



Community Network tools – All at No-Cost

- To Save and Improve Human Lives as a Community

Sorry, not QUAD7

Team Cymru Community Outreach Team

outreach@cymru.com

Massimiliano Stucchi

Outreach Team

- Recently joined Team Cymru as Data Acquisition specialist
- Prior: Internet Society, RIPE NCC, ISP Founder
- Involved in a number of Programme Committees and conferences
- Team Cymru's Mission: To Save and Improve Human Lives



Mission

BOGONS

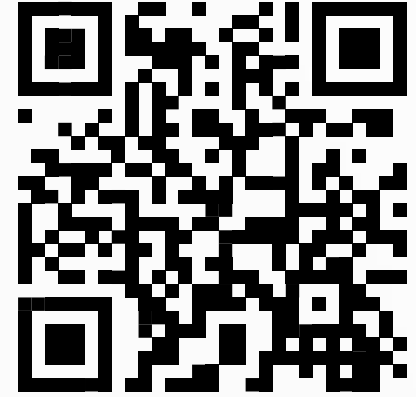
The original list



- BOGON and MARTIAN lists – Updated hourly
- BOGONS: IANA unallocated + RFC reserved space
- FULL BOGONS: adds unassigned by RIRs
- Available over HTTP(s), BGP, RIPE NCC, RADb, DNS
- Most convenient is BGP peering

IP-TO-ASN

BGP-based Whois lookup



- Enter IP addresses or CIDR blocks
- Returns advertising AS
- Yes, sometimes multiple ASNs advertise same IPs
- Delivered over WHOIS, DNS, and HTTPS
- WHOIS is the most popular
- Bulk Mode Available – please use with netcat*

CSIRT Assistance Program (CAP)

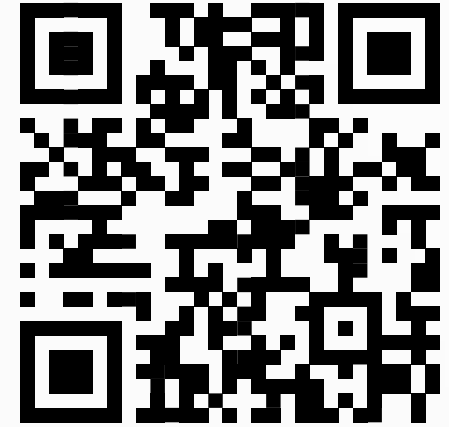
Free service for Government & National CSIRT/CERTs



- IP reputation data
- Regional or National CSIRT & CERT teams
- Contains our filtered set of threat intelligence - specific to “jurisdiction”
- Actionable Intelligence – Assists in Victim Notification

Malware Hash Registry - MHR

Malware Validation



- Malware detection & validation
- Searches against 30+ antivirus databases
- WHOIS, DNS, HTTPS support; HTTPS - hash.cymru.com
- REST API support requires signup
- Built into ZEEK -
<https://docs.zeeq.org/en/current/scripts/policy/frameworks/files/detect-MHR.zeeq.html>

Malware Hash Registry - MHR

Malware Validation



Search Signup Docs ▾

Malware Hash Registry (MHR)

This web form provides a manual interface for checking hashes against our malware data. Type in one or more hashes into the box below, then press "submit" to see if we recognize the hash as malicious.

Max Hash limit: 1000

Submit Reset

Supported Hashes

- MD5
- SHA1
- SHA256

Format

- Hashes can be newline and/or comma-separated
- White space is ignored
- There is a limit of 1000 hashes per-submission

APIs

- DNS
- WHOIS
- REST (requires [signup!](#))

Sample Input

```
1d31bd48b2e864c773ca6a3b9fd0019416809066
22232b5821a1ea9afa2c89bcd87392755e6d643b
30906e3f8bae78f852eb441965a957e68c6c4957
64fd93ef54bbab55b956de71089ee3c4aae852de
36127f11432f4e6cc0df0080da271a1b6060d553
2e9f41ca2846683158cd2e108fe405079910bdd7
436879fe88a928f483c6066434fb7c3c40ce9da2
46c6a243281c2590a0e1499412ba4d3eab38e91f
60765071b09254a3e53c945350edc965be2ff3fe
68ff97056ee6cdb74f9c73717c3ed114de271663
```

Results

Hash: The queried hash, plus its conversion to the other supported hash types, if available.
AV Hit Rate: The percent of anti-virus (AV) engines we tested that detected this hash as malicious.
Last Seen: The last time we ran this hash against our AVs and determined this hash was malicious.
Error: If there was an error searching for this hash's data, it will be displayed here.

Hash	AV Hit Rate	Last Seen	Error
MD5: 02f07327c6e0123c18fd7764e12e015a SHA1: 436879fe88a928f483c6066434fb7c3c40ce9da2 SHA256: -	67%	2013-10-14T02:35:10Z	-

WARNING: Sources that are seen making batch requests to the MHR server with large numbers of individual queries instead of using the available bulk interfaces may be rate limited. Sources issuing an abusively large number of queries may be null routed.

Copyright © 2025 [Team Cymru](#). All Rights Reserved.

DDOS Mitigation

Unwanted Traffic Removal Service - UTRS

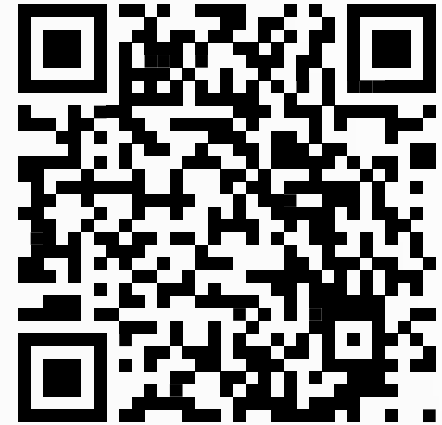
Distributed RTBH

- Like RTBH, but **upstream** and **global**
- BGP based triggers
 - You send an address (/32 or /128) to blackhole
 - You must hold the prefix for the address
 - You agree to blackhole route received prefixes
- Over 750 partner networks
- Reduces unwanted traffic hitting your peers
- Flowspec supported for port-level filtering



ISP Protect / Nimbus

Netflow-based Threat detection for mid-to-large ISPs



- Elasticsearch-based netflow analyzer
- Matches network flows to network reputation insights & CTI context
- Send specialized rules to your SIEM/XDR
- Encrypted flow supported
- Supports all common flow protocols & IPv6
- Over 600 active ASNs partners

ISP Protect! / Nimbus

Netflow Analyzer



Protect!

IX Protect! / VPS Protect!

Multi-tenant Threat Monitor



- Multi-Tenant Threat Monitor
- View high-level context & alerts
- Matches network flows to network reputation insights
- Requires IX to join + each member wanting to contribute
- Bad Actors Variant – Only flows to/from known malicious IPs will be saved
- To opt-in: <https://www.team-cymru.com/ixprotect-signup>

IX Protect! / VPS Protect!

Multi-tenant Threat Monitor



Network Security Intelligence Platform

Q All Issues

Enter IP for details

Q Search IP

Std Queries

15 / 5000

Fresh data

IP Grid Overview

43.241.59.50
malware
vpn → I2tp

27.254.146.12
malware

43.241.56.14
malware

27.254.153.12
malware

27.254.153.51
malware

43.241.56.3
malware

27.254.153.135
malware
vpn → I2tp

27.254.153.17
malware

43.241.56.5
malware
vpn → I2tp

43.241.58.36
malware

IP Information

Filter results...

Export

43.241.59.50

TH

AS: 63940 (DRAGONHISPEED-AS-AP dragonhispeed, TH)

Org: dragonhispeed

Tags: malware

vpn → I2tp

OpenPorts: 443 443 443 80

Issuer: None

Last Seen: 2025-06-24

27.254.146.12

TH

AS: 63940 (DRAGONHISPEED-AS-AP dragonhispeed, TH)

Org: Unknown

Tags: malware

OpenPorts: 443 443 443 443 80

Issuer: None

Last Seen: 2025-06-24

43.241.56.14

TH

AS: 63940 (DRAGONHISPEED-AS-AP dragonhispeed, TH)

Org: Unknown

Tags: malware

OpenPorts: 80 80 2222 443 80

Issuer: None

Last Seen: 2025-06-24

27.254.153.12

TH

AS: 63940 (DRAGONHISPEED-AS-AP

Tags: malware

OpenPorts: 443 443 443 443 2222

Issuer: None

Filter Categories

Malware

Controller (Not Found)

OST (Not Found)

Openresolvers

Team Cymru. Copyright ©2026 All Rights Reserved. | Visit Us At www.team-cymru.com

BPH Protect!

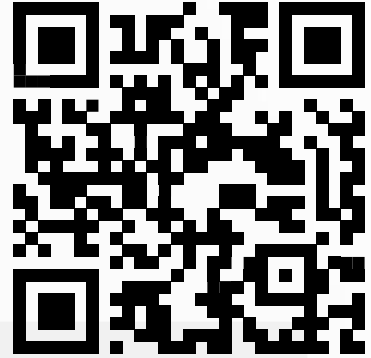
Multi-tenant Threat Monitor



- Bulletproof Hosting Provider Block List
- For hosting providers with hugely poor reputation
- Extremely high confidence block-list
- Only available to community members
- Coming Q3 2026

EVENTS

Flagship Technical Events



Underground Economy

- Annual - 4-Day event
- Building bridges between LEOs and InfoSec Pros
- 20%-35% LEOs, 50% InfoSec Pros, 15% Financial Sector, X% edu + industry
- First full week of September
- Past Co-Hosts: Interpol, Europol, Council of Europe, Qatar MOI, La Caixa Bank, CERT-UK, RoEduNet (Romania)

Regional Internet Security Event - RISE

- 2-Day event – 3 times per year
- Localized version of UE
- Design to build bridges
- 2-300 attendees
- Locations Unique per event
- Past Co-Hosts: KISA, CERT.LV, Tietoevry, Interpol Singapore

THANK YOU!

Questions?

mstucchi@cymru.com
outreach@cymru.com