## ·III 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.

Categorie Malwar IP Addresse Network Portoc Source Recorde	8488 Bab biol 6 (TCP) and Future Network Intelligence on Jun 13, 2024, 15:35 Istrative communications from 176.97.**, ** to 38.54.*, *** observed via Recorded Future Network Intelligence Istrative communication refers to the communication channel that is used to manage the C2 and does not represent any of the malware.
Malwar IP Addresse Network Portoco Source Recorde II Admini 2. Admini 4. 5. Malwar 6. Start 7. End Tr	Admin Traffic re Platypus solutions 176.97.**** 38.54.**** ts 42592 8488 tol 6 (TCP) tol 4 CTCP) tol 4 CTCP) tol 5 CTCP tol 5 CT
IP Addresse Network Portoc Source Recorde	re Platypus se 176.97.**.** 38.54.**** ts 42592 8488 iol 6 (TCP) dd Future Network Intelligence on Jun 13, 2024, 15:35 istrative communications from 176.97.**.* to 38.54.*.*** observed via Recorded Future Network Intelligence istrative communication refers to the communication channel that is used to manage the C2 and does not represent any of the malware.
IP Addresse Network Portoc Source Recorde	es 176-97.**** 38.54.**** 15 42592 8488 iol 6 (TCP) id Future Network Intelligence on Jun 13, 2024, 15:35 istrative communications from 176.97.*** to 38.54.*.*** observed via Recorded Future Network Intelligence istrative communication refers to the communication channel that is used to manage the C2 and does not represent any of the malware.
Network Portoc Source Recorde I. Admini 2. Admini 2. Admini 4. Start 5. Matwar 6. Start 7. End Tr	38.54.**** ts 42592 8488 iol 6 (TCP) bd Future Network Intelligence on Jun 13, 2024, 15:35 istrative communications from 176.97.**,** to 38.54.*,*** observed via Recorded Future Network Intelligence istrative communication refers to the communication channel that is used to manage the C2 and does not represent any of the malware.
Network Protoc Source Recorde	ts 42592 8488 sol 6 (TCP) ad Future Network Intelligence on Jun 13, 2024, 15:35 istrative communications from 176.97.**.** to 38.54.*.*** observed via Recorded Future Network Intelligence istrative communication refers to the communication channel that is used to manage the C2 and does not represent any of the malware.
Network Protoc Source Recorde	8488 Bab biol 6 (TCP) and Future Network Intelligence on Jun 13, 2024, 15:35 Istrative communications from 176.97.**, ** to 38.54.*.*** observed via Recorded Future Network Intelligence Istrative communication refers to the communication channel that is used to manage the C2 and does not represent any of the malware.
Source Recorde	of 6 (TCP) d Future Network Intelligence on Jun 13, 2024, 15:35 istrative communications from 176.97.*** to 38.54.*.*** observed via Recorded Future Network Intelligence istrative communication refers to the communication channel that is used to manage the C2 and does not represent any of the malware.
Source Recorde	d Future Network Intelligence on Jun 13, 2024, 15:35 istrative communications from 176.97.*** to 38.54.*.*** observed via Recorded Future Network Intelligence istrative communication refers to the communication channel that is used to manage the C2 and does not represent any of the malware.
III Admini 2. 3. Admini victim 4. 5. Malwar 6. Start T 7. End Tr	istrative communications from 176.97.**.** to 38.54.*.*** observed via Recorded Future Network Intelligence istrative communication refers to the communication channel that is used to manage the C2 and does not represent any of the malware.
III Admini 2. 3. Admini victim 4. 5. Malwar 6. Start T 7. End Tr	istrative communications from 176.97.**.** to 38.54.*.*** observed via Recorded Future Network Intelligence istrative communication refers to the communication channel that is used to manage the C2 and does not represent any of the malware.
1. Admini 2. 3. Admini victim o 4. 5. Malwai 6. Start T 7. End Tr	istrative communication refers to the communication channel that is used to manage the C2 and does not represent any of the malware.
2. 3. Admini victim o 4. 5. Malwai 6. Start T 7. End Tr	istrative communication refers to the communication channel that is used to manage the C2 and does not represent any of the malware.
4. 5. Malwa 6. Start T 7. End Tr	of the malware.
4. 5. Malwa 6. Start T 7. End Tr	
5. Malwa 6. Start T 7. End Tr	re: Platynus
<ol> <li>Start T</li> <li>End Tr</li> </ol>	re: Platvous
7. End Tr	raffic Date: 2024-06-12 06:50:16
	ramc Date: 2024-06-12 06:50:16 affic Date: 2024-06-12 07:20:56
9.	0.0
	IP: 176.97.**.**
	Port: 42592
12. Admin	IP ASN: 9009
13. Recent	t DNS resolution to Admin IP: None
14. Revers	se DNS Name for Admin IP at time of communication: None
15.	
16. C2 IP:	
17. C2 Por	
	ASN: 138915 t DNS resolution to C2 IP: None
20. Revers	



## ·III 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.

Malicious Infrastructure on Monitored IP Addresses	Assignee SOC	Mobile	Emai	Q	1
Malware Infections on Monitored IP Addresses Threat	Assignee SOC	Mobile OT	Emai	Q,	1
Monitored Brands as DDoS Victims Trreat	Assignee SOC	Mobile O	Emai	٩	I
Monitored IP Addresses as DDoS Sources Treat	Assignee SOC	Mobile OTD	Email	Q	I
Monitored IP Addresses as DDoS Victims Terest Terest	Assignee SOC	Mobile Ditte	Emai	Q	1

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<sup>™</sup> 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.

Iriggere	d Risk Rules on Jun 13	, 2024	
All (6)	Very Malicious (2)	Suspicious (3)	Unusual (1)
Active	ly Communicating Val	idated C&C Server	0
0.0000000	, .		communications observed between 86.33.***** on port 35796 and 104.243.**** (validated AsyncR.
Recor	, .	telligence. Multiple c	

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