SECURITY ADVISORY

CYBER STASH

October, 2023

Quasar RAT Stealthy DLL Side-Loading

Context

The Quasar RAT, an open-source remote access trojan, has been observed employing DLL side-loading techniques to discreetly operate and siphon data from compromised Windows hosts. This method takes advantage of the implicit trust these files hold within the Windows environment, utilizing ctfmon.exe and calc.exe as integral components of its attack chain.

Quasar RAT, also recognized as CinaRAT or Yggdrasil, operates as a C#-based remote administration tool, offering functionalities such as collecting system information, listing running applications, accessing files, logging keystrokes, capturing screenshots, and executing arbitrary shell commands.

This trojan's utilization of DLL side-loading adds a layer of stealth to its activities, enabling it to navigate undetected through security measures while conducting its malicious operations on the compromised systems.

Mitigation

Effective mitigation strategies against Quasar RAT DLL Side-Loading require a multi-faceted approach, including:

Adversary Behavior Detection: Monitor for unusual behavior patterns to detect adversary attacks early, gaining insights into their tactics.

Forensic Depth Analysis: Conduct static and dynamic analysis of operating system artifacts with a focus on detecting post-breach compromises, allowing for timely response and mitigation of security incidents.

Anomaly Analysis of Operating System Artifacts: Identify irregularities in operating system artifacts by stacking and comparing outliers, enabling automated detection for swift response to potential security breaches.

Blocking Network Traffic: Implement proactive network traffic blocking measures, including the restriction of suspicious IPs, domains, and connections from high-risk Autonomous System Numbers, Top-Level Domains, and countries.

Technical Details

Operational Summary

- Quasar RAT's sophisticated attack begins with an ISO image file containing a legitimate binary, ctfmon.exe (renamed as eBill-997358806.exe), a disguised MsCtfMonitor.dll file (renamed as monitor.ini), and a malicious MsCtfMonitor.dll.

- The malicious code is hidden within the file 'eBill-997358806.exe,' which triggers the loading of 'MsCtfMonitor.dll' through DLL side-loading. This concealed code further injects "FileDownloader.exe" into Regasm.exe, launching the next stage involving the authentic calc.exe file.

- DLL side-loading is again employed to load the rogue Secure32.dll, ultimately delivering the Quasar RAT payload. The trojan establishes connections with a remote server, transmitting system information and enabling a reverse proxy for remote access.

- The RAT establishes a socket connection to CNC (3[.]94[.]91[.]208 >> ec2 -3-94-91-208[.]compute-1[.]amazonaws.com), transmitting victim information such as IP and Country code.

Upon decoding additional content, discernible strings associated with Quasar RAT, such as "Quasar Server," come into view.

Decoding Base64 content reveals strings such as:

⇒ SELECT * FROM Win32_OperatingSystem WHERE Primary='true'
⇒ SELECT * FROM Win32_BaseBoard
⇒ SELECT * FROM FirewallProduct
⇒ SELECT * FROM Win32_Processor
⇒ SELECT * FROM AntivirusProduct

The RAT queries for AntiVirusProduct and Firewall WMI class, indicating its interest in system security. Additionally, it seeks BIOS infrastructure, GPU details, hostname, etc.

The malicious software creates a lasting presence by adding an enduring entry to the Windows registry

⇒ HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\WindowsCalculator “c:\Users\Public\Pictures\Calc.exe /quit”

Technical Details

Tactics, Techniques and Procedures

The notable TTPs related to the Quasar RAT are:

T1073 - DLL Side-Loading

Quasar RAT conceals its malicious code within the legitimate 'eBill-997358806.exe,' triggering the loading of 'MsCtfMonitor.dll' through DLL side-loading. This allows the trojan to operate within the trusted environment of the Windows system.

T1036 - Masquerading

Legitimate binaries like ctfmon.exe are renamed to 'eBill-997358806.exe' to masquerade as innocuous files, evading suspicion during execution.

T1055 - Process Injection

The concealed code within 'MsCtfMonitor.dll' injects "FileDownloader.exe" into the legitimate process Regasm.exe, maintaining persistence and launching subsequent stages.

T1021 - Remote Services

Quasar RAT establishes connections with a remote server, enabling the transmission of system information and facilitating remote access functionalities.

T1090 - Connection Proxy

Quasar RAT sets up a reverse proxy for remote access to the compromised endpoint, allowing the attacker to control and manipulate the compromised system

Cyber Threat Intelligence

Over time, various APT groups have been recognized for employing Quasar, either in its original state or customized to align with their objectives. A few notable instances include:

APT10 (MenuPass Group)
https://attack.mitre.org/groups/G0045/

Gorgon Group
https://attack.mitre.org/groups/G0078/

References

Related IOC’s

- https://github.com/executemalware/Malware-IOCs/blob/main/2022-07-21%20Quasar%20RAT%20IOCs
- https://github.com/executemalware/Malware-IOCs/blob/main/2023-01-28%20AsyncRAT_Quasar%20RAT%20IOCs
- https://threatfox.abuse.ch/browse/malware/win.quasar_rat/

Public Intelligence

- https://blog.qualys.com/vulnerabilities-threat-research/2022/07/29/new-qualys-research-report-evolution-of-quasar-rat
- https://thehackernews.com/2023/10/quasar-rat-leverages-dll-side-loading.html?&web_view=true
- https://hackdojo.io/articles/XZKXRENKO/quasar-rat-leverages-dll-side-loading-to-fly-under-the-radar
- https://medium.com/@yua.mikanana19/quasar-rat-the-evolution-of-open-source-malware-9b828589afce