TEAM CYMRU

Community Services

Tools to help network operators globally

https://team-cymru.com/community-services/

@whois

Samuel Muchiri, smuchiri@cymru.com

Linkedin:in/samuel-nduru-muchiri/

Business Development Rep, Community Services

1.5yrs at Team Cymru

helping communities globally access cyber security tools and services

https://team-cymru.com/community-services/

Team Cymru (pronounced come-ree)

Mission: To Save and Improve Human Lives

Founded 2005

1000s ISP,s Hosting companies globally get free Threat Intelligence

Work with 145+ CSIRT teams in 86+ countries

free tools used; millions of query times per day

https://team-cymru.com/community-services/

Team Cymru’s Other Free Service Solutions

Free Community Services for ASN Owners

- Nimbus Threat Monitor
- BOGON Reference
- Unwanted Traffic Removal Service (UTRS) – DDoS mitigation tool

Free Services for All

- Dragon News Bytes (threat news feed)
- IP to ASN Service
- Malware Hash Registry (MHR)
- Events (UE, Regional Internet Security Events)

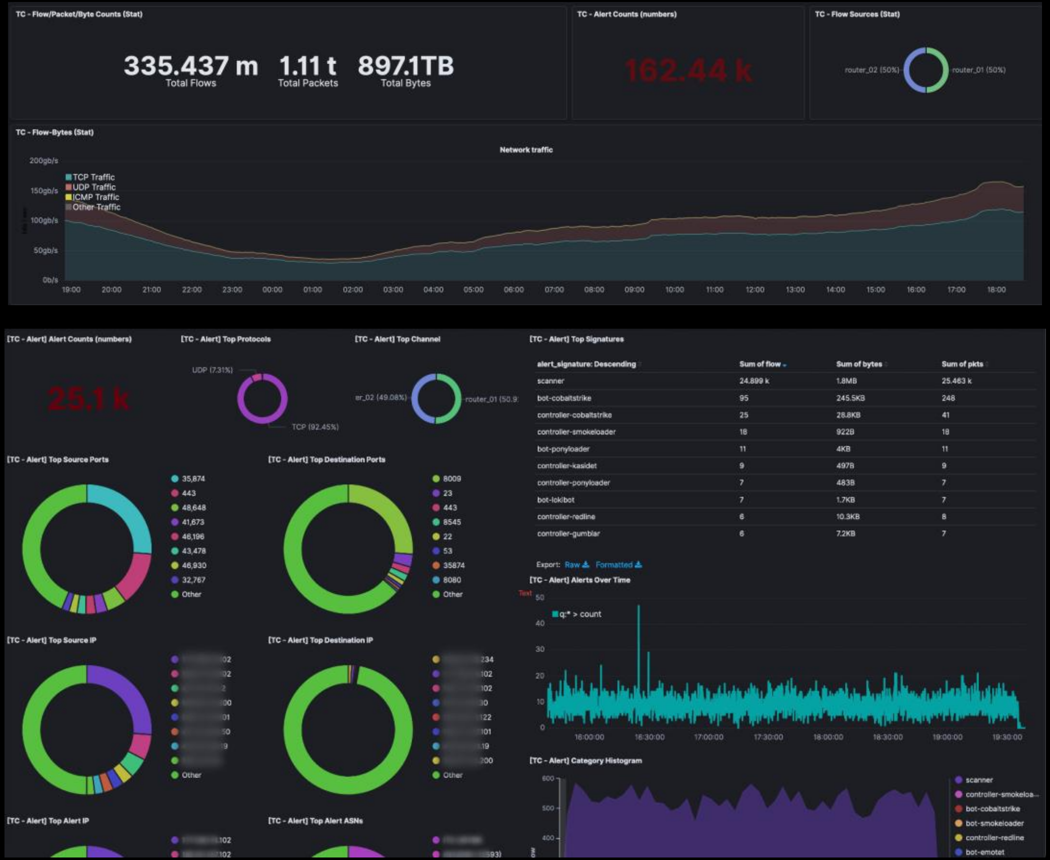
https://team-cymru.com/community-services/

NimbusTM

https://team-cymru.com/community-services/

What is NimbusTM?

- A tool that helps the community improve their network security & contribute to the global effort of securing the internet.
- Cloud-based flow collector, built on Elastic / Kibana.
- Correlates flow data with reputation feed



[TC - Alert] Top Signatures

alert_signature: Descending	Sum of flow	Sum of bytes	Sum of pkts
scanner	24.899 k	1.8MB	25.463 k
bot-cobaltstrike	95	245.5KB	248
controller-cobaltstrike	25	28.8KB	41
controller-smokeloader	18	922B	18
bot-ponyloader	11	4KB	11
controller-kasidet	9	497B	9
controller-ponyloader	7	483B	7
bot-lokibot	7	1.7KB	7
controller-redline	6	10.3KB	8
controller-gumblar	6	7.2KB	7

Export: Raw Formatted

https://team-cymru.com/community-services/nimbus-threat-monitor/

BOGON Reference

https://team-cymru.com/community-services/

What are Bogons?

Bogons are defined as Martians (private and reserved addresses defined by RFC 1918, RFC 5735, and RFC 6598) and netblocks that have not been allocated to a regional internet registry (RIR) by the Internet Assigned Numbers Authority.

https://team-cymru.com/community-services/bogon-reference/

https://team-cymru.com/community-services/

How are the lists managed?

We try to break up the lists into more specific types to allow for more flexibility based on your use case needs.

- Bogons
- Full Bogons
- IPv4
- IPv6

https://team-cymru.com/community-services/

How can I access the Bogon list?

Supported list of formats and methods by which you can receive these updates:

- HTTP
- BGP Peering (Bogon Route Service Project)
- Routing Registries (RADb and RIPE NCC Partnerships)
- DNS

All formats are updated at the same intervals

Our data is based on relevant RFCs, IANA IPV4 allocation list (IPv4 summary page) and RIR data

We constantly monitor for changes and update quickly when changes occur

https://team-cymru.com/community-services/

Based on a study - a frequently attacked website to discover that 60% of the bad packets were obvious bogons (e.g. 127.1.2.3, 0.5.4.3, etc.). Your mileage may vary, and you may opt to filter more conservatively or more liberally. As always, you must KNOW YOUR NETWORK to understand the effects of such filtering.

https://team-cymru.com/community-services/

Malware Hash Registry (MHR)

https://team-cymru.com/community-services/

Malware Hash Registry (MHR) Overview

A free malware validation tool that queries against 30+ undisclosed antivirus databases and plus TC 8+ years Db.

Various collection techniques, such as honeypots and crawlers, as well as leveraging private data-sharing agreements with partners.

Identify new or emerging malware that may not be detected by your existing anti-malware tools

We support MD5, SHA1, and SHA256 hashes

https://team-cymru.com/community-services/

How to use Malware Hash Registry (MHR)

- hash.cymru.com - UI based great for one-off queries
- Whois API - CLI based, great for one-off queries
- Netcat API – CLI based, best for bulk queries
- DNS API – CLI based, great for bulk queries and best performance
- Rest API – great for bulk queries and integrating into work-flows

https://team-cymru.com/community-services/

What is UTRS 2.0 (Unwanted Traffic Removal Service)?

- A **FREE** Community Driven Free DDOS mitigation service
- Similar to Remote Trigger Black Hole (RTBH) except: **Upstream** and **Global**
- Team Cymru validates the request then forwards out to the 1600+ participating networks
- Thanks to our participating partner networks, we effectively reduce the impact of threat actors
- A single BGP announcement to rule them all

https://team-cymru.com/community-services/

UTRS 2.0 Features

Increased IPv4 prefix size and IPv6 support added!

- Increases the prefix size for IPv4 from /32 to IPv4/25
- Added IPv6 support up to a /49

https://team-cymru.com/community-services/

Redundant Route Servers and RPKI Validation

- Support for Geographically diverse networks
- Better peering
- Route efficiency
- RPKI Validation based on Regional Internet Registry (RIR) information

https://team-cymru.com/community-services/

Comparisson of UTRS v1 & UTRS v2

UTRS v1

- IP v4 addresses only
- One router on our side
- BGP support only
- Accepts only /32’s
- Validates based on Global Table

UTRS v2

- IP v4 and IPv6 support
- 2 geographically distinct routers.
- BGP and BGP flowspec support
- Accepts /25’s and /49’s
- Global Table or RPKI ROA’s
  - (mitigation provider friendly)

SAFE

Safe is a service whereby we create an “Exchange ”, where members can provide abuse and fraud related feedback, as well as check for the same

It allows members to both submit information as well as check information. The information gathered includes:

Email

- cc_mumber
- cc_lasr_four
- alt_payment _id
- sign_up_source_ip
- linked_source_ips
- country
- domain_names
- user_agent_strings category
- submitting_provider_id
- submitting_provider_case_id
- submission_timestamp
- notes

Thank You!

outreach@cymru.com