SOLUTION BRIEF

TEAM CYMRU™

Threat Intelligence Feeds

The Most Comprehensive, Pure Signal™ Intelligence

Threat Intelligence Feeds

The Most Comprehensive, Pure Signal™ Intelligence

Team Cymru is a threat intelligence pioneer, and our data powers many security vendors' offerings. We maintain unmatched visibility through a global collaboration model that no other vendor can duplicate.

In addition to a global network of sinkholes, honeypots, darknets and sensors, we work with ISPs, hosting providers and over 130 CSIRT teams across 86+ countries to make the Internet a safer place. We deliver free services to these partners, and in exchange, they enrich our threat intelligence. As a result, we are observing activity across every ASN on the Internet and scoring that activity to bring you unparalleled threat intelligence.

94,000,000 system interactions scored per day

400,000 command and control servers polled per month

Observing activity across **every ASN on the Internet**

Our Knowledge is Your Intelligence...

Botnet Analysis & Reporting (BARS)

For malware analysts, researchers and threat hunters

- Holistic adversarial campaign view
- Correlation across C2s, victim IP addresses, malware, targets and DDoS attack instructions
- Geolocation victimology info
- Complete campaign history of malware used
- Covers only tracked malware families
- Only controllers that we have reverse engineered

Controllers

For network security teams

- DNS Centric
- All controllers we observe – no victims –URIs and DSNRRs
- Broadest range of controller family-types
- Includes tracked malware families, as well as new and unnamed malware families
- Provides the full URL, malware hash, and DNS resource record
- Block compromised nodes from calling out
- Block malicious attachments
- Application-level firewalling
- Block MD5/SHA1 files from being executed or downloaded via group policy

IP Reputation

For network and gateway security teams

- IP centric
- Widest range of victims
- Lighter weight feed of controller and victim IP addresses
- No URIs
- Puts the power of curation in your hands
- Vet visitors to a service
- EDR as a service
- Firewall optimization
- Auto de-prioritization of low-criticality alerts (e.g. scanners)

Reputation Scoring

Each entry is assigned a score based on factors, such as number of days appearing, categories appearing, detection method, SSL presence, ports and other variables, such as shared hosting factors. The intention is that partners determine what issues are most important to them and adapt their policy accordingly.

Botnet Analysis and Reporting Service (BARS)

Discover or mitigate malware that detection tools have missed.

This service provides in-depth analysis, tracking, and history of malware families that utilize unique control protocols and possibly encryption mechanisms. It is a subset of everything we track, focused on correlation and context for researchers and analysts.

The data is broken into three separate XML schemas updated hourly.

.Bot XML File

- Includes botnet IP, BGP and GeoIP
- Each host categorized with type of malware infection, including additional elements

Command and Control XML File

- Includes botnet type, host information and malware hashes when available
- Three botnet types across IRC (Internet Relay Chat), HTTP, and P2P (Peer to Peer)
- Additional details, such as IP addresses, ports, channels or C2 passwords.

DDOS XML File

- Provides attack targets, victim location, time of attack, and duration

Manually decoded and decrypted

- Fast insights into C2 and DDoS attacks without processing efforts

Updated every 60 minutes

- Near-real-time, global Internet visibility

In-depth analysis and tracking of 40+ malware families

- Comprehensive reference database of the highest occurring and most impactful malware

DDoS Attack Categorization

TCP:	TCP-based traffic attack
UDP:	UDP-based traffic attack
ICMP:	ICMP-based traffic attack
SYN:	Syn flood attack
HTTP:	HTTP/HTTPS-based resource attack

DNSamp:
DNSamplification attacks (DNS recursion)

Undetermined:
The category could not be determined on available info

Command and Control (C2) Feed

Every controller we observe and associated malware.

The controller feed delivers near-real-time data on threat actor infrastructure, allowing you to prevent malicious communications and prevent payload execution. This service provides the full URL and all known details, including malware hashes, of C2 infrastructure.

Our data allows for real-time identification of botnet command and control (C2) IP addresses (IRC, http, and P2P) built for DDoS, warez, and underground economy — to include bot types, passwords, channels, and our own insight.

Use Cases

- Block compromised nodes from calling out
- Block malicious attachments
- Application-level firewalling
- Block MD5/SHA1 files from being executed or downloaded via group policy

Controller Feed Entries Include:

- All possible IP addresses.
- Domain name and HTTP URL
- First seen time
- Last checked time
- Recent up and down times
- Family, sub-family and version details
- Protocol and port
- Whether currently resolves or active in DNS
- Confidence score
- SHA1 and MD5 for malware samples
- SSL and request type for HTTP C2s
- Password, channel and key for IRC servers

Mechanically verified every 60 minutes; manual verification after 7 days

- Entries no longer responding on a given IP address and port are removed.

Continuous monitoring of inactive nodes and networks

40+ tracked malware families, as well as generic and unnamed malware families specific to C2s

- Includes SHA1/ MD5 hashes

Broadest range of generic controllers

Updated every 60 minutes

IP Reputation Feed

Lightweight, near-real-time feed of all controllers and victims

Team Cymru is known for having the most comprehensive visibility into global Internet traffic telemetry. Our IP Reputation Feed is a full list of IP addresses known to have communicated with a C2 in the last 60 minutes. In addition, every C2 IP address for IRC-based, HTTP-based and P2P-based botnets is included, providing visibility into botnets that normally evade monitoring.

Other categories of potentially compromised devices like routers, darknet visitors, and abused proxies are also included.

Use Cases

- Secure gateway and CASB optimization
- EDR as a service
- Firewall optimization
- Auto de-prioritization of low-criticality alerts (e.g. scanners)

Lightweight and near-real-time, the IP Reputation feed includes...

- **Controllers:** All controllers from the controller feed –(no urls or malware hashes).
- **Bots:** Infected clients participating in a botnet
- **Scanner:** IP addresses observed scanning organizations' networks
- **Darknet:** IP addresses that scan dark space for vulnerable hosts
- **Proxy:** Systems being used as a proxie to connect to the public Internet
- **Open Resolvers:** DNS servers capable of using DNS amplification and reflection DDoS attacks
- **Bruteforce:** IP addresses seen to be trying to attack authentication services
- **Phishing:** Infected systems involved in hosting malicious phishing pages
- **Honeypot:** IP addresses interacting our honeypot networks
- **Spam:** IP addresses engaged in sending spam emails

Mechanically verified and updated every 60 minutes; manual verification after 7 days

- Entries no longer responding on a given IP address and port are removed.

Widest range of victims

Team Cymru's complete bot coverage