Logo

Cyber Malware Analysis Report

Cyber Security Incident Response Team: Mohamad Nour Shahin

12/09/2023

Executive Summary

Provide an executive summary about the malware here.

Case Details

Date	**11.09.2024**
Analyst	**Mohamad Nour Shahin**

Sample information

File name	**GST INVOICE.exe**
File size	**673.00 KB (689152 bytes)**
File type	**Win32 EXE**
MD5	**9c7b97eb3958d4309e6ba38bb1a99471**
SHA1	**76c5317147306c477d793dc6aea9814d8111f82e**
SHA256	**01ec7b1066df7c55e262dc375bff5fd13a1fc9706c3db4b3522ac8b9d2453b52**
Packer / compiler info	**.NET executable**
Compile time	**2023-12-05 13:31:17 UTC**

Case Specific Requirements

- **Request?** (Who/what brought your attention to the malware? Maybe it was detected on your SIEM platform?)
    a. The malware was detected via a Security Information and Event Management (SIEM) platform alert. The alert was triggered due to suspicious network traffic that matched known malicious patterns.
- Where was the sample found? (You can state a fictitious endpoint)

    a. The sample was found on a fictitious endpoint named `FIN01-EP-09`, which is a finance department user's workstation running Windows 10.

- Why is this sample interesting?

    a. This malware is interesting because it is targeting a financial services endpoint, suggesting a possible data exfiltration attempt. Additionally, it is a .NET executable, indicating it could be leveraging the Windows environment for persistence and execution.

Standing Information Requirements

- **What functionality does the malware provide the attacker once it is installed successfully?**
    a. Remote access and control over the infected machine.
    b. The ability to exfiltrate sensitive files and data.
    c. Process injection and execution of arbitrary commands.
    d. Persistence on the system for prolonged exploitation.

- **Is this known malware affecting multiple organizations, malware targeting the Software Health Industry or are there indicators that this is a tailored attack?**

    a. There are indications that this may be a targeted attack, possibly tailored to financial services due to its detection on a finance department endpoint. However, further investigation is required to determine if other organizations are affected.

    b. According to virusTotal 65/75 security vendors flagged this file as malicious.

- **What indicators of compromise are associated with this malware?**
    a. Network related (IP Addresses, URLs, email addresses, unique traffic patterns)
        i. Autonomous IP addresses and domains are detected communicating with external servers.
            1. 40.127.240.158
            2. 239.255.255.250
    b. Running processes / RAM artifacts
        i. Suspicious process: `svchost.exe,WScript.exe,vkl.exe,MSBuild.exe` running under a legitimate process `svchost.exe,WScript.exe,vkl.exe,MSBuild.exe`.
    c. Registry keys of interest
        i. Registry modification detected at: `HKEY_CURRENT_USER\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN` with the key pointing to the malicious executable.
    d. File created
        i. A dropper file in `C:\Users\admin\AppData\Local\Temp\01ec7b1066df7c55e262dc375bff5fd13a1fc9706c3db4b3522ac8b9d2453b52.exe`
        ii. A persistent file located in `C:\Windows\SysWOW64\schtasks.exe`

- **Does the malware maintain persistence on the victim system? If so, how?**
    a. Yes, the malware maintains persistence by creating a startup entry in the Windows registry (`HKEY_CURRENT_USER\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN`). It also drops a copy of itself in `C:\Users\admin\AppData\Local\Temp\01ec7b1066df7c55e262dc375bff5fd13a1fc9706c3db4b3522ac8b9d2453b52.exe` and sets up a scheduled task to run on startup(`C:\Windows\SysWOW64\schtasks.exe`).

- **Which application, service or other vulnerability does this malware exploit?**
    a. The malware exploits vulnerabilities in outdated versions of Windows, specifically via a known .NET framework vulnerability.

b. Is it related to an existing CVE?
    i. If yes, list all related CVE numbers
        1. CVE-2021-42299 (related to .NET framework execution vulnerability)
        2. CVE-2020-0601 (spoofing vulnerability in Windows CryptoAPI)
    ii. If not, could it be an unknown 0-day vulnerability?
c. Does a patch exist?
d. Does Endpoint Protection protect against this attack?
    i. Some endpoint protection solutions are detecting variants of this malware, but not all AV solutions offer comprehensive coverage.

- **What remediation options are available to effectively remove the malware and return the system to a secure state?**
    a. **Isolation: Immediately isolate the infected endpoint from the network.**
    b. **Analysis: Perform full memory and disk forensics to extract additional IOCs.**
    c. **Removal: Use a robust anti-malware solution to remove the malware and associated files. Manually remove the registry entries and scheduled tasks.**
    d. **Patching: Ensure all systems are patched, especially the .NET framework vulnerabilities.**
    e. **Monitoring: Continuously monitor the network for any suspicious traffic or reinfection attempts.**

Additional Information / Examiner Notes

- The malware appears to target finance-related endpoints, making it critical to ensure that other systems in the finance department are checked for signs of compromise.
- Initial analysis suggests this malware may have advanced data exfiltration capabilities, necessitating a close review of outbound network traffic.

IOCs

- **MD5**: 9c7b97eb3958d4309e6ba38bb1a99471
- **SHA-1**: 76c5317147306c477d793dc6aea9814d8111f82e
- **SHA-256**: 01ec7b1066df7c55e262dc375bff5fd13a1fc9706c3db4b3522ac8b9d2453b52
- **File Path**: `C:\Users\admin\AppData\Local\Temp\01ec7b1066df7c55e262dc375bff5fd13a1fc9706c3db4b3522ac8b9d2453b52.exe`
- **Registry Key**: `HKEY_CURRENT_USER\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN`
- **Process Name**: `svchost.exe,WScript.exe,vkl.exe,MSBuild.exe`

Attachments

- https://www.virustotal.com/gui/file/01ec7b1066df7c55e262dc375bff5fd13a1fc9706c3db4b3522ac8b9d2453b52/community
- https://any.run/report/01ec7b1066df7c55e262dc375bff5fd13a1fc9706c3db4b3522ac8b9d2453b52/8ee8109d-d072-42d3-ab8c-98de8991229c
- https://bazaar.abuse.ch/sample/01ec7b1066df7c55e262dc375bff5fd13a1fc9706c3db4b3522ac8b9d2453b52/#file_info
- https://docs.google.com/document/d/1f-XbtqpuUVP4onX5ifxlIbvzRd0QvM3F/edit
- the Lab03 that I will submit with this docs