

Network Intelligence by Recorded Future

Recorded Future's Network Intelligence offers powerful, global internet traffic 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 **tens of thousands of 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 undeersratnaable the scope of the threat.

This powerful internet traffic telemetry 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.

Analysis Report Learn More

Administrative communications between 176.97.*.* and validated LummaC2 38.54.*.* on 2024-06-12

Categories: **Automated Threat Analysis**
Admin Traffic

Malware: **Platypus**

IP Addresses: **176.97.*.***
38.54.*.*

Network Ports: **42592**
8488

Network Protocol: **6 (TCP)**

Source: Recorded Future Network Intelligence on Jun 13, 2024, 15:35

1. Administrative communications from 176.97.*.* to 38.54.*.* observed via Recorded Future Network Intelligence
- 2.
3. Administrative communication refers to the communication channel that is used to manage the C2 and does not represent any victim of the malware.
- 4.
5. Malware: Platypus
6. Start Traffic Date: 2024-06-12 06:50:16
7. End Traffic Date: 2024-06-12 07:20:56
8. Protocol: 6
- 9.
10. Admin IP: 176.97.*.*
11. Admin Port: 42592
12. Admin IP ASN: 9009
13. Recent DNS resolution to Admin IP: None
14. Reverse DNS Name for Admin IP at time of communication: None
- 15.
16. C2 IP: 38.54.*.*
17. C2 Ports: 8488
18. C2 IP ASN: 138915
19. Recent DNS resolution to C2 IP: None
20. Reverse DNS Name for C2 IP at time of communication: None

Figure 1: Sample Network Intelligence Results for a LummaC2 Server

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 command and 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.

RECORDED FUTURE NETWORK INTELLIGENCE DERIVED THREAT DETECTION				
Identify if my organization's IPs and/or Brands and/or have been involved in malicious activity, using Recorded Future Network Intelligence and Recorded Future Inskit Group methodology for validating malicious infrastructure				
Malicious Infrastructure on Monitored IP Addresses	Assigned	SOC	Mobile	Email
Malware Infections on Monitored IP Addresses	Assigned	SOC	Mobile	Email
Monitored Brands as DDoS Victims	Assigned	SOC	Mobile	Email
Monitored IP Addresses as DDoS Sources	Assigned	SOC	Mobile	Email
Monitored IP Addresses as DDoS Victims	Assigned	SOC	Mobile	Email

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.

Triggered Risk Rules on Jun 13, 2024			
All (6)	Very Malicious (2)	Suspicious (3)	Unusual (1)
Actively Communicating Validated C&C Server			
Recorded Future Network Intelligence. Multiple communications observed between 86.33.*** on port 35796 and 104.243.*** (validated AsyncRAT on port 4016 on 2024-06-12 at 09:11 UTC.			
383 sightings on 1 source			

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