Hive Pro®

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

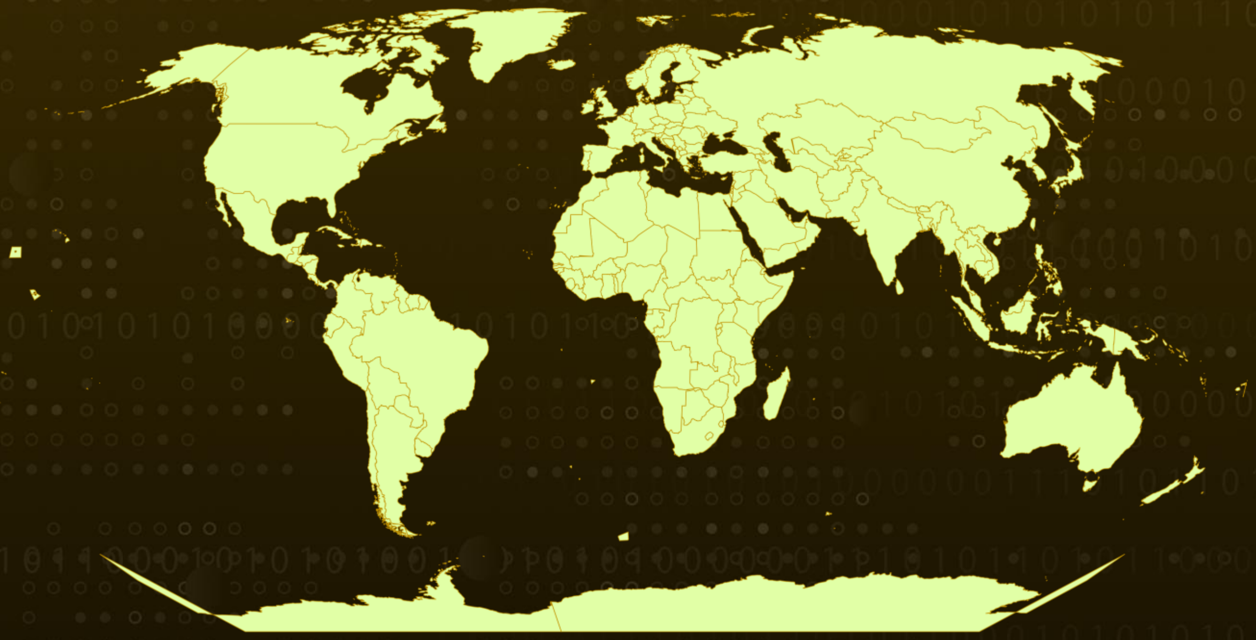
Quasar RAT Utilizes DLL Side-Loading to Evade Detection

Date of Publication	Admiralty Code	TA Number
October 23, 2023	A1	TA2023430

Summary

First appeared: July 2014
Malware: Quasar RAT (aka xRAT, CinaRAT, Yggdrasil)
Attack Region: Worldwide
Affected Platform: Windows
Attack: Quasar RAT is an open-source remote access trojan that has been used by cybercriminals and threat actors for various malicious purposes. The use of DLL side-loading is a sophisticated technique that allows malware like the Quasar RAT to blend in with legitimate processes and avoid detection. The technique is used to leverage trusted Microsoft files, to achieve objectives of dropping, deploying, and executing malicious payloads without raising suspicions.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom, Zenrin

Attack Details

#1 Quasar RAT is an open-source remote access trojan that has been used by cybercriminals and threat actors for various malicious purposes. The use of DLL side-loading is a sophisticated technique that allows malware like the Quasar RAT to blend in with legitimate processes and avoid detection.

#2 Quasar RAT is a remote administration tool developed in C#. It comes with a variety of features, including the ability to gather system information, list running applications, retrieve files, log keystrokes, capture screenshots, and execute arbitrary shell commands on the compromised host.

#3 The Quasar RAT was discovered to be distributed through advanced attack methods, including DLL side-loading and process hollowing. The attack started with utilizing legitimate ctfmon.exe binary for side-loading a malicious DLL which acquires the initial "stage 1" payload. This method capitalizes on trusted system files to evade detection.

#4 The malicious DLL launches regasm.exe and generates 'stage 1' payload called FileDownloader.exe. Within FileDownloader.exe, three binaries are stored in an archive, which are later extracted and dropped into the Public Pictures Folder. Among these files is the genuine 'calc.exe,' which is manipulated to load the rogue 'Secure32.dll' using DLL side-loading and process hollowing techniques. These series of actions ultimately leads to the deployment of the final Quasar RAT payload, injected into the computer's memory. These intricate steps underscore the attacker's high level of expertise in evading security measures.

Recommendations

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Update Software and Operating System: It is crucial to keep both your software and operating systems up to date. Regular updates often include security patches and fixes that help protect your system from potential threats.

Implement Behavioral Analysis: Deploy advanced security solutions that employ behavioral analysis and anomaly detection to identify unusual patterns of activity indicative of malware presence. This proactive approach can help catch sophisticated threats before they fully compromise your systems.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0005 Defense Evasion	TA0011 Command and Control	T1027 Obfuscated Files or Information
T1140 Deobfuscate/Decode Files or Information	T1056 Input Capture	T1055 Process Injection	T1036 Masquerading
T1055.012 Process Hollowing	T1574 Hijack Execution Flow	T1574.002 DLL Side-Loading	

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	e4eb623a0f675960acb002d225c6f1d6, B0DB6ADA5B81E42AADB82032CBC5FD60, 32DE5C2E0BA35CEAC3C515FA767E42BF, d07e4afd8f26f3e2ce4560e08b7278fb, 532AF2DB4C10352B2199724D528F535F
IP	3.94.91[.]208
URL	ec2-3-94-91-208[.]compute-1[.]amazonaws.com

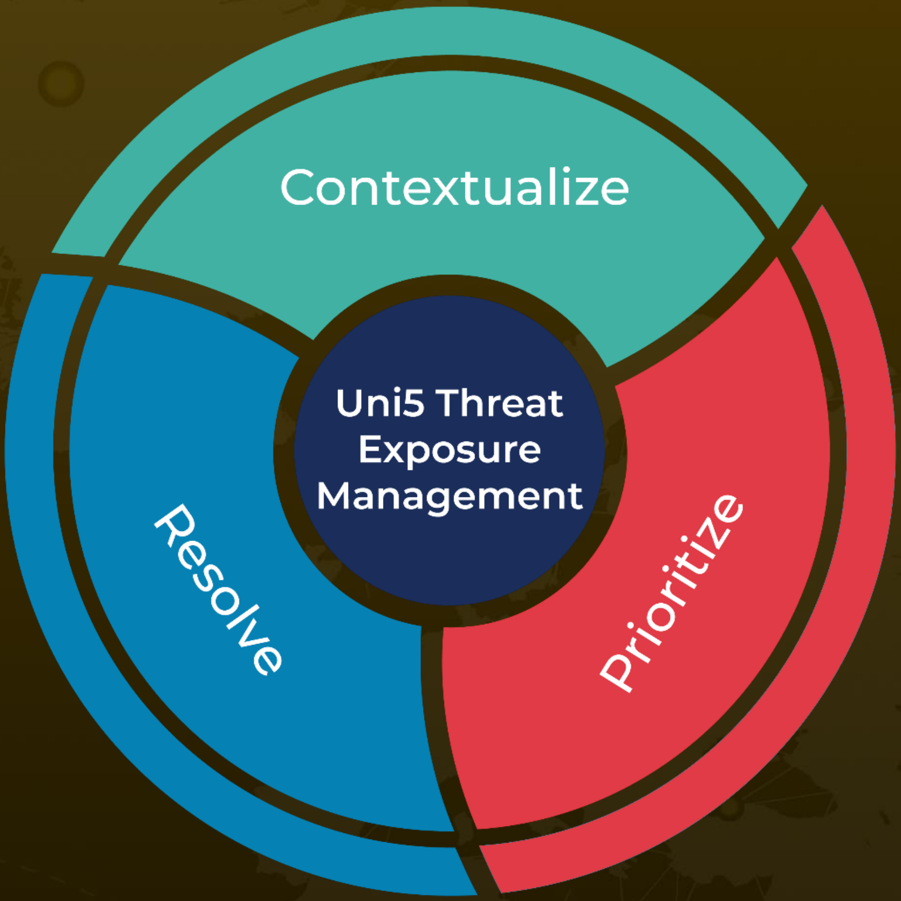
References

https://www.uptycs.com/blog/quasar-rat

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

October 23, 2023 • 7:30 AM

More at www.hivepro.com