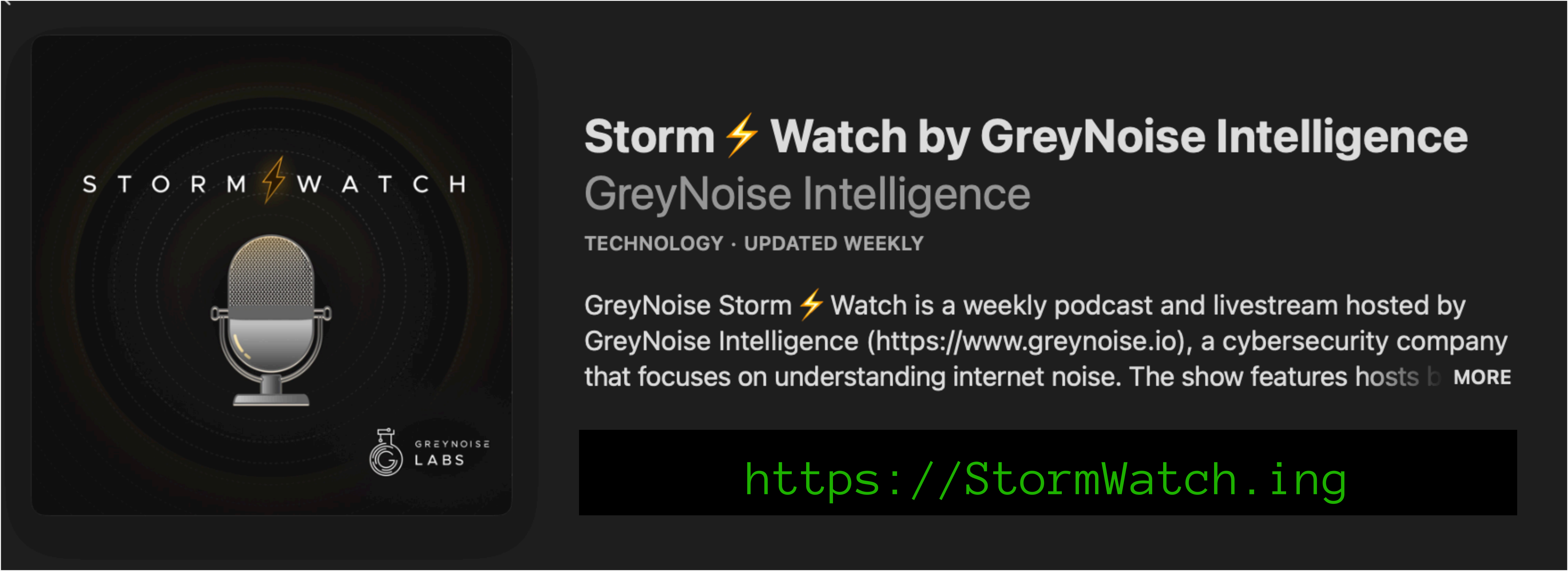
STORMWATCH

CYBERSECURITY NEWS

Dateline: 2024-03-26

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

Professor Ross Anderson, FRS, FREng

Our dear friend and treasured long term campaigner for privacy and security, Professor of Security Engineering at Cambridge University and Edinburgh University, Lovelace Medal winner, died suddenly at the family home in Cambridge overnight.

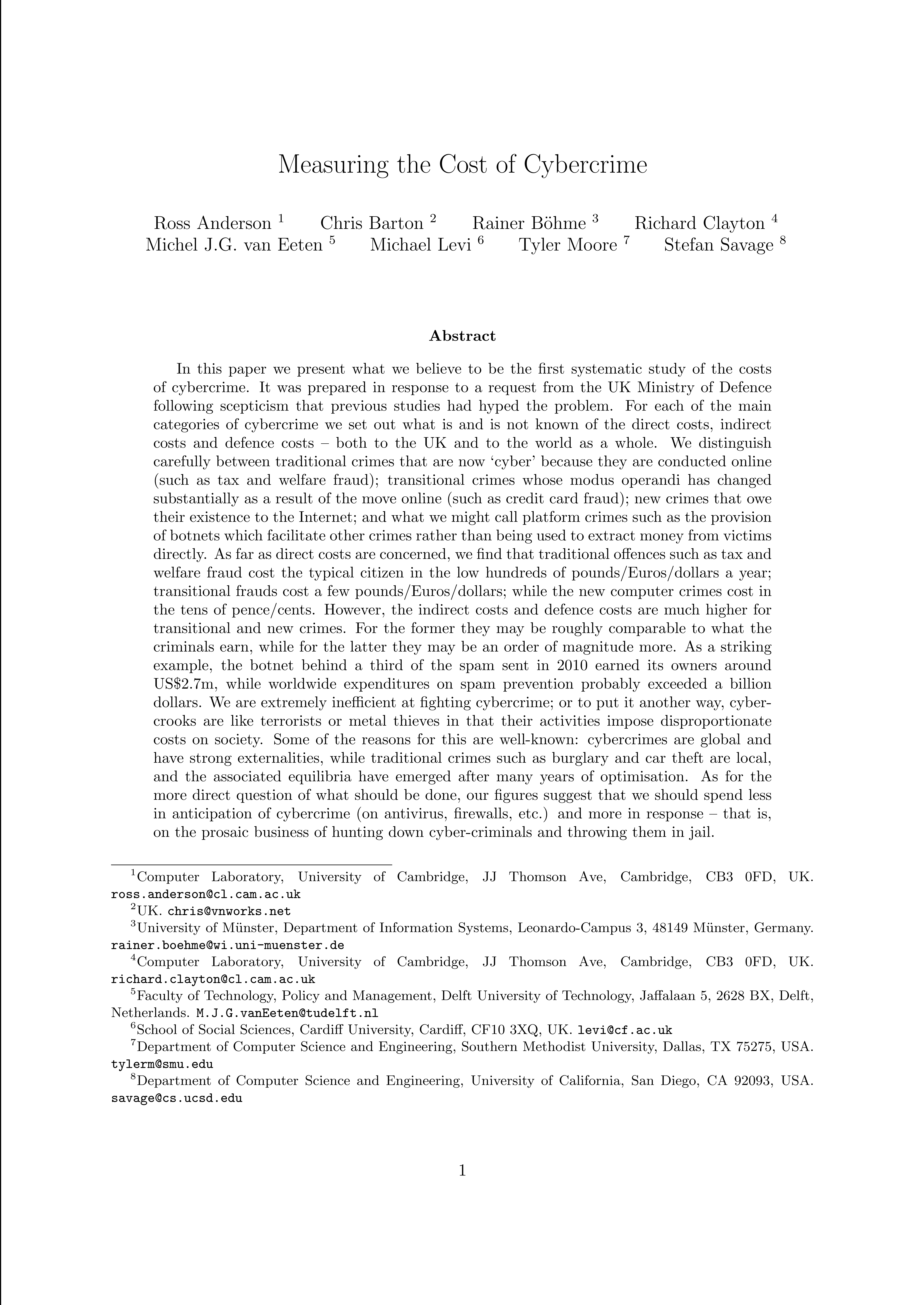
Duncan Campbell

15 September 1956 – 28 March 2024

Professor of Security Engineering at the University of Cambridge, Department of Computer Science and Technology

Bachelor of Arts in mathematics and natural science, University of Cambridge; PhD in Computer Engineering

Awarded the Lovelace Medal (2015)



Measuring the Cost of Cybercrime

Ross Anderson [1] Chris Barton [2] Rainer Böhme [3] Richard Clayton [4]
Michel J.G. van Eeten [5] Michael Levi [6] Tyler Moore [7] Stefan Savage [8]

Abstract

In this paper we present what we believe to be the first systematic study of the costs of cybercrime. It was prepared in response to a request from the UK Ministry of Defence following scepticism that previous studies had hyped the problem. For each of the main categories of cybercrime we set out what is and is not known of the direct costs, indirect costs and defence costs – both to the UK and to the world as a whole. We distinguish carefully between traditional crimes that are now 'cyber' because they are conducted online (such as tax and welfare fraud); transitional crimes whose modus operandi has changed substantially as a result of the move online (such as credit card fraud); new crimes that owe their existence to the Internet; and what we might call platform crimes such as the provision of botnets which facilitate other crimes rather than being used to extract money from victims directly. As far as direct costs are concerned, we find that traditional offences such as tax and welfare fraud cost the typical citizen in the low hundreds of pounds/Euros/dollars a year; transitional frauds cost a few pounds/Euros/dollars; while the new computer crimes cost in the tens of pence/cents. However, the indirect costs and defence costs are much higher for transitional and new crimes. For the former they may be roughly comparable to what the criminals earn, while for the latter they may be an order of magnitude more. As a striking example, the botnet behind a third of the spam sent in 2010 earned its owners around US$2.7m, while worldwide expenditures on spam prevention probably exceeded a billion dollars. We are extremely inefficient at fighting cybercrime; or to put it another way, cyber-crooks are like terrorists or metal thieves in that their activities impose disproportionate costs on society. Some of the reasons for this are well-known: cybercrimes are global and have strong externalities, while traditional crimes such as burglary and car theft are local, and the associated equilibria have emerged after many years of optimisation. As for the more direct question of what should be done, our figures suggest that we should spend less in anticipation of cybercrime (on antivirus, firewalls, etc.) and more in response – that is, on the prosaic business of hunting down cyber-criminals and throwing them in jail.

[1] Computer Laboratory, University of Cambridge, JJ Thomson Ave, Cambridge, CB3 0FD, UK. ross.anderson@cl.cam.ac.uk

[2] UK. chris@vnworks.net

[3] University of Münster, Department of Information Systems, Leonardo-Campus 3, 48149 Münster, Germany. rainer.boehme@wi.uni-muenster.de

[4] Computer Laboratory, University of Cambridge, JJ Thomson Ave, Cambridge, CB3 0FD, UK. richard.clayton@cl.cam.ac.uk

[5] Faculty of Technology, Policy and Management, Delft University of Technology, Jaffalaan 5, 2628 BX, Delft, Netherlands. M.J.G.vanEeten@tudelft.nl

[6] School of Social Sciences, Cardiff University, Cardiff, CF10 3XQ, UK. levi@cf.ac.uk

[7] Department of Computer Science and Engineering, Southern Methodist University, Dallas, TX 75275, USA. tylerm@smu.edu

[8] Department of Computer Science and Engineering, University of California, San Diego, CA 92093, USA. savage@cs.ucsd.edu

https://econinfosec.org/archive/weis2012/papers/Anderson_WEIS2012.pdf

STORMWATCH

CYBERSECURITY NEWS

CYBERSIDE CHAT

👻 🔥

HORIZON3.ai
~~TRUST~~ BUT VERIFY
SOLUTIONS
NEW
PCI PENTESTING
ATTACK RESEARCH
RESOURCES
COMPANY
LOG IN

Attack Path

These are the steps NodeZero took, the assets it found, and the weaknesses it exploited to reach the target.

0:00:00
0:00:46
0:01:24
0:07:37
0:18:18
0:18:46
0:21:52
NodeZero
10.0.222.200
Found Host
Domain Controller
10.0.4.2
dc02.pod04.h3airange.internal
Found Service
SMB Service
10.0.4.2 : 445
dc02.pod04.h3airange.internal
Found Host
10.0.4.4
svr01.pod04.h3airange.internal
Found Service
Java Service
10.0.4.4 : 1099
svr01.pod04.h3airange.internal
PROOF
Exploited Weakness
H3-2020-0022
Insecure Java JMX
10.0.4.4 : 1099
HOST COMPROMISE
Loaded RAT
Remote Access Tool
Running as administrator
10.0.4.4
PROOF
Exploited Weakness
H3-2021-0042
SAM Dump
10.0.4.4
Discovered Credential
NTLM Hash
cbr-user
PROOF
Compromised Credential
Domain Admin
cbr-user
POD04.H3AIRANGE.INTERNAL
DOMAIN COMPROMISE
DOMAIN USER COMPROMISE

In this autonomous pentest attack path, NodeZero exploited two weaknesses — a Java JMX misconfiguration and SAM credential dumping — to achieve domain compromise.

Learn More →

Continuously find, fix, and verify your exploitable attack surface

The NodeZero^{TM} platform empowers you to reduce your security risk and continuously improve your security posture

- Autonomously reveals proven attack paths in your network
- Prioritizes and details the fixes you should make immediately
- Shows you how these weaknesses impact your organization
- Enables quick and ongoing verification that your fixes are effective

https://www.horizon3.ai/

https://www.horizon3.ai/nodezero/

NodeZero™
Pentests
External Assets
Runners
Go to Legacy Portal
Horizon 3 AI inc

ATK daily smoke test

Impacts 540 | Weaknesses 507 | Credentials 479 | AD Password Audit 71 | Data 125 | Hosts 105 | Subdomains 45 | Services 1.4K | URLs 158 | Certificates 72 | Users 300 | Compare

ATTACK PATHS
540

IMPACT TYPES
7

ATTACK PATHS BY IMPACT TYPE

Domain Compromise	21
Critical Infrastructure Compromise	36
Host Compromise	318
AWS User Role Compromise	6
Domain User Compromise	28

ATTACK PATHS BY WEAKNESS

Insecure Java JMX @10.0.4.4 : 1099	197
SAM Dump @10.0.4.4	148
LLMNR Poisoning Poss... @10.0.222.51	60
Cracked Creds @a-jsmith	58
SAM Dump @10.0.229.6	57

ATTACK PATHS BY CREDENTIAL

a-jsmith @SMOKE	58
administrator @10.0.220.53	47
administrator @10.0.220.54	39
a-jsmith @SMOKE.NET	34
win10$ @SMOKE.NET	32

ATTACK PATHS BY HOST

10.0.4.4	209
10.0.229.2	144
10.0.229.6	100
10.0.4.2	78
10.0.222.51	60

Search

SCORE	NAME	TYPE	WEAKNESSES	CREDENTIALS	HOSTS	TIME TO COMPROMISE
10 CRITICAL	Domain Admin administrator in domain SMOKE.NET	Domain Compromise	Insecure Java JMX LSASS Dump	administrator@SMOKE.NET	10.0.4.4 10.0.229.2	1h 12m 4s
10 CRITICAL	Windows Print Spooler Remote Code Execution Vulnerability (CVE-2021-34527) found on Domain Controller 10.0.4.1 (dc01.pod04.h3airange.internal)	Domain Compromise	PrintNightmare Insecure Java JMX LSASS Dump	svr01$@POD04.H3AIRANGE.INTERNAL	10.0.4.1 10.0.4.2 10.0.4.4	23m 37s
10 CRITICAL	Windows SMB Remote Code Execution Vulnerability (CVE-2017-0144) found on Domain Controller 10.0.229.2 (dc2.smoke.net)	Domain Compromise	EternalBlue		10.0.229.2	46m 46s
10 CRITICAL	Microsoft Windows Active Directory Certificate Services (ADCS) Privilege Escalation via User Specified Machine Account DNSHostName (CVE-2022-26923) affecting application Microsoft Active Directory Certificate Services on Domain Controller 10.0.229.2 (dc2.smoke.net)	Domain Compromise	Certifried Insecure Java JMX Cred Reuse	win10$@SMOKE.NET jsmith@SMOKE.NET administrator@10.0.220.53	10.0.4.4 10.0.220.53 10.0.229.1	1h 36m 32s
10 CRITICAL	Domain Admin Administrator in domain SMOKE.NET	Domain Compromise	ServiceDesk+ RCE SAM Dump Shared Local and Domain Cred	Administrator@SMOKE.NET	10.0.229.2 10.0.229.6	1h 44m 21s
10 CRITICAL	Windows Print Spooler Remote Code Execution Vulnerability (CVE-2021-34527) found on Domain Controller 10.0.4.2 (dc02.pod04.h3airange.internal)	Domain Compromise	PrintNightmare Cracked Creds LLMNR Poisoning Possible	a-jsmith@SMOKE a-jsmith@POD04.H3AIRANGE.INTERNAL	10.0.4.2 10.0.222.51	23m 51s
10 CRITICAL	Windows SMB Remote Code Execution Vulnerability (CVE-2017-0144) found on Domain Controller 10.0.4.2 (dc02.pod04.h3airange.internal)	Domain Compromise	EternalBlue		10.0.4.2	3m 44s

https://www.horizon3.ai/downloads/research/elevate-your-cybersecurity-strategy-download-the-2023-year-in-review/

HORIZON3.ai
~~TRUST BUT~~ VERIFY

2023 YEAR IN REVIEW

Proactive Cybersecurity **Unleashed**

Observations of the Challenges
Organizations Continue to Face

STORMWATCH

CYBERSECURITY NEWS

CYBER SPOTLIGHT

TECH

Sanctions on APT31 Hackers

The United States Treasury Department has imposed sanctions on individuals and entities linked to the Chinese state-sponsored hacking group known as APT31. This group has been implicated in a series of cyberattacks targeting U.S. critical infrastructure sectors, including defense, aerospace, and energy. The sanctions specifically target a front company for the Ministry of State Security (MSS), and two Chinese nationals, for their roles in these campaigns. The sanctions are part of a collaborative effort with the U.S. Department of Justice, Federal Bureau of Investigation (FBI), Department of State, and the United Kingdom Foreign, Commonwealth & Development Office (FCDO).

Homework

- https://home.treasury.gov/news/press-releases/jy2205
- https://www.securityweek.com/us-treasury-slaps-sanctions-on-china-linked-apt31-hackers/
- https://www.theguardian.com/technology/2024/mar/25/us-sanctions-chinese-hackers
- https://therecord.media/us-sanctions-chinese-hackers-infrastructure-attacks
- https://www.reuters.com/technology/cybersecurity
- https://nymag.com/intelligencer/article/big-tech-still-has-a-big-addiction-to-china.html
- https://www.aljazeera.com/news/2024/3/25/
- https://www.voanews.com/a/us-uk-bring-charges-sanctions-in-response-to-chinese-hacking-operation/7542641.html

Volt Typhoon & H2O Facilities

Volt Typhoon is another Chinese state-sponsored hacking group that has been compromising U.S. critical infrastructure, including water and wastewater systems. The White House, in collaboration with the Environmental Protection Agency (EPA), announced the formation of a Water Sector Cybersecurity Task Force in response to these threats. The task force aims to engage state water sectors and water government coordinating councils to reduce the risks of cyberattacks on nationwide water systems. This initiative follows the discovery that Volt Typhoon has compromised the IT environments of multiple U.S. critical infrastructure organizations with the end goal of a future cyberattack.

Homework

- https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a
- https://www.meritalk.com/articles/
- https://www.darkreading.com/ics-ot-security/new-us-warning-highlights-vulnerability-of-us-water-systems-to-cyberattacks

China Hacks U.K. Politihacks

The U.K. has also been a target of Chinese state-sponsored cyber espionage. Hackers affiliated with APT31 have been accused of conducting a years-long cyber-attack targeting politicians, journalists, and businesses. The operation saw political dissidents and critics of China targeted by sophisticated phishing campaigns, resulting in some email systems and networks being compromised. The U.K. government announced sanctions against individuals and a front company linked to APT31. The New Zealand government has also raised concerns with the Chinese government about its involvement in an attack.

Homework

- https://www.theguardian.com/politics/live/2024/mar/25/rishi-sunak-conservatives-oliver-dowden-china-cyber-attacks-keir-starmer-labour-wales-uk-politics-live

China Expands State Secrets / "Work Secrets" Law

China has revised its state secrets law, which now requires business entities in China to identify and disclose "work secrets," or non-classified information, to the government. This revision is purposely ambiguous, allowing China to potentially force U.S. tech firms to turn over proprietary information that could be used to target the U.S. government or impact the data security of Americans. The law poses a significant dilemma for U.S. tech companies operating in China, as compliance could threaten U.S. national security, while refusal could result in losing access to the Chinese market.

Homework

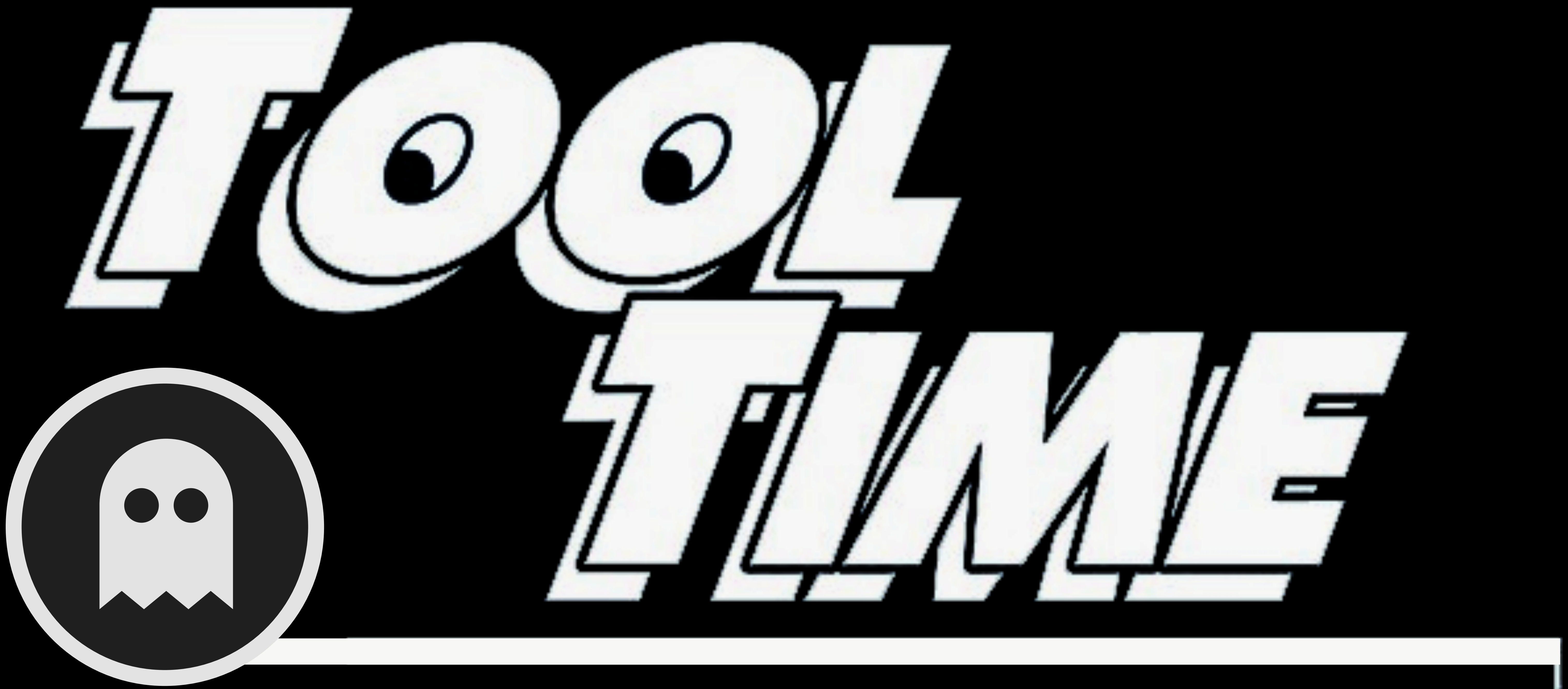
- https://thehill.com/opinion/technology/
- https://www.forbes.com/sites/lorenthompson/2023/12/14/why-chinas-growing-challenge-to-big-tech-is-a-problem-for-the-pentagon/?sh=58d510604990
- https://www.cnbc.com/2024/02/28/china-doubles-down-on-national-security-expanding-its-state-secrets-law.html
- http://politics.people.com.cn/n1/2024/0227/c1001-40184585.html

U.S. vs. TikTok

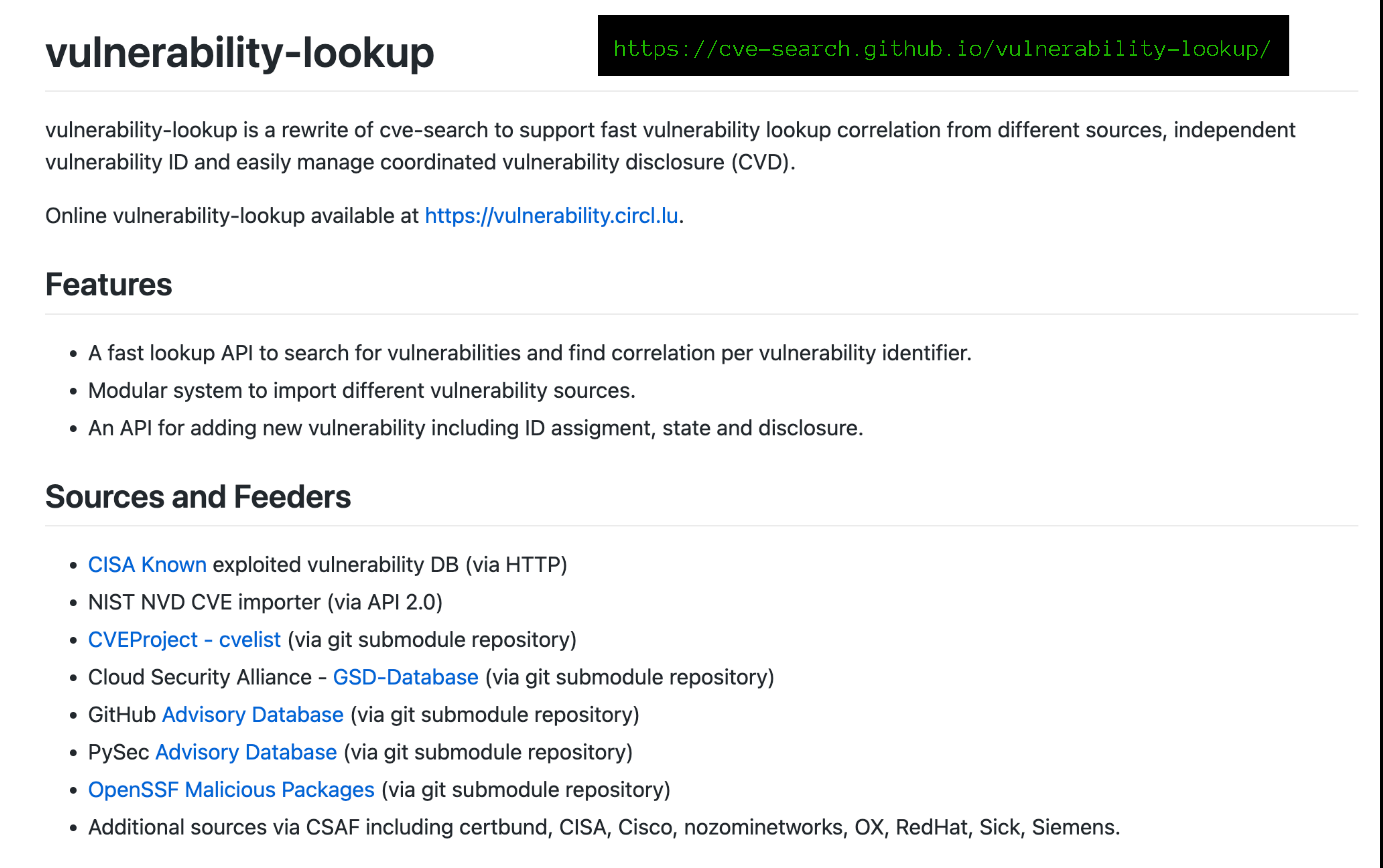
The U.S. government's scrutiny of TikTok, a popular social media platform owned by the Chinese company ByteDance, has escalated amid concerns over national security and data privacy. There have been discussions and reactions to the potential ban of TikTok in the U.S., with China criticizing the move as politicization of cybersecurity issues. The debate centers around the risks associated with the Chinese government's potential access to the data of U.S. citizens through TikTok, which has led to calls for the app to be banned or its operations in the U.S. to be segregated from its parent company.

Homework

- https://www.cnn.com/2024/03/14/tech/china-reactions-tiktok-potential-ban-intl-hnk/index.html


TOOL
TIME

https://cve-search.github.io/vulnerability-lookup/



vulnerability-lookup

vulnerability-lookup is a rewrite of cve-search to support fast vulnerability lookup correlation from different sources, independent vulnerability ID and easily manage coordinated vulnerability disclosure (CVD).

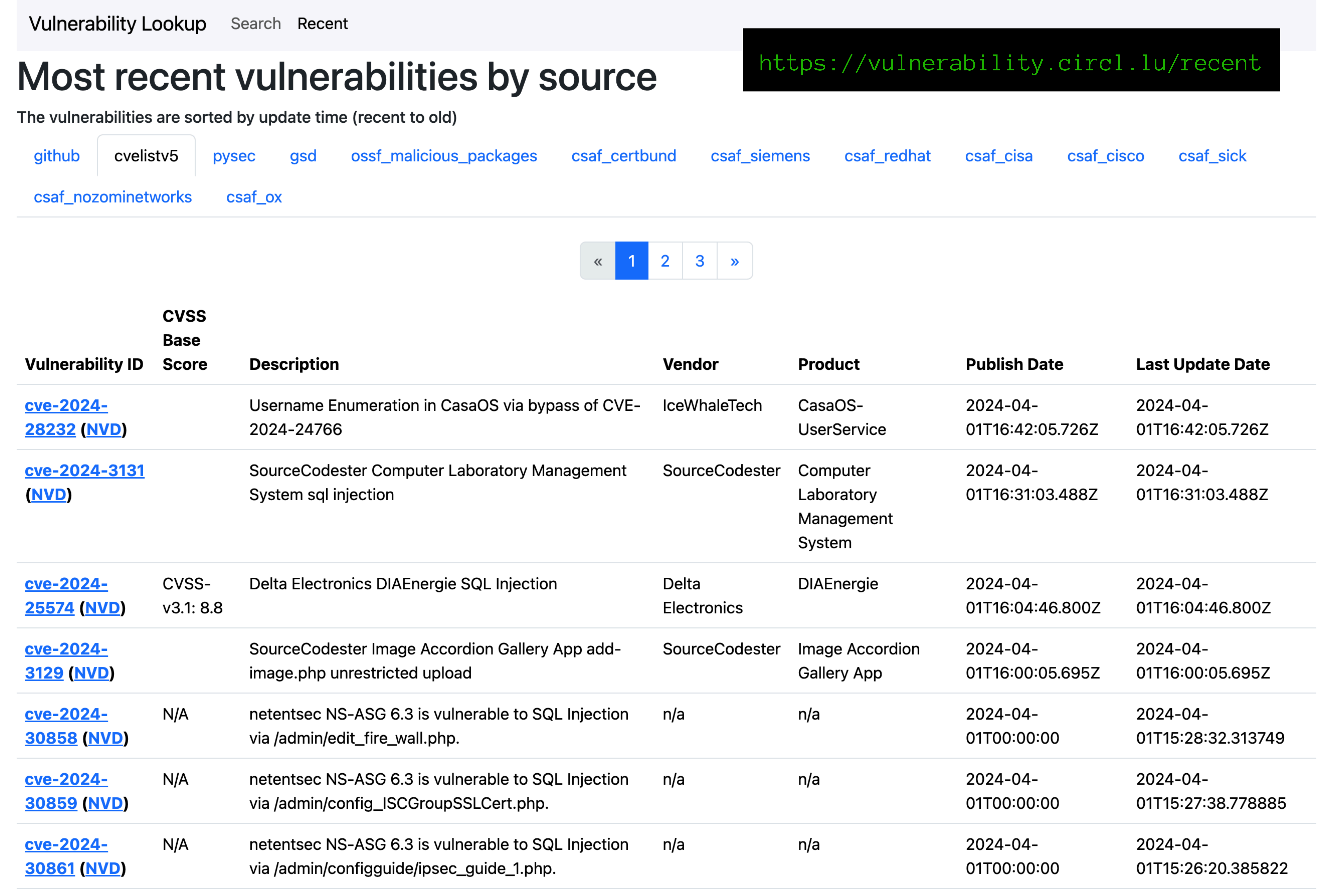
Online vulnerability-lookup available at https://vulnerability.circl.lu.

Features

- A fast lookup API to search for vulnerabilities and find correlation per vulnerability identifier.
- Modular system to import different vulnerability sources.
- An API for adding new vulnerability including ID assigment, state and disclosure.

Sources and Feeders

- CISA Known exploited vulnerability DB (via HTTP)
- NIST NVD CVE importer (via API 2.0)
- CVEProject - cvelist (via git submodule repository)
- Cloud Security Alliance - GSD-Database (via git submodule repository)
- GitHub Advisory Database (via git submodule repository)
- PySec Advisory Database (via git submodule repository)
- OpenSSF Malicious Packages (via git submodule repository)
- Additional sources via CSAF including certbund, CISA, Cisco, nozominetworks, OX, RedHat, Sick, Siemens.



`https://vulnerability.circl.lu/recent`

Most recent vulnerabilities by source

The vulnerabilities are sorted by update time (recent to old)

Vulnerability ID	CVSS Base Score	Description	Vendor	Product	Publish Date	Last Update Date
cve-2024-28232 (NVD)		Username Enumeration in CasaOS via bypass of CVE-2024-24766	IceWhaleTech	CasaOS-UserService	2024-04-01T16:42:05.726Z	2024-04-01T16:42:05.726Z
cve-2024-3131 (NVD)		SourceCodester Computer Laboratory Management System sql injection	SourceCodester	Computer Laboratory Management System	2024-04-01T16:31:03.488Z	2024-04-01T16:31:03.488Z
cve-2024-25574 (NVD)	CVSS-v3.1: 8.8	Delta Electronics DIAEnergie SQL Injection	Delta Electronics	DIAEnergie	2024-04-01T16:04:46.800Z	2024-04-01T16:04:46.800Z
cve-2024-3129 (NVD)		SourceCodester Image Accordion Gallery App add-image.php unrestricted upload	SourceCodester	Image Accordion Gallery App	2024-04-01T16:00:05.695Z	2024-04-01T16:00:05.695Z
cve-2024-30858 (NVD)	N/A	netentsec NS-ASG 6.3 is vulnerable to SQL Injection via /admin/edit_fire_wall.php.	n/a	n/a	2024-04-01T00:00:00	2024-04-01T15:28:32.313749
cve-2024-30859 (NVD)	N/A	netentsec NS-ASG 6.3 is vulnerable to SQL Injection via /admin/config_ISCGroupSSLCert.php.	n/a	n/a	2024-04-01T00:00:00	2024-04-01T15:27:38.778885
cve-2024-30861 (NVD)	N/A	netentsec NS-ASG 6.3 is vulnerable to SQL Injection via /admin/configguide/ipsec_guide_1.php.	n/a	n/a	2024-04-01T00:00:00	2024-04-01T15:26:20.385822

STORMWATCH

CYBERSECURITY NEWS

SHAMELESS SELF-PROMOTION

censys

Join Censys for a Threat Hunting Workshop & Happy Hour!

April 17, 2024 | City Winery | Philadelphia

```
https://go.censys.com/threat-hunting-workshop-philadelphia-2024.html
```

Lunch | 12 - 1:30 p.m.
Threat Hunting Workshop | 1:30 - 4:30 p.m. (see below for 'who should attend')
Happy Hour to follow | 4:30 p.m. (everyone welcome!)

https://www.labs.greynoise.io/grimoire/2024-03-28-panning-for-gold/

Panning For Gold: Sifting Through Network Logs to Write a New Tag

How do we find vulnerabilities that aren't making the news right now? By Sifting through the sensor logs!

VULNERABILITIES DISCLOSURE TOOLS

AUTHOR
Brianna Cluck

PUBLISHED
March 28, 2024

https://www.greynoise.io/blog/what-were-reading-march-2024

COMPANY

What We're Reading: March 2024

The GreyNoise Team | March 28, 2024

STORMWATCH

CYBERSECURITY NEWS

TAG ROUND-UP

- 🏷 NUUO Firmware CVE-2016-5674 Command Injection Attempt (CVE-2016-5674)
- 🏷 Looks Like CERT.at
- 🏷 Apache OFBiz CVE-2023-49070 Auth Bypass Attempt (CVE-2023-49070)
- 🏷 Embedthis GoAhead CVE-2017-17562 RCE Attempt (CVE-2017-17562)
- 🏷 Hytec Inter HWL-2511-SS CVE-2022-36553 RCE Attempt (CVE-2022-36553)
- 🏷 Symfony Profiler Debug Mode RCE Attempt

https://viz.greynoise.io/trends?view=recent

WE NEED

TO TALK

ABOUT

KEV

It Has Been

7

Days Since The
Last KEV Release

```
https://kev.hrbrmstr.app
```

https://www.cisa.gov/known-exploited-vulnerabilities-catalog

CVE-2023-24955: Microsoft SharePoint Server Code Injection Vulnerability