Recorded Future®

Network Intelligence by Recorded Future

Recorded Future's Network Intelligence offers powerful, global visibility within its platform and integrations to track and alert on many kinds of malicious activity.

Through proprietary sources, Recorded Future monitors a wide range of malicious infrastructure in real-time including the top **100 malware** families and over **1 million command and control (C2)** servers scanned monthly.

Network Intelligence data and alerts can power dashboards and drive actions within other security platforms. A notification of communication with a command & control (C2) server can launch a threat hunt in other tools for related activity to understand the scope of the threat.

This powerful combination lets you see potential threats targeting your company, partners, or even your entire region all within the familiar interface of Recorded Future's SecOps and Threat Intelligence modules.

Introduction to Network Intelligence

Network Intelligence refers to the analytics derived from monitoring and analyzing data traveling through a network. This capability provides a mechanism to detect and respond to adversaries.

Recorded Future categorizes our network intelligence into three categories: **Malicious Traffic Analysis, DDoS Traffic Analysis** and **Internet Scanners**.

- **Malicious Traffic Analysis** identifies activities such as Command and Control (C2), Data Exfiltration, Malware Distribution, and Botnets. Malicious Traffic Analysis is further split into victim and admin traffic to accurately identify the threat from actor to victim.
- **DDoS Traffic Analysis** monitors for surges in internet traffic associated with DDoS attacks, including the top source and target IP addresses with associated companies.

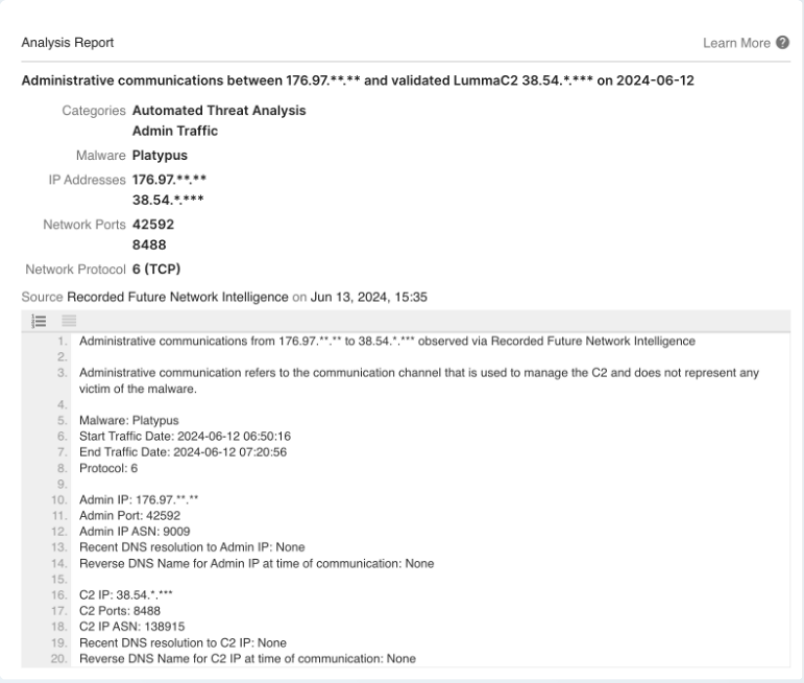

Figure 1: Sample Network Intelligence Results for a LummaC2 Server

Recorded Future®

Network Intelligence by Recorded Future

Use Cases

Understand how your company's infrastructure is directly impacted

Quickly identify if a company server has been compromised, such as acting as a C2 or is a source or victim of DDoS traffic.

Receive notifications of relevant traffic involving company infrastructure within minutes with five pre-built alerts.

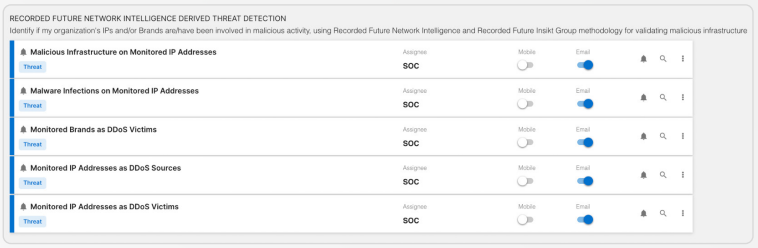

Figure 2: Pre-Built Alerts for Company Brand Name, IP Addresses within Network Intelligence Dataset

Investigate what is happening external to your environment

Monitor for malicious traffic across proprietary sources and network metadata to better understand the infrastructure of an attack, particularly admin traffic.

Analysts can use the advanced query builder (AQB) to identify attack patterns and trends, such as DNS Reflection attacks. For example, an analyst can track if there is a targeted infostealer campaign against companies in a specific country or track specific threat actors.

Automatically Enrich Indicators of Compromise (IoCs)

Network Intelligence powers risk rules within Intelligence Cards™ to help operators quickly identify malicious indicators (IoCs) and how to escalate.

Recorded Future recognizes not only whether an IP address is a C2 server, but validates it is an active admin IP. This intelligence decreases the number of false positives an analyst needs to review, reducing workload.

Third-Party Intelligence users can also understand which third parties are experiencing active company infections.

Figure 3: Valid C&C Server Risk Rule for an AsyncRAT IP Address

Recorded Future Network Intelligence is available within multiple modules, including SecOps, Brand, Threat and Third-Party for applicable use cases described above.