STORM WATCH

CYBERSECURITY NEWS

Dateline: 2024-05-28

LIKE

SUBSCRIBE

Storm ⚡ Watch by GreyNoise Intelligence

GreyNoise Intelligence

TECHNOLOGY · UPDATED WEEKLY

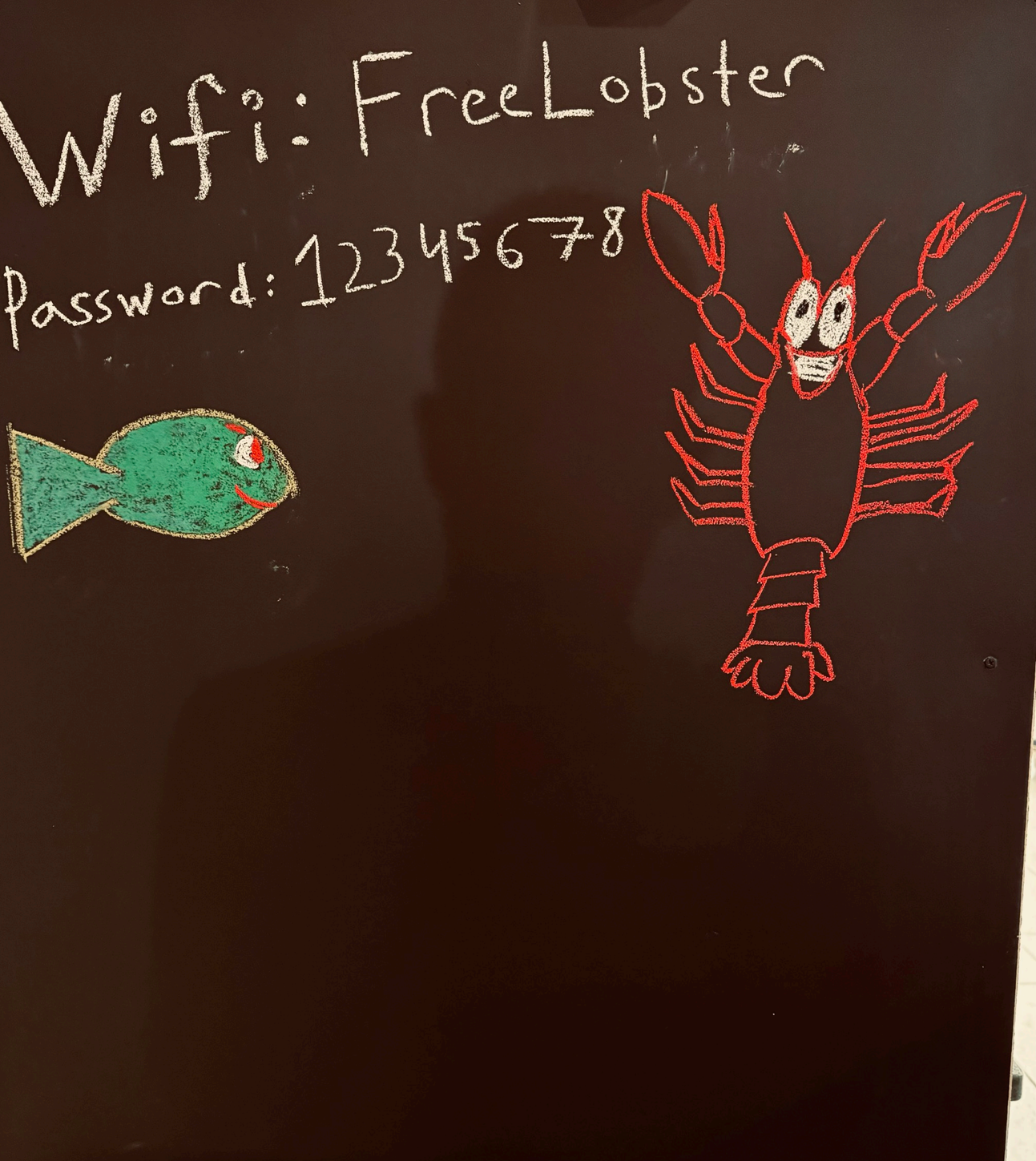
GreyNoise Storm ⚡ Watch is a weekly podcast and livestream hosted by GreyNoise Intelligence (https://www.greynoise.io), a cybersecurity company that focuses on understanding internet noise. The show features hosts b MORE

https://StormWatch.ing

LEAVE A COMMENT

SHARE


L.L. Bean Inc.
90th Anniversary
Bean Boot
For your own safety,
please do not climb
on the boot.


Wifi: FreeLobster
Password: 12345678

https://blog.checkpoint.com/security/enhance-your-vpn-security-posture?campaign=checkpoint&eid=guvrs&advisory=1

SECURITY MAY 27, 2024

Important Security Update – Enhance your VPN Security Posture!

By Check Point Team

Over the past few months, we have observed increased interest of malicious groups in leveraging remote-access VPN environments as an entry point and attack vector into enterprises.

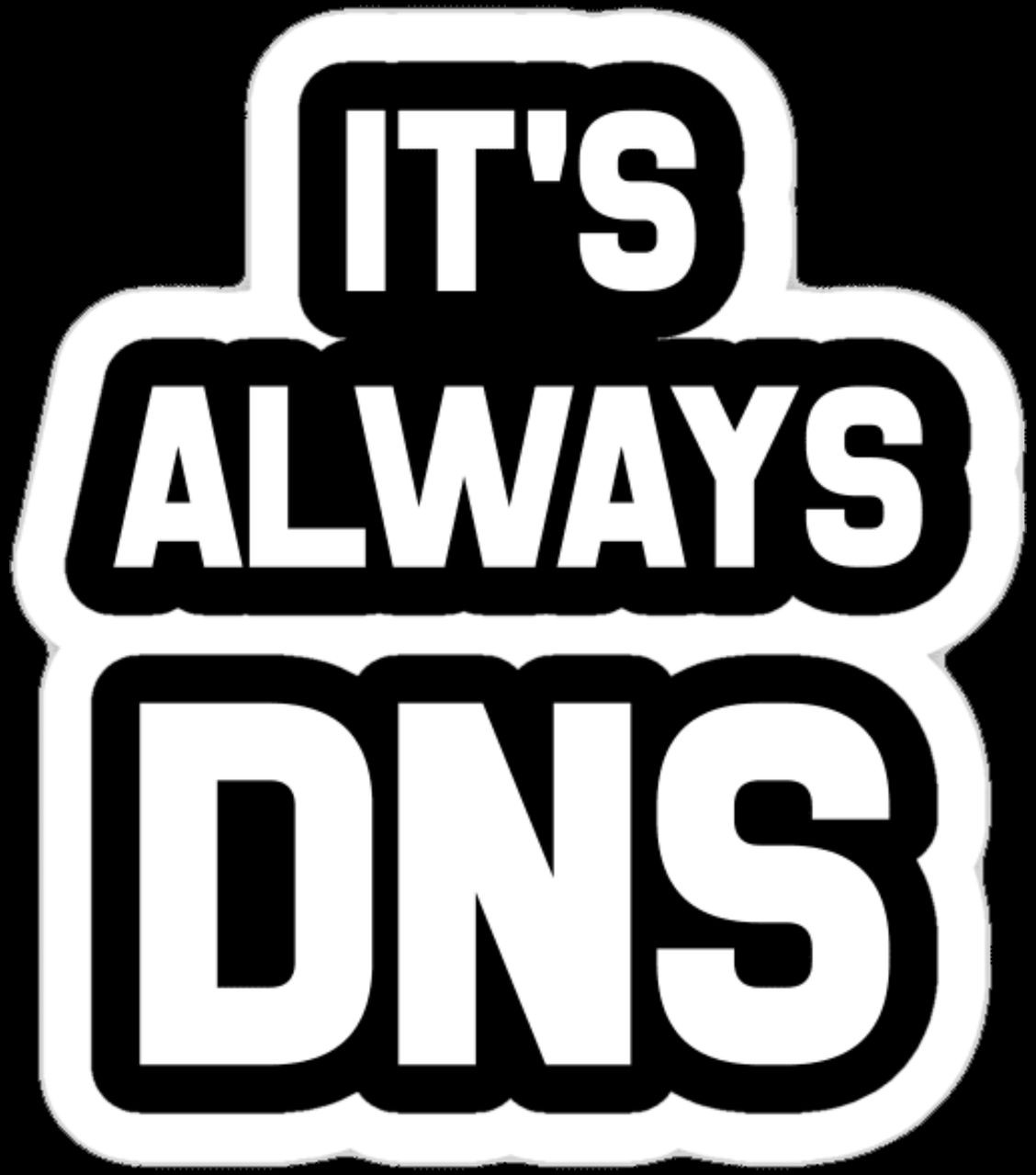
Attackers are motivated to gain access to organizations over remote-access setups so they can try to discover relevant enterprise assets and users, seeking for vulnerabilities in order to gain persistence on key enterprise assets.

We have recently witnessed compromised VPN solutions, including various cyber security vendors. In light of these events, we have been monitoring attempts to gain unauthorized access to VPNs of Check Point's customers.

STORM WATCH

CYBERSECURITY NEWS

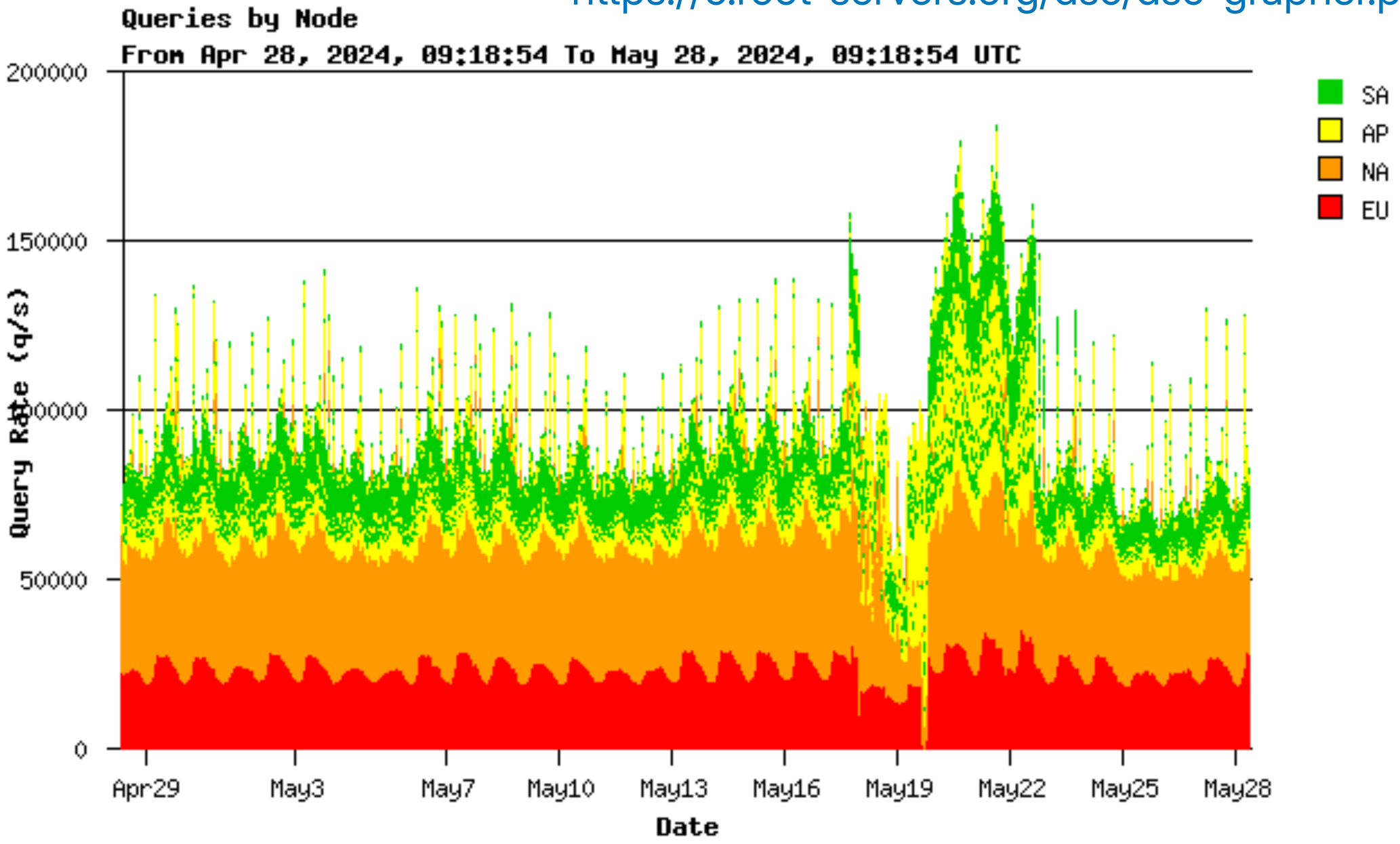
CYBERSIDE CHAT

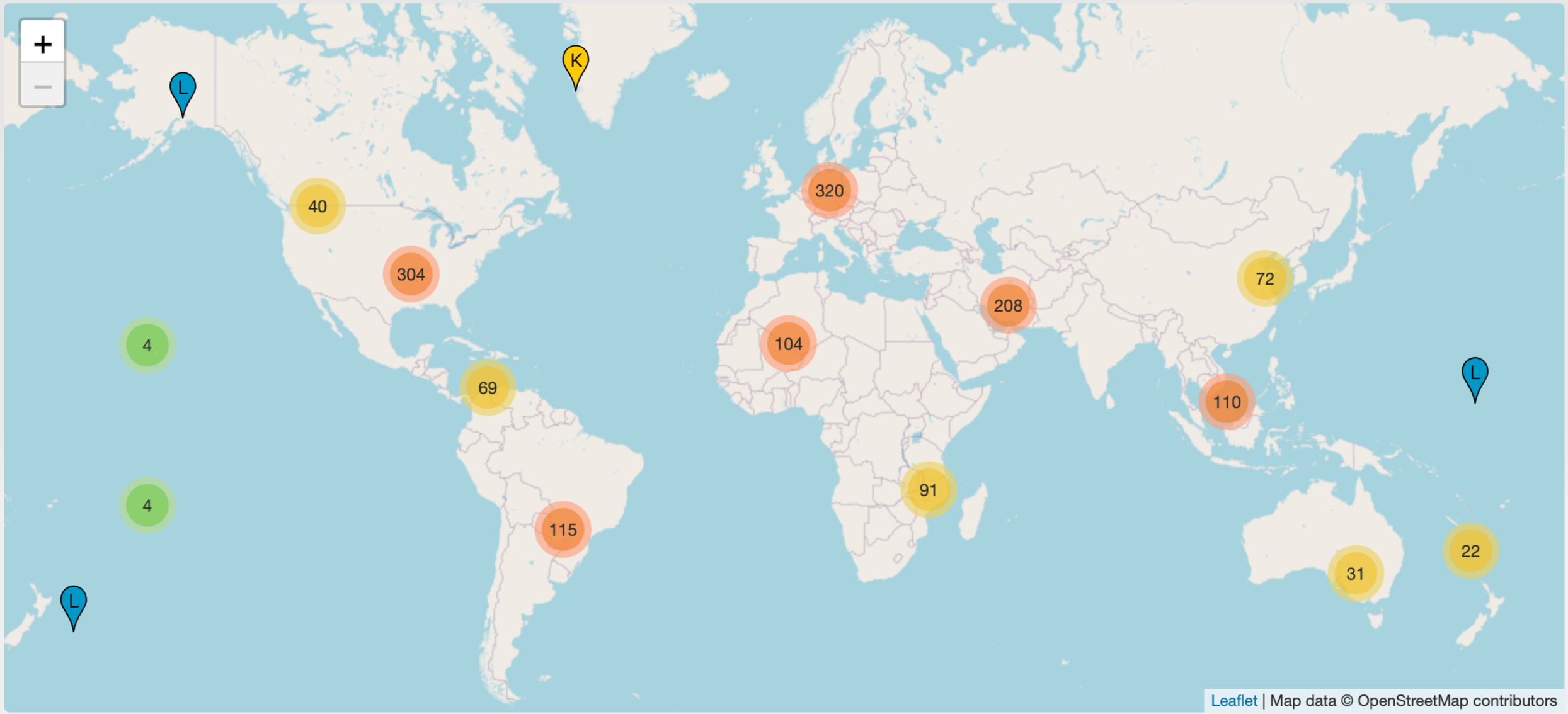

IT'S
ALWAYS
DNS

https://arstechnica.com/security/2024/05/dns-glitch-that-threatened-internet-stability-fixed-cause-remains-unclear/

> On May 21 at 15:30 UTC the c-root team at Cogent Communications was informed that the root zone as served by c-root had ceased to track changes from the root zone publication server after May 18. Analysis showed this to have been caused by an unrelated routing policy change whose side effect was to silence the relevant monitoring systems. No production DNS queries went unanswered by c-root as a result of this outage, and the only impact was on root zone freshness. Root zone freshness as served by c-root was fully restored on May 22 at 16:00 UTC.

https://c.root-servers.org/dsc/dsc-grapher.pl

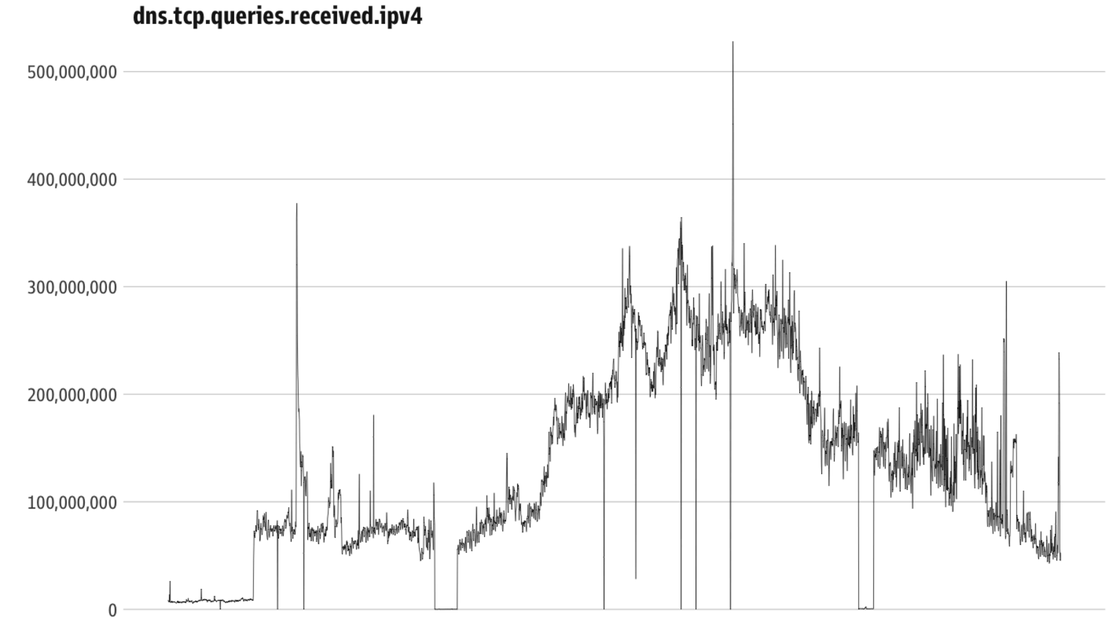


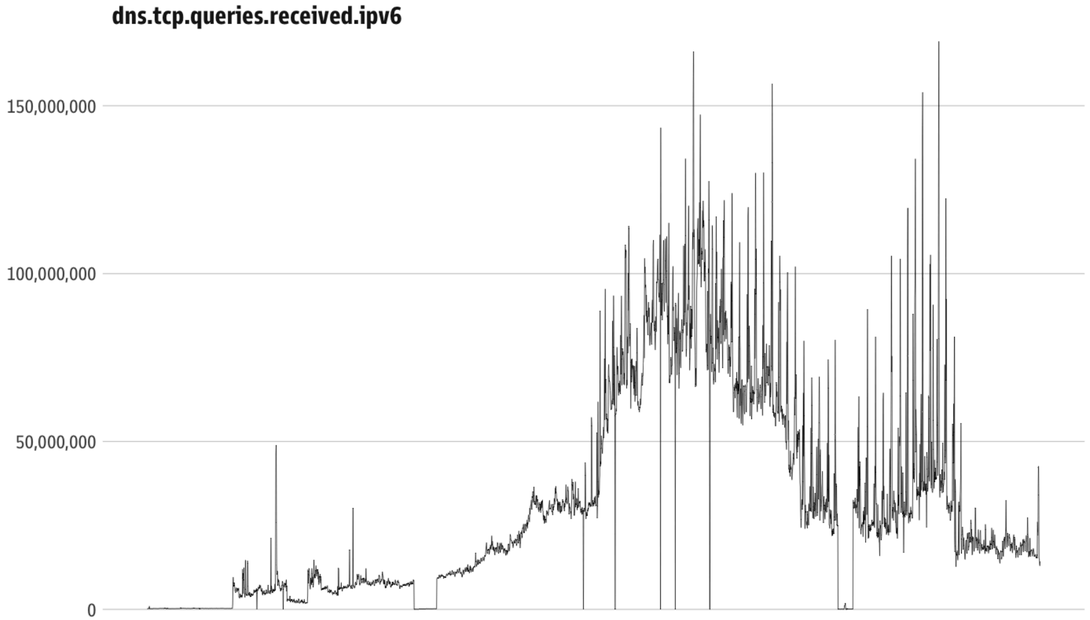


As of 2024-05-28T10:08:28Z, the root server system consists of 1843 instances operated by the 12 independent root server operators.

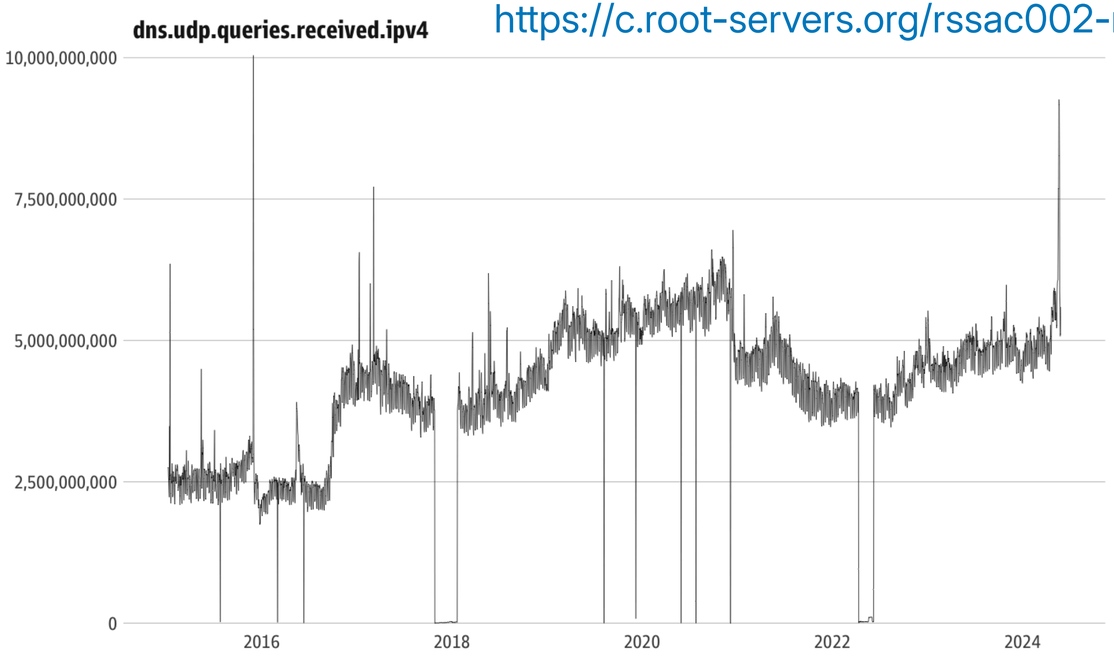

EUROPE
ASIA
AFRICA
SOUTH AMERICA
OCEANIA
Atlantic Ocean
Pacific Ocean
Indian Ocean
Google
Map data ©2018

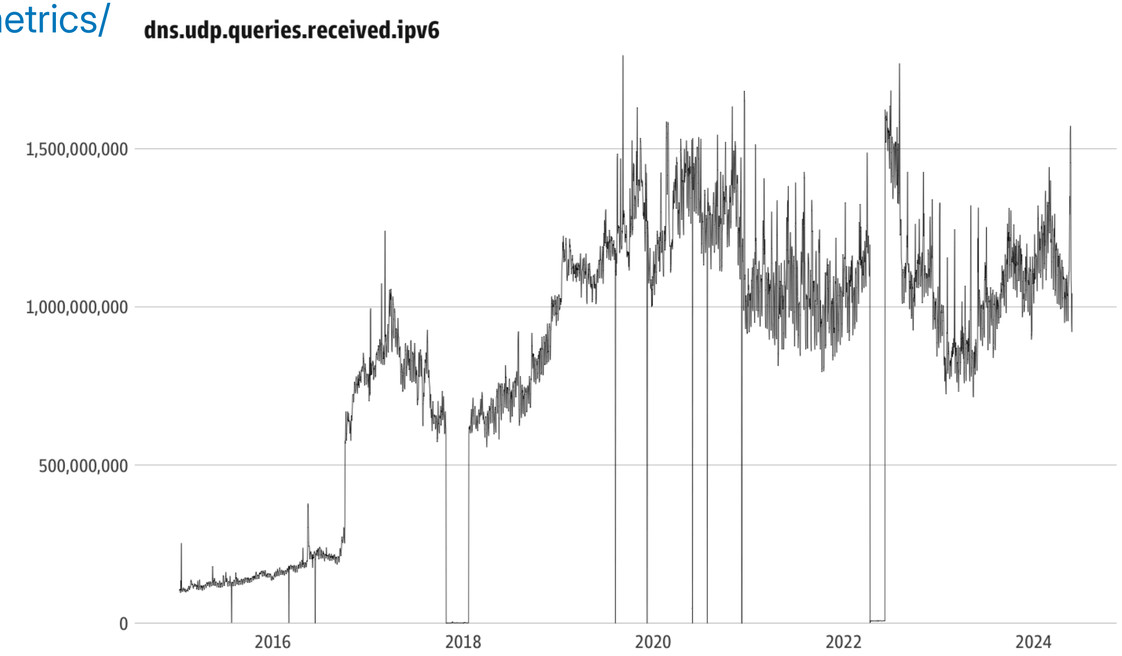
- 1997: C.ROOT-SERVERS.NET was known as C.NYSER.NET
- 1994: C.NYSER.NET became C.PSI.NET
- 2002: Cogent Communications acquired PSINet's major U.S assets, which included responsibility for operation of C.ROOT-SERVERS.NET





https://c.root-servers.org/rssac002-metrics/






You keep using that phrase.
I do not think it means what you think it means.
I run the C root-server!
cogent

The DNS system relies on the synchronization of those 13 root servers to maintain stability. If one server falls out of sync, it can lead to inconsistencies in DNS responses, potentially causing parts of the Internet to become unreachable or misdirected.

Root servers store cryptographic keys used to authenticate DNS responses. If these keys are not identical across all root servers, it increases the risk of DNS cache poisoning attacks, where an attacker could inject malicious data into the DNS cache.

With the c-root server out of sync, attackers could exploit the discrepancy in DNS responses to poison the DNS cache. This involves injecting false DNS records into the cache of a resolver, redirecting users to malicious website.

If the cryptographic keys used in DNSSEC are not properly synchronized, attackers could exploit this to bypass DNSSEC validation, leading to successful DNS spoofing attacks.

2019-08-21 - RFO for zone staleness: at 2019-08-14 1700Z, a configuration change to disable connection tracking of DNS traffic had the harmful side effect of preventing internal synchronization of the root zone to all C-root anycast nodes.

At 2019-08-17 0021Z, the staleness problem was corrected, and also, the internal monitoring which should have detected this staleness problem was corrected.

This was not an attack, and all queries heard by c-root were answered.

STORM WATCH

CYBERSECURITY NEWS

CYBER SPOTLIGHT

vmw  re®

- https://medium.com/mitre-engenuity
  - /infiltrating-defenses-abusing-vmware-in-mitres-cyber-intrusion-4ea647b83f5b
  - /technical-deep-dive-understanding-the-anatomy-of-a-cyber-intrusion-080bddc679f3
  - /advanced-cyber-threats-impact-even-the-most-prepared-56444e980dc8

File Edit Layout View Help

PROPERTIES

Name

MITRE NERVE

Description

A nation-state actor intrusion starting in Jan 2024. © 2024 MITRE Engenuity. Approved for public release. Document number CT0121.

Author

Center for Threat-Informed Defense

Scope

Incident

External References

MITRE Engenuity

Add

PROBLEMS

https://center-for-threat-informed-defense.github.io/attack-flow/ui/?src=../corpus/MITRE NERVE.afb

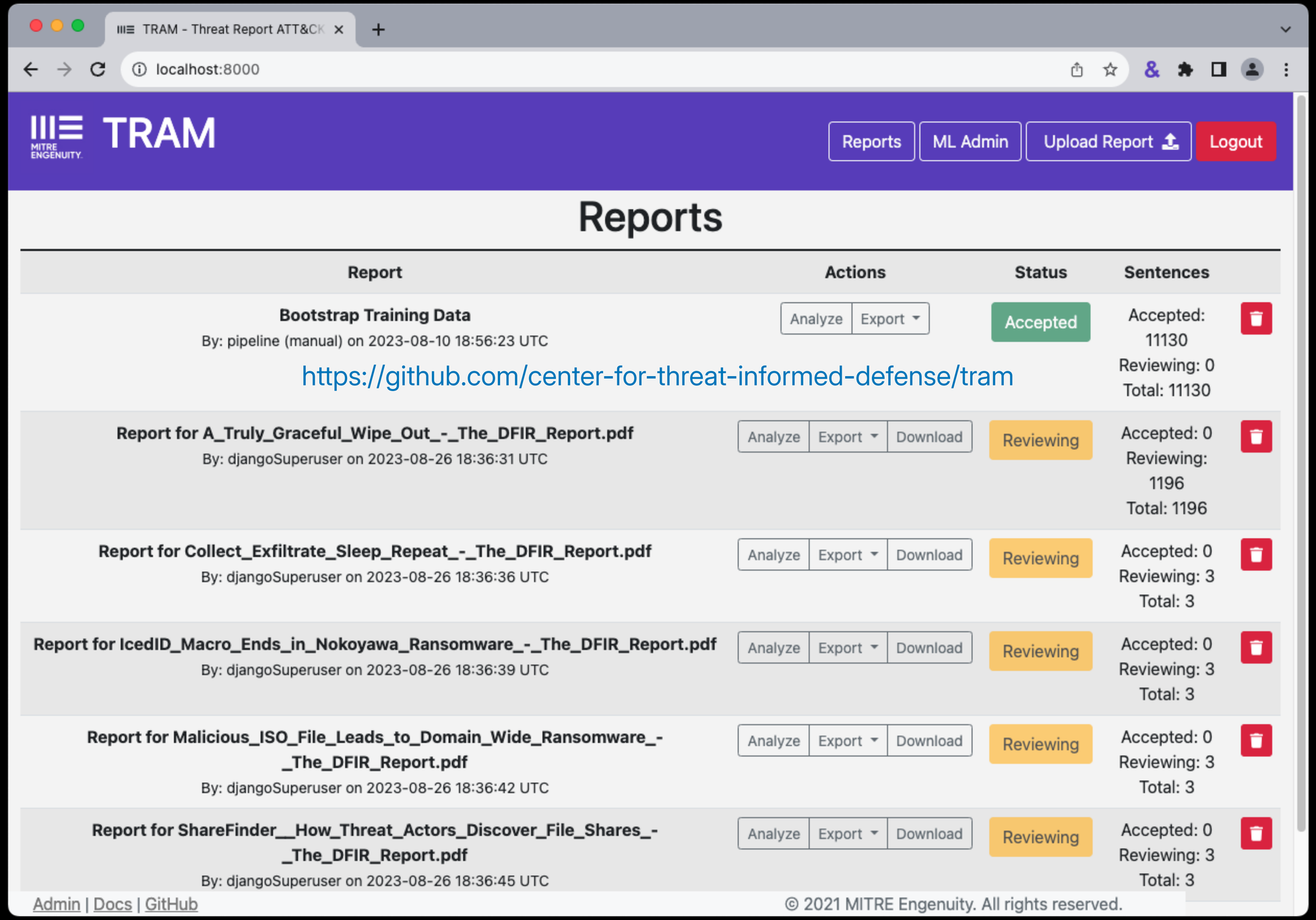
Starting in January 2024, a threat actor performed reconnaissance of our networks, exploited one of our Virtual Private Networks (VPNs) through two Ivanti Connect Secure zero-day vulnerabilities, and skirted past our multi-factor authentication using session hijacking. From there, they moved laterally and dug deep into our network's VMware infrastructure using a compromised administrator account. They employed a combination of sophisticated backdoors and webshells to maintain persistence and harvest credentials.

The adversary created their own rogue VMs within the VMware environment, leveraging compromised vCenter Server access. They wrote and deployed a JSP web shell (**BEEFLUSH**) under the vCenter Server's Tomcat server to execute a Python-based tunneling tool, facilitating SSH connections between adversary-created VMs and the ESXi hypervisor infrastructure.

Bee Flu! SHHHH!!

STORM WATCH

CYBERSECURITY NEWS


TRAM - Threat Report ATT&CK
localhost:8000
TRAM
MITRE ENGENUITY
Reports
ML Admin
Upload Report
Logout
Reports
Report
Actions
Status
Sentences
Bootstrap Training Data
By: pipeline (manual) on 2023-08-10 18:56:23 UTC
Analyze
Export
Accepted
Accepted: 11130
Reviewing: 0
Total: 11130
https://github.com/center-for-threat-informed-defense/tram
Report for A_Truly_Graceful_Wipe_Out_-_The_DFIR_Report.pdf
By: djangoSuperuser on 2023-08-26 18:36:31 UTC
Analyze
Export
Download
Reviewing
Accepted: 0
Reviewing: 1196
Total: 1196
Report for Collect_Exfiltrate_Sleep_Repeat_-_The_DFIR_Report.pdf
By: djangoSuperuser on 2023-08-26 18:36:36 UTC
Analyze
Export
Download
Reviewing
Accepted: 0
Reviewing: 3
Total: 3
Report for IcedID_Macro_Ends_in_Nokoyawa_Ransomware_-_The_DFIR_Report.pdf
By: djangoSuperuser on 2023-08-26 18:36:39 UTC
Analyze
Export
Download
Reviewing
Accepted: 0
Reviewing: 3
Total: 3
Report for Malicious_ISO_File_Leads_to_Domain_Wide_Ransomware_-_The_DFIR_Report.pdf
By: djangoSuperuser on 2023-08-26 18:36:42 UTC
Analyze
Export
Download
Reviewing
Accepted: 0
Reviewing: 3
Total: 3
Report for ShareFinder__How_Threat_Actors_Discover_File_Shares_-_The_DFIR_Report.pdf
By: djangoSuperuser on 2023-08-26 18:36:45 UTC
Analyze
Export
Download
Reviewing
Accepted: 0
Reviewing: 3
Total: 3
Admin | Docs | GitHub
© 2021 MITRE Engenuity. All rights reserved.

https://github.com/center-for-threat-informed-defense/tram

Methodology and toolset for creating the annotations required for machine learning.

Open-source, annotated dataset that covers 50 ATT&CK techniques.

Pre-trained Large Language Model (LLM) for labeling ATT&CK techniques found in human-readable CTI reports.

Web application for running reports through the machine learning model and viewing the results.

STORM WATCH

CYBERSECURITY NEWS

SHAMELESS SELF-PROMOTION

censys

Products Solutions Federal Resources Company Search Now

https://censys.com/cve-2023-43208/

BLOGS

May 22, 2024: Active Exploitation of Healthcare Platform NextGen Mirth Connect RCE (CVE-2023-43208)

https://info.greynoise.io/webinar/ai-for-cybersecurity

WEBINAR

AI for Cybersecurity: Sifting the Noise

Thursday, May 30th, 1:00pm CT / 2:00pm ET

STORM WATCH

CYBERSECURITY NEWS

TAG ROUND-UP

Fluent Bit CVE-2024-4323 Memory Corruption Attempt

Confluence Data Center and Server RCE CVE-2024-21683 Attempt

POSSIBLE BAD RABBIT/PETYA WEBDAV /ADMIN$ INFORMATION DISCLOSURE ATTEMPT

INTENTION
UNKNOWN

CATEGORY
Activity

CVES
No associated CVEs

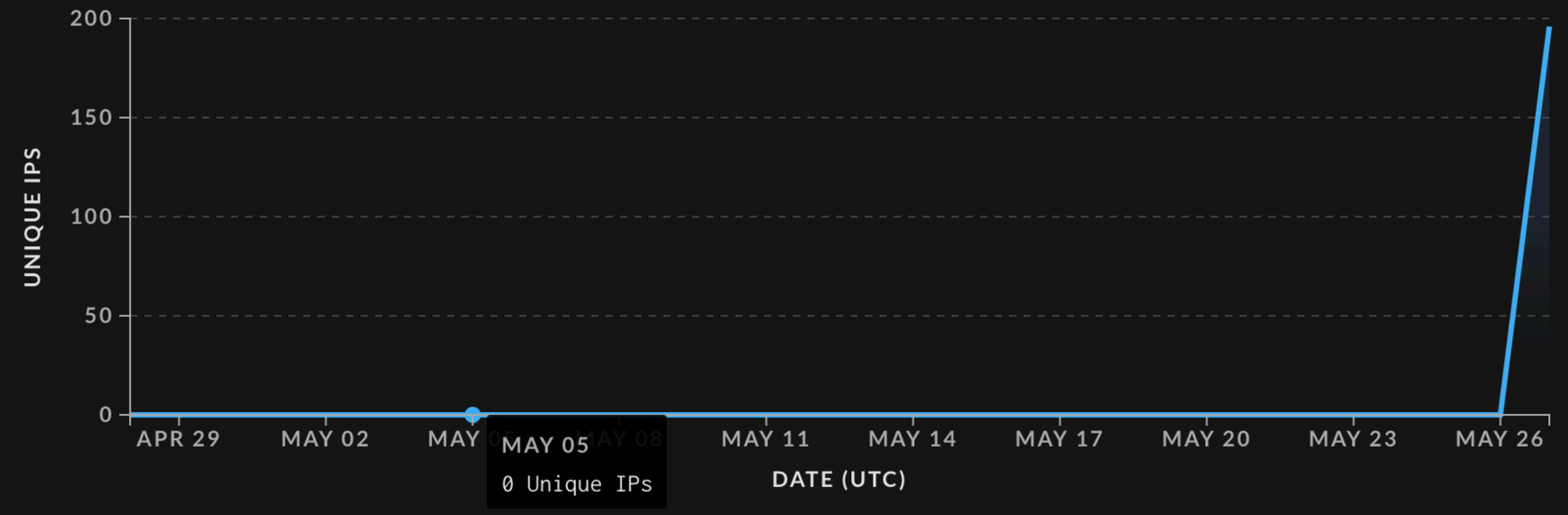
IP addresses with this tag have been observed attempting to locate and enumerate the properties of the resource or collection located at the WebDAV /admin$ path. This activity is known to have been associated with Petya and Bad Rabbit campaigns.

24 HOURS | 10 DAYS | •30 DAYS | April 28, 2024 - May 27, 2024 (UTC)

https://viz.greynoise.io/tags/possible-bad-rabbit-petya-webdav-admin-information-disclosure-attempt?days=30

Unique IPs Observed

Last 30 days



Timeline

Sequence of recorded events

GreyNoise Created Tag 2023-11-30 00:00 UTC

1,089
Observed IPs →

- Export IPs
- Create alert
- View integrations
- Block at firewall

Related Tags:

No related tags

References:

- https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/petya-from-the-wire-detection-using-idps/
- https://www.fortinet.com/blog/threat-research/tracking-the-bad-rabbit
- https://www.pwc.com/vn/en/assurance/assets/pwc-petya-strategic-report.pdf

[+] SHOW 1 MORE

WE NEED

TO TALK

ABOUT

KEV

STORM WATCH

It Has Been

5

Days Since The Last KEV Release

https://kev.hrbrmstr.app

CVE-2020-17519: Apache Flink Improper Access Control Vulnerability

GreyNoise Trends

APACHE FLINK PATH TRAVERSAL

https://viz.greynoise.io/tags/apache-flink-path-traversal-attempt?days=30

INTENTION
MALICIOUS

CATEGORY
Activity

CVES
CVE-2020-17519

IP addresses with this tag have been observed attempting to use CVE-2020-17519, a path traversal vulnerability in Apache Flink that could enable arbitrary file retrieval.

4,189
Observed IPs →

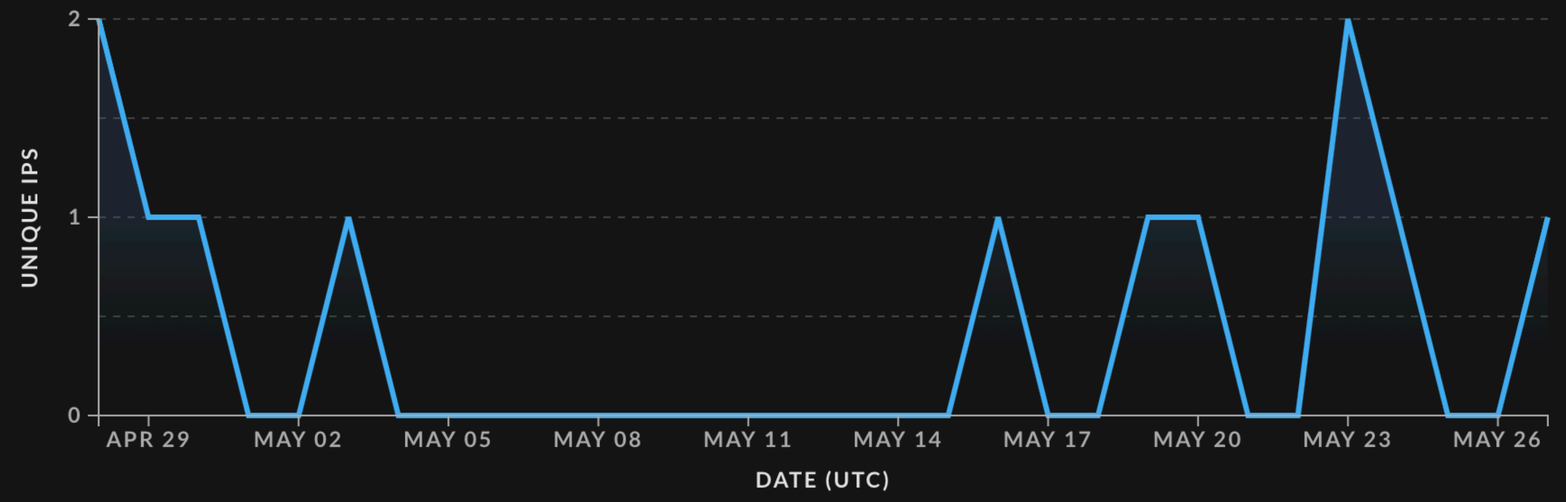
- Export IPs
- Create alert
- View integrations
- Block at firewall

24 HOURS | 10 DAYS | •30 DAYS

April 28, 2024 - May 27, 2024 (UTC)

Unique IPs Observed

Last 30 days



Timeline

Sequence of recorded events

- GreyNoise Created Tag — 2021-02-19 00:00 UTC
- CVE-2020-17519 Published — 2021-01-05 12:15 UTC

Related Tags:

No related tags

References:

- https://nvd.nist.gov/vuln/detail/CVE-2020-17519
- https://github.com/apache/flink/commit/b561010b0ee741543c3953306037f00d7a9f0801
- https://github.com/B1anda0/CVE-2020-17519/blob/main/CVE-2020-17519.py