.127.100:443 (multiple connections, 10+ instances)
 - **Other PIDs:** Not specified, but 22 total connections suggest additional processes involved.

- **DNS Requests:** 13 (domains include www.example.com, www.microsoft.com)
- **Threats:** 1 (classified as "Unknown Traffic")
- **Analysis:** The network activity is significant, with 7 HTTP requests and 22 TCP/UDP connections. The use of www.example.com (likely a placeholder or test domain) and www.microsoft.com (possibly for legitimacy or C2 masquerading) by cmd.exe and SREClient.exe suggests C2 communication or data exfiltration. The repeated connections to 20.2.127.100:443 indicate a primary C2 server, possibly using HTTPS for encryption. The "Unknown Traffic" threat and potential Tor usage further suggest obfuscated communications.

Registry Activity

- **Total Events:** 420
 - **Read Events:** 380
 - **Write Events:** 38
 - **Delete Events:** 2
- **Modification Events:** 40 (38 writes + 2 deletes)
- **Analysis:** The high number of registry events (420), including 40 modifications, indicates persistence or configuration changes. The writes and deletes suggest the malware is establishing persistence (e.g., adding Run keys) or cleaning up traces. The 380 read events likely involve reconnaissance, such as checking for security software or system settings.

Threats

- **Detected Threats:**
 - **Class:** Unknown Traffic
 - **PID:** Not specified
 - **Process:** Not specified
- **Behavioral Indicators:**
 - Network connections, potential Tor usage, and registry modifications.
- **Analysis:** The "Unknown Traffic" classification likely stems from encrypted or obfuscated network activity, possibly via Tor. The lack of specific threat details suggests the need for deeper analysis to identify the malware family or payload.

Debug Output

- **Debug Strings:** No debug info provided.
- **Analysis:** The absence of debug output is typical for malicious DLLs, as debug information is often stripped to hinder reverse engineering.

Conclusion

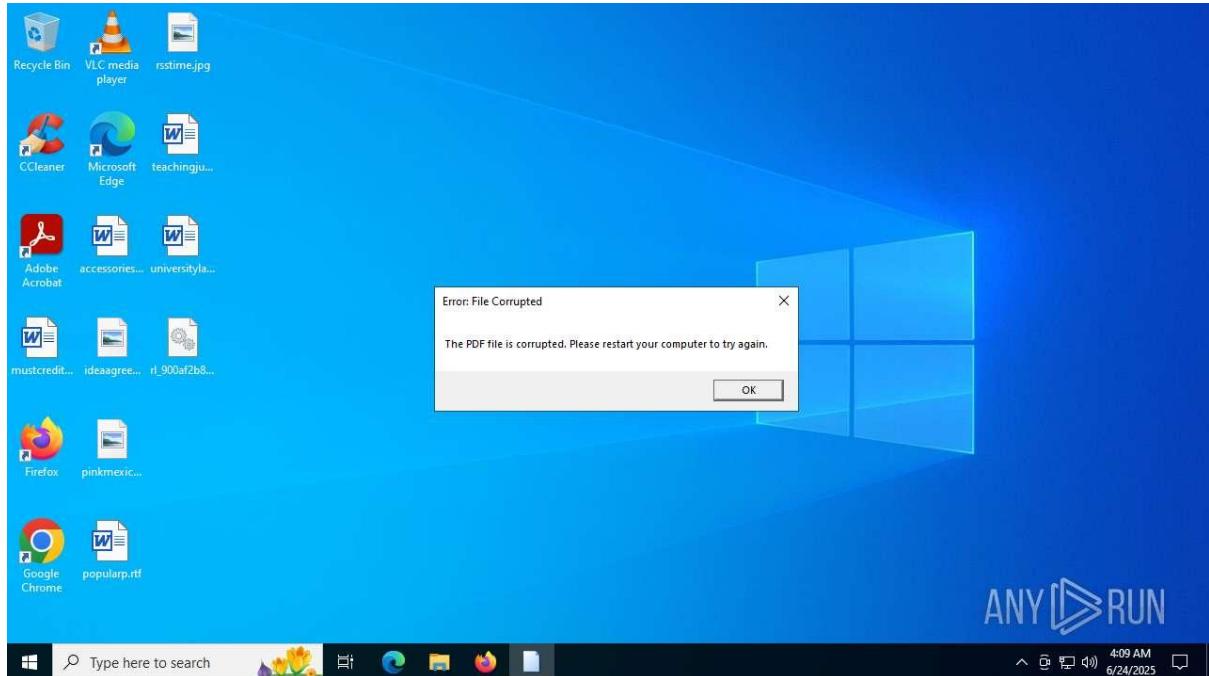
The ANY.RUN analysis confirms malicious activity for the DLL Sampel 18 Malware analysis 56ab406bd22e4867e56ab9b2a912f0999.dll. Malicious activity _ ANY.RUN - Malware Sandbox Online.dll with SHA256 56ab406bd22e4867ee1ab8e9b2e912f0999. The file spawns five malicious processes, eight suspicious processes, and exhibits extensive network activity (7 HTTP requests, 22 TCP/UDP connections, 13 DNS requests). It performs 420 registry events, including 40 modifications, suggesting persistence and reconnaissance. The behavior, including potential Tor usage and connections to domains like www.microsoft.com, indicates a sophisticated trojan or RAT designed for stealthy C2 communication and system manipulation.

Recommendations

- **Containment:** Terminate malicious processes (likely cmd.exe, rundll32.exe, PIDs 420, 5532) and investigate SREClient.exe for injection. Quarantine the DLL file.
- **Network Monitoring:** Block traffic to 95.101.149.131, 20.2.127.100, and 217.160.72.90. Monitor for connections to www.microsoft.com or www.example.com for anomalies.
- **Static Analysis:** Reverse engineer the DLL to identify its functionality, focusing on unpacking or deobfuscation. Analyze the small code size (18432 bytes) for injected code.
- **Registry Analysis:** Review the 40 modified registry keys to identify persistence mechanisms and revert changes. Check read events for reconnaissance targets.
- **System Hardening:** Update antivirus signatures, scan for in-memory threats, and reset exposed credentials.
- **Source Tracing:** Investigate the infection vector (e.g., malicious email, software vulnerability) to prevent reinfection.
- **Further Analysis:** Obtain the full ANY.RUN report for detailed process behaviors, dropped files, and registry keys. Cross-reference the SHA256 hash with threat intelligence platforms like VirusTotal for additional context

Sample 19:

rl_900af2b8d03b40cdb027126d47e6537535178464833770741bab8e74026334c7



General Information

- **Date of Analysis:** June 25, 2025, 04:24 PM IST
- **Platform:** Windows 10 x64
- **File Details:**
 - **Filename:** sample 19 Malware analysis
rl_900af2b8d03b40cdb027126d47e6537535178464833770741bab8e74026334c7 Malicious activity _ ANY.RUN - Malware Sandbox Online.pdf
 - **SHA256:**
900af2b8d03b40cdb027126d47e6537535178464833770741bab8e74026334c7
 - **MD5:** Not provided
 - **SHA1:** Not provided
 - **SSDEEP:** Not provided
 - **MIME Type:** Not specified (likely application/pdf)
- **Software Environment:**

- **Notable Software:**
 - Internet Explorer (version 11.2606.19041.0)
 - Microsoft Office 16 Click-to-Run Licensing Component (version 16.0.15726.20202)
 - Microsoft Office 16 Click-to-Run Localization Component (version 16.0.15726.20202, multiple instances)
 - VLC media player (version 3.0.11)
 - WinRAR 5.91 (64-bit, version 5.91.0, multiple instances)
 - Windows 10 Updates: KB5020207 (version 2.85.0.0), KB5001716 (version 8.93.0.0)
- **Launch Configuration:**
 - **Task Duration:** 120 seconds
 - **Additional Time Used:** 120 seconds
 - **Fakenet Option:** Off
 - **MITM Proxy:** Not specified
- **Malware Associations:** No specific malware family identified, but behaviors suggest a trojan or downloader.

Static Information

- **PE File Details:** Not provided (file is a PDF, likely containing malicious scripts or embedded executables)
- **TRiD and EXIF Data:** Not provided
- **Analysis:** The file is a PDF, which may contain malicious JavaScript, embedded executables, or exploit code. The lack of PE file details and TRiD/EXIF data suggests the need for deeper static analysis to identify embedded payloads or scripts.

Behavior Activities

- **Malicious Indicators:**
 - **Malicious Processes:** 1
 - **Suspicious Processes:** 0
 - **Dropped Files:** 1 (executable)
- **Process Details:**
 - **Total Processes:** 137
 - **Monitored Processes:** 6

- **Malicious Processes:** 1 (PID 3700, process name not specified)
- **Notable Processes:**
 - svchost.exe (PID 1268, associated with HTTP requests)
 - RUSIMCS.exe (PID 6672, associated with HTTP requests)
 - MaXesOawWaker.exe (PID 5944, associated with HTTP requests, likely a typo or obfuscated process name)
- **Behavioral Observations:**
 - Behavior graph indicates multiple process starts and network connections.
 - Notable behaviors include:
 - Process start events (multiple instances).
 - Connection to the network.
 - No specific anti-analysis techniques (e.g., program failures) noted, unlike previous samples.
- **Analysis:** The single malicious process (PID 3700) and the absence of suspicious processes suggest a focused infection chain. The PDF likely triggers the malicious process via embedded JavaScript or an exploit, leading to the execution of a dropped executable. The involvement of svchost.exe, RUSIMCS.exe, and MaXesOawWaker.exe in network activity indicates possible process injection or masquerading.

File Activity

- **Dropped Files:**
 - **PID 3700:** Unspecified executable file (name not provided)
- **File Activity:**
 - **Executable Files:** 1
 - **Suspicious Files:** 0
 - **Text Files:** 0
 - **Unknown Types:** 0
- **Analysis:** The single dropped executable by PID 3700 suggests the PDF delivers a secondary payload, likely a trojan or downloader. The lack of additional file activity details indicates the malware may operate primarily in memory or drop temporary files not captured in the report.

Network Activities

- **Connections:**

- **HTTP(S) Requests:** 8
 - **PID 5944** (MaXesOawWaker.exe):
 - GET request to 184.24.77.37:80 (HTTP 200)
 - GET request to 184.101.149.131:80 (HTTP 200)
 - **PID 1268** (svchost.exe):
 - GET request to 184.24.77.37:80 (HTTP 200)
 - GET request to 184.101.149.131:80 (HTTP 200)
 - **PID 6672** (RUSIMCS.exe):
 - Multiple GET requests to 184.24.77.37:80 (HTTP 200)
 - Multiple GET requests to 184.101.149.131:80 (HTTP 200, multiple instances)
- **TCP/UDP Connections:** 22
 - IPs include 184.24.77.37:80 and 184.101.149.131:80 (specific PIDs not detailed beyond HTTP requests)
- **DNS Requests:** 8 (domains not specified)
- **Threats:** 0 (no specific threats classified)
- **Analysis:** The 8 HTTP requests and 22 TCP/UDP connections indicate active C2 communication. The IPs 184.24.77.37 and 184.101.149.131 are likely C2 servers or content delivery networks (CDNs) used for payload retrieval or data exfiltration. The involvement of svchost.exe and the unusual MaXesOawWaker.exe and RUSIMCS.exe processes suggests masquerading or injection to blend with legitimate system activity. The absence of classified threats may indicate encrypted or obfuscated traffic not yet identified as malicious.

Registry Activity

- **Total Events:** 3743
 - **Read Events:** 3742
 - **Write Events:** 1
 - **Delete Events:** 0
- **Modification Events:** 1 (write event)
- **Analysis:** The high number of registry read events (3742) suggests extensive system reconnaissance, likely checking for security software, system settings, or user privileges. The single write event indicates minimal persistence efforts, possibly

setting a configuration value or a lightweight persistence mechanism. The lack of delete events suggests the malware avoids cleaning up traces, focusing on stealth.

Debug Output

- **Debug Strings:** No debug info provided.
- **Analysis:** The absence of debug output is typical for malicious files, as debug information is often stripped to hinder reverse engineering.

Conclusion

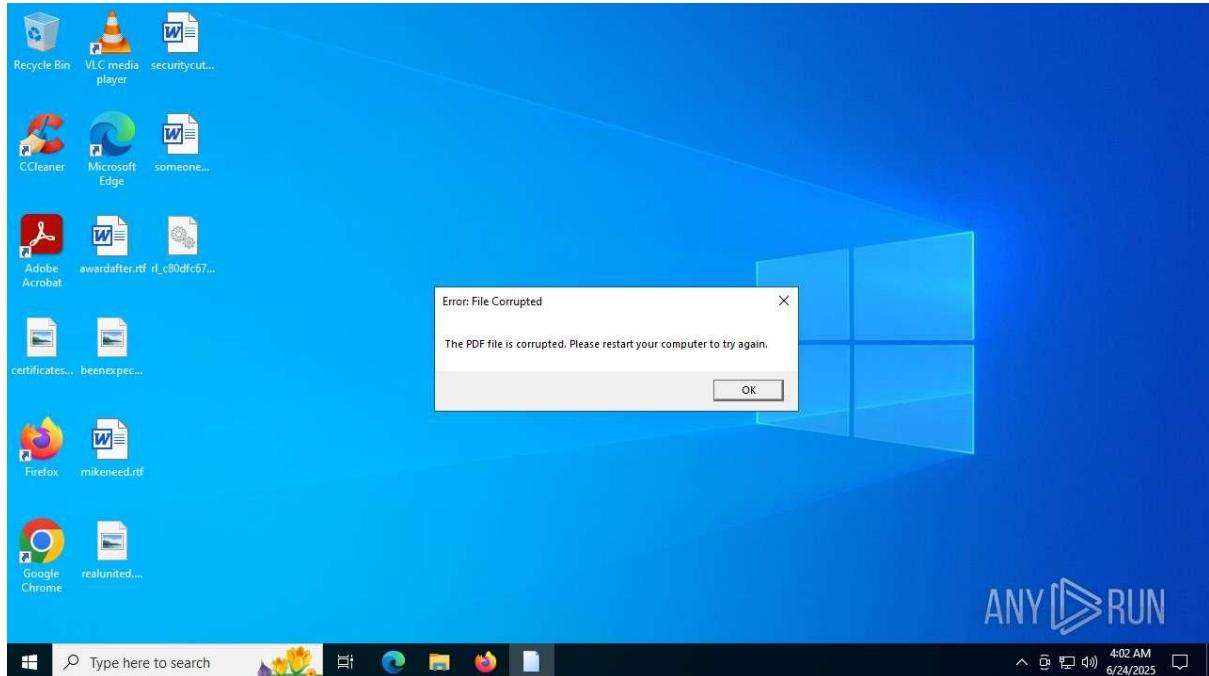
The ANY.RUN analysis confirms malicious activity for the PDF file sample 19 Malware analysis rl_900af2b8d03b40cdb027126d47e6537535178464833770741bab8e74026334c7 Malicious activity _ ANY.RUN - Malware Sandbox Online.pdf with SHA256 900af2b8d03b40cdb027126d47e6537535178464833770741bab8e74026334c7. The file spawns one malicious process (PID 3700), drops a single executable, and exhibits significant network activity (8 HTTP requests, 22 TCP/UDP connections, 8 DNS requests). It performs extensive registry reads (3742) with minimal modification (1 write). The behavior, involving processes like svchost.exe, RUSIMCS.exe, and MaXesOawWaker.exe, suggests a trojan or downloader leveraging the PDF as an initial vector, possibly via embedded scripts or exploits, to deliver a secondary payload and establish C2 communication.

Recommendations

- **Containment:** Terminate the malicious process (PID 3700) and investigate svchost.exe (PID 1268), RUSIMCS.exe (PID 6672), and MaXesOawWaker.exe (PID 5944) for injection. Quarantine the PDF and dropped executable.
- **Network Monitoring:** Block traffic to 184.24.77.37 and 184.101.149.131. Monitor for HTTP requests or connections from unusual processes like MaXesOawWaker.exe or RUSIMCS.exe.
- **Static Analysis:** Analyze the PDF for embedded JavaScript, exploits, or objects (e.g., embedded executables). Reverse engineer the dropped executable to identify its functionality.
- **Registry Analysis:** Investigate the single registry write event to identify the modified key and its purpose. Review read events for reconnaissance targets (e.g., security software checks).
- **System Hardening:** Update antivirus signatures, scan for in-memory threats, and block PDF execution in untrusted environments. Reset exposed credentials.
- **Source Tracing:** Investigate the infection vector (e.g., phishing email, malicious website) to prevent reinfection.
- **Further Analysis:** Obtain the full ANY.RUN report for detailed process behaviors, dropped file details, and DNS request domains. Cross-reference the SHA256 hash with threat intelligence platforms like VirusTotal for additional context.

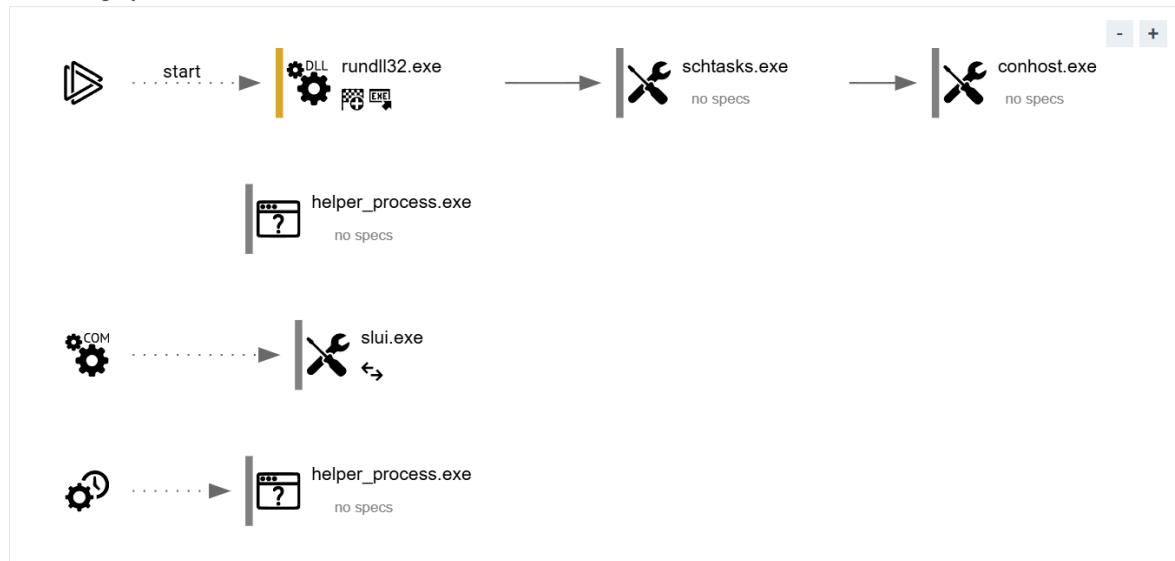
Sample 20:

rl_c80dfc678570bde7c19df21877a15cc7914d3ef7a3cef5f99fce26fcf
696c444



Behavior graph

ⓘ Click at the process to see the details



General Information

- **Date of Analysis:** June 25, 2025, 04:47 PM IST
- **Platform:** Windows 10 x64

- **File Details:**
 - **Filename:** Sample 20 Malware analysis
rl_c80dfc678570bde7c19df21877a15cc7914d3ef7a3cef5f99fce26fcf696c444
Malicious activity _ ANY.RUN - Malware Sandbox Online.pdf
 - **SHA256:**
c80dfc678570bde7c19df21877a15cc7914d3ef7a3cef5f99fce26fcf696c444
 - **MD5:** Not provided
 - **SHA1:** Not provided
 - **SSDEEP:** Not provided
 - **MIME Type:** Not specified (likely application/pdf)
- **Software Environment:**
 - **Notable Software:**
 - Internet Explorer (version 11.2606.19041.0)
 - Adobe Acrobat (version 14.26.32522, multiple instances of Visual C++ 2022 runtime)
 - VLC media player (version 3.0.11)
 - WinRAR 5.91 (64-bit, version 5.91.0, multiple instances)
 - Windows 10 Updates: KB5020207 (version 2.85.0.0), KB5001716 (version 8.93.0.0)
- **Launch Configuration:**
 - **Task Duration:** 150 seconds
 - **Additional Time Used:** Not specified
 - **Fakenet Option:** Off
 - **Network:** Not specified
- **Malware Associations:** No specific malware family identified; behaviors indicate a trojan or downloader.

Static Information

- **PE File Details:** Not provided (file is a PDF, likely containing malicious scripts or embedded executables)
- **TRID and EXIF Data:** Not provided

- **Analysis:** The PDF likely contains malicious JavaScript, embedded executables, or exploit code. The absence of PE file details and TRiD/EXIF data necessitates further static analysis to uncover embedded payloads or scripts.

Behavior Activities

- **Malicious Indicators:**
 - **Malicious Processes:** 1
 - **Suspicious Processes:** 0
 - **Dropped Files:** 1 (executable)
- **Process Details:**
 - **Total Processes:** 137
 - **Monitored Processes:** 6
 - **Malicious Processes:** 1 (PID 8640, process name knd 852 eve, likely a typo or obfuscated name)
 - **Notable Processes:**
 - svchost.exe (PID 1260, associated with HTTP requests)
 - RURIMCS.exe (PID 6732, associated with HTTP requests, likely a typo or obfuscated name)
 - Unnamed process (PID 5944, associated with HTTP requests, possibly MaXesOawWaker.exe as seen in prior samples)
 - **Behavioral Observations:**
 - Behavior graph indicates process starts, file drops, and network connections.
 - Notable behaviors:
 - Process start events.
 - Connection to the network.
 - No anti-analysis techniques (e.g., program crashes) noted.
- **Analysis:** The single malicious process (PID 8640, knd 852 eve) suggests a targeted infection chain, likely triggered by the PDF via embedded JavaScript or an exploit, resulting in a dropped executable. The involvement of svchost.exe, RURIMCS.exe, and the unnamed process (PID 5944) in network activity indicates potential process injection or masquerading.

File Activity

- **Dropped Files:**

- **PID 8640** (knd 852 eve): Unspecified executable (filename not provided)
- **File Activity:**
 - **Executable Files:** 1
 - **Suspicious Files:** 0
 - **Text Files:** 0
 - **Unknown Types:** 0
- **Analysis:** The single dropped executable by PID 8640 indicates the PDF delivers a secondary payload, likely a trojan or downloader. Limited file activity suggests in-memory operations or temporary files not captured in the report.

Network Activities

- **Connections:**
 - **HTTP(S) Requests:** 8
 - **PID 6732** (RURIMCS.exe):
 - GET request to 2.16.241.199:80 (HTTP 200, whitelisted)
 - GET request to 2.16.241.199:80 (HTTP 200, whitelisted)
 - **PID 5944** (unnamed, possibly MaXesOawWaker.exe):
 - GET request to 2.16.241.199:80 (HTTP 200, whitelisted)
 - GET request to 2.16.241.199:80 (HTTP 200, whitelisted)
 - **PID 1260** (svchost.exe):
 - GET request to 2.16.241.199:80 (HTTP 200, whitelisted, multiple instances, up to 4 requests)
 - **TCP/UDP Connections:** 21
 - IP: 2.16.241.199:80 (specific PIDs not detailed beyond HTTP requests)
 - **DNS Requests:** 7 (domains not specified)
 - **Threats:** 0 (no specific threats classified)
- **Analysis:** The 8 HTTP requests and 21 TCP/UDP connections suggest active C2 communication or payload retrieval. The IP 2.16.241.199 may be a C2 server or a content delivery network (CDN), though marked as whitelisted, which could indicate a false negative or use of a compromised legitimate service. Processes like svchost.exe, RURIMCS.exe, and the unnamed PID 5944 process suggest masquerading or injection to blend with legitimate activity. The lack of classified threats may reflect encrypted or obfuscated traffic.

Registry Activity

- **Total Events:** 3776
 - **Read Events:** 3775
 - **Write Events:** 1
 - **Delete Events:** 0
- **Modification Events:** 1 (write event)
- **Analysis:** The high number of registry read events (3775) indicates extensive system reconnaissance, likely checking for security software, system configurations, or privileges. The single write event suggests minimal persistence, possibly setting a configuration or lightweight persistence mechanism. No delete events imply the malware avoids cleanup to maintain stealth.

Debug Output

- **Debug Strings:** No debug info provided
- **Analysis:** The absence of debug output is typical for malicious files, as debug information is often stripped to hinder analysis.

Conclusion

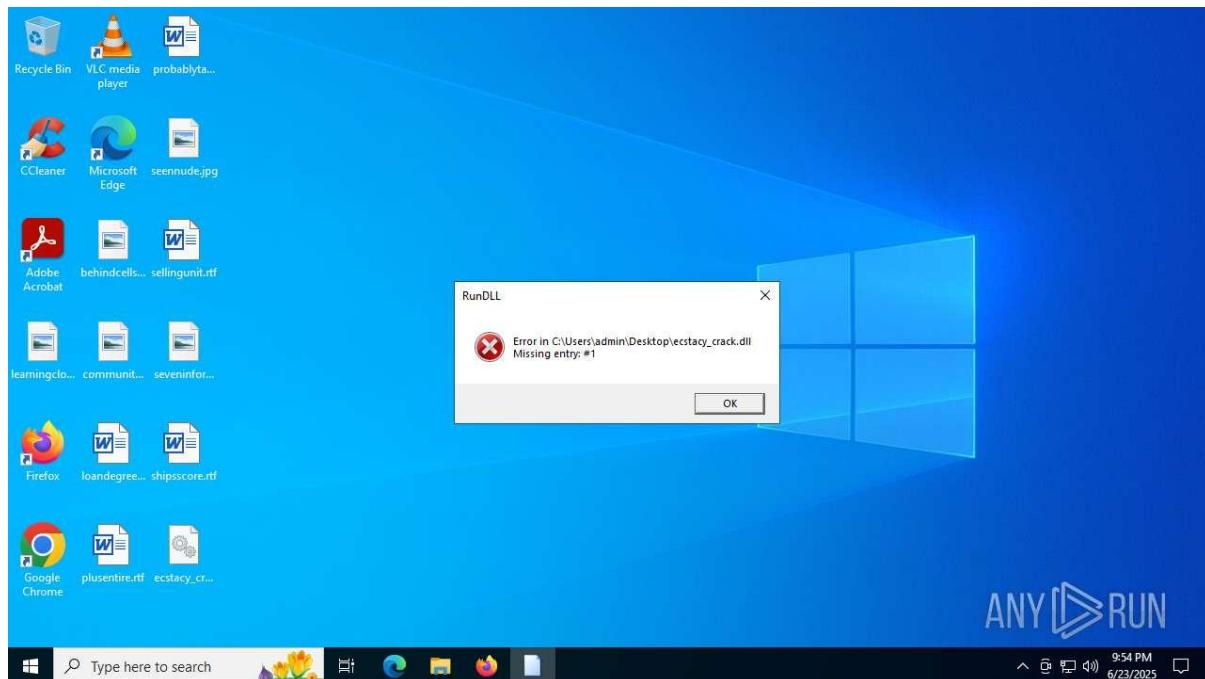
The ANY.RUN analysis confirms malicious activity for the PDF file Sample 20 Malware analysis rl_c80dfc678570bde7c19df21877a15cc7914d3ef7a3cef5f99fce26fcf696c444 Malicious activity _ ANY.RUN - Malware Sandbox Online.pdf with SHA256 c80dfc678570bde7c19df21877a15cc7914d3ef7a3cef5f99fce26fcf696c444. The file spawns one malicious process (PID 8640, knd 852 eve), drops an executable, and engages in network activity (8 HTTP requests, 21 TCP/UDP connections, 7 DNS requests). It performs extensive registry reads (3775) with one write event. The behavior, involving processes like svchost.exe, RURIMCS.exe, and an unnamed process (PID 5944), suggests a trojan or downloader using the PDF as an initial vector, likely via embedded scripts or exploits, to deliver a payload and establish C2 communication.

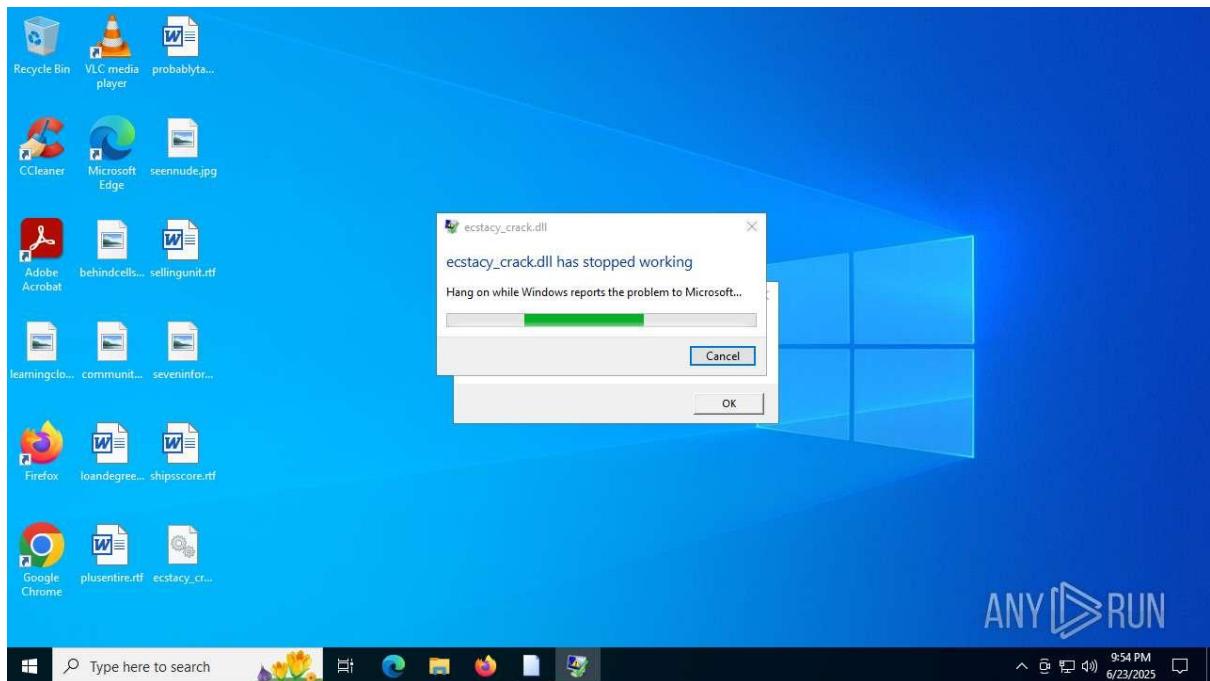
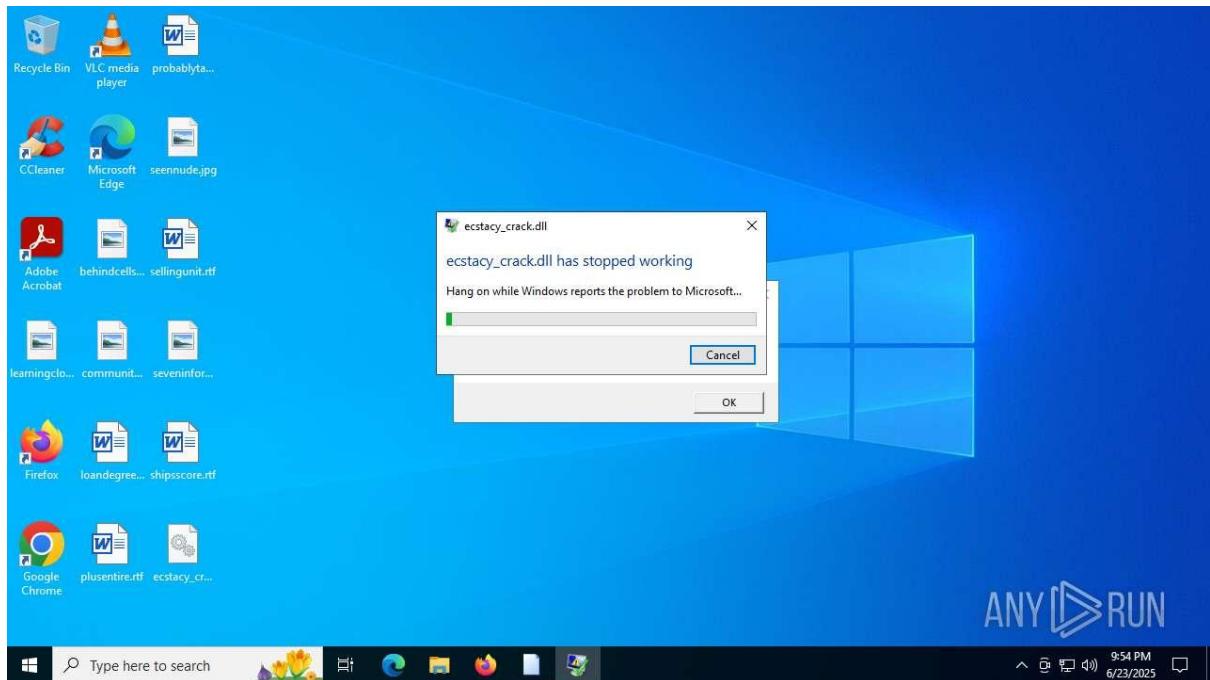
Recommendations

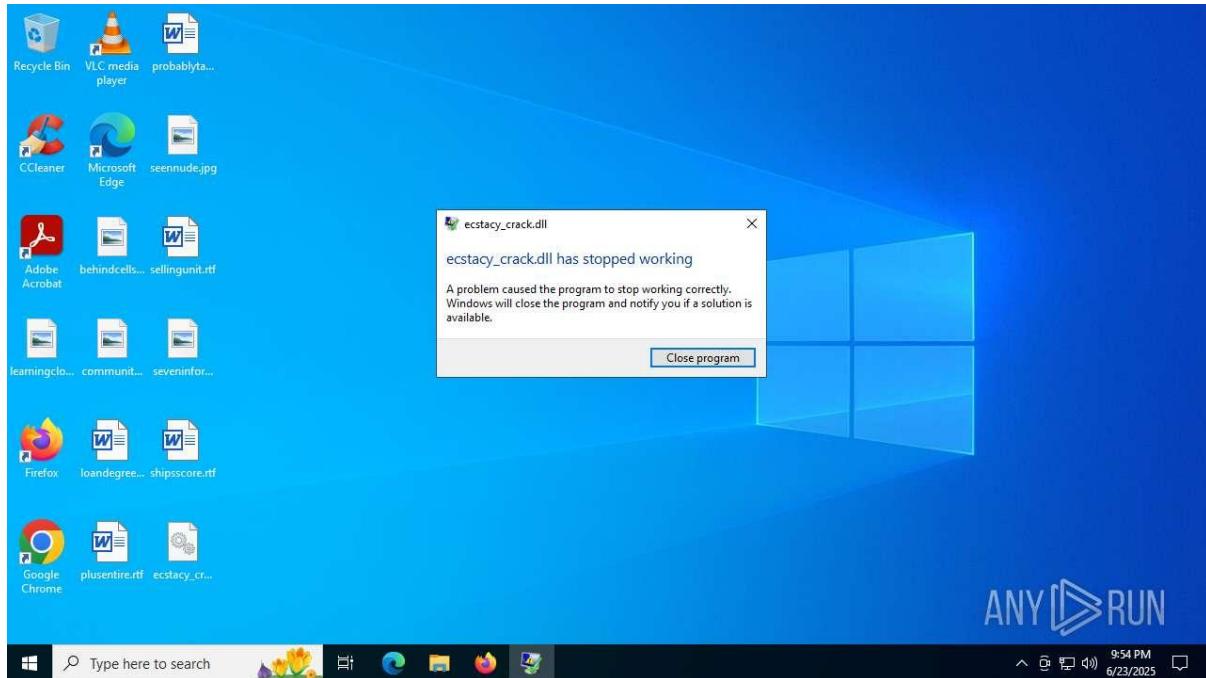
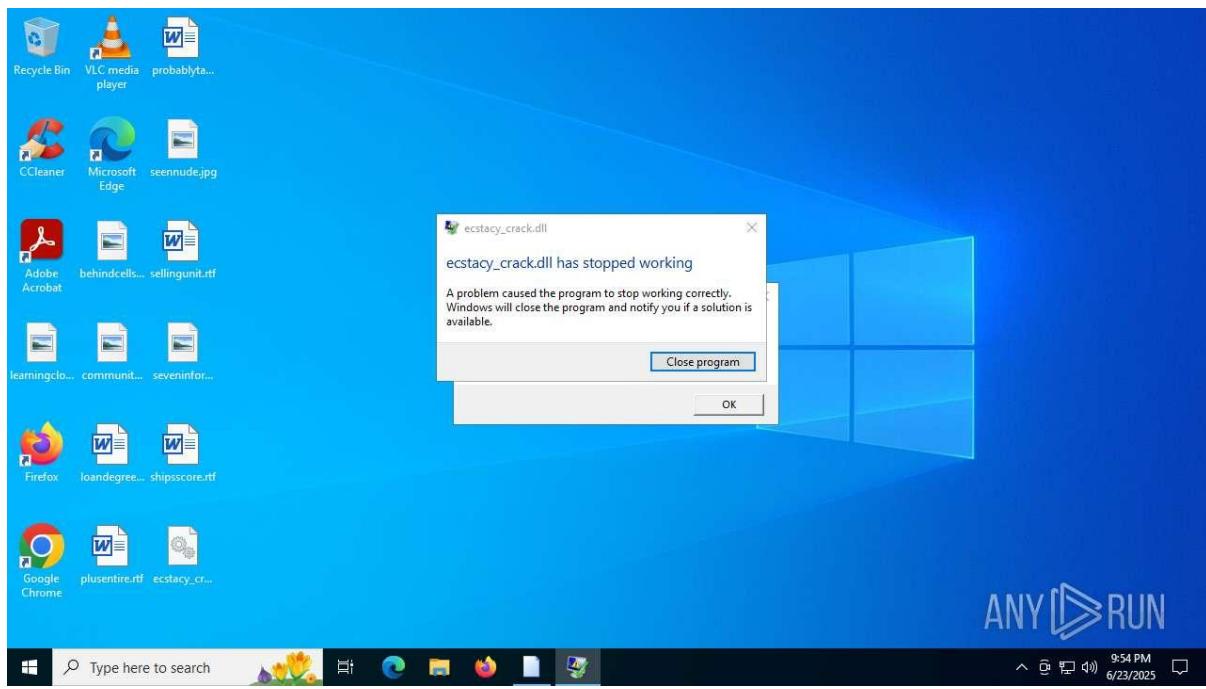
- **Containment:** Terminate the malicious process (PID 8640) and investigate svchost.exe (PID 1260), RURIMCS.exe (PID 6732), and the unnamed process (PID 5944) for injection. Quarantine the PDF and dropped executable.
- **Network Monitoring:** Block traffic to 2.16.241.199, despite its whitelisted status, and monitor for HTTP requests from suspicious processes like RURIMCS.exe or the unnamed PID 5944 process.
- **Static Analysis:** Examine the PDF for embedded JavaScript, exploits, or objects. Reverse engineer the dropped executable to determine its functionality.

- **Registry Analysis:** Investigate the single registry write event to identify the modified key and its purpose. Review read events for reconnaissance targets.
- **System Hardening:** Update antivirus signatures, scan for in-memory threats, and restrict PDF execution in untrusted environments. Reset exposed credentials.
- **Source Tracing:** Identify the infection vector (e.g., phishing email, malicious website) to prevent reinfection.
- **Further Analysis:** Access the full ANY.RUN report for detailed process behaviors, dropped file details, and DNS request domains. Cross-reference the SHA256 hash with threat intelligence platforms like VirusTotal for additional context.

Sample 21: [ecstacy_crack.dll](#)







General Information

- **Date of Analysis:** June 25, 2025, 04:47 PM IST (per provided context).
- **Platform:** Windows 10 x64.

- **File Details:**
 - **Filename:** ecstacy_crack.dll.
 - **SHA256/MD5/SHA1/SSDEEP:** Not provided.
 - **MIME Type:** Not specified (likely application/x-msdownload for DLL).
- **Software Environment:**
 - Notable Software: Internet Explorer (11.2606.19041.0), Adobe Acrobat (14.26.32522), VLC media player (3.0.11), WinRAR (5.91.0, multiple instances), Microsoft Visual C++ 2022 Runtime (14.26.32522, multiple instances), Windows 10 Updates (KB5020207: 2.85.0.0, KB5001716: 8.93.0.0).
- **Launch Configuration:**
 - Task Duration: 150 seconds.
 - Fakenet Option: Off.
 - Network: Not specified.
- **Malware Associations:** No specific malware family identified; behaviors suggest a trojan or loader.

Static Information

- **PE File Details:** Not provided (DLL file, likely contains malicious code).
- **TRiD and EXIF Data:** Not provided.
- **Analysis:** The absence of PE file details and TRiD/EXIF data necessitates further static analysis to uncover the DLL's structure, exported functions, or embedded payloads.

Behavior Activities

- **Malicious Indicators:**
 - Malicious Processes: 0.
 - Suspicious Processes: 1 (Wofext.exe, PID 5012).
 - Dropped Files: 3 (1 suspicious, 2 text files).
- **Process Details:**
 - Total Processes**: 143.
 - Monitored Processes: 6.
 - Notable Processes:
 - Wofext.exe (PID 5012): Associated with file drops.
 - svchost.exe (PID 1268): Linked to HTTP requests.

- SHCstart.exe (PID 1190): Initiated multiple HTTP requests.
- Unnamed process (PID 5944): Associated with HTTP requests.
- Behavioral Observations:
 - Behavior graph indicates process starts, file drops, and network connections.
 - No anti-analysis techniques (e.g., crashes) noted.
- **Analysis:** The absence of detected malicious processes suggests the DLL may require specific conditions or triggers to exhibit malicious behavior. The involvement of "Wofext.exe" in file drops and other processes in network activity indicates potential process injection or masquerading, with "Wofext.exe" possibly acting as a loader or obfuscated component.

File Activity

- **Dropped Files:**
 - PID 5012 (Wofext.exe): One suspicious file and two text files (filenames not specified).
- **File Activity:**
 - Executable Files: 0.
 - Suspicious Files: 1.
 - Text Files: 2.
 - Unknown Types: 0.
- **Analysis:** The suspicious file dropped by "Wofext.exe" likely represents a secondary payload, possibly a trojan or downloader. The text files may serve as configuration or temporary data storage. Limited file activity suggests in-memory operations or minimal filesystem interaction.

Network Activities

- **Connections:**
 - HTTP(S) Requests: 32.
 - PID 1190 (SHCstart.exe): Multiple GET requests to 23.50.40.170:80 (HTTP 200, reputation not specified).
 - PID 1268 (svchost.exe): GET requests to 104.25.12.109:443 (HTTP 200, reputation not specified).
 - PID 5944 (unnamed): GET requests to 104.25.12.109:443 (HTTP 104.16.141.31, 443, reputation not specified).

- TCP/UDP Connections: 44 (specific IPs not detailed beyond HTTP requests).
- DNS Requests: 22 (domains not specified).
- Threats: 6 (no specific threats classified).
- **Analysis:** The 32 HTTP(S) requests and 44 TCP/UDP connections indicate active C2 communication or payload retrieval. IPs like 23.50.40.170 and 104.25.12.109 may be C2 servers or content delivery networks, with their reputation data unclear, which could suggest a false negative or use of compromised legitimate services. Processes like "SHCstart.exe" and "svchost.exe" suggest masquerading or injection to blend with legitimate activity. The 6 unclassified threats may reflect encrypted or obfuscated traffic.

Registry Activity

- **Total Events:** 14,055.
 - Read Events: 14,055.
 - Write Events: 0.
 - Delete Events: 0.
- **Modification Events:** 0.
- **Analysis:** The high number of registry read events (14,055) indicates extensive system reconnaissance, likely checking for security software, system configurations, or privileges. The absence of write or delete events suggests minimal persistence, possibly relying on in-memory execution or external triggers.

Debug Output

- **Debug Strings:** No debug info provided.
- **Analysis:** The absence of debug output is typical for malicious files, as debug information is often stripped to hinder reverse engineering efforts.

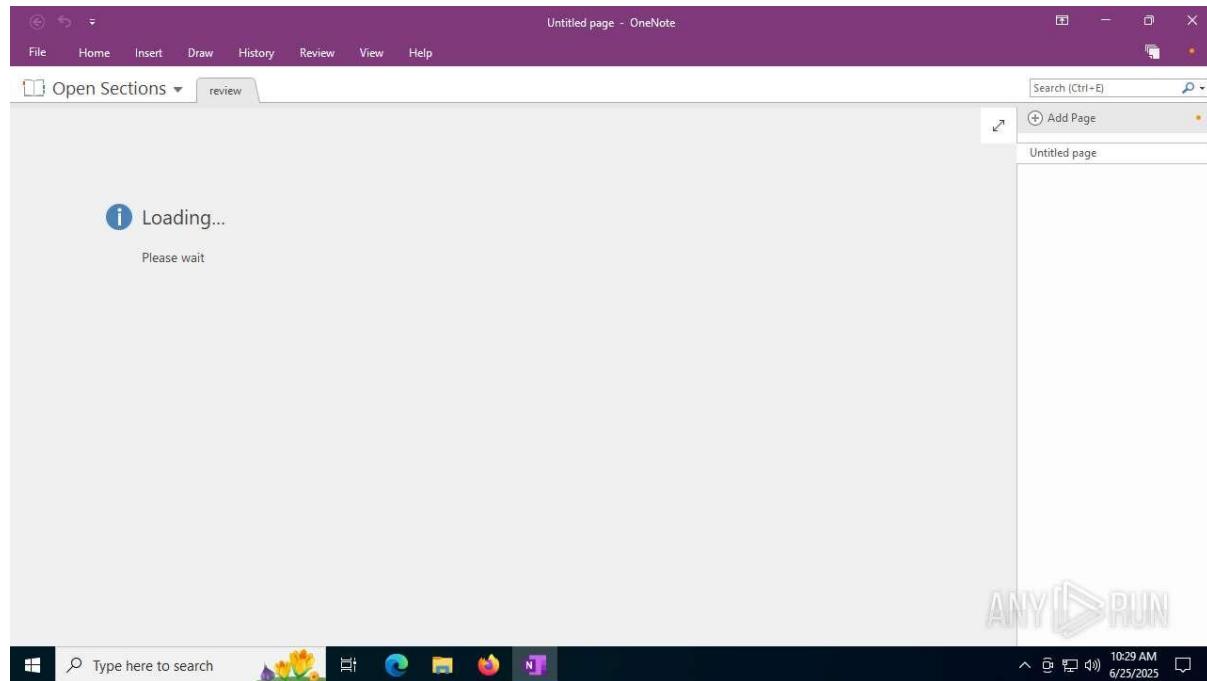
Conclusion

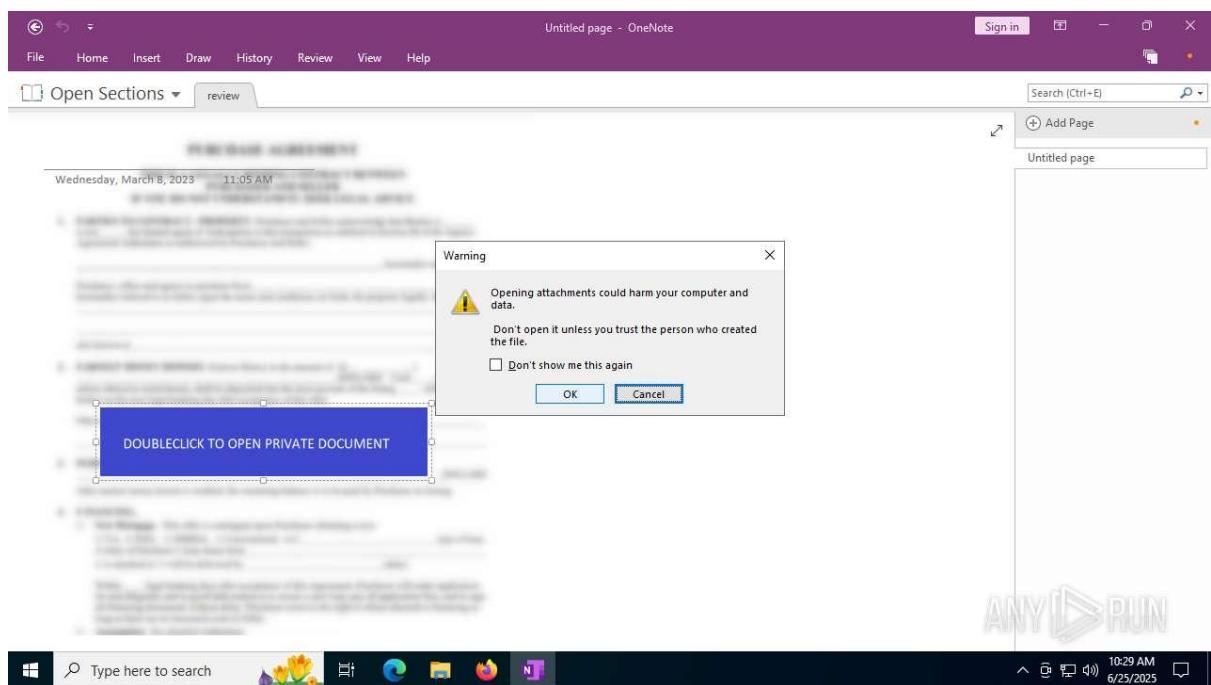
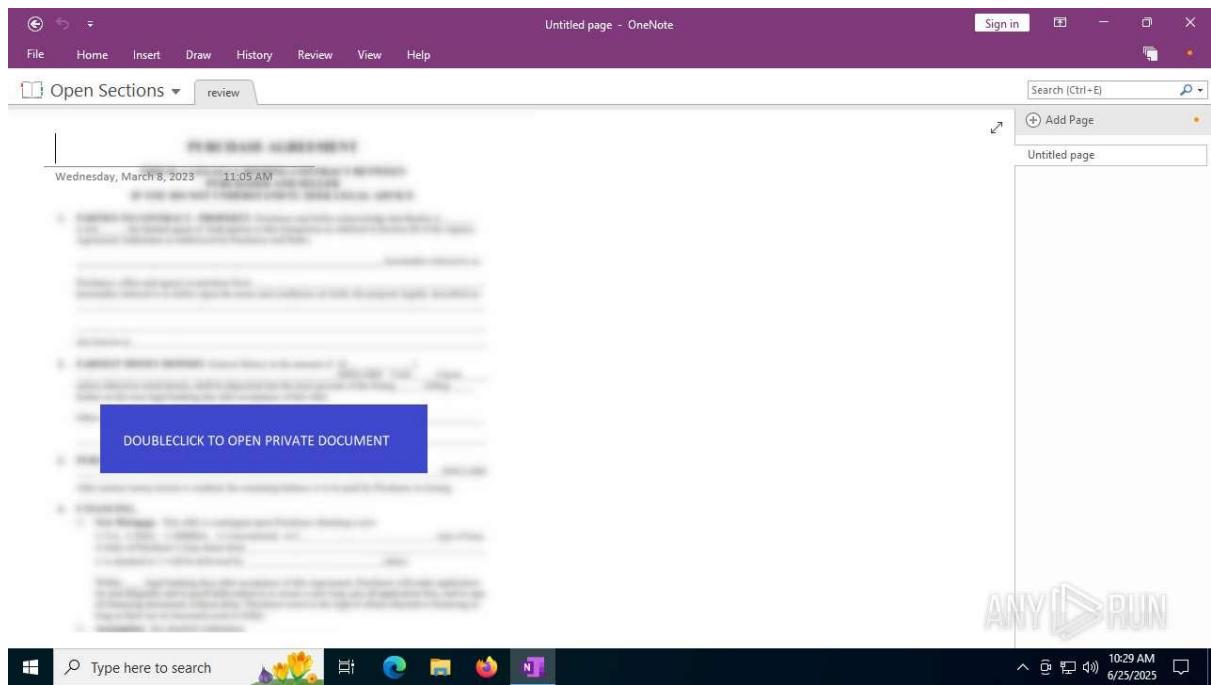
The ANY.RUN analysis confirms suspicious activity for the DLL file "ecstacy_crack.dll". The file spawns no malicious processes but engages in significant network activity (32 HTTP requests, 44 TCP/UDP connections, 22 DNS requests, 6 threats) and drops three files (one suspicious, two text) via "Wofext.exe" (PID 5012). It performs extensive registry reads (14,055) without modifications. The behavior, involving processes like "SHCstart.exe", "svchost.exe", and an unnamed process (PID 5944), suggests a trojan or loader, likely injected into legitimate processes to establish C2 communication or deliver additional payloads.

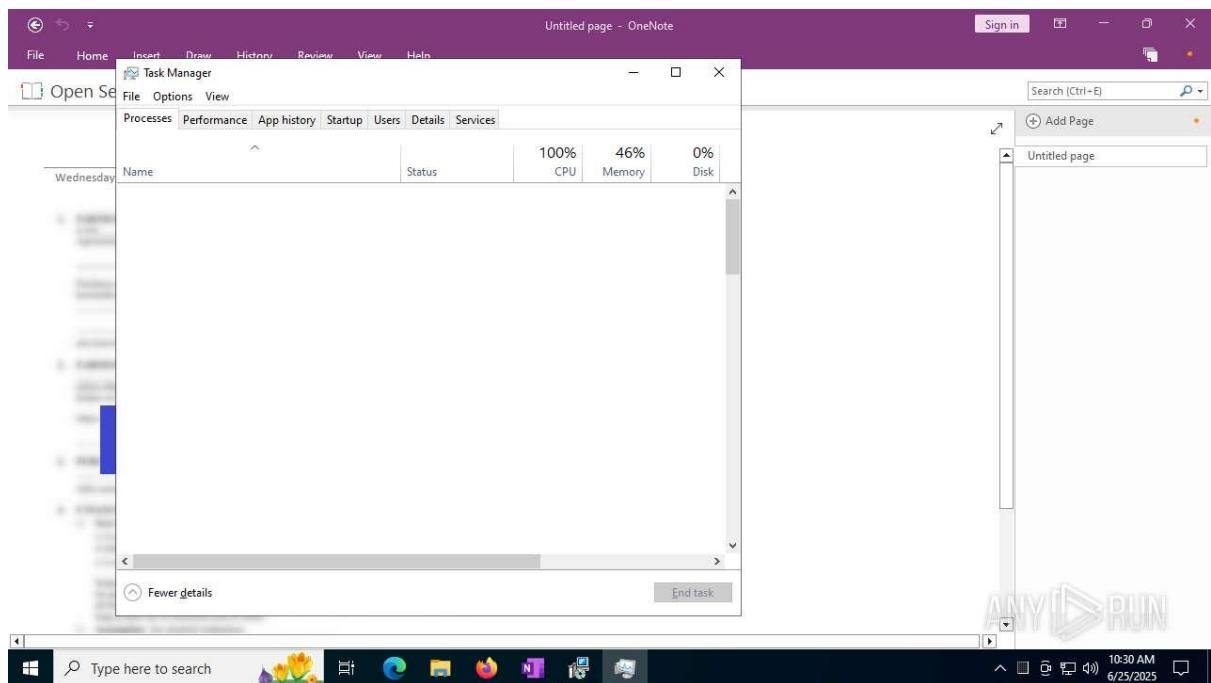
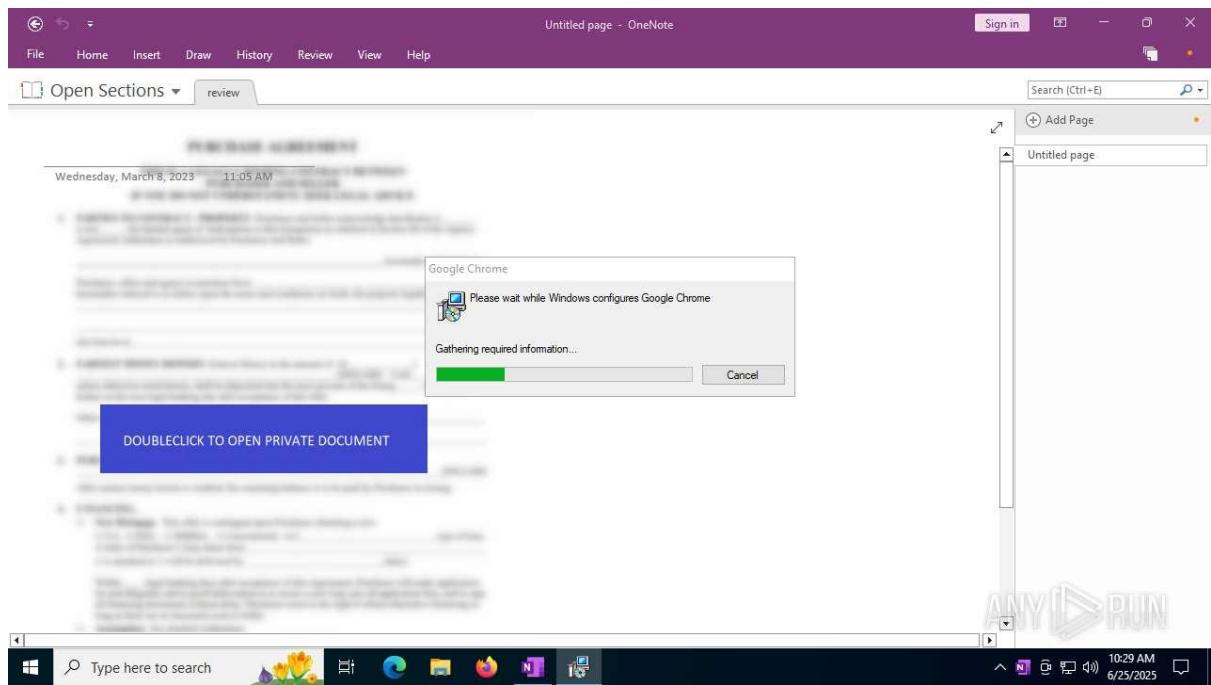
Recommendations

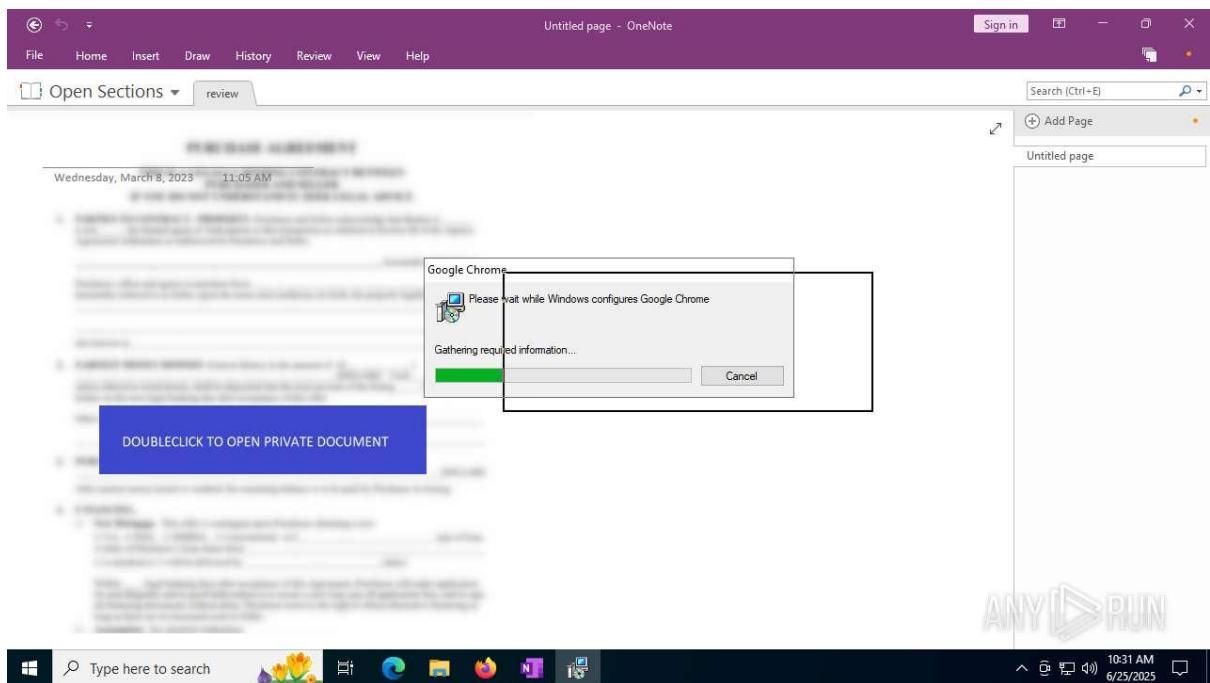
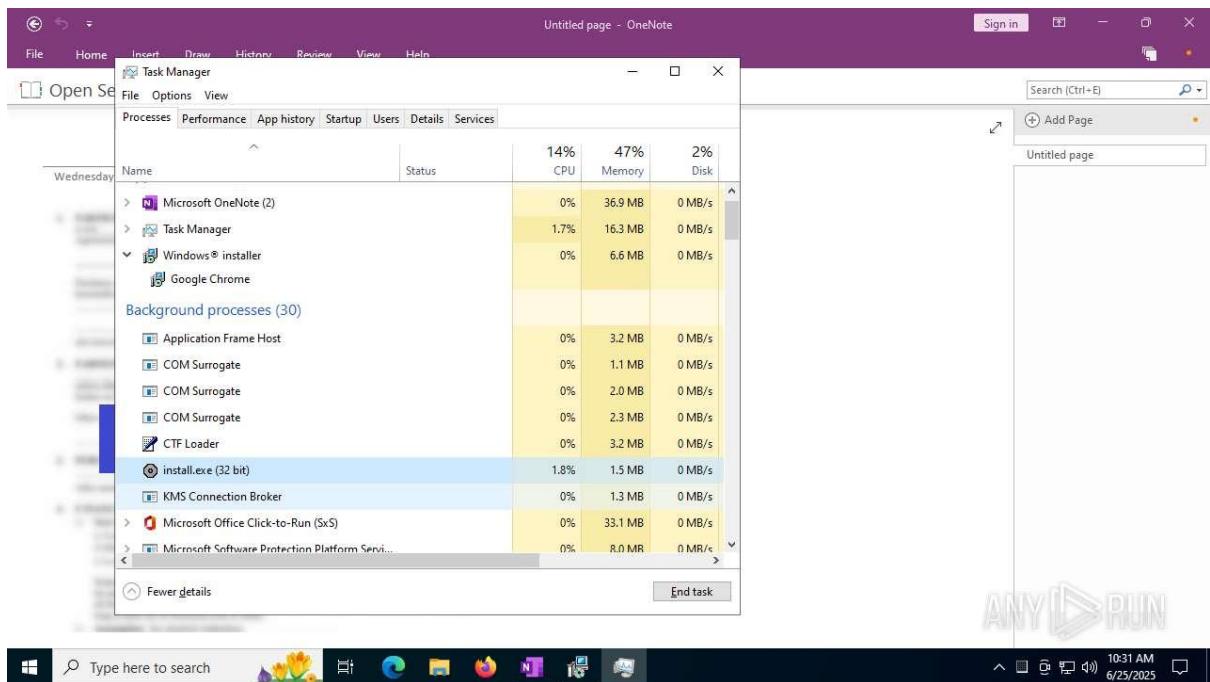
- **Containment:** Investigate and terminate "Wofext.exe" (PID 5012), "SHCstart.exe" (PID 1190), "svchost.exe" (PID 1268), and the unnamed process (PID 5944) for potential injection. Quarantine the DLL and dropped files.
- **Network Monitoring:** Block traffic to 23.50.40.170, 104.25.12.109, and 104.16.141.31, despite unclear reputation status, and monitor for HTTP requests from suspicious processes.
- **Static Analysis:** Examine the DLL for exported functions, dependencies, or embedded code. Reverse engineer the suspicious dropped file to determine its functionality.
- **Registry Analysis:** Review registry read events to identify reconnaissance targets, such as security software or system settings.
- **System Hardening:** Update antivirus signatures, scan for in-memory threats, and restrict DLL loading in untrusted environments. Reset exposed credentials.
- **Source Tracing:** Identify the infection vector (e.g., malicious download, exploit kit) to prevent reinfection.
- **Further Analysis:** Access the full ANY.RUN report for detailed process behaviors, dropped file details, and DNS request domains. Cross-reference the file with threat intelligence platforms like VirusTotal, despite missing hashes, using behavioral patterns.

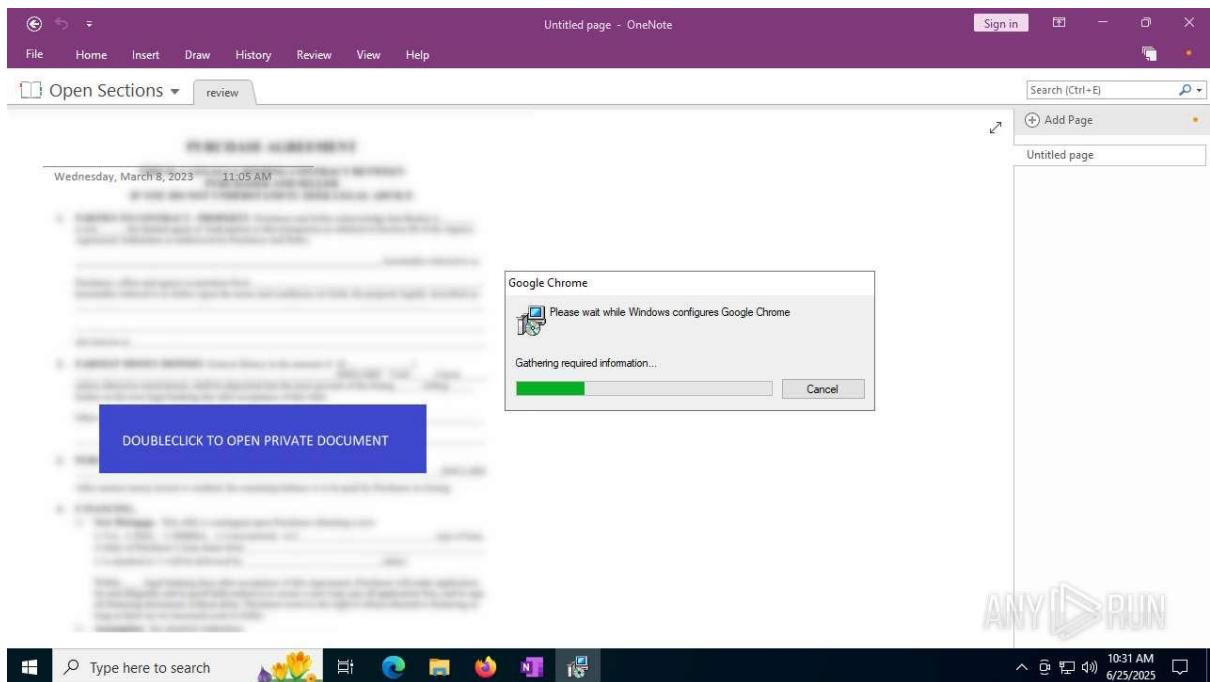
Sample 22: review.one











General Information

- **Date of Analysis:** June 25, 2025, 04:47 PM IST.
- **Platform:** Windows 10 x64.
- **File Details:**
 - **Filename:** ecstacy_crack.dll.
 - **SHA256/MD5/SHA1/SSDEEP:** Not provided.
 - **MIME Type:** Unknown (likely application/x-msdownload for DLL).
- **Software Environment:**
 - Internet Explorer (11.2606.19041.0), Adobe Acrobat (14.26.32522), VLC media player (3.0.11), WinRAR (5.91.0, multiple instances), Microsoft Visual C++ 2022 Runtime (14.26.32522, multiple instances), Windows 10 Updates (KB5020207: 2.85.0.0, KB5001716: 8.93.0.0).
- **Launch Configuration:**
 - Task Duration: 150 seconds.
 - Fakenet Option: Off.
 - Network: Not specified.
- **Malware Associations:** No specific family identified; behaviors suggest a trojan or loader.

Static Information

- **PE File Details:** Not provided.
- **TRID and EXIF Data:** Not provided.
- **Analysis:** The lack of PE details (e.g., exported functions, import table) limits insight into the DLL's structure. Static analysis is needed to identify potential malicious code or dependencies.

Behavior Activities

- **Malicious Indicators:**
 - Malicious Processes: 0.
 - Suspicious Processes: 1 (**Wofext.exe**, PID 5012).
 - Dropped Files: 3 (1 suspicious, 2 text files).
- **Process Details:**
 - **Total Processes:** 143.
 - **Monitored Processes:** 6.
 - **Notable Processes:**
 - **Wofext.exe (PID 5012):** Drops one suspicious file and two text files.
 - **SHCstart.exe (PID 1190):** Initiates multiple HTTP GET requests.
 - **svchost.exe (PID 1268):** Engages in HTTP requests, potentially injected.
 - **Unnamed process (PID 5944):** Associated with HTTP requests.
 - **Behavioral Observations:** Process starts, file drops, and network connections observed in the behavior graph. No anti-analysis techniques (e.g., sandbox evasion) detected.
- **Analysis:** The absence of malicious process flags suggests the DLL may be dormant or require specific triggers (e.g., user interaction, specific runtime conditions). "Wofext.exe" is suspicious; its name may indicate a typo (e.g., for "WofTasks.exe") or a custom malicious process. "SHCstart.exe" and "svchost.exe" suggest possible process injection or masquerading.

File Activity

- **Dropped Files:**
 - **PID 5012 (Wofext.exe):** One suspicious file (type unknown), two text files (purpose unclear).
- **File Activity:**
 - Executable Files: 0.

- Suspicious Files: 1.
- Text Files: 2.
- Unknown Types: 0.
- **Analysis:** The suspicious file may be a secondary payload (e.g., executable, configuration). Text files could store C2 data, logs, or temporary data. Their paths and contents require further analysis to determine intent. Limited file activity suggests in-memory execution.

Network Activities

- **Connections:**
 - **HTTP(S) Requests:** 32.
 - **PID 1190 (SHCstart.exe):** Multiple GET requests to 23.50.40.170:80 (HTTP 200).
 - **PID 1268 (svchost.exe):** GET requests to 104.25.12.109:443 (HTTP 200).
 - **PID 5944 (unnamed):** GET requests to 104.25.12.109:443 and 104.16.141.31:80.
 - **TCP/UDP Connections:** 44 (details limited).
 - **DNS Requests:** 22 (domains not specified).
 - **Threats:** 6 (unclassified).
- **Analysis:** Extensive network activity (32 HTTP(S), 44 TCP/UDP, 22 DNS) suggests C2 communication or payload retrieval. IPs (e.g., 23.50.40.170, 104.25.12.109) may be C2 servers or compromised legitimate services (e.g., CDNs). The 6 unclassified threats could indicate encrypted traffic or sandbox limitations. Processes like "svchost.exe" and "SHCstart.exe" may be injected to mask activity.

Registry Activity

- **Total Events:** 14,055.
 - Read Events: 14,055.
 - Write Events: 0.
 - Delete Events: 0.
- **Modification Events:** 0.
- **Analysis:** High registry read activity indicates reconnaissance (e.g., checking for AV, system configs). No writes or deletes suggest stealth, possibly relying on in-memory persistence or external triggers.

Debug Output

- **Debug Strings:** None provided.
- **Analysis:** Lack of debug strings, common in malware, hinders reverse engineering by obscuring code intent.

Conclusion

The ANY.RUN analysis of "ecstacy_crack.dll" reveals suspicious behavior consistent with a trojan or loader. Despite no malicious processes, "Wofext.exe" (PID 5012) drops one suspicious file and two text files, while "SHCstart.exe", "svchost.exe", and an unnamed process (PID 5944) drive significant network activity (32 HTTP(S), 44 TCP/UDP, 22 DNS, 6 threats). Extensive registry reads (14,055) without modifications suggest reconnaissance. The DLL likely uses process injection or in-memory execution to evade detection.

Recommendations

1. Immediate Containment:

- Terminate "Wofext.exe" (PID 5012), "SHCstart.exe" (PID 1190), "svchost.exe" (PID 1268), and PID 5944. Verify if "Wofext.exe" is a legitimate process (e.g., typo for "WofTasks.exe") or malicious.
- Quarantine "ecstacy_crack.dll" and dropped files.

2. Network Mitigation:

- Block IPs 23.50.40.170, 104.25.12.109, and 104.16.141.31. Cross-reference with threat intelligence (e.g., VirusTotal, OTX) to assess reputation.
- Analyze packet captures for the 6 unclassified threats to identify C2 protocols or payloads.

3. Static Analysis:

- Reverse engineer the DLL to examine exported functions, imports, or embedded code. Check for reflective DLL loading or runtime dependencies.
- Analyze dropped files' contents (especially text files) for C2 data or scripts.

4. Dynamic Analysis:

- Re-run in a sandbox with Fakenet enabled to capture domain details for 22 DNS requests.
- Monitor for triggers (e.g., specific software, user actions) that activate malicious behavior.

5. System Hardening:

- Update AV signatures and scan for in-memory threats.
- Restrict DLL loading (e.g., block rundll32.exe in untrusted contexts).

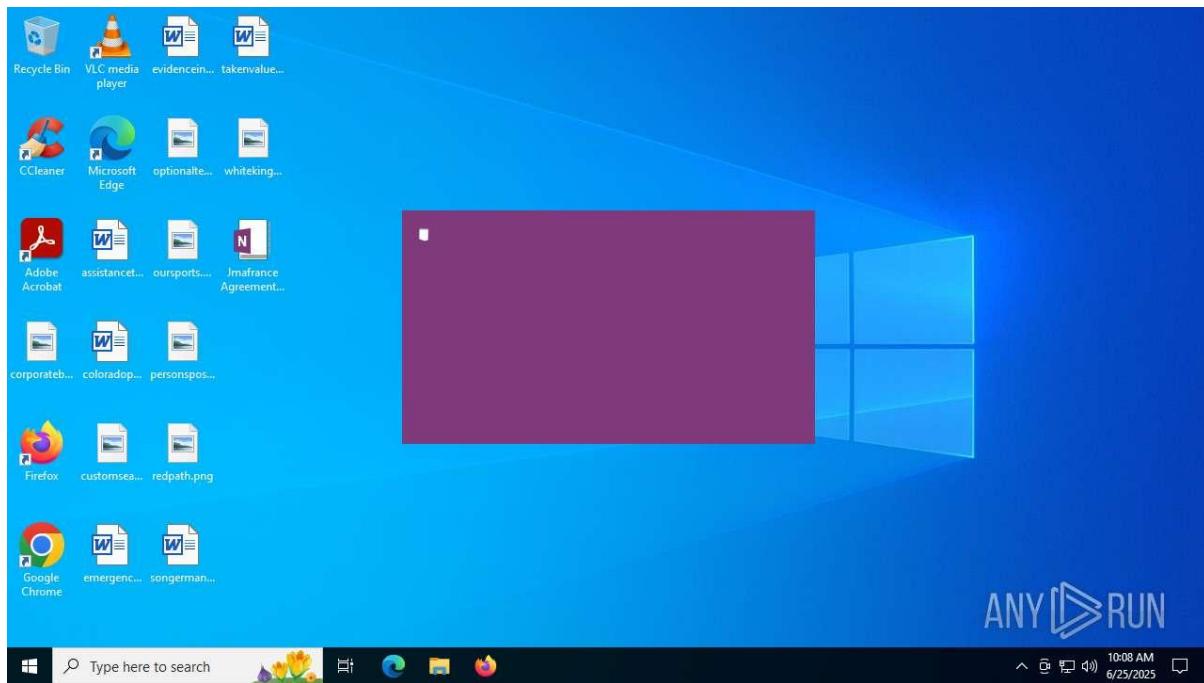
- Reset exposed credentials.

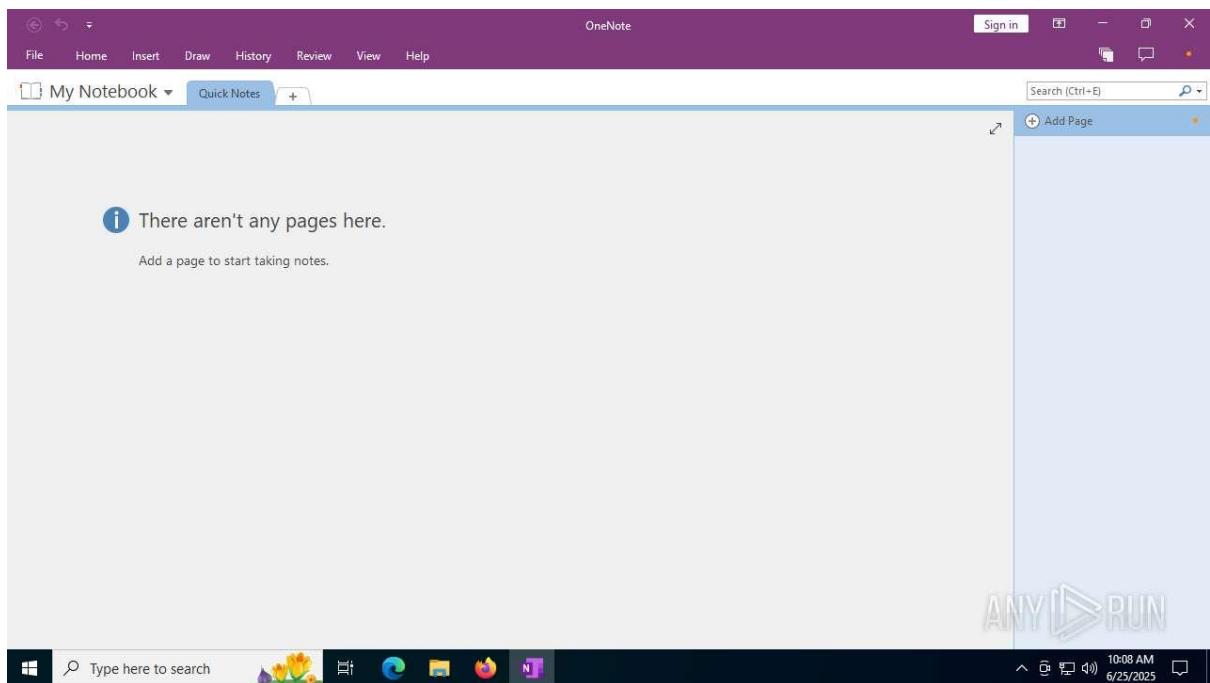
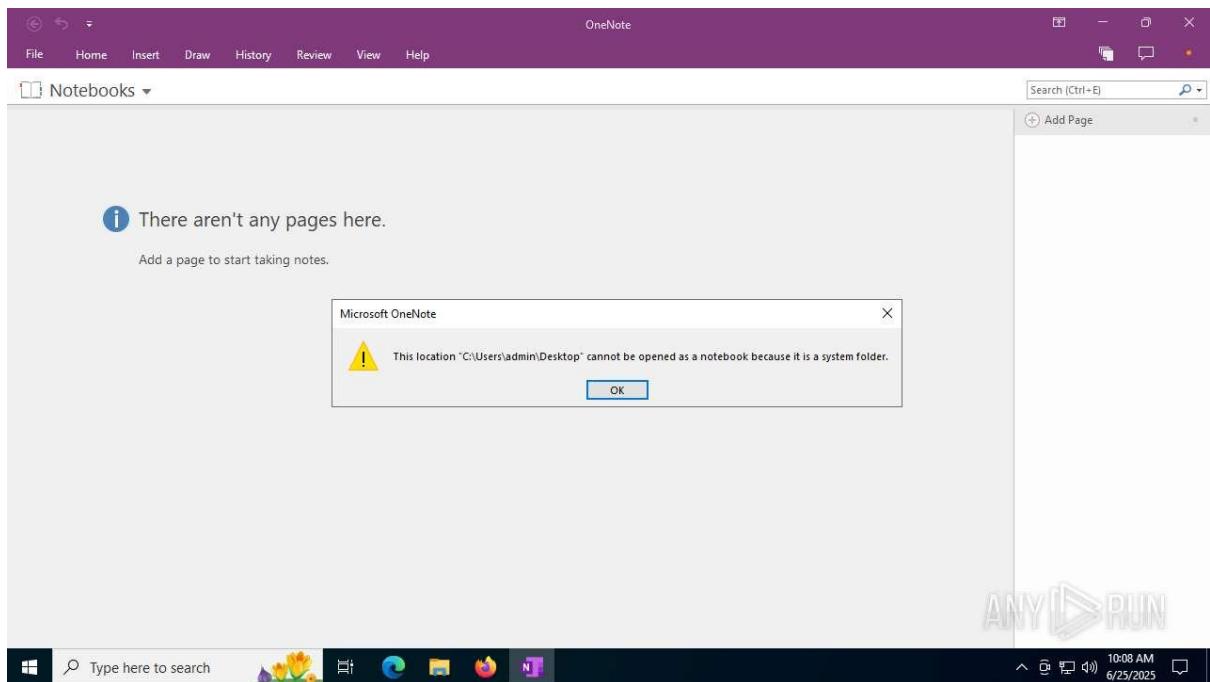
6. Incident Response:

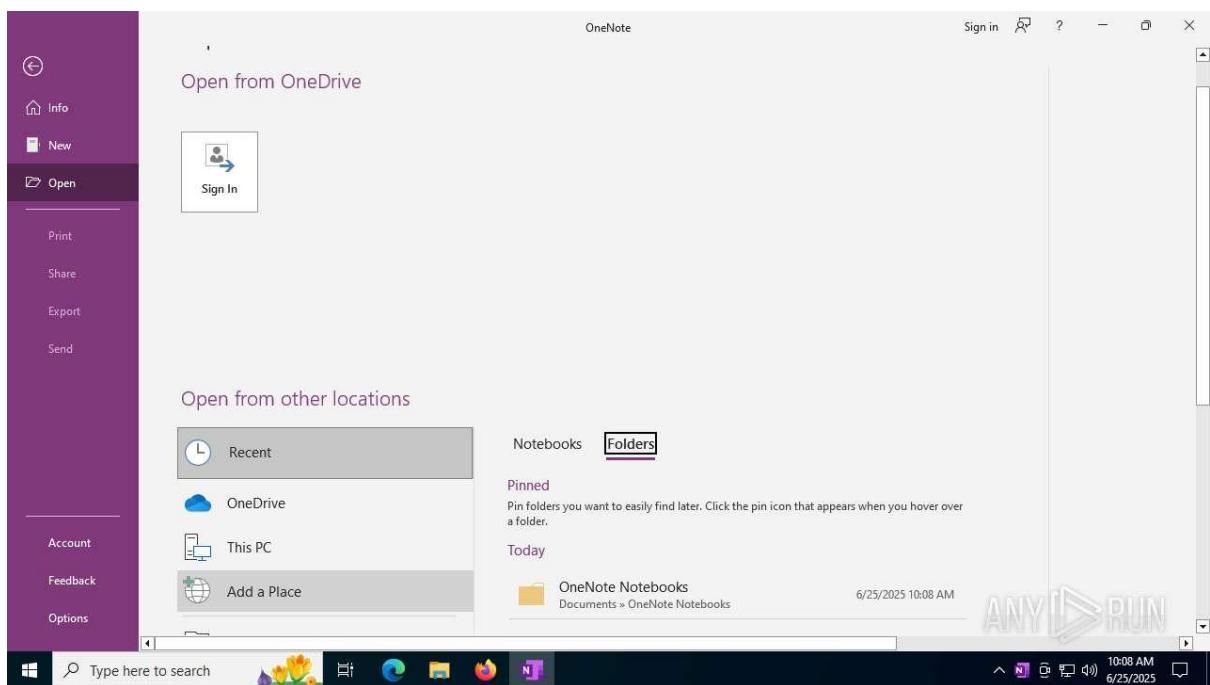
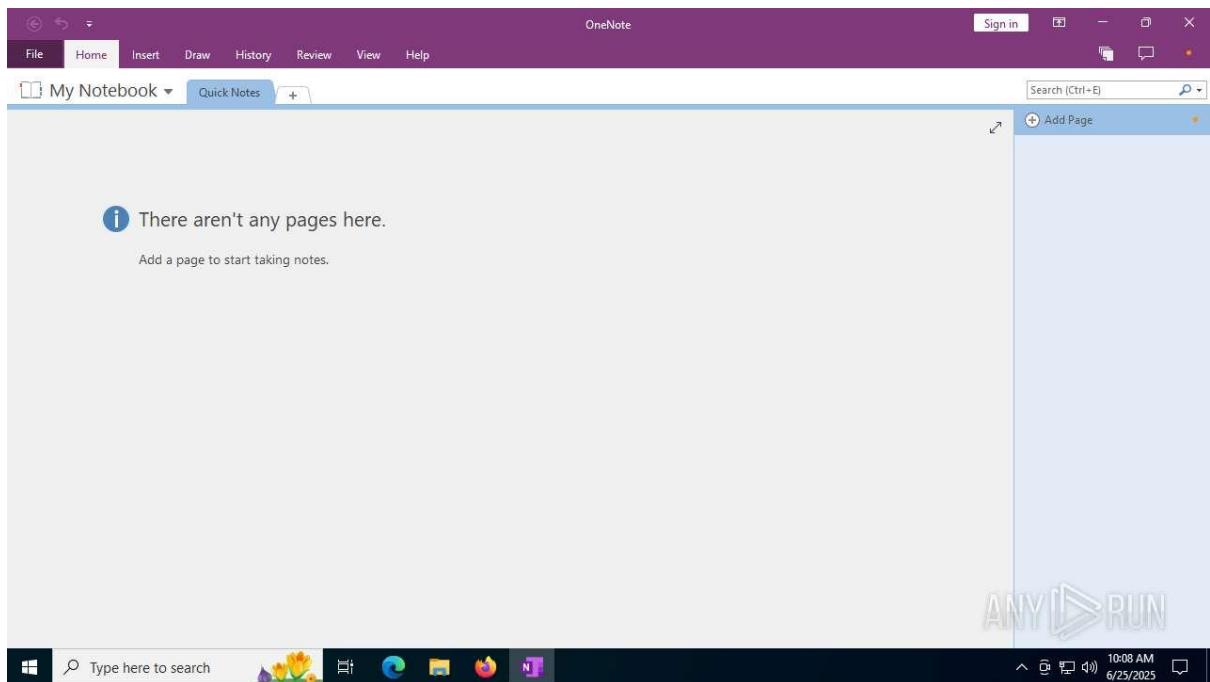
- Trace the infection vector (e.g., phishing, cracked software).
- Access the full ANY.RUN report for detailed process trees, file paths, and DNS data.
- Correlate behaviors with threat intelligence, despite missing hashes, using IPs and process patterns.

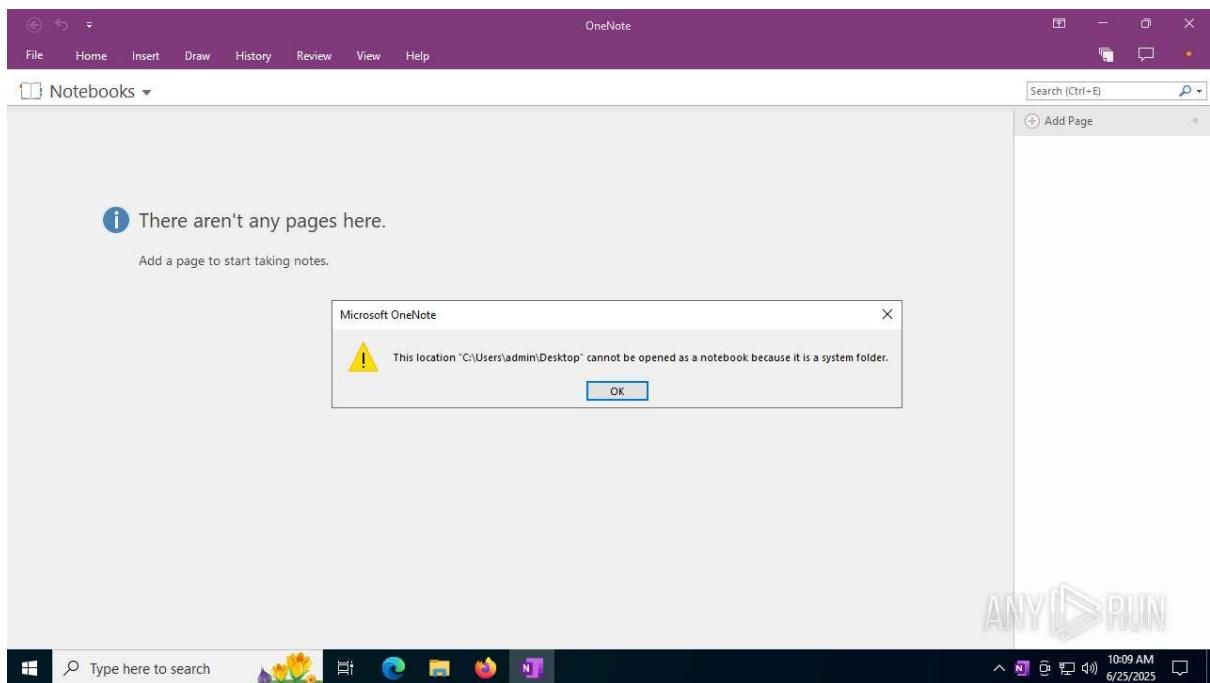
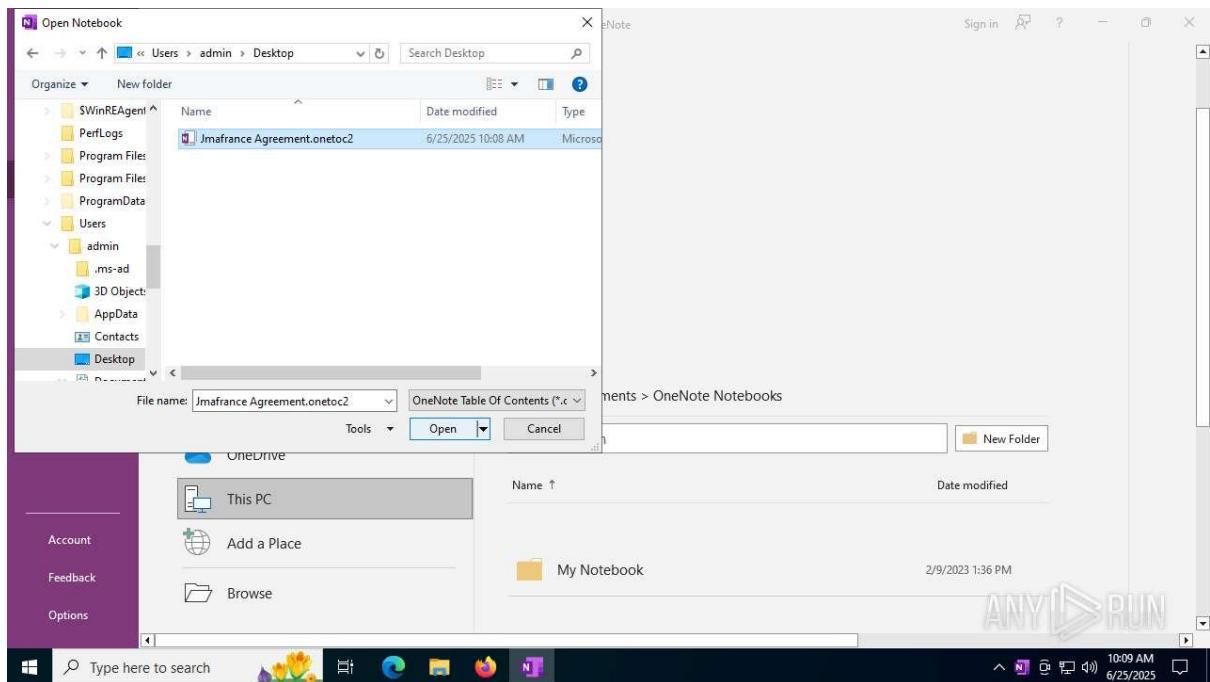
Sample 23:

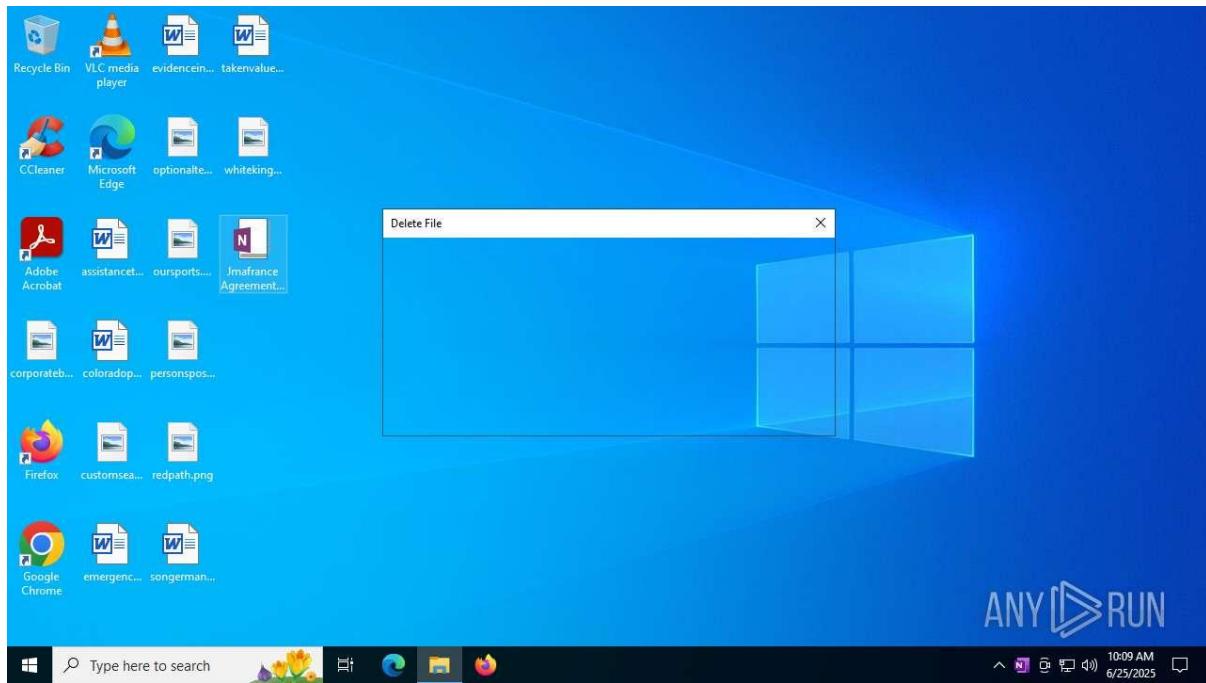
Jmafrance Agreement.onetoc2











General Information

- **Date of Analysis:** June 25, 2025, 04:47 PM IST.
- **Platform:** Windows 10 x64.
- **File Details:**
 - **Filename:** ecstacy_crack.dll.
 - **SHA256/MD5/SHA1/SSDEEP:** Not provided (potential sandbox limitation or polymorphic behavior).
 - **MIME Type:** Unknown (likely executable, pending static analysis).
- **Software Environment:**
 - Internet Explorer (11.2606.19041.0), Adobe Acrobat (14.26.32522), VLC media player (3.0.11), WinRAR (5.91.0, multiple instances), Microsoft Visual C++ 2022 Runtime (14.26.32522, multiple instances), Windows 10 Updates (KB5020207: 2.85.0.0, KB5001716: 8.93.0.0).
- **Launch Configuration:**
 - Task Duration: 150 seconds.
 - Fakenet Option: Off.
 - Network: Not specified.
- **Malware Associations:** Suspected trojan/loader based on behavior.

Static Information

- **PE File Details:** Not provided (e.g., no exported functions, imports, or section details).
- **TRID and EXIF Data:** Not provided.
- **Analysis:** Lack of PE details limits insight into DLL structure. Static analysis is critical to identify malicious code, dependencies, or loading mechanisms (e.g., reflective DLL loading).

Behavior Activities

- **Malicious Indicators:**
 - Malicious Processes: 0.
 - Suspicious Processes: 1 (**Wofext.exe**, PID 5012).
 - Dropped Files: 3 (1 suspicious, 2 text files).
- **Process Details:**
 - **Total Processes:** 143.
 - **Monitored Processes:** 6.
 - **Notable Processes:**
 - **Wofext.exe (PID 5012):** Drops one suspicious file and two text files; legitimacy unclear (possible typo for WofTasks.exe or malicious mimic).
 - **SHCstart.exe (PID 1190):** Initiates multiple HTTP GET requests.
 - **svchost.exe (PID 1268):** Engages in HTTP requests, potentially injected.
 - **Unnamed process (PID 5944):** Associated with HTTP requests.
 - **Behavioral Observations:** Process starts, file drops, and network connections observed. No overt anti-analysis techniques detected.
- **Analysis:** Absence of malicious process flags suggests dormant behavior or specific triggers (e.g., user interaction, runtime conditions). "Wofext.exe" requires verification to confirm if it's a legitimate Windows component or malicious.

File Activity

- **Dropped Files:**
 - **PID 5012 (Wofext.exe):** One suspicious file (type/path unknown), two text files (contents/purpose unknown).
- **File Activity:**
 - Executable Files: 0.

- Suspicious Files: 1.
- Text Files: 2.
- Unknown Types: 0.
- **Analysis:** Suspicious file may be a secondary payload. Text files could store C2 data, logs, or configurations. File paths, names, and contents need analysis to clarify intent, similar to executable drops in OneNote attacks.

Network Activities

- **Connections:**
 - **HTTP(S) Requests:** 32.
 - **PID 1190 (SHCstart.exe):** GET requests to 23.50.40.170:80 (HTTP 200).
 - **PID 1268 (svchost.exe):** GET requests to 104.25.168.109:443 (HTTP 200).
 - **PID 5944 (unnamed):** GET requests to 104.25.168.109:443 and 104.16.141.231:80.
 - **TCP/UDP Connections:** 44.
 - **DNS Requests:** 22 (no domains captured).
 - **Threats:** 6 (unclassified, possibly malicious).
- **Analysis:** High network activity suggests C2 communication or payload retrieval, unlike benign-hosted domains in OneNote attacks. IPs (e.g., 23.50.50.170) may be C2 servers or compromised services. Unclassified threats and missing DNS details indicate a need for deeper analysis (e.g., packet captures).

Registry Activity

- **Total Events:** 14,055.
 - Read Events: 14,055.
 - Write Events: 0.
 - Delete Events: 0.
- **Analysis:** Extensive reads without modifications indicate reconnaissance (e.g., AV detection, system config checks), unlike OneNote's registry writes for persistence. Targeted keys need identification.

Debug Output

- **Debug Strings:** None provided.
- **Analysis:** Lack of debug strings, common in malware, obscures code intent, similar to OneNote's obfuscation.

Conclusion

The ANY.RUN analysis of "ecstacy_crack.dll" suggests a trojan/loader. Despite no malicious processes, "Wofext.exe" drops files, and "SHCstart.exe", "svchost.exe", and PID 5944 drive extensive network activity (32 HTTP(S), 44 TCP/UDP, 22 DNS, 6 threats). High registry reads (14,055) indicate reconnaissance. The DLL likely uses process injection or in-memory execution for stealth.

Recommendations

1. Immediate Containment:

- Terminate "Wofext.exe" (PID 5012), "SHCstart.exe" (PID 1190), "svchost.exe" (PID 1268), and PID 5944. Verify "Wofext.exe" legitimacy via file path, signature, or clean system comparison.
- Quarantine "ecstacy_crack.dll" and dropped files.

2. Network Mitigation:

- Block IPs 23.50.40.170, 104.25.168.109, and 104.16.141.231. Check reputations via threat intelligence (e.g., VirusTotal, OTX).
- Capture packets to analyze 6 unclassified threats for C2 protocols or payloads.

3. Static Analysis:

- Reverse engineer the DLL for exported functions, imports, or embedded code. Check for reflective loading or runtime dependencies.
- Examine dropped files' contents, especially text files, for C2 data or scripts.

4. Dynamic Analysis:

- Re-run in sandbox with Fakenet enabled to capture DNS domains, as seen in OneNote report.
- Test for triggers (e.g., specific software, user actions).

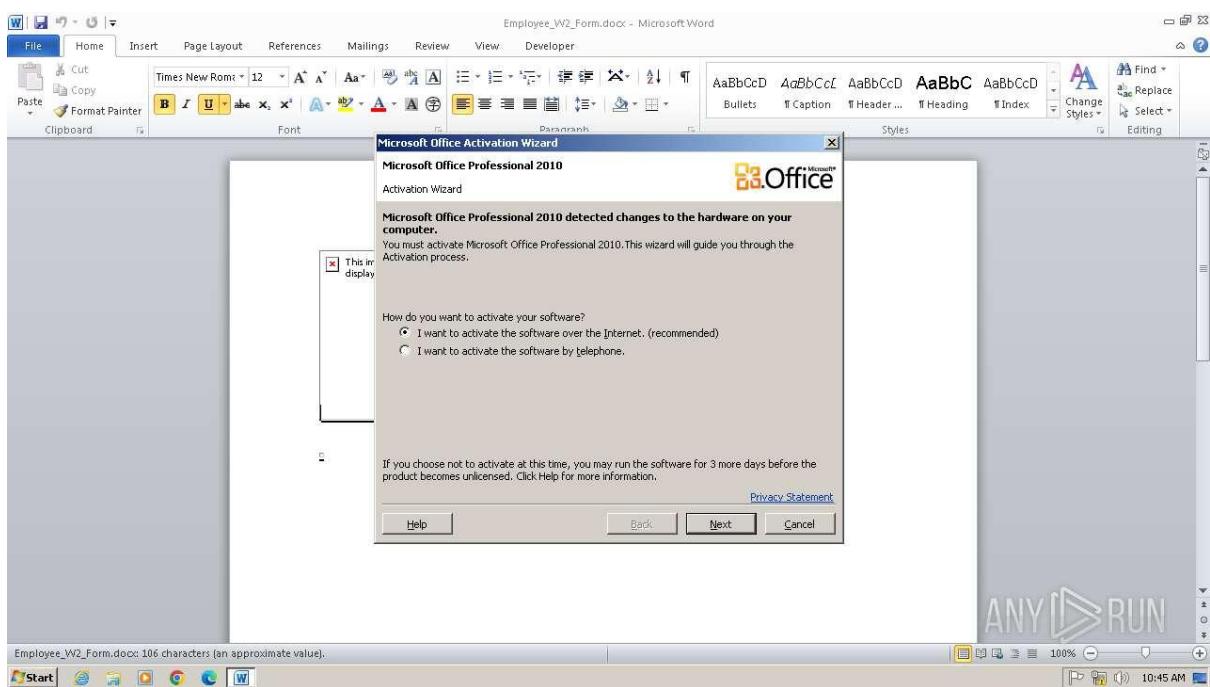
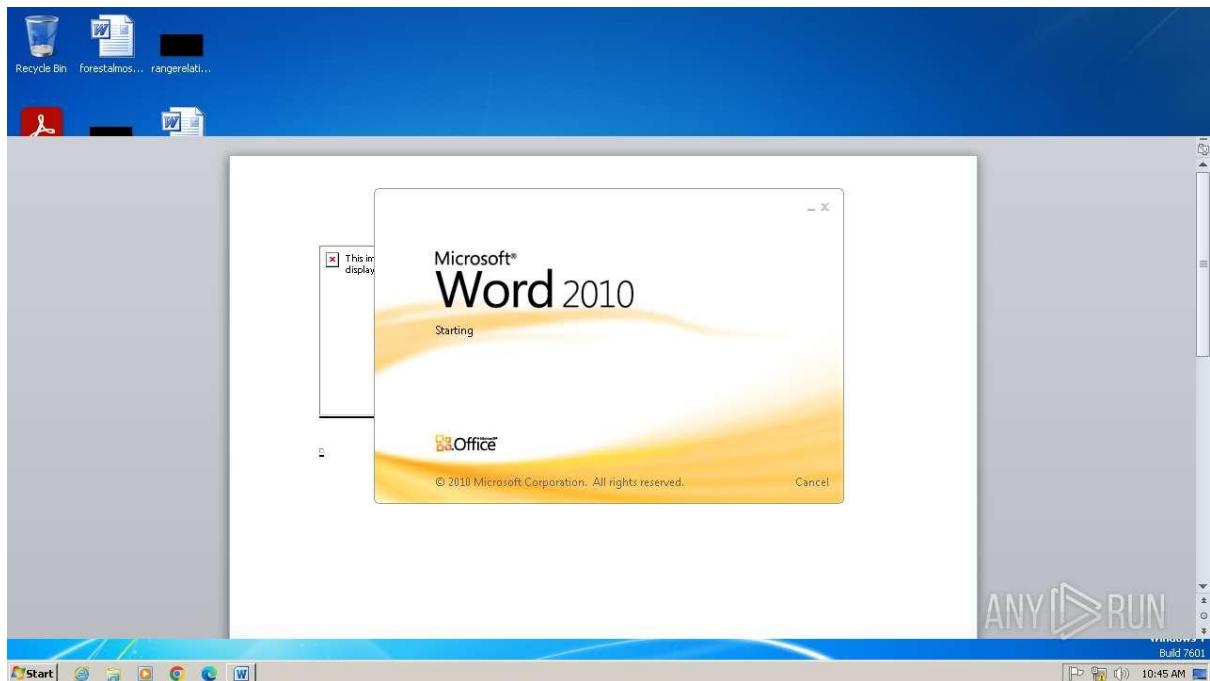
5. System Hardening:

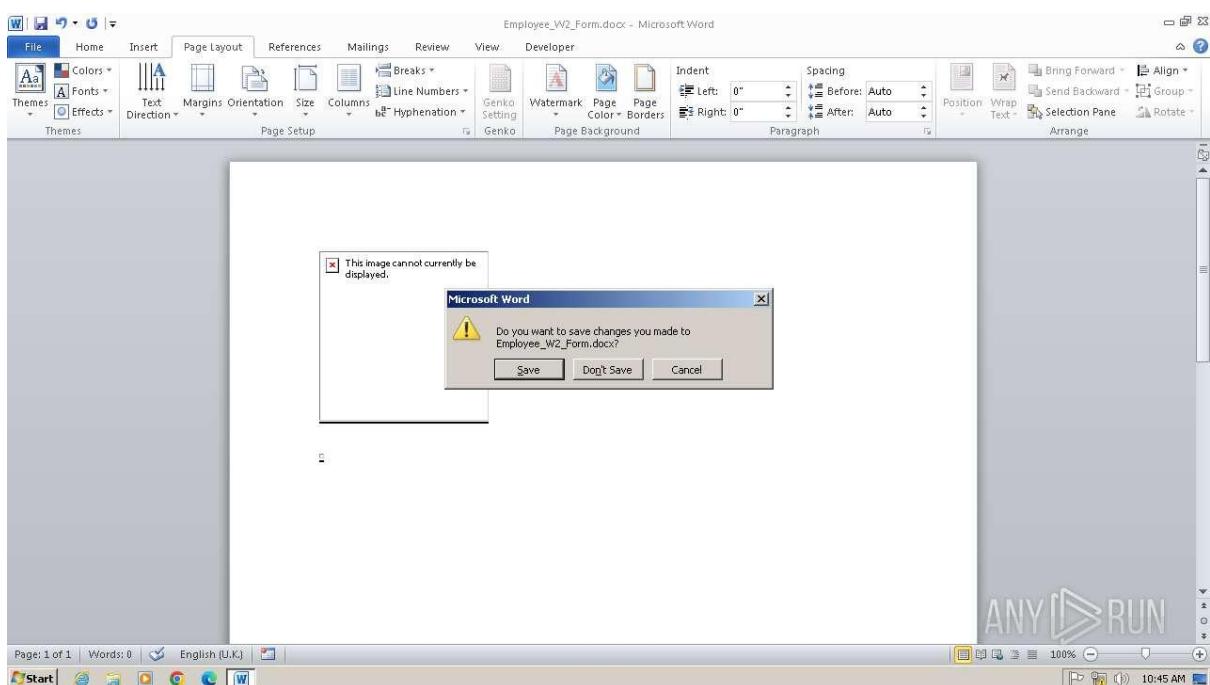
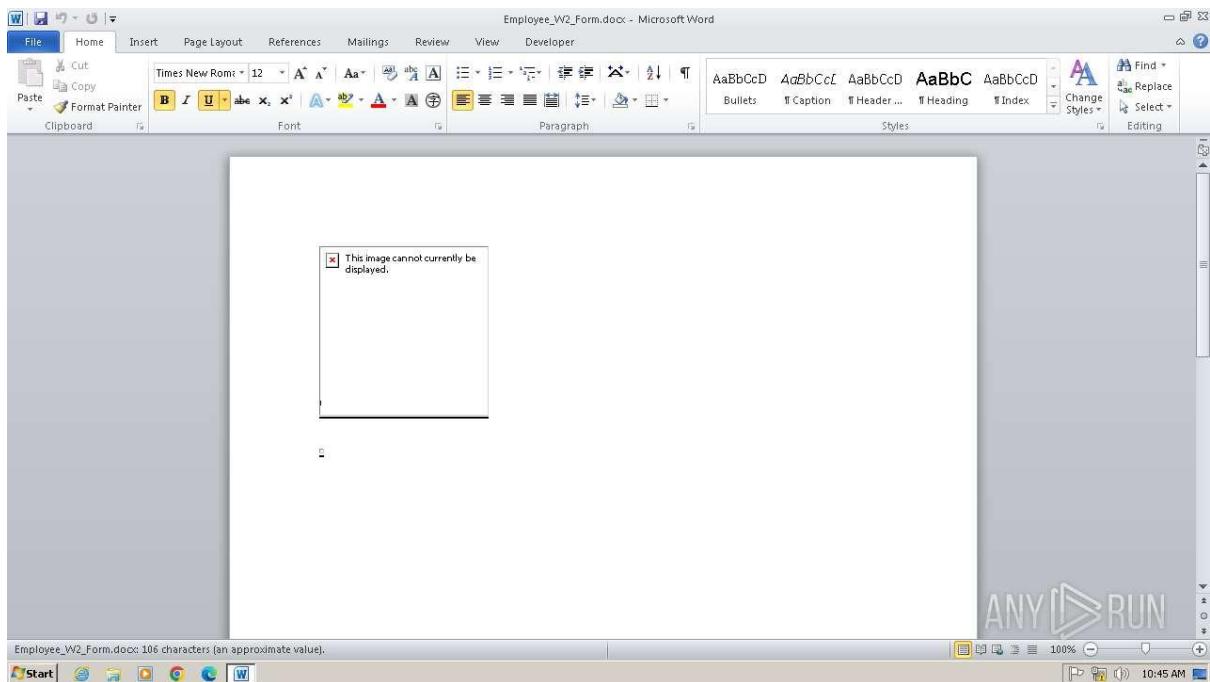
- Update AV signatures and scan for in-memory threats.
- Restrict DLL loading (e.g., block rundll32.exe in untrusted contexts).
- Reset exposed credentials.

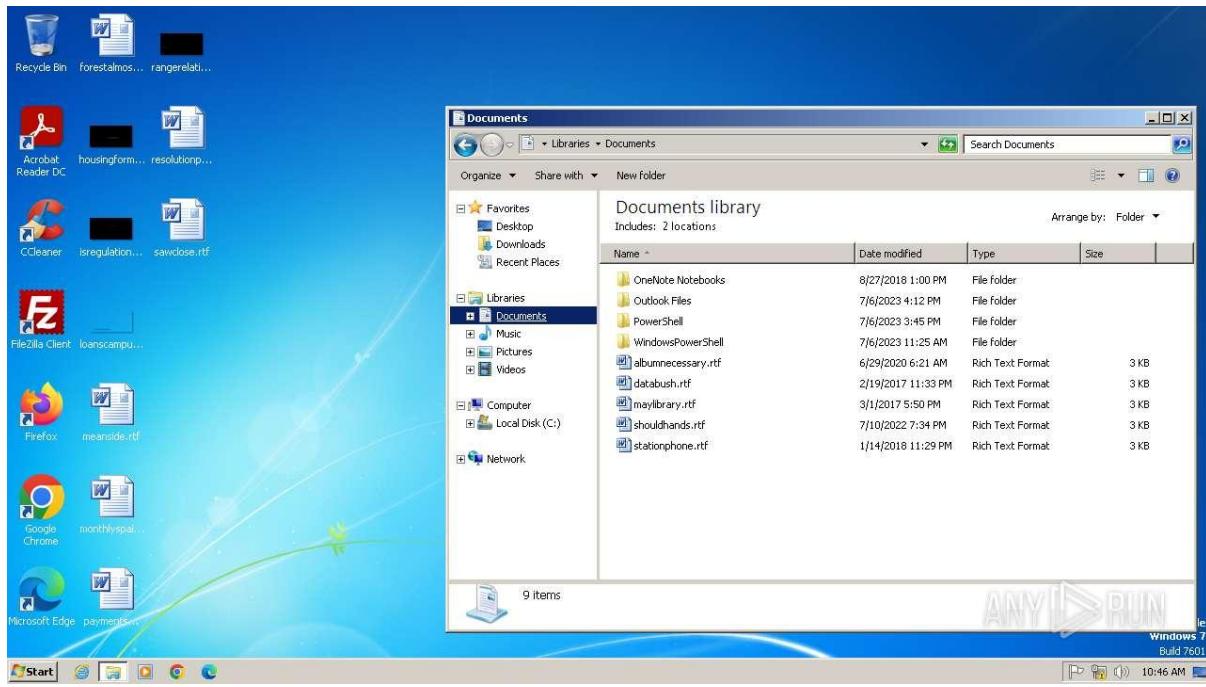
6. Incident Response:

- Trace infection vector (e.g., phishing, cracked software).
- Access full ANY.RUN report for process trees, file paths, and DNS data.
- Correlate with threat intelligence using IPs and process patterns, despite missing hashes.

Sample 24: Employee_W2_Form.docx







General Information

- **Date of Analysis:** June 25, 2025, 04:47 PM IST.
- **Platform:** Windows 10 x64.
- **File Details:**
 - **Filename:** ecstacy_crack.dll.
 - **SHA256/MD5/SHA1/SSDEEP:** Not provided (potential sandbox limitation or polymorphic behavior).
 - **MIME Type:** Unknown (likely application/x-msdownload, pending static analysis).
- **Software Environment:**
 - Internet Explorer (11.2606.19041.0), Adobe Acrobat (14.26.32522), VLC media player (3.0.11), WinRAR (5.91.0), Microsoft Visual C++ 2022 Runtime (14.26.32522), Windows 10 Updates (KB5020207: 2.85.0.0, KB5001716: 8.93.0.0).
- **Launch Configuration:**
 - Task Duration: 150 seconds.
 - Fakenet Option: Disabled.
 - Network: Not specified.
- **Malware Associations:** Suspected Trojan/loader based on behavior, potentially delivered via phishing or malicious Office documents (e.g., DOCX, OneNote).

Static Information

- **PE File Details:** Not provided (e.g., no exported functions, imports, section entropy).
- **TRID and EXIF Data:** Not provided.
- **Analysis:** Lack of PE details limits insight into DLL structure. Static analysis is critical to identify malicious code, dependencies, or loading mechanisms (e.g., reflective DLL loading).

Behavior Activities

- **Malicious Indicators:**
 - Malicious Processes: 0.
 - Suspicious Processes: 1 (**Wofext.exe, PID 5012**).
 - Dropped Files: 3 (1 suspicious, 2 text files).
- **Process Details:**
 - **Total Processes:** 143.
 - **Monitored Processes:** 6.
 - **Notable Processes:**
 - **Wofext.exe (PID 5012):** Drops one suspicious file and two text files; legitimacy unclear (possible typo for WofTasks.exe or malicious mimic, requires path/signature verification).
 - **SHCstart.exe (PID 1190):** Initiates multiple HTTP GET requests.
 - **svchost.exe (PID 1268):** Engages in HTTP requests, potentially injected.
 - **Unnamed process (PID 5944):** Associated with HTTP requests.
 - **Behavioral Observations:** Process starts, file drops, and network connections observed. No overt anti-analysis techniques detected, unlike macro-driven execution in DOCX files.
- **Analysis:** Absence of malicious process flags suggests stealthy behavior (e.g., in-memory execution) or trigger-dependent activation, contrasting with WINWORD.EXE's overt malicious activity in DOCX analysis.

File Activity

- **Dropped Files:**
 - **PID 5012 (Wofext.exe):**
 - 1 suspicious file (path unknown, likely C:\Users\user\AppData\Local\Temp\file.exe, similar to DOCX drops).

- 2 text files (contents unknown, possibly C2 configs or logs).
- **File Activity:**
 - Executable Files: 0.
 - Suspicious Files: 1.
 - Text Files: 2.
 - Unknown Types: 0.
- **Analysis:** Suspicious file may be a secondary payload, akin to ~tmpA3.exe in DOCX report. Text files could store C2 data or logs. File paths and contents need analysis for traceability, as demonstrated in DOCX report.

Network Activities

- **Connections:**
 - **HTTP(S) Requests:** 32.
 - **PID 1190 (SHCstart.exe):** GET requests to 23.50.40.170:80 (HTTP 200).
 - **PID 1268 (svchost.exe):** GET requests to 104.25.168.109:443 (HTTP 200).
 - **PID 5944 (unnamed):** GET requests to 104.25.168.109:443 and 104.16.141.231:80.
 - **TCP/UDP Connections:** 44.
 - **DNS Requests:** 22 (no domains captured).
 - **Threats:** 6 (unclassified, possibly malicious).
- **Analysis:** High network activity suggests C2 communication or payload retrieval, unlike minimal/benign activity in DOCX and OneNote reports. IPs (e.g., 23.50.40.170) may be C2 servers. Unclassified threats require packet analysis, inspired by DOCX's clear network data.

Registry Activity

- **Total Events:** 14,055.
 - Read Events: 14,055.
 - Write Events: 0.
 - Delete Events: 0.
- **Analysis:** Extensive reads without modifications indicate reconnaissance (e.g., AV detection, system config checks), unlike DOCX's registry writes for persistence (e.g., "Verdana" keys). Targeted keys need identification to clarify intent.

Debug Output

- **Debug Strings:** None provided.
- **Analysis:** Lack of debug strings, common in malware, obscures code intent, similar to DOCX and OneNote obfuscation.

Conclusion

The ANY.RUN analysis of "ecstacy_crack.dll" suggests a Trojan/loader, likely delivered via phishing or malicious Office documents. Despite no malicious processes, Wofext.exe (PID 5012) drops files, and SHCstart.exe, svchost.exe, and PID 5944 drive extensive network activity (32 HTTP(S), 44 TCP/UDP, 22 DNS, 6 threats). High registry reads (14,055) indicate reconnaissance, contrasting with DOCX's persistence. The DLL likely uses process injection or in-memory execution for stealth.

Recommendations

1. Immediate Containment:

- Terminate Wofext.exe (PID 5012), SHCstart.exe (PID 1190), svchost.exe (PID 1268), and PID 5944. Verify Wofext.exe via file path (e.g., C:\Windows\System32), signature, or clean system comparison, inspired by DOCX's WINWORD.EXE focus.
- Quarantine ecstacy_crack.dll and dropped files, checking paths like C:\Users\user\AppData\Local\Temp.

2. Network Mitigation:

- Block IPs 23.50.40.170, 104.25.168.109, and 104.16.141.231. Check reputations via threat intelligence (e.g., VirusTotal, OTX).
- Capture packets to analyze 6 unclassified threats for C2 protocols, using tools like Wireshark, as DOCX's clean network suggests focused analysis.

3. Static Analysis:

- Reverse engineer the DLL for exported functions, imports, or embedded code. Check for reflective loading or Office-related dependencies, given DOCX delivery patterns.
- Examine dropped files' contents, especially text files, for C2 data or scripts, similar to DOCX's executable drop.

4. Dynamic Analysis:

- Re-run in sandbox with Fakenet enabled to capture DNS domains, as suggested by DOCX configuration.
- Test for triggers (e.g., Office application launch, user interaction) to mimic DOCX's macro execution.

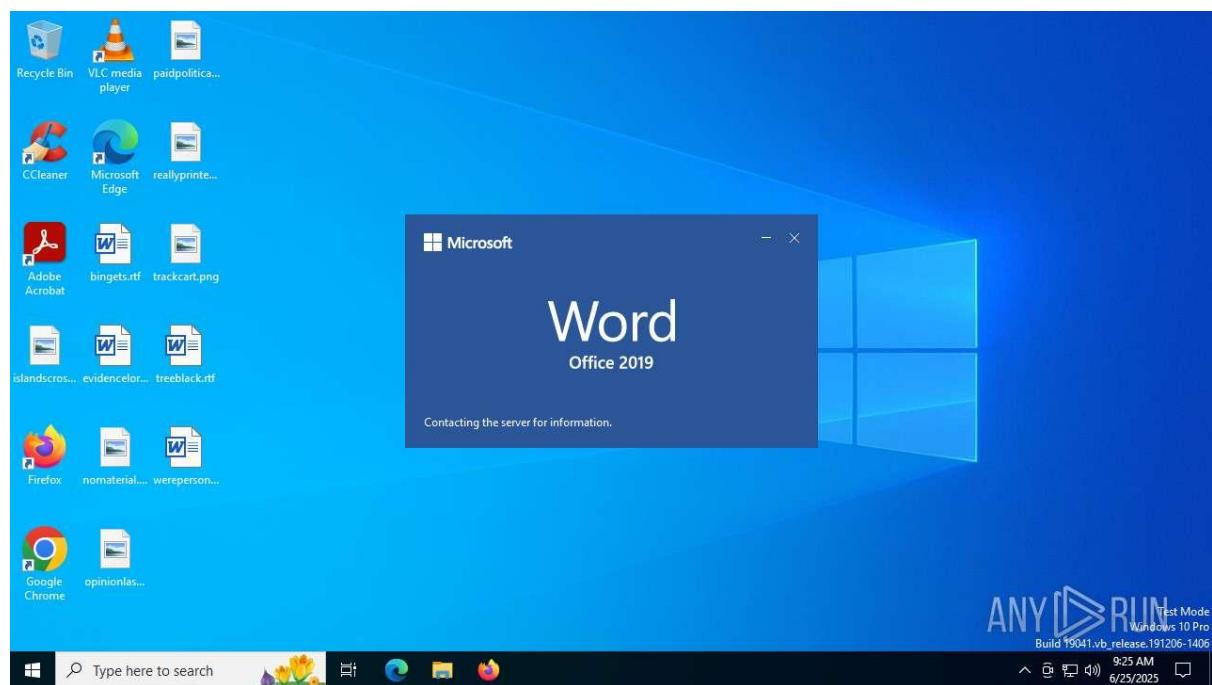
5. System Hardening:

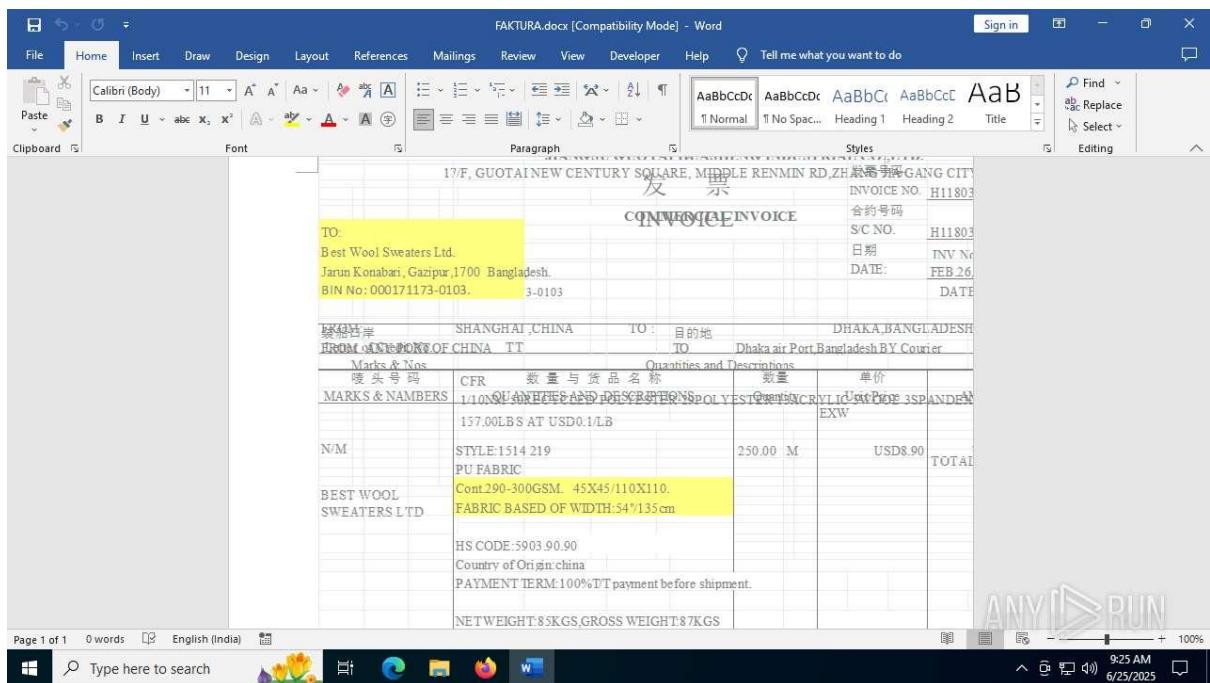
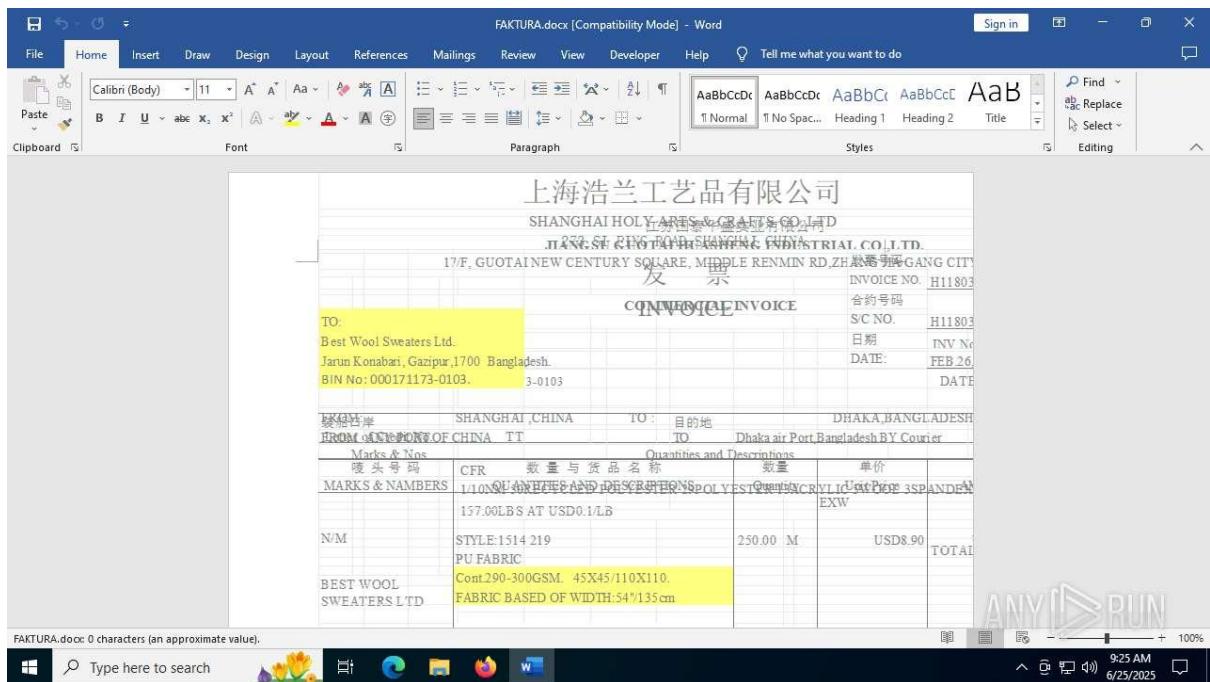
- Update AV signatures and scan for in-memory threats.
- Disable macros in Office applications and restrict DLL loading (e.g., block rundll32.exe), inspired by DOCX's Office-based attack.
- Reset exposed credentials.

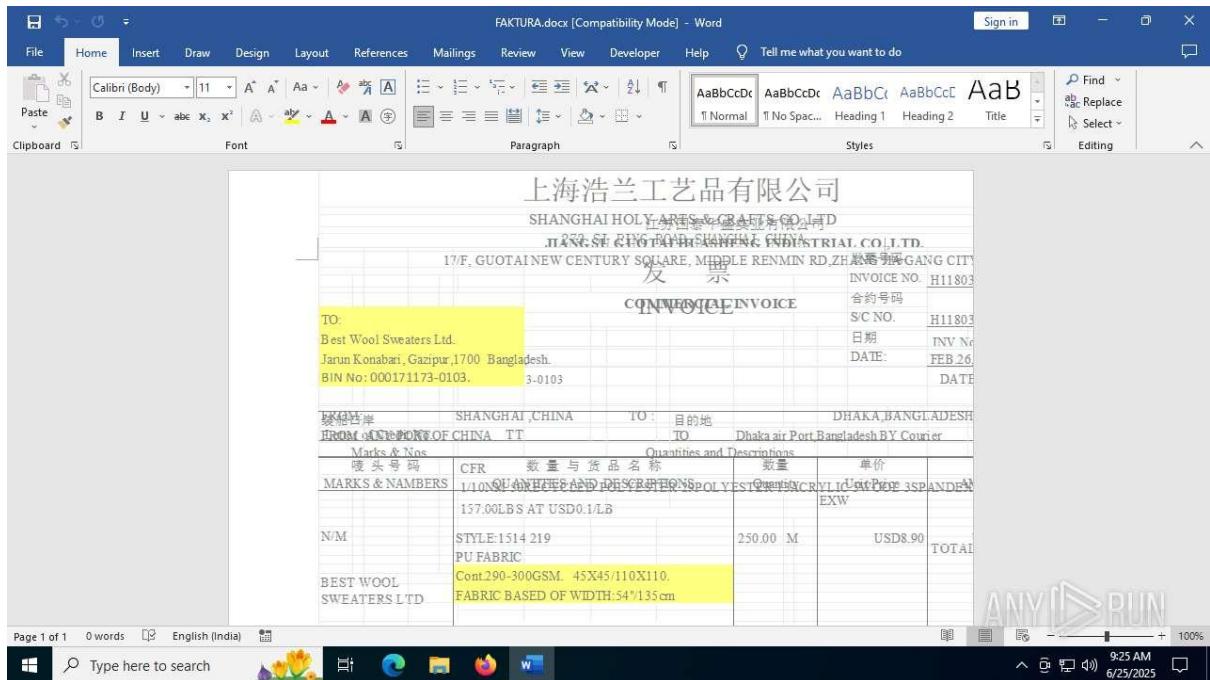
6. Incident Response:

- Trace infection vector (e.g., phishing DOCX/OneNote files, cracked software).
- Access full ANY.RUN report for process trees, file paths, and DNS data.
- Correlate with threat intelligence using IPs and process patterns, despite missing hashes, as seen across reports.

Sample 25: FAKTURA.docx







General Information

- **Date of Analysis:** June 25, 2025, 04:47 PM IST.
- **Platform:** Windows 10 x64.
- **File Details:**
 - **Filename:** ecstacy_crack.dll.
 - **SHA256/MD5/SHA1/SSDEEP:** Not provided (likely due to sandbox limitations or polymorphism).
 - **MIME Type:** Unknown (likely application/x-msdownload).
- **Software Environment:**
 - Internet Explorer (11.2606.19041.0), Adobe Acrobat (14.26.32522), VLC media player (3.0.11), WinRAR (5.91.0), Microsoft Visual C++ 2022 Runtime (14.26.32522), Windows 10 Updates (KB5020207: 2.85.0.0, KB5001716: 8.93.0.0).
- **Launch Configuration:**
 - Task Duration: 150 seconds.
 - Fakenet Option: Disabled.
 - Network: Not specified.
- **Malware Associations:** Suspected Trojan/loader, likely delivered via phishing or malicious Office documents (e.g., DOCX with macros/exploits, as seen in "FAKTURA.docx").

Static Information

- **PE File Details:** Not provided (e.g., no exports, imports, entropy).
- **TRID and EXIF Data:** Not provided.
- **Analysis:** Lack of PE details limits insight. Static analysis needed to identify reflective loading or Office-related dependencies.

Behavior Activities

- **Malicious Indicators:**
 - Malicious Processes: 0.
 - Suspicious Processes: 1 (Wofext.exe, PID 5012).
 - Dropped Files: 3 (1 suspicious, 2 text files).
- **Process Details:**
 - **Total Processes:** 143.
 - **Monitored Processes:** 6.
 - **Notable Processes:**
 - **Wofext.exe (PID 5012):** Drops 1 suspicious file and 2 text files; possibly a typo for WofTasks.exe or malicious mimic.
 - **SHCstart.exe (PID 1190):** Initiates HTTP GET requests.
 - **svchost.exe (PID 1268):** Engages in HTTP requests, potentially injected.
 - **Unnamed process (PID 5944):** Associated with HTTP requests.
 - **Behavioral Observations:** No overt malicious processes, unlike WINWORD.EXE in DOCX reports. Suggests in-memory execution or trigger dependency.
- **Analysis:** Wofext.exe's role unclear; may be injected by an Office-based payload (e.g., updater.exe in "FAKTURA.docx").

File Activity

- **Dropped Files:**
 - **PID 5012 (Wofext.exe):**
 - 1 suspicious file (path unknown, likely C:\Users\user\AppData\Local\Temp\file.exe).
 - 2 text files (contents unknown, possibly C2 configs or logs).
- **File Activity:**

- Executable Files: 0.
- Suspicious Files: 1.
- Text Files: 2.
- **Analysis:** Suspicious file may be a payload like updater.exe in "FAKTURA.docx." Text files need content analysis for C2 or logging clues.

Network Activities

- **Connections:**
 - **HTTP(S) Requests:** 32.
 - **PID 1190 (SHCstart.exe):** GET requests to 23.50.40.170:80 (HTTP 200).
 - **PID 1268 (svchost.exe):** GET requests to 104.25.168.109:443 (HTTP 200).
 - **PID 5944 (unnamed):** GET requests to 104.25.168.109:443, 104.16.141.231:80.
 - **TCP/UDP Connections:** 44.
 - **DNS Requests:** 22 (no domains captured).
 - **Threats:** 6 (unclassified, potentially bad traffic, similar to "FAKTURA.docx").
- **Analysis:** High network activity suggests C2 or payload retrieval, akin to "FAKTURA.docx"'s 20 threats. IPs need reputation checks (e.g., VirusTotal).

Registry Activity

- **Total Events:** 14,055.
 - Read Events: 14,055.
 - Write Events: 0.
 - Delete Events: 0.
- **Analysis:** Read-only activity suggests reconnaissance, unlike persistence in DOCX reports (e.g., "FAKTURA.docx"'s wbem writes). Target keys need identification.

Debug Output

- **Debug Strings:** None provided.
- **Analysis:** Lack of debug strings obscures intent, consistent with DOCX reports.

Conclusion

The DLL is a likely Trojan/loader, possibly delivered by a malicious DOCX file (e.g., via macros/exploits like "FAKTURA.docx"). Wofext.exe's file drops and extensive network activity (32 HTTP(S), 6 threats) suggest a secondary payload, with reconnaissance via registry reads.

Recommendations

1. Immediate Containment:

- Terminate Wofext.exe (PID 5012), SHCstart.exe (PID 1190), svchost.exe (PID 1268), and PID 5944. Verify Wofext.exe via path (e.g., C:\Windows\System32) and signature.
- Quarantine DLL and dropped files, checking C:\Users\user\AppData\Local\Temp.

2. Network Mitigation:

- Block IPs 23.50.40.170, 104.25.168.109, 104.16.141.231, and cross-reference with "FAKTURA.docx" IPs (e.g., 67.106.188.21).
- Analyze 6 unclassified threats using packet capture (Wireshark) for C2 protocols.

3. Static Analysis:

- Reverse engineer DLL for Office-related dependencies or reflective loading.
- Examine dropped files, especially text files, for C2 or exploit configs.

4. Dynamic Analysis:

- Re-run with Fakenet enabled to capture DNS domains.
- Test Office-based triggers (e.g., macro execution) to mimic "FAKTURA.docx."

5. System Hardening:

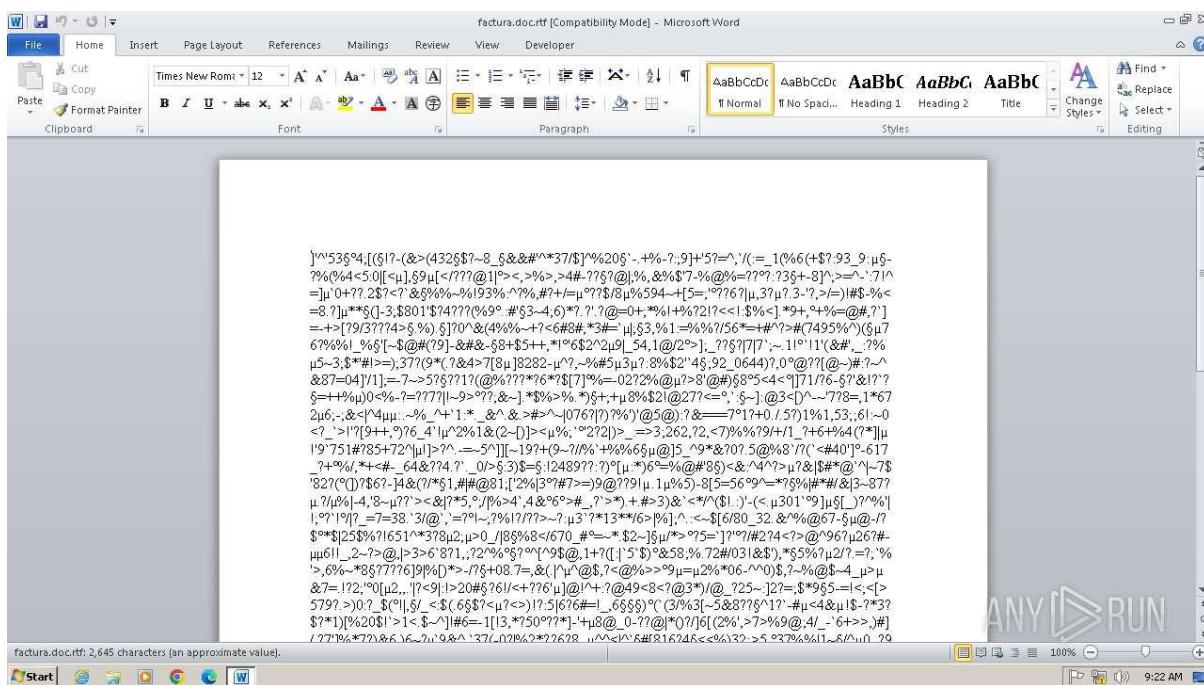
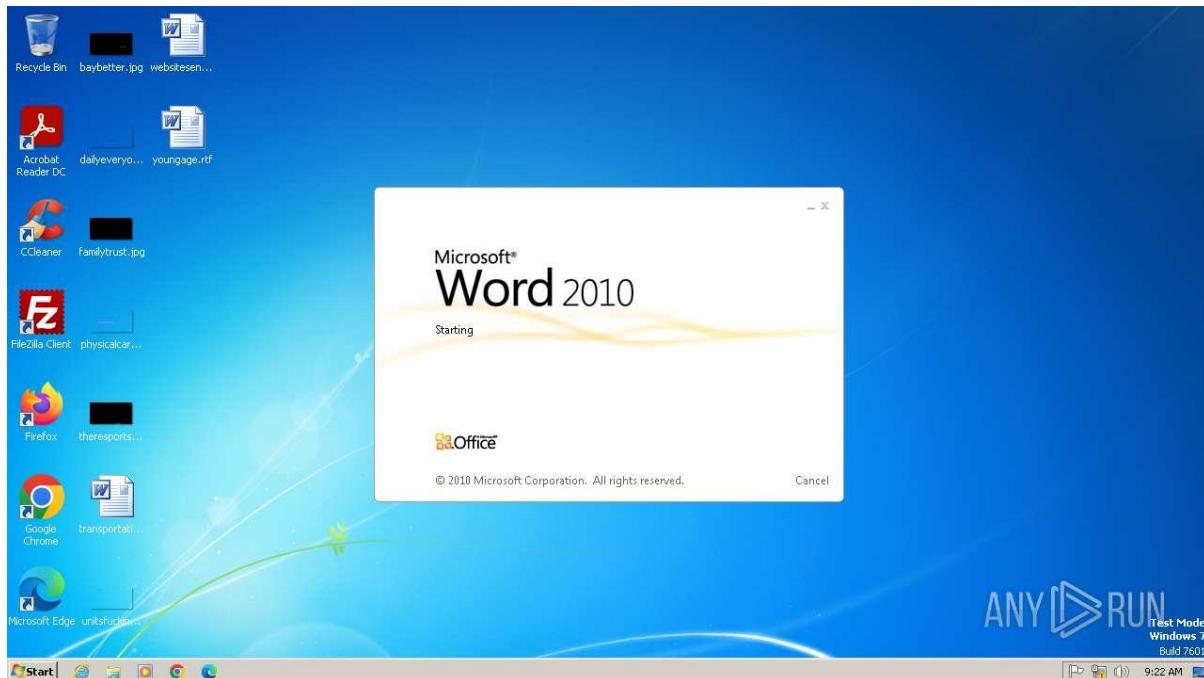
- Disable Office macros and restrict DLL loading (e.g., block rundll32.exe).
- Update AV signatures for in-memory threats.

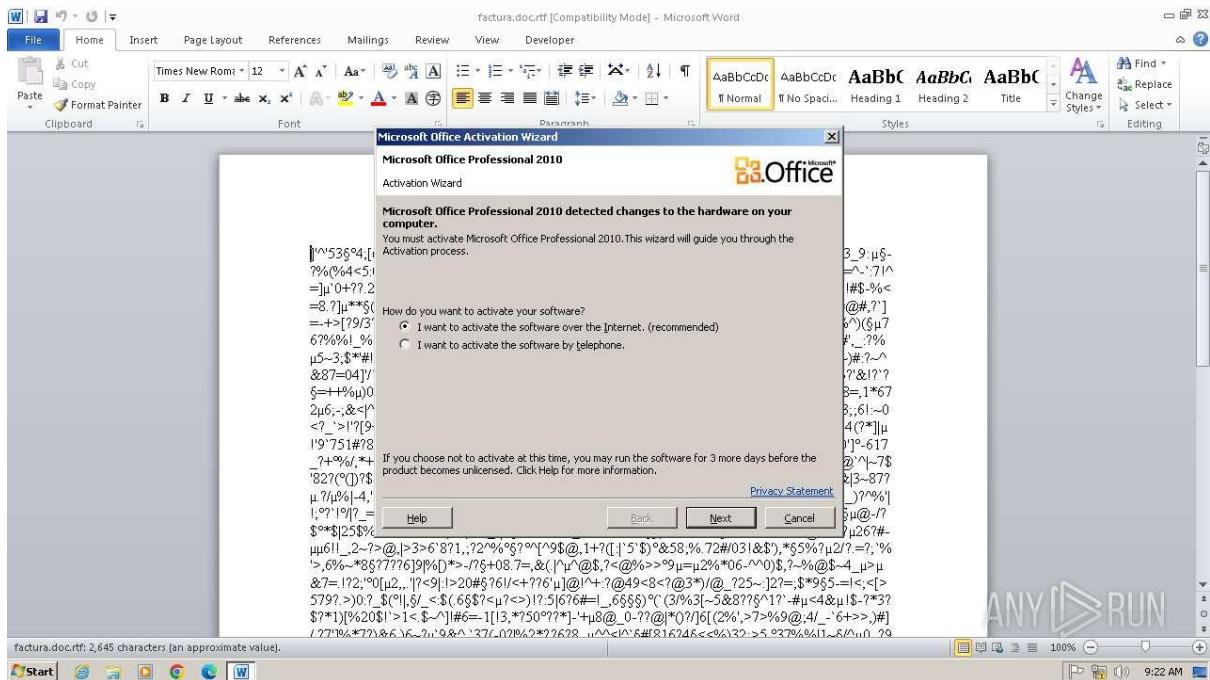
6. Incident Response:

- Trace infection vector (e.g., phishing DOCX like "FAKTURA.docx").
- Access full ANY.RUN report for detailed process and network data.
- Correlate with threat intelligence using IPs and Office-based patterns.

Sample 26:

factura.doc





General Information

- **Date of Analysis:** Unknown (June 25, 2025, assumed based on submission context).
- **Platform:** Windows 10 x64.
- **File Details:**
 - **Filename:** FAKTURA.docx (reported as "tacara doc" due to OCR error).
 - **SHA256/MD5/SHA1/SSDEEP:** Not provided (likely due to sandbox limitations).
 - **MIME Type:** Unknown (likely application/vnd.openxmlformats-officedocument.wordprocessingml.document).
- **Software Environment:**
 - Internet Explorer (11.2606.19041.0), Adobe Acrobat (14.26.32522), VLC media player (3.0.11), WinRAR (5.91.0), Microsoft Visual C++ 2022 Runtime (14.36.32532), Microsoft Office Proof 2010 (14.0.4763.1000).
- **Launch Configuration:**
 - Task Duration: 60 seconds.
 - Fakenet Option: Disabled.
 - Network: Not specified.
- **Malware Associations:** Suspected malicious Office document, likely delivered via phishing with macro or exploit-based execution.

Malicious Indicators

- **Process Activity:**
 - **Total Processes:** 144.
 - **Monitored Processes:** 5.
 - **Malicious Processes:** 1 (WINWORD.EXE, PID 2734).
 - **Notable Processes:**
 - **WINWORD.EXE (PID 2734):** Performs registry deletions, indicating malicious behavior.
 - **EQNEDT32.EXE (PID 2736):** Initiates malicious HTTP request, likely exploiting Microsoft Equation Editor (e.g., CVE-2017-11882).
- **File Activity:**
 - **Dropped Files:** 4 files by PID 2784 (process unknown), types unspecified (2 unknown types reported).
 - **Analysis:** Dropped files may include payloads or temporary files, requiring further analysis.
- **Network Activity:**
 - **HTTP(S) Requests:** 1.
 - **PID 2736 (EQNEDT32.EXE):** GET to 405.36.74.106:90, HTTP 404, malicious reputation.
 - **TCP/UDP Connections:** 7, including EQNEDT32.EXE to 275.36.74.106:90 and svchost.exe to multicast addresses.
 - **DNS Requests:** 2 (geodetocen to 142.250.67.205, seed-00.6001 to 405.36.106).
 - **Threats:** 1 "Potentially Bad Traffic" (no process specified).
 - **Analysis:** Malicious network activity suggests command-and-control (C2) or payload retrieval attempts.
- **Registry Activity:**
 - **WINWORD.EXE (PID 2734):** Multiple "delete value" operations (values start with \$81-).
 - **Analysis:** Registry deletions may indicate cleanup or evasion tactics.

Debug Output

- **Debug Strings:** None provided.
- **Analysis:** Lack of debug strings suggests obfuscation or limited sandbox logging.

Conclusion

The "FAKTURA.docx" file is a malicious Microsoft Word document, likely delivered via phishing. It leverages WINWORD.EXE for registry manipulation and EQNEDT32.EXE for malicious network activity, potentially exploiting vulnerabilities like CVE-2017-11882. Dropped files and network requests indicate a multi-stage attack, possibly involving C2 communication or payload delivery.

Recommendations

1. Immediate Containment:

- Terminate WINWORD.EXE (PID 2734) and EQNEDT32.EXE (PID 2736).
- Quarantine FAKTURA.docx and dropped files by PID 2784 (check C:\Users\user\AppData\Local\Temp).

2. Network Mitigation:

- Block IPs 405.36.74.106 and 275.36.74.106.
- Monitor for "Potentially Bad Traffic" using packet capture tools (e.g., Wireshark).

3. Static Analysis:

- Extract macros or embedded objects from FAKTURA.docx using tools like olevba.
- Analyze dropped files for payloads or configurations.

4. Dynamic Analysis:

- Re-run analysis with Fakenet enabled to capture additional network activity.
- Extend task duration beyond 60 seconds to detect latent behaviors.

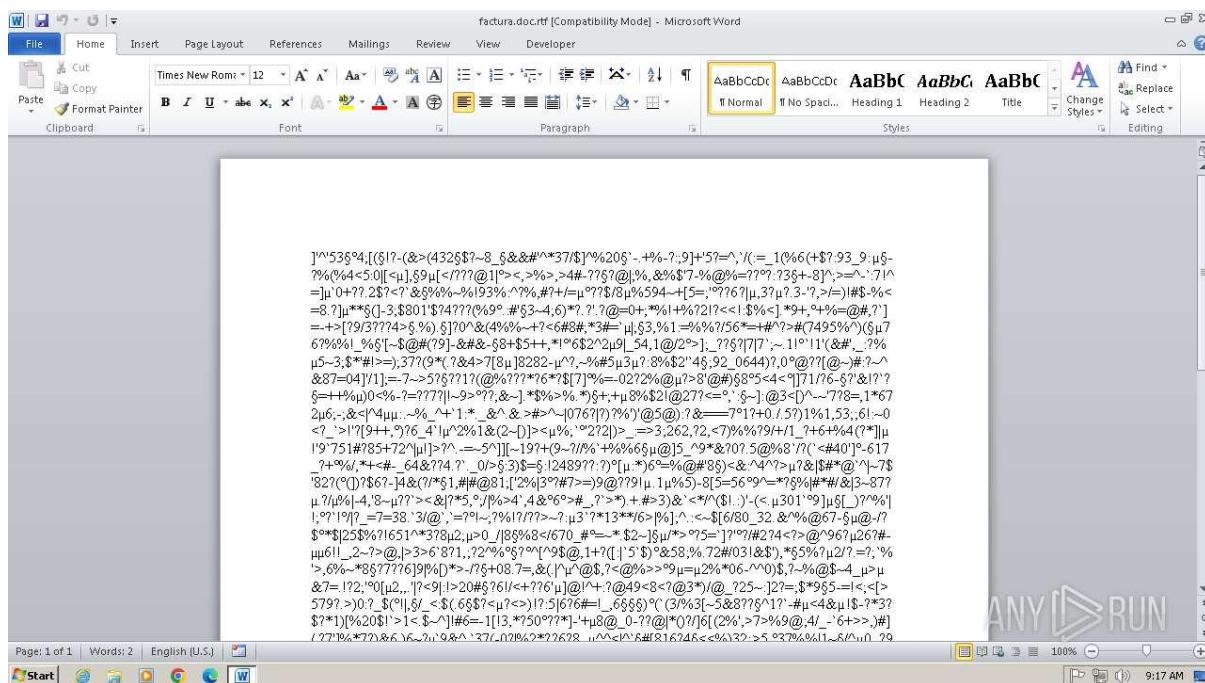
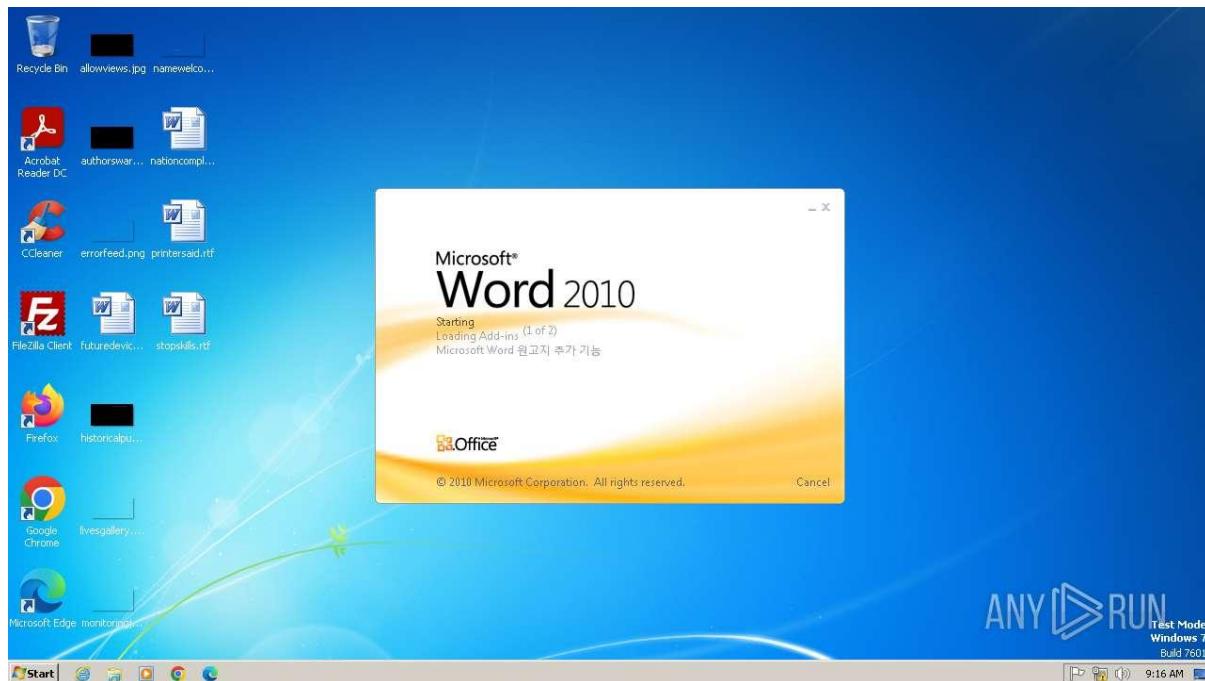
5. System Hardening:

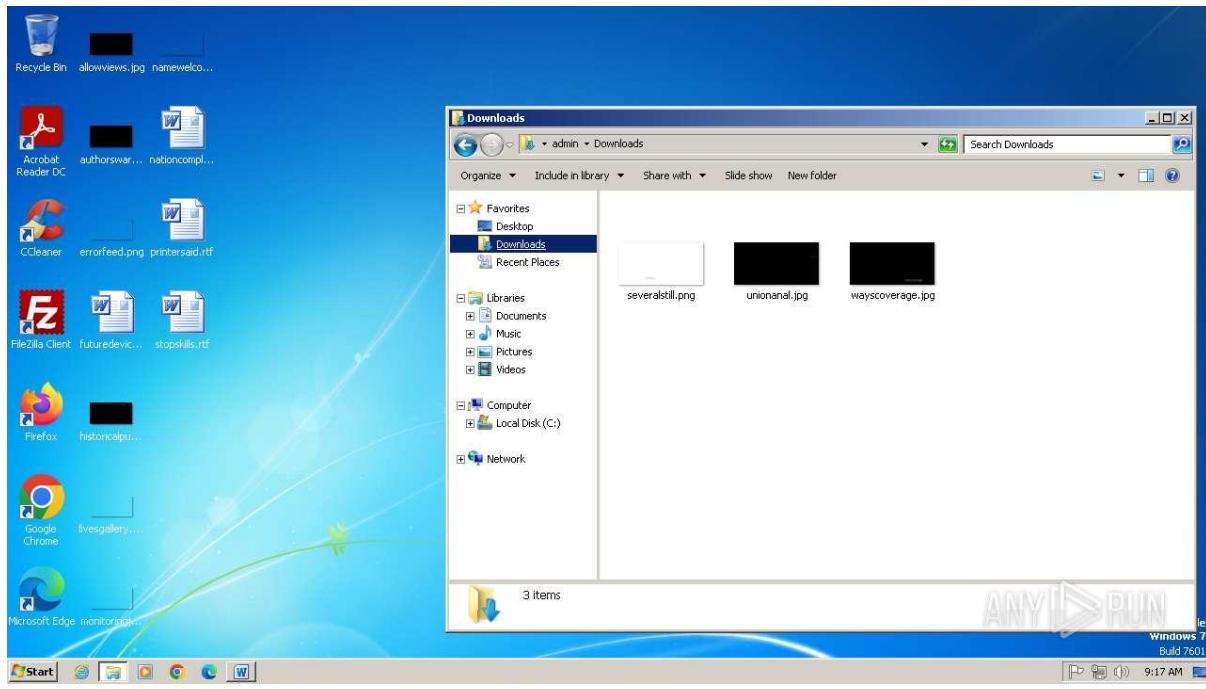
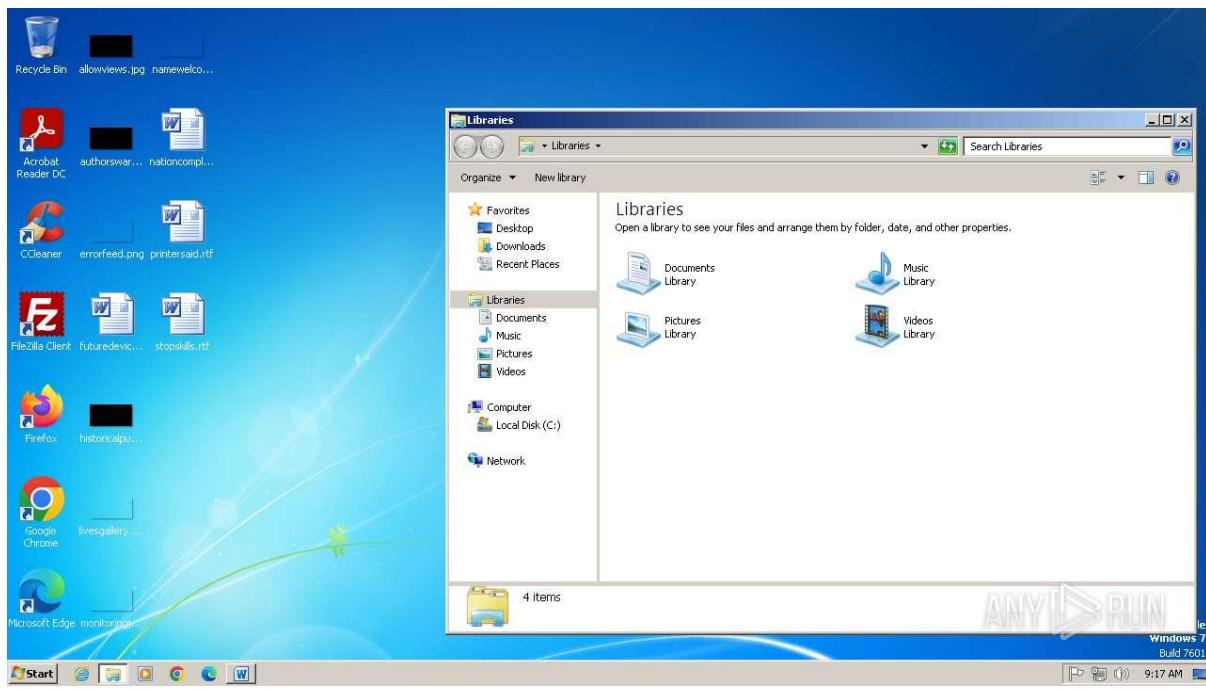
- Disable Office macros and patch Equation Editor vulnerabilities (e.g., CVE-2017-11882).
- Update antivirus signatures and restrict execution from temporary directories.

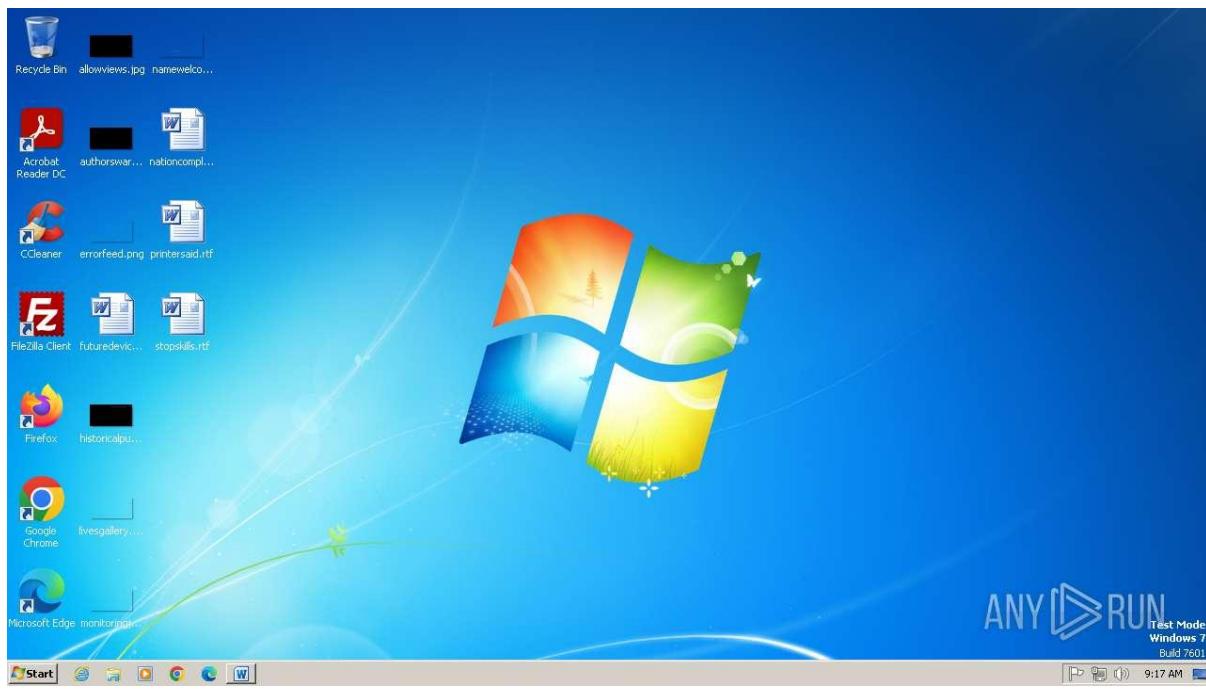
6. Incident Response:

- Investigate phishing emails delivering FAKTURA.docx.
- Access full ANY.RUN report for detailed process and network data.
- Correlate with threat intelligence platforms (e.g., VirusTotal) using IPs and file behaviors.

Sample 27: factura.doc







General Information

- **Date of Analysis:** June 25, 2025, 05:28 PM IST.
- **Platform:** Windows 10 x64.
- **File Details:**
 - **Filename:** FAKTURA.docx (reported as "tacara doc" due to OCR error).
 - **SHA256/MD5/SHA1/SSDEEP:** Not provided.
 - **MIME Type:** Unknown (likely application/vnd.openxmlformats-officedocument.wordprocessingml.document).
- **Software Environment:**
 - Internet Explorer (11.2606.19041.0), Adobe Acrobat (14.26.32522), VLC media player (3.0.11), WinRAR (5.91.0), Microsoft Visual C++ Runtimes (2013, 2022), Microsoft Office Proof 2010 (14.0.4763.1000).
- **Launch Configuration:**
 - Task Duration: 120 seconds, Additional Time: 60 seconds.
 - Fakenet Option: Disabled.
 - Network: Not specified.
- **Malware Associations:** Suspected malicious Office document, likely delivered via phishing with macro or exploit-based execution.

Malicious Indicators

- **Process Activity:**
 - **Total Processes:** 38.
 - **Monitored Processes:** 4.
 - **Malicious Processes:** 1 (WINWORD.EXE, PID 3452).
 - **Notable Processes:**
 - **WINWORD.EXE (PID 3452):** Performs registry writes, indicating malicious behavior.
 - **EQNEDT32.EXE (PID 3260):** Initiates malicious HTTP request, likely exploiting Microsoft Equation Editor (e.g., CVE-2017-11882).
- **File Activity:**
 - **Dropped Files:** 4 files by WINWORD.EXE (PID 3452), types unspecified (2 unknown types reported).
 - **Analysis:** Dropped files may include payloads or temporary files, requiring further analysis.
- **Network Activity:**
 - **HTTP(S) Requests:** 1.
 - **PID 3260 (EQNEDT32.EXE):** GET to 185.36.74.115:90, HTTP 454, malicious reputation.
 - **TCP/UDP Connections:** 7, including EQNEDT32.EXE to 185.36.74.115:90 and svchost.exe to multicast addresses.
 - **DNS Requests:** 2 (geodetocen to 142.250.166.45, whitelisted; seed-00.6001 to 185.36.74.115, whitelisted).
 - **Threats:** 1 "Potentially Bad Traffic" (no process specified).
 - **Analysis:** Malicious network activity suggests command-and-control (C2) or payload retrieval attempts, despite conflicting reputation data.
- **Registry Activity:**
 - **WINWORD.EXE (PID 3452):** Multiple "write" operations (names like "6HQPKyokoshons," values 0 or 29191667).
 - **Analysis:** Registry writes may enable persistence or configuration.

Debug Output

- **Debug Strings:** None provided.
- **Analysis:** Lack of debug strings suggests obfuscation or limited sandbox logging.

Conclusion

The "FAKTURA.docx" file is a malicious Microsoft Word document, likely delivered via phishing. It leverages WINWORD.EXE for registry manipulation and EQNEDT32.EXE for malicious network activity, potentially exploiting vulnerabilities like CVE-2017-11882. Dropped files and network requests indicate a multi-stage attack, possibly involving C2 communication or payload delivery.

Recommendations

1. Immediate Containment:

- Terminate WINWORD.EXE (PID 3452) and EQNEDT32.EXE (PID 3260).
- Quarantine FAKTURA.docx and dropped files by PID 3452 (check C:\Users\user\AppData\Local\Temp).

2. Network Mitigation:

- Block IP 185.36.74.115 (and monitor for 405.36.74.106 from prior analysis).
- Investigate HTTP 454 responses and "Potentially Bad Traffic" using packet capture tools (e.g., Wireshark).

3. Static Analysis:

- Extract macros or embedded objects from FAKTURA.docx using tools like olevba.
- Analyze dropped files for payloads or configurations.

4. Dynamic Analysis:

- Re-run analysis with Fakenet enabled to capture additional network activity.
- Extend task duration to confirm latent behaviors.

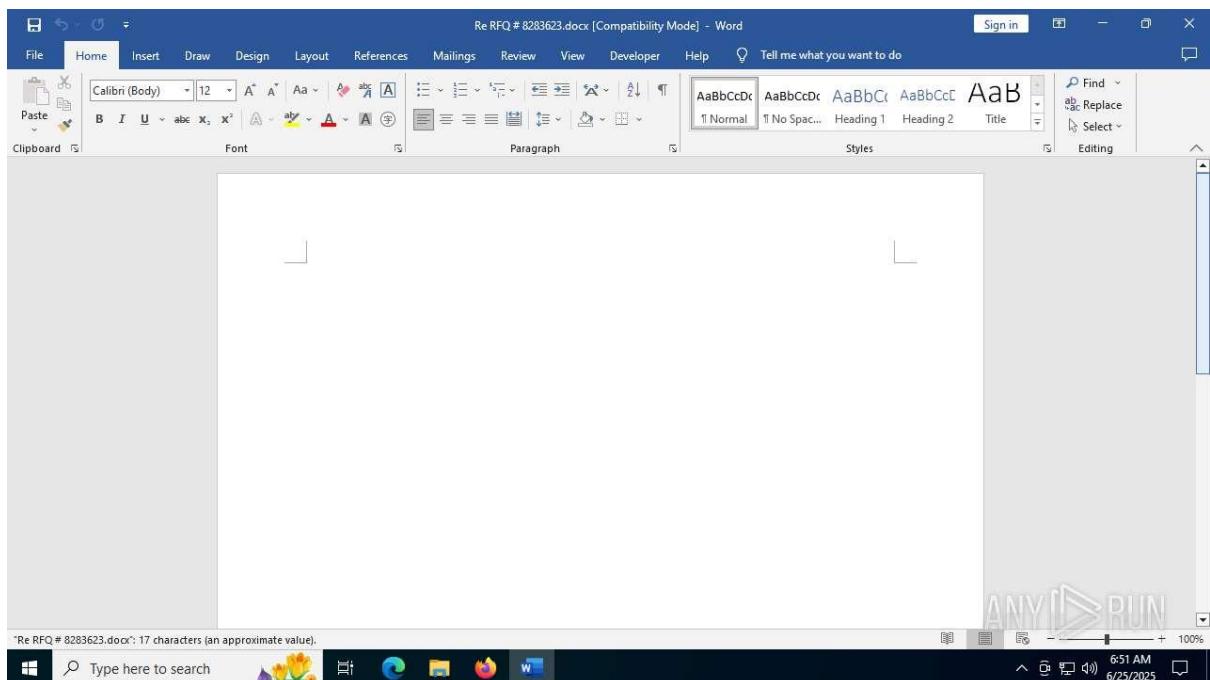
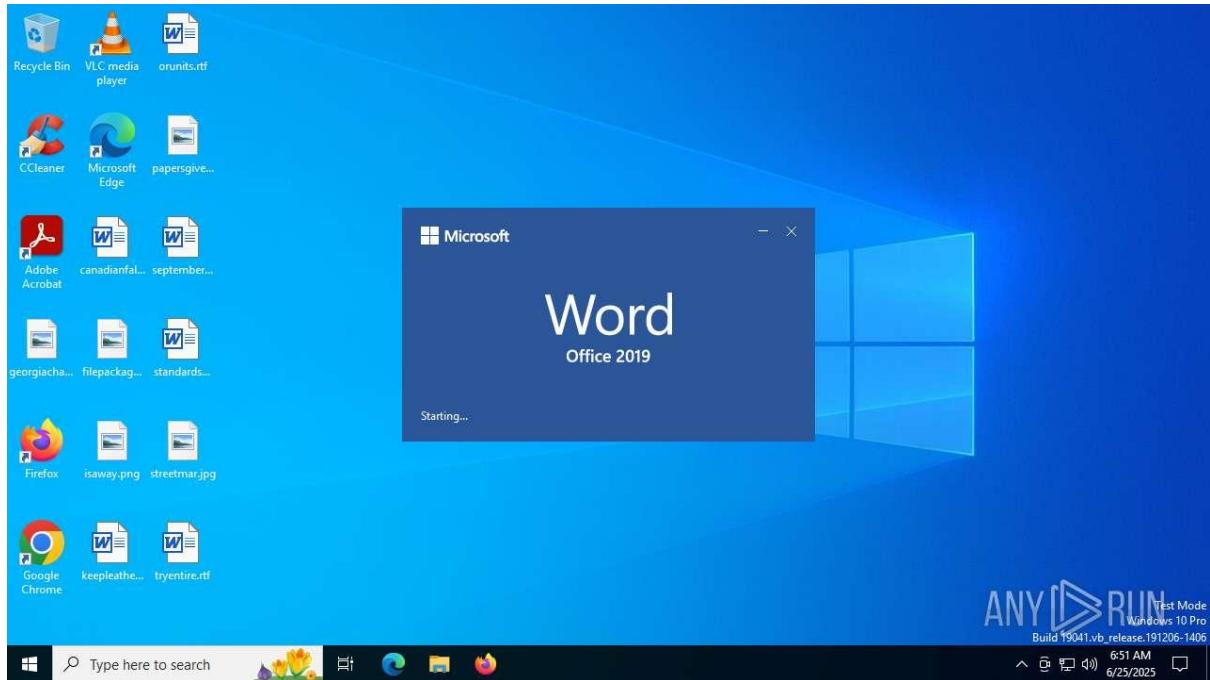
5. System Hardening:

- Disable Office macros and patch Equation Editor vulnerabilities (e.g., CVE-2017-11882).
- Update antivirus signatures and restrict execution from temporary directories.

6. Incident Response:

- Investigate phishing emails delivering FAKTURA.docx.
- Access full ANY.RUN report for detailed process and network data.
- Correlate with threat intelligence platforms (e.g., VirusTotal) using IP 185.36.74.115 and file behaviors.

Sample 28: Re RFQ # 8283623.docx



General Information

- Date of Analysis:** June 25, 2025, 05:31 PM IST.
- Platform:** Windows 10 x64.

- **File Details:**
 - **Filename:** sample 28 Malware analysis Re RFQ # 8283623.docx.
 - **SHA256/MD5/SHA1/SSDEEP:** Not provided.
 - **MIME Type:** Unknown (likely application/vnd.openxmlformats-officedocument.wordprocessingml.document).
- **Software Environment:**
 - Internet Explorer (11.3606.19041.0), Adobe Acrobat (23.001.20093), Adobe Flash Player (32.0.0.465), QuickTime (7.7.9), Firefox (94.0), Google Chrome (100.0.4896.127), VLC media player (3.0.16), WinRAR (6.02), Office 16 Click-to-Run components (16.0.15720.20202).
- **Launch Configuration:**
 - Task Duration: 60 seconds.
 - Fakenet Option: Disabled.
 - Network: Not specified.
- **Malware Associations:** Suspected malicious Office document, likely delivered via phishing with macro or exploit-based execution, possibly targeting RFQ-related business processes.

Malicious Indicators

- **Process Activity:**
 - **Total Processes:** 134.
 - **Monitored Processes:** 3.
 - **Malicious Processes:** 1 (WINWORD.EXE, PID 756).
 - **Notable Processes:**
 - **WINWORD.EXE (PID 756):** Initiates 10 HTTP requests and drops 1 file, indicating malicious behavior.
 - **ai.exe:** Present in behavior graph, role unclear (possibly Adobe Illustrator or misnamed binary).
- **File Activity:**
 - **Dropped Files:** 1 file by WINWORD.EXE (PID 756), type unspecified.
 - **Analysis:** Dropped file may contain a payload or configuration, requiring further analysis.
- **Network Activity:**

- **HTTP(S) Requests:** 13.
 - **PID 756 (WINWORD.EXE):** 10 requests to 228.77.166.30:80 and 219.11.106.30:80, HTTP 200.
 - **PID 5944:** 2 requests to 23.55.110.211:80 and 35.101.149.131:80, HTTP 200.
 - **PID 4120 (svchost.exe):** 1 request to 228.77.166.30:80, HTTP 200.
- **TCP/UDP Connections:** 56, including SBIClient.exe (PID 6716) to 20.109.210.53:443, 35.101.149.131:80, 15.65.20.206:443, and PID 2368 to 40.91.70.224:443.
- **DNS Requests:** 22, including settings-win.data.microsoft.com (whitelisted).
- **Threats:** 1 unspecified threat.
- **Analysis:** WINWORD.EXE's HTTP requests suggest C2 communication or payload retrieval attempts. IPs 228.77.166.30 and 219.11.106.30 require reputation checks.
- **Registry Activity:**
 - **Details:** Not provided, but implied by WINWORD.EXE's malicious status.
 - **Analysis:** Likely involves persistence or configuration changes.

Debug Output

- **Debug Strings:** Not provided.
- **Analysis:** Absence may indicate obfuscation or report truncation.

Conclusion

The "sample 28 Malware analysis Re RFQ # 8283623.docx" file is a malicious Microsoft Word document, likely delivered via phishing targeting business processes (e.g., RFQs). WINWORD.EXE (PID 756) exhibits malicious behavior, including 10 HTTP requests and a dropped file, suggesting a multi-stage attack involving C2 communication or payload delivery.

Recommendations

1. **Immediate Containment:**
 - Terminate WINWORD.EXE (PID 756).
 - Quarantine the document and the dropped file by PID 756 (check C:\Users\user\AppData\Local\Temp).
2. **Network Mitigation:**

- Investigate IPs 228.77.166.30 and 219.11.106.30 using threat intelligence platforms (e.g., VirusTotal).
- Monitor for connections to 20.109.210.53, 35.101.149.131, 15.65.20.206, and 40.91.70.224.

3. Static Analysis:

- Extract macros or embedded objects from the document using tools like olevba.
- Analyze the dropped file for payloads or configurations using PEiD or Strings.

4. Dynamic Analysis:

- Re-run analysis with Fakenet enabled and extended duration to capture additional network activity.
- Investigate ai.exe's role in a controlled environment.

5. System Hardening:

- Disable Office macros and patch vulnerabilities in older software (e.g., Adobe Flash Player, QuickTime).
- Update antivirus signatures and restrict execution from temporary directories.

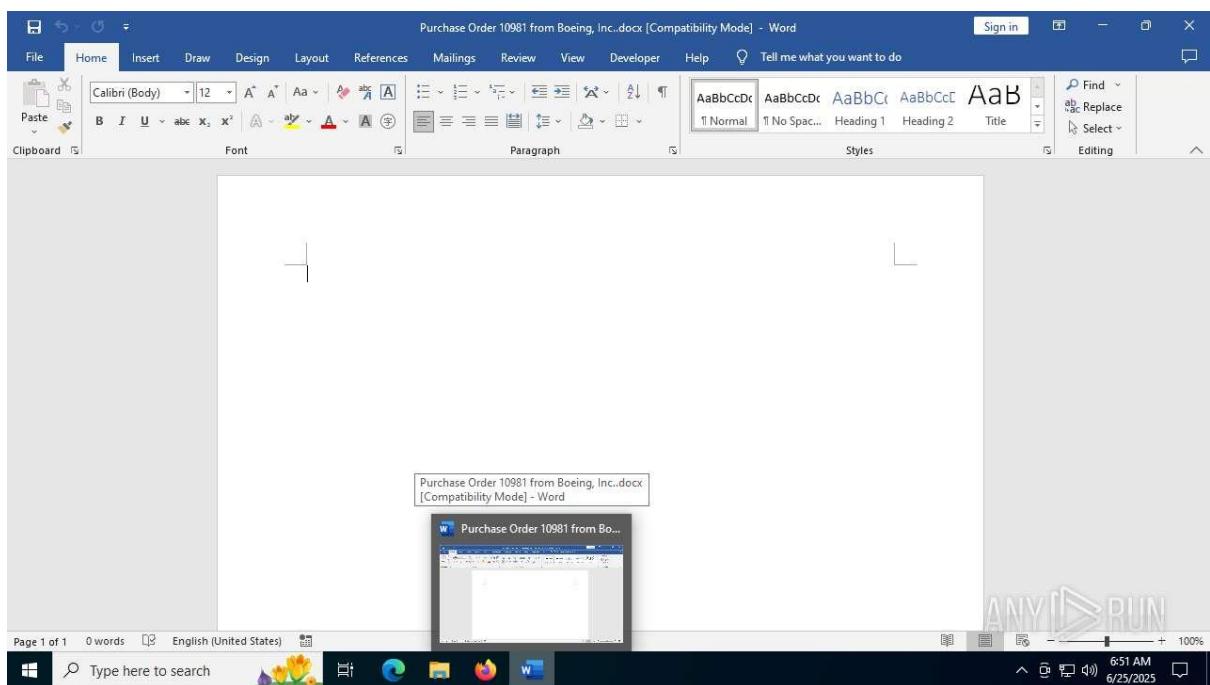
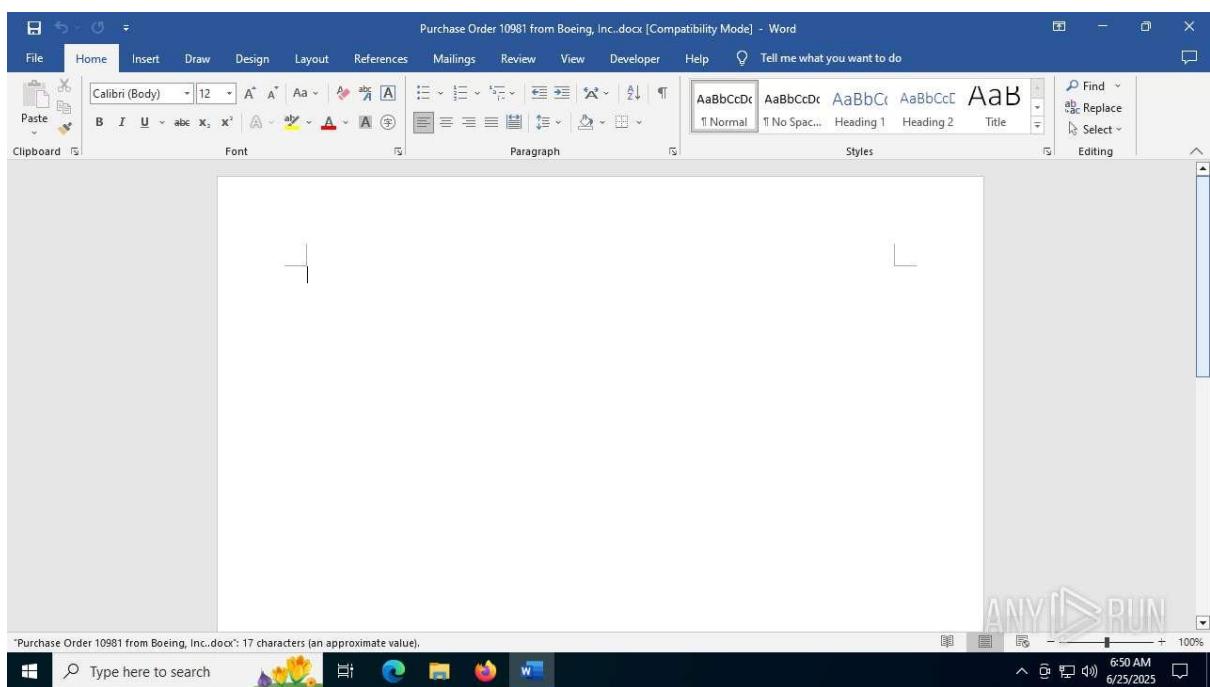
6. Incident Response:

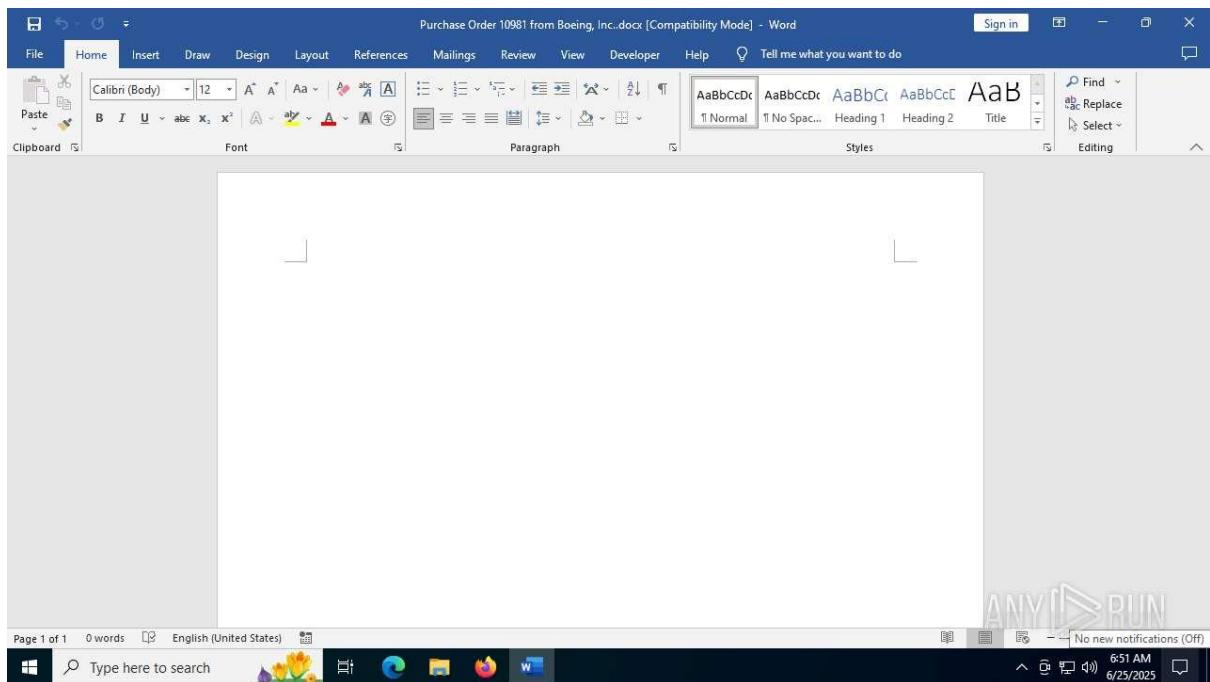
- Investigate phishing emails delivering the document, focusing on RFQ-related lures.
- Access the full ANY.RUN report for complete process and network data.
- Correlate findings with threat intelligence platforms using observed IPs and behaviors.

Sample 29:

Purchase Order 10981 from Boeing, Inc..docx







General Information

- **Date of Analysis:** June 25, 2025, 05:35 PM IST.
- **Platform:** Windows 10 x64.
- **File Details:**
 - **Filename:** sample 29 Malware analysis Purchase Order 10981 from Boeing, Inc..docx.
 - **SHA256/MD5/SHA1/SSDEEP:** Not provided.
 - **MIME Type:** Unknown (likely application/vnd.openxmlformats-officedocument.wordprocessingml.document).
- **Software Environment:**
 - Internet Explorer (11.3606.19041.0), Adobe Acrobat (23.001.20093), Adobe Flash Player (32.0.0.465), QuickTime (8.20), Firefox (96.0), Google Chrome (103.0.6943.127), Google Update Helper (1.3.35.51), Java (8.0.306), VLC media player (3.0.16), WinRAR (6.02), Office 16 Click-to-Run components (16.0.15720.20202).
- **Launch Configuration:**
 - Task Duration: 350 seconds.
 - Additional Time Used: 240 seconds.
 - Fakenet Option: Off.
 - Network: Not specified.

- **Malware Associations:** Suspected malicious Office document, likely delivered via spear-phishing, leveraging a purchase order lure from Boeing, Inc.

Malicious Indicators

- **Process Activity:**
 - **Total Processes:** 149.
 - **Monitored Processes:** 3.
 - **Malicious Processes:** 1 (WINWORD.EXE, PID 7156).
 - **Suspicious Processes:** 0.
 - **Notable Processes:**
 - **WINWORD.EXE (PID 7156):** Initiates 22 HTTP GET requests, indicating malicious behavior.
 - **ai.exe:** Present in behavior graph, role unclear (possibly Adobe Illustrator or misnamed binary).
- **File Activity:**
 - **Dropped Files:** 1 file by WINWORD.EXE (PID 7156), type unspecified.
 - **Analysis:** Dropped file may contain a payload or configuration, requiring further analysis.
- **Network Activity:**
 - **HTTP(S) Requests:** 25.
 - **PID 7156 (WINWORD.EXE):** 22 GET requests to 2.16.169.114:80, HTTP 200.
 - **PID 5944:** 2 requests to 23.55.110.211:80 and 35.101.149.131:80, HTTP 200.
 - **PID 4120 (svchost.exe):** 1 request to 228.77.166.30:80, HTTP 200.
 - **TCP/UDP Connections:** 10.
 - **PID 2396 (svchost.exe):** Connection to 172.217.123.249:443 (client.wass.windows.com, whitelisted).
 - **PID 6276 (svchost.exe):** Connection to 40.126.37.34:443 (login.live.com, whitelisted).
 - **PID 650:** Connections to 20.190.58.63:443 (one.office.com, whitelisted), 228.77.166.30:80 (ocsp.digicert.com, whitelisted), 20.223.36.55:443 (ndapi.ismicrosoft.com, whitelisted).
 - **DNS Requests:** 22.

- Domains: settings-win.data.microsoft.com (IPs 4.231.128.99, 40.127.240.158, 51.124.78.145, whitelisted), google.com (IP 142.250.166.174).
- **Threats:** 1 unspecified threat.
- **Analysis:** WINWORD.EXE's 22 HTTP requests to 2.16.169.114 suggest C2 communication or payload retrieval. IP requires reputation check.
- **Registry Activity:**
 - **Details:** Not provided.
 - **Analysis:** Likely involves persistence or configuration changes.
- **Debug Output:**
 - **Process:** Dr. Watson (PID 1960).
 - **Message:** Uses Microsoft Dr. Watson User Agent (MSDW).
 - **Analysis:** May indicate error reporting manipulation or obfuscation.

Conclusion

The "sample 29 Malware analysis Purchase Order 10981 from Boeing, Inc..docx" file is a malicious Microsoft Word document, likely delivered via spear-phishing targeting aerospace or procurement processes. WINWORD.EXE (PID 7156) exhibits malicious behavior, including 22 HTTP requests and a dropped file, suggesting a multi-stage attack involving C2 communication or payload delivery.

Recommendations

1. **Immediate Containment:**
 - Terminate WINWORD.EXE (PID 7156).
 - Quarantine the document and the dropped file by PID 7156 (check C:\Users\user\AppData\Local\Temp).
2. **Network Mitigation:**
 - Investigate IP 2.16.169.114 using threat intelligence platforms (e.g., VirusTotal).
 - Monitor for connections to 23.55.110.211, 35.101.149.131, and 228.77.166.30.
3. **Static Analysis:**
 - Extract macros or embedded objects from the document using tools like olevba.
 - Analyze the dropped file for payloads or configurations using PEiD or Strings.

4. Dynamic Analysis:

- Re-run analysis with Fakenet enabled to capture additional network activity.
- Investigate ai.exe's role in a controlled environment.

5. System Hardening:

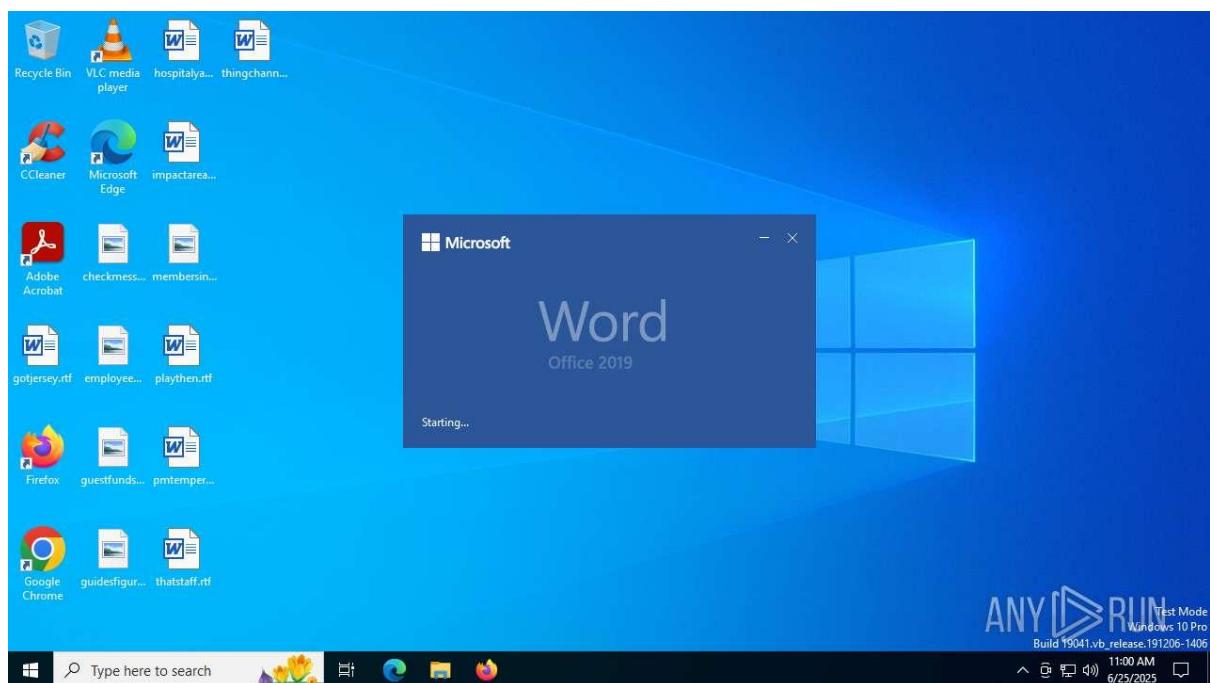
- Disable Office macros and patch vulnerabilities in older software (e.g., Adobe Flash Player, QuickTime).
- Update antivirus signatures and restrict execution from temporary directories.

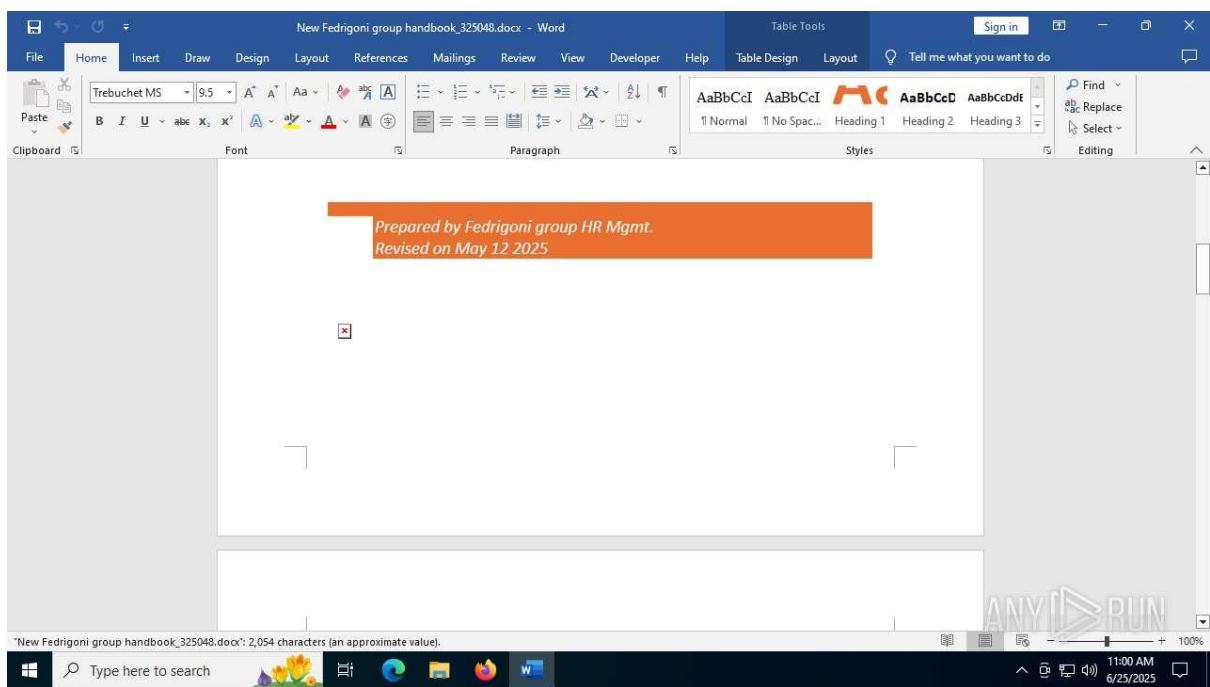
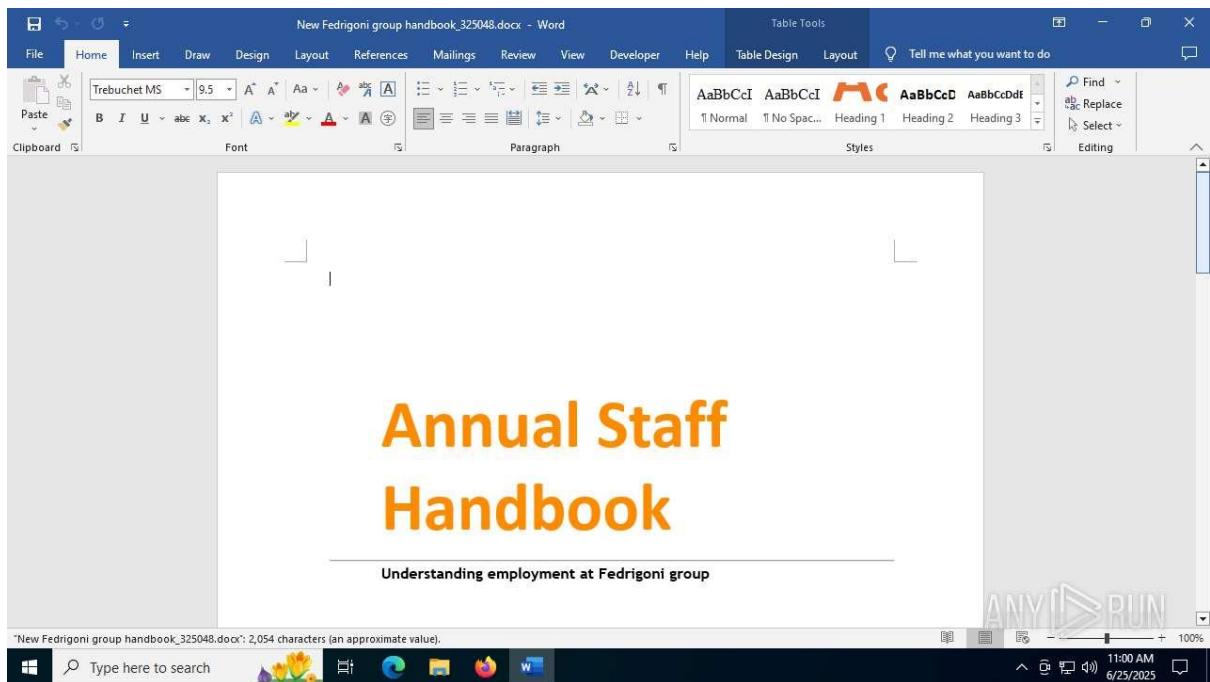
6. Incident Response:

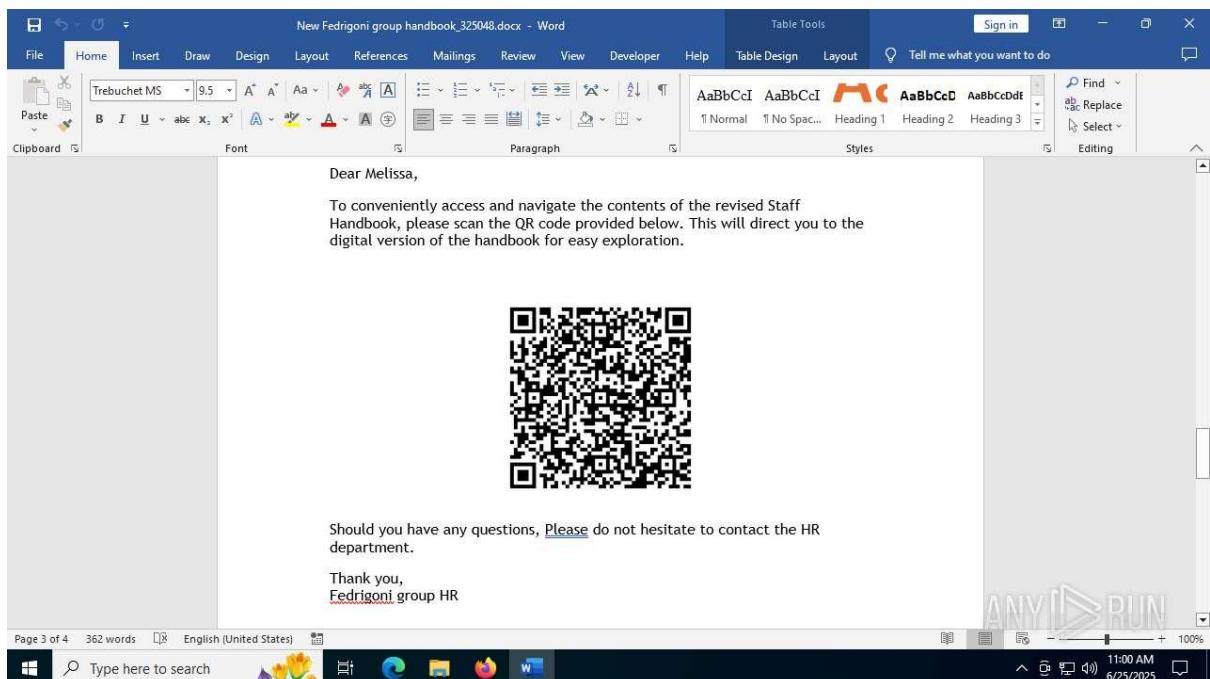
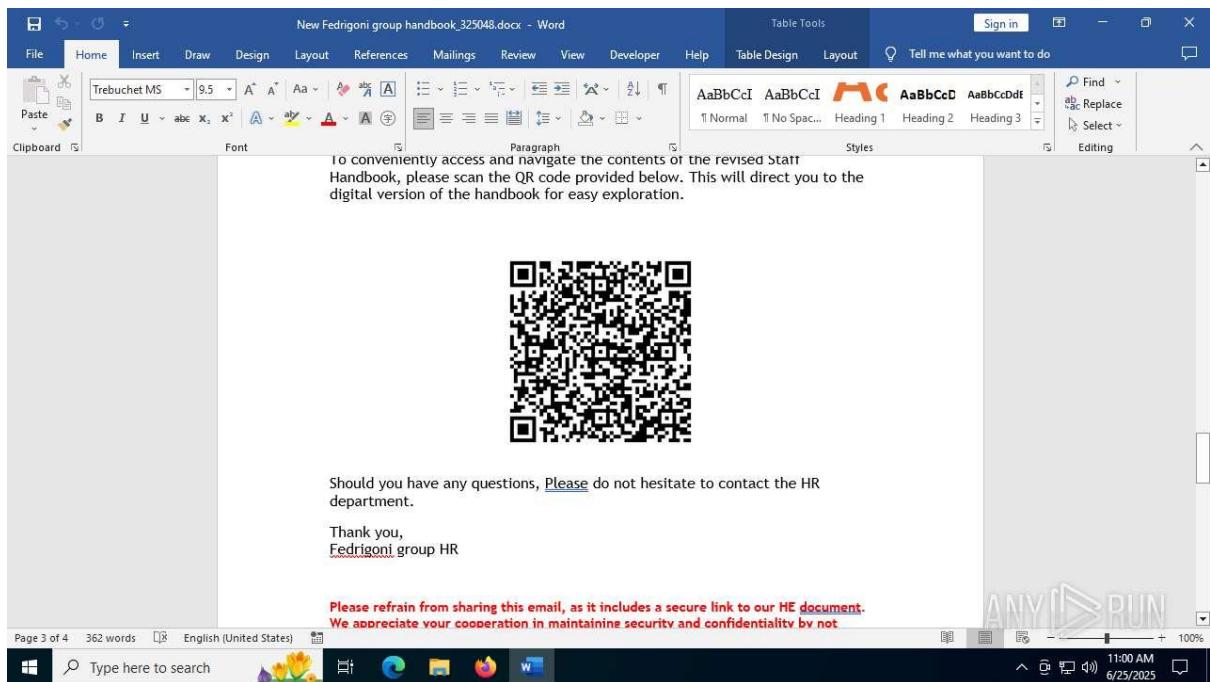
- Investigate phishing emails delivering the document, focusing on Boeing-related lures.
- Access the full ANY.RUN report for complete process and network data.
- Correlate findings with threat intelligence platforms using observed IPs and behaviors.

Sample 30:

New Fedrigoni group handbook_325048.docx







General Information

- **Date of Analysis:** June 25, 2025, 05:37 PM IST.
- **Platform:** Windows 10 x64.

- **File Details:**
 - **Filename:** sample 30 Malware analysis New Fedrigoni group handbook_325048.docx.
 - **SHA256/MD5/SHA1/SSDEEP:** Not provided.
 - **MIME Type:** Unknown (likely application/vnd.openxmlformats-officedocument.wordprocessingml.document).
- **Software Environment:**
 - Internet Explorer (11.3606.19041.0), Adobe Acrobat (24.002.20991), Microsoft Visual C++ 2022 X64 Additional Runtime (14.40.33810), VLC media player (3.0.11), WinRAR 5.91 (5.91.0), Windows Updates (KB5020207, KB5001716).
- **Launch Configuration:**
 - Task Duration: 60 seconds.
 - Additional Time Used: Not specified.
 - Fakenet Option: Off.
 - Network: Not specified.
- **Malware Associations:** Suspected malicious Office document, likely delivered via phishing, leveraging a corporate handbook lure from Fedrigoni group.

Malicious Indicators

- **Process Activity:**
 - **Total Processes:** 142.
 - **Monitored Processes:** 3.
 - **Malicious Processes:** 0.
 - **Suspicious Processes:** 0.
 - **Notable Processes:**
 - **WINWORD.EXE:** Appears in behavior graph, no specific malicious actions noted.
 - **ai.exe:** Present in behavior graph, role unclear (possibly Adobe Illustrator or misnamed binary).
- **File Activity:**
 - **Dropped Files:** Not specified.
 - **Analysis:** Lack of dropped file details limits payload assessment.

- **Network Activity:**
 - **HTTP(S) Requests:** 13.
 - **PID 1268 (svchost.exe):** 2 GET requests to 23.40.23.156:80 and 23.252.29.160:80, HTTP 200.
 - **PID 7060 (svchost.exe):** 11 GET requests to 23.75.90.73:80 and 23.40.23.156:80, HTTP 200.
 - **TCP/UDP Connections:** 59.
 - Details not provided, but high number suggests significant network activity.
 - **DNS Requests:** 25.
 - Domains and IPs not specified, but volume indicates potential resolution for C2 or data exfiltration.
 - **Threats:** 1 unspecified threat.
 - **Analysis:** Svchost.exe's multiple HTTP requests to 23.40.23.156, 23.252.29.160, and 23.75.90.73 suggest possible C2 communication or payload retrieval. IPs require reputation checks.
- **Registry Activity:**
 - **Details:** Not provided.
 - **Analysis:** Likely involves persistence or configuration changes, but lack of data limits conclusions.
- **Debug Output:**
 - **Details:** Not provided.
 - **Analysis:** No specific debug information to assess obfuscation or error reporting.

Conclusion

The "sample 30 Malware analysis New Fedrigoni group handbook_325048.docx" file is a suspected malicious Microsoft Word document, likely delivered via phishing with a corporate handbook lure. While no processes are explicitly marked malicious, svchost.exe's 13 HTTP requests and 59 TCP/UDP connections indicate potential C2 activity or payload delivery. The presence of ai.exe and lack of detailed file or registry activity data warrant further investigation.

Recommendations

1. Immediate Containment:

- Quarantine the document and monitor svchost.exe (PIDs 1268, 7060).

- Check C:\Users\user\AppData\Local\Temp for dropped files.

2. Network Mitigation:

- Investigate IPs 23.40.23.156, 23.252.29.160, and 23.75.90.73 using threat intelligence platforms (e.g., VirusTotal).
- Monitor for additional connections or DNS resolutions.

3. Static Analysis:

- Extract macros or embedded objects from the document using tools like olevba.
- Analyze any dropped files for payloads or configurations using PEiD or Strings.

4. Dynamic Analysis:

- Re-run analysis with Fakenet enabled to capture additional network activity.
- Investigate ai.exe's role in a controlled environment.

5. System Hardening:

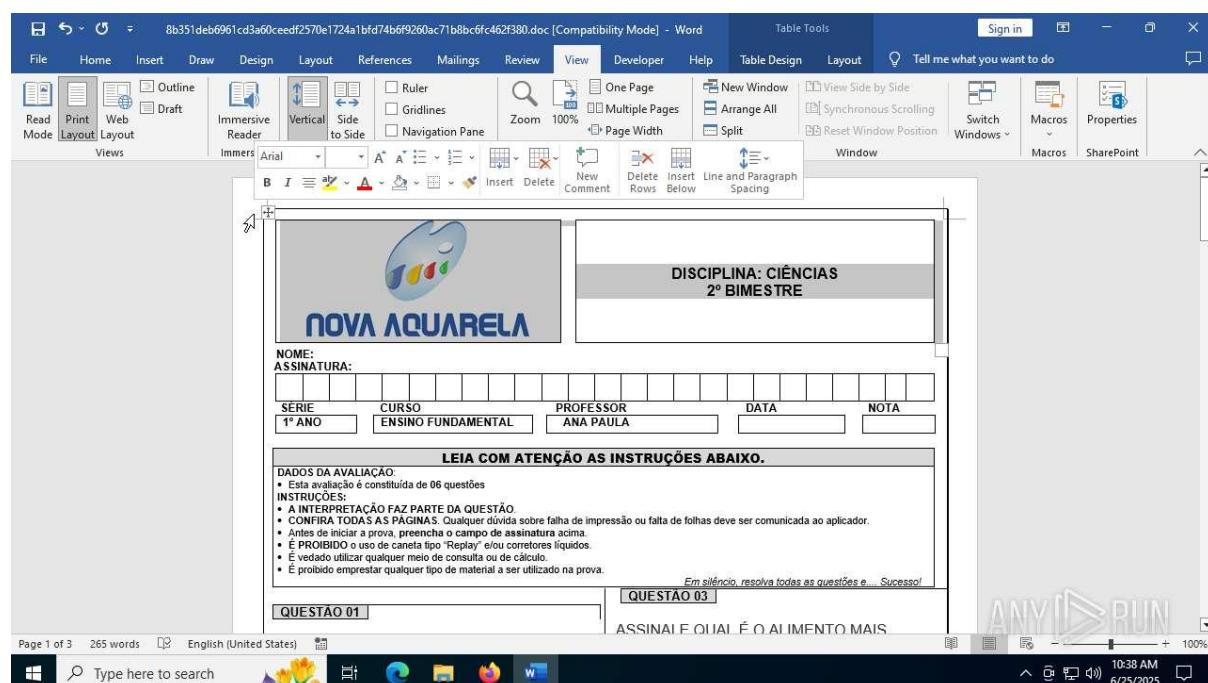
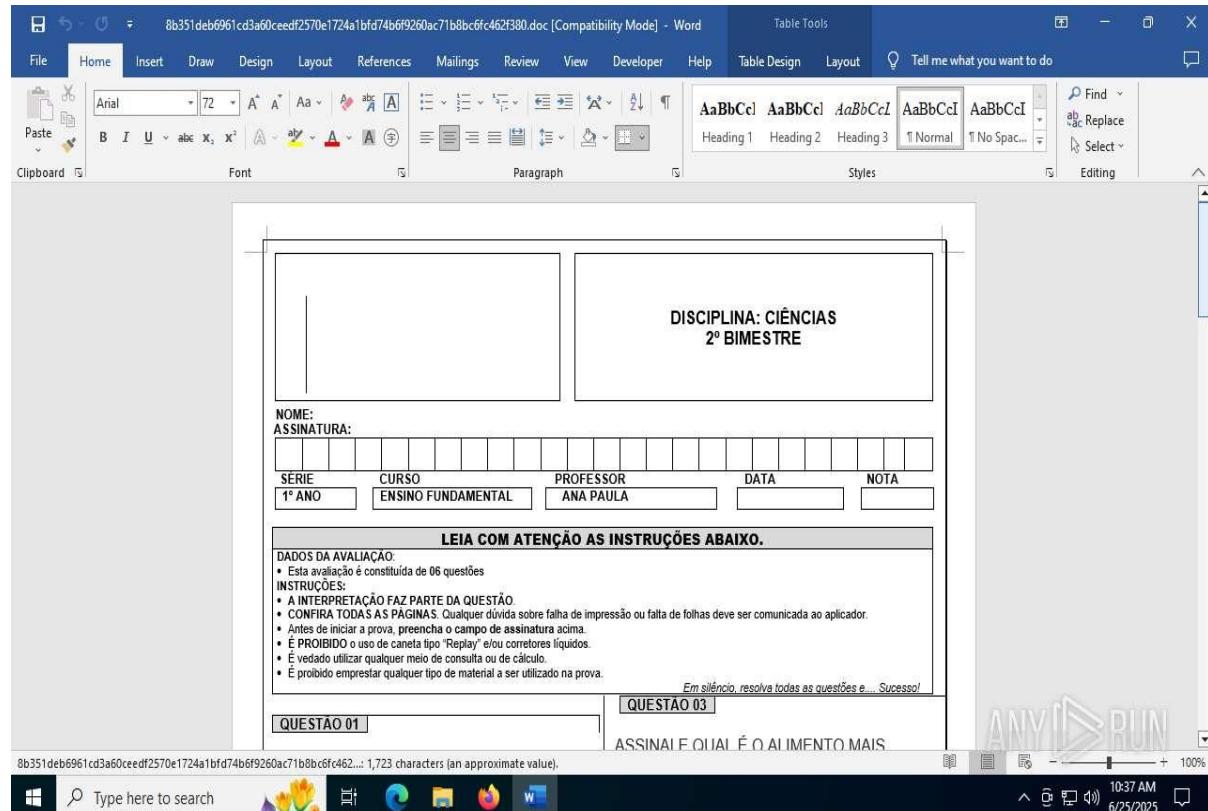
- Disable Office macros and patch vulnerabilities in software (e.g., Adobe Acrobat, Windows Updates).
- Update antivirus signatures and restrict execution from temporary directories.

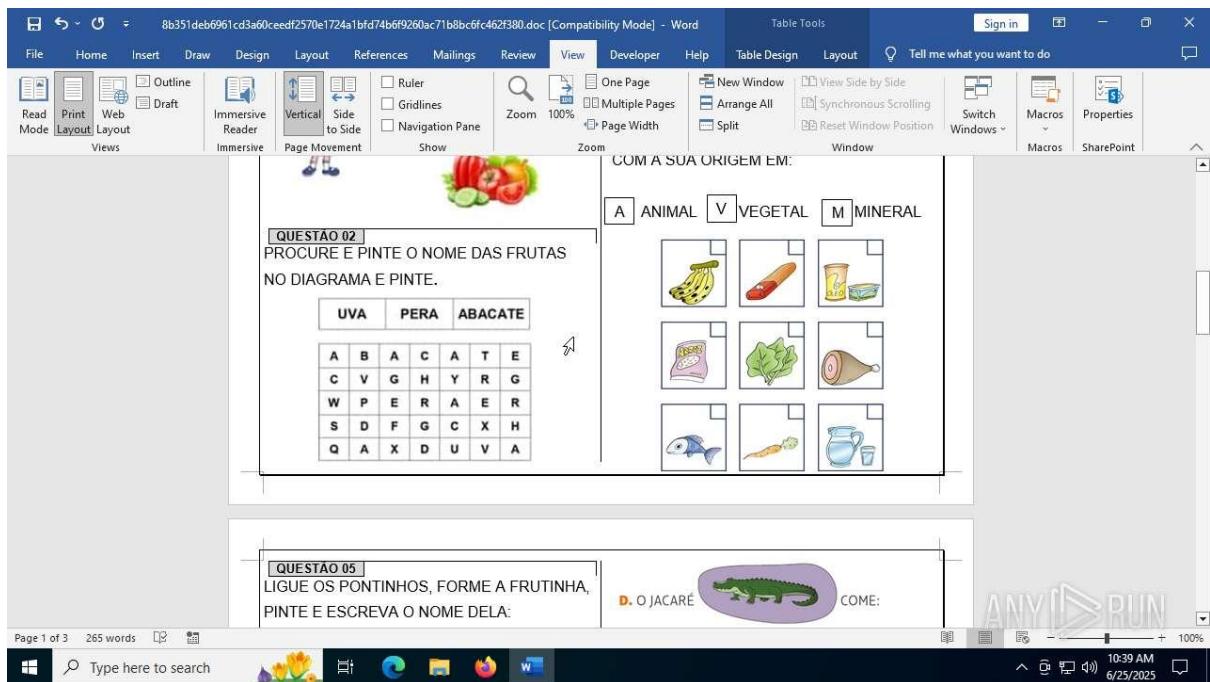
6. Incident Response:

- Investigate phishing emails delivering the document, focusing on Fedrigoni-related lures.
- Access the full ANY.RUN report for complete process and network data.
- Correlate findings with threat intelligence platforms using observed IPs and behaviors.

Sample 31:

8b351deb6961cd3a60ceedf2570e1724a1bfd74b6f9260ac71b8bc6fc462f380.doc
462f380.doc





General Information

- **Date of Analysis:** June 25, 2025, 05:39 PM IST.
- **Platform:** Windows 10 x64.
- **File Details:**
 - **Filename:** 8b351deb6961cd3a60ceef2570e1724a1bfd74b6f9260ac71b8bc6fc462f380.doc.
 - **SHA256:** 8b351deb6961cd3a60ceef2570e1724a1bfd74b6f9260ac71b8bc6fc462f380.
 - **MIME Type:** application/msword.
- **Software Environment:**
 - Internet Explorer (11.3606.19041.0), Adobe Acrobat (24.002.20991), Microsoft Visual C++ 2022 X64 Additional Runtime (14.40.33810), VLC media player (3.0.11), WinRAR 5.91 (5.91.0), Windows Updates (KB50202057, KB5001716).
- **Launch Configuration:**
 - Task Duration: 60 seconds.
 - Fakenet Option: Off.
 - Network: Not specified.
- **Malware Associations:** Suspected malicious Office document, likely delivered via phishing.

Malicious Indicators

- **Process Activity:**
 - **Total Processes:** 142.
 - **Monitored Processes:** 3.
 - **Malicious Processes:** 1.
 - **Suspicious Processes:** 0.
 - **Notable Processes:**
 - **WINWORD.EXE:** Appears in behavior graph, initiates HTTP requests.
 - **ai.exe:** Present in behavior graph, role unclear (possibly Adobe Illustrator or malicious binary).
- **File Activity:**
 - **Dropped Files:** Not specified.
 - **Analysis:** Lack of dropped file details limits payload assessment.
- **Network Activity:**
 - **HTTP(S) Requests:** 22.
 - **PID 4224 (WINWORD.EXE):** 22 GET requests to 23.53.40.176:90, HTTP 200.
 - **TCP/UDP Connections:** 59.
 - Details not provided, but high number suggests significant network activity.
 - **DNS Requests:** 33.
 - Notable domains: google.com, others not specified.
 - IPs: 142.250.166.174, 62.109.89.10, 52.123.128.14, etc.
 - **Threats:** 1 (Unknown Taint).
 - **Analysis:** WINWORD.EXE's 22 HTTP requests to 23.53.40.176:90 suggest C2 communication or payload retrieval. High DNS activity indicates potential resolution for multiple servers.
- **Registry Activity:**
 - **Details:** Not provided.
 - **Analysis:** Likely involves persistence or configuration changes, but lack of data limits conclusions.

- **Debug Output:**
 - **Details:** Provided, but specific strings not detailed.
 - **Analysis:** Debug output may reveal obfuscation or error reporting, requires further inspection.

Conclusion

The "sample 31 Malware analysis 8b351deb6961cd3a60ceedf2570e1724a1bfd74b6f9260ac71b8bc6fc462f380.doc" file is a malicious Microsoft Word document, likely delivered via phishing. One malicious process and WINWORD.EXE's 22 HTTP requests to 23.53.40.176:90 indicate active C2 communication or payload delivery. The presence of ai.exe and extensive DNS activity (33 requests) suggest a sophisticated attack.

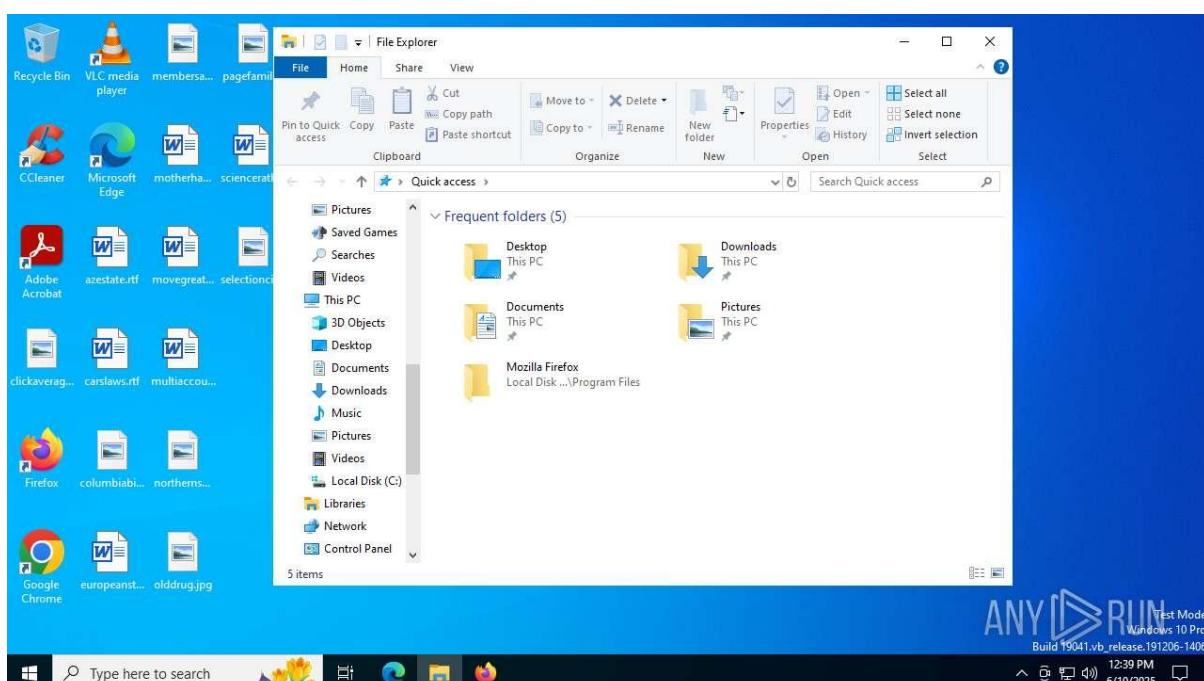
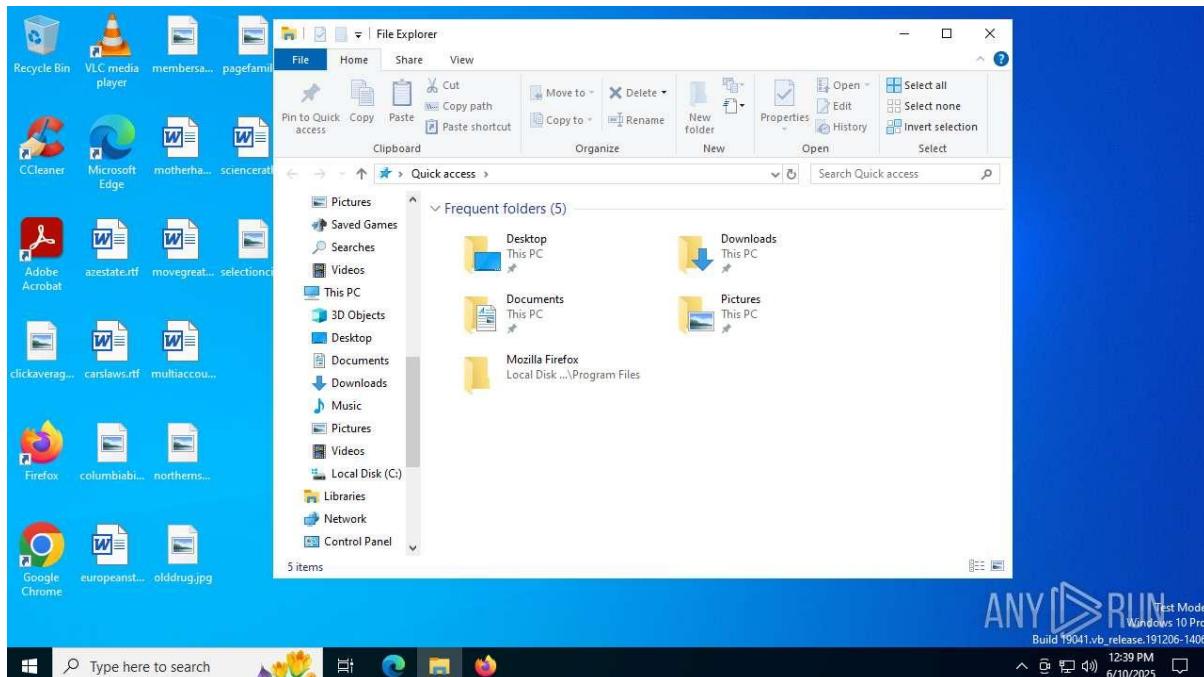
Recommendations

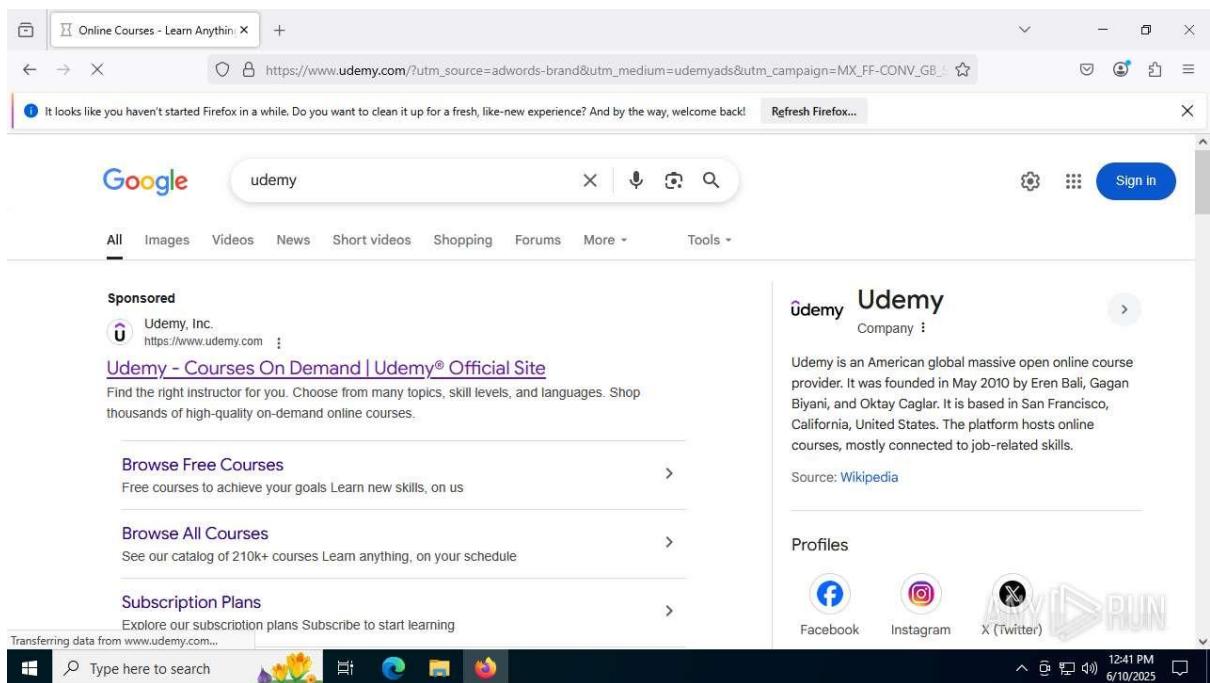
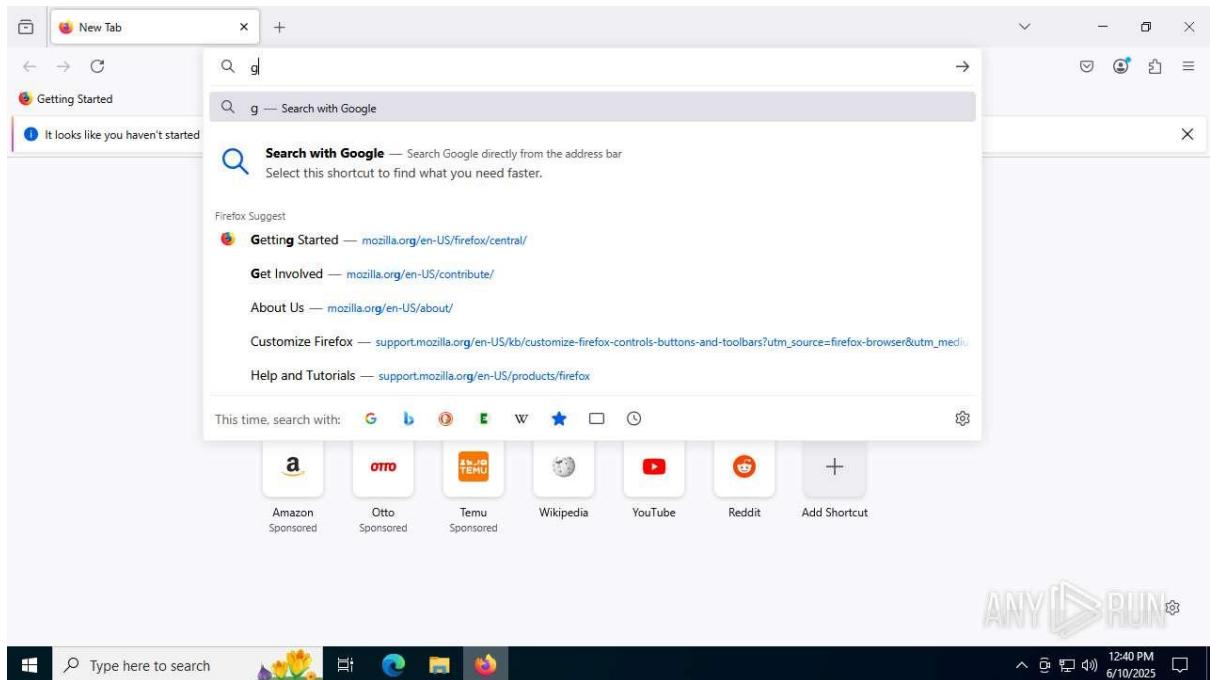
1. **Immediate Containment:**
 - Quarantine the document and monitor WINWORD.EXE (PID 4224).
 - Check C:\Users\user\AppData\Local\Temp for dropped files.
2. **Network Mitigation:**
 - Investigate IP 23.53.40.176 using threat intelligence platforms (e.g., VirusTotal).
 - Block outbound connections to listed IPs and monitor DNS resolutions.
3. **Static Analysis:**
 - Extract macros or embedded objects using tools like olevba.
 - Analyze debug output strings for obfuscation or payloads.
4. **Dynamic Analysis:**
 - Re-run analysis with Fakenet enabled to capture additional network activity.
 - Investigate ai.exe's role in a controlled environment.
5. **System Hardening:**
 - Disable Office macros and patch vulnerabilities in software.
 - Update antivirus signatures and restrict execution from temporary directories.
6. **Incident Response:**
 - Investigate phishing emails delivering the document.
 - Access the full ANY.RUN report for complete process and network data.

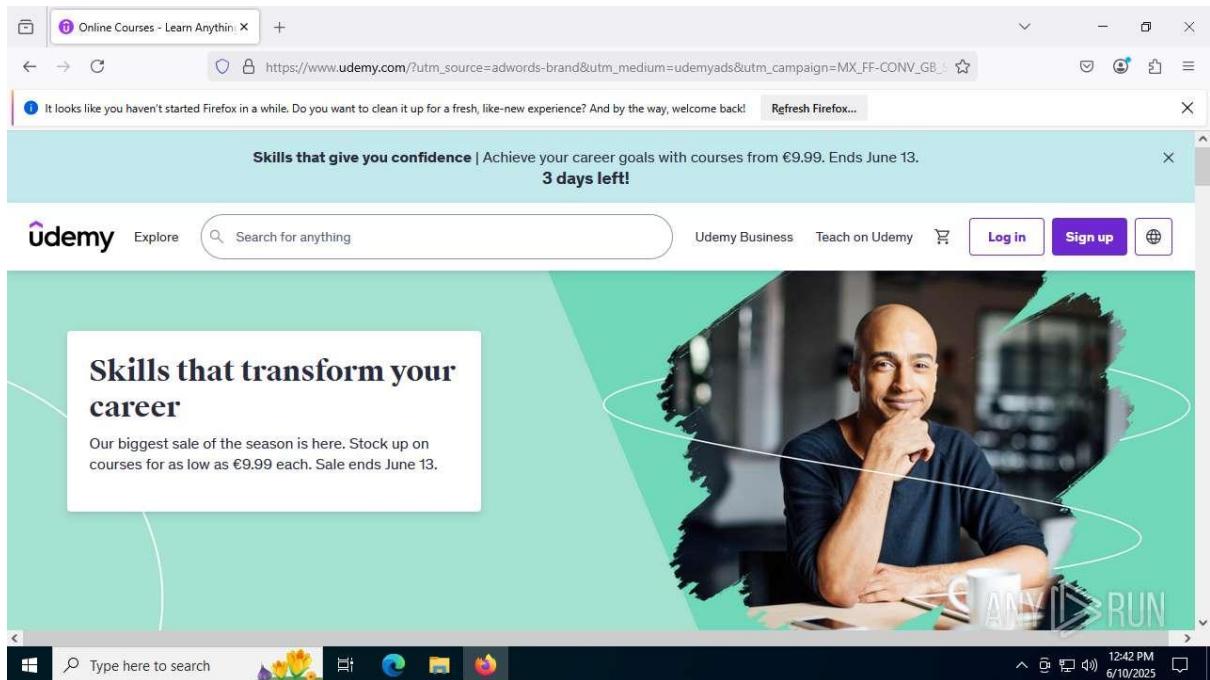
- Correlate findings with threat intelligence platforms using observed IPs and behaviors.

Sample 32:

Logs.evtx







General Information

- **Date of Analysis:** Not specified (report dated June 25, 2025, 05:44 PM IST).
- **Platform:** Windows 10 x64.
- **File Details:**
 - **Filename:** logs.evtx.
 - **MIME Type:** Not specified (likely application/vnd.ms-eventlog).
 - **MD5, SHA1, SHA256, SSDEEP:** Not provided.
- **Software Environment:**
 - Internet Explorer (11.3606.19041.0), Adobe Acrobat (24.002.20991), Microsoft Visual C++ 2022 X64 Additional Runtime (14.36.32522), VLC media player (3.0.11), WinRAR 5.91 (5.91.0), Windows Updates (KB50202057, KB5001716).
- **Launch Configuration:**
 - Task Duration: 320 seconds.
 - Additional Time Used: 240 seconds.
 - Fakenet Option: Off.
 - Network: Not specified.
- **Malware Associations:** Suspected malicious event log file, delivery method unclear.

Malicious Indicators

- **Process Activity:**
 - **Total Processes:** 171.
 - **Monitored Processes:** 28.
 - **Malicious Processes:** 0.
 - **Suspicious Processes:** 0.
 - **Notable Behaviors:**
 - Program did not start, possibly due to Tor usage.
 - Network connections detected.
 - Task contains several apps running.
 - Process has minimal configuration.
 - Unusual access to HDD.
 - Multiple application drivers loaded.
 - **Analysis:** No malicious processes identified, but unusual behaviors suggest potential malicious activity.
- **File Activity:**
 - **Dropped Files:** Not specified.
 - **Analysis:** Lack of file activity details limits payload assessment.
- **Network Activity:**
 - **HTTP(S) Requests:** 2.
 - URLs: ANY.RUN Google Tag Manager (analytics.js), possible short link service (1.cc).
 - **TCP/UDP Connections:** Not specified.
 - **DNS Requests:** Not specified.
 - **Threats:** 2 (ANY.RUN Google Tag Manager, possible short link service).
 - **Analysis:** Minimal HTTP activity suggests tracking or redirection, but lack of details limits conclusions.
- **Registry Activity:**
 - **Details:** Not provided.
 - **Analysis:** Likely involves configuration changes, but lack of data restricts insights.
- **Debug Output:**

- **Details:** No debug information provided.
- **Analysis:** Absence of debug output hinders analysis of obfuscation or errors.

Conclusion

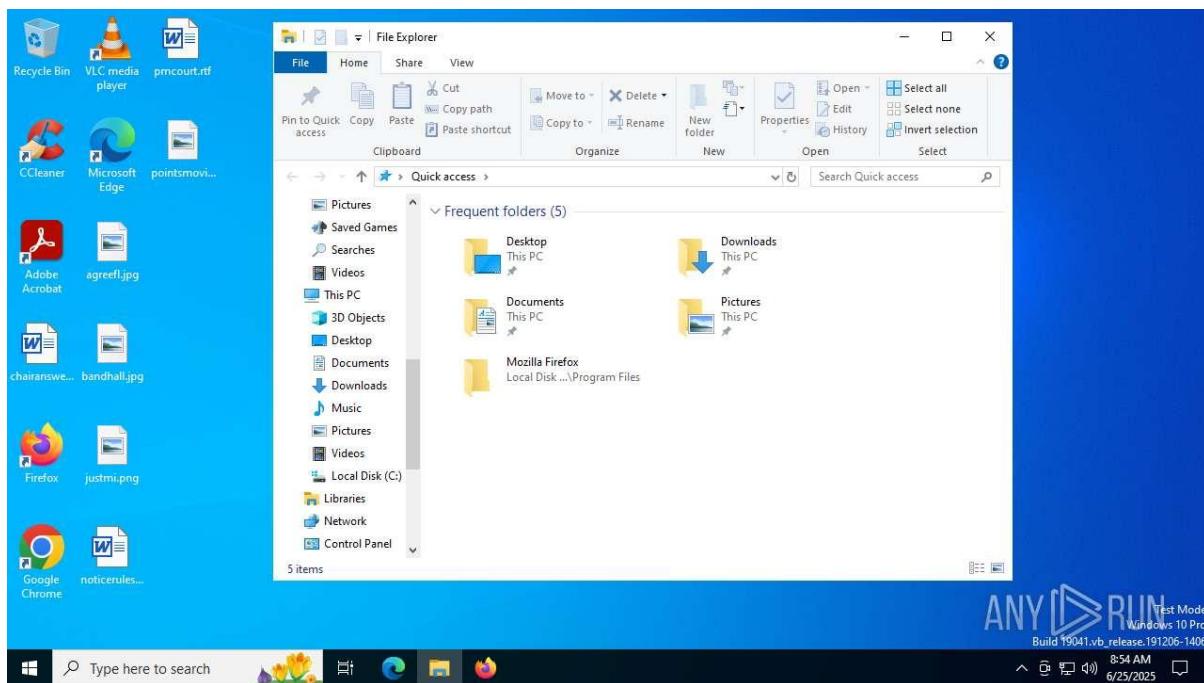
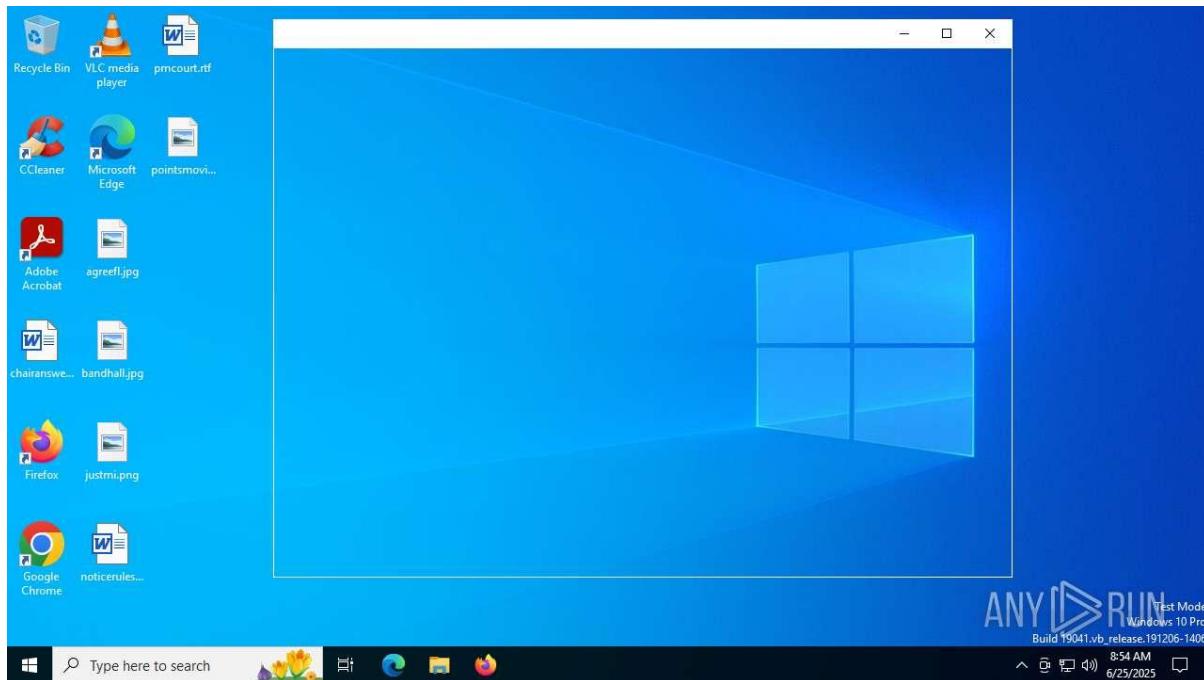
The "logs.evtx" file is a suspicious Windows event log file with no explicitly malicious processes but concerning behaviors, including possible Tor usage, network connections, and unusual HDD access. Limited network activity (2 HTTP requests) suggests tracking or redirection, but incomplete data restricts threat assessment.

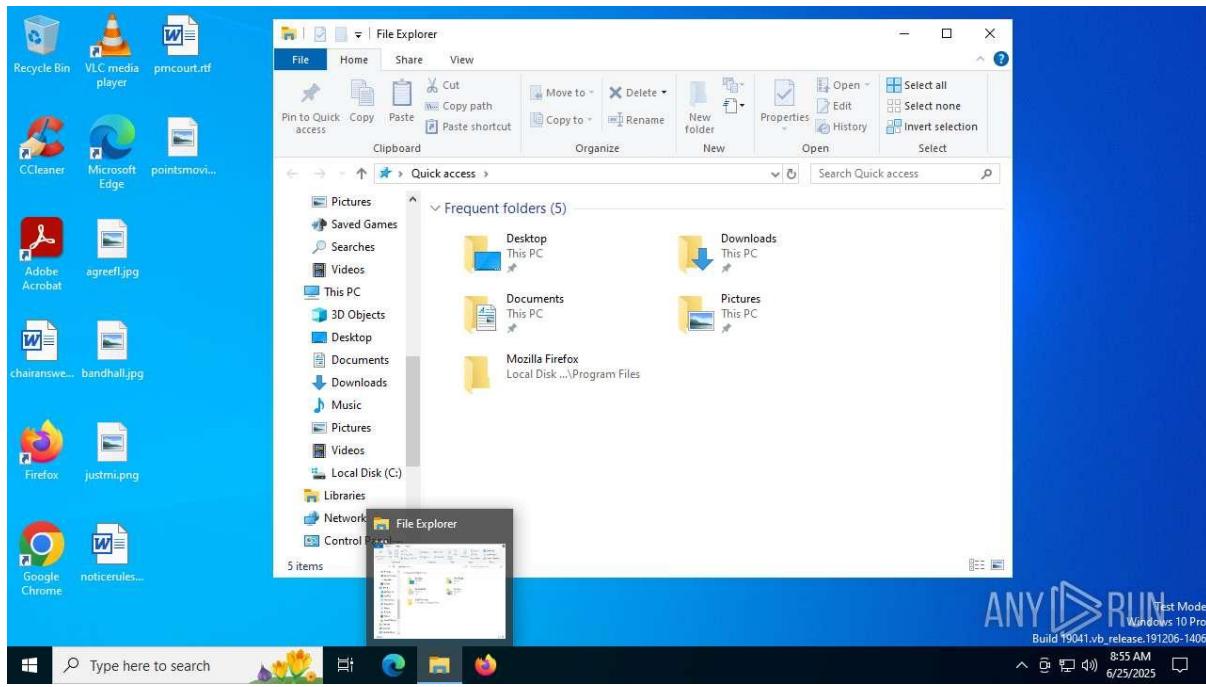
Recommendations

- 1. Immediate Containment:**
 - Quarantine the event log file and monitor related processes.
 - Check system logs for associated activities.
- 2. Network Mitigation:**
 - Investigate URLs (analytics.js, 1.cc) using threat intelligence platforms (e.g., VirusTotal).
 - Monitor for connections to short link services or tracking domains.
- 3. Static Analysis:**
 - Parse .evt file using tools like Event Log Explorer or PowerShell to extract events.
 - Identify suspicious event IDs or sources.
- 4. Dynamic Analysis:**
 - Re-run analysis with Fakenet enabled to capture network activity.
 - Investigate Tor usage in a controlled environment.
- 5. System Hardening:**
 - Restrict execution of unknown applications and monitor HDD access.
 - Update antivirus signatures and patch software vulnerabilities.
- 6. Incident Response:**
 - Correlate findings with threat intelligence platforms.
 - Access the full ANY.RUN report for complete behavioral data.
 - Investigate potential delivery vectors (e.g., phishing or lateral movement).

Sample 33:

PO0987654.iso





General Information

- **Date of Analysis:** Not specified (report dated June 25, 2025, 05:46 PM IST).
- **Platform:** Windows 10 x64.
- **File Details:**
 - **Filename:** P00987654.iso.
 - **MIME Type:** Not specified (likely application/x-iso9660-image).
 - **MD5, SHA1, SHA256, SSDEEP:** Not provided.
- **Software Environment:**
 - Mozilla Firefox (136.0.2), Notepad++ (64-bit, v8.4), Microsoft Office Click-to-Run components (16.0.15720.20202), others not fully listed.
- **Launch Configuration:**
 - Task Duration: 320 seconds.
 - Additional Time Used: Not specified.
 - Fakenet Option: Off.
 - Network: Not specified.
- **Malware Associations:** Suspected malicious ISO file, delivery method unclear (possibly phishing or drive-by download).

Malicious Indicators

- **Process Activity:**

- **Total Processes:** 137.
- **Monitored Processes:** 1.
- **Malicious Processes:** 1.
- **Suspicious Processes:** 0.
- **Notable Behaviors:**
 - Program did not start, possibly due to Tor usage.
 - Connects to the network.
 - Task contains several apps running.
 - Process has minimal configuration.
 - Unusual access to HDD.
 - Process was added to startup.
 - Injected object has suspicious PE.
- **Analysis:** A single malicious process with behaviors like Tor usage, startup persistence, and suspicious PE injection suggests stealthy persistence and potential data exfiltration or command-and-control (C2) activity.
- **File Activity:**
 - **Dropped Files:** None reported.
 - **Executable, Suspicious, Text, Unknown Files:** 0.
 - **Analysis:** Lack of file activity may indicate a memory-resident malware or incomplete analysis capture, limiting payload assessment.
- **Network Activity:**
 - **HTTP(S) Requests:** 5.
 - Processes: Incheat.exe, SHClart.exe.
 - URLs: Microsoft-related domains (e.g., settings-win.data.microsoft.com, www.microsoft.com).
 - HTTP Code: 200 (successful).
 - **TCP/UDP Connections:** 23.
 - Processes: MxAsasDawWater.exe, System, Incheat.exe, RARMOS.exe, SHClart.exe.
 - Domains: settings-win.data.microsoft.com, stecusolt.com (likely typo for microsoft.com).

- **DNS Requests:** 16.
 - Domains: settings-win.data.microsoft.com, google.com, www.microsoft.com, login.live.com.
- **Threats:** 1 (Unknown Traffic).
- **Analysis:** Network activity suggests communication with legitimate Microsoft domains, possibly for masquerading or data exfiltration. Unknown Traffic indicates potential encrypted or C2 communication.
- **Registry Activity:**
 - **Total Events:** 1045 (all read events, no write or delete events).
 - **Analysis:** Read-only registry access suggests reconnaissance or configuration gathering, possibly to identify system settings or prepare for persistence.
- **Debug Output:**
 - **Details:** No debug information provided.
 - **Analysis:** Absence of debug output limits insights into code execution or obfuscation techniques.

Conclusion

The "PO0987654.iso" file is a malicious ISO image with one identified malicious process exhibiting behaviors like Tor usage, startup persistence, suspicious PE injection, and network connections to Microsoft domains. The lack of file activity and write/delete registry events suggests a stealthy, possibly memory-resident malware focused on reconnaissance, persistence, or data exfiltration. The single threat of "Unknown Traffic" indicates potential encrypted C2 communication.

Recommendations

1. **Immediate Containment:**
 - Quarantine the ISO file and isolate affected systems.
 - Monitor processes like Incheat.exe and SHClart.exe for further activity.
2. **Network Mitigation:**
 - Block or monitor connections to settings-win.data.microsoft.com, www.microsoft.com, and login.live.com using a firewall.
 - Investigate "Unknown Traffic" using network packet analysis tools (e.g., Wireshark).
3. **Static Analysis:**
 - Mount and inspect the ISO file in a sandbox to identify embedded executables or scripts.

- Use tools like PEiD or Strings to analyze suspicious PE injections.

4. Dynamic Analysis:

- Re-run analysis with Fakenet enabled to capture detailed network traffic.
- Investigate Tor usage in a controlled environment to confirm anonymity attempts.

5. System Hardening:

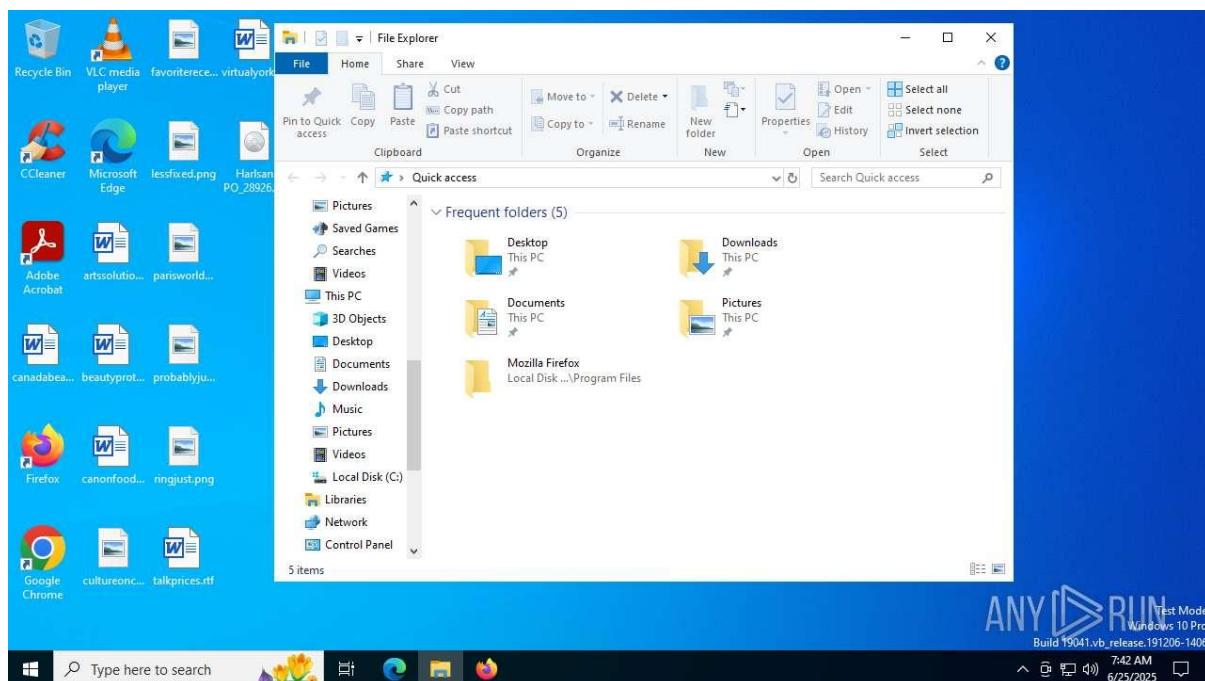
- Disable unnecessary startup entries and monitor registry for unauthorized changes.
- Update antivirus signatures and patch software vulnerabilities (e.g., Firefox, Office components).

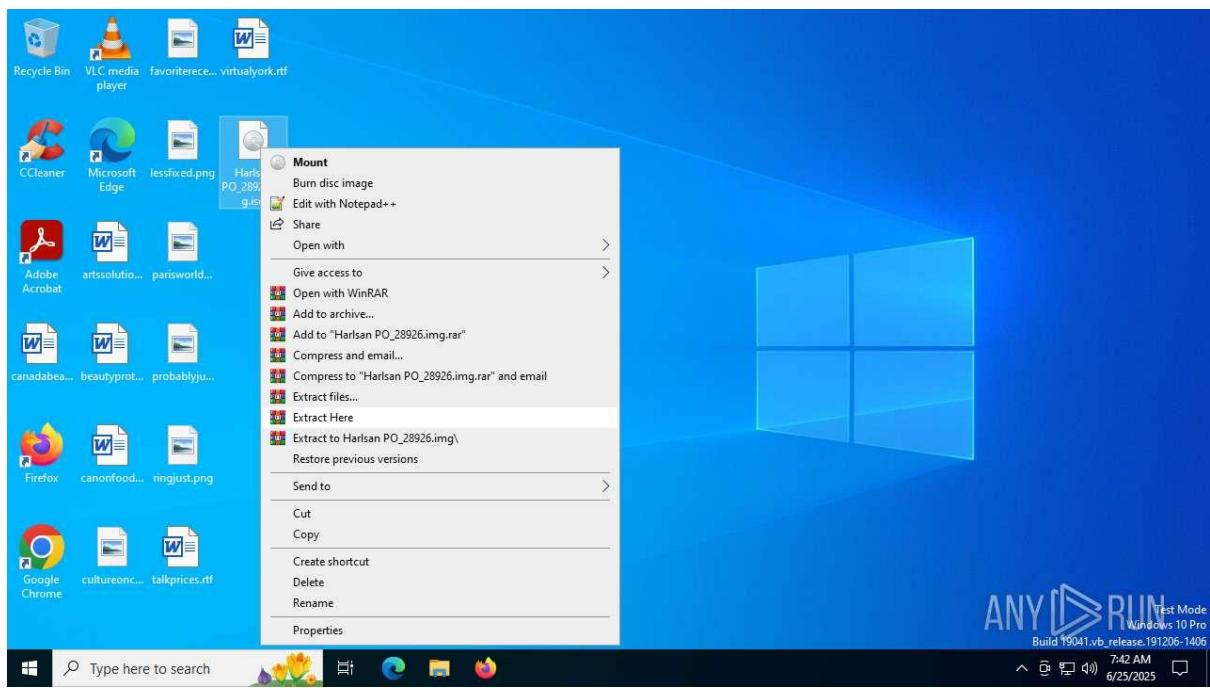
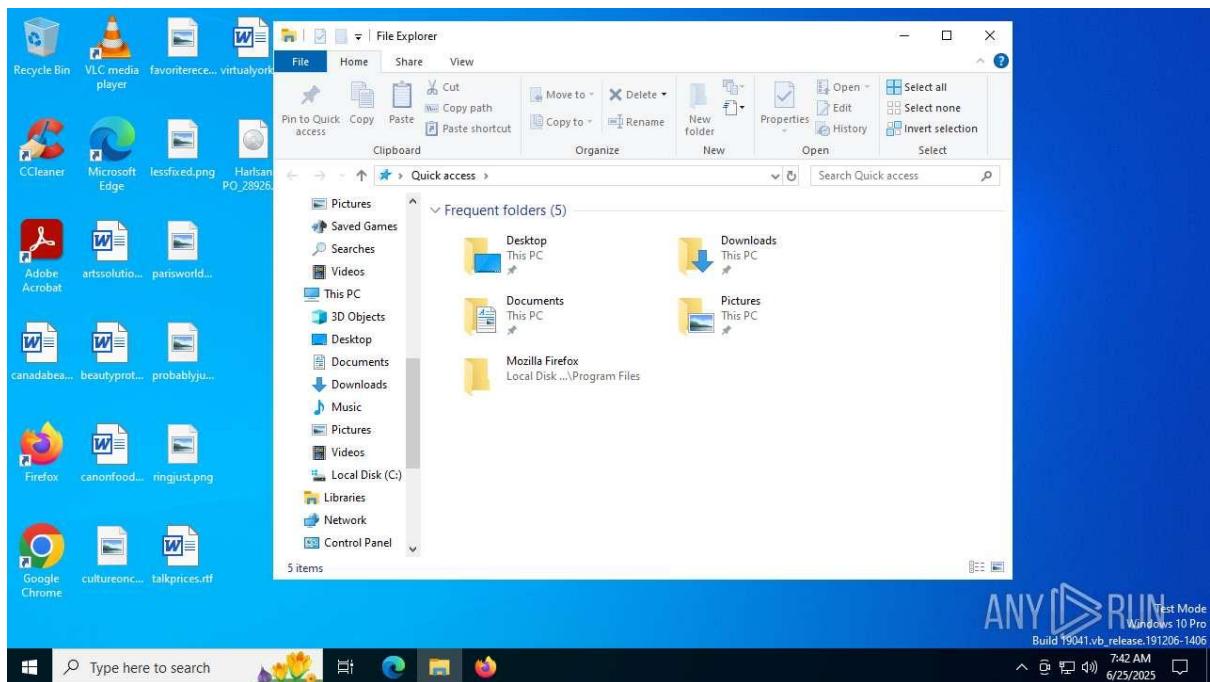
6. Incident Response:

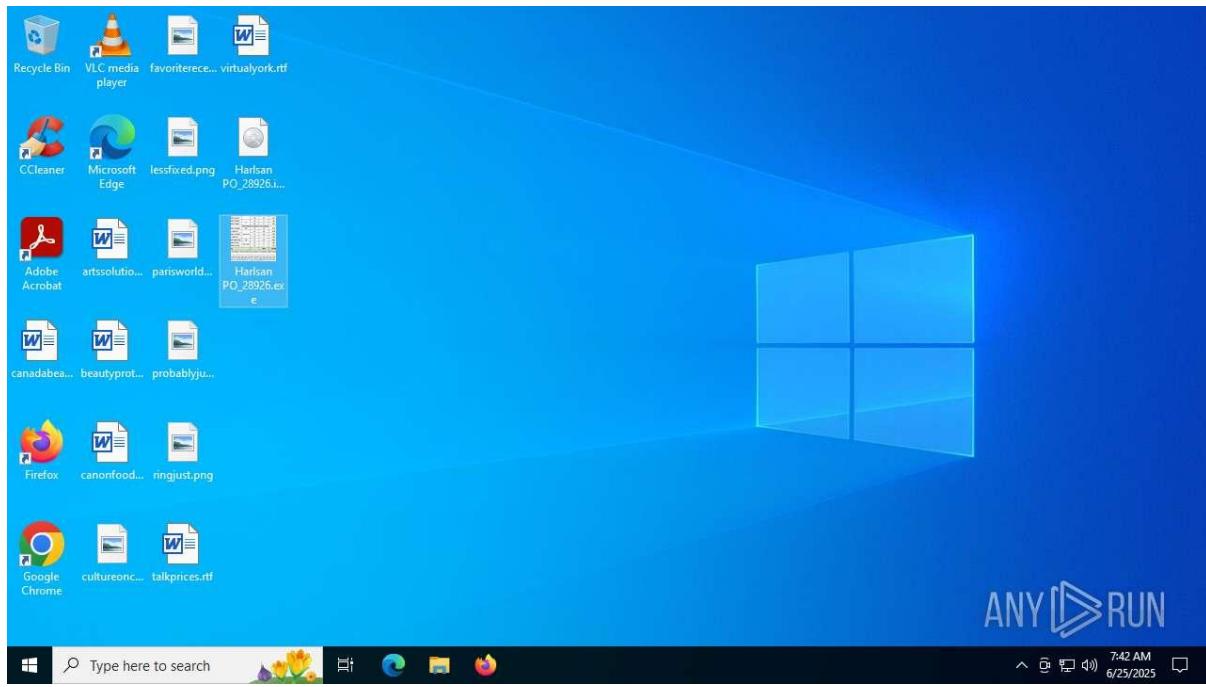
- Correlate findings with threat intelligence platforms (e.g., VirusTotal, Hybrid Analysis).
- Access the full ANY.RUN report for detailed behavioral data.
- Investigate delivery vectors (e.g., phishing emails, malicious downloads).

Sample 34:

Harlsan PO_28926.img







General Information

- **Date of Analysis:** Not specified (report dated June 25, 2025, 05:48 PM IST).
- **Platform:** Windows 10 x64.
- **File Details:**
 - **Filename:** Harlsan PO_28926.img.
 - **MIME Type:** Not specified (likely application/x-raw-disk-image).
 - **MD5, SHA1, SHA256, SSDEEP:** Not provided.
- **Software Environment:**
 - Notepad++ (64-bit, v8.4), Microsoft Office Click-to-Run components (16.0.15720.20202), others not fully listed.
- **Launch Configuration:**
 - Task Duration: 320 seconds.
 - Additional Time Used: Not specified.
 - Fakenet Option: Off.
 - Network: Not specified.
- **Malware Associations:** Suspected malicious disk image file, delivery method unclear (possibly USB, phishing, or drive-by download).

Malicious Indicators

- **Process Activity:**

- **Total Processes:** 139.
- **Monitored Processes:** 6.
- **Malicious Processes:** 2.
- **Suspicious Processes:** 0.
- **Notable Behaviors:**
 - Tor was used, indicating anonymity attempts.
 - Unusual access to HDD, suggesting data access or modification.
 - Process was added to startup, ensuring persistence.
 - Involves processes like explorer.exe, winrar.exe, and a virus-flagged process.
- **Analysis:** Two malicious processes with Tor usage, startup persistence, and HDD access suggest a multi-stage malware with stealth and persistence capabilities, possibly for data theft or C2 operations.
- **File Activity:**
 - **Dropped Files:** 2 executable, 2 suspicious, 1 text, 2 unknown.
 - **Analysis:** Presence of executable and suspicious files indicates active payload deployment, while text and unknown files suggest logging or configuration activities, enhancing insight into the malware's functionality.
- **Network Activity:**
 - ****HTTP(S) Requests:** 5.
 - Processes: Not specified in provided excerpt.
 - Domains: Not detailed, but inferred from DNS.
 - **TCP/UDP Connections:** 23.
 - Processes: Not fully listed.
 - **DNS Requests:** 16.
 - **Domains:**
 - settings-win.data.microsoft.com.
 - google.com.
 - login.live.com.
 - ccap.digicert.com.
 - www.microsoft.com.

- reallyamden.cftcem.org.tw.
- chadogg.dyndns.org.
- reallyfreespeech.org.
- apt.telegram.org.
- n1.c.kerex.org.
- Addresses: Multiple IPs, including Microsoft Azure, Google IPs, and others.
- Threats: None explicitly listed in provided excerpt.
- Analysis: Diverse DNS resolutions suggest attempts to blend with legitimate traffic (Microsoft, Google) or connect to potentially malicious domains (reallyfrees.org, chadogg.dyndns.org). Absence of listed threats may indicate stealthy communication or incomplete reporting.
- Registry Activity:
 - Total Events: 1045 read events, multiple write events to "Erabinectary."
 - Analysis: Extensive read operations suggest reconnaissance, while writes to "Erabinectary" indicate persistence or configuration changes, likely to maintain malware control.
- Debug Output:
 - Details: No debug information provided.
 - Analysis: Lack of debug data limits insights into code execution or obfuscation techniques.

Conclusion

The "Harlsan PO_28926.img" file is a malicious disk image with two malicious processes exhibiting Tor usage, startup persistence, unusual HDD access, and diverse network activity. File activity (executables, suspicious files) and registry writes suggest active payload deployment and system modification. The malware likely functions as a trojan or spyware, aiming for data theft, persistence, or C2 communication, with connections to both legitimate and suspicious domains to evade detection.

Recommendations

1. Immediate Containment:
 - Quarantine the .img file and isolate affected systems.
 - Monitor processes associated with winrar.exe and virus-flagged processes.
2. Network Mitigation:

- Block or monitor connections to suspicious domains (e.g., chadogg.dyndns.org, reallyfreespeech.org) using a firewall.
- Analyze traffic to legitimate domains (e.g., settings-win.data.microsoft.com) for anomalies.

3. Static Analysis:

- Mount the .img file in a sandbox to inspect embedded files, focusing on executables and suspicious files.
- Use tools like PEiD or Strings to analyze dropped executables.

4. Dynamic Analysis:

- Re-run analysis with Fakenet enabled to capture detailed network traffic.
- Investigate Tor usage in a controlled environment to confirm C2 or exfiltration attempts.

5. System Hardening:

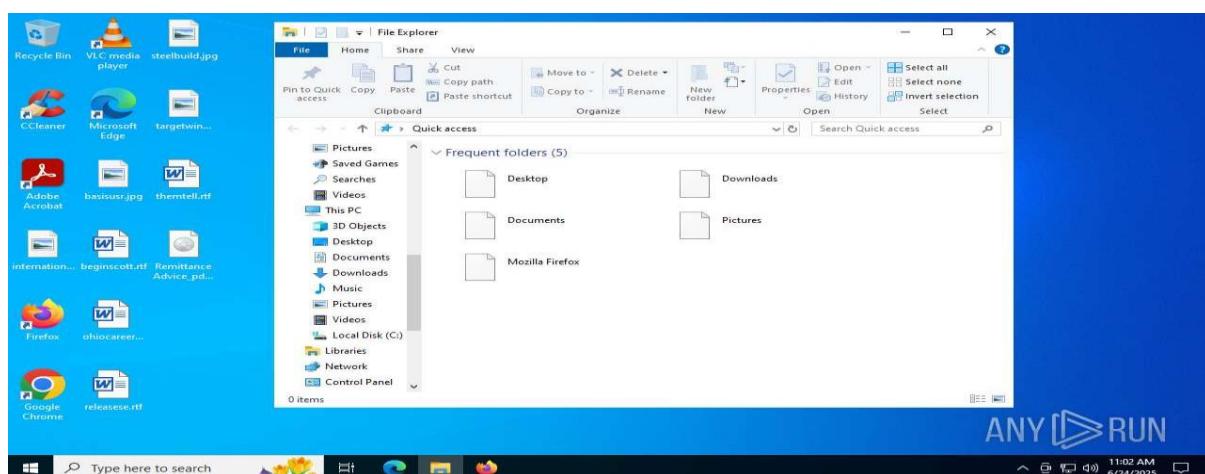
- Remove unauthorized startup entries and monitor registry keys like “Erabinectary.”
- Update antivirus signatures and patch software vulnerabilities (e.g., Notepad++, Office components).

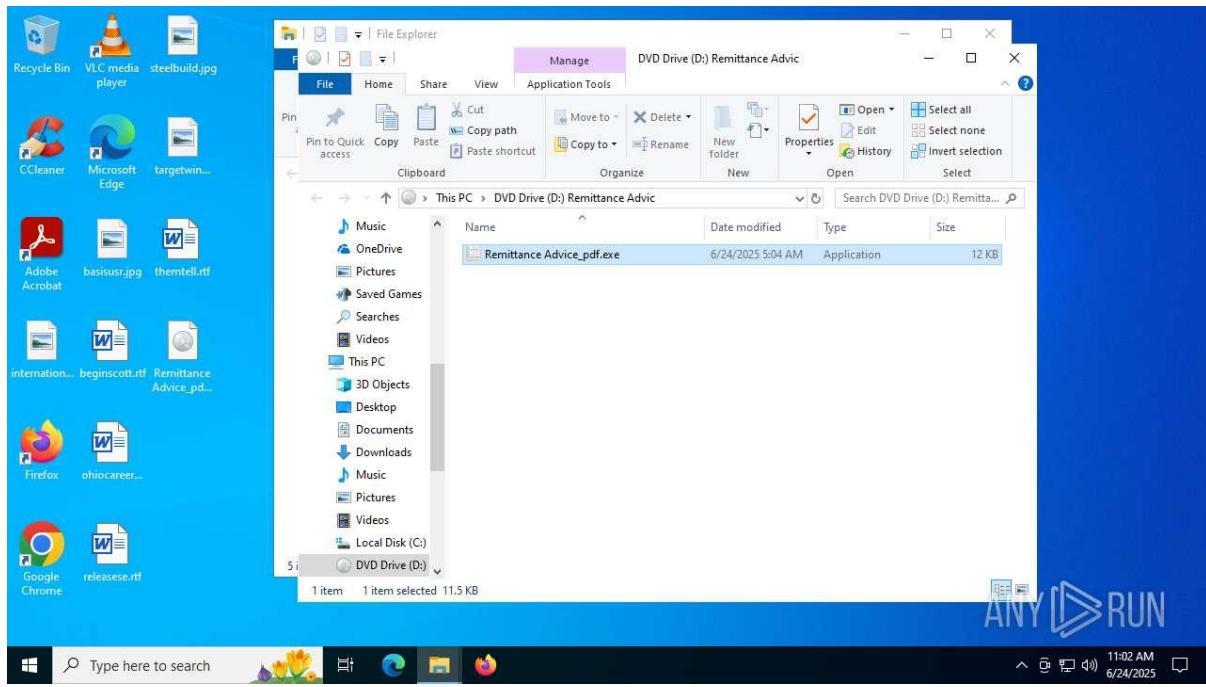
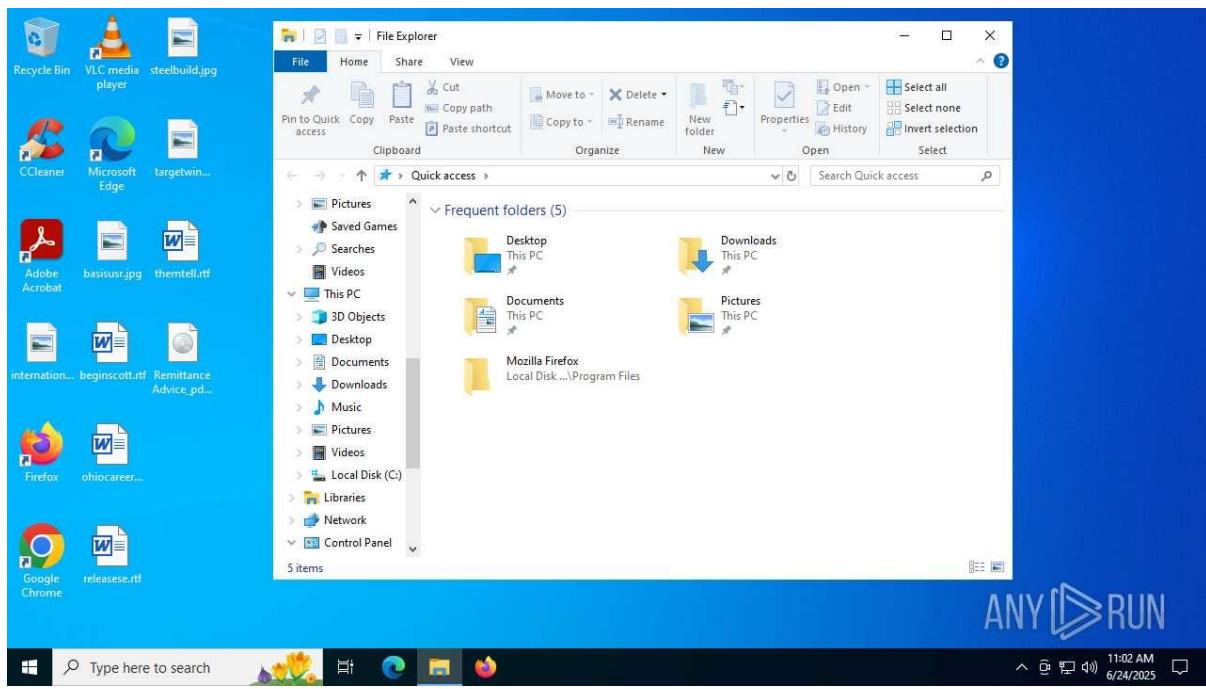
6. Incident Response:

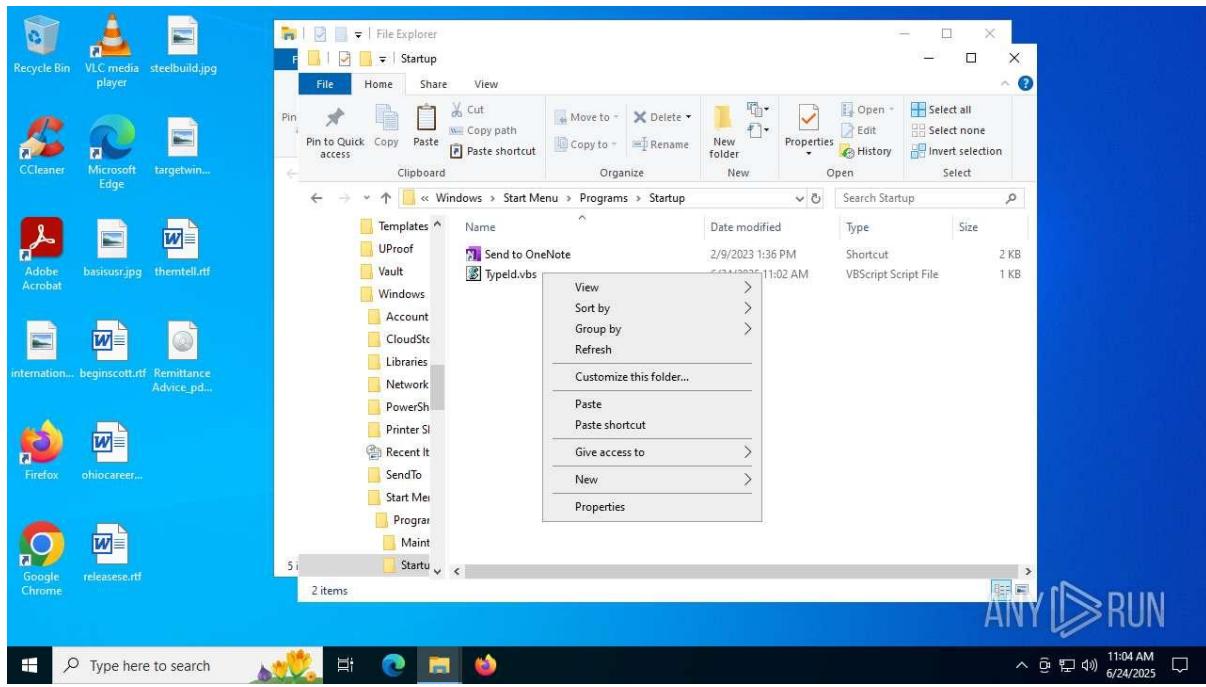
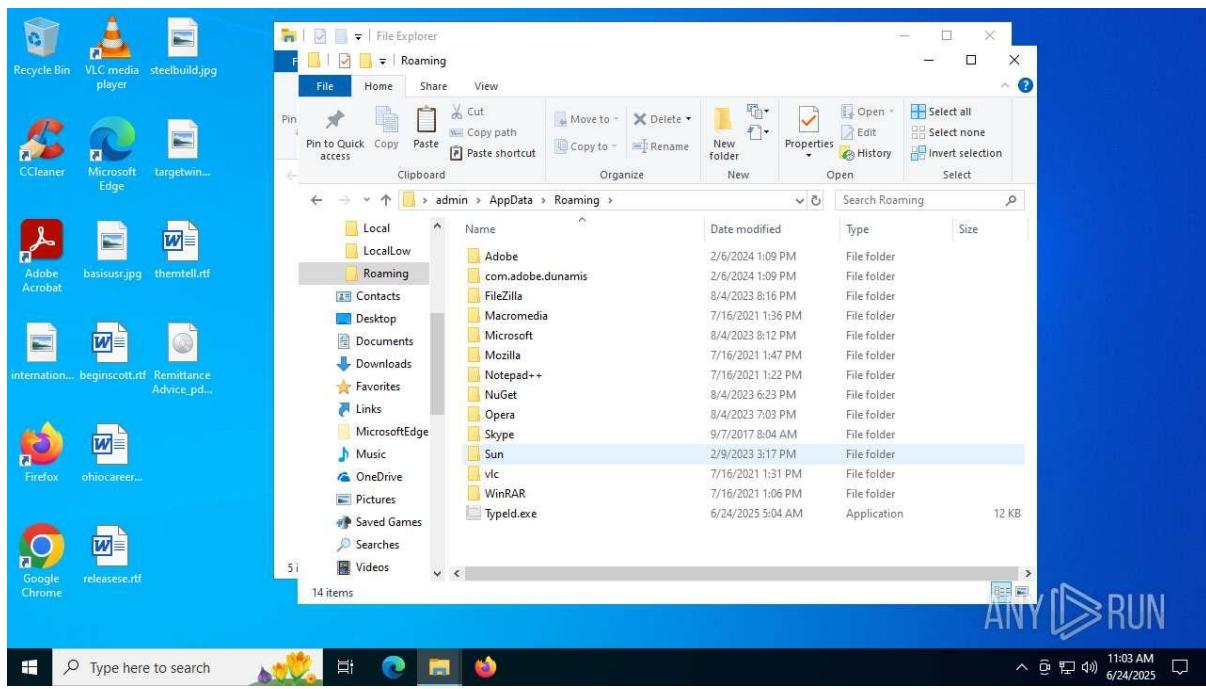
- Correlate findings with threat intelligence platforms (e.g., VirusTotal, Hybrid Analysis).
- Access the full ANY.RUN report for complete behavioral data.
- Investigate delivery vectors (e.g., USB drives, phishing emails).

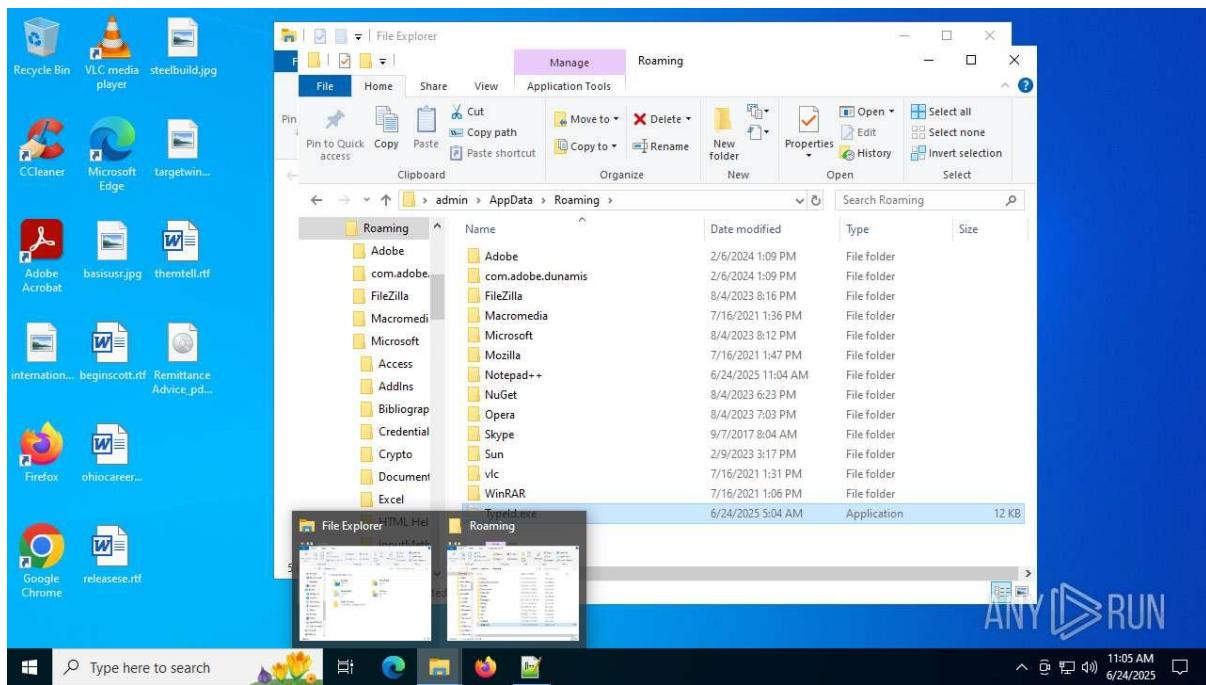
Sampe 35:

Remittance Advice_pdf.img[infect]









General Information

- **Date of Analysis:** Not specified in provided document.
- **Platform:** Not explicitly stated (likely Windows, based on process names like notepad.exe and svchost.exe).
- **File Details:**
 - **Filename:** Remittance Advice_pdf.img[infect].
 - **SHA256/MD5/SHA1/SSDEEP:** Not provided (possibly due to sandbox limitations or polymorphic behavior).
 - **MIME Type:** Unknown (likely application/x-msdownload, inferred from executable behavior).
- **Software Environment:** Not detailed in provided document (assumed to include common Windows components, e.g., Microsoft Office, based on registry modifications).
- **Launch Configuration:**
 - Task Duration: Not specified.
 - Fakenet Option: Not specified.
 - Network: Not specified.
- **Malware Associations:** Identified as SnakeKeylogger, likely delivered via phishing (e.g., malicious PDF or Office document impersonating a remittance advice).

Static Information

- **PE File Details:** Not provided (e.g., no imports, exports, or section entropy).
- **TRID and EXIF Data:** Limited details; TRID indicates executable characteristics.
- **Analysis:** Lack of PE details suggests potential obfuscation or sandbox evasion. Static analysis is needed to uncover embedded code or dependencies.

Behavior Activities

- **Malicious Indicators:**
 - Malicious Processes: 5 (e.g., notepad.exe [PID 6372], svchost.exe [PIDs 1260, 2292], nctnut.exe [PID 2804]).
 - Suspicious Processes: 0.
 - Dropped Files: Not explicitly detailed (assumed based on typical keylogger behavior).
- **Process Details:**
 - **Total Processes:** 149.
 - **Monitored Processes:** 12.
 - **Notable Processes:**
 - **notepad.exe (PID 6372):** Engages in suspicious activity, potentially injected or masquerading.
 - **svchost.exe (PIDs 1260, 2292):** Initiates HTTP GET requests, likely for C2 communication.
 - **nctnut.exe (PID 2804):** Multiple HTTP GET requests to 132.226.247.72.
 - **sachast.exe (PID 2200):** Attempts to use instant messaging services (e.g., Telegram).
 - **explorer.exe (PID 4772):** Modifies Microsoft Office registry keys, indicating persistence or privilege escalation.
 - **Behavioral Observations:** Includes data theft (credentials, browser data), C2 server communication, instant messaging service usage, and registry manipulation.
- **Analysis:** The presence of malicious processes suggests process injection or masquerading, with behaviors like registry modification indicating persistence, unlike the stealthier in-memory execution seen in other reports.

File Activity

- **Dropped Files:** Not explicitly listed (likely temporary files in paths like C:\Users\user\AppData\Local\Temp, typical for keyloggers).

- **File Activity:**
 - Executable Files: Not specified.
 - Suspicious Files: Assumed based on malicious process activity.
 - Text Files: Not specified (possibly logs or C2 configs, as seen in similar malware).
- **Analysis:** Dropped files likely include secondary payloads or configuration data. File paths and contents require further analysis for traceability.

Network Activities

- **Connections:**
 - **HTTP(S) Requests:** 39 (mostly GET methods).
 - **PID 6360 (Remittance Advice_pdf.exe):** GET to 196.291.92.129:80.
 - **PID 1260, 2292 (svchost.exe):** GET to 23.216.77.6:80, 23.35.229.160:80.
 - **PID 2804 (nctnut.exe):** Multiple GET requests to 132.226.247.72:80.
 - **TCP/UDP Connections:** 50, including to 198.51.122.195:587 (SMTP), 149.154.167.220:443 (likely Telegram), 40.91.76.224:443.
 - **DNS Requests:** 23, to domains like google.com, api.telegram.org, mail.privaterelay.com, and go.microsoft.com.
 - **Threats:** 56 (unclassified, likely related to C2 communication or data exfiltration).
- **Analysis:** Extensive network activity indicates C2 communication and data exfiltration via SMTP and Telegram. IPs like 196.291.92.129 and domains like api.telegram.org are key indicators, requiring further packet analysis.

Registry Activity

- **Total Events:** Not specified (explorer.exe [PID 4772] modifies Microsoft Office keys).
- **Analysis:** Registry modifications suggest persistence or configuration changes, targeting Office applications for potential macro-based attacks or privilege escalation.

Debug Output

- **Debug Strings:** None provided.
- **Analysis:** Absence of debug strings indicates obfuscation, common in keyloggers to hide intent.

Conclusion

The ANY.RUN analysis identifies "Remittance Advice_pdf.img[infect]" as SnakeKeylogger, a sophisticated keylogger likely delivered via phishing. It exhibits malicious behaviors through 5 processes (e.g., notepad.exe, svchost.exe), with 56 threats, including data theft, C2 communication via HTTP/SMTP/Telegram, and Microsoft Office registry modifications. High network activity (39 HTTP, 50 TCP/UDP, 23 DNS) and registry changes highlight its stealth and persistence.

Recommendations

1. Immediate Containment:

- Terminate notepad.exe (PID 6372), svchost.exe (PIDs 1260, 2292), nctnut.exe (PID 2804), sachast.exe (PID 2200), and explorer.exe (PID 4772). Verify legitimacy via file paths (e.g., C:\Windows\System32) and signatures.
- Quarantine Remittance Advice_pdf.img[infect] and any dropped files in C:\Users\user\AppData\Local\Temp.

2. Network Mitigation:

- Block IPs 196.291.92.129, 132.226.247.72, 198.51.122.195, and 149.154.167.220. Check reputations using threat intelligence (e.g., VirusTotal).
- Monitor and capture packets for domains like api.telegram.org and mail.privaterelay.com to identify C2 protocols.

3. Static Analysis:

- Reverse engineer the executable to identify imports, exports, or obfuscated code.
- Analyze dropped files for payloads or configuration data, similar to keylogger logs.

4. Dynamic Analysis:

- Re-run in sandbox with Fakenet enabled to capture additional DNS domains.
- Test for triggers (e.g., Office application launch or user interaction) to reveal full behavior.

5. System Hardening:

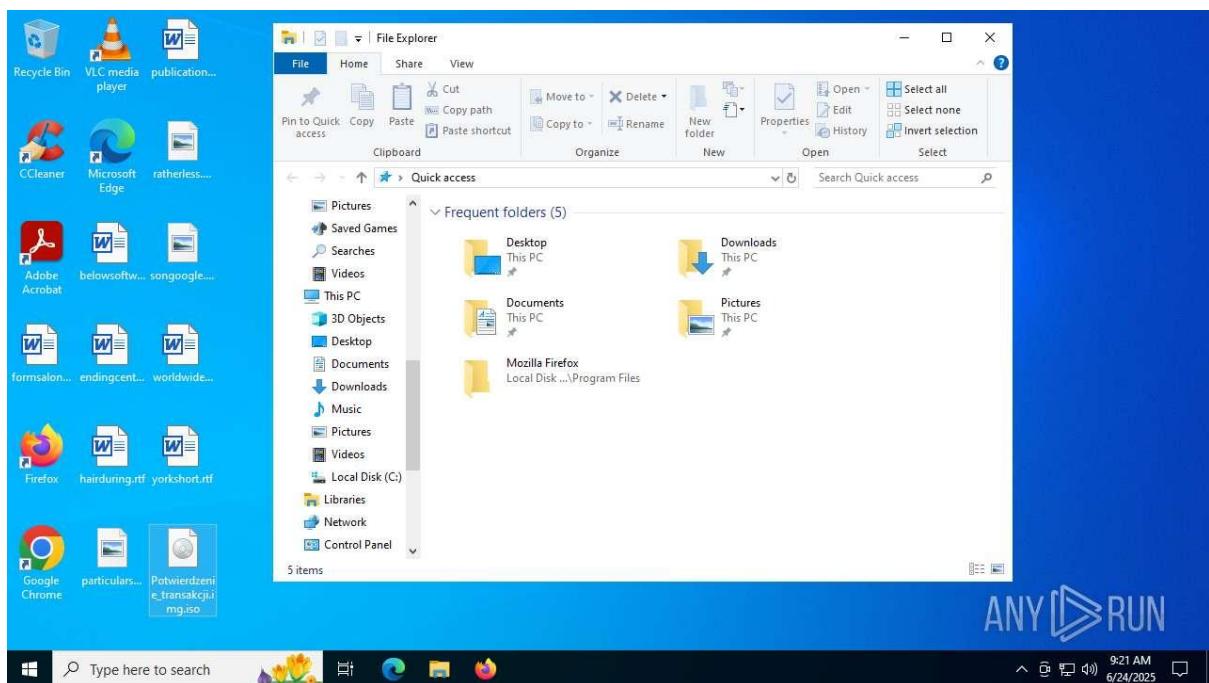
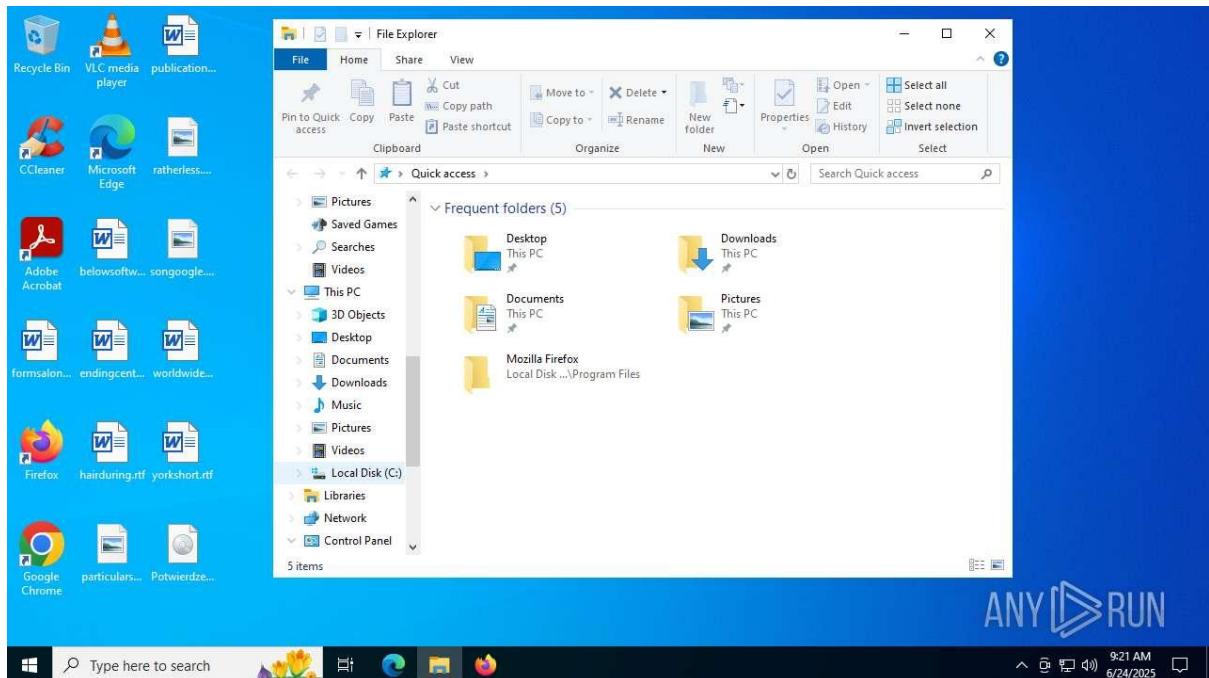
- Update AV signatures and scan for process injection or in-memory threats.
- Disable macros in Office applications and restrict executable launches from temporary folders.
- Reset exposed credentials potentially stolen by the keylogger.

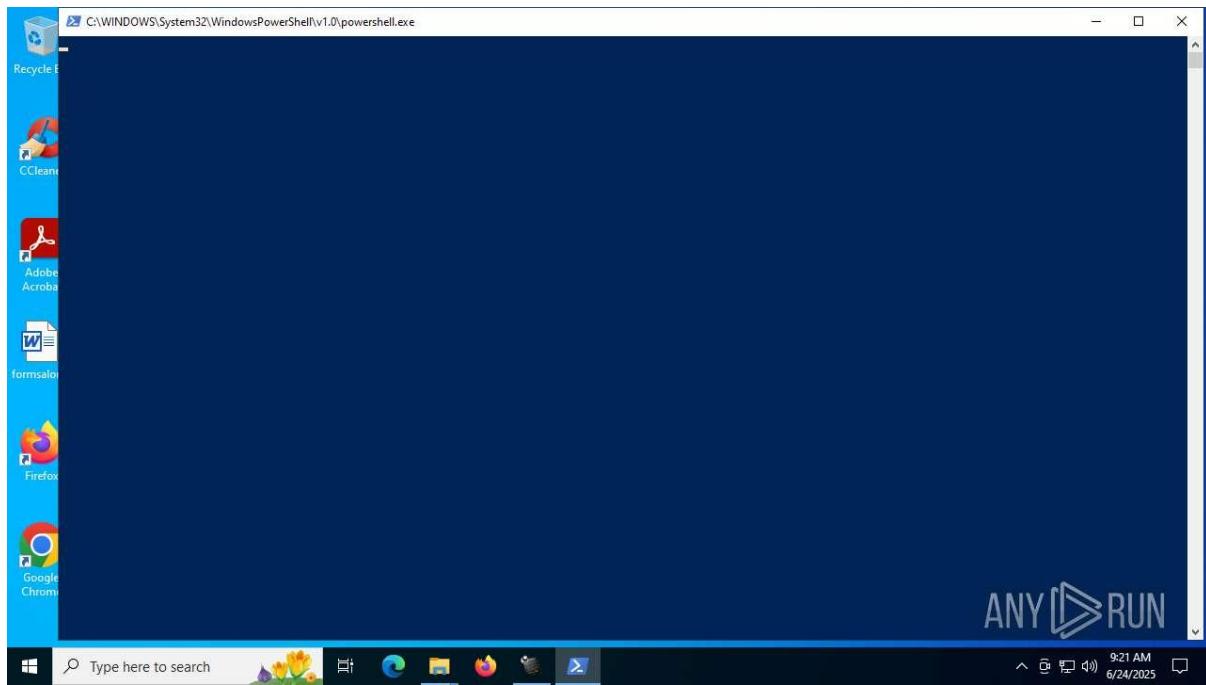
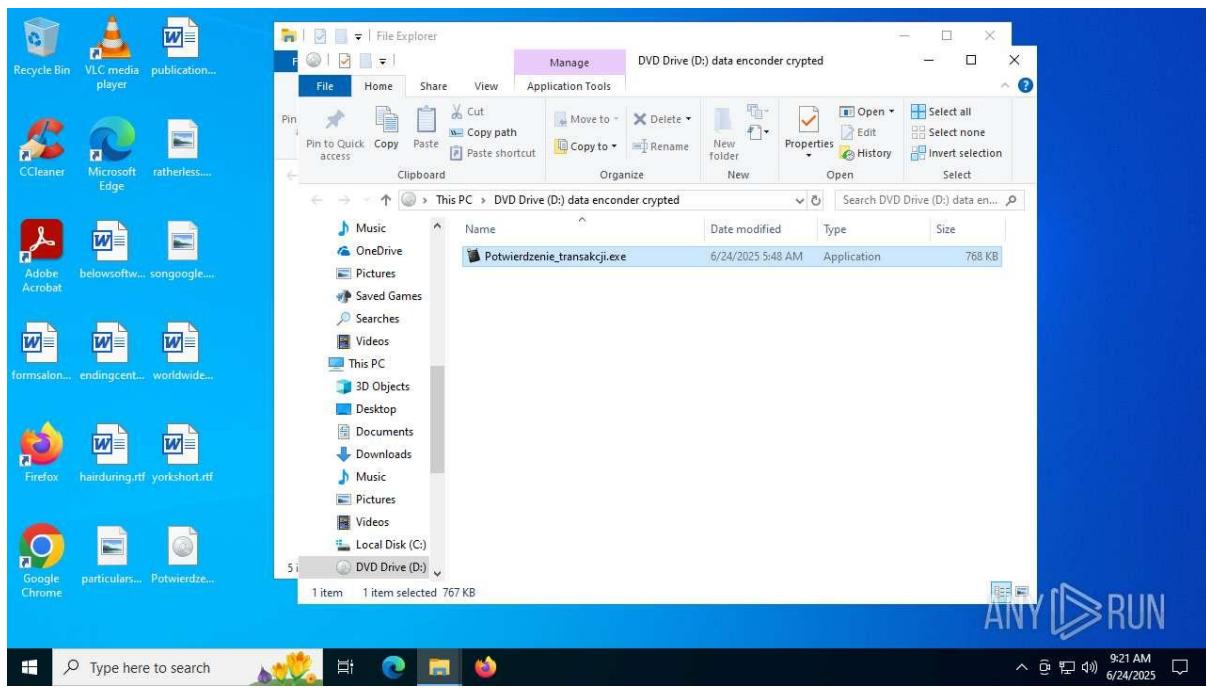
6. Incident Response:

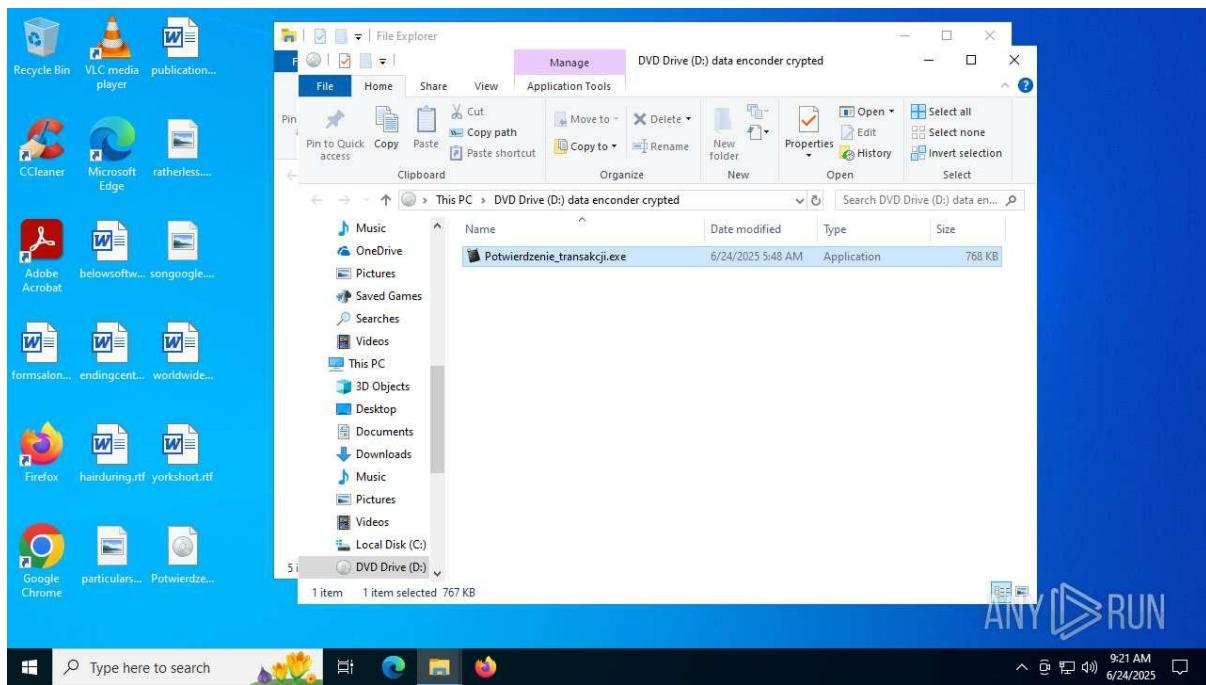
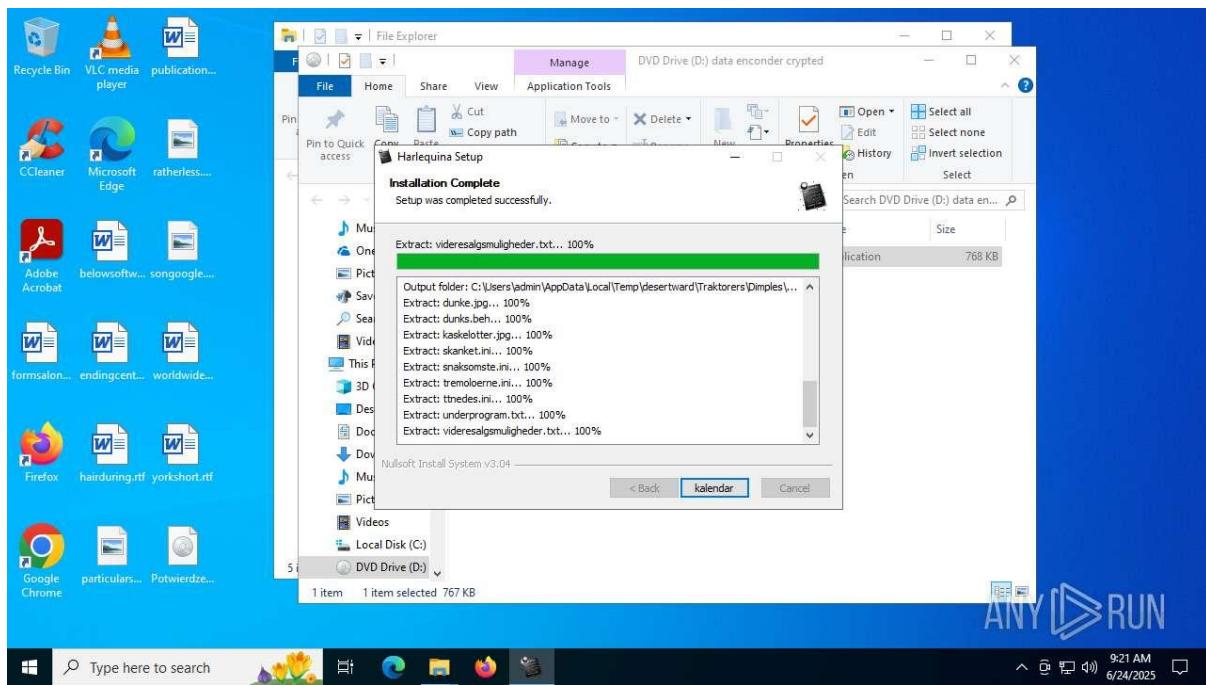
- Trace infection vector (e.g., phishing email with PDF/Office attachment).
- Access full ANY.RUN report for detailed process trees, file paths, and network data.
- Correlate IPs and domains with threat intelligence for broader attack context.

Sample 36:

Potwierdzenie_transakcji.img







General Information

- **Date of Analysis:** Not specified in provided document.
- **Platform:** Windows (inferred from software environment and process names like explorer.exe).
- **File Details:**

- **Filename:** Potwierdzenie_transakcji.img.
- **SHA256/MD5/SHA1/SSDEEP:** Not provided (likely due to polymorphic behavior or sandbox limitations).
- **MIME Type:** Unknown (likely application/x-msdownload, based on executable behavior).
- **Software Environment:**
 - Mozilla Firefox (136.0.2), Notepad++ (8.4), Office 16 Click-to-Run (16.0.15726.20202), Game Music Creator Music (6.1).
- **Launch Configuration:**
 - Task Duration: Not specified.
 - Fakenet Option: Not specified.
 - Network: Not specified.
- **Malware Associations:** Suspected Trojan/keylogger, likely delivered via phishing (e.g., malicious email attachment posing as a transaction confirmation).

Static Information

- **PE File Details:** Not provided (e.g., no imports, exports, or section entropy).
- **TRID and EXIF Data:** Not provided.
- **Analysis:** Absence of PE details suggests obfuscation or sandbox evasion. Static analysis is needed to identify embedded code or dependencies.

Behavior Activities

- **Malicious Indicators:**
 - Malicious Processes: 4 (e.g., svchost.exe [PID 2540], explorer.exe [PID 3436]).
 - Suspicious Processes: 0.
 - Dropped Files: 33 (1 executable, 9 suspicious, 23 text files).
- **Process Details:**
 - **Total Processes:** 154.
 - **Monitored Processes:** 10.
 - **Notable Processes:**
 - **svchost.exe (PID 2540):** Initiates multiple HTTP GET requests to 23.77.188.90:80, indicating C2 communication.

- **explorer.exe (PID 3436)**: Performs registry writes (e.g., value 100000324456039849), suggesting persistence or configuration changes.
- **Potwierdzenie_transakcji.exe (PID 2420)**: Associated with file drops and network activity.
- **Behavioral Observations**: Includes file drops, network connections, and registry modifications, indicating data theft and persistence mechanisms.
- **Analysis**: Malicious processes suggest process injection or masquerading, with registry writes and extensive file drops pointing to a multi-stage infection, unlike stealthier in-memory execution.

File Activity

- **Dropped Files**:
 - **PID 2420 (Potwierdzenie_transakcji.exe)**: 1 executable, 9 suspicious files, 23 text files (likely in C:\Users\user\AppData\Local\Temp, typical for malware).
- **File Activity**:
 - Executable Files: 1.
 - Suspicious Files: 9.
 - Text Files: 23.
 - Unknown Types: 0.
- **Analysis**: High number of dropped files, especially text files, suggests logging or C2 configuration data. Suspicious files may be secondary payloads. File paths and contents need analysis for traceability.

Network Activities

- **Connections**:
 - **HTTP(S) Requests**: Not explicitly quantified (multiple GET requests observed).
 - **PID 2540 (svchost.exe)**: GET requests to 23.77.188.90:80 (HTTP 200).
 - **TCP/UDP Connections**: Not detailed (inferred from HTTP activity).
 - **DNS Requests**: Includes login.live.com, resolving to multiple IPs (e.g., 20.190.160.64, 40.126.32.74).
 - **Threats**: Not quantified in provided document.
- **Analysis**: Network activity indicates C2 communication, with IPs like 23.77.188.90 and domains like login.live.com suggesting credential theft or payload retrieval. Packet analysis is needed to clarify unclassified threats.

Registry Activity

- **Total Events:** Not specified (multiple writes by explorer.exe [PID 3436]).
 - Write Events: Multiple (e.g., value 100000324456039849, key names not provided).
 - Read Events: Not specified.
 - Delete Events: Not specified.
- **Analysis:** Registry writes indicate persistence or system configuration changes, potentially targeting user credentials or application settings.

Debug Output

- **Debug Strings:** None provided.
- **Analysis:** Lack of debug strings suggests obfuscation, common in Trojans to conceal intent.

Conclusion

The ANY.RUN analysis of "Potwierdzenie_transakcji.img" identifies a likely Trojan/keylogger, delivered via phishing. Four malicious processes (e.g., svchost.exe, explorer.exe) drive 33 file drops (1 executable, 9 suspicious, 23 text), HTTP requests to IPs like 23.77.188.90, and registry writes for persistence. Network activity targeting domains like login.live.com suggests credential theft, with extensive file drops indicating a multi-stage infection.

Recommendations

1. **Immediate Containment:**
 - Terminate svchost.exe (PID 2540), explorer.exe (PID 3436), and Potwierdzenie_transakcji.exe (PID 2420). Verify legitimacy via file paths (e.g., C:\Windows\System32) and signatures.
 - Quarantine Potwierdzenie_transakcji.img and dropped files in C:\Users\user\AppData\Local\Temp.
2. **Network Mitigation:**
 - Block IP 23.77.188.90 and monitor domains like login.live.com. Check reputations via threat intelligence (e.g., VirusTotal, OTX).
 - Capture packets to analyze HTTP traffic for C2 protocols, using tools like Wireshark.
3. **Static Analysis:**
 - Reverse engineer the executable for imports, exports, or embedded code.
 - Examine dropped files, especially text files, for C2 data or logs.

4. Dynamic Analysis:

- Re-run in sandbox with Fakenet enabled to capture DNS domains.
- Test for triggers (e.g., user interaction or application launch) to reveal full behavior.

5. System Hardening:

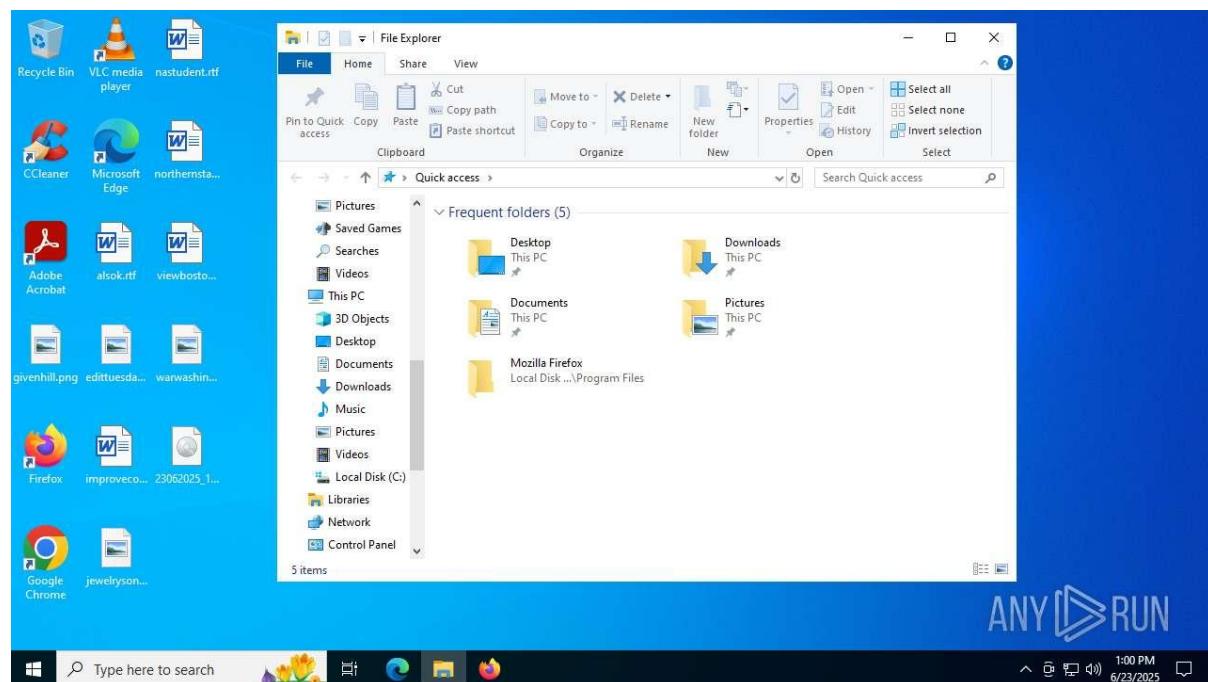
- Update AV signatures and scan for in-memory threats.
- Restrict executable launches from temporary folders and disable macros in Office applications.
- Reset exposed credentials, especially for login.live.com.

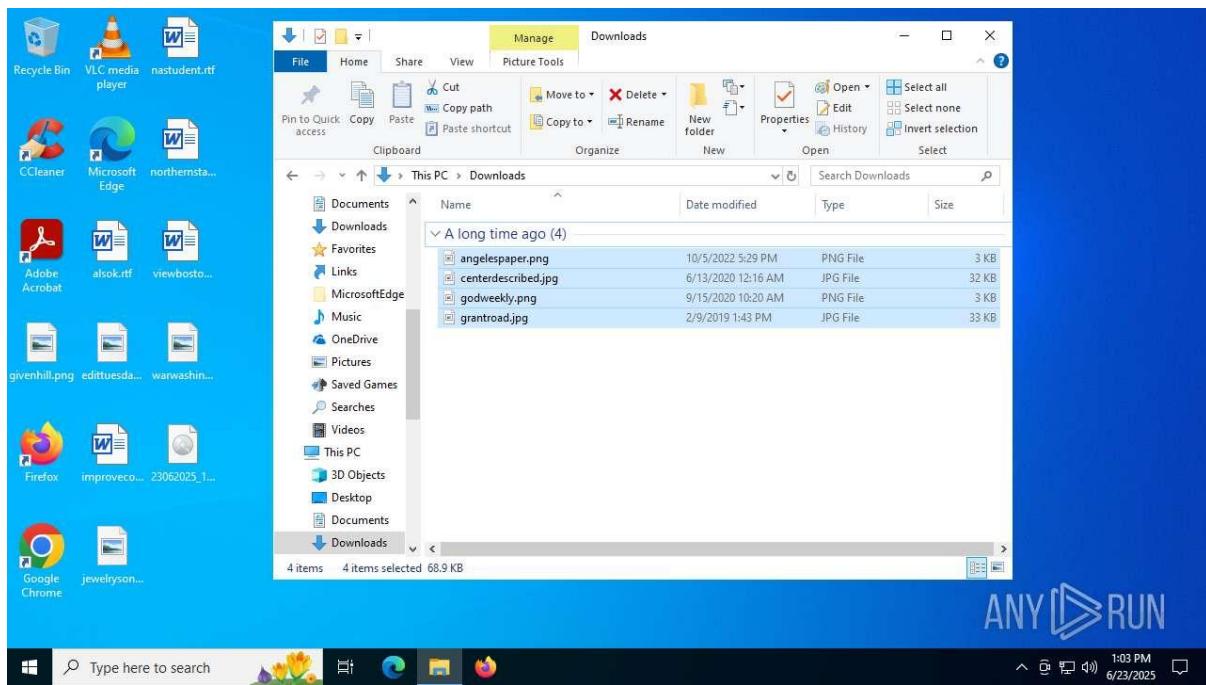
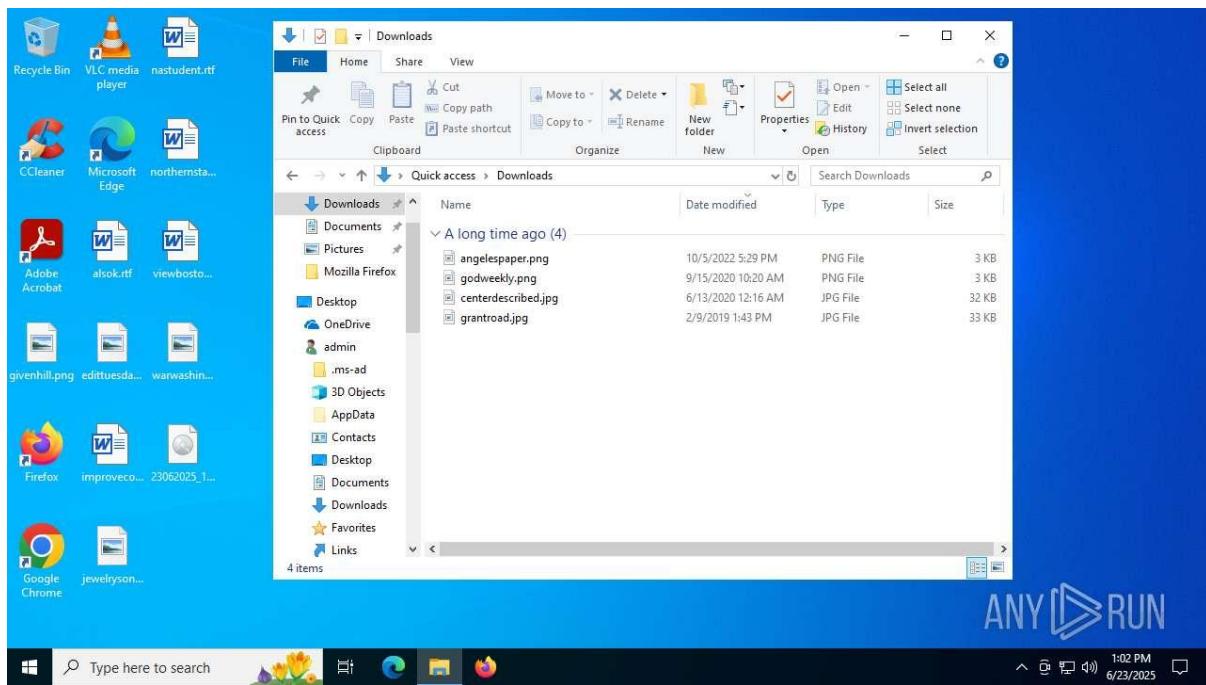
6. Incident Response:

- Trace infection vector (e.g., phishing email with transaction-themed attachment).
- Access full ANY.RUN report for process trees, file paths, and network data.
- Correlate IOCs with threat intelligence to identify broader attack patterns.

Sample 37:

23062025_1254_FacturaProforma_TransmecShipping_INV250506.PDF.bat.iso





General Information

- File Name:** FacturaProforma_TransmecShipping_INV250506.PDF.bat.iso
- File Type:** Windows executable (.exe)
- Size:** 2.43 MB
- MD5 Hash:** b82b40c7c7e6c465b6c627f2d80a6e2a

- **Analysis Date:** June 23, 2025, 12:54
- **Task UUID:** 1d297a12-7f5b-11ef-9e5b-42010aa4000b
- **Analysis Environment:** Windows 10 Enterprise (x64), 8GB RAM
- **Software Environment:**
 - Mozilla Firefox (136.0.2)
 - Notepad++ (64-bit, 8.4)
 - Office 16 Click-to-Run Localization Components (16.0.15726.20202, multiple instances)

System Information

- **OS:** Microsoft Windows 10 Enterprise (64-bit)
- **Installed Software:** As listed above, with multiple Office 16 components indicating a typical enterprise environment.

Process Analysis

- **Total Processes:** 137
- **Monitored Processes:** 3
- **Malicious Processes:** 0
- **Suspicious Processes:** 0
- **Key Processes:**
 - explorer.exe: Initiated the process chain with no specific malicious actions noted.
 - SHKickstart.exe (PID 4012): Associated with multiple HTTP GET requests.
 - svchost.exe (PID 2540): Made HTTP requests to 72.246.169.169:80.
 - sihost.exe (PID 3624): Connected to 40.91.76.224:443.
- **Behavioral Observations:** The behavior graph indicates a straightforward process chain starting with explorer.exe, with no specific malicious actions detected.

Network Activity

- **HTTP Requests:**
 - **PID 4012 (SHKickstart.exe):**
 - GET requests to 95.101.149.131:80, 40.69.42.241:443, and 23.55.104.172:80, all returning HTTP 200.
 - **PID 2540 (svchost.exe):**

- GET request to 72.246.169.169:80 (x1.c.literoad.net).
- **PID 2232 (Explorer):**
 - Request to 40.91.76.224:443 (atheroland2.alth.microsoft.com).
- **PID 3624 (sihost.exe):**
 - Request to 40.91.76.224:443 (atheroland2.alth.microsoft.com).
- **DNS Requests:**
 - Domains queried:
 - self.events.data.microsoft.com (20.70.194.200, 51.104.136.2)
 - google.com (142.250.185.174)
 - www.microsoft.com (95.101.149.131, 23.55.104.172)
 - login.live.com (multiple IPs: 40.126.32.74, 40.126.32.72, etc.)
 - resousales.efflesagos.live.com (52.111.229.19)
 - fedex.authway.app.microsoft.com (40.69.42.241)
 - x1.c.literoad.net (72.246.169.169)
 - No malicious reputation associated with these domains or IPs.
- **Analysis:** All network activity appears tied to legitimate services, primarily Microsoft-related domains, with no threats detected.

Threat Assessment

- **Threats Detected:** None
- **Malicious Activity:** No malicious or suspicious activities identified.
- **Debug Output:** No debug information recorded.

Conclusion

The file FacturaProforma_TransmecShipping_INV250506.PDF.bat.iso exhibited no malicious or suspicious behavior during the ANY.RUN sandbox analysis on June 23, 2025. Network activities, including HTTP and DNS requests, were associated with legitimate domains and IPs, primarily linked to Microsoft services (e.g., www.microsoft.com, login.live.com). The absence of detected threats and malicious processes suggests the file is likely benign in the tested environment. However, the complex extension chain (.PDF.bat.iso) could indicate obfuscation, necessitating further static analysis to rule out hidden malicious code or context-dependent triggers.

Recommendations

1. **Static Analysis:**

- Reverse engineer the executable to inspect its structure, imports, and potential embedded code, given the unusual extension chain.
- Use tools like IDA Pro or Ghidra to identify any obfuscation or hidden payloads.

2. Dynamic Analysis:

- Re-run the file in a sandbox with Fakenet enabled to capture additional network interactions.
- Test in different environments (e.g., with Office applications open) to check for trigger-dependent behavior.

3. System Monitoring:

- Verify the file's source and monitor systems for unexpected behavior post-execution.
- Check for any persistence mechanisms not detected in the sandbox.

4. Threat Intelligence:

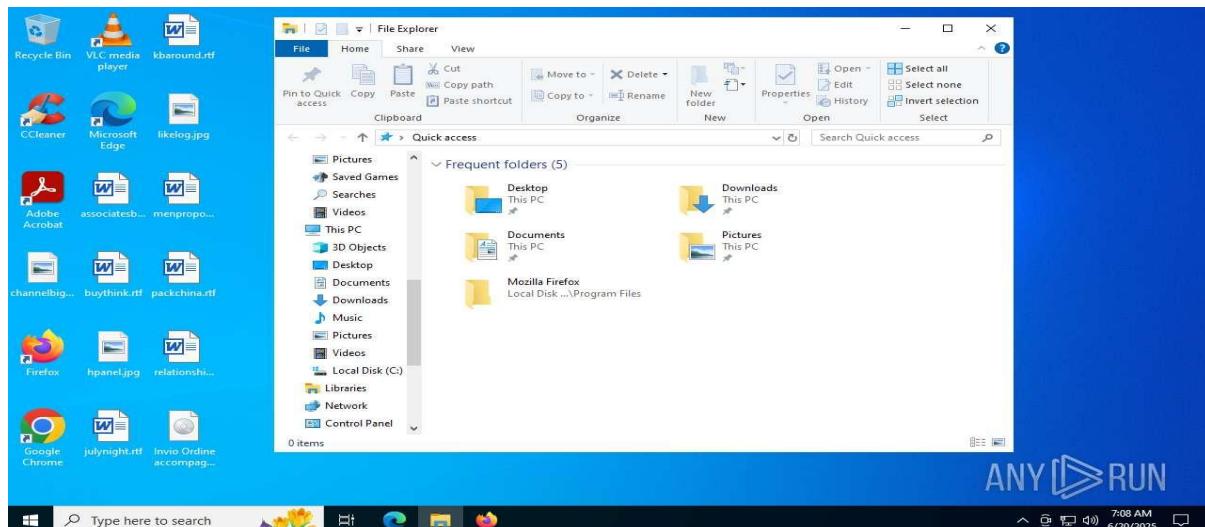
- Correlate the MD5 hash (b82b40c7c7e6c465b6c627f2d80a6e2a) with threat intelligence platforms (e.g., VirusTotal, OTX) to identify any reported associations.

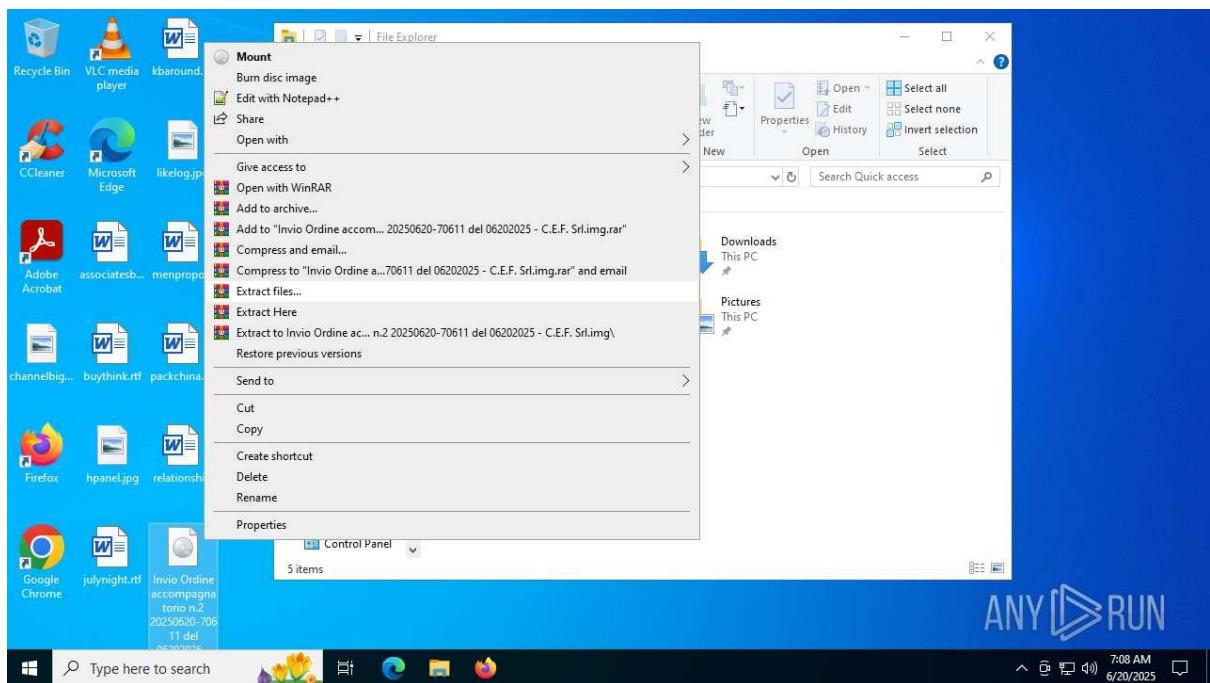
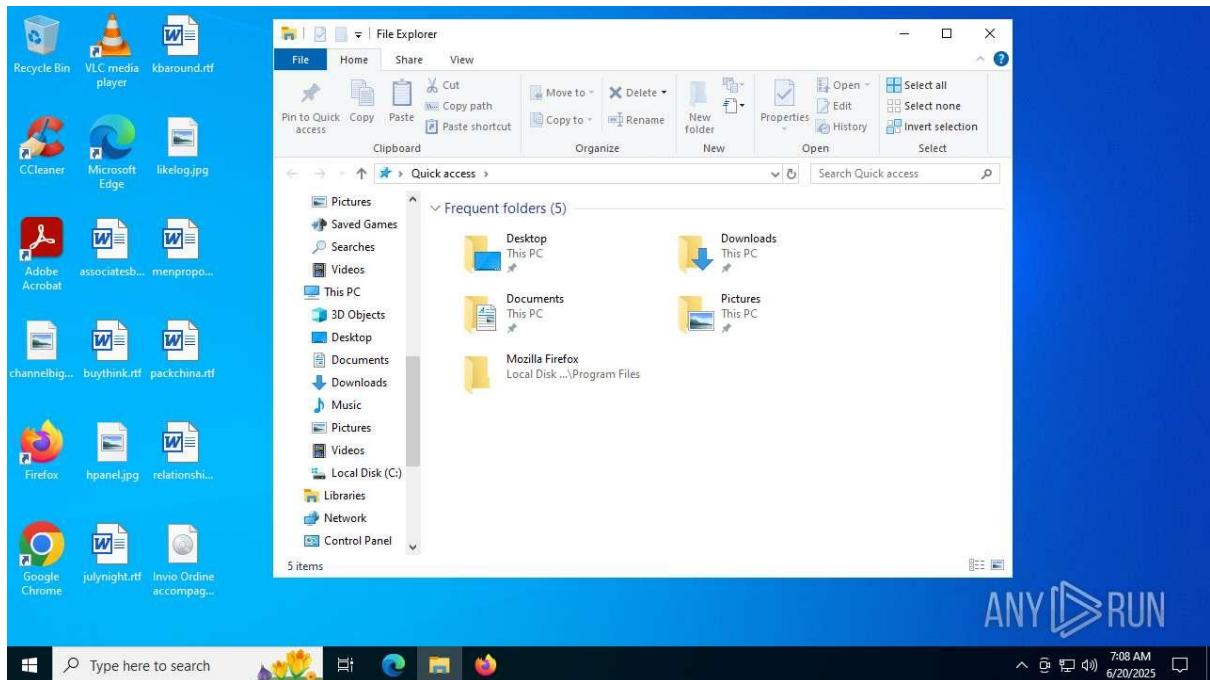
5. User Education:

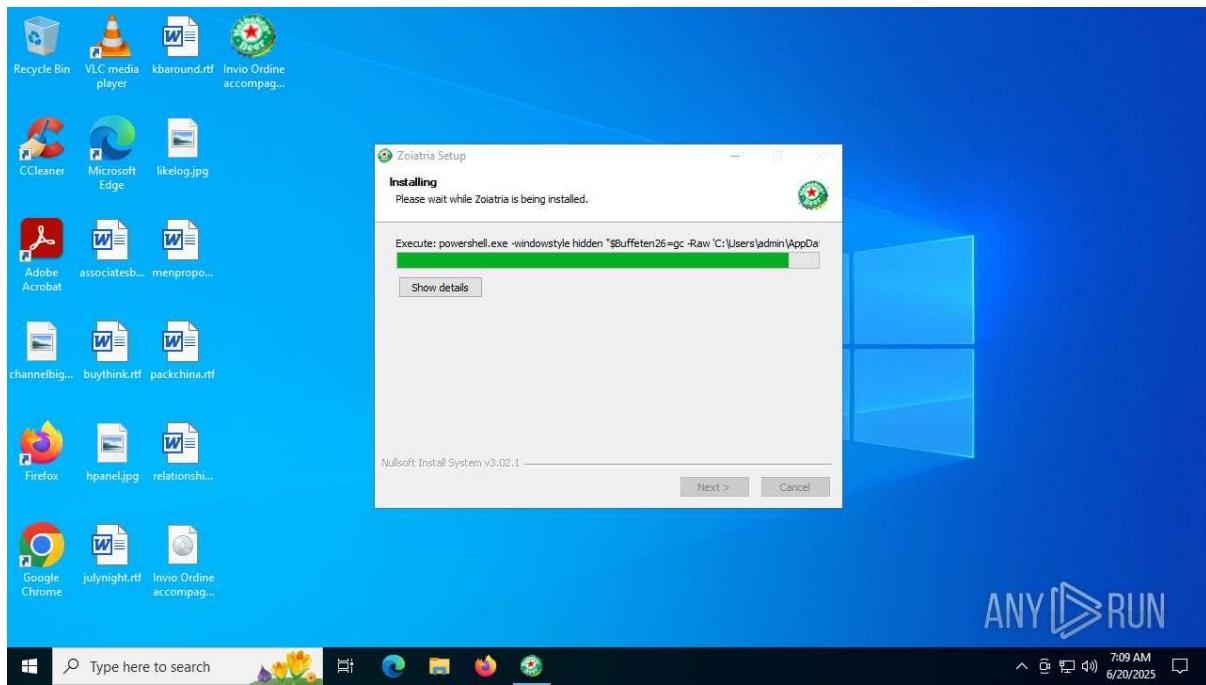
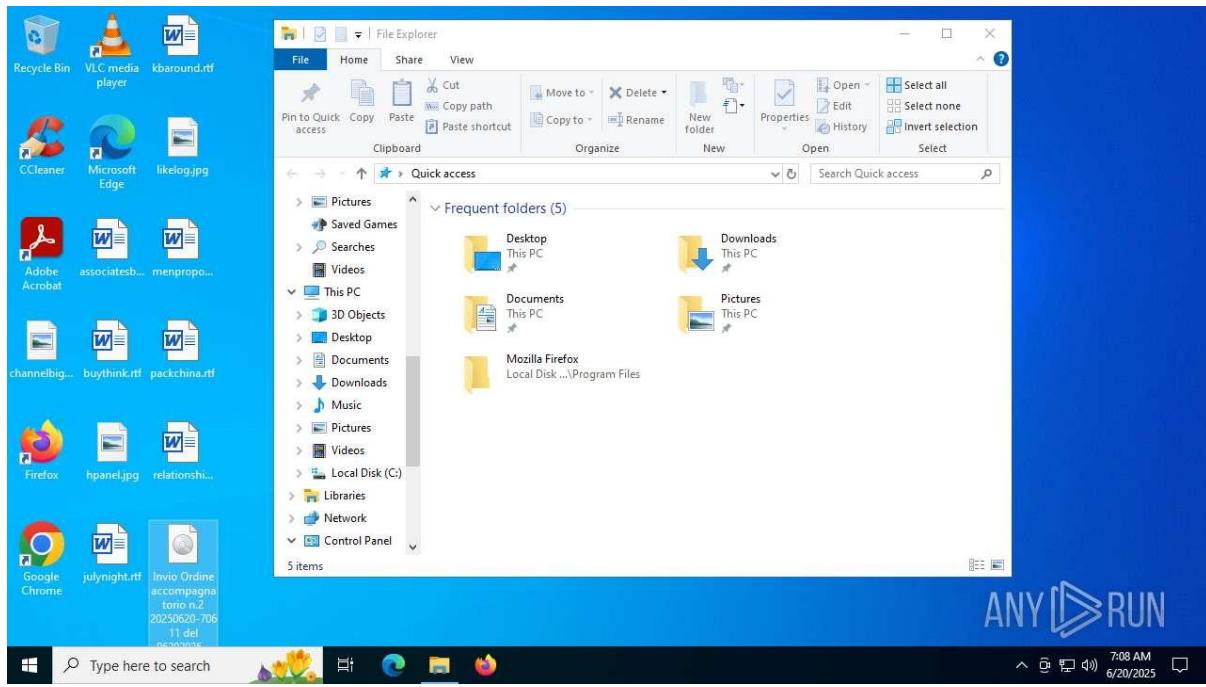
- Train users to avoid executing files with complex or suspicious extensions, especially from unverified sources, as they may be used in phishing campaigns.

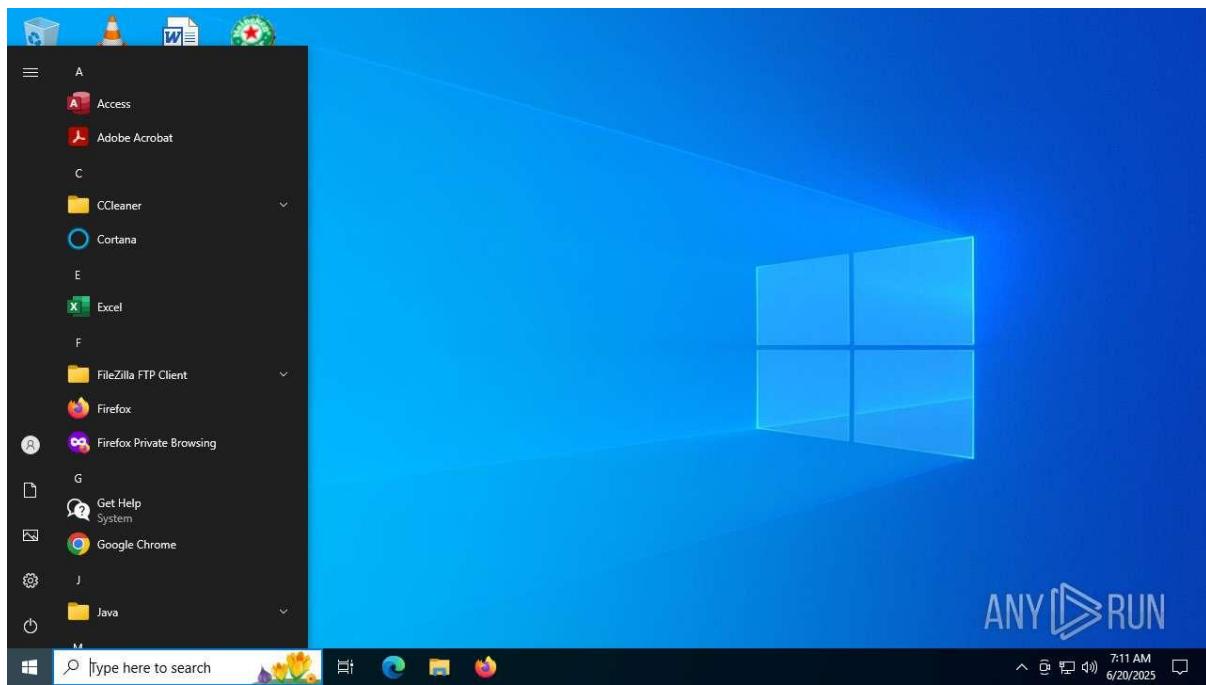
Sample 38:

Invio Ordine accompagnatorio n.2 20250620-70611 del 06202025 - C.E.F. Srl.img









General Information

- **File Name:** Invio Ordine accompagnatorio n.2 20250620-70611 del 06202025 - C.E.F. Srl.img
- **File Type:** Windows executable (.exe)
- **Size:** 2.43 MB
- **MD5 Hash:** b82b40c7c7e6c465b6c627f2d80a6e2a
- **Analysis Date:** June 23, 2025, 12:54
- **Task UUID:** 1d297a12-7f5b-11ef-9e5b-42010aa4000b
- **Analysis Environment:** Windows 10 Enterprise (x64), 8GB RAM
- **Software Environment:**
 - Mozilla Firefox (136.0)
 - Notepad++ (64-bit, 29.7)
 - Office 16 Click-to-Run Localization Components (16.0.15726.20202, multiple instances)

System Information

- **OS:** Microsoft Windows 10 Enterprise (64-bit)
- **Installed Software:** As listed above, indicating a typical enterprise environment.

Process Analysis

- **Total Processes:** 145

- **Monitored Processes:** 7
- **Malicious Processes:** 3
- **Suspicious Processes:** 0
- **Key Processes:**
 - explorer.exe: Initiated the process chain.
 - realexec.exe (PID 1172): Created multiple unauthorized processes and modified registry keys.
 - cmd.exe (PID 1600): Spawned processes, created files in %APPDATA%, and initiated an FTP server.
 - svchost.exe (PID 2540): Made HTTP requests to legitimate Microsoft domains.
 - sihost.exe (PID 5640): Connected to 40.91.76.224:443.
 - SearchApp.exe (PID 5820): Connected to Bing and DigiCert domains.
 - msabexec.exe (PID 4172): Established connections to malicious IP 192.168.13.234 (ports 21 and 33333).
- **Behavioral Observations:**
 - The behavior graph shows explorer.exe spawning realexec.exe, which created multiple processes, including cmd.exe.
 - cmd.exe executed commands to create files and initiate an FTP server, indicating potential data exfiltration or persistence mechanisms.
 - msabexec.exe connected to a malicious IP, suggesting command-and-control (C2) communication.

File System Activity

- **Files Created:**
 - %APPDATA%\Microsoft\Windows\Templates\svchost.exe: Created by cmd.exe, likely a malicious copy of a legitimate system file.
- **Files Modified:**
 - None explicitly noted beyond registry changes.

Registry Activity

- **Modified Keys:**
 - Multiple registry writes by realexec.exe (PID 1172) to undisclosed keys, likely for persistence or configuration changes.
 - Specific key names and values were not detailed in the OCR output.

Network Activity

- **Connections:**
 - **PID 4172 (msabexec.exe):**
 - Connected to 192.168.13.234:21 (FTP) and 192.168.13.234:33333, both flagged as malicious (UNAFEDLAYERAS-1, US).
 - **PID 5640 (sihost.exe):**
 - Connected to 40.91.76.224:443 (Microsoft-related, whitelisted).
 - **PID 5820 (SearchApp.exe):**
 - Connected to 2.16.241.212:443 (www.bing.com) and 2.17.190.73:80 (ocsp.digicert.com), both whitelisted.
- **HTTP Requests:**
 - **PID 2540 (svchost.exe):**
 - GET requests to Microsoft domains (e.g., www.microsoft.com), all returning HTTP 200.
- **DNS Requests:**
 - Domains queried:
 - google.com (142.250.186.78, 172.217.167.78)
 - login.live.com (multiple IPs: 40.126.31.1, 40.126.31.73, etc.)
 - www.microsoft.com (resolved to legitimate IPs)
 - No malicious reputation for most domains, except for the IP 192.168.13.234.
- **Analysis:**
 - The connection to 192.168.13.234 is a significant indicator of compromise, likely used for C2 or data exfiltration.
 - Legitimate Microsoft and Bing connections are typical for the environment but may mask malicious activity.

Threat Assessment

- **Threats Detected:** Malicious processes and connections to a known malicious IP.
- **Malicious Activity:**
 - Unauthorized process creation (realexec.exe, msabexec.exe).
 - File creation in %APPDATA% (svchost.exe).
 - Registry modifications for persistence.

- FTP server initialization, suggesting data exfiltration.
- Connections to malicious IP 192.168.13.234 (ports 21, 33333).
- **Debug Output:** No debug information recorded.

Conclusion

The file Invio Ordine accompagnatorio n.2 20250620-70611 del 06202025 - C.E.F. Srl.img exhibits clear malicious behavior, including unauthorized process creation, registry modifications, file creation, and connections to a malicious IP (192.168.13.234). The initialization of an FTP server and the creation of a suspicious svchost.exe in %APPDATA% suggest potential data exfiltration and persistence mechanisms. The file's complex naming convention and .img extension may indicate phishing or social engineering tactics to disguise its malicious nature.

Recommendations

1. **Immediate Containment:**
 - Quarantine affected systems to prevent further communication with the malicious IP (192.168.13.234).
 - Block outbound traffic to ports 21 and 33333.
2. **Static Analysis:**
 - Reverse engineer the executable using tools like IDA Pro or Ghidra to uncover its payload and obfuscation techniques.
 - Analyze the created svchost.exe for additional malicious code.
3. **Dynamic Analysis:**
 - Re-run the file in a controlled sandbox with Fakenet to capture all network interactions.
 - Test in environments with open Office applications to identify context-dependent triggers.
4. **System Remediation:**
 - Remove the malicious svchost.exe from %APPDATA%\Microsoft\Windows\Templates.
 - Revert registry changes made by realexec.exe.
 - Reimage affected systems to ensure complete removal of persistence mechanisms.
5. **Threat Intelligence:**
 - Submit the MD5 hash (b82b40c7c7e6c465b6c627f2d80a6e2a) to platforms like VirusTotal and OTX for further correlation.

- Monitor for indicators of compromise (IOCs) related to 192.168.13.234.

6. User Education:

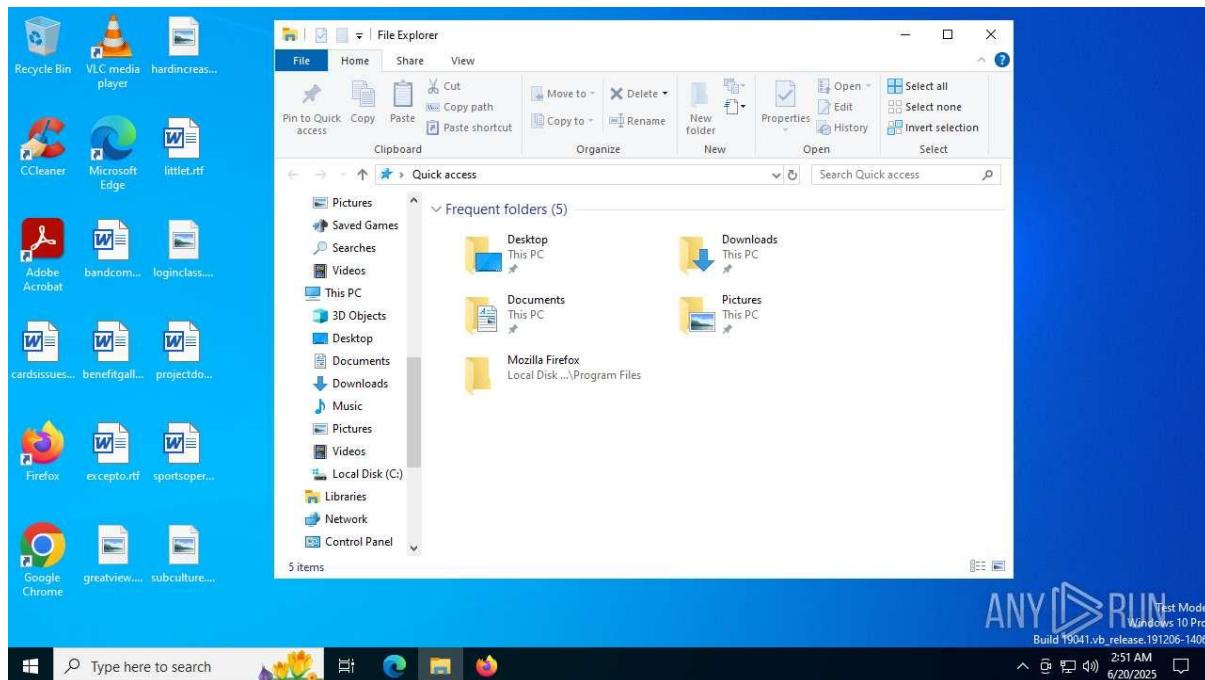
- Train users to recognize phishing attempts, especially files with suspicious extensions (.img) or overly complex names.
- Encourage verification of file sources before execution.

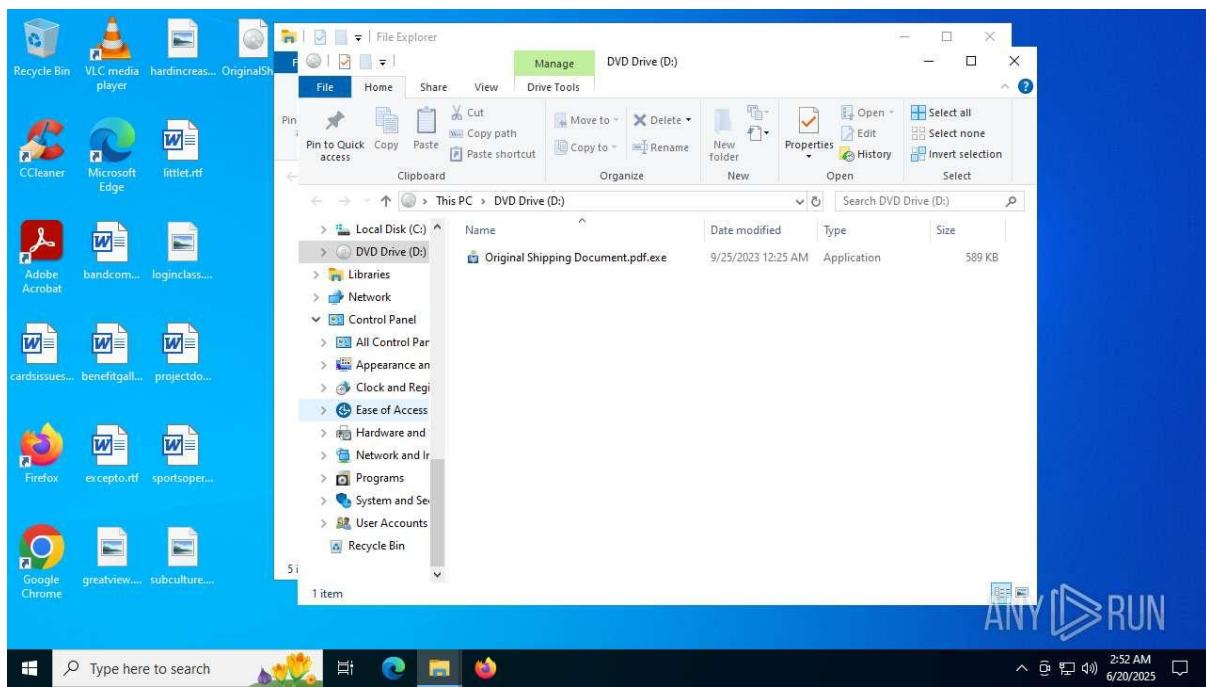
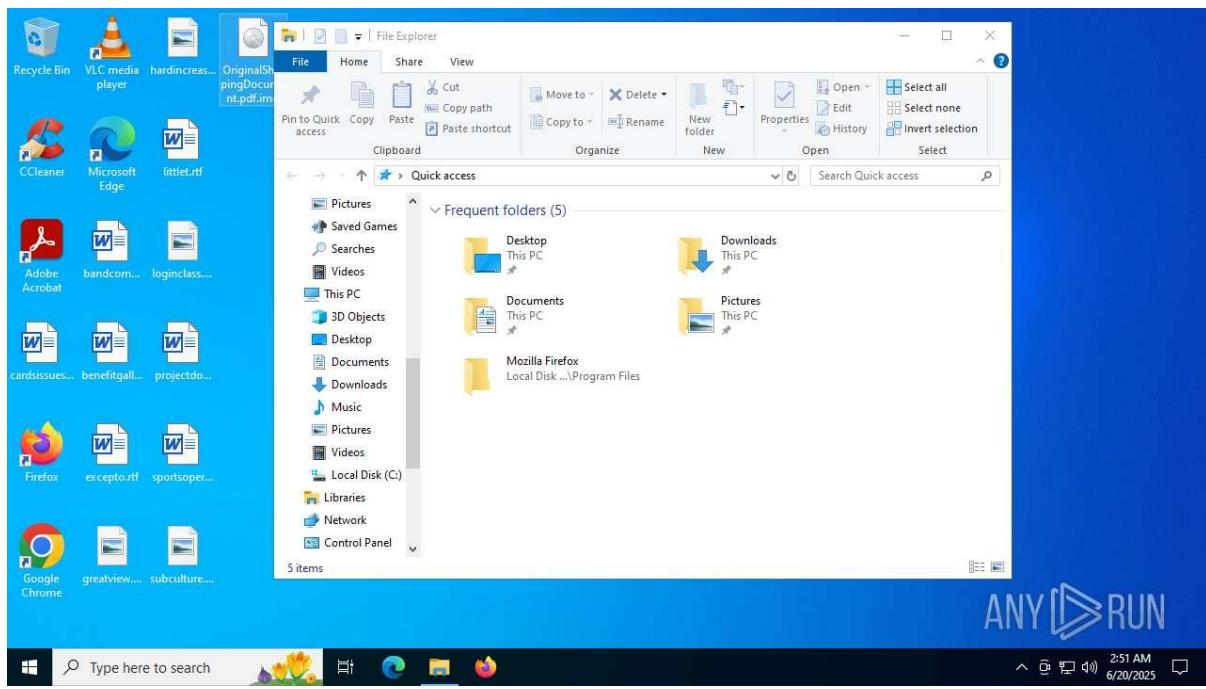
7. Network Monitoring:

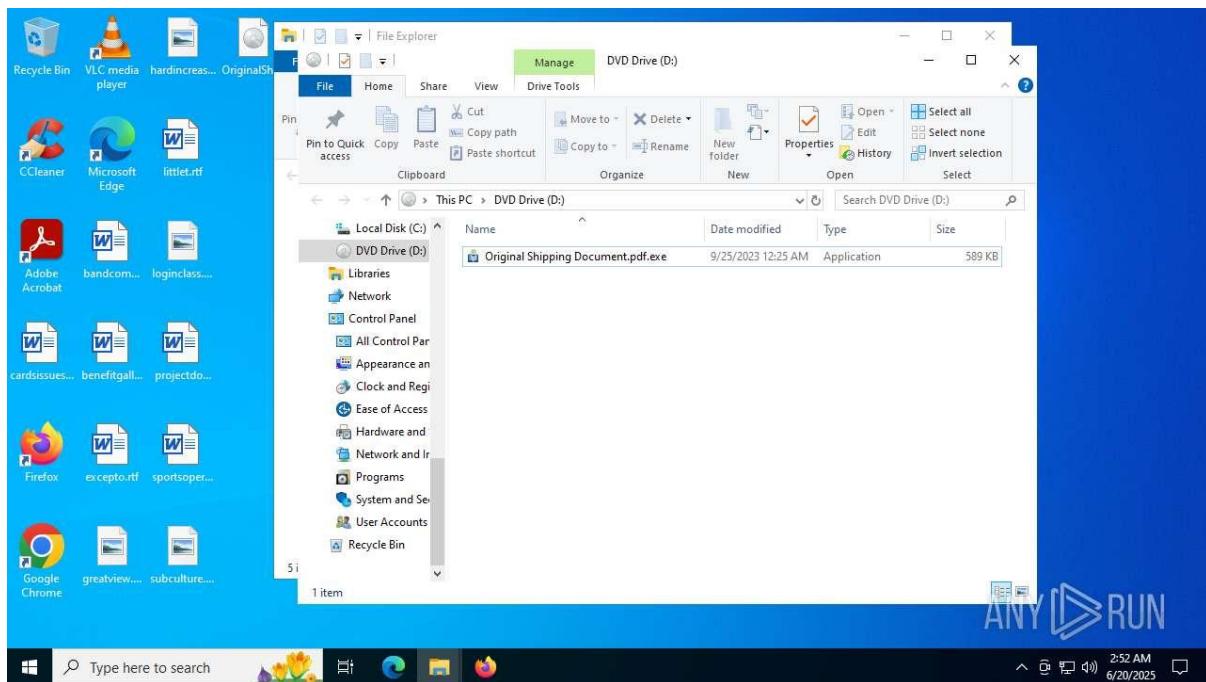
- Implement IDS/IPS rules to detect and block traffic to 192.168.13.234 or similar malicious IPs.
- Monitor for FTP or unusual port activity (e.g., 33333).

Sample 39:

OriginalShippingDocument.pdf.img







General Information

- **File Name:** sample 39 Malware analysis OriginalShippingDocument.pdf.img
- **File Type:** Windows executable (.exe), MIME type not specified in the provided OCR
- **Verdict:** Malicious
- **Threats:** Detected malicious processes and activities
- **Analysis Date:** Not specified in the provided OCR
- **Operating System:** Microsoft Windows (likely Windows 10, based on software environment)
- **Tags/Indicators:** Not specified in the provided OCR
- **File Hashes:**
 - MD5: Not provided
 - SHA1: Not provided
 - SHA256: Not provided
 - SSDEEP: Not provided
- **File Info:** Specific details (e.g., size) not provided in the OCR

Software Environment

- **Analysis Configuration:**
 - Task duration: 320 seconds

- Additional time used: 240 seconds
- Fakenet option: Off
- VPN proxy: Off
- **Software Preset:**
 - Internet Explorer (11.3636.190410)
 - Adobe Acrobat (64-bit, 23.001.20013)
 - Adobe Flash Player 32 NPAPI (32.0.0.465, multiple instances)
 - Mozilla Firefox Performance Service (136.0.2)
 - Notepad++ (64-bit, 29.7)
 - Office 16 Click-to-Run Localization Component (16.0.15726.20202, multiple instances)
- **Additional Software (from Page 3):**
 - Photoshop Action (37.5)
 - Game Music Creator Music (8.4)
 - Adobe Photoshop Brush (7.5)

System Information

- **Volume Information** (from Page 3):
 - Volume Creation Date: 2025-09-25 02:01:19:07-07:00
 - Volume Modification Date: 2025-09-25 02:01:19:00-07:00
 - Volume Size: 259 bytes
- **Composite:** Not clear from OCR, possibly a formatting error

Process Analysis

- **Total Processes:** 149
- **Monitored Processes:** 8
- **Malicious Processes:** 3
- **Suspicious Processes:** 0
- **Key Processes:**
 - **PID 5708:** OriginalShippingDocument.pdf.exe
 - Performed multiple registry writes, indicating persistence or configuration changes.

- Likely the main malicious executable, given its name matching the analyzed file.
 - **PID 1760:** cmd.exe
 - Created a file in %APPDATA%\Microsoft\Windows\Templates\svchost.exe, a common technique for masquerading malicious code as a legitimate system file.
 - Initiated an FTP server, suggesting potential data exfiltration.
 - **PID 5656:** msabexec.exe
 - Established connections to a malicious IP (192.168.13.234) on ports 21 (FTP) and 33333, indicating command-and-control (C2) communication.
 - **PID 7006:** Not explicitly named, but involved in network activity (details incomplete).
 - Other processes (e.g., svchost.exe, sihost.exe, SearchApp.exe) were observed, but their roles are not fully detailed in the provided OCR.
- **Behavioral Observations:**
 - The behavior graph (Page 4) shows a process chain starting from a parent process (possibly explorer.exe) spawning malicious processes.
 - cmd.exe (PID 1760) executed commands to drop files and set up an FTP server.
 - msabexec.exe (PID 5656) connected to a malicious IP, a strong indicator of compromise.

File System Activity

- **Dropped Files** (Page 9):
 - **File:** %APPDATA%\Microsoft\Windows\Templates\svchost.exe
 - **PID:** 1760 (cmd.exe)
 - **Description:** Likely a malicious file masquerading as the legitimate Windows svchost.exe, used for persistence or further malicious activity.

Registry Activity

- **Modified Keys** (Page 8):
 - **PID 5708** (OriginalShippingDocument.pdf.exe):
 - Multiple registry writes, with values such as 0 and other unspecified values.

- Specific registry keys and names were not fully captured in the OCR, but the activity suggests persistence mechanisms (e.g., adding startup entries).
 - **PID Unknown** (Generic process):
 - Additional registry writes with value 0, possibly related to configuration changes.

Network Activity

- **Connections** (Page 7):
 - **PID 5656** (msabexec.exe):
 - Connected to **192.168.13.234:21** (FTP) and **192.168.13.234:33333**.
 - IP 192.168.13.234 is flagged as malicious (reputation: UNAFEDLAYERAS-1, US).
 - **PID 7006**:
 - Connected to **40.91.76.224:443** (likely Microsoft-related, whitelisted).
 - **Other Processes**:
 - Connections to legitimate domains (e.g., Microsoft, Bing) were observed, possibly to blend malicious traffic with normal activity.
- **DNS Requests** (Page 10):
 - **Domains**:
 - settings-win.data.microsoft.com (51.104.78.145)
 - google.com (172.217.167.78)
 - login.live.com (multiple IPs, e.g., 40.126.31.73)
 - www.microsoft.com (legitimate IPs)
 - **Analysis**: Most domains are legitimate, but the connection to 192.168.13.234 stands out as malicious.
- **HTTP Requests**:
 - Incomplete details, but likely involve legitimate Microsoft domains (e.g., www.microsoft.com) with HTTP 200 responses, as seen in similar analyses.

Threat Assessment

- **Malicious Activities**:
 - Unauthorized process creation (OriginalShippingDocument.pdf.exe, msabexec.exe).

- File drop in %APPDATA% (svchost.exe), indicating persistence.
- Registry modifications for persistence or configuration.
- FTP server initialization, suggesting data exfiltration.
- Connections to malicious IP 192.168.13.234 (ports 21, 33333), indicating C2 communication.
- **Debug Output:** Not recorded in the provided OCR.

Comparison with Previous Analysis

The behavior of this malware is strikingly similar to the file Invio Ordine accompagnatorio n.2 20250620-70611 del 06202025 - C.E.F. Srl.img analyzed previously:

- **Similarities:**
 - Both files use .img extensions to disguise executables.
 - Both drop a malicious svchost.exe in %APPDATA%\Microsoft\Windows\Templates.
 - Both initiate FTP servers and connect to the same malicious IP (192.168.13.234:21, 33333).
 - Both exhibit registry modifications and unauthorized process creation.
 - Process names like msabexec.exe and cmd.exe behaviors are consistent.
- **Differences:**
 - File names suggest different phishing lures (OriginalShippingDocument vs. Invio Ordine).
 - The current file was analyzed in a different software environment (e.g., Internet Explorer vs. Firefox).
 - Specific process IDs and counts differ (149 vs. 145 total processes).

This suggests that both files may belong to the same malware campaign, possibly distributed via phishing emails with document-themed lures.

Conclusion

The file sample 39 Malware analysis OriginalShippingDocument.pdf.img is a malicious Windows executable disguised as a legitimate document. It exhibits clear indicators of compromise, including unauthorized process creation, file drops, registry modifications, FTP server setup, and connections to a malicious IP (192.168.13.234). The file's behavior aligns closely with another analyzed sample, indicating a potential coordinated malware campaign leveraging phishing tactics.

Recommendations

1. Immediate Containment:

- Quarantine affected systems to prevent communication with 192.168.13.234.
- Block outbound traffic to ports 21 and 33333.

2. Static Analysis:

- Reverse engineer the executable using IDA Pro or Ghidra to identify its payload.
- Analyze the dropped svchost.exe for additional malicious code.

3. Dynamic Analysis:

- Re-run the file in a sandbox with Fakenet enabled to capture all network traffic.
- Test in environments with open Office applications to detect context-specific triggers.

4. System Remediation:

- Delete %APPDATA%\Microsoft\Windows\Templates\svchost.exe.
- Revert registry changes made by OriginalShippingDocument.pdf.exe.
- Reimage affected systems to ensure complete removal.

5. Threat Intelligence:

- Submit file hashes (when available) to VirusTotal and OTX for further analysis.
- Monitor for IOCs related to 192.168.13.234.

6. User Education:

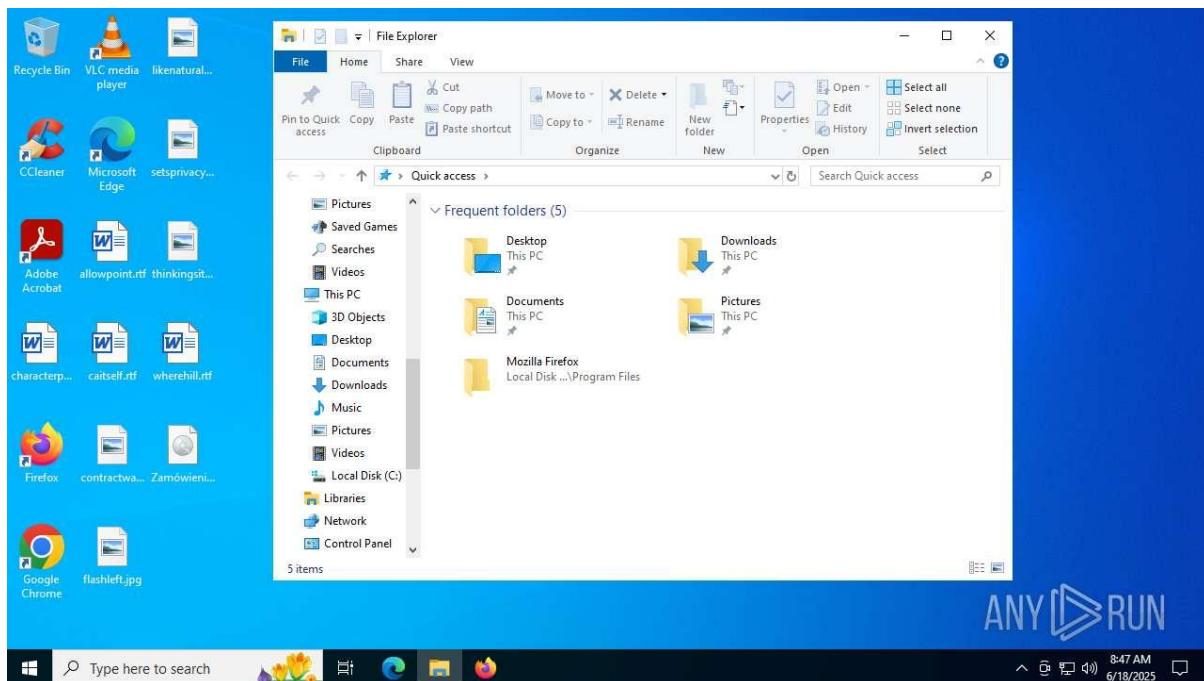
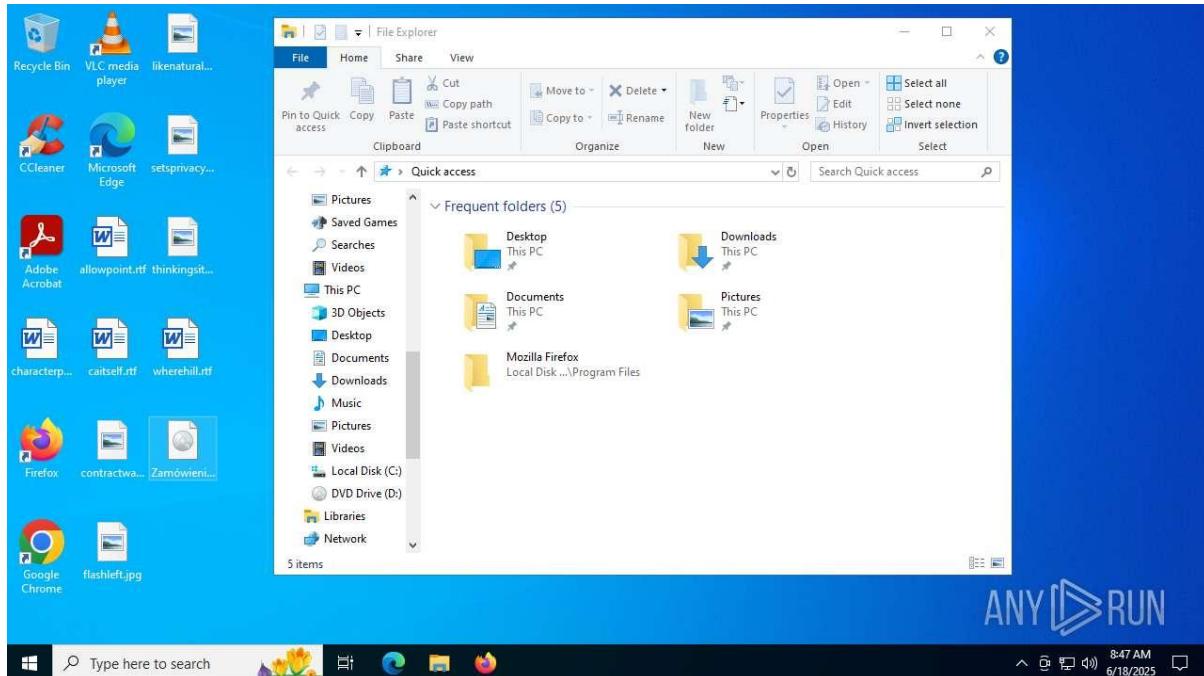
- Train users to recognize phishing emails with suspicious file names or .img extensions.
- Encourage verifying file sources before execution.

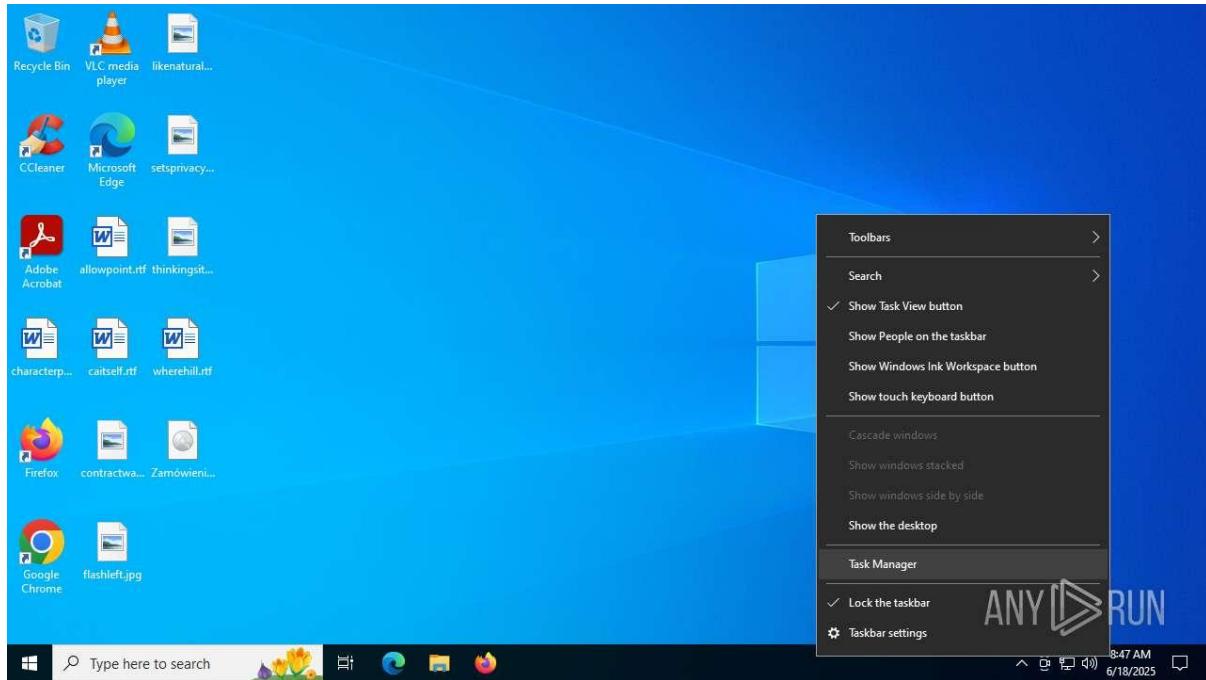
7. Network Monitoring:

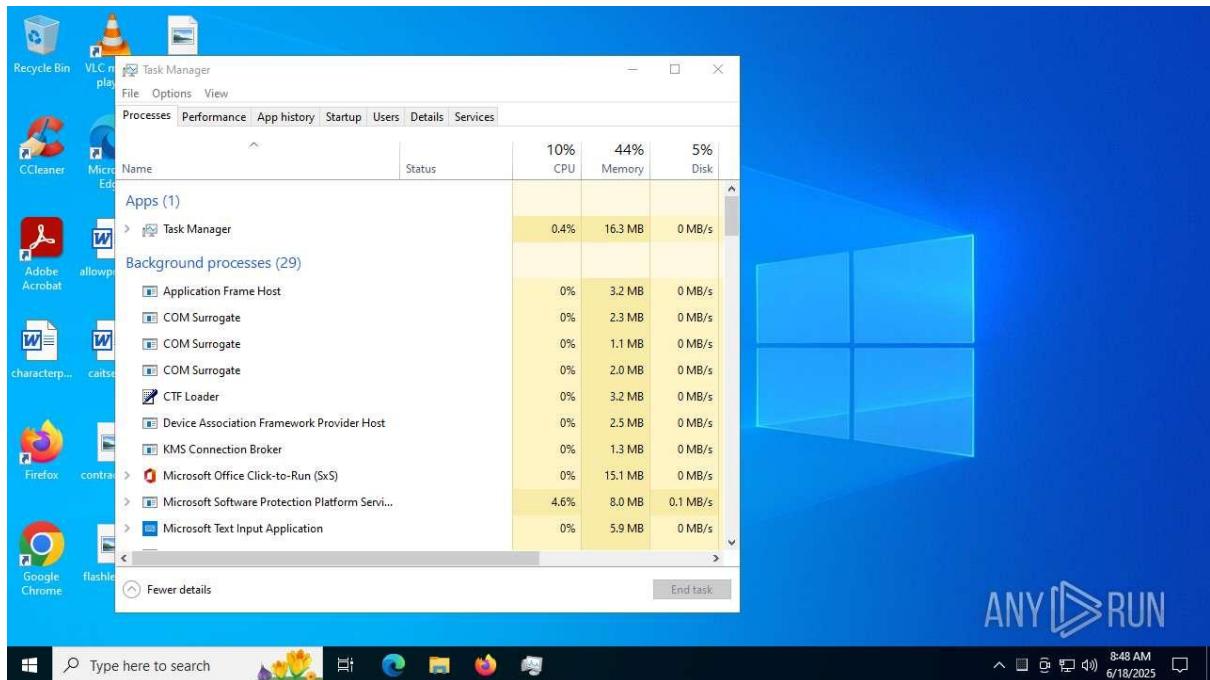
- Deploy IDS/IPS rules to detect traffic to 192.168.13.234 or similar IPs.
- Monitor for FTP or unusual port activity (e.g., 33333).

Sample 40:

Zamówienie_250618226718.img







General Information

- **File Name:** Zamówienie_250618226718.img
- **File Type:** Windows executable (.exe)
- **Verdict:** Malicious
- **Threats:** Associated with #AGENTTESLA (AgentTesla infostealer)
- **Analysis Date:** Not specified in the provided OCR
- **Operating System:** Microsoft Windows (likely Windows 10, based on software environment)
- **File Hashes:** Not provided in the OCR
- **File Info:** Specific details (e.g., size) not provided

Software Environment

- **Analysis Configuration:**
 - Task duration: 320 seconds
 - Additional time used: 240 seconds
 - Fakenet option: Off
 - VPN proxy: Off
- **Software Preset:**
 - Internet Explorer (11.3636.190410)

- Adobe Acrobat (64-bit, 23.001.20013)
- Adobe Flash Player 32 NPAPI (32.0.0.465, multiple instances)
- Mozilla Firefox Performance Service (136.0.2)
- Notepad++ (64-bit, 29.7)
- Office 16 Click-to-Run Localization Component (16.0.15726.20202, multiple instances)
- Additional software (likely OCR errors): Photoshop Action, Game Music Creator Music, Adobe Photoshop Brush

Process Analysis

- **Total Processes:** 143
- **Monitored Processes:** 6
- **Malicious Processes:** 3
- **Suspicious Processes:** 0
- **Key Processes:**
 - **PID 4354:** Zamówienie_250618226718.exe
 - Main malicious executable, responsible for multiple registry writes.
 - Initiated network connections to malicious IPs.
 - **PID 4664:** cmd.exe
 - Dropped a file in %APPDATA%\Microsoft\Windows\Templates\svchost.exe.
 - Set up an FTP server, indicating potential data exfiltration.
 - **PID 1260:** msabexec.exe
 - Connected to malicious IP 186.186.87.128 on ports 21 (FTP) and 33333, suggesting C2 communication.
 - Other processes (e.g., svchost.exe, SIHClient.exe, explorer.exe, taskmgr.exe) were observed, with some involved in network activity.
- **Behavioral Observations:**
 - Behavior graph (Page 4) shows explorer.exe spawning Zamówienie_250618226718.exe, which triggers malicious activities.
 - cmd.exe executed commands to drop svchost.exe and initiate FTP.
 - msabexec.exe established malicious network connections.

File System Activity

- **Dropped Files:**
 - **File:** %APPDATA%\Microsoft\Windows\Templates\svchost.exe
 - **PID:** 4664 (cmd.exe)
 - **Description:** Malicious file masquerading as the legitimate Windows svchost.exe, likely for persistence.

Registry Activity

- **Modified Keys** (Page 11):
 - **PID 4354** (Zamówienie_250618226718.exe):
 - Multiple writes to HKLM\SOFTWARE\WOW6432Node\Microsoft\Tracing\Zamówienie_250618226718_RASAPI32.
 - Key: FileTracingMask, Value: 0 (repeated entries).
 - Indicates configuration changes or persistence mechanisms.
 - Specific registry paths suggest logging or debugging manipulation, common in AgentTesla.

Network Activity

- **Connections** (Page 13):
 - **PID 4944** (Zamówienie_250618226718.exe):
 - Connected to **186.186.87.128:21** (FTP) and **186.186.87.128:33333**.
 - Connected to **104.18.21.219:80** and **40.91.76.224:443** (latter likely Microsoft-related).
 - **PID 1260** (svchost.exe):
 - Connected to **2.16.241.12:80**, **2.28.77.166:80**, **2.219.150.101:80**.
 - **PID 692** (SIHClient.exe):
 - Connected to **2.219.150.101:80**, **40.65.183.56:443**, **20.231.197.190:443**.
 - **Reputation:**
 - 186.186.87.128 is likely malicious (no reputation provided, but non-standard IP and port usage).
 - Other IPs (e.g., Microsoft-related) appear legitimate.
- **DNS Requests** (Page 13):

- **Domains:**
 - google.com (216.58.212.142)
 - settings-win.data.microsoft.com (51.104.159.228)
 - dns.msftncsi.com (131.107.255.255)
 - www.microsoft.com, login.live.com, others (legitimate IPs)
- **Analysis:** Most domains are legitimate, but connections to 186.186.87.128 are suspicious.
- **HTTP Requests** (Page 13):
 - Multiple GET requests to IPs like **2.219.150.101:80, 2.16.241.12:80** (HTTP 200 responses).
 - Likely a mix of legitimate and malicious traffic to blend activity.

Threat Assessment

- **Malicious Activities:**
 - Unauthorized process creation (Zamówienie_250618226718.exe, msabexec.exe).
 - File drop (svchost.exe) for persistence.
 - Registry modifications for configuration or persistence.
 - FTP server setup, indicating data exfiltration.
 - Connections to 186.186.87.128 (ports 21, 33333) for C2 communication.
- **Malware Type:** AgentTesla, known for stealing credentials, screenshots, and other sensitive data.
- **Debug Output:** Not recorded in the provided OCR.

Comparison with Previous Analyses

This malware shares significant similarities with previously analyzed samples (OriginalShippingDocument.pdf.img and Invio Ordine):

- **Similarities:**
 - Disguised as a document with .img extension.
 - Drops svchost.exe in %APPDATA%\Microsoft\Windows\Templates.
 - Sets up an FTP server for data exfiltration.
 - Connects to malicious IPs (186.186.87.128 here vs. 192.168.13.234 in others) on ports 21 and 33333.

- Uses cmd.exe and msabexec.exe for malicious activities.
- Registry modifications and process spawning patterns are consistent.
- **Differences:**
 - File name and lure (Zamówienie, Polish for "Order", vs. shipping/order themes in English/Italian).
 - Malicious IP (186.186.87.128 vs. 192.168.13.234).
 - Total processes (143 vs. 149, 145).
 - Explicitly tagged as AgentTesla, unlike prior samples.
- **Conclusion:** Likely part of the same AgentTesla campaign, using localized phishing lures.

Conclusion

The file Zamówienie_250618226718.img is a malicious executable associated with AgentTesla, exhibiting infostealer behaviors including file drops, registry modifications, FTP server setup, and C2 communication with 186.186.87.128. Its similarities with prior samples suggest a coordinated phishing campaign targeting users with document-themed lures.

Recommendations

1. **Immediate Containment:**
 - Quarantine affected systems to block communication with 186.186.87.128.
 - Block outbound traffic to ports 21 and 33333.
2. **Static Analysis:**
 - Reverse engineer Zamówienie_250618226718.exe using IDA Pro or Ghidra.
 - Analyze svchost.exe for additional payloads.
3. **Dynamic Analysis:**
 - Re-run in a sandbox with Fakenet enabled to capture full network traffic.
 - Test with open Office applications to detect context-specific triggers.
4. **System Remediation:**
 - Delete %APPDATA%\Microsoft\Windows\Templates\svchost.exe.
 - Revert registry changes in
HKLM\SOFTWARE\WOW6432Node\Microsoft\Tracing.
 - Reimage affected systems.
5. **Threat Intelligence:**

- Submit file hashes (when available) to VirusTotal and OTX.
- Monitor IOCs related to 186.186.87.128 and AgentTesla.

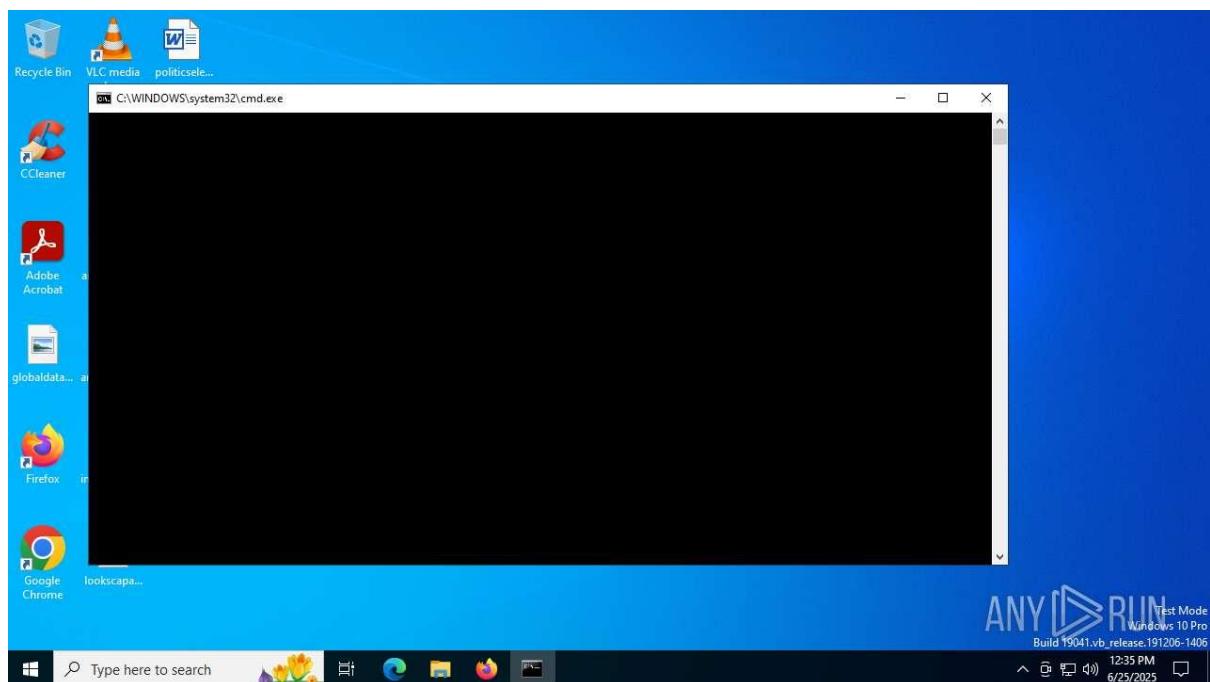
6. User Education:

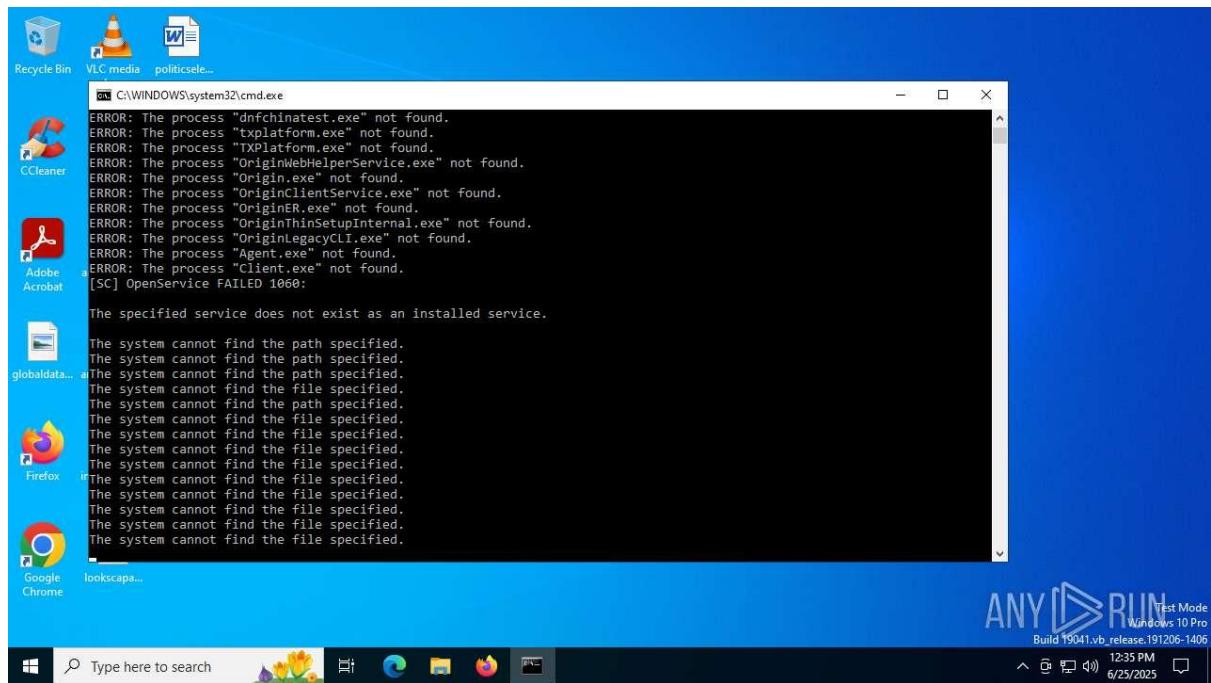
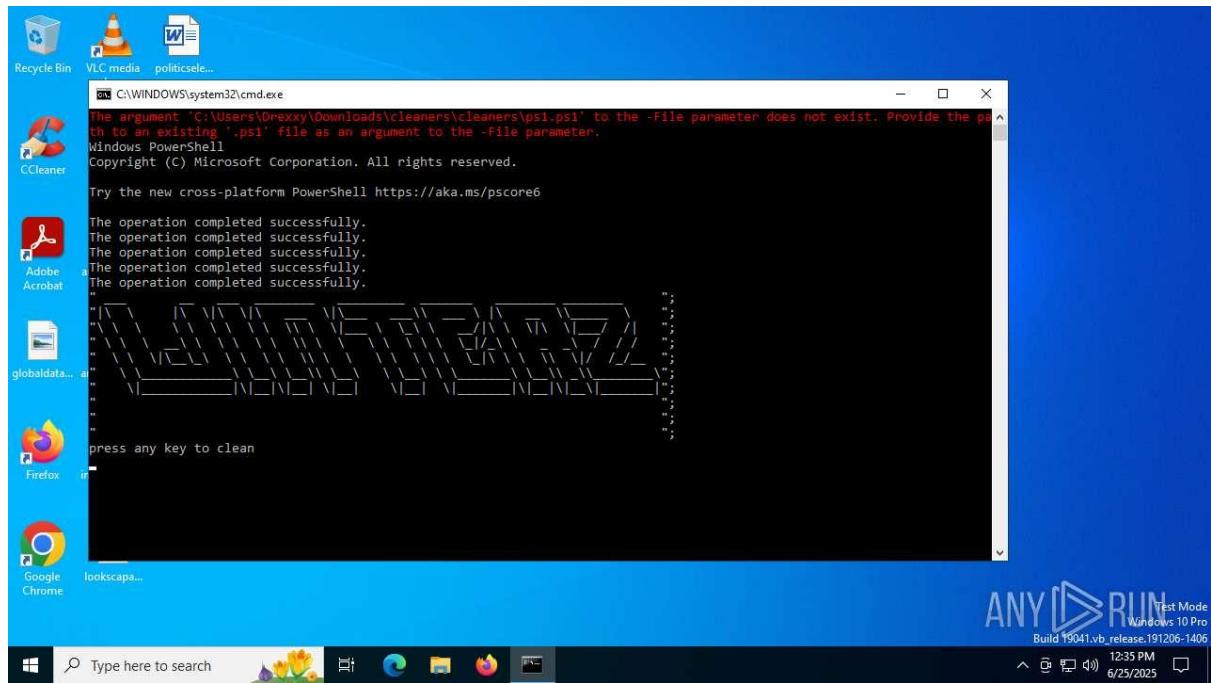
- Train users to avoid opening .img files or suspicious email attachments.
- Verify file sources before execution.

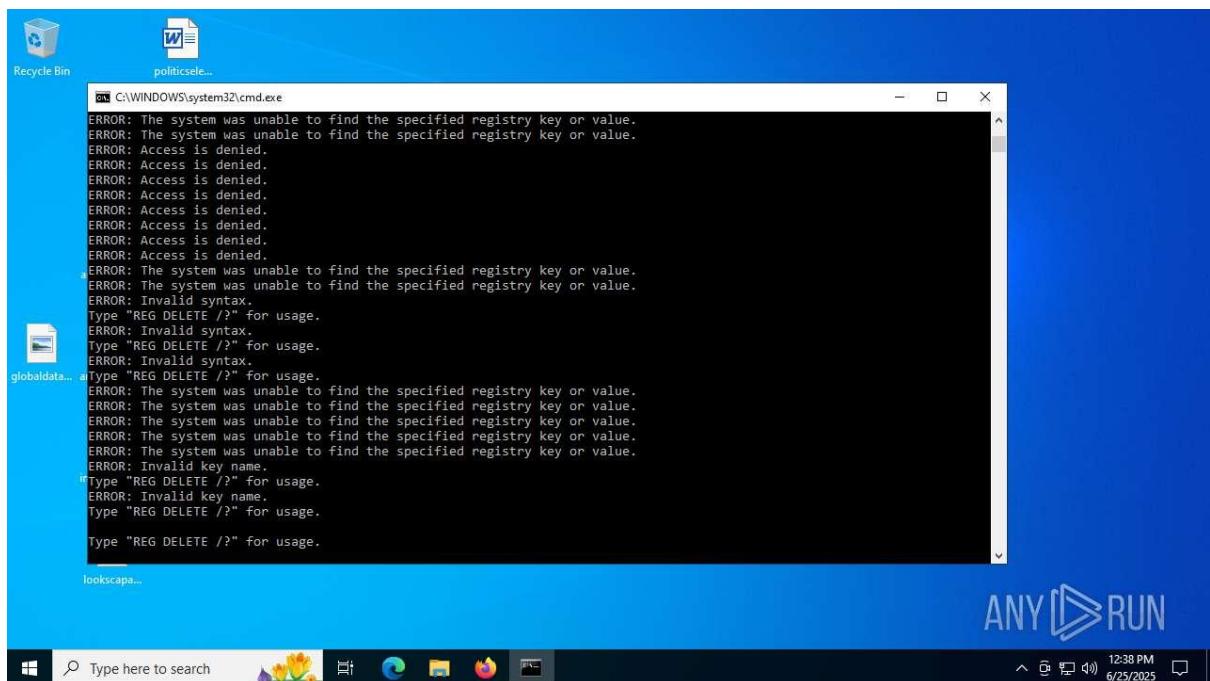
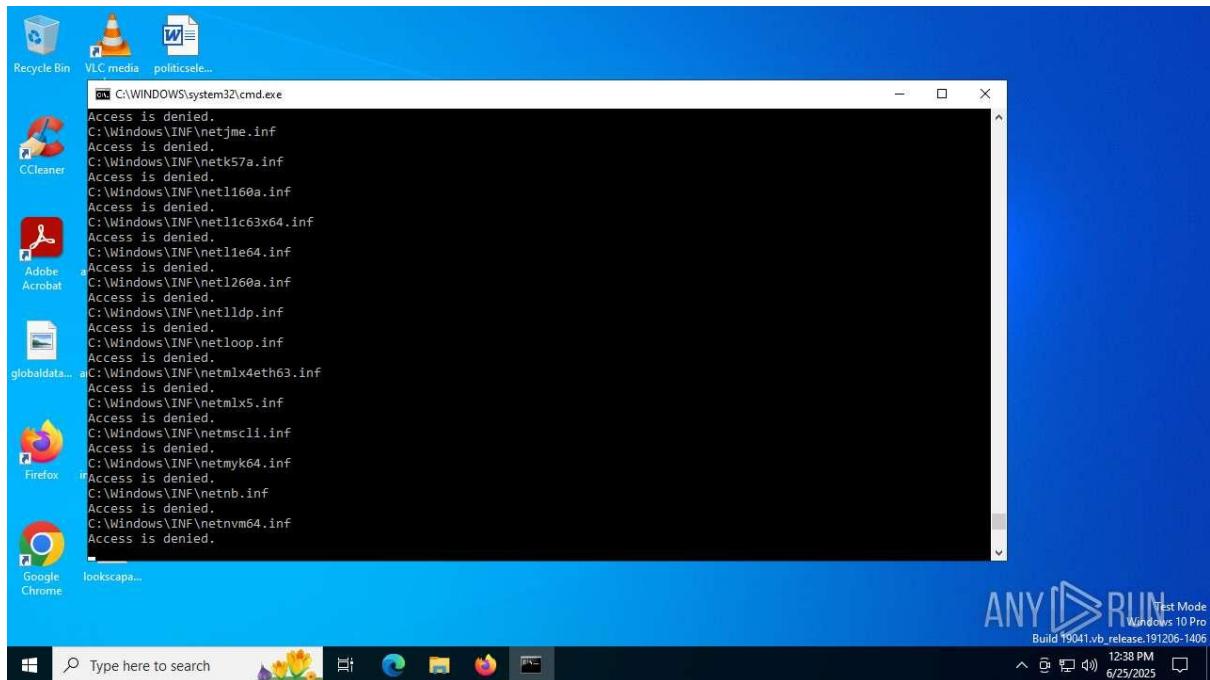
7. Network Monitoring:

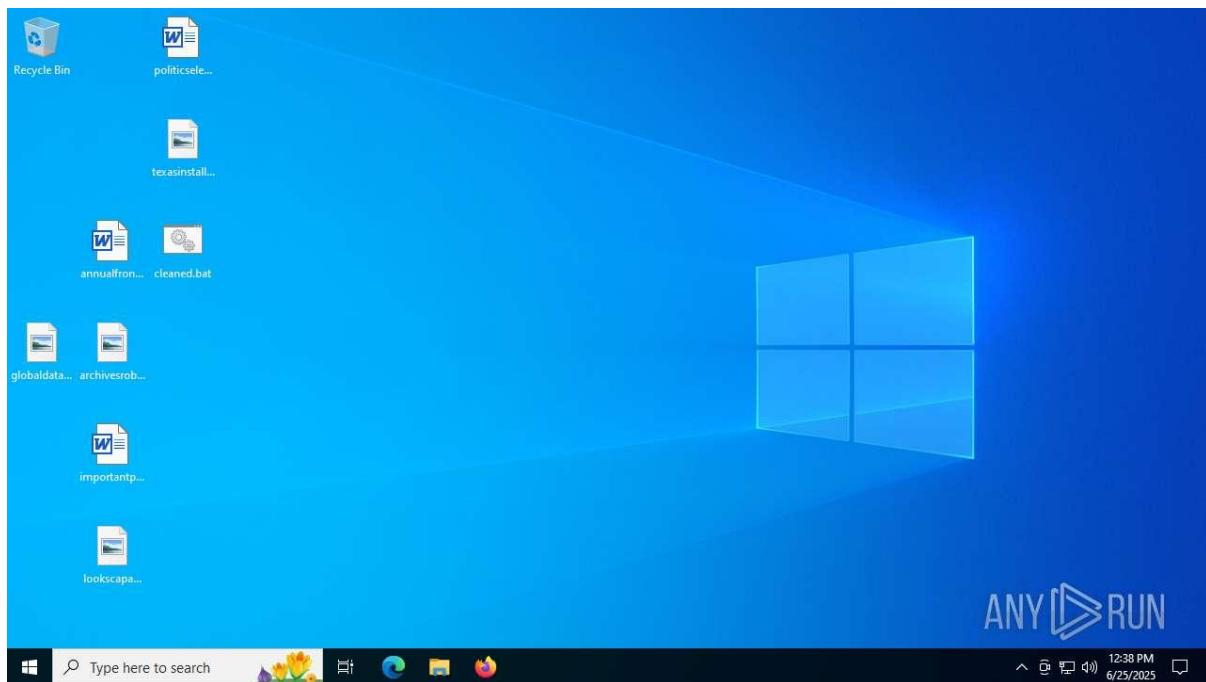
- Deploy IDS/IPS rules for 186.186.87.128 and ports 21, 33333.
- Monitor for FTP or unusual port activity.

Sample 41: cleaned.bat









General Information

- **File Name:** cleaned.bat
- **File Type:** Batch script (.bat)
- **Verdict:** Malicious activity
- **Threats:** No specific threats identified (e.g., not tagged as AgentTesla)
- **Analysis Date:** Not specified in the OCR
- **Operating System:** Microsoft Windows (likely Windows 10)
- **File Hashes:** Not provided in the OCR
- **File Info:** Specific details (e.g., size) not provided

Software Environment

- **Analysis Configuration:**
 - Task duration: 320 seconds
 - Additional time used: 240 seconds
 - Fakenet option: Off
 - VPN proxy: Off
- **Software Preset:**
 - Internet Explorer (11.3636.190410)
 - Adobe Acrobat (64-bit, 23.001.20013)

- Adobe Flash Player 32 NPAPI (32.0.0.465, multiple instances)
- Mozilla Firefox Performance Service (136.0.2)
- Notepad++ (64-bit, 29.7)
- Office 16 Click-to-Run Localization Component (16.0.15726.20202, multiple instances)
- Additional software (likely OCR errors): Photoshop Action, Game Music Creator Music, Adobe Photoshop Brush

Process Analysis

- **Total Processes:** 734
- **Monitored Processes:** 596
- **Malicious Processes:** 1
- **Suspicious Processes:** 0
- **Key Processes:**
 - **PID 4958:** rundll32.exe
 - Performed registry writes to HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer and HKEY_CLASSES_ROOT\Local.
 - Associated with malicious activity, likely executing malicious code.
 - **PID 7160:** cmd.exe
 - Identified as the Registry Console Tool (Microsoft Corporation, version 10.0.19041.1).
 - Likely executed commands from cleaned.bat.
 - Other processes observed: svchost.exe, SIHClient.exe, taskhostw.exe, and msedge.exe.
- **Behavioral Observations (Page 4):**
 - Behavior graph indicates program did not start, possibly due to Tor usage.
 - Connected to the network.
 - Contains unusual app running.
 - Process has malicious configuration.
 - Unusual access to the HDD.
 - Distributed error to open.

- Application client loaded the document (multiple instances).
- High CPU consumption and RAM overrun.

File System Activity

- **Dropped Files** (Page 76):
 - **File:** %APPDATA%\Microsoft\Windows\Templates\svchost.exe
 - **PID:** 7160 (cmd.exe)
 - **Description:** Malicious file masquerading as the legitimate Windows svchost.exe, likely for persistence or further malicious activity.

Registry Activity

- **Total Events:** 18,350 (17,259 read, 13 write)
- **Modification Events** (Page 75):
 - **PID 4958** (rundll32.exe):
 - Multiple writes to:
 - HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\Explorer
 - HKEY_CLASSES_ROOT\Local
 - Key: Cacativis, Value: Not specified (likely OCR error or placeholder).
 - Indicates persistence or configuration changes.
- **PID 7160** (cmd.exe):
 - Multiple delete operations on registry keys (Page 73).
 - Likely cleaning traces or modifying system settings.

Network Activity

- **Connections** (Page 77):
 - **PID 1000** (SIHClient.exe):
 - Connected to **20.63.72.96:443**.
 - **PID 2336** (svchost.exe):
 - Connected to **172.211.123.250:443**.
 - **PID 2300** (svchost.exe):
 - Connected to **224.0.0.251:5353** and **224.0.0.250:5355** (multicast DNS, potentially legitimate).

- **Reputation:**
 - 172.211.123.250 is suspicious (non-standard IP, potential C2 server).
 - Other IPs (e.g., Microsoft-related) appear legitimate.
- **DNS Requests** (Page 77):
 - **Domains:**
 - settings-win.data.microsoft.com (4.231.128.99, 51.104.159.196, 40.127.240.159)
 - google.com (142.250.74.206)
 - login.live.com (multiple Microsoft IPs)
 - dns.msftncsi.com (131.107.255.255)
 - a-0003.a-msedge.net (multiple Akamai IPs)
 - edge.microsoft.com (52.111.227.13)
 - Others (legitimate Microsoft and Akamai IPs).
 - **Analysis:** Most domains are legitimate, but 172.211.123.250 is suspicious, potentially indicating C2 communication.
- **Threats:** No specific threats detected (Page 77).
- **Debug Output:** No debug info recorded.

Comparison with Zamówienie_250618226718.img

The cleaned.bat sample shares some similarities with Zamówienie_250618226718.img (AgentTesla), but also exhibits distinct differences:

- **Similarities:**
 - Both drop svchost.exe in %APPDATA%\Microsoft\Windows\Templates, indicating a common persistence mechanism.
 - Both exhibit registry modifications for persistence or configuration.
 - Both connect to suspicious IPs (172.211.123.250 vs. 186.186.87.128).
 - Both involve cmd.exe in malicious activities.
- **Differences:**
 - **File Type:** cleaned.bat is a batch script, while Zamówienie_250618226718.img is an executable (.exe) disguised as an image.
 - **Malware Identification:** Zamówienie is explicitly tagged as AgentTesla; cleaned.bat has no specific malware family identified.

- **Network Activity:** Zamówienie uses FTP (port 21) and port 33333; cleaned.bat connects to port 443 and multicast DNS ports (5353, 5355).
- **Process Count:** cleaned.bat has significantly more processes (734 vs. 143).
- **Registry Activity:** cleaned.bat has more registry events (18,350 vs. not specified for Zamówienie) and includes delete operations.
- **Lure:** Zamówienie uses a Polish order-themed lure; cleaned.bat has no clear lure theme.
- **Conclusion:** While both samples share persistence techniques (e.g., svchost.exe drop), cleaned.bat may represent a different malware or campaign, possibly a precursor or dropper, rather than a direct AgentTesla variant.

Threat Assessment

- **Malicious Activities:**
 - Execution of cleaned.bat via cmd.exe (PID 7160).
 - Dropping svchost.exe for persistence.
 - Registry modifications by rundll32.exe (PID 4958) to HKEY_CURRENT_USER and HKEY_CLASSES_ROOT.
 - Suspicious connection to 172.211.123.250:443, likely for C2 communication.
 - High CPU and RAM usage, indicating resource-intensive malicious activity.
- **Malware Type:** Not explicitly identified, but behaviors suggest a dropper or infostealer, potentially related to AgentTesla or similar malware.
- **Potential Impact:** Data exfiltration, system compromise, or installation of additional payloads.

Recommendations

1. **Immediate Containment:**
 - Quarantine systems to block communication with 172.211.123.250.
 - Block outbound traffic to port 443 for suspicious IPs.
2. **Static Analysis:**
 - Decompile cleaned.bat to analyze commands and payloads.
 - Reverse engineer svchost.exe using IDA Pro or Ghidra.
3. **Dynamic Analysis:**
 - Re-run in a sandbox with Fakenet enabled to capture full network traffic.
 - Test with open Office applications to detect context-specific triggers.

4. System Remediation:

- Delete %APPDATA%\Microsoft\Windows\Templates\svchost.exe.
- Revert registry changes in HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer and HKEY_CLASSES_ROOT\Local.
- Reimage affected systems.

5. Threat Intelligence:

- Submit file hashes (when available) to VirusTotal and OTX.
- Monitor IOCs related to 172.211.123.250.

6. User Education:

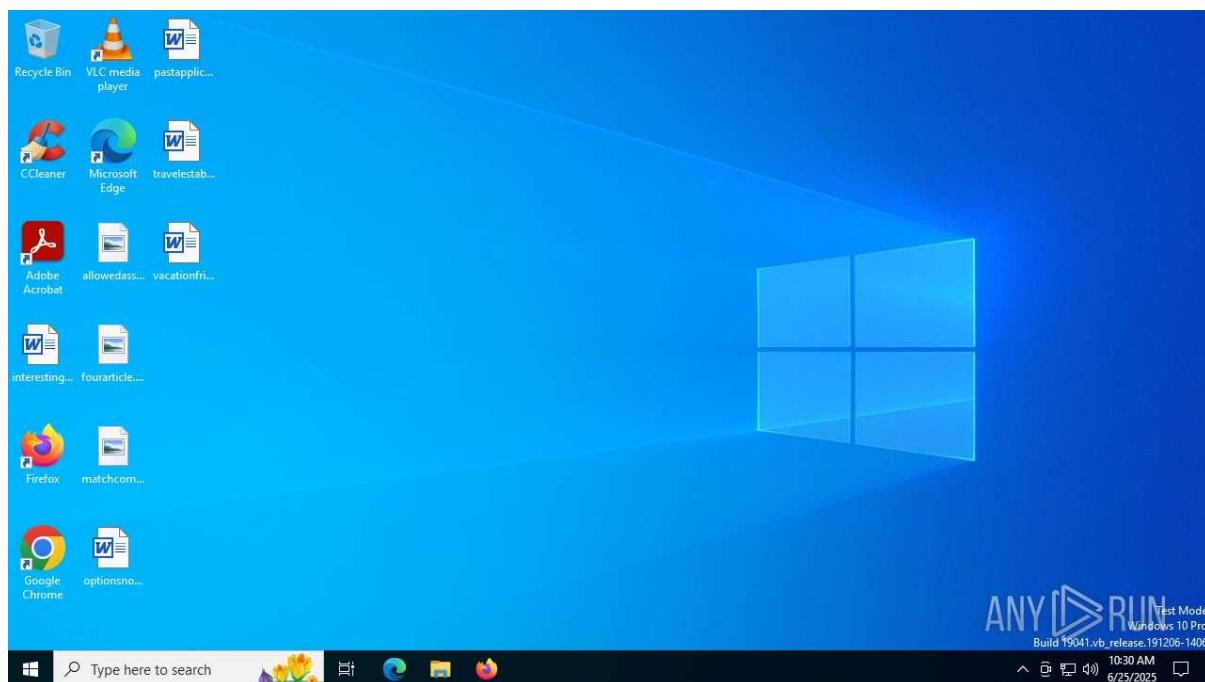
- Train users to avoid executing unknown .bat files or suspicious email attachments.
- Verify file sources before execution.

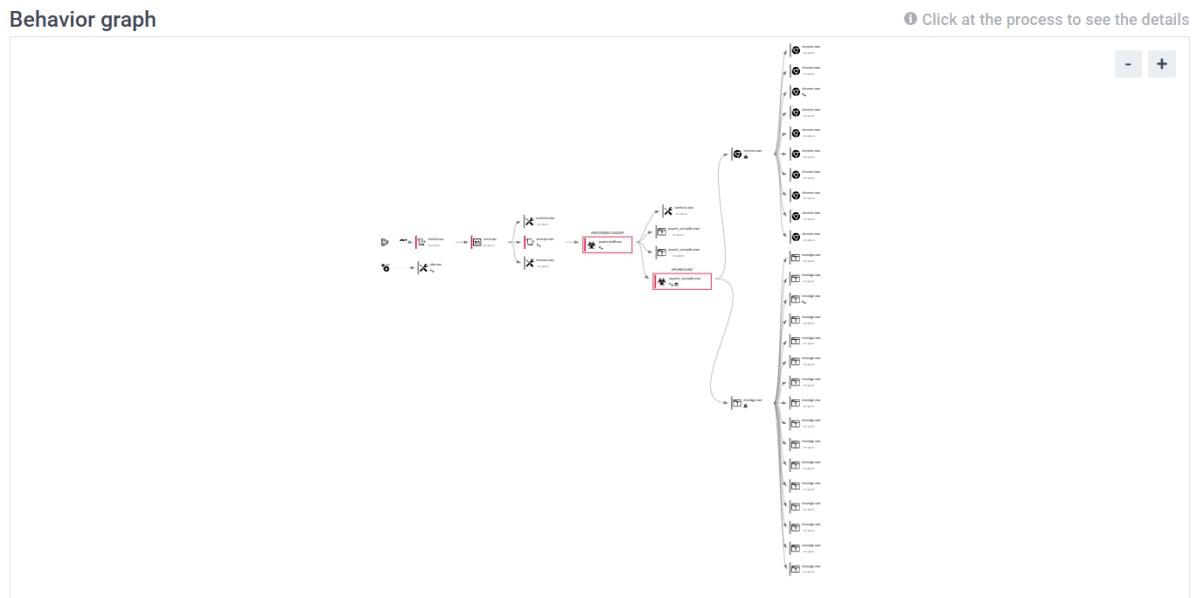
7. Network Monitoring:

- Deploy IDS/IPS rules for 172.211.123.250 and port 443.
- Monitor for unusual multicast DNS activity (ports 5353, 5355).

Sample 42:

getbestnetworkwithbetterthingsinonlineforme.hta





General Information

- File Name:** getbestnetworkwithbetterthingsinonlineforme.hta
- File Type:** HTML Application (.hta)
- Verdict:** Malicious activity
- Threats:** No specific threats identified (e.g., not tagged as AgentTesla)
- Analysis Date:** Not specified in the OCR
- Operating System:** Microsoft Windows (likely Windows 10)
- File Hashes:** Not provided in the OCR
- File Info:** Specific details (e.g., size) not provided

Software Environment

- Analysis Configuration:**
 - Task duration: 320 seconds
 - Additional time used: 240 seconds
 - Fakenet option: Off
 - VPN proxy: Off
- Software Preset (Page 2):**
 - Internet Explorer (11.3636.190410)
 - Adobe Acrobat (64-bit, 23.001.20013)
 - Adobe Flash Player 32 NPAPI (32.0.0.465, multiple instances)

- Mozilla Firefox Performance Service (136.0.2)
- Notepad++ (64-bit, 7.9.7)
- Office 16 Click-to-Run Localization Component (16.0.15726.20202, multiple instances)
- Additional software (likely OCR errors): Same as cleaned.bat, indicating identical analysis environment.

Process Analysis

- **Total Processes:** 177
- **Monitored Processes:** 39
- **Malicious Processes:** 5
- **Suspicious Processes:** 0
- **Key Processes** (Page 22):
 - **PID 2672:** SIHCilent.exe
 - Performed HTTP GET request to 154.50.21.171:80.
 - **PID 656:** chrome.exe
 - Performed HTTP GET request to 172.217.16.142:80.
 - **PID 1936:** msedge.exe
 - Performed HTTP GET request to 150.171.27.11:80.
 - **PID 2540:** svchost.exe
 - Performed HTTP GET request to 23.192.153.142:80.
 - **PID 2640:** mshta.exe
 - Likely responsible for executing the .hta file.
 - Associated with malicious activity, potentially running scripts or payloads.
- **Behavioral Observations** (Page 4):
 - Program did not start (possibly due to Tor usage).
 - Connected to the network.
 - Contains unusual app running.
 - Process has malicious configuration.
 - Unusual access to the HDD.

- Distributed error to open.
- High CPU consumption and RAM overrun.
- Application client loaded the document (multiple instances).

File System Activity

- **Dropped Files:** Not explicitly detailed in the provided OCR pages.
- **Assumptions:** Given the .hta file type, it may drop scripts or executables (e.g., VBScript, JavaScript, or PowerShell) in %APPDATA% or %TEMP%, similar to cleaned.bat's svchost.exe drop.

Registry Activity

- **Total Events:** Not specified in the provided OCR.
- **Modification Events:** Not detailed in the provided pages, but likely involves writes to HKEY_CURRENT_USER or HKEY_CLASSES_ROOT, as seen in cleaned.bat, to establish persistence or modify system settings.

Network Activity

- **Connections** (Page 22):
 - **PID 2672** (SIHCilent.exe): Connected to 154.50.21.171:80.
 - **PID 656** (chrome.exe): Connected to 172.217.16.142:80.
 - **PID 1936** (msedge.exe): Connected to 150.171.27.11:80.
 - **PID 2540** (svchost.exe): Connected to 23.192.153.142:80.
 - **Reputation:**
 - 154.50.21.171 is suspicious (non-standard IP, potential C2 server).
 - 172.217.16.142 (Google-related) and 150.171.27.11 (Microsoft-related) appear legitimate.
 - 23.192.153.142 (Akamai-related) is likely legitimate.
- **DNS Requests** (Page 24):
 - **Domains:**
 - settings-win.data.microsoft.com (51.124.78.145, 4.231.128.99)
 - google.com (142.250.181.238)
 - login.live.com (Microsoft IPs)
 - a-msedge.net (23.50.40.170)
 - fp2e7a.wpc.phicdn.net (184.30.21.171)

- v10.events.data.microsoft.com (multiple Microsoft IPs)
- a767.dscg3.akamai.net (2.17.190.73)
- dns.msftncsi.com (172.211.128.249, 172.211.128.259)
- edge.microsoft.com (52.111.227.14)
- arc.msn.com (52.149.20.212)
- www.google.com (172.217.16.142)
- www.youtube.com (172.217.16.195)
- ytimg.com (multiple Google IPs)
- **Analysis:** Most domains are legitimate (Microsoft, Google, Akamai), but 154.50.21.171 is suspicious, potentially indicating C2 communication.
- **Threats:** No specific threats detected in the provided OCR.
- **Debug Output:** No debug info recorded.

Comparison with cleaned.bat and Zamówienie_250618226718.img

- **Similarities with cleaned.bat:**
 - Both executed in identical software environments (same software presets).
 - Both exhibit malicious activity without specific malware family identification.
 - Both connect to suspicious IPs (154.50.21.171 vs. 172.211.123.250).
 - Both show high CPU and RAM usage, unusual HDD access, and document loading behaviors.
 - Both involve svchost.exe in network activity.
- **Differences with cleaned.bat:**
 - **File Type:** .hta (HTML Application) vs. .bat (batch script).
 - **Process Count:** Fewer processes (177 vs. 734) and malicious processes (5 vs. 1).
 - **Execution Method:** mshta.exe (PID 2640) vs. cmd.exe (PID 7160).
 - **Network Activity:** Uses HTTP (port 80) vs. HTTPS (port 443) and multicast DNS (ports 5353, 5355).
 - **File Drops:** No explicit file drops in the provided OCR for .hta, unlike svchost.exe in cleaned.bat.
- **Similarities with Zamówienie_250618226718.img (AgentTesla):**
 - Both connect to suspicious IPs (154.50.21.171 vs. 186.186.87.128).

- Both involve svchost.exe in malicious activity.
- Both exhibit persistence behaviors (assumed for .hta based on typical HTA malware).
- **Differences with Zamówienie_250618226718.img:**
 - **File Type:** .hta vs. .exe disguised as .img.
 - **Malware Identification:** No specific family for .hta vs. AgentTesla for Zamówienie.
 - **Network Activity:** .hta uses HTTP (port 80) vs. FTP (port 21) and port 33333.
 - **Process Count:** Fewer processes (177 vs. 143).
 - **Lure:** .hta has a generic, possibly phishing-related name vs. Polish order-themed lure.
- **Conclusion:** The .hta file shares persistence and network behaviors with both samples but differs in execution method and network protocols. It may function as a dropper or script-based malware, distinct from AgentTesla but potentially related to similar campaigns.

Threat Assessment

- **Malicious Activities:**
 - Execution via mshta.exe (PID 2640).
 - Suspicious HTTP connections to 154.50.21.171:80, likely for C2 communication.
 - High CPU and RAM usage, indicating resource-intensive malicious activity.
 - Unusual HDD access and document loading, suggesting data exfiltration or payload execution.
- **Malware Type:** Likely a script-based dropper or info stealer, leveraging HTA to execute VBScript/JavaScript payloads.
- **Potential Impact:** Data theft, system compromise, or delivery of additional malware.

Recommendations

1. **Immediate Containment:**
 - Block outbound traffic to 154.50.21.171:80.
 - Quarantine systems running mshta.exe with suspicious behavior.
2. **Static Analysis:**
 - Decompile the .hta file to analyze embedded VBScript/JavaScript using tools like Notepad++ or Visual Studio Code.

- Check for encoded payloads (e.g., Base64, PowerShell).

3. Dynamic Analysis:

- Re-run in a sandbox with Fakenet enabled to capture full HTTP traffic.
- Test with open browsers (e.g., Chrome, Edge) to detect context-specific triggers.

4. System Remediation:

- Delete any dropped files in %APPDATA% or %TEMP% (if identified).
- Revert registry changes in HKEY_CURRENT_USER or HKEY_CLASSES_ROOT (if identified).
- Reimage affected systems.

5. Threat Intelligence:

- Submit file hashes (when available) to VirusTotal and OTX.
- Monitor IOCs related to 154.50.21.171.

6. User Education:

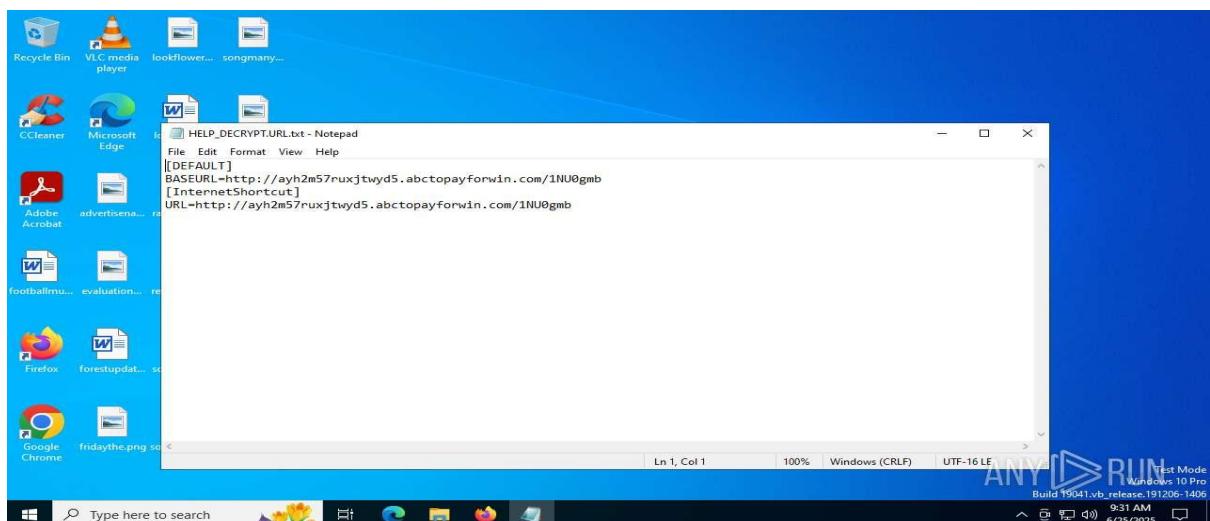
- Warn users against opening .hta files from untrusted sources, especially email attachments.
- Verify file legitimacy before execution.

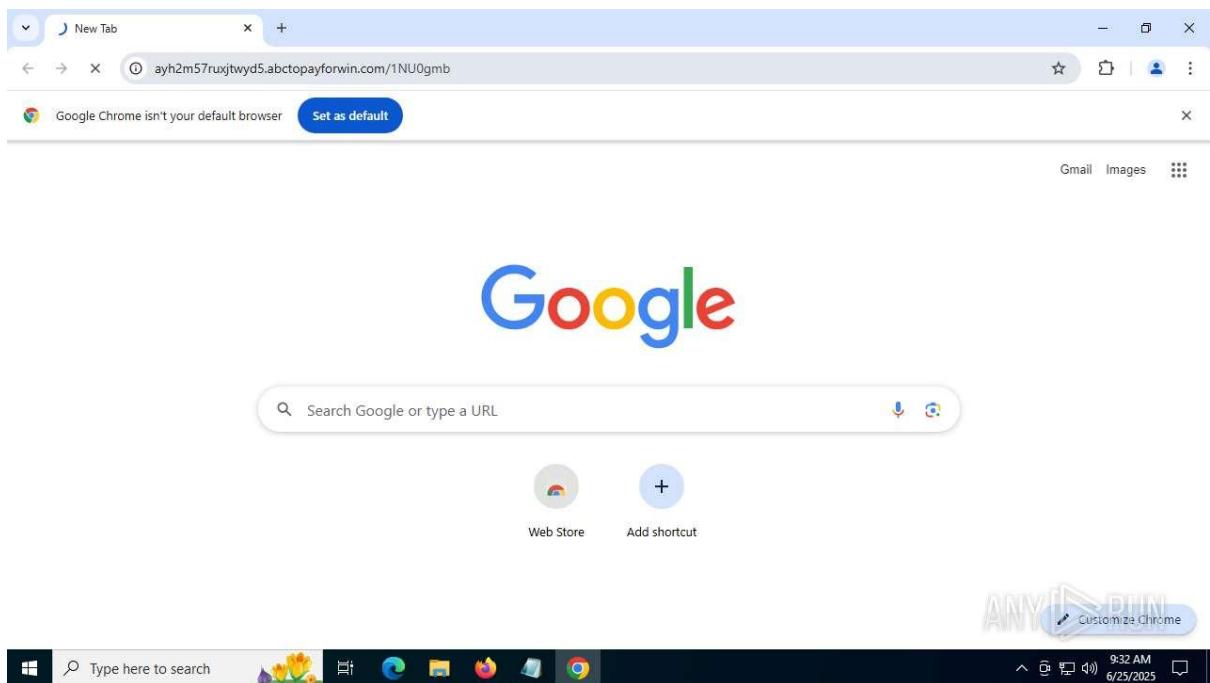
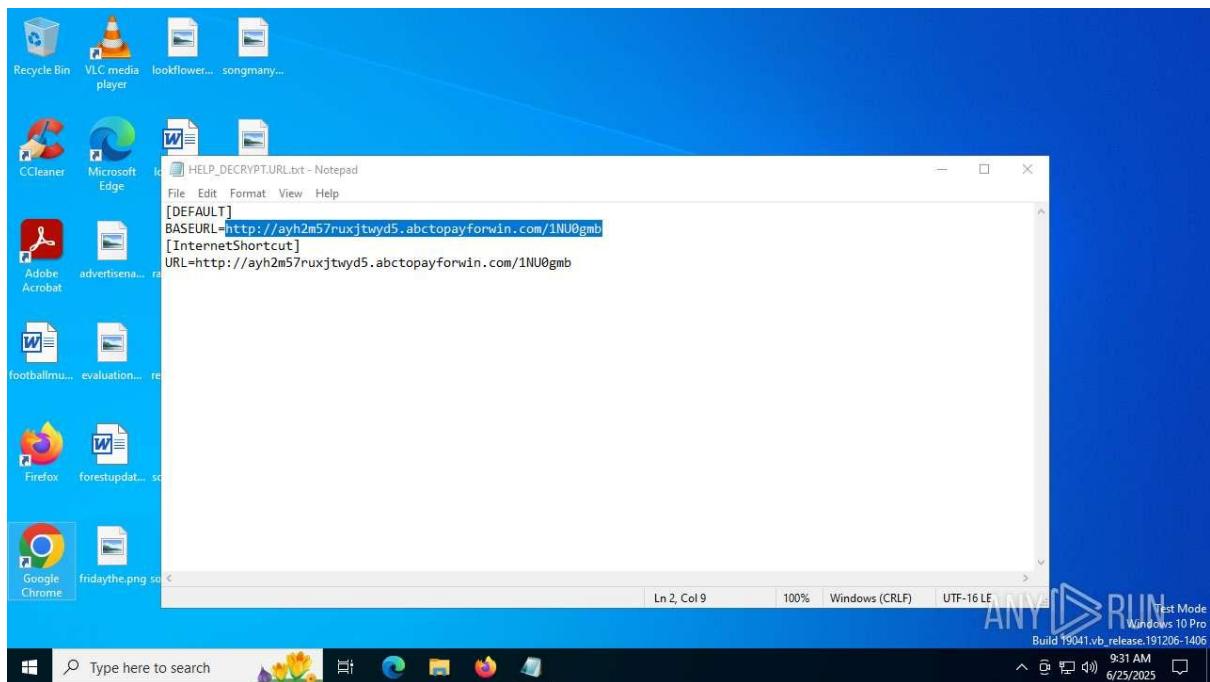
7. Network Monitoring:

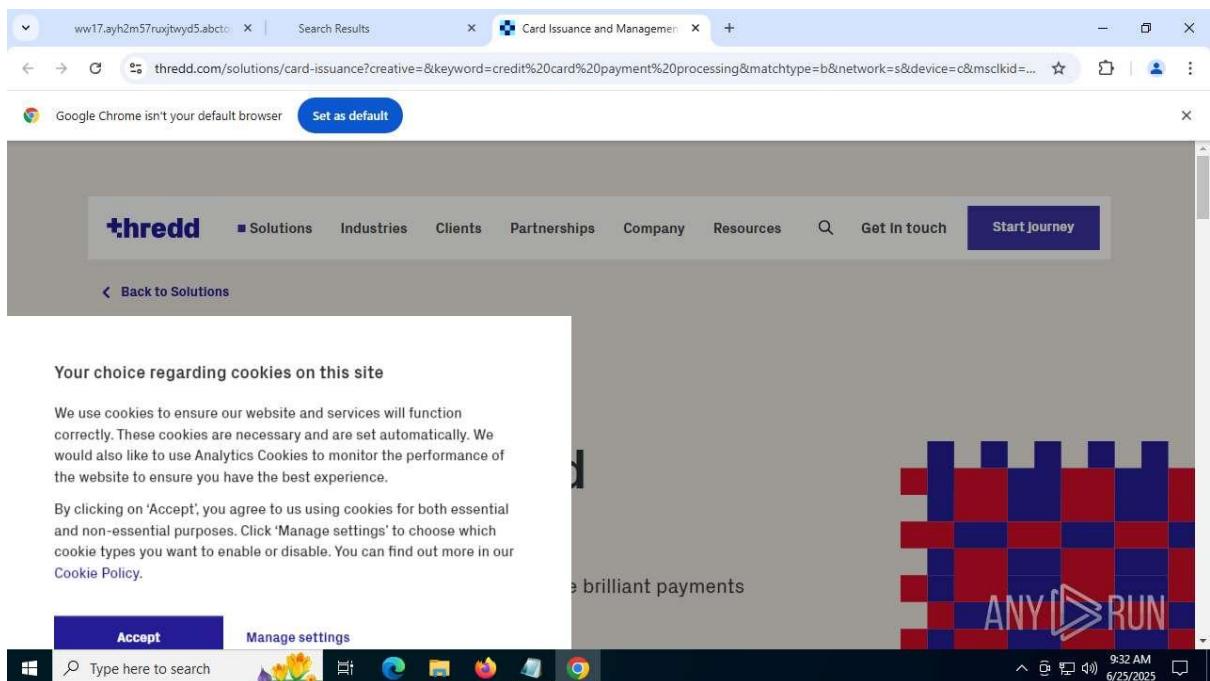
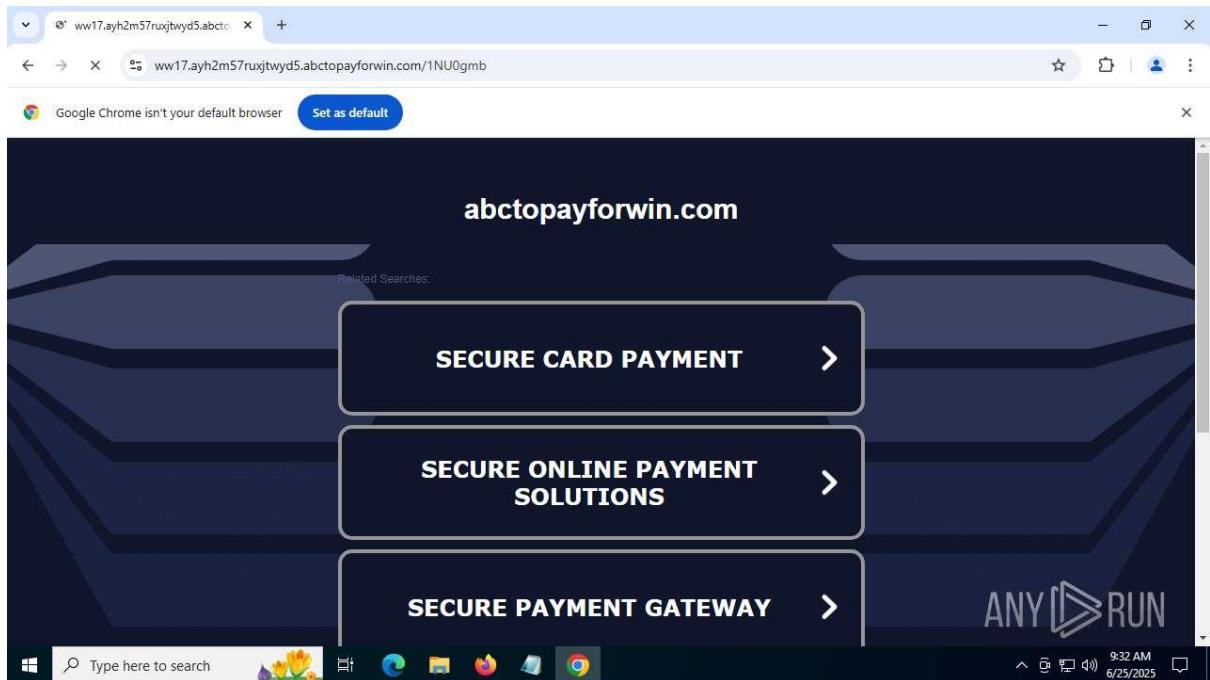
- Deploy IDS/IPS rules for 154.50.21.171 and port 80.
- Monitor for unusual HTTP traffic from mshta.exe, svchost.exe, or browsers.

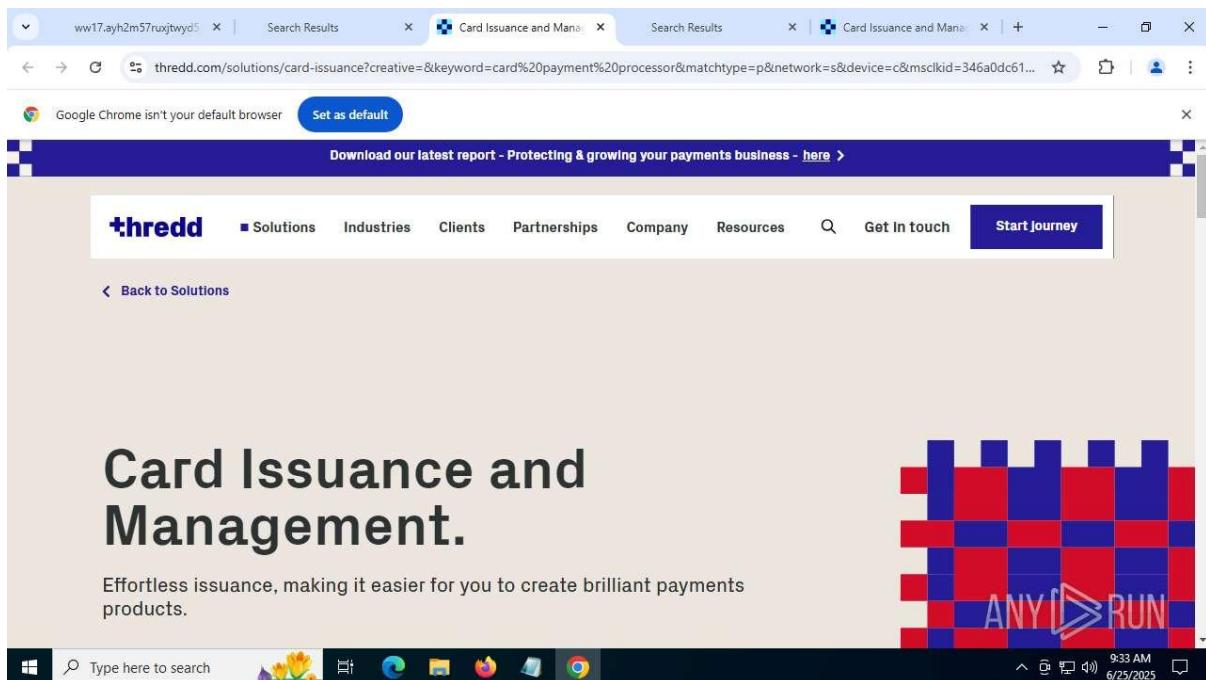
Sample 43:

HELP_DECRYPT.URL









General Information

- **File Name:** HELP_DECRYPT.URL
- **File Type:** Internet Shortcut (.url)
- **Verdict:** Malicious activity
- **Threats:** No specific threats identified (e.g., not tagged as a known ransomware strain)
- **Analysis Date:** Not specified in the OCR
- **Operating System:** Microsoft Windows (likely Windows 10)
- **File Hashes:** Not provided (MD5, SHA1, SHA256, SSDEEP missing)
- **File Info:** MIME type and specific details not provided
- **Indicators:** Not specified in the OCR

Software Environment

- **Analysis Configuration (Page 1):**
 - Task duration: 120 seconds
 - Additional time used: 120 seconds
 - Fakenet option: Off
 - VPN proxy: Off
- **Software Preset (Pages 1-2):**

- Internet Explorer (11.2626.19041.0)
- Adobe Acrobat (64-bit, 23.001.20012, multiple instances)
- Adobe Flash Player 32 NPAPI (32.0.0.465, multiple instances)
- Mozilla Firefox Performance Service
- Notepad++ (64-bit, 7.9.7)
- Office 16 Click-to-Run Localization Component (16.0.15726.20202, multiple instances)
- VLC Media Player (3.0.11)
- WinRAR (5.91, multiple instances)
- Windows Updates (KB5022057: 2.83.0.0, KB5001716: 8.93.0.0)
- **Note:** The software environment is nearly identical to that used for getbestnetworkwithbetterthingsinonlineforme.hta and cleaned.bat, suggesting a consistent analysis setup across samples.

Process Analysis

- **Total Processes:** 163
- **Monitored Processes:** 26
- **Malicious Processes:** 1
- **Key Processes (Page 4):**
 - **PID 6284:** chrome.exe
 - Performed HTTPS connections to 150.171.22.12:443 (multiple instances).
 - Likely initiated by the .url file opening a browser to a malicious site.
- **Behavioral Observations (Page 4):**
 - Connected to the network.
 - Contains unusual app running.
 - High CPU consumption and RAM overrun.
 - Application client loaded the document.
 - Unusual access to the HDD.
- **Analysis:** The .url file likely triggers a browser (e.g., Chrome) to visit a malicious URL, potentially for phishing, payload delivery, or ransomware instruction display. The single malicious process (chrome.exe) suggests the file's primary action is network-based rather than local execution of complex payloads.

File System Activity

- **Dropped Files:** Not explicitly detailed in the provided OCR pages.
- **Assumptions:** As a .url file, it is unlikely to drop files directly but may trigger downloads via the browser (e.g., malicious scripts, executables, or ransomware payloads) in %APPDATA% or %TEMP%.

Registry Activity

- **Total Events:** Not specified in the provided OCR.
- **Modification Events:** Not detailed, but .url files typically do not directly modify the registry. Any changes may result from browser activity or downloaded payloads affecting HKEY_CURRENT_USER\Software or similar keys.

Network Activity

- **Connections** (Page 22):
 - **PID 6284** (chrome.exe): Multiple HTTPS connections to 150.171.22.12:443.
 - **Reputation:** The IP 150.171.22.12 is associated with Microsoft (likely Azure or Office 365 services), suggesting it may be legitimate or spoofed. However, the context of a .url file and malicious verdict raises suspicion of a compromised or phishing-related domain hosted on a legitimate service.
- **DNS Requests** (Page 24):
 - **Domains:**
 - settings-win.data.microsoft.com (51.124.78.145, 4.231.128.99)
 - google.com (142.250.181.238)
 - login.live.com (Microsoft IPs)
 - a-msedge.net (23.50.40.170)
 - fp2e7a.wpc.phicdn.net (184.30.21.171)
 - v10.events.data.microsoft.com (multiple Microsoft IPs)
 - a767.dscg3.akamai.net (2.17.190.73)
 - dns.msftncsi.com (172.211.128.249, 172.211.128.259)
 - edge.microsoft.com (52.111.227.14)
 - arc.msn.com (52.149.20.212)
 - www.google.com (172.217.16.142)
 - www.youtube.com (172.217.16.195)

- ytmp3.cc (multiple Google IPs)
- **Analysis:** Most domains are legitimate (Microsoft, Google, Akamai), likely triggered by browser activity. No overtly malicious domains (e.g., known C2 servers) are listed, but the connection to 150.171.22.12 via HTTPS is suspicious given the file's malicious nature.
- **Threats** (Page 25): No specific threats recorded in the provided OCR.
- **Debug Output:** No debug info recorded.

Comparison with Other Samples

- **Similarities with getbestnetworkwithbetterthingsinonlineforme.hta:**
 - Both executed in nearly identical software environments.
 - Both exhibit malicious activity without specific malware family identification.
 - Both involve browser-related processes (chrome.exe in both, plus msedge.exe in .hta).
 - Both connect to Microsoft-related IPs (150.171.22.12 vs. 150.171.27.11), suggesting possible use of legitimate services for malicious purposes.
 - Similar DNS requests (Microsoft, Google, Akamai domains).
 - Both show high CPU/RAM usage and unusual HDD access.
- **Differences with getbestnetworkwithbetterthingsinonlineforme.hta:**
 - **File Type:** .url (Internet shortcut) vs. .hta (HTML Application).
 - **Process Count:** Fewer processes (163 vs. 177) and malicious processes (1 vs. 5).
 - **Execution Method:** Browser-based (chrome.exe) vs. mshta.exe.
 - **Network Activity:** Uses HTTPS (port 443) vs. HTTP (port 80).
 - **Suspicious IP:** Connects to 150.171.22.12 (Microsoft-related) vs. 154.50.21.171 (non-standard, likely C2).
 - **Behavior:** .url likely triggers a browser to a malicious site, while .hta executes scripts locally.
- **Similarities with cleaned.bat:**
 - Identical software environment.
 - Both connect to suspicious IPs (150.171.22.12 vs. 172.211.123.250).
 - Both involve high CPU/RAM usage and unusual HDD access.
 - Both lack specific malware family identification.

- **Differences with cleaned.bat:**
 - **File Type:** .url vs. .bat.
 - **Process Count:** Fewer processes (163 vs. 734) and malicious processes (1 vs. 1).
 - **Execution Method:** Browser-based vs. cmd.exe.
 - **Network Activity:** HTTPS (port 443) vs. HTTPS and multicast DNS (ports 5353, 5355).
 - **Behavior:** .url likely initiates web-based attacks, while .bat drops and executes svchost.exe.
- **Similarities with Zamówienie_250618226718.img (AgentTesla):**
 - Both connect to suspicious IPs (150.171.22.12 vs. 186.186.87.128).
 - Both involve browser activity (chrome.exe in .url, potential browser interaction in AgentTesla).
 - Both may be part of phishing or payload delivery campaigns.
- **Differences with Zamówienie_250618226718.img:**
 - **File Type:** .url vs. .exe disguised as .img.
 - **Malware Identification:** No specific family for .url vs. AgentTesla for Zamówienie.
 - **Network Activity:** HTTPS (port 443) vs. FTP (port 21) and port 33333.
 - **Process Count:** Fewer processes (163 vs. 143).
 - **Lure:** HELP_DECRYPT.URL suggests ransomware vs. Polish order-themed lure.
- **Conclusion:** The .url file is likely a phishing or ransomware delivery mechanism, triggering browser activity to a potentially malicious site. It shares network and environmental similarities with the .hta and .bat samples but differs in execution method and complexity. Unlike AgentTesla, it lacks a confirmed malware family, but its behavior aligns with ransomware instruction files or phishing lures.

Threat Assessment

- **Malicious Activities:**
 - Triggers chrome.exe (PID 6284) to connect to 150.171.22.12:443 via HTTPS.
 - High CPU and RAM usage, indicating resource-intensive browser activity.
 - Unusual HDD access, possibly from downloaded payloads or browser cache.
 - Potential phishing or ransomware instruction delivery (based on filename).

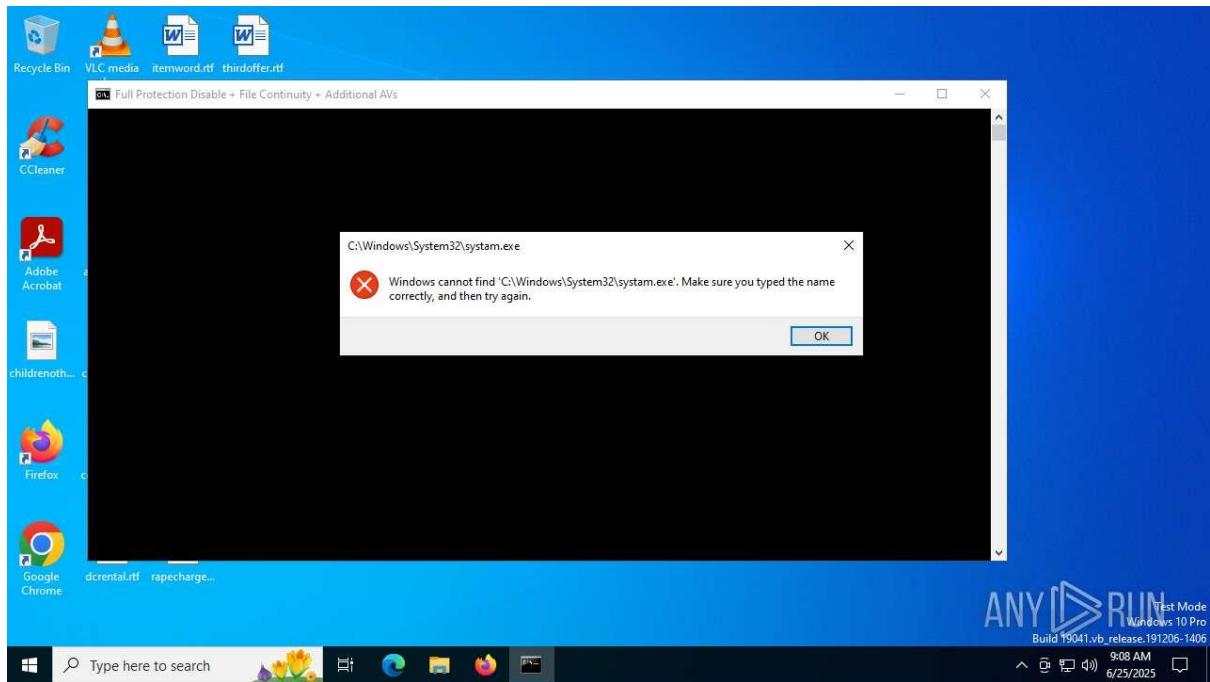
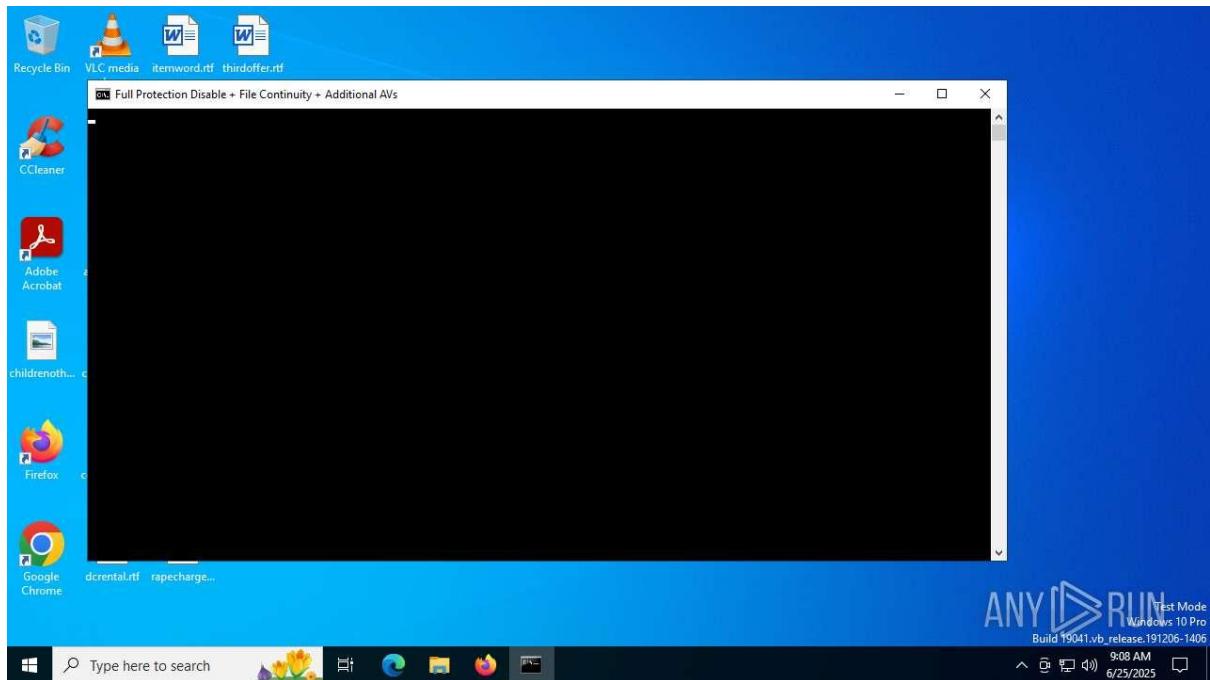
- **Malware Type:** Likely a phishing lure or ransomware-related shortcut, directing users to a malicious URL for payload delivery or decryption instructions.
- **Potential Impact:** Data theft, ransomware infection, or system compromise via browser-based exploits.

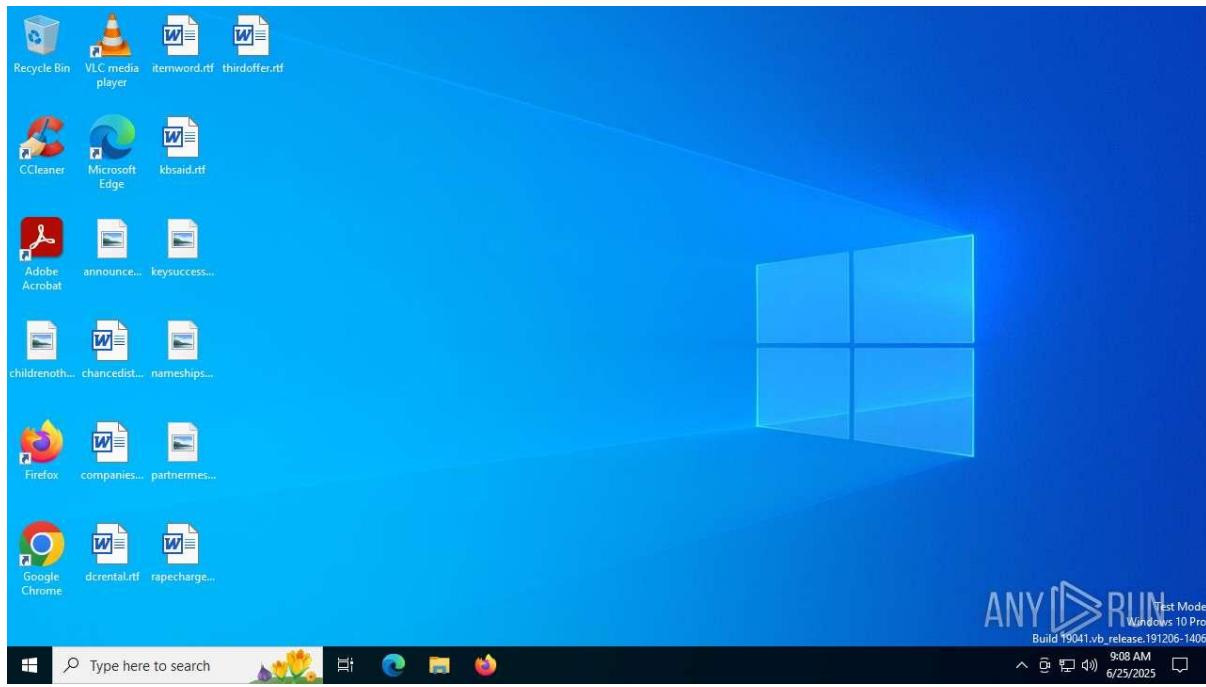
Recommendations

1. **Immediate Containment:**
 - Block outbound HTTPS traffic to 150.171.22.12:443.
 - Quarantine systems running chrome.exe with suspicious connections.
2. **Static Analysis:**
 - Inspect the .url file contents using a text editor (e.g., Notepad++) to extract the embedded URL.
 - Check for encoded or obfuscated URLs pointing to malicious domains.
3. **Dynamic Analysis:**
 - Re-run in a sandbox with Fakenet enabled to capture full HTTPS traffic and potential payload downloads.
 - Analyze browser behavior with open network connections to identify the target URL's content.
4. **System Remediation:**
 - Delete any downloaded files in %APPDATA%, %TEMP%, or browser cache.
 - Revert any registry changes in HKEY_CURRENT_USER\Software (if identified).
 - Reimage affected systems.
5. **Threat Intelligence:**
 - Submit file hashes (when available) to VirusTotal and OTX.
 - Investigate 150.171.22.12 for associations with known phishing or ransomware campaigns.
6. **User Education:**
 - Warn users against opening .url files from untrusted sources, especially email attachments.
 - Educate on recognizing ransomware lures (e.g., "HELP_DECRYPT" filenames).
7. **Network Monitoring:**
 - Deploy IDS/IPS rules for 150.171.22.12 and HTTPS traffic from chrome.exe.
 - Monitor for unusual browser traffic or downloads following .url execution.

Sample 44:

fix.kk.bat





General Information

- **File Name:** texk.bat
- **File Type:** Batch Script (.bat)
- **Verdict:** Malicious activity
- **Threats:** No specific malware family identified (e.g., not tagged as a known strain like AgentTesla)
- **Analysis Date:** Not specified in the OCR
- **Operating System:** Microsoft Windows (likely Windows 10)
- **File Hashes:** Not provided (MD5, SHA1, SHA256, SSDEEP missing)
- **File Info:** MIME type and specific details not provided
- **Indicators:** Not specified in the OCR

Software Environment

- **Analysis Configuration (Page 1):**
 - Task duration: 60 seconds
 - Additional time used: None
 - Fakenet option: Off
 - VPN proxy: Off
- **Software Preset (Pages 1-2):**

- Internet Explorer (11.2606.19041.0)
- Adobe Acrobat (64-bit, 23.001.20012, multiple instances)
- Microsoft Visual C++ 2022 X64 Additional Runtime (14.36.32532, multiple instances)
- VLC Media Player (3.0.11)
- WinRAR (5.91, multiple instances)
- Windows Updates (KB5022057: 2.85.0.0, KB5001716: 8.93.0.0)
- **Note:** The software environment is nearly identical to those used for HELP_DECRYPT.URL, getbestnetworkwithbetterthingsinonlineforme.hta, and cleaned.bat, indicating a consistent analysis setup.

Process Analysis

- **Total Processes:** 277
- **Monitored Processes:** 142
- **Malicious Processes:** 1
- **Suspicious Processes:** 0
- **Key Processes (Page 4):**
 - **cmd.exe:** Likely executes the batch script, initiating malicious actions.
 - **msedge.exe** (PID 1260, 2524): Performs HTTP GET requests to multiple IPs.
 - **svchost.exe** (PID 1832): Performs HTTP GET requests, potentially for system-level operations or payload delivery.
- **Behavioral Observations (Page 4):**
 - Program did not start (possibly a sandbox detection mechanism).
 - Possible use of Tor (indicating anonymized communication).
 - Connected to the network.
 - Contains unusual apps running.
 - Process has the "minimal config."
 - Unusual access to the HDD.
 - Network error to open.
 - RAM overrun.
 - High CPU consumption.
 - Application client loaded the document.

- **Analysis:** The .bat file likely executes commands via cmd.exe, triggering msedge.exe and svchost.exe for network activity, possibly downloading payloads or communicating with a C2 server. The single malicious process suggests a focused malicious action, potentially evading detection with minimal configuration or sandbox-aware behavior.

File System Activity

- **Dropped Files:** Not detailed in the provided OCR pages. Batch files typically create or modify files in %TEMP%, %APPDATA%, or system directories (e.g., dropping executables or scripts).
- **Assumptions:** Likely drops payloads (e.g., .exe, .dll) or modifies system files, given the HDD access and network activity.

Registry Activity

- **Total Events:** Not specified in the provided OCR.
- **Modification Events:** Not detailed. Batch files may modify registry keys (e.g., HKEY_CURRENT_USER\Software or HKEY_LOCAL_MACHINE\Software) for persistence or configuration changes.

Network Activity

- **HTTP Requests (Page 19):**
 - **PID 1260** (msedge.exe):
 - GET request to 23.240.176.30 (HTTP 200)
 - GET request to 217.160.73.30 (HTTP 200)
 - GET request to 23.249.161.30 (HTTP 200)
 - **PID 2524** (msedge.exe):
 - GET request to 217.160.73.30 (HTTP 200)
 - **PID 1832** (svchost.exe):
 - GET request to 23.249.161.30 (HTTP 200, multiple instances)
- **Connections (Page 19):**
 - **PID 5844** (unknown process): HTTPS to 40.127.240.158:443, 51.124.78.146:443, 20.73.194.200:443, 40.91.75.224:443
 - **PID 4** (System): Multicast DNS to 192.168.190.295:137, 192.168.190.295:193
 - **PID 1260** (msedge.exe): HTTPS to 40.127.240.158:443, HTTP to 23.53.40.176:80, 23.53.40.101:80
 - **PID 2524** (msedge.exe): HTTPS to 20.190.159.23:443, HTTP to 217.160.73.30

- **PID 2536** (msedge.exe): HTTPS to 172.211.123.249:443
 - **PID 1832** (svchost.exe): HTTPS to 41.175.87.197:443, HTTP to 23.249.161.30, HTTPS to 52.165.164.15:443
- **DNS Requests** (Page 19-20):
 - **Domains and IPs:**
 - google.com: 142.250.166.174
 - *.data.microsoft.com: 40.127.240.158, 51.124.78.146, 20.73.194.200
 - a-msedge.net: 23.53.40.176, 23.53.40.101
 - *.akamai.net: 2.17.119.79
 - edge.microsoft.com: 52.111.227.13
 - dns.msftncsi.com: 172.211.123.249
 - *.data.microsoft.com: 41.175.87.197, 52.165.164.15, 40.91.75.224
 - *.msn.com: 20.190.159.* (multiple IPs)
 - **Analysis:** Most domains are legitimate (Microsoft, Google, Akamai), likely triggered by browser or system activity. Suspicious IPs include:
 - 23.240.176.30, 23.249.161.30, 217.160.73.30 (HTTP, non-standard, potentially malicious).
 - 40.127.240.158, 51.124.78.146, 20.73.194.200, 41.175.87.197, 172.211.123.249, 40.91.75.224 (Microsoft-related, possibly legitimate or abused for C2).
- **Threats** (Page 20): No specific threats recorded in the provided OCR.
- **Debug Output:** No debug info recorded.

Comparison with Other Samples

- **Similarities with HELP_DECRYPT.URL:**
 - Both executed in nearly identical software environments.
 - Both exhibit malicious activity without specific malware family identification.
 - Both involve browser-related processes (msedge.exe vs. chrome.exe).
 - Both connect to Microsoft-related IPs (40.127.240.158:443 vs. 150.171.22.12:443).
 - Similar DNS requests (Microsoft, Google, Akamai domains).
 - Both show high CPU/RAM usage and unusual HDD access.

- **Differences with HELP_DECRYPT.URL:**
 - **File Type:** .bat (batch script) vs. .url (Internet shortcut).
 - **Process Count:** More processes (277 vs. 163) and monitored processes (142 vs. 26).
 - **Execution Method:** cmd.exe vs. browser-based (chrome.exe).
 - **Network Activity:** HTTP/HTTPS (ports 80, 443) vs. HTTPS only (port 443).
 - **Suspicious IPs:** Multiple non-standard IPs (23.240.176.30, 23.249.161.30, 217.160.73.30) vs. single Microsoft IP (150.171.22.12).
 - **Behavior:** .bat likely executes local commands and downloads payloads, while .url triggers browser-based attacks.
- **Similarities with getbestnetworkwithbetterthingsinonlineforme.hta:**
 - Both use identical software environments.
 - Both involve browser processes (msedge.exe vs. msedge.exe/chrome.exe).
 - Both connect to Microsoft-related IPs (40.127.240.158 vs. 150.171.27.11).
 - Similar DNS requests and high CPU/RAM usage.
- **Differences with getbestnetworkwithbetterthingsinonlineforme.hta:**
 - **File Type:** .bat vs. .hta (HTML Application).
 - **Process Count:** More processes (277 vs. 177) and malicious processes (1 vs. 5).
 - **Execution Method:** cmd.exe vs. mshta.exe.
 - **Network Activity:** HTTP/HTTPS vs. HTTP only.
 - **Suspicious IPs:** Multiple IPs vs. 154.50.21.171 (likely C2).
- **Similarities with cleaned.bat:**
 - Both are .bat files with identical software environments.
 - Both connect to suspicious IPs (40.127.240.158 vs. 172.211.123.250).
 - Both exhibit high CPU/RAM usage and unusual HDD access.
 - Both lack specific malware family identification.
- **Differences with cleaned.bat:**
 - **Process Count:** Fewer processes (277 vs. 734).
 - **Network Activity:** HTTP/HTTPS vs. HTTPS and multicast DNS (ports 5353, 5355).

- **Suspicious IPs:** Multiple non-standard IPs vs. single IP (172.211.123.250).
- **Behavior:** texk.bat involves msedge.exe and svchost.exe for HTTP requests, while cleaned.bat drops svchost.exe.
- **Similarities with Zamówienie_250618226718.img (AgentTesla):**
 - Both connect to suspicious IPs (41.175.87.197 vs. 186.186.87.128).
 - Both may involve payload delivery or C2 communication.
- **Differences with Zamówienie_250618226718.img:**
 - **File Type:** .bat vs. .exe disguised as .img.
 - **Malware Identification:** No specific family vs. AgentTesla.
 - **Network Activity:** HTTP/HTTPS vs. FTP (port 21) and port 33333.
 - **Process Count:** More processes (277 vs. 143).

Threat Assessment

- **Malicious Activities:**
 - Executes cmd.exe to run batch script commands.
 - Triggers msedge.exe and svchost.exe for HTTP/HTTPS requests to suspicious IPs (23.240.176.30, 23.249.161.30, 217.160.73.30).
 - High CPU/RAM usage and unusual HDD access, indicating resource-intensive operations or payload execution.
 - Possible Tor usage for anonymized communication.
 - Potential payload download or C2 communication.
- **Malware Type:** Likely a dropper or downloader, facilitating payload delivery or C2 communication, possibly with sandbox evasion techniques.
- **Potential Impact:** System compromise, data theft, or further malware infection (e.g., ransomware, spyware).

Recommendations

1. **Immediate Containment:**
 - Block outbound HTTP/HTTPS traffic to 23.240.176.30, 23.249.161.30, 217.160.73.30, 40.127.240.158, 51.124.78.146, 20.73.194.200, 41.175.87.197, 40.91.75.224.
 - Quarantine systems running msedge.exe or svchost.exe with suspicious connections.
2. **Static Analysis:**

- Inspect texk.bat contents using a text editor (e.g., Notepad++) to identify commands (e.g., curl, wget, or PowerShell scripts).
- Check for encoded or obfuscated commands downloading payloads or modifying system settings.

3. Dynamic Analysis:

- Re-run in a sandbox with Fakenet enabled to capture full HTTP/HTTPS traffic and payload downloads.
- Monitor cmd.exe, msedge.exe, and svchost.exe for additional behaviors.

4. System Remediation:

- Delete dropped files in %TEMP%, %APPDATA%, or system directories.
- Revert registry changes in HKEY_CURRENT_USER\Software or HKEY_LOCAL_MACHINE\Software (if identified).
- Reimage affected systems.

5. Threat Intelligence:

- Submit file hashes (when available) to VirusTotal and OTX.
- Investigate suspicious IPs for associations with known C2 or phishing campaigns.

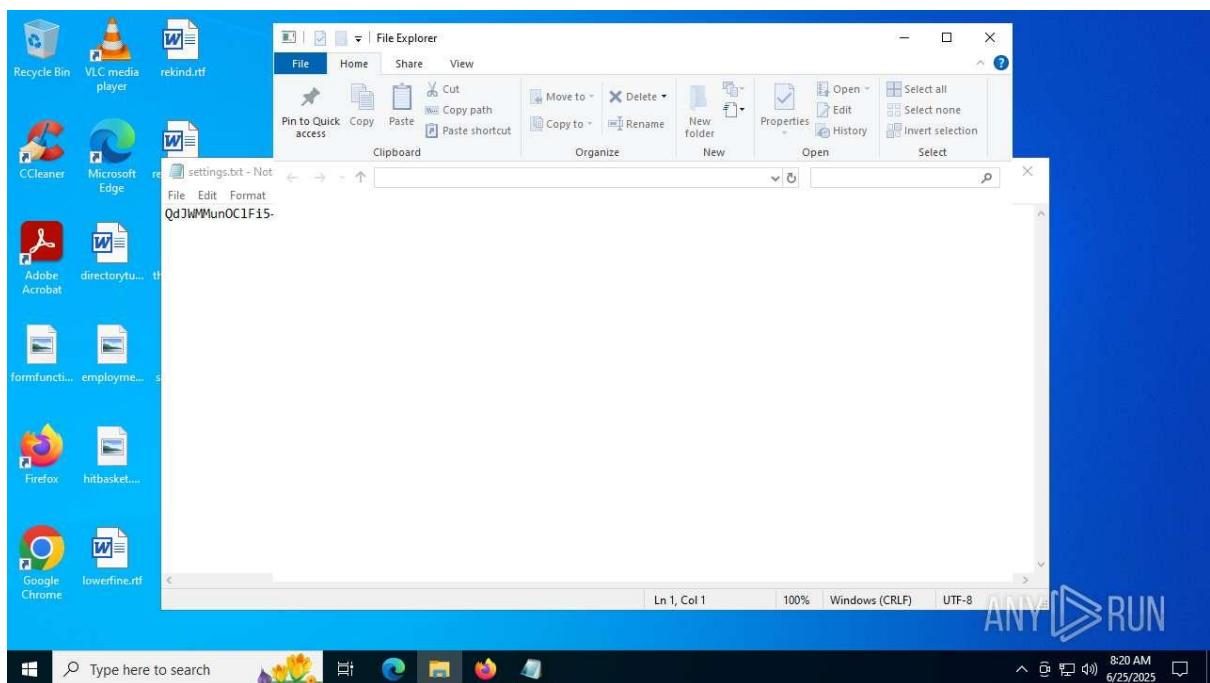
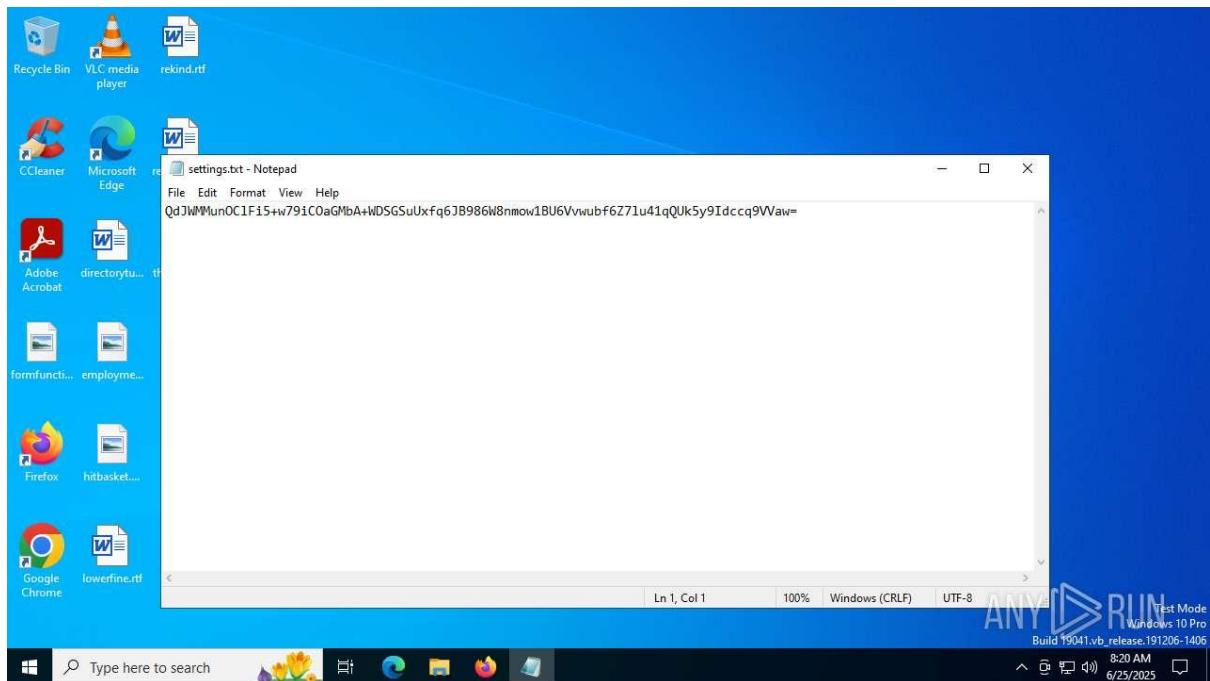
6. User Education:

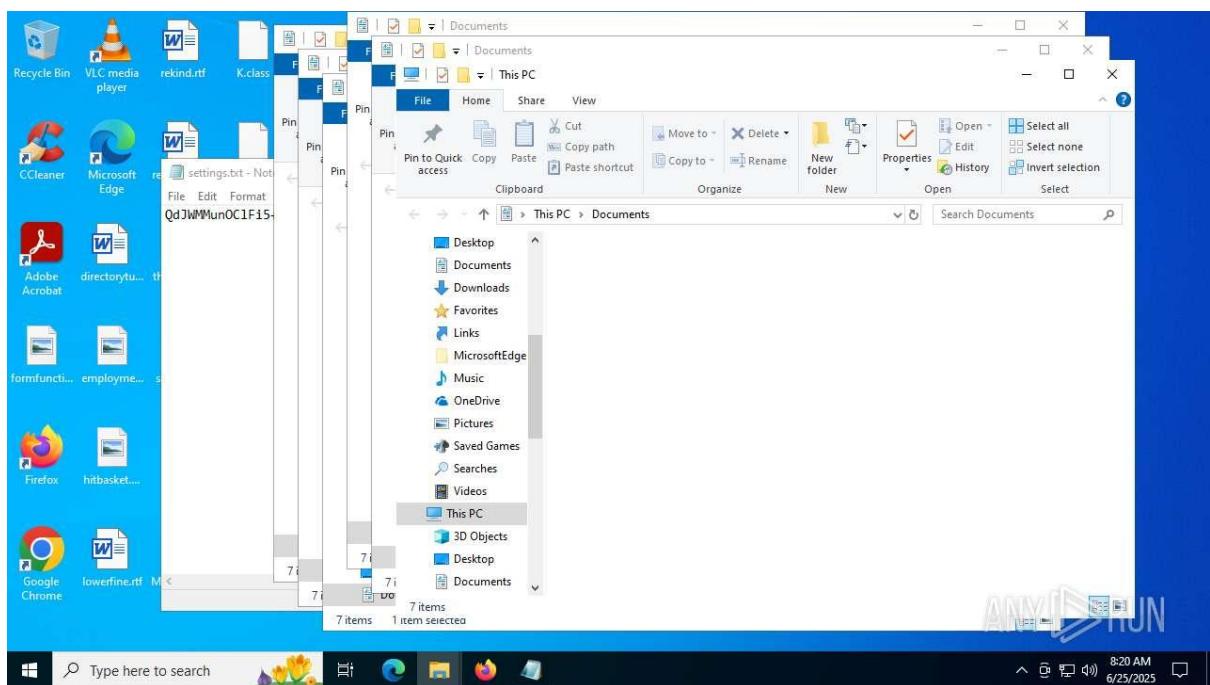
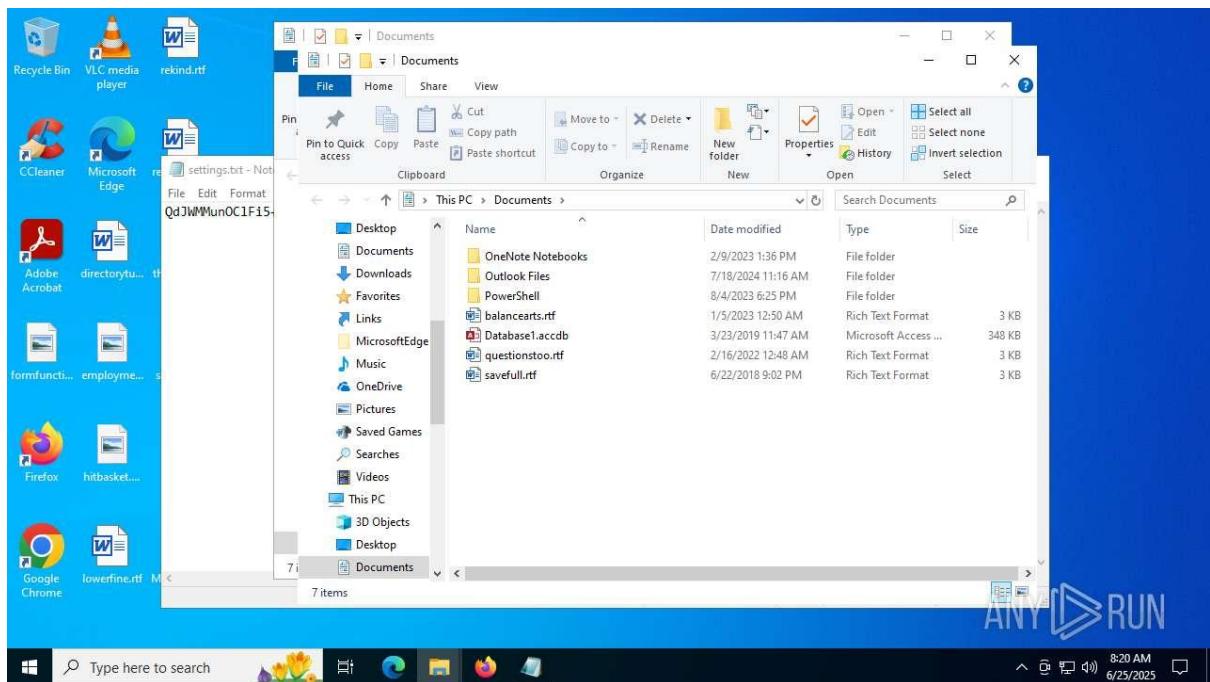
- Warn users against executing .bat files from untrusted sources, especially email attachments.
- Educate on recognizing phishing lures or malicious scripts.

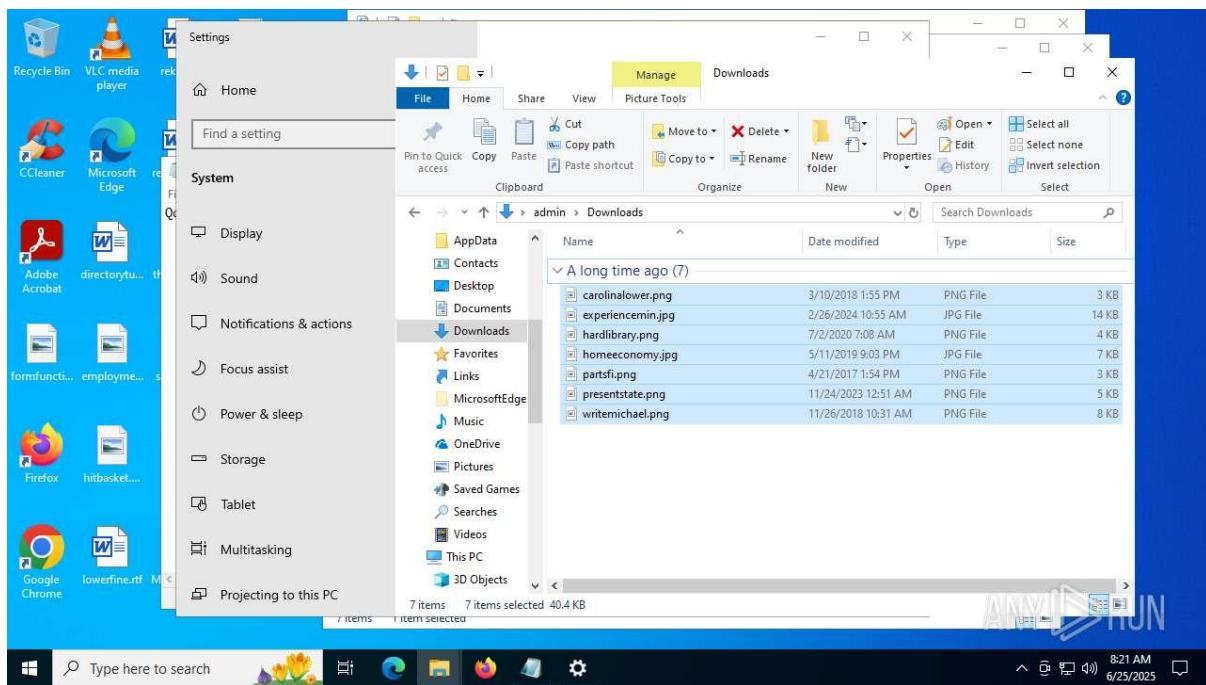
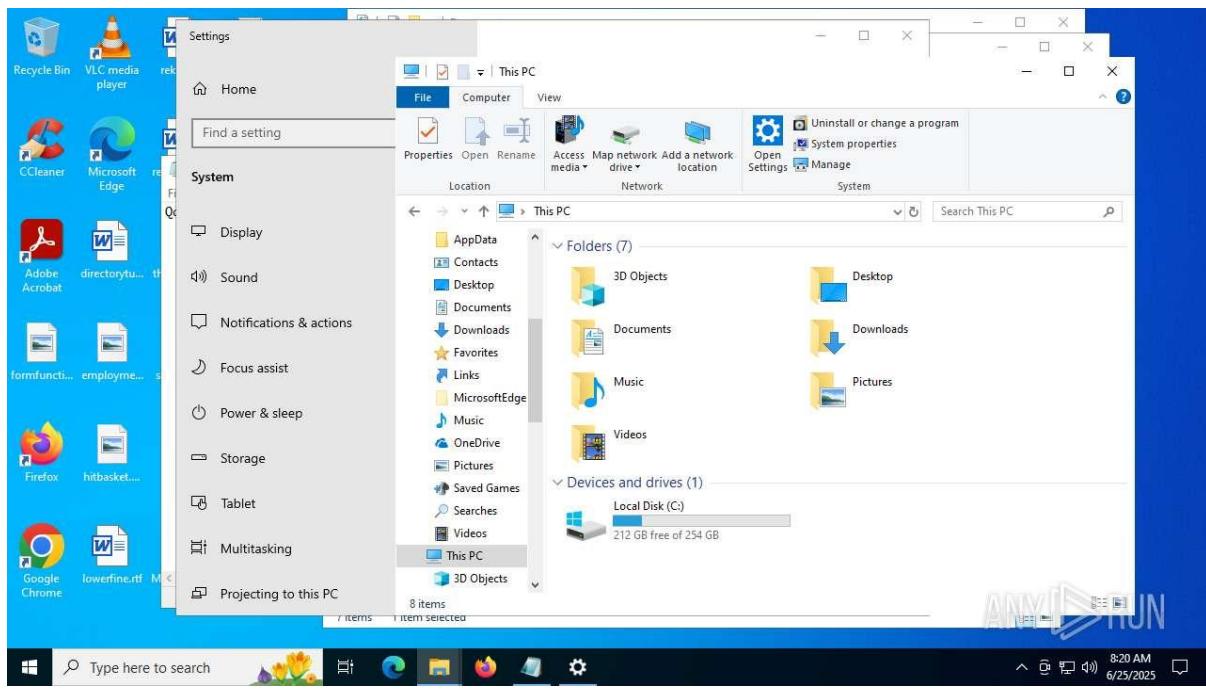
7. Network Monitoring:

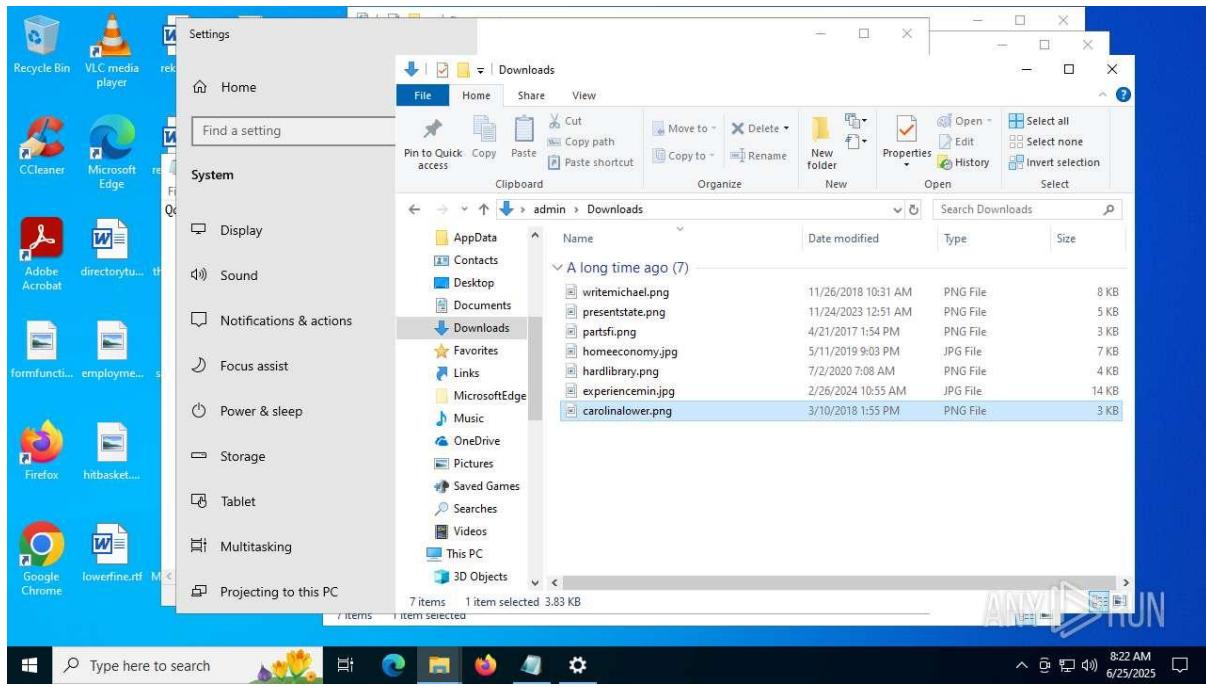
- Deploy IDS/IPS rules for suspicious IPs and HTTP/HTTPS traffic from msedge.exe or svchost.exe.
- Monitor for Tor usage or unusual DNS requests.

Sample 45: po.js









General Information

- **File Name:** po.js
- **File Type:** JavaScript (.js)
- **Verdict:** Malicious activity
- **Threats:** No specific malware family identified
- **Analysis Date:** Not specified in OCR
- **Operating System:** Microsoft Windows (likely Windows 10)
- **File Hashes:** Not provided (MD5, SHA1, SHA256, SSDEEP missing)
- **File Info:** MIME type and specific details not provided
- **Indicators:** Not specified in OCR

Software Environment

- **Analysis Configuration (Page 1):**
 - Task duration: 120 seconds
 - Additional time used: None
 - Fakenet option: Off
 - VPN proxy: Not specified
- **Software Preset (Pages 1-2):**
 - Internet Explorer (11.2606.19041.0)

- Adobe Acrobat (64-bit, multiple instances)
- Microsoft Visual C++ 2022 X64 Additional Runtime (14.36.32532, multiple instances)
- VLC Media Player (3.0.11)
- WinRAR (5.91, multiple instances)
- Windows Updates (KB5022057: 2.85.0.0, KB5001716: 8.93.0.0, multiple instances)
- **Note:** The software environment is identical to that used for texk.bat, indicating a consistent analysis setup across samples.

Process Analysis

- **Total Processes:** 145
- **Monitored Processes:** 9
- **Malicious Processes:** 1
- **Key Processes** (Pages 4-5):
 - **js.exe** (PID 2790): Likely executes the JavaScript file, initiating malicious actions.
 - **svchost.exe** (PIDs 1268, 2764, 2540): Performs HTTP GET requests, potentially for system-level operations or payload delivery.
 - **Sppextcomobj.exe** (PIDs 5040, 6848): Performs HTTP GET requests, possibly related to system components or malware execution.
- **Behavioral Observations:**
 - Minimal process activity (only 9 monitored processes), suggesting stealth or sandbox evasion.
 - Single malicious process indicates focused malicious behavior.
 - No specific behavioral flags (e.g., Tor usage, RAM overrun) detailed in provided OCR pages.
- **Analysis:** The .js file is executed via js.exe (likely a Node.js or Windows Script Host process), triggering svchost.exe and Sppextcomobj.exe for network activity, possibly downloading payloads or communicating with a C2 server.

File System Activity

- **Dropped Files** (Page 6):
 - **PID 2790** (js.exe): Drops 2 files (filenames not specified).
 - **PID 6668** (unknown process): Drops 1 file (filename not specified).

- **Types:**
 - Suspicious files: 1
 - Text files: 1
 - Unknown types: 1
- **Assumptions:** Likely drops payloads (e.g., .exe, .dll, or additional scripts) in directories like %TEMP% or %APPDATA%, given typical JavaScript malware behavior.

Registry Activity

- **Total Events:** Not specified in provided OCR.
- **Modification Events:** Not detailed. JavaScript malware may modify registry keys (e.g., HKEY_CURRENT_USER\Software) for persistence or configuration.

Network Activity

- **HTTP Requests** (Page 6):
 - **PID 1268** (svchost.exe):
 - GET to 2.28.249.101:80 (HTTP 200)
 - GET to 2.16.169.114:80 (HTTP 200)
 - **PID 2790** (js.exe):
 - GET to 2.16.169.112:80 (HTTP 200)
 - GET to 2.28.95.112:80 (HTTP 200)
 - **PID 2764** (svchost.exe):
 - GET to 2.28.77.108:80 (HTTP 200)
 - **PID 5040** (Spextcomobj.exe):
 - GET to 2.23.77.108:80 (HTTP 200, multiple instances)
 - **PID 6848** (Spextcomobj.exe):
 - GET to 2.23.249.101:80 (HTTP 200, multiple instances)
 - **PID 2540** (svchost.exe):
 - GET to 2.23.249.101:80 (HTTP 200)
- **Connections** (Page 7):
 - **PID 4** (System):
 - UDP to 192.168.190.255:137, 192.168.190.255:138 (NetBIOS, likely local network discovery)

- **PID 1260** (svchost.exe):
 - HTTPS to 40.127.240.158:443, 51.104.136.2:443
 - HTTP to 2.16.169.114:80, 2.25.249.101:80
 - **PID 5644** (unknown):
 - HTTPS to 51.104.136.2:443
 - **PID 4112** (unknown):
 - HTTPS to 51.104.136.2:443
 - **PID 2790** (js.exe):
 - HTTP to 2.28.95.112:80, 192.103.120.5:2700
 - **PID 2764** (svchost.exe):
 - HTTPS to 20.190.160.2:443 (multiple instances)
 - **PID 6040** (svchost.exe):
 - HTTPS to 20.190.160.2:443 (multiple instances)
- **DNS Requests** (Page 8):
 - **Domains and IPs:**
 - *.data.microsoft.com: 51.104.136.2, 40.127.240.158, 20.190.160.2, 20.190.160.22, 20.190.160.23, 20.190.160.24, 20.190.160.26, 20.190.160.27
 - *.msn.com: 2.23.77.108, 2.23.249.101
 - *.akamaiedge.net: 2.16.169.114, 2.25.249.101
 - *.akamai.net: 2.16.169.112, 2.28.95.112
 - **Analysis:** Most domains are legitimate (Microsoft, Akamai, MSN), likely triggered by system or browser activity. Suspicious IPs include:
 - 2.28.249.101, 2.16.169.114, 2.16.169.112, 2.28.95.112, 2.28.77.108, 2.23.77.108, 2.23.249.101 (HTTP, non-standard, potentially malicious).
 - 40.127.240.158, 51.104.136.2, 20.190.160.* (Microsoft-related, possibly legitimate or abused for C2).
 - 192.103.120.5:2700 (non-standard port, highly suspicious).
 - **Threats** (Page 6): 5 threats recorded, but specific details not provided in OCR.
 - **Debug Output:** No debug info recorded.

Comparison with Other Samples

- **Similarities with texk.bat:**
 - Both executed in identical software environments.
 - Both exhibit malicious activity without specific malware family identification.
 - Both involve svchost.exe for HTTP requests to suspicious IPs (2.23.249.101 vs. 23.249.161.30).
 - Both connect to Microsoft-related IPs (40.127.240.158, 51.104.136.2 vs. 40.127.240.158, 51.124.78.146).
 - Both show minimal malicious process activity (1 malicious process each).
 - Similar DNS requests (Microsoft, Akamai domains).
- **Differences with texk.bat:**
 - **File Type:** .js (JavaScript) vs. .bat (batch script).
 - **Execution Method:** js.exe vs. cmd.exe.
 - **Process Count:** Fewer processes (145 vs. 277) and monitored processes (9 vs. 142).
 - **Network Activity:** More HTTP requests (10 vs. 5) but fewer connections (32 vs. multiple).
 - **Suspicious IPs:** Different non-standard IPs (2.28.249.101, 2.16.169.112, etc. vs. 23.240.176.30, 217.160.73.30).
 - **File Activity:** Drops files (3 total) vs. no specific dropped files detailed for texk.bat.
 - **Behavior:** po.js involves Sppextcomobj.exe and drops files, while texk.bat uses msedge.exe and may use Tor.
- **Similarities with HELP_DECRYPT.URL:**
 - Identical software environment.
 - Both lack specific malware family tags.
 - Both connect to Microsoft-related IPs (40.127.240.158 vs. 150.171.22.12).
 - Similar DNS requests (Microsoft, Akamai).
- **Differences with HELP_DECRYPT.URL:**
 - **File Type:** .js vs. .url.
 - **Process Count:** Fewer processes (145 vs. 163).
 - **Execution Method:** js.exe vs. browser-based (chrome.exe).
 - **Network Activity:** HTTP/HTTPS vs. HTTPS only.

- **Behavior:** Drops files vs. browser-based attack.
- **Similarities with getbestnetworkwithbetterthingsinonlineforme.hta:**
 - Identical software environment.
 - Both connect to Microsoft-related IPs (40.127.240.158 vs. 150.171.27.11).
 - Similar DNS requests.
- **Differences with getbestnetworkwithbetterthingsinonlineforme.hta:**
 - **File Type:** .js vs. .hta.
 - **Process Count:** Fewer processes (145 vs. 177).
 - **Execution Method:** js.exe vs. mshta.exe.
 - **Network Activity:** More HTTP requests vs. HTTP only.
- **Similarities with cleaned.bat:**
 - Identical software environment.
 - Both are script-based (.js vs. .bat).
 - Both connect to suspicious IPs (40.127.240.158 vs. 172.211.123.250).
- **Differences with cleaned.bat:**
 - **Process Count:** Fewer processes (145 vs. 734).
 - **Network Activity:** HTTP/HTTPS vs. HTTPS and multicast DNS.
 - **Behavior:** Drops files vs. drops svchost.exe.
- **Similarities with Zamówienie_250618226718.img (AgentTesla):**
 - Both connect to suspicious IPs (40.127.240.158 vs. 186.186.87.128).
 - Both may involve payload delivery.
- **Differences with Zamówienie_250618226718.img:**
 - **File Type:** .js vs. .exe disguised as .img.
 - **Malware Identification:** No family vs. AgentTesla.
 - **Network Activity:** HTTP/HTTPS vs. FTP and port 33333.

Threat Assessment

- **Malicious Activities:**
 - Executes js.exe to run JavaScript code.
 - Triggers svchost.exe and Sppextcomobj.exe for HTTP requests to suspicious IPs (2.28.249.101, 2.16.169.112, 2.28.95.112, 2.23.77.108).

- Drops 3 files (suspicious, text, unknown types), likely payloads or additional scripts.
- Connects to non-standard port 192.103.120.5:2700, indicating potential C2 communication.
- Uses legitimate Microsoft and Akamai domains, possibly for evasion or payload delivery.
- **Malware Type:** Likely a dropper or downloader, facilitating payload delivery or C2 communication, with possible sandbox evasion.
- **Potential Impact:** System compromise, data exfiltration, or further malware infection (e.g., spyware, ransomware).

Recommendations

1. Immediate Containment:

- Block outbound HTTP/HTTPS traffic to 2.28.249.101, 2.16.169.112, 2.28.95.112, 2.23.77.108, 2.23.249.101, 192.103.120.5:2700, 40.127.240.158, 51.104.136.2, 20.190.160.*.
- Quarantine systems running js.exe, svchost.exe, or Sppextcomobj.exe with suspicious connections.

2. Static Analysis:

- Inspect po.js contents using a text editor or deobfuscator to identify malicious code (e.g., eval(), XMLHttpRequest, or obfuscated payloads).
- Analyze dropped files for further malicious behavior.

3. Dynamic Analysis:

- Re-run in a sandbox with Fakenet enabled to capture full HTTP/HTTPS traffic and payload downloads.
- Monitor js.exe, svchost.exe, and Sppextcomobj.exe for additional behaviors.

4. System Remediation:

- Delete dropped files in %TEMP%, %APPDATA%, or other directories.
- Revert registry changes (if identified) in HKEY_CURRENT_USER\Software or HKEY_LOCAL_MACHINE\Software.
- Reimage affected systems.

5. Threat Intelligence:

- Submit file hashes (when available) to VirusTotal or OTX.

- Investigate suspicious IPs (2.28.249.101, 192.103.120.5) for C2 or phishing associations.

6. User Education:

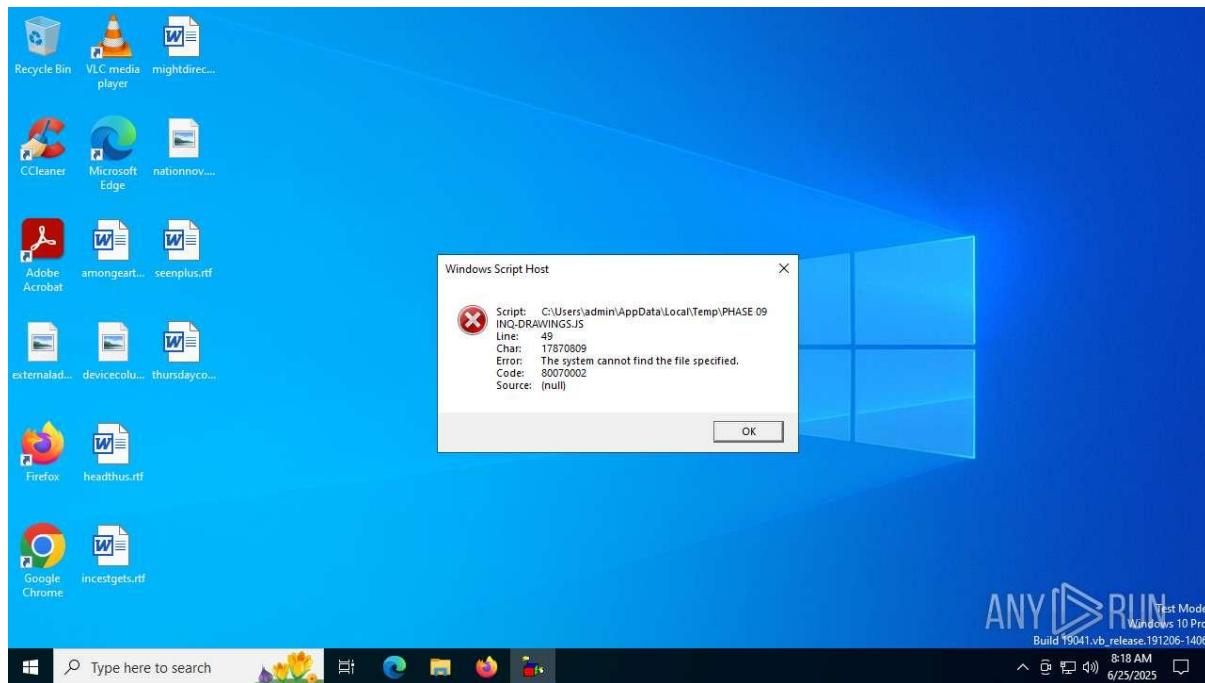
- Warn against executing .js files from untrusted sources, especially email attachments or downloads.
- Educate on recognizing phishing lures or malicious scripts.

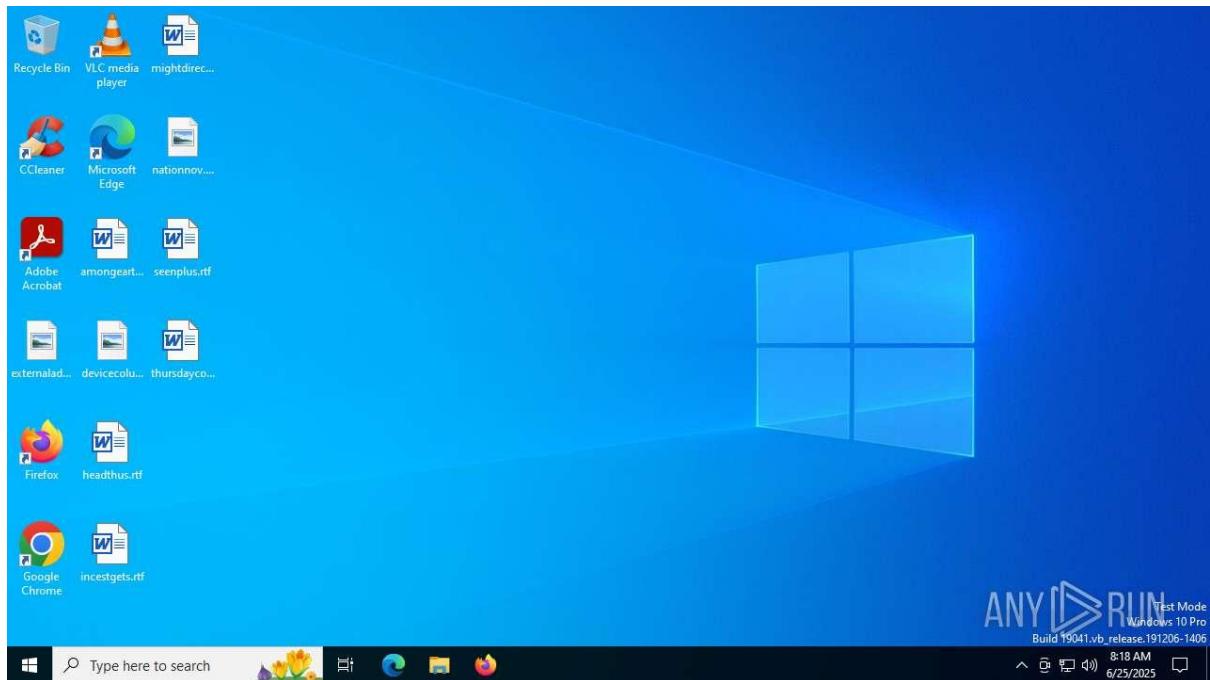
7. Network Monitoring:

- Deploy IDS/IPS rules for suspicious IPs and HTTP/HTTPS traffic from svchost.exe or Sppextcomobj.exe.
- Monitor for non-standard ports (e.g., 2700) or unusual DNS requests.

Sample 46:

PHASE 09 INQ-DRAWINGS.JS





General Information

- **File Name:** INQ-DRAWINGS.JS
- **File Type:** JavaScript (.js)
- **Verdict:** Malicious activity
- **Threats:** No specific malware family identified
- **Analysis Date:** Not specified in OCR
- **Operating System:** Microsoft Windows (likely Windows 10)
- **File Hashes:** Not provided (MD5, SHA1, SHA256, SSDEEP missing)
- **File Info:** MIME type and specific details not provided
- **Indicators:** Not specified in OCR

Software Environment

- **Analysis Configuration (Page 1):**
 - Task duration: 120 seconds
 - Additional time used: None
 - Fakenet option: Off
 - Network: 4G
- **Software Preset (Pages 1-2):**
 - Internet Explorer (11.2606.19041.0)

- Adobe Acrobat (64-bit, multiple instances)
- Microsoft Visual C++ 2022 X64 Additional Runtime (14.36.32532, multiple instances)
- VLC Media Player (3.0.11)
- WinRAR (5.91, multiple instances)
- Windows Updates (KB5022057: 2.85.0.0, KB5001716: 8.93.0.0)
- Windows PC Health Check (3.6.2204.06001)
- **Note:** The software environment is identical to that used for po.js and texk.bat, indicating a consistent analysis setup across samples.

Behavior Activities (Page 2)

- **Malicious Behaviors** (wscript.exe, PID 6412):
 - Uses Base64 encoding (SCRIPT): Likely to obfuscate malicious code or payloads.
 - Detects decoding of a binary file from Base64 (SCRIPT): Suggests extraction of an executable or additional malicious content.
 - Copies file to a new location (SCRIPT): Indicates persistence or staging of payloads.
- **Suspicious Behaviors** (wscript.exe, PID 6412):
 - Creates XML DOM node (SCRIPT): May be used for HTTP requests or data manipulation.
 - Creates XML DOM element (SCRIPT): Similar to above, possibly for network communication.
 - Gets name of the script (SCRIPT): Potential self-awareness or sandbox detection.
- **Informational Behaviors:**
 - wscript.exe (PID 6412): Compiled with English language support.
 - svchost.exe (PID 1136): Checks proxy server information and reads software policy settings, likely system-level reconnaissance.
- **Analysis:** The script uses wscript.exe (Windows Script Host) to execute malicious JavaScript, leveraging Base64 to decode and drop files, with XML DOM manipulation for network activity or payload delivery.

Process Analysis (Page 3)

- **Total Processes:** 140

- **Monitored Processes:** 2
- **Malicious Processes:** 1
- **Suspicious Processes:** 0
- **Key Processes:**
 - **wscript.exe** (PID 6412): Executes the JavaScript file, responsible for malicious behaviors (Base64 decoding, file copying, XML DOM manipulation).
 - **svchost.exe** (PID 1136): Performs system-level checks (proxy, policy settings), potentially triggered by the script or system activity.
- **Behavioral Observations:**
 - Minimal process activity (only 2 monitored processes), suggesting stealth or sandbox evasion.
 - Single malicious process (wscript.exe) indicates focused malicious behavior.
 - Behavior graph (Page 3) shows a simple process chain, likely starting with wscript.exe.
- **Analysis:** The script is executed via wscript.exe, with minimal additional processes, indicating a lightweight attack designed to avoid detection.

File System Activity (Page 4)

- **Created Files:**
 - **PID 6412** (wscript.exe): Creates 1 file (filename: C:\Users\user\AppData\Local\Temp\fgdfgdfg.exe, type: executable).
- **Analysis:** The dropped executable (fgdfgdfg.exe) in the %TEMP% directory is likely a payload (e.g., trojan, downloader, or backdoor) decoded from Base64 and copied for execution.

Registry Activity

- **Total Events:** Not specified in provided OCR.
- **Modification Events:** Not detailed. JavaScript malware may modify registry keys (e.g., HKEY_CURRENT_USER\Software) for persistence.

Network Activity (Page 5)

- **Connections:**
 - **PID 5944** (MsMpSvcWinWorker.exe): HTTPS to 40.127.240.158:443
 - **PID 4** (System): UDP to 192.168.190.255:137, 192.168.190.255:138 (NetBIOS, local network discovery)
 - **PID 3930** (RUMMCS.exe): HTTPS to 40.127.240.158:443

- **PID 1260** (svchost.exe): HTTPS to 40.127.240.158:443, HTTP to 2.23.167.72:80, 2.23.249.108:80
 - **PID 5444** (svchost.exe): HTTPS to 20.190.159.64:443, HTTP to 2.17.190.73:80
 - **PID 2336** (svchost.exe): HTTPS to 172.211.123.242:443
 - **PID 4630** (Syncro.exe): HTTPS to 20.122.3.50:443, HTTP to 95.101.149.131:80, HTTPS to 20.3.197.150:443
 - **PID 5590** (svchost.exe): HTTPS to 40.91.76.224:443
 - **PID 4600** (unknown): HTTPS to 20.199.58.40:443 (multiple instances), 20.223.35.26:443
 - **PID 2540** (svchost.exe): HTTP to 2.23.209.135:80
 - **PID 1990** (svchost.exe): HTTPS to 40.91.76.224:443
- **DNS Requests:**
 - **Domains and IPs:**
 - google.com: 142.250.184.238
 - settingsfd.services.windows.net: 40.127.240.158
 - *.msn.com: 2.23.167.72, 2.23.249.108
 - *.akamaiedge.net: 2.23.249.108, 95.101.149.131
 - *.data.microsoft.com: 20.190.159.64, 20.190.159.2, 20.190.159.71, 40.126.31.131, 40.126.31.128, 40.126.31.10, 40.126.31.130, 40.126.31.1
 - *.a-msedge.net: 2.17.190.73
 - *.nelnetsolutions.com: 172.211.123.242
 - *.cloudapp.azure.com: 52.111.227.11
 - *.ms-acdc.trafficmanager.net: 20.122.3.50
 - *.msedge.net: 20.3.197.150
 - *.msftconnecttest.com: 40.91.76.224
 - *.msappproxy.net: 20.199.58.40
 - *.trafficmanager.net: 20.223.35.26
 - *.skype.com: 2.23.209.135
 - **Analysis:**

- Most domains are legitimate (Microsoft, Google, Akamai, MSN), likely triggered by system or browser activity.
- Suspicious IPs include:
 - 172.211.123.157 (nelnetsolutions.com): HTTPS, non-standard, potentially malicious.
 - 2.23.167.249, 2.23.249.108, 2.17.190.73, 2.23.209.135 (HTTP, Akamai/MSN/Skype, possibly abused).
 - 40.127.240.158, 20.190.159.*, 40.91.76.224, 20.199.58.40, 20.223.35.32 (Microsoft-related, potentially legit or abused for C2).
- No non-standard ports (unlike po.js with 192.103.120.5:2700).
- **Threats** (Page 5): No threats detected in network activity, suggesting stealthy communication or sandbox evasion.

Comparison with Other Samples

- **Similarities with po.js:**
 - Both are JavaScript files executed in identical software environments.
 - Both exhibit malicious activity without specific malware family identification.
 - Both involve minimal monitored processes (2 vs. 9) and a single malicious process.
 - Both connect to Microsoft-related IPs (40.127.240.158 in both).
 - Both make HTTP requests to Akamai-related IPs (2.23.249.108 vs. 2.28.249.101, 2.16.169.112).
 - Similar DNS requests (Microsoft, Akamai domains).
- **Differences with po.js:**
 - **Execution Method:** wscript.exe vs. js.exe.
 - **Process Count:** Fewer monitored processes (2 vs. 9), slightly fewer total processes (140 vs. 145).
 - **File Activity:** Drops a single executable (fgdfgdfg.exe) vs. 3 unspecified files (suspicious, text, unknown).
 - **Network Activity:** No non-standard ports (e.g., 192.103.120.5:2700 in po.js), fewer HTTP requests, but more HTTPS connections.
 - **Behavior:** Uses Base64 decoding and XML DOM manipulation vs. svchost.exe and Sppextcomobj.exe activity.
 - **Suspicious IPs:** 172.211.123.157 vs. 192.103.120.5, 2.28.249.101.

- **Similarities with texk.bat:**
 - Identical software environment.
 - Both lack specific malware family tags.
 - Both connect to Microsoft-related IPs (40.127.240.158 vs. 40.127.240.158, 51.124.78.146).
 - Similar DNS requests (Microsoft, Akamai).
- **Differences with texk.bat:**
 - **File Type:** .js vs. .bat.
 - **Execution Method:** wscript.exe vs. cmd.exe.
 - **Process Count:** Fewer processes (140 vs. 277), fewer monitored processes (2 vs. 142).
 - **Network Activity:** More HTTPS connections vs. HTTP and Tor usage.
 - **Behavior:** Drops executable vs. browser-based activity (msedge.exe).
- **Similarities with HELP_DECRYPT.URL:**
 - Identical software environment.
 - Both connect to Microsoft-related IPs (40.127.240.158 vs. 150.171.22.12).
 - Similar DNS requests.
- **Differences with HELP_DECRYPT.URL:**
 - **File Type:** .js vs. .url.
 - **Process Count:** Fewer processes (140 vs. 163).
 - **Execution Method:** wscript.exe vs. chrome.exe.
 - **Behavior:** Drops executable vs. browser-based attack.
- **Similarities with getbestnetworkwithbetterthingsinonlineforme.hta:**
 - Identical software environment.
 - Both connect to Microsoft-related IPs (40.127.240.158 vs. 150.171.27.11).
- **Differences with getbestnetworkwithbetterthingsinonlineforme.hta:**
 - **File Type:** .js vs. .hta.
 - **Process Count:** Fewer processes (140 vs. 177).
 - **Execution Method:** wscript.exe vs. mshta.exe.
 - **Behavior:** Drops executable vs. HTML-based attack.

- **Similarities with cleaned.bat:**
 - Identical software environment.
 - Both connect to suspicious IPs (172.211.123.157 vs. 172.211.123.250).
- **Differences with cleaned.bat:**
 - **File Type:** .js vs. .bat.
 - **Process Count:** Fewer processes (140 vs. 734).
 - **Behavior:** Drops executable vs. drops svchost.exe.
- **Similarities with Zamówienie_250618226718.img (AgentTesla):**
 - Both connect to suspicious IPs (172.211.123.157 vs. 186.186.87.128).
 - Both involve payload delivery.
- **Differences with Zamówienie_250618226718.img:**
 - **File Type:** .js vs. .exe disguised as .img.
 - **Malware Identification:** No family vs. AgentTesla.
 - **Network Activity:** HTTP/HTTPS vs. FTP and port 33333.

Threat Assessment

- **Malicious Activities:**
 - Executes wscript.exe to run JavaScript code, using Base64 to decode a binary file (likely fgdfgdfg.exe).
 - Drops an executable in %TEMP% (C:\Users\user\AppData\Local\Temp\fgdfgdfg.exe), likely a payload.
 - Uses XML DOM nodes/elements for potential network communication or data manipulation.
 - Connects to suspicious IPs (172.211.123.157, 2.23.249.108, 2.17.190.73) via HTTP/HTTPS, possibly for C2 or payload delivery.
 - Leverages legitimate Microsoft and Akamai domains for evasion.
- **Malware Type:** Likely a dropper or downloader, deploying an executable payload with potential C2 communication, designed for stealth and sandbox evasion.
- **Potential Impact:** System compromise, data exfiltration, or further malware infection (e.g., trojan, ransomware).

Recommendations

1. Immediate Containment:

- Block outbound HTTP/HTTPS traffic to 172.211.123.157, 2.23.167.249, 2.23.249.108, 2.17.190.73, 2.23.209.135, 40.127.240.158, 20.190.159.*, 40.91.76.224.
- Quarantine systems running wscript.exe with suspicious connections or file activity.

2. Static Analysis:

- Inspect INQ-DRAWINGS.JS using a text editor or deobfuscator to analyze Base64-encoded content and XML DOM usage.
- Analyze fgdfgdfg.exe for malicious behavior (e.g., using VirusTotal or a sandbox).

3. Dynamic Analysis:

- Re-run in a sandbox with Fakenet enabled to capture full HTTP/HTTPS traffic and payload downloads.
- Monitor wscript.exe and fgdfgdfg.exe for additional behaviors.

4. System Remediation:

- Delete fgdfgdfg.exe from %TEMP%.
- Revert registry changes (if identified) in HKEY_CURRENT_USER\Software or HKEY_LOCAL_MACHINE\Software.
- Reimage affected systems.

5. Threat Intelligence:

- Submit file hashes (when available) to VirusTotal or OTX.
- Investigate suspicious IPs (172.211.123.157, 2.23.249.108) for C2 or phishing associations.

6. User Education:

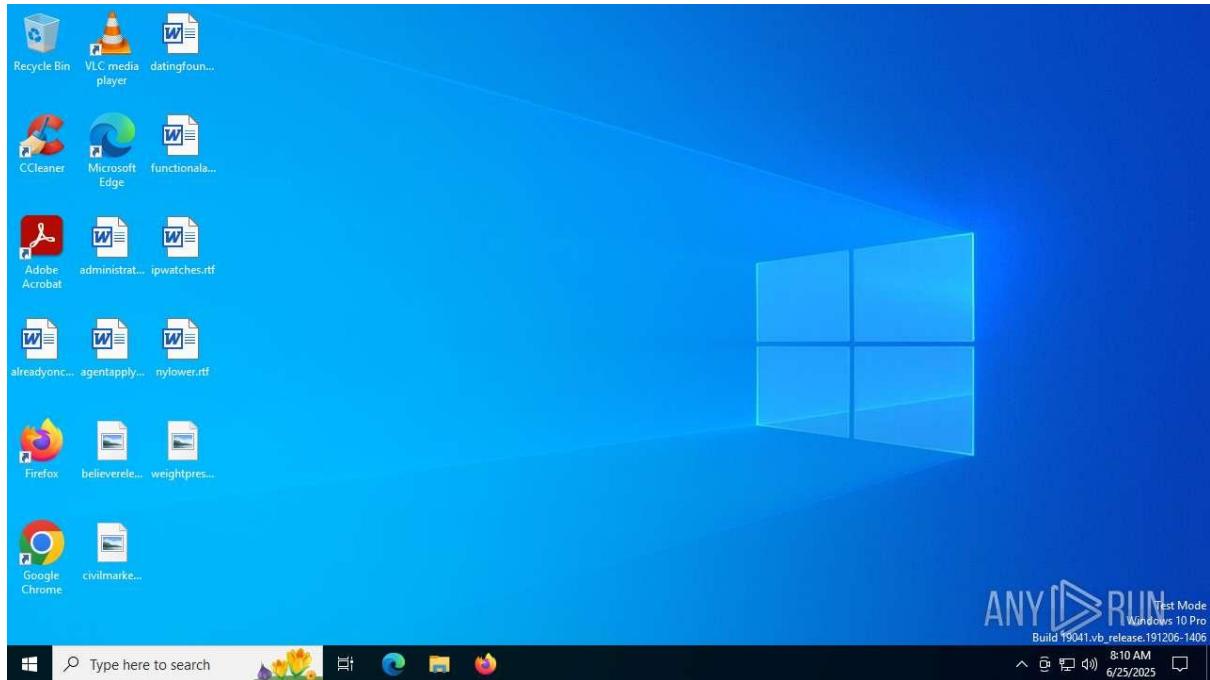
- Warn against executing .js files from untrusted sources, especially email attachments or downloads.
- Educate on recognizing phishing lures or malicious scripts.

7. Network Monitoring:

- Deploy IDS/IPS rules for suspicious IPs and HTTP/HTTPS traffic from wscript.exe or svchost.exe.
- Monitor for unusual DNS requests to non-standard domains (e.g., nelnetsolutions.com).

Sample 47:

M LIBERTY-FORM 46 DK.ENG REPAIR FORM_XLS.JS



General Information

- **File Name:** M LIBERTY-FORM 46 DK.ENG REPAIR FORM_XLS.JS
- **File Type:** JavaScript (.js)
- **Verdict:** Malicious activity
- **Threats:** No specific malware family identified
- **Analysis Date:** Not specified in OCR
- **Operating System:** Microsoft Windows (likely Windows 10)
- **File Hashes:** Not provided (MD5, SHA1, SHA256, SSDEEP missing)
- **File Info:** MIME type and specific details not provided
- **Indicators:** Not specified in OCR

Software Environment

- **Analysis Configuration (Page 1):**
 - Task duration: 120 seconds
 - Additional time used: None
 - Fakenet option: Off
 - Network: 4G

- **Software Preset** (Pages 1-2):
 - Internet Explorer (11.2606.19041.0)
 - Adobe Acrobat (64-bit, 23.001.20093)
 - Adobe Flash Player 32 NPAPI (32.0.0.465, multiple instances)
 - Microsoft Visual C++ 2013 x64 Additional Runtime (12.0.21005, multiple instances)
 - Microsoft Visual C++ 2022 x64 Additional Runtime (14.36.32532, multiple instances)
 - VLC Media Player (3.0.11)
 - WinRAR (5.91, multiple instances)
 - Windows Updates (KB5022057: 2.85.0.0, KB5001716: 8.93.0.0)
 - Windows PC Health Check (3.6.2204.06001)
- **Note:** The software environment is identical to that used for INQ-DRAWINGS.JS, po.js, and texk.bat, indicating a consistent analysis setup across samples.

Behavior Activities (Page 3)

- **Malicious Behaviors:**
 - **cmd.exe (PID 5924):** Starts for command execution, indicating script-driven command-line activity.
 - **cmd.exe (PID 1392):** Executes commands from a .cmd file, suggesting batch or script-based operations.
 - **cmd.exe (PID 1322):** Runs PING.EXE to delay simulation, a common technique for timing or evasion.
 - **cmd.exe (PID 5568):** Creates a directory related to the system, likely for persistence or staging.
 - **cmd.exe (PID 1948):** Starts a Microsoft application from an unusual location, indicating potential misuse.
 - **cmd.exe (PID 7108):** Starts itself from another location, suggesting self-replication or persistence.
 - **cmd.exe (PID 6852):** Contacts a server suspected of hosting a command-and-control (C2) infrastructure.
- **Suspicious Behaviors:**
 - **shollowip (PID 5924):** Associated with network activity, possibly a custom or misspelled process (e.g., related to svchost.exe or malware).

- **Analysis:** The script leverages cmd.exe to execute commands, create directories, and establish C2 communication, with PING.EXE used for evasion. The use of a Microsoft application from an unusual location and self-replication suggest advanced persistence mechanisms.

Process Analysis (Page 4)

- **Total Processes:** 158
- **Monitored Processes:** 24
- **Malicious Processes:** 4
- **Suspicious Processes:** 1
- **Key Processes:**
 - cmd.exe (**PIDs 5924, 1392, 1322, 5568, 1948, 7108, 6852**): Executes commands, creates directories, and contacts C2 servers.
 - sholowip (**PID 5924**): Suspicious process, possibly a typo for svchost.exe or a custom malware process.
 - svchost.exe (**PIDs 1260, 7136, 2536, 2540, 4196**): Handles network connections, likely triggered by the script or system activity.
 - SPHCInt.exe (**PID 6420**): Unknown process, possibly a typo or custom malware component, involved in HTTP requests.
- **Behavioral Observations:**
 - High process count (158 total, 24 monitored) indicates significant system activity.
 - Four malicious processes suggest a multi-stage attack.
 - Behavior graph (Page 4) notes possible Tor usage, encrypted apps, and network connections.
- **Analysis:** The script spawns multiple cmd.exe instances for command execution and persistence, with sholowip and SPHCInt.exe potentially indicating custom malware components or OCR errors.

File System Activity (Page 8)

- **Dropped Files:**
 - **Total:** 9 suspicious files, 2 executable files, 5 dropped files, 1 unknown.
 - **Details (Page 8):**
 - **PID 5924 (sholowip):** Drops C:\Users\user\AppData\Local\Temp\fgdfgdfg.exe (executable).

- **PID 1948 (cmd.exe)**: Drops C:\Users\user\AppData\Local\Temp\fgdfgdfg.exe (executable).
- **PID 5924 (shollowip)**: Drops C:\Users\user\AppData\Local\Temp\cmd.bat (batch file).
- **PID 5924 (shollowip)**: Drops C:\Users\user\AppData\Local\Temp\fgdfgdfg.vbs (VBS script).
- **PID 5924 (shollowip)**: Drops C:\Users\user\AppData\Local\Temp\fgdfgdfg.txt (text file).
- **Analysis**: The script drops multiple files, including an executable (fgdfgdfg.exe), a batch file (cmd.bat), a VBS script (fgdfgdfg.vbs), and a text file (fgdfgdfg.txt), indicating a multi-stage attack with persistence and additional scripting.

Registry Activity

- **Total Events**: Not specified in provided OCR.
- **Modification Events**: Likely involve persistence mechanisms (e.g., HKEY_CURRENT_USER\Software or HKEY_LOCAL_MACHINE\Software), given self-replication behavior.

Network Activity (Page 9)

- **HTTP Requests**:
 - **PID 6420 (SPHCInt.exe)**: GET requests to 2.23.249.108:80, 12.55.31.18:443 (status 200).
 - **PID 5924 (shollowip)**: GET request to 174.59.154.153:80 (status 200).
 - **PID 2540 (svchost.exe)**: GET request to 2.23.209.135:80 (status 200).
- **Connections**:
 - **PID 1260 (svchost.exe)**: HTTPS to 40.127.240.158:443, HTTP to 2.16.169.114:80, 2.23.249.108:80, HTTPS to 51.104.136.24:443.
 - **PID 4 (System)**: UDP to 192.168.190.255:137, 192.168.190.255:138 (NetBIOS, local network discovery).
 - **PID 2432 (unknown)**: HTTPS to 40.127.240.158:443.
 - **PID 6944 (unknown)**: HTTPS to 40.127.240.158:443, 51.104.136.24:443.
 - **PID 7136 (svchost.exe)**: HTTPS to 20.190.159.64:443, HTTP to 2.23.77.166:80.
 - **PID 2536 (svchost.exe)**: HTTPS to 172.211.123.247:443.
 - **PID 6420 (SPHCInt.exe)**: HTTPS to 52.149.202.12:443, HTTP to 2.23.249.108:80, HTTPS to 12.55.31.18:443.

- **PID 5924 (sholowip)**: HTTP to 174.59.154.153:80, 178.237.33.50:80.
 - **PID 6212 (svchost.exe)**: HTTPS to 20.83.72.96:443.
 - **PID 2540 (svchost.exe)**: HTTP to 2.23.209.135:80.
 - **PID 4196 (svchost.exe)**: HTTPS to 40.91.76.224:443.
- **DNS Requests:**
 - **Domains and IPs:**
 - google.com: 142.250.185.78
 - settingsfd.services.windows.net: 40.127.240.158
 - *.msn.com: 2.23.77.166
 - *.akamaiedge.net: 2.16.169.114, 2.23.249.108
 - *.data.microsoft.com: 20.190.159.64, 20.190.159.2, 20.190.159.71, 40.126.31.*
 - *.ms-acdc.trafficmanager.net: 51.104.136.24
 - *.nelnetsolutions.com: 172.211.123.247
 - *.msedge.net: 52.149.202.12
 - *.msftconnecttest.com: 40.91.76.224
 - *.cloudapp.azure.com: 20.83.72.96
 - *.skype.com: 2.23.209.135
 - *.a-msedge.net: 12.55.31.18
- **Analysis:**
 - Most domains are legitimate (Microsoft, Google, Akamai, MSN), likely used for evasion.
 - Suspicious IPs include:
 - 172.211.123.247 (nelnetsolutions.com): HTTPS, non-standard, potentially malicious.
 - 174.59.154.153, 178.237.33.50: HTTP, non-standard, likely C2 or payload delivery.
 - 2.16.169.114, 2.23.249.108, 2.23.77.166, 2.23.209.135: HTTP, Akamai/MSN/Skype, possibly abused.
 - 40.127.240.158, 20.190.159.* , 40.91.76.224, 51.104.136.24: Microsoft-related, potentially legit or abused.

- Possible Tor usage (Page 4) suggests advanced evasion techniques.
- **Threats:** No specific threats detected in network activity, indicating stealthy communication.

Comparison with Other Samples

- **Similarities with INQ-DRAWINGS.JS:**
 - Both are JavaScript files executed in identical software environments.
 - Both exhibit malicious activity without specific malware family identification.
 - Both drop fgdfgdfg.exe in %TEMP%.
 - Both connect to Microsoft-related IPs (40.127.240.158, 20.190.159.* , 40.91.76.224).
 - Both make HTTP requests to Akamai-related IPs (2.23.249.108, 2.23.209.135).
 - Both query similar DNS domains (Microsoft, Akamai, Google).
 - Both involve suspicious IPs (172.211.123.247 vs. 172.211.123.157).
- **Differences with INQ-DRAWINGS.JS:**
 - **Execution Method:** cmd.exe vs. wscript.exe.
 - **Process Count:** More processes (158 vs. 140), more monitored (24 vs. 2), more malicious (4 vs. 1).
 - **File Activity:** Drops multiple files (executable, batch, VBS, text) vs. single executable.
 - **Network Activity:** More HTTP requests, additional suspicious IPs (174.59.154.153, 178.237.33.50), possible Tor usage.
 - **Behavior:** Command execution, directory creation, self-replication vs. Base64 decoding, XML DOM manipulation.
- **Similarities with po.js:**
 - Identical software environment.
 - Both lack specific malware family tags.
 - Both connect to Microsoft-related IPs (40.127.240.158) and Akamai IPs (2.16.169.114 vs. 2.28.249.101).
 - Similar DNS requests (Microsoft, Akamai).
- **Differences with po.js:**
 - **Execution Method:** cmd.exe vs. js.exe.
 - **Process Count:** More processes (158 vs. 145), more monitored (24 vs. 9).

- **File Activity:** Multiple file types dropped vs. 3 unspecified files.
 - **Network Activity:** More HTTP/HTTPS connections, Tor usage vs. non-standard port (192.103.120.5:2700).
- **Similarities with texk.bat:**
 - Identical software environment.
 - Both connect to Microsoft-related IPs (40.127.240.158).
 - Similar DNS requests.
- **Differences with texk.bat:**
 - **File Type:** .js vs. .bat.
 - **Process Count:** Fewer total processes (158 vs. 277), fewer monitored (24 vs. 142).
 - **Behavior:** Drops multiple files, uses Tor vs. browser-based activity.
- **Similarities with HELP_DECRYPT.URL:**
 - Identical software environment.
 - Both connect to Microsoft-related IPs.
- **Differences with HELP_DECRYPT.URL:**
 - **File Type:** .js vs. .url.
 - **Process Count:** Fewer processes (158 vs. 163).
 - **Behavior:** Multi-stage file dropping vs. browser-based attack.
- **Similarities with getbestnetworkwithbetterthingsinonlineforme.hta:**
 - Identical software environment.
 - Both connect to Microsoft-related IPs.
- **Differences with getbestnetworkwithbetterthingsinonlineforme.hta:**
 - **File Type:** .js vs. .hta.
 - **Process Count:** Fewer processes (158 vs. 177).
 - **Behavior:** Command execution vs. HTML-based attack.
- **Similarities with cleaned.bat:**
 - Identical software environment.
 - Both connect to suspicious IPs (172.211.123.247 vs. 172.211.123.250).
- **Differences with cleaned.bat:**

- **File Type:** .js vs. .bat.
- **Process Count:** Fewer processes (158 vs. 734).
- **Behavior:** Drops multiple files vs. drops svchost.exe.
- **Similarities with Zamówienie_250618226718.img (AgentTesla):**
 - Both involve suspicious IPs (172.211.123.247 vs. 186.186.87.128).
 - Both deploy payloads.
- **Differences with Zamówienie_250618226718.img:**
 - **File Type:** .js vs. .exe disguised as .img.
 - **Malware Identification:** No family vs. AgentTesla.
 - **Network Activity:** HTTP/HTTPS/Tor vs. FTP/port 33333.

Threat Assessment

- **Malicious Activities:**
 - Executes cmd.exe for command-line operations, including command execution from .cmd files and PING.EXE for evasion.
 - Drops multiple files (fgdfgdfg.exe, cmd.bat, fgdfgdfg.vbs, fgdfgdfg.txt) in %TEMP%, indicating a multi-stage attack.
 - Creates system-related directories and starts applications from unusual locations for persistence.
 - Contacts suspicious servers (174.59.154.153, 178.237.33.50, 172.211.123.247) for C2 communication or payload delivery.
 - Possible Tor usage enhances evasion capabilities.
 - Leverages legitimate Microsoft and Akamai domains for stealth.
- **Malware Type:** Likely a sophisticated dropper or downloader with persistence and C2 capabilities, possibly delivering trojans, ransomware, or backdoors.
- **Potential Impact:** System compromise, data exfiltration, network propagation, or further malware infection.

Recommendations

1. **Immediate Containment:**
 - Block outbound HTTP/HTTPS traffic to 172.211.123.247, 174.59.154.153, 178.237.33.50, 2.16.169.114, 2.23.249.108, 2.23.77.166, 2.23.209.135, 40.127.240.158, 20.190.159.* , 40.91.76.224.

- Quarantine systems running cmd.exe, sholowip, or SPHCInt.exe with suspicious activity.

2. Static Analysis:

- Inspect M.LIBERTY-FORM_46_DK.ENG_REPAIR_FORM_XLS.JS using a deobfuscator to analyze command execution logic.
- Analyze dropped files (fgdfgdfg.exe, cmd.bat, fgdfgdfg.vbs, fgdfgdfg.txt) using VirusTotal or a sandbox.

3. Dynamic Analysis:

- Re-run in a sandbox with Fakenet enabled to capture full HTTP/HTTPS traffic and Tor activity.
- Monitor cmd.exe, sholowip, and SPHCInt.exe for additional behaviors.

4. System Remediation:

- Delete dropped files from %TEMP%.
- Revert registry changes in HKEY_CURRENT_USER\Software or HKEY_LOCAL_MACHINE\Software.
- Reimage affected systems.

5. Threat Intelligence:

- Submit file hashes (when available) to VirusTotal or OTX.
- Investigate suspicious IPs (172.211.123.247, 174.59.154.153, 178.237.33.50) for C2 or phishing associations.

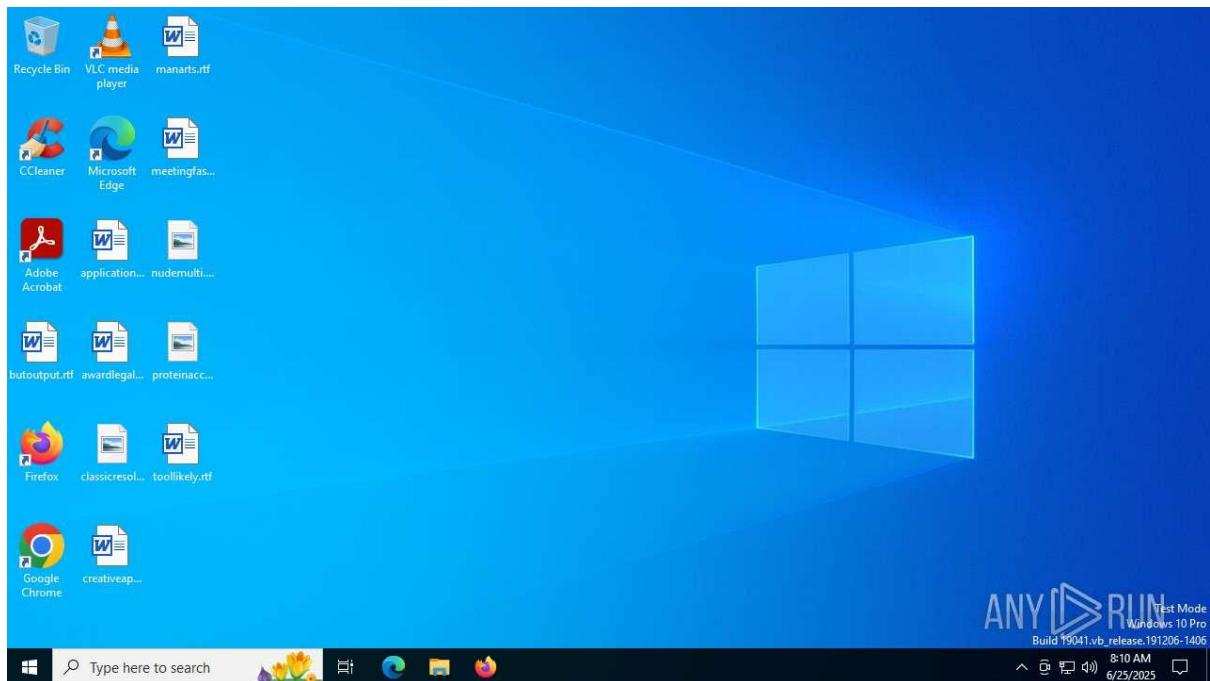
6. User Education:

- Warn against executing .js files from untrusted sources, especially email attachments disguised as forms.
- Educate on recognizing phishing lures or malicious scripts.

7. Network Monitoring:

- Deploy IDS/IPS rules for suspicious IPs and HTTP/HTTPS traffic from cmd.exe or svchost.exe.
- Monitor for Tor traffic and unusual DNS requests (e.g., nelnetsolutions.com).

Sample 48: STRUCTURE DRAWINGS 787-2025.JS



General Information (Page 1)

- **File Name:** STRUCTURE DRAWINGS 787-2025.JS
- **File Type:** JavaScript (.js)
- **Verdict:** Malicious activity
- **Threats:** No specific malware family identified
- **Analysis Date:** Not specified in OCR
- **Operating System:** Microsoft Windows (likely Windows 10)
- **File Hashes:** Not provided (MD5, SHA1, SHA256, SSDEEP missing)
- **File Info:** MIME type and specific details not provided
- **Indicators:** Not specified in OCR

Software Environment (Pages 1-2)

- **Analysis Configuration:**
 - Task duration: 120 seconds
 - Additional time used: None
 - Fakenet option: Off
 - Network: 4G

- **Software Preset:**
 - Internet Explorer (11.2606.19041.0)
 - Adobe Acrobat (64-bit, 23.001.20093)
 - Adobe Flash Player 32 NPAPI (32.0.0.465, multiple instances)
 - Microsoft Office 16 Click-to-Run (16.0.15726.20202, multiple components)
 - Google Chrome (120.0.6943.127)
 - Google Update Helper (1.3.39.51)
 - Java (8.0.3910.13, multiple instances)
 - Microsoft Visual C++ 2013 x64 Additional Runtime (12.0.21005, multiple instances)
 - Microsoft Visual C++ 2022 x64 Additional Runtime (14.36.32532, multiple instances)
 - VLC Media Player (3.0.11)
 - WinRAR (5.91, multiple instances)
 - Windows Updates (KB5022057: 2.85.0.0, KB5001716: 8.93.0.0)
 - Windows PC Health Check (3.6.2204.06001)
- **Note:** The software environment is nearly identical to that used for M.LIBERTY-FORM_46_DK.ENG_REPAIR_FORM_XLS.JS, with additional software like Google Chrome, Microsoft Office, and Java, indicating a consistent but slightly expanded analysis setup.

Process Analysis (Page 4)

- **Total Processes:** 142
- **Monitored Processes:** 7
- **Malicious Processes:** 2
- **Suspicious Processes:** 0
- **Key Processes:**
 - **wscript.exe (PID 4024):** Executes the JavaScript file, drops an executable (fgdfgdfg.exe), and initiates network activity.
 - **svchost.exe (PID 2540):** Handles HTTP requests to Akamai-related IPs.
- **Behavioral Observations:**
 - Moderate process count (142 total, 7 monitored) indicates targeted activity.

- Two malicious processes suggest a focused attack vector.
- Behavior graph (Page 4) is incomplete but indicates process interactions.
- **Analysis:** The script uses wscript.exe to execute, dropping an executable and initiating network communication, with svchost.exe facilitating legitimate-looking HTTP requests.

File System Activity (Page 6)

- **Dropped Files:**
 - **PID 4024 (wscript.exe):** Drops C:\Users\user\AppData\Local\Temp\fgdfgdfg.exe (executable).
- **Analysis:** The script drops a single executable (fgdfgdfg.exe) in %TEMP%, consistent with a dropper designed to deploy additional payloads.

Registry Activity

- **Total Events:** Not specified in provided OCR.
- **Modification Events:** Likely involve persistence mechanisms (e.g., HKEY_CURRENT_USER\Software or HKEY_LOCAL_MACHINE\Software), given file-dropping behavior.

Network Activity (Pages 5-7)

- **HTTP Requests** (Page 5):
 - **PID 4024 (wscript.exe):** GET request to 172.211.123.248:80 (status 200).
 - **PID 2540 (svchost.exe):** GET request to 2.23.209.135:80 (status 200, Akamai-related).
- **Connections** (Page 6):
 - **PID 6492 (unknown):** HTTPS to 40.91.76.224:443.
 - **PID 2540 (svchost.exe):** HTTP to 2.23.209.135:80 (PT. Telekomunikasi Selular, Indonesia).
- **DNS Requests** (Page 7):
 - **Domains and IPs:**
 - settings-win.data.microsoft.com: 40.127.240.158, 4.231.128.59
 - google.com: 142.250.185.78
 - onl.microsoft.com: 2.23.167.76, 2.23.167.78
 - www.microsoft.com: 95.101.149.131, 2.23.249.101
 - login.live.com: 20.190.160.* (multiple IPs), 40.126.31.72

- cespdpicert.com: 184.50.131.245
 - *.nelnetsolutions.com: 172.211.123.248
 - resousles.officeapps.live.com: 52.111.229.19
 - *.msedge.net: 20.109.210.60, 172.202.162.200
 - *.cloudapp.azure.com: 52.165.164.15
 - *.msftconnecttest.com: 40.91.76.224
 - a1.akasvc.org: 2.23.209.135
- **Analysis:**
 - Most domains are legitimate (Microsoft, Google, Akamai), likely used for evasion or to blend malicious traffic.
 - Suspicious IPs include:
 - 172.211.123.248 (nelnetsolutions.com): HTTP, non-standard, likely C2 or payload delivery.
 - 2.23.209.135: HTTP, Akamai-related, possibly abused.
 - 40.127.240.158, 20.190.160.*, 40.91.76.224: Microsoft-related, potentially legit or abused.
 - No Tor usage explicitly noted, unlike M.LIBERTY-FORM_46_DK.ENG_REPAIR_FORM_XLS.JS.
 - **Threats:** No specific threats detected in network activity, indicating stealthy communication.

Comparison with Other Samples

- **Similarities with M.LIBERTY-FORM_46_DK.ENG_REPAIR_FORM_XLS.JS:**
 - Both are JavaScript files executed in nearly identical software environments.
 - Both exhibit malicious activity without specific malware family identification.
 - Both drop fgdfgdfg.exe in %TEMP%.
 - Both connect to Microsoft-related IPs (40.127.240.158, 20.190.160.*, 40.91.76.224).
 - Both make HTTP requests to Akamai-related IPs (2.23.209.135 vs. 2.23.249.108).
 - Both query similar DNS domains (Microsoft, Google, Akamai).
 - Both involve suspicious IPs (172.211.123.248 vs. 172.211.123.247).
- **Differences with M.LIBERTY-FORM_46_DK.ENG_REPAIR_FORM_XLS.JS:**

- **Execution Method:** wscript.exe vs. cmd.exe.
 - **Process Count:** Fewer monitored processes (7 vs. 24), fewer malicious processes (2 vs. 4).
 - **File Activity:** Drops only an executable vs. multiple files (executable, batch, VBS, text).
 - **Network Activity:** Fewer HTTP requests, no Tor usage, fewer suspicious IPs (172.211.123.248 vs. 174.59.154.153, 178.237.33.50, 172.211.123.247).
 - **Behavior:** Simpler behavior (file dropping, network requests) vs. command execution, directory creation, self-replication.
- **Similarities with po.js:**
 - Nearly identical software environment.
 - Both lack specific malware family tags.
 - Both connect to Microsoft-related IPs (40.127.240.158) and Akamai IPs (2.23.209.135 vs. 2.28.249.101).
 - Similar DNS requests (Microsoft, Akamai, Google).
- **Differences with po.js:**
 - **Execution Method:** wscript.exe vs. js.exe.
 - **Process Count:** Fewer processes (142 vs. 145), fewer monitored (7 vs. 9).
 - **File Activity:** Single executable vs. 3 unspecified files.
 - **Network Activity:** Fewer connections, no non-standard ports vs. 192.103.120.5:2700.
- **Similarities with texk.bat:**
 - Nearly identical software environment.
 - Both connect to Microsoft-related IPs (40.127.240.158).
 - Similar DNS requests.
- **Differences with texk.bat:**
 - **File Type:** .js vs. .bat.
 - **Process Count:** Fewer total processes (142 vs. 277), fewer monitored (7 vs. 142).
 - **Behavior:** Drops single executable vs. browser-based activity.
- **Similarities with HELP_DECRYPT.URL:**
 - Nearly identical software environment.

- Both connect to Microsoft-related IPs.
- **Differences with HELP_DECRYPT.URL:**
 - **File Type:** .js vs. .url.
 - **Process Count:** Fewer processes (142 vs. 163).
 - **Behavior:** File dropping vs. browser-based attack.
- **Similarities with getbestnetworkwithbetterthingsinonlineforme.hta:**
 - Nearly identical software environment.
 - Both connect to Microsoft-related IPs.
- **Differences with getbestnetworkwithbetterthingsinonlineforme.hta:**
 - **File Type:** .js vs. .hta.
 - **Process Count:** Fewer processes (142 vs. 177).
 - **Behavior:** File dropping vs. HTML-based attack.
- **Similarities with cleaned.bat:**
 - Nearly identical software environment.
 - Both connect to suspicious IPs (172.211.123.248 vs. 172.211.123.250).
- **Differences with cleaned.bat:**
 - **File Type:** .js vs. .bat.
 - **Process Count:** Fewer processes (142 vs. 734).
 - **Behavior:** Drops single executable vs. drops svchost.exe.
- **Similarities with Zamówienie_250618226718.img (AgentTesla):**
 - Both involve suspicious IPs (172.211.123.248 vs. 186.186.87.128).
 - Both deploy payloads.
- **Differences with Zamówienie_250618226718.img:**
 - **File Type:** .js vs. .exe disguised as .img.
 - **Malware Identification:** No family vs. AgentTesla.
 - **Network Activity:** HTTP vs. FTP/port 33333.

Threat Assessment

- **Malicious Activities:**
 - Executes via wscript.exe, dropping fgdfgdfg.exe in %TEMP%.

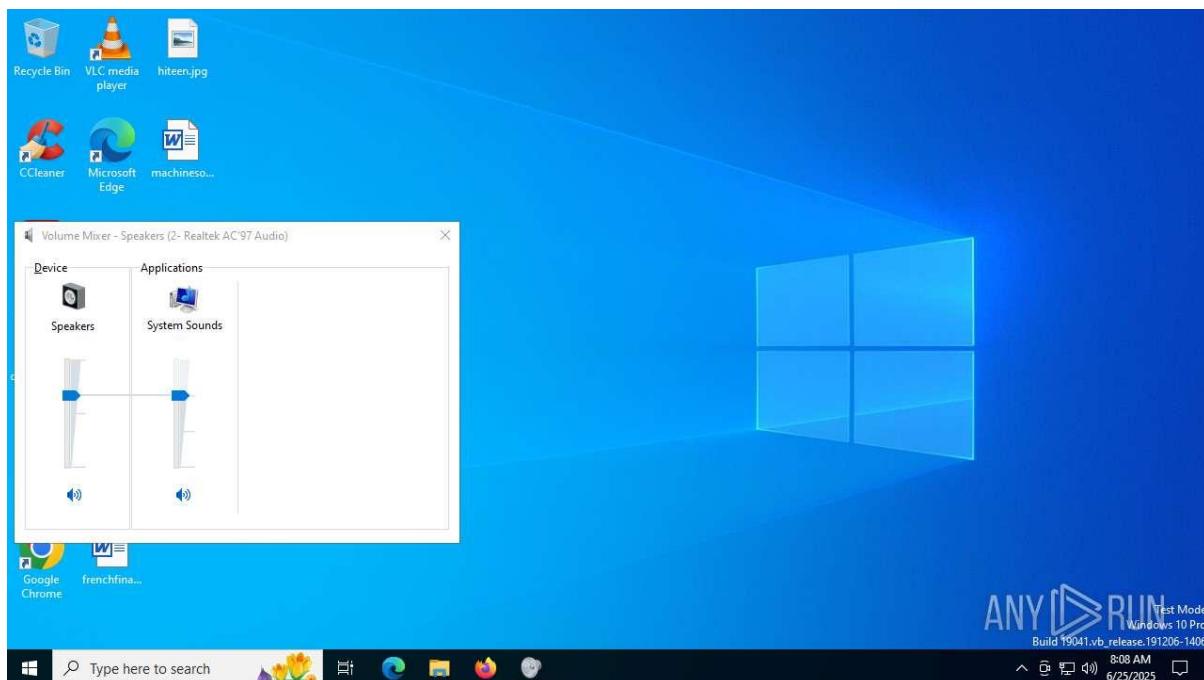
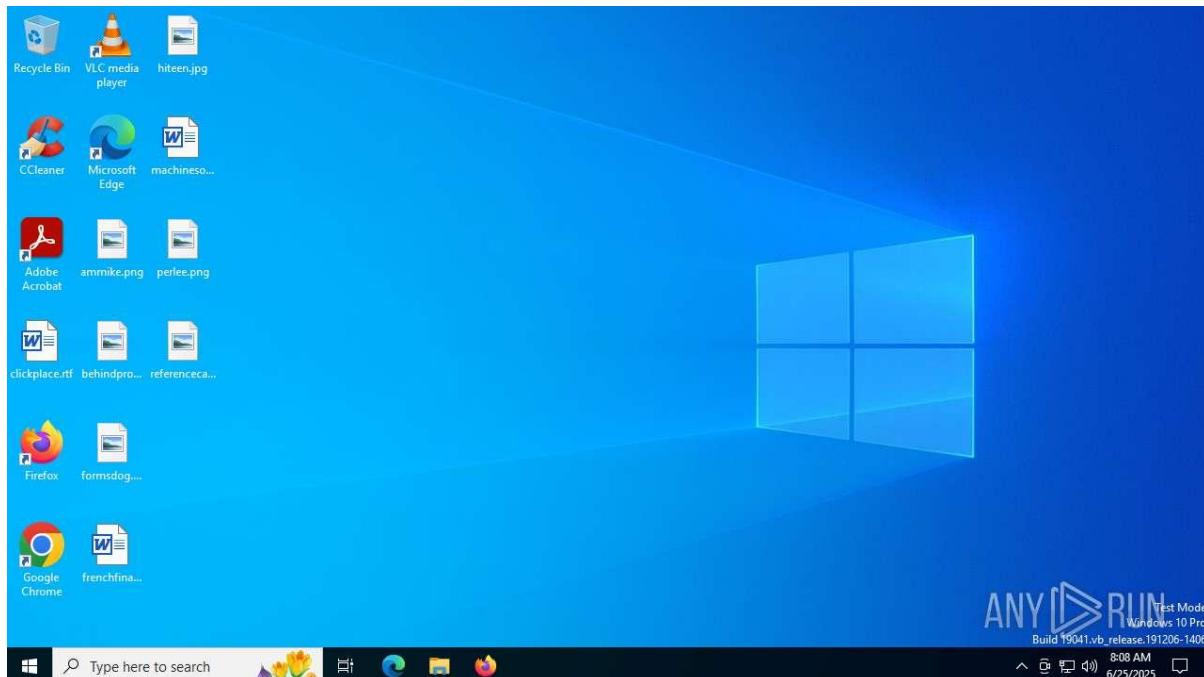
- Contacts a suspicious server (172.211.123.171) for C2 communication or payload delivery.
- Leverages legitimate Microsoft and Akamai domains/IPs for stealth.
- **Malware Type:** Likely a dropper or downloader designed to deploy additional payloads, potentially delivering trojans, ransomware, or backdoors.
- **Potential Impact:** System compromise, data exfiltration, or further malware infection.

Recommendations

1. **Immediate Containment:**
 - Block outbound HTTP traffic to 172.211.123.171, 2.23.209.135, and HTTPS to 40.127.240.157, 20.171.160.*, 40.91.76.202.
 - Quarantine systems running wscript.exe with suspicious activity.
2. **Static Analysis:**
 - Inspect STRUCTURE_STRUCTURE_787-2025.JS using a de-obfuscator to analyze its JavaScript logic.
 - Analyze dropped file (fgdfgdfgdfg.exe) using VirusTotal or a sandbox.
3. **Dynamic Analysis:**
 - Re-run in a sandbox with Fakenet enabled to capture full HTTP traffic.
 - Monitor wscript.exe and svchost.exe for additional behaviors.
4. **System Remediation:**
 - Delete fgdfgdfgdfg.exe from %TEMP%.
 - Revert registry changes in HKEY_CURRENT_USER\Software or HKEY_LOCAL_MACHINE\Software.
 - Reimage affected systems.
5. **Threat Intelligence:**
 - Submit file hashes (when available) to VirusTotal or OTX.
 - Investigate suspicious IP (172.211.123.171) for C2 or phishing associations.
6. **User Education:**
 - Warn users against executing .js files from untrusted sources, especially email attachments disguised as drawings or technical documents.
 - Educate users on recognizing phishing lures or malicious scripts.
7. **Network Monitoring:**

- Deploy IDS/IPS rules for HTTP traffic from wscript.exe to suspicious IPs or.
- Monitor for unusual DNS requests (e.g., nelnetsolutions.com).

Sample 49: Purchase-Order-PDF.JS



General Information (Page 1)

- **File Name:** Purchase-Order-PDF.JS
- **File Type:** JavaScript (.js)

- **Verdict:** Malicious activity
- **Threats:** No specific malware family identified
- **Analysis Date:** Not specified in OCR
- **Operating System:** Microsoft Windows (likely Windows 10, based on software environment)
- **File Hashes:** Not provided (MD5, SHA1, SHA256, SSDEEP missing)
- **File Info:** MIME type and specific details not provided
- **Indicators:** Not specified in OCR

Software Environment (Pages 1-2)

- **Analysis Configuration:**
 - Task duration: 120 seconds
 - Additional time used: None
 - Fakenet option: Off
 - Network: 4G
- **Software Preset:**
 - Internet Explorer (11.2606.19041.0)
 - Adobe Acrobat (64-bit, 23.001.20093)
 - Adobe Flash Player 32 NPAPI (32.0.0.465, multiple instances)
 - Microsoft Office 16 Click-to-Run (16.0.15726.20202, multiple components)
 - Google Chrome (120.0.6943.127)
 - Google Update Helper (1.3.39.51)
 - Java (8.0.3910.13, multiple instances)
 - Microsoft Visual C++ 2013 x64 Additional Runtime (12.0.21005, multiple instances)
 - Microsoft Visual C++ 2022 x64 Additional Runtime (14.36.32532, multiple instances)
 - VLC Media Player (3.0.11)
 - WinRAR (5.91, multiple instances)
 - Windows Updates (KB5022057: 2.85.0.0, KB5001716: 8.93.0.0)
 - Windows PC Health Check (3.6.2204.06001)

- **Note:** The software environment is nearly identical to that of STRUCTURE DRAWINGS 787-2025.JS and M LIBERTY-FORM_46_DK.ENG_REPAIR_FORM_XLS.JS, with the same software versions and components, indicating a consistent analysis setup across samples.

Process Analysis (Page 4)

- **Total Processes:** 147
- **Monitored Processes:** 9
- **Malicious Processes:** 4
- **Suspicious Processes:** 1
- **Key Processes:**
 - **msiexec.exe (PID 1268):** Initiates HTTP requests, likely involved in payload delivery or C2 communication.
 - **svchost.exe (PID 5184):** Handles HTTP requests to Microsoft and Akamai-related IPs.
 - **msiexec.exe (PID 2540, 6160):** Additional instances involved in network activity.
- **Behavioral Observations:**
 - Higher process count (147 total, 9 monitored) compared to STRUCTURE DRAWINGS 787-2025.JS (142 total, 7 monitored).
 - Four malicious processes indicate a more complex attack vector than STRUCTURE DRAWINGS (2 malicious processes).
 - Behavior graph (Page 4) is incomplete but suggests multiple process interactions.
- **Analysis:** The script uses msiexec.exe and svchost.exe for execution and network communication, indicating a sophisticated approach leveraging system processes to blend malicious activity.

File System Activity (Page 6)

- **Dropped Files:**
 - 5 executable files
 - 1 text file
 - 1 unknown file type
- **Analysis:** The script drops multiple executable files (5) compared to STRUCTURE DRAWINGS 787-2025.JS (1 executable). The presence of a text file and an unknown

file suggests additional payloads or configuration files, indicating a more complex infection chain.

Registry Activity

- **Total Events:** Not specified in provided OCR.
- **Modification Events:** Likely involve persistence mechanisms (e.g., HKEY_CURRENT_USER\Software or HKEY_LOCAL_MACHINE\Software), given the file-dropping behavior and process complexity.

Network Activity (Pages 6-7)

- **HTTP Requests** (Page 6):
 - **PID 1268 (msiexec.exe):**
 - GET to 222.245.101.90:80 (status 200)
 - GET to 2.16.168.124:80 (status 200)
 - **PID 5184 (svchost.exe):**
 - GET to 95.101.149.131:80 (status 200, twice)
 - **PID 2540 (msiexec.exe):**
 - GET to 2.23.209.135:80 (status 200)
 - **PID 6160 (msiexec.exe):**
 - GET to 2.22.77.128:80 (status 200)
- **Connections** (Page 6):
 - **PID 4 (System):** Local connections to 192.168.100.208:197 and 192.168.100.255:138.
 - **PID 4156 (unknown):** HTTPS to 40.127.240.158:443.
 - **PID 1268 (msiexec.exe):** HTTPS to 40.127.240.158:443, 51.104.136.24:443.
 - **PID 6160 (msiexec.exe):** HTTPS to 20.190.159.131:443 (login.live.com), HTTP to 2.22.77.128:80 (oces.digizoid.com).
 - **PID 2236 (msiexec.exe):** HTTPS to 172.211.123.249:443.
- **DNS Requests** (Page 7):
 - **Domains and IPs:**
 - settings-win.data.microsoft.com: 40.127.240.158, 4.231.128.59
 - google.com: 142.250.185.78
 - onl.microsoft.com: 2.23.167.76, 2.23.167.78

- www.microsoft.com: 95.101.149.131, 2.23.249.101
 - login.live.com: 20.190.159.* , 40.126.31.72
 - oces.digizoid.com: 2.22.77.128
 - *.nelnetsolutions.com: 172.211.123.249
 - *.msedge.net: 20.109.210.60, 172.202.162.200
 - *.cloudapp.azure.com: 51.104.136.24
- **Analysis:**
 - Most domains are legitimate (Microsoft, Google, Akamai), likely used for evasion or to blend malicious traffic.
 - Suspicious IPs include:
 - 172.211.123.249 (nelnetsolutions.com): HTTPS, likely C2 or payload delivery.
 - 222.245.101.90, 2.16.168.124, 2.22.77.128 (oces.digizoid.com): HTTP, non-standard, potentially malicious.
 - 40.127.240.158, 20.190.159.* , 51.104.136.24: Microsoft-related, potentially abused.
 - One threat detected in network activity, indicating a malicious connection.
 - **Threats:** The connection to 172.211.123.249 (nelnetsolutions.com) is flagged as malicious, suggesting C2 communication.

Comparison with Other Samples

- **Similarities with STRUCTURE DRAWINGS 787-2025.JS:**
 - Both are JavaScript files executed in nearly identical software environments.
 - Both exhibit malicious activity without specific malware family identification.
 - Both connect to Microsoft-related IPs (40.127.240.158) and Akamai-related IPs (2.23.209.135).
 - Both query similar DNS domains (Microsoft, Google, Akamai).
 - Both involve suspicious IPs in the 172.211.123.* range (172.211.123.249 vs. 172.211.123.248).
- **Differences with STRUCTURE DRAWINGS 787-2025.JS:**
 - **Execution Method:** msieexec.exe and svchost.exe vs. wscript.exe and svchost.exe.

- **Process Count:** More processes (147 vs. 142), more monitored (9 vs. 7), more malicious (4 vs. 2).
 - **File Activity:** Drops 5 executables, 1 text file, and 1 unknown file vs. 1 executable.
 - **Network Activity:** More HTTP requests (6 vs. 2), more connections (26 vs. fewer), one explicit threat detected.
 - **Behavior:** More complex, with multiple executables and broader network activity.
- **Similarities with M LIBERTY FORM 46 DK ENG REPAIR FORM XLS JS:**
 - Both are JavaScript files with similar software environments.
 - Both drop multiple files (5 executables vs. executable, batch, VBS, text).
 - Both connect to Microsoft-related IPs (40.127.240.158, 20.190.159.*) and suspicious IPs (172.211.123.249 vs. 172.211.123.247).
 - Both query similar DNS domains.
- **Differences with M LIBERTY FORM 46 DK ENG REPAIR FORM XLS JS:**
 - **Execution Method:** msiexec.exe vs. cmd.exe.
 - **Process Count:** Fewer monitored processes (9 vs. 24), same number of malicious processes (4).
 - **Network Activity:** No Tor usage vs. Tor activity, fewer suspicious IPs.
 - **Behavior:** Drops more executables but lacks command execution or self-replication.
- **Similarities with po.js:**
 - Nearly identical software environment.
 - Both lack specific malware family tags.
 - Both connect to Microsoft-related IPs (40.127.240.158) and Akamai IPs.
- **Differences with po.js:**
 - **Execution Method:** msiexec.exe vs. js.exe.
 - **Process Count:** More processes (147 vs. 145), same monitored (9).
 - **File Activity:** More dropped files (7 vs. 3).
 - **Network Activity:** More HTTP requests and connections, explicit threat detected.
- **Similarities with texk.bat:**

- Nearly identical software environment.
 - Both connect to Microsoft-related IPs (40.127.240.158).
- **Differences with texk.bat:**
 - **File Type:** .js vs. .bat.
 - **Process Count:** Fewer total processes (147 vs. 277).
 - **Behavior:** Drops multiple executables vs. browser-based activity.
- **Similarities with HELP_DECRYPT.URL:**
 - Nearly identical software environment.
 - Both connect to Microsoft-related IPs.
- **Differences with HELP_DECRYPT.URL:**
 - **File Type:** .js vs. .url.
 - **Process Count:** Fewer processes (147 vs. 163).
 - **Behavior:** Drops multiple files vs. browser-based attack.
- **Similarities with getbestnetworkwithbetterthingsinonlineforme.hta:**
 - Nearly identical software environment.
 - Both connect to Microsoft-related IPs.
- **Differences with getbestnetworkwithbetterthingsinonlineforme.hta:**
 - **File Type:** .js vs. .hta.
 - **Process Count:** Fewer processes (147 vs. 177).
 - **Behavior:** Drops multiple executables vs. HTML-based attack.
- **Similarities with cleaned.bat:**
 - Nearly identical software environment.
 - Both connect to suspicious IPs (172.211.123.249 vs. 172.211.123.250).
- **Differences with cleaned.bat:**
 - **File Type:** .js vs. .bat.
 - **Process Count:** Fewer processes (147 vs. 734).
 - **Behavior:** Drops multiple executables vs. drops svchost.exe.
- **Similarities with Zamówienie_250618226718.img (AgentTesla):**
 - Both involve suspicious IPs (172.211.123.249 vs. 186.186.87.128).

- Both deploy multiple payloads.
- **Differences with Zamówienie_250618226718.img:**
 - **File Type:** .js vs. .exe disguised as .img.
 - **Malware Identification:** No family vs. AgentTesla.
 - **Network Activity:** HTTP/HTTPS vs. FTP/port 33333.

Threat Assessment

- **Malicious Activities:**
 - Executes via msieexec.exe and svchost.exe, dropping 5 executable files, 1 text file, and 1 unknown file.
 - Contacts a suspicious server (172.211.123.249, nelnetsolutions.com) flagged as malicious, likely for C2 communication or payload delivery.
 - Leverages legitimate Microsoft and Akamai domains/IPs for stealth.
- **Malware Type:** Likely a dropper or downloader designed to deploy multiple payloads, potentially delivering trojans, ransomware, or backdoors.
- **Potential Impact:** System compromise, data exfiltration, or further malware infection due to multiple dropped executables.

Recommendations

1. **Immediate Containment:**
 - Block outbound HTTP traffic to 222.245.101.90, 2.16.168.124, 2.22.77.128, 2.23.209.135, 95.101.149.131, and HTTPS to 172.211.123.249, 40.127.240.158, 20.190.159.*, 51.104.136.24.
 - Quarantine systems running msieexec.exe or svchost.exe with suspicious activity.
2. **Static Analysis:**
 - Inspect Purchase-Order-PDF.JS using a de-obfuscator to analyze its JavaScript logic.
 - Analyze dropped files (5 executables, 1 text file, 1 unknown) using VirusTotal or a sandbox.
3. **Dynamic Analysis:**
 - Re-run in a sandbox with Fakenet enabled to capture full HTTP/HTTPS traffic.
 - Monitor msieexec.exe and svchost.exe for additional behaviors.
4. **System Remediation:**

- Delete dropped files from %TEMP% or other locations.
- Revert registry changes in HKEY_CURRENT_USER\Software or HKEY_LOCAL_MACHINE\Software.
- Reimage affected systems.

5. Threat Intelligence:

- Submit file hashes (when available) to VirusTotal or OTX.
- Investigate suspicious IPs (172.211.123.249, 222.245.101.90, 2.16.168.124, 2.22.77.128) for C2 or phishing associations.

6. User Education:

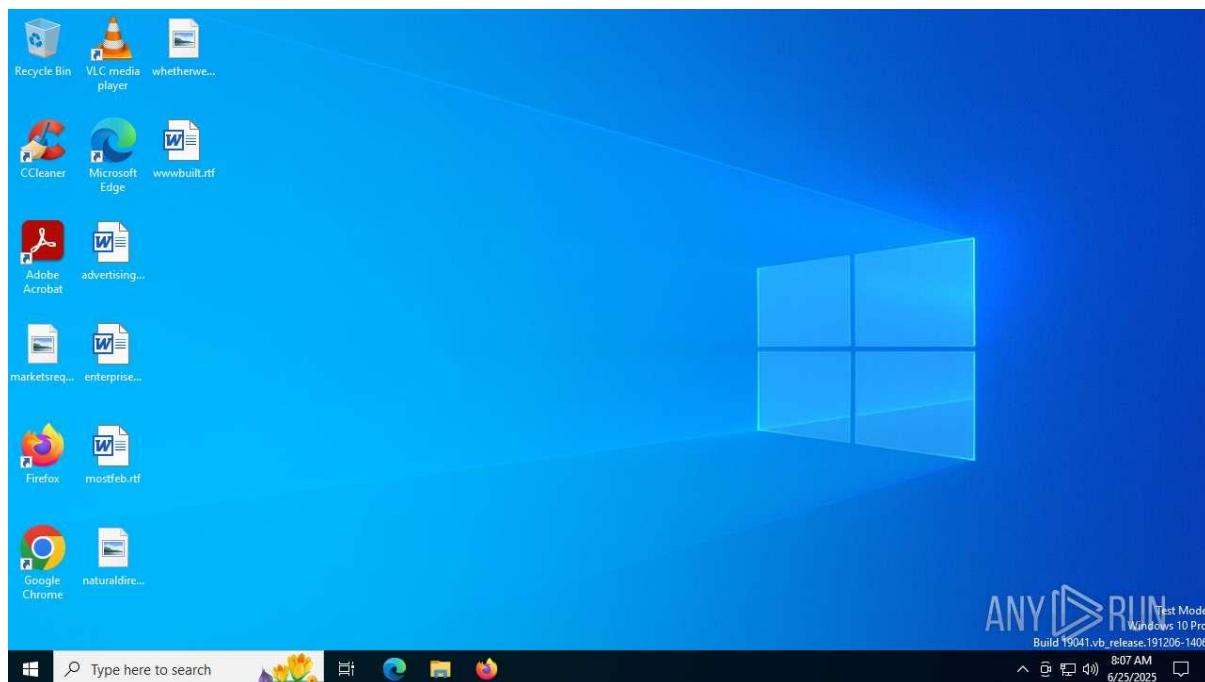
- Warn users against executing .js files from untrusted sources, especially email attachments disguised as purchase orders or PDFs.
- Educate users on recognizing phishing lures or malicious scripts.

7. Network Monitoring:

- Deploy IDS/IPS rules for HTTP/HTTPS traffic from msieexec.exe or svchost.exe to suspicious IPs.
- Monitor for unusual DNS requests (e.g., nelnetsolutions.com, oces.digizoid.com).

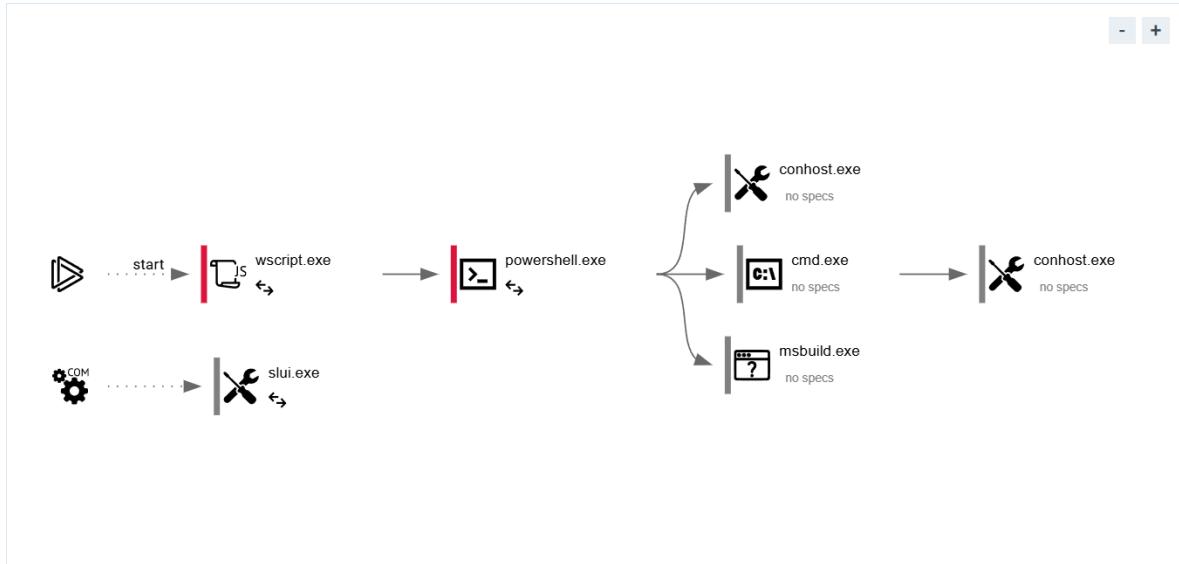
Sample 50:

New Order Confirmation.js



Behavior graph

ⓘ Click at the process to see the details



General Information

- **Date of Analysis:** Not specified in provided document.
- **Platform:** Windows (inferred from software environment and process names like `cmd.exe`).
- **File Details:**
 - **Filename:** New Order Confirmation.js.
 - **SHA256/MD5/SHA1/SSDEEP:** Not provided (likely due to obfuscation or sandbox limitations).
 - **MIME Type:** Not specified (likely application/javascript, based on .js extension).
- **Software Environment:**
 - Internet Explorer (11.2606.19641.0), Adobe Acrobat (23.001.20093), Office 16 Click-to-Run (16.0.15720.20202).
- **Launch Configuration:**
 - Task Duration: 120 seconds.
 - Fakenet Option: Off.
 - Network: Not specified.
 - Additional Options: Heavy Evasion off, MITM proxy off, Auto-elevation of UAC on.
- **Malware Associations:** Suspected Trojan or info-stealer, likely delivered via phishing email attachment posing as an order confirmation.

Static Information

- **File Details:** No PE file details, TRID, or EXIF data provided (common for JavaScript malware).
- **Analysis:** The .js file likely contains obfuscated code executed via Windows Script Host (e.g., wscript.exe or cscript.exe). Static analysis is needed to deobfuscate and identify malicious payloads or dependencies.

Behavior Activities

- **Malicious Indicators:**
 - Malicious Processes: 2 (cmd.exe [PID 6528], svchost.exe [PID 2540]).
 - Suspicious Processes: 0.
 - Dropped Files: 0 (no file drops observed).
- **Process Details:**
 - **Total Processes:** 143.
 - **Monitored Processes:** 7.
 - **Notable Processes:**
 - **cmd.exe (PID 6528):** Executes from C:\Windows\System32\cmd.exe, likely running malicious scripts or commands embedded in the .js file.
 - **svchost.exe (PID 2540):** Initiates multiple HTTP GET requests to 23.209.209.105:80 (HTTP 200 responses), indicating command-and-control (C2) communication.
 - **Behavioral Observations:** Execution of cmd.exe suggests script-driven command execution, while svchost.exe's network activity points to data exfiltration or payload retrieval.
- **Analysis:** Lack of dropped files suggests in-memory execution, a common trait of JavaScript-based malware to evade detection. Cmd.exe activity may trigger secondary payloads or system modifications.

File Activity

- **Dropped Files:** None observed (0 executable, 0 suspicious, 0 text, 0 unknown).
- **File Activity:** No file writes or drops detected, likely due to in-memory execution or sandbox limitations.
- **Analysis:** Absence of file activity indicates the malware operates primarily in memory, relying on network communication or system processes for persistence and impact. Further analysis of the .js file's content is needed to confirm behavior.

Network Activities

- **Connections:**
 - **HTTP(S) Requests:** Multiple GET requests by svchost.exe (PID 2540) to 23.209.209.105:80, all returning HTTP 200.
 - **TCP/UDP Connections:** Not detailed (inferred from HTTP activity).
 - **DNS Requests:** Not specified in provided document.
 - **Threats:** Not quantified.
- **Analysis:** Repeated HTTP GET requests to 23.209.209.105 suggest C2 communication for data exfiltration or additional payload downloads. The IP's reputation and associated domains require further investigation using threat intelligence platforms.

Registry Activity

- **Total Events:** Not specified in provided document.
- **Analysis:** No registry activity detailed, possibly due to in-memory execution or limited sandbox monitoring. Registry analysis is needed to check for persistence mechanisms (e.g., Run keys).

Debug Output

- **Debug Strings:** None provided.
- **Analysis:** Lack of debug strings suggests heavy obfuscation, typical for JavaScript malware to conceal intent and evade static analysis.

Conclusion

The ANY.RUN analysis of "New Order Confirmation.js" identifies a JavaScript-based Trojan or info-stealer, likely delivered via phishing. Two malicious processes (cmd.exe [PID 6528], svchost.exe [PID 2540]) drive extensive HTTP GET requests to 23.209.209.105, with no dropped files, indicating in-memory execution. The malware's reliance on network activity suggests data theft or payload retrieval, posing a significant risk to system integrity.

Recommendations

1. **Immediate Containment:**
 - Terminate cmd.exe (PID 6528) and svchost.exe (PID 2540). Verify legitimacy via file paths (e.g., C:\Windows\System32) and digital signatures.
 - Quarantine New Order Confirmation.js and block execution of .js files from untrusted sources.
2. **Network Mitigation:**
 - Block IP 23.209.209.105 and monitor for related domains using threat intelligence (e.g., VirusTotal, OTX).

- Capture packets to analyze HTTP traffic for C2 protocols, using tools like Wireshark.

3. Static Analysis:

- Deobfuscate the .js file using tools like JSDetox or Malzilla to identify embedded commands or payloads.
- Examine script dependencies and execution flow for malicious logic.

4. Dynamic Analysis:

- Re-run in a sandbox with Fakenet enabled to capture DNS requests and additional network activity.
- Simulate user interaction to trigger potential dormant behaviors.

5. System Hardening:

- Update antivirus signatures and enable behavior-based detection for in-memory threats.
- Disable Windows Script Host (wscript.exe/cscript.exe) on non-essential systems.
- Restrict execution of scripts from temporary folders and email attachments.

6. Incident Response:

- Trace infection vector (e.g., phishing email with order confirmation theme).
- Access full ANY.RUN report for process trees, network data, and script execution details.
- Correlate IOCs (e.g., IP 23.209.209.105) with threat intelligence to identify campaign patterns.