


Mphasis SOC – Information Security News

Date & Time Issued: 27-JUN-2024, 21:30 IST

Title	Quasar Remote Access Trojan	
Summary	<ul style="list-style-type: none"> Quasar virus is a Remote Access Trojan (RAT) that is often abused by cybercriminals to take remote control over users' computers for malicious purposes. The Quasar RAT was first discovered and is known for its ability to evade detection by most anti-virus software. The Quasar RAT is typically spread through phishing emails or other social engineering tactics. Once a victim clicks on a malicious link or downloads a malicious file, the Quasar RAT will be installed on their computer without their knowledge. Quasar RAT is a .NET framework open-source remote access trojan family used in cyber-criminal and cyber-espionage campaigns to target Windows operating system devices. It is often delivered via malicious attachments in phishing and spear-phishing emails. 	
Severity	Medium 	
Attack Vectors	<p>Quasar RAT allows the attacker to perform a variety of malicious actions, including:</p> <ul style="list-style-type: none"> Viewing and manipulating files on the victim's computer. Recording keystrokes and stealing login credentials. Taking screenshots and recording audio and video from the victim's webcam and microphone. Installing other malware or tools to further compromise the victim's computer or network. Using the victim's computer as a part of a botnet to launch attacks on other targets. This tool is capable of various functions such as gathering system data, running applications, transferring files, recording keystrokes, taking screenshots or camera captures, recovering system passwords, and overseeing operations like File Manager, Startup Manager, Remote Desktop, and executing shell commands. The attacker's identity and initial access method remain uncertain, but phishing emails likely distribute the attack. This highlights the need for user caution with suspicious emails, links, and attachments. 	
Indicator of Compromise	INDICATOR TYPE	INDICATORS
	File Hash	<ul style="list-style-type: none"> 01d7838a7a970a4fca588740cf6f8129f4ae01b0d9936eb43a1aff9436b848a2 653798b0c7226a4189bde9afaae0f0c540216c2acda512c809a61008e4ae169 1b586bfe3423ef03ecba497e90fd31b42022dd8e1f325e212c1e23cc58ba7be7 a451e748bc1e4c05bdaa722b35a5f6dd1a78765ac8967187a61b846f819c8bf6 76f06975c4f0772d68e2a30d8e0c62b1f8c484e2ce7b0979c63c4cf519a40b61 4e85fc6b1d7119195b46633bd051c65074eebf181d8f9cd142ecc0e7a9bcc3b8 164e19d48c8d3ed423d4d4c68dff47899f375b6ef4f2a27005562e16b3a8d33f 4833f6e7b2beb3821ccd544a936f3d6db6403ee58c05038f15f2d1544f2acd3c d53df5b6b080ba24773ca16c7a8b70eeb783ead278712e0c5b44abc84805e60e 7c5919ffcd3234d3c520120fbb9204e11ca3adfbfc175175a1e087492cbbba
Recommendations	<ul style="list-style-type: none"> Security administrators should block the IoCs on all applicable security solutions post-validation. Security administrators should make sure that all applications, databases, servers, and network devices are periodically hardened and are adequately configured. Users should not download suspicious applications or attachments received over the internet and should be vigilant against social engineering and phishing attacks. Users are recommended to use a unique and strong password at every site with the help of a password manager and use Multi-Factor Authentication (MFA) wherever possible. Users should not download, accept, or execute files and do not visit websites or follow links provided by unknown or untrusted sources. Organizations are recommended to have a behavioral detection solution in place to successfully detect the presence of malware payloads. Keep AV signatures, operating systems, and third-party applications up to date on all systems, mobile devices, and servers. <p>NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre -Prod or test environment before implementing. diligence and impact analysis.</p>	

References

- <https://www.rewterz.com/threat-advisory/quasar-rat-aka-cinarat-active-iocs-3>

The information contained in this message is proprietary. It is for Mphasis and its customers only.
Copyright © 2023. All rights reserved by Mphasis.