INTELLIGENCE FEEDS
As a Security Professional or Product Manager it’s critical that you have the right insight to help with the problem you’re looking to solve.

Be it command and control data related to DDoS or botnets for your service or application, IP address reputation data for your e-commerce services, or fresh malware data for your research team, we have data to suit your needs.

WITH THREAT INTELLIGENCE, YOU CAN CUSTOMIZE YOUR TYPE OF SECURITY

REPUTATION DATA

Our reputation data provides rich categorical reputation information based on IP addresses. If you need to know if an IP address is a known compromised device, an infected bot, or even the source of spam, this feed is ideal.

Updated hourly, the data includes an event timestamp along with supporting detail for a number of categories of reputation affecting activities. Using our global network of sinkholes, Darknets, and sensors, we deliver unparalleled reputation data for your service or product. This data can be found in the Reputation Feed as well as the premium BARS Feed.

CONTROLLER DATA

We track thousands of controllers (C&Cs) every day. This dataset includes the IP address, domain and URL information, and the associated malware hash or hashes responsible for infection, updated hourly.

All of this information as well as first and last seen timestamps are provided in an easily interpreted XML format. Controller data can be found in the Controller Feed as well as the premium BARS Feed.
The Controller Feed contains all of our botnet controller data from the Botnet Analysis and Reporting System (BARS), a unique system that enables visibility into botnets that normally evade monitoring, plus other sources for our most comprehensive view of Command and Control (C2) for IRC-based, HTTP-based, and P2P-based botnets. This feed provides the full URL, malware hash, and DNS resource record of the controllers enabling you to cross reference, monitor, or block connections.

The full Controller Feed XML Schema is available and documented with entries varying based on the type of botnet and the insight we have been able to obtain. All times are UTC.

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

Contains all confirmed, active botnet, warez, underground economy and other malware distribution command points.

Recipients of this report can use data to automatically filter access to C&C IP addresses, thus preventing client hosts contributing to the purpose of the malware.

The report is updated every 60 minutes with manual reverification of each entry after seven days, and removal of those entries that no longer respond on given IP and port.

Controller Feed Entries Include:
- Multiple IP addresses for a single botnet
- 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 value
- SHA1 and MD5 for malware samples
- SSL and request type for HTTP C2s
- Password, channel and key for IRC servers
FREQUENTLY ASKED QUESTIONS

HOW DO I GET THE CONTROLLER FEED?
Partners simply navigate to our Content Delivery Network (CDN) with the credentials we provide.

WHICH TIME ZONE IS USED?
This feed has multiple timestamps for C2 (Command and Control Server) entries including generated, first_seen, first_active, came_up, went_down, last_checked. All follow the same time format in UTC of the form: YYYY-MM-DD HH:MM:SS

WHAT ABOUT THE MALWARE?
In addition to specific URL and DNSRR (DNS Resource Record) information for IRC, HTTP and other non-standard or unique controllers (popular with DDoS botnet families), the feed includes the appropriate SHA1/MD5 malware hashes responsible for infection. This represents a single piece of malware that has been observed to connect to this botnet and helps to trace, triage, and eradicate an internal infection.

WHAT IS AN ‘INACTIVE’ ENTRY?
We pool all the currently known C2 data into this feed from all our different feeds, including HTTP based botnets that we were unable to verify mechanically over the most recent 24 hour period, as they are no longer active for some reason. This serves as a great additional line of defense in the event that these botnets come back online as they occasionally do: there is no delay in reading them, you already have the protection.

WHAT IS THE ‘CONFIDENCE’ ENTRY?
As part of the XML schema for this report, each controller and bot has been assigned a “confidence” value, which is a range of 0-100, with 100 being the highest confidence rating. The data in this feed is derived from one or more methods. The confidence value entry depends on the method of collection and analysis. The intention is that partners determine what issues are most important to them and adapt their policy accordingly. At Team Cymru, we understand that no one can make that determination for you better than you. To facilitate that decision making capability we prefer to give you a confidence value to assist you. You may decide that some threats are important, and others are not. This score will help you along the way.

HOW OFTEN ARE ENTRIES CHECKED?
HTTP based entries are mechanically verified every 60 minutes.

THE CONTROLLER FEED IS AVAILABLE ON AN ANNUAL SUBSCRIPTION BASIS

To get started with the Controller Feed, simply email sales@cymru.com. You can use the PGP key here: https://www.team-cymru.com/About/teammcymru-pgp.txt
An hourly XML feed of every IP address that is part of thousands of botnets we are tracking (controllers and infected clients) plus six further categories of malicious activity.

Along with every Command and Control IP address (C2) for IRC-based, HTTP-based and P2P-based botnets, included is also a full list of IP addresses known to have communicated with the C2 in the last 60 minutes. We also operate a number of sinkhole efforts that contribute additional bot families like Conficker to the feed. Finally, other categories of potentially compromised devices like routers, darknet visitors, and abused proxies are also provided, forming the most comprehensive feed we have ever provided. The Reputation Feed contains botnet controller and infection data from the Botnet Analysis and Reporting System (BARS), a unique system that enables visibility into botnets that normally evade monitoring.

The full Reputation Feed XML Schema is available. All times are UTC.

Near-real time information feed designed to allow subscribers to monitor for infected computers visiting their networks.

- Feed consists of a list of IP addresses exhibiting behavior consistent with infection by malware.
- Subscribers can use to monitor or block these infected hosts.

Entries included that indicate the type of malicious behavior observed:

- **Controller**: IP used to control botnets
- **Bot**: IP was observed talking with a known botnet C&C
- **Darknet**: IP was observed scanning dark IP space for vulnerable hosts
- **Proxy**: IP was observed being used as a proxy to connect to the public Internet
- **Router**: IP is a router that was observed being used as a proxy
- **openresolvers**: IP of a DNS server capable of use in DNS amplification and reflection DDoS attacks
- **bruteforce**: IP seen to be trying to attack authentication services
- **phishing**: IP involved in hosting a malicious phishing page
- **honeypot**: IP seen to be interacting our Honeypot networks
- **spam**: IP engaged in sending spam email

**XML FILE IS GENERATED HOURLY AND INCLUDES A 24-HOUR AGGREGATE VIEW**
FREQUENTLY ASKED QUESTIONS

HOW DO I GET THE REPUTATION FEED?
Partners simply navigate to our Content Delivery Network (CDN) with the credentials we provide.

HOW DO I USE THE REPUTATION FEED?
This is designed to be a lightweight, near-real time feed to allow subscribers to monitor for infected computers visiting their networks. Subscribers can utilize the Reputation Feed to identify compromised hosts as they access their networks, thus enabling them to monitor or block these infected hosts before they can cause any damage. Combine the other categories we include and you have the most complete list possible. Possible uses include:

- Banks checking for infected customers at sign-on
- Companies pro-actively monitoring for exfiltration of data via bots
- ISPs checking for infected customers and other abuse
- Vendors importing data for enterprise appliances

WHERE DO YOU GET THE DATA?
This information is gathered through a number of methods, including malware analysis, observation of botnet command and control (C&C) botnets that we have uniquely decoded, and monitoring of dark IP space (Darknets).

WHAT IS THE ‘CONFIDENCE’ ENTRY?
As part of the XML schema for this report, each controller and bot has been assigned a “confidence” value, which is a range of 0-100, with 100 being the highest confidence rating. The data in this feed is derived from one or more methods.

The confidence value entry depends on the method of collection and analysis. The intention is that partners determine what issues are most important to them and adapt their policy accordingly. At Team Cymru, we understand that no one can make that determination for you better than you. To facilitate that decision making capability we prefer to give you a confidence value to assist you. You may decide that some threats are important, and others are not. This score will help you along the way.

THE REPUTATION FEED IS AVAILABLE ON AN ANNUAL SUBSCRIPTION BASIS
To get started with the Reputation Feed, simply email sales@cymru.com.
You can use the PGP key here: https://www.team-cymru.com/About/teamcymru-pgp.txt
The Botnet Analysis & Reporting Service (BARS) provides in-depth analysis, tracking, and history of malware families that utilize unique control protocols and possibly encryption mechanisms.

We’ve manually decoded and decrypted these control mechanisms and track over 40 different malware families.

We provide the following unique elements as part of our BARS package:

**Infrastructure** to provide automated tracking and reporting of known botnets

**Analysts** focused on investigating new malware families and/or variants

**Developers** writing specialized code to track and report on these new threats

Our data set contains information related to bots including:

- IP
- BGP
- Geolite information related to each bot

**EXAMPLE CATEGORIES INCLUDE**

AldiBot, Alina, Andromeda, ArmageddoN (2 subtypes), Asprox, AZORUlt, BetaBot, Blackenergy (v1.x, v2.x), ColdDeath, Conficker, Corebot, DarkComet, DarkShell (3 subtypes), DDoSer (v3.4x, 3.6x, 4.x), DiamondFox, DirtJumper, DoFoI, Dridex, Drive, Dyreza, Elmer, Ezbro, Godzilla, Gumblar, Hancitor, Illusion, ISRSstealer, JackPOS, Jedobot, Kasidet, Katrina, KeyBase Kronos, Laziok, Locky, LokiBot, Madness, MinerPanel, MyLoader, Neverquest, NewPoS, Nitol (3 subtypes), Nivdort, Optima, Pandora, PonyLoader, Poseidon (2 subtypes), ProxyBack, Quant, Rarog, RedGirl, Shifu, Smokeloader (2 subtypes), Snap, Solar, Stealrat, Storm, TDSS (3 subtypes), Teslacrypt v4.x, Torpig, TreasureHunt, Trickbot, Umbra, Vertexnet, Waledac, YZF, Zeus, Zezin
FREQUENTLY ASKED QUESTIONS

WHAT ARE THE XML SCHEMAS?
The data specification for this project is broken into three separate XML schemas: a Bot schema, a Botnet schema and a DDoS schema, all generated and uploaded hourly.

Bot XML schema – contains information related to hosts infected with malware (bots), including the IP, BGP and GeoIP information related to each Bot. Each infected host is also categorized with the type of malware it is infected with, including additional elements. For example, an entry for a Waledac bot will include a Waledac element, listing the HTTP proxy used by the bot and possible SHA1 signatures for the malware the host is infected with.

Botnet XML schema – contains information related to command and control servers (botnets), including the family, the infected hosts connecting to that botnet, and details regarding the hosts used to control the botnet (if any). The schema also includes the type of botnet, the infected hosts that belong to that botnet, and details about the host(s) being used to control the botnet. We list three different types of botnets: IRC (Internet Relay Chat), HTTP, and P2P (Peer to Peer), each with additional elements. For example, the XML entry for an IRC based botnet may include the IPs, ports, channels and passwords of multiple servers being used to control the botnet.

DDoS XML schema – contains information related to DDoS (distributed denial of service) attacks. Each DDoS element represents a separate attack recorded by our monitoring systems. The target of each attack is provided, along with attack details such as the location of the victim, the time of the attack, the duration, and (when available) details on the nature and strength of the attack.

Each attack is categorized as one of:
- TCP: TCP-based traffic attack
- UDP: UDP-based traffic attack
- ICMP: ICMP-based traffic attack
- SYN: TCP Syn flood attack
- HTTP: HTTP/HTTPS-based resource attack
- DNSamp: DNSamplification attacks (DNS recursion)
- Undetermined: The category could not be determined on available info

HOW DO I GET BARS?
Partners simply navigate to our Content Delivery Network (CDN) with the credentials we provide.

WHAT IS THE REPUTATION SCORE?
As part of the XML schema for this report, each entry has been 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. At Team Cymru, we understand that no one can make that determination for you better than you. To facilitate that decision making capability we prefer to give you a confidence value to assist you. You may decide that some threats are important, and others are not. This score will help you along the way.

Example code and a website to obtain specific score characteristics are both available.

OUR BARS FEED IS AVAILABLE ON AN ANNUAL SUBSCRIPTION BASIS
To get started with BARS, simply email sales@cymru.com.
You can use the PGP key here: https://www.team-cymru.com/About/teamcymru-pgp.txt
GENERAL QUESTIONS

WHERE DO YOU GET THE DATA?
We do collection of various forms all over the world, yielding up to a quarter of a million analyzed malware samples every day and on the order of 3,000 controllers for our botnet feeds at any one time.

WHAT ABOUT REPORTING FALSE POSITIVES?
Suspected false positives can be sent to our support team by emailing support@cymru.com for review and whitelisting as appropriate.

WHAT IS YOUR FALSE POSITIVE RATE?
Our current false positive rate is of the order of one in several tens of millions.

WHAT CAN WE DO WITH THE DATA?
The feeds are designed to assist our partners in protecting their users and cleaning up their networks. We can provide detailed use case scenarios and explain how others typically implement our insight, but you may not use our data in legal proceedings or otherwise cite us as the source of the data.

DON'T YOU GIVE SOME OF THIS DATA AWAY FOR FREE?
We have a strong reputation for donating insight to networks that can use specific insight to prevent or disrupt miscreant activity. However, the data provided in such cases only relates to IP addresses in that specific network’s Autonomous System Number (ASN) and its use is restricted by a data sharing agreement.

The commercial feeds listed here are much larger in that they contain all data for each category (IPs/Domains/MD5s etc.) for all ASNs globally. As such, the data is significantly more actionable for most of our partners and includes commercial terms and service levels.