Quasar Remote Access Trojan (RAT)

Author: Christopher Kim

Overview

During 24-26 September, we discovered a large malicious email (malspam) campaign distributing the Quasar remote administration tool. The emails used a payment theme, and each email contained a ZIP file attachment with one of three Quasar client executables. Based on the client's traffic patterns, we believe that the actor built these executables using the open-source Quasar server client builder v1.3.0.0.

Customer Impact

Quasar is an open-source tool designed for Microsoft Windows operating systems and is publicly available on GitHub.[1] It comes with built-in keylogging, image capturing, and webcam recording capabilities. Threat actors, including advanced persistent threat (APT) actors, can use Quasar as a remote access trojan (RAT) to penetrate and control systems, as well as steal and exfiltrate data.

In December of last year, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) reported that APT actors used Quasar for cyber espionage campaigns.[2] On 20 December, we also published information on a group of Chinese threat actors called APT10 and their use of Quasar.[3]

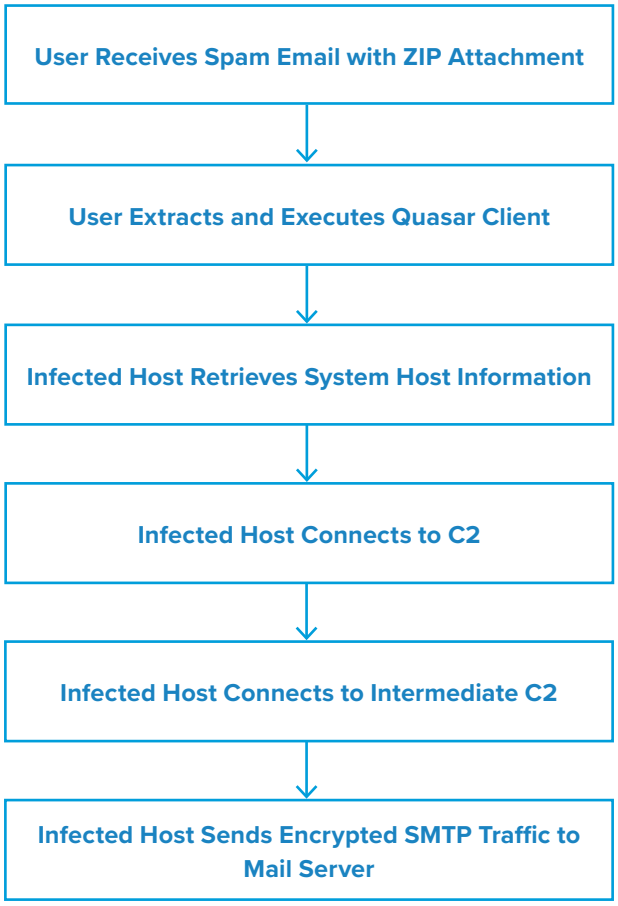
Campaign Analysis

Previous Quasar malspam campaigns reportedly delivered specially crafted documents with embedded macros to download the malicious client executables.[4,5] In this recent campaign, the email subjects were "Hello <recipient> Urgent Account details confirmation for payment" and the attachment was a ZIP file that directly contained the client executable without a downloader.

Attack Chain

When we launched several of the executables in a Windows virtual machine, they dropped the Quasar clients in the C:\Users\admin\AppData\Roaming\ directory and wrote them as filename.exe. This is a typical setup for Quasar clients. The server client builder limits the folder locations in which clients are placed to the base directories %APPDATA%, Program Files, and Windows\SysWOW64.

The network behavior and traffic data indicated that the installed clients were built using Quasar v1.3.0.0, which is the latest available version on GitHub. Clients used the browser agent "Mozilla/5.0 (Windows NT 6.3; rv:48.0) Gecko/20100101 Firefox/48.0" and made HTTP GET requests to a free IP geolocation lookup service. The response



provided them with host system information including geolocation metadata, WAN IP address, and Internet service provider (ISP) details.

The executable modified the value of the Windows registry key HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run to automatically run Quasar clients during Windows launch, a common malware technique to achieve persistence on a victim's machine. We only observed Quasar generating traffic to the IP lookup service and its command and control (C2). However, on 25 September, the Internet Storm Center reported on additional processes that connected to an intermediate C2 and encrypted SMTP traffic from the infected host to a mail server.[6] The security community has also seen other malware such as keyloggers that use the same intermediate C2.[7]

Vulnerabilities & Mitigation

In addition to the general safety tips related to malicious emails, network defenders can use unique traffic patterns and proxy log information to detect Quasar activities in their network. Network defenders should also note that the following mitigation tips may be less effective if the actor uses a customized version of the Quasar tool.

- Identify browser user-agent strings that Quasar uses in the proxy server logs. Quasar v1.3.0.0 uses "Mozilla/5.0 (Windows NT 6.3; rv:48.0) Gecko/20100101 Firefox/48.0" for querying GeoIP services.
- Determine whether systems are making calls to IP check services during Windows startup.
- Apply some of the Snort signatures related to user-agent strings and traffic payload sizes provided by CISA.[8]
- Implement reputable antivirus solutions that can detect various RAT executables.

Endnotes

1. https://github.com/quasar/QuasarRAT
2. https://www.us-cert.gov/ncas/analysis-reports/AR18-352A
3. https://sites.google.com/a/infoblox.com/cyberint-threat-labs/home/publication-repo/20181220_APT10_CTA_ Endnotes.pdf
4. https://cofense.com/advanced-phishing-campaign-delivers-quasar-rat/
5. https://community.rsa.com/community/products/netwitness/blog/2017/10/02/malspam-delivers-rat-spyware-quasar-9-27-2017
6. https://isc.sans.edu/diary/rss/25354?utm_source=dlvr.it&utm_medium=twitter
7. https://myonlinesecurity.co.uk/more-compromised-windstream-email-sending-malspam-with-orion-keylogger/
8. https://www.us-cert.gov/ncas/analysis-reports/AR18-352A

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com