New Qualys Research Report: Evolution of Quasar RAT

blog.qualys.com/vulnerabilities-threat-research/2022/07/29/new-qualys-research-report-evolution-of-quasar-rat

Viren Chaudhari

July 29, 2022

The Qualys Threat Research Team continues to inform enterprise cybersecurity teams of emerging threats that could impact their business. These threat intelligence reports summarize individual threat exploits and provide practical recommendations for protecting against them.

In this free research report, we analyze Quasar RAT which has been widely leveraged by multiple threat actor groups targeting both government and private organizations in Southeast Asia and other geographies.

Quasar RAT (aka: CinaRAT, Yggdrasil) is an open-source remote access trojan (RAT) that has been widely adopted by bad actors due to its powerful techniques. Quasar RAT has been behind multiple attack campaigns by advanced persistent threat (APT) groups and most recently, a Chinese threat group APT10 was observed using it for targeted attacks.

The intelligence in this report can be used by SOC analysts, threat hunting teams, cyberthreat intelligence analysts, and digital forensics teams.

This complementary paper examines the evolution of the Quasar RAT payload, unpacks its configuration, details a technical analysis of the malware payload, and finally presents possible detection parameters using Qualys Multi-Vector EDR.

Download your copy of the report now to learn about our key research findings:

- Quasar RAT is a full featured remote administration tool that has been open source since at least 2014
- The .NET executable has its communication encrypted through HTTPS which uses a TLS1.2 protocol
- Quasar RAT features provide techniques related to persistence, injection, and defense mechanisms
- The RAT has been actively leveraged by various APT groups such as APT10 to achieve its malicious objectives

Get your copy of this new Qualys Threat Research Report now. No registration required.

DOWNLOAD REPORT