Exterminating a RAT

FIREEYE MANAGED DEFENSE IN ACTION

Sometimes limited visibility can hinder alert validation or malicious activity investigation efforts. FireEye Managed Defense analysts’ main objective is to discover malicious activity as early as possible to reduce the consequences of a breach using whatever technology is available to them.

Managed Defense analysts continue to analyze data from all sources of evidence to determine the extent of an intrusion, and help customers address critical questions such as: What is the impact? Who did it? How did they get in? Are they gone?

In a recent incident, Managed Defense analysts were alerted to suspicious activity involving a variant of Quasar RAT specific to threat group APT10. Despite limited visibility into the environment, Managed Defense analysts provided the victim organization full remediation recommendations within 23 hours of the alert.

PROBLEM:
Network alert triggered for Quasar RAT at customer with network only visibility. Difficult to investigate impact based on network only visibility.

HOW WE DID IT:
Leveraged network full packet capture capabilities to validate the original detection, pulled additional evidence for scoping and analysis, and augmented the customer’s response capabilities where needed.

HOW WE DID IT BETTER:
Our malware reverse engineers decrypted the attacker traffic, including every command the attacker executed. As a result, the customer knew the attacker’s actions - what they did and how they did it, with minimal investigative effort. This allowed for a comprehensive remediation effort.

RESULT:
Managed Defense analysts were able to provide the network only client with full transparent visibility into a serious Advanced Persistent Threat actor in their environment from a single network alert.
Exterminating a RAT

**BUSINESS IMPACT**

The Managed Defense team’s ability to identify malicious activity as early as possible and to leverage highly specialized resources minimized the impact of the breach. Analysts were able to confirm suspicious activity, investigate the incident, and provide remediation recommendations within 23hrs, all despite minimal visibility. This activity enabled the client to avoid major business impact from the breach.

Because the threat was identified early enough, there was minimal business impact, allowing the client to avoid having to send breach notifications; avoid going into a costly IR effort; avoid any litigation fees and experience no impact on revenue.

---

**Initial Detection**
- Alert triggered from product detection
- Customer notified of suspicious activity

**Investigation**
- Triaged all alerts for Quasar RAT network detections
- Collected additional files from client for increased visibility
- Merged all packet capture files to analyze larger data sets
- Confirmed detection was a true positive

**Remediation Recommendations**
- Performed manual network protocol analysis
- Compared captured data to previously confirmed Quasar RAT traffic captures.
- Attempted to decode network traffic file using FireEye internal tooling

**Report written and remediation recommendations sent to customer**

---

**101 Days**
Average days before a breach is detected*

**$3.62 M**
Average cost of a breach**

**$0**
Cost of Breach for Managed Defense Client

**23 Hours**
Managed Defense Alert to Remediation Recs

---

*2018 Malware Report **2017 Ponemon Report
TALES FROM THE TRENCHES

Exterminating a RAT

FULL STORY

Managed Defense analysts triaged the alert, successfully confirmed that the alert was a true positive for Quasar RAT (specifically the APT10 variant of the Quasar RAT network protocol) and provided remediation recommendations to the customer.

Analysts didn’t stop there. Even though the customer was protected and knew something had transpired, the details of the attacker’s activities were unclear. At this point there was zero visibility into the activity and what the attackers had done.

After ensuring the client was protected, analysts began to dig into the network traffic captured by the FireEye network sensor. Original attempts to decode network traffic files using FireEye internal tooling designed for decoding known common or custom network protocols (e.g.: Microsoft SMB, Quasar RAT, CHOPPER web shell, etc.) did not provide the full story.

Working closely with the client, Managed Defense analysts were able to obtain additional files to analyze as suspected Quasar RAT payloads. Analysts conducted reverse engineering and sandbox analysis and were able to identify the files as a dropper/loader for a final .NET payload. This is a common approach for APT10, but it still did not include the final malicious payload, which should contain the encryption keys for communicating with the C2 server.

After continuing to collect and analyze new data from the client, including new files acquired from endpoints, analysts found a .NET file that was the actual Quasar RAT payload. The customer provided third party analysis of the sample and extracted keys from the payload which they provided along with the samples. Analysts confirmed the keys with the samples provided and used these keys to decrypt the Quasar RAT network traffic.

Once decrypted, Managed Defense analysts obtained more visibility into the activity performed by APT10 - at least what was acquired in the network captures. Analysts could see commands executed, tools uploaded and files extracted from the client environment. A full report was written to reflect these new findings and sent to the client.

About Quasar Rat

Quasar RAT is a publicly available remote access Trojan (RAT) that is a fully functional .NET backdoor and is advertised on GitHub as a legitimate remote administration tool, but its features can be easily leveraged for malicious intent.

Some of the malware’s capabilities include enumerating local drives and directories, downloading and uploading files to a remote server, collecting and exfiltrating sensitive system information, executing system commands, establishing a TCP proxy, and downloading and executing additional plugins for added capabilities.

THREAT TYPE: Unknown Threat

THREAT ACTORS: APT10

CAPABILITY: Backdoor, Beaconing, Command and Control, Data Theft

MALWARE: QUASAR RAT