

STORM4WATCH

CYBERSECURITY NEWS

Dateline: 2024-04-16

	_	_		_	_	_		
								Ş
								P
								K
								Z
								4
								1
								т
								' 5
								0
								N
								C
								F
								K
								0
								F
								E
								S
								Ι
								I E
								I E R
			D = S B					I E R
								I R C









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 моre

https://StormWatch.ing



n E



Erick Galinkin

AI Security Researcher

NVIDIA





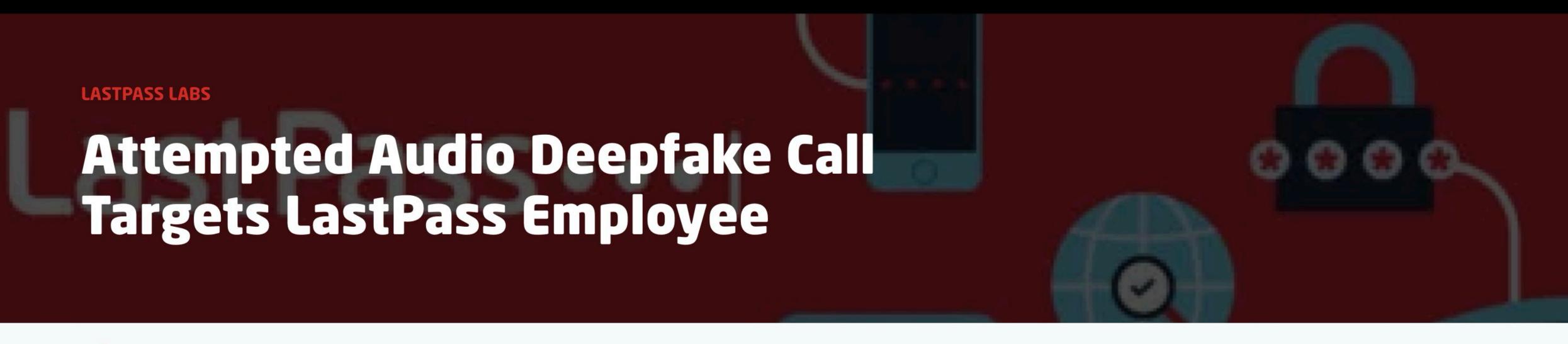


STORMATCH

CYBERSECURITY NEWS



	_	_		_	_	_		
								Ş
								P
								K
								Z
								4
								1
								т
								' 5
								0
								N
								C
								F
								K
								0
								F
								E
								S
								Ι
								I E
								I E R
			D = S B					I E R
								I R C





Mike Kosak - April 10, 2024

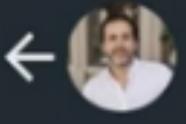
https://blog.lastpass.com/posts/2024/04/attempted-audio-deepfake-call-targets-lastpass-employee



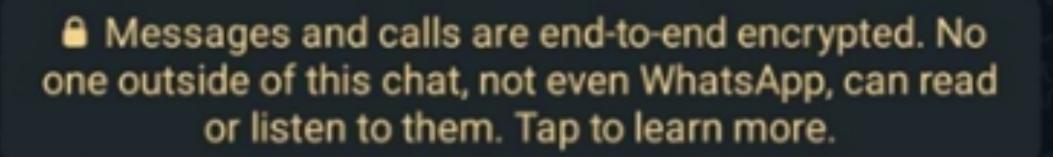
06:07 🖂 💀 📲 🔹

🖙 🦻 💐 🗟 📶 53% 🛢

ł



+1 (216) 315-6189 last seen today at 05:35





+1 (216) 315-6189

~ Karim Toubba

Phone number from United States • Not a contact • No common groups

Gafety tools

+• Add

O Block





Deepfake technology, which uses AI to create fabricated audio/visual recordings, has become more accessible and is being used for fraud and disinformation campaigns. This includes cases of deepfake audio being used to impersonate company executives and trick employees into transferring funds.

LastPass recently experienced an attempted deepfake attack, where an employee received calls, texts, and a voicemail from a threat actor impersonating the LastPass CEO using deepfake audio. The employee recognized the signs of a social engineering attempt and reported it to the security team.

While there was no impact to LastPass, the company is sharing this incident to raise awareness that deepfake attacks are becoming more common, even targeting private companies, and organizations should verify suspicious contacts through established internal channels.[1]





Health Sector Cybersecurity Coordination Center

HC3: Sector Alert April 3, 2024 TLP:CLEAR Report: 202404031000

Social Engineering Attacks Targeting IT Help Desks in the Health Sector

Executive Summary

HC3 has recently observed threat actors employing advanced social engineering tactics to target IT help desks in the health sector and gain initial access to target organizations. In general, threat actors continue to evolve their tactics, techniques, and procedures (TTPs) to achieve their goals. HC3 recommends various mitigations outlined in this alert, which involve user awareness training, as well as policies and procedures for increased security for identity verification with help desk requests.

Report

Social engineering is being used across the Healthcare and Public Health (HPH) sector to gain unauthorized access to systems. Threat actors are employing sophisticated social engineering techniques to target an organization's IT help desk with phone calls from an area code local to the target organization, claiming to be an employee in a financial role (specifically in revenue cycle or administrator roles). The threat actor is able to provide the required sensitive information for identity verification, including the last four digits of the target employee's social security number (SSN) and corporate ID number, along with other demographic details. These details were likely obtained from professional networking sites and other publicly available information sources, such as previous data breaches. The threat actor claimed that their phone was broken, and therefore could not log in or receive MFA tokens. The threat actor then successfully convinced the IT help desk to enroll a new device in multi-factor authentication (MFA) to gain access to corporate resources.

After gaining access, the threat actor specifically targeted login information related to payer websites, where they then submitted a form to make ACH changes for payer accounts. Once access has been gained to employee email accounts, they sent instructions to payment processors to divert legitimate payments to attacker-controlled U.S. bank accounts. The funds were then transferred to overseas accounts. During the malicious campaign, the threat actor also registered a domain with a single letter variation of the target organization and created an account impersonating the target organization's Chief Financial Officer (CFO).

Analysis

There was a recent high profile incident leveraging these social engineering techniques to target an organization in the hospitality and entertainment industry in September 2023. While the threat actor Scattered Spider (also known as UNC3944) claimed responsibility for this attack, which led to the deployment of ALPHV (also known as BlackCat) ransomware, there is currently no public attribution for the incident in the health sector.

While these recent campaigns in the health sector did not involve ransomware, both of these incidents did leverage spearphishing voice techniques and impersonation of employees with specific access related to the threat actors' end goals. Spearphishing voice (<u>T1566.004</u>) is a specific variant of spearphishing. It is different from other forms of spearphishing in that it employs the use of manipulating a user into providing access to systems through a phone call or other forms of voice communications. Spearphishing frequently involves social engineering techniques, such as posing as a trusted source (impersonation) and/or creating a sense of urgency or alarm for the recipient.

It is important to note that threat actors may also attempt to leverage AI voice impersonation techniques to social engineer targets, making remote identity verification increasingly difficult with these technological [TLP:CLEAR, ID#202404031000, Page 1 of 4]

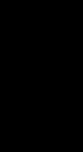
While these recent campaigns in the health sector did not involve ransomware, both of these incidents did leverage spearphishing voice techniques and impersonation of employees with specific access related to the threat actors' end goals. Spearphishing voice (T1566.004) is a specific variant of spearphishing. It is different from other forms of spearphishing in that it employs the use of manipulating a user into providing access to systems through a phone call or other forms of voice communications. Spearphishing frequently involves social engineering techniques, such as posing as a trusted source (impersonation) and/or creating a sense of urgency or alarm for the recipient.

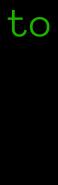
It is important to note that threat actors may also attempt to leverage AI voice impersonation techniques to social engineer targets, making remote identity verification increasingly difficult with these technological advancements. A recent global study found that out of 7,000 people surveyed, one in four said that they had experienced an AI voice cloning scam or knew someone who had.

https://www.hhs.gov/sites/default/files/help-desk-social-engineering-sector-alert-tlpclear.pdf

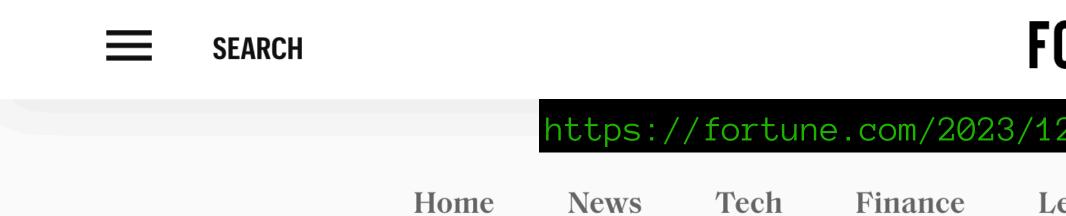












COMMENTARY · BRAINSTORM AI

Countering AI-driven cyberattacks with AIdriven cybersecurity

BY **RUPAL HOLLENBECK**

December 29, 2023 at 2:00 PM EST



Artificial intelligence is already changing the way we interact with technology. But it can be challenging to identify where it can have the most impact operationally. Use cases for AI are broad but work best when applied to specific tasks as a force multiplier for human teams. For many organizations, one of the most impactful AI investments they make will be in cybersecurity.

Cyberattacks are among the biggest risks for a modern organization of any size. Our research has

FORTUNE

https://fortune.com/2023/12/29/ai-cybersecurity-checkpoint/

Leadership Well Recommends Fortune 500



Al is already changing the way we interact with technology, but it can be challenging to identify where it can have the most impact.

GETTY IMAGES



Joint Cybersecurity Information



Best Practices for Deploying Secure and Resilient AI Systems

Executive summary

Deploying artificial intelligence (AI) systems securely requires careful setup and configuration that depends on the complexity of the AI system, the resources required (e.g., funding, technical expertise), and the infrastructure used (i.e., on premises, cloud, or hybrid). This report expands upon the 'secure deployment' and 'secure operation and maintenance' sections of the <u>Guidelines for secure AI system development</u> and incorporates mitigation considerations from <u>Engaging with Artificial Intelligence (AI)</u>. It is for organizations deploying and operating AI systems designed and developed by another entity. The best practices may not be applicable to all environments, so the mitigations should be adapted to specific use cases and threat profiles. [1], [2]

Al security is a rapidly evolving area of research. As agencies, industry, and academia discover potential weaknesses in Al technology and techniques to exploit them, organizations will need to update their Al systems to address the changing risks, in addition to applying traditional IT best practices to Al systems.

This report was authored by the U.S. National Security Agency's Artificial Intelligence Security Center (AISC), the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), the Australian Signals Directorate's Australian Cyber Security Centre (ACSC), the Canadian Centre for Cyber Security (CCCS), the New Zealand National Cyber Security Centre (NCSC-NZ), and the United Kingdom's National Cyber Security Centre (NCSC-UK). The goals of the AISC and the report are to:

- 1. Improve the confidentiality, integrity, and availability of AI systems;
- 2. Assure that known cybersecurity vulnerabilities in AI systems are appropriately mitigated; and
- 3. Provide methodologies and controls to protect, detect, and respond to malicious activity against AI systems and related data and services.

This document is marked TLP:CLEAR. Recipients may share this information without restriction. Information is subject to standard copyright rules. For more on the Traffic Light Protocol, see cisa.gov/tlp/.



Secure the deployment environment

- Establish robust governance over the AI system deployment, including understanding risks, defining roles/responsibilities, and collaborating across teams.
- Ensure a secure and well-designed architecture for the deployment environment, applying zero trust principles and protecting data sources.
- Harden configurations by applying security best practices like encryption, authentication, and vulnerability management.
- Protect the deployment networks using detection and response capabilities.

Continuously protect the AI system

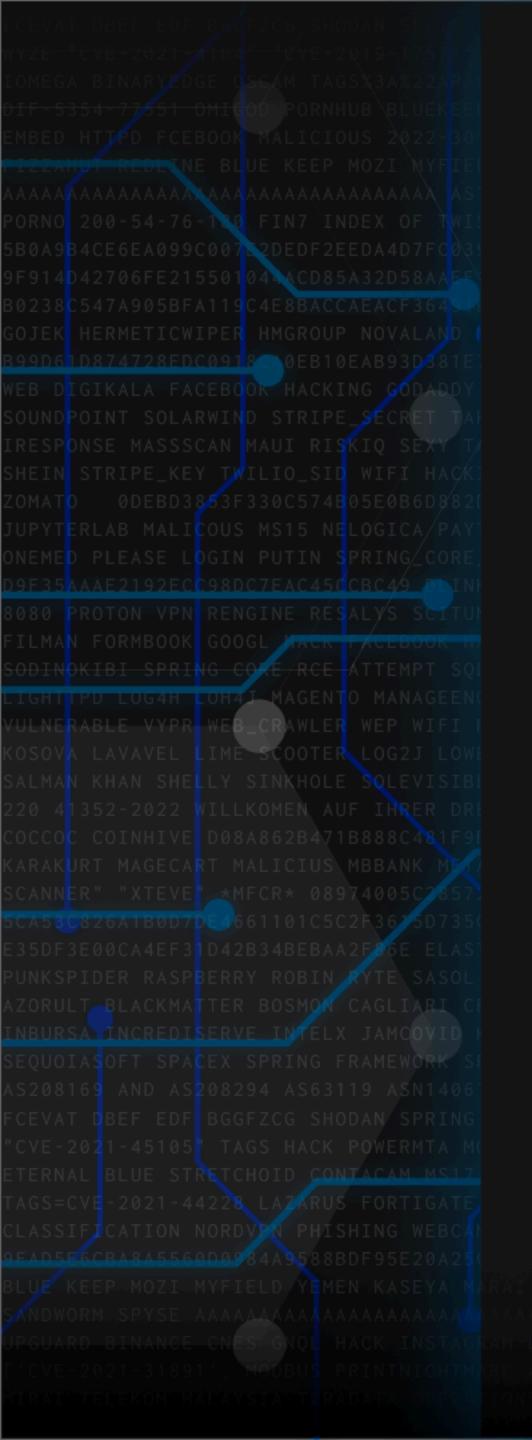
- Validate the AI system before and during use through testing, integrity checks, and supply chain security.
- Secure exposed APIs and actively monitor model behavior for anomalies.
- Implement strong protections for the AI model weights and parameters.

Securely operate and maintain the AI system

- Enforce strict access controls and user awareness/ training.
- Conduct regular audits, penetration testing, and monitoring.
- Maintain a rigorous patch and update management process.

Threat actors are experts at finding malicious applications for technology advances, and ChatGPT is no exception. They discovered that despite its safeguards, they could easily use the tool to write malicious emails for phishing campaigns. Prior to this, many phishing emails contained obvious red flags: poor grammar, abnormal word choice, typos, and other deviations that raised questions. This fortunate last line of defense has disappeared as threat actors use generative AI to draft phishing lures that are formally perfect and often personalized. These engines typically feature a natural speech-to-code function, which can be used to build malicious files to deploy.

Generative AI lowers the barrier to entry across the entire attack life cycle. The generative AI boom may be having an impact already: Our research shows that email-delivered attacks have spiked in 2023, representing 86% of all file-based attacks we recorded. Other types of AI also amplify threat actors' capacity by automating attacks, finding vulnerabilities, managing botnets, and more. They use artificial intelligence as a force multiplier.



STORMATCH

CYBERSECURITY NEWS

	_	_		_	_	_		
								Ş
								P
								K
								Z
								4
								1
								т
								' 5
								0
								N
								C
								F
								K
								0
								F
								E
								S
								Ι
								I E
								I E R
			D = S B					I E R
								I R C



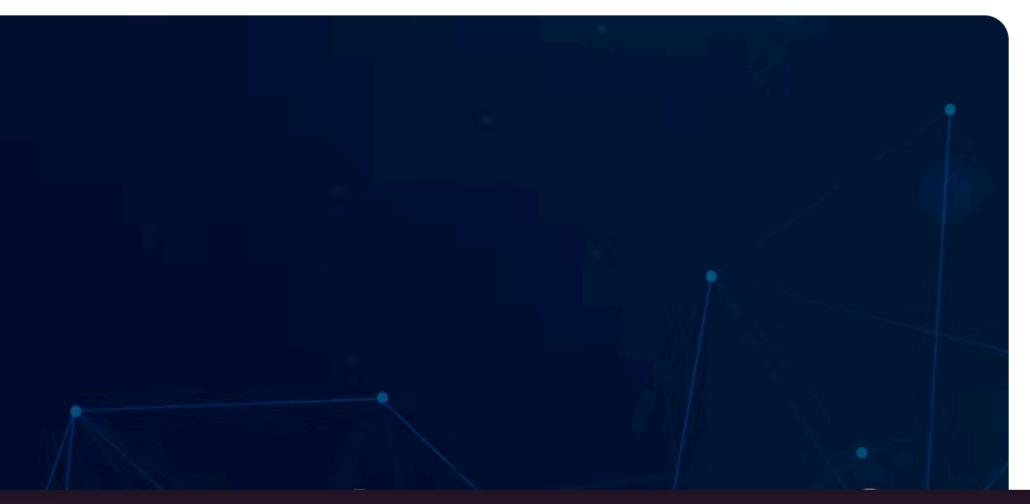
https://openjsf.org/blog/openssf-openjs-alert-social-engineering-takeovers

Community

Open Source Security (OpenSSF) and OpenJS **Foundations Issue Alert for Social Engineering Takeovers of Open Source Projects**

XZ Utils cyberattack likely not an isolated incident



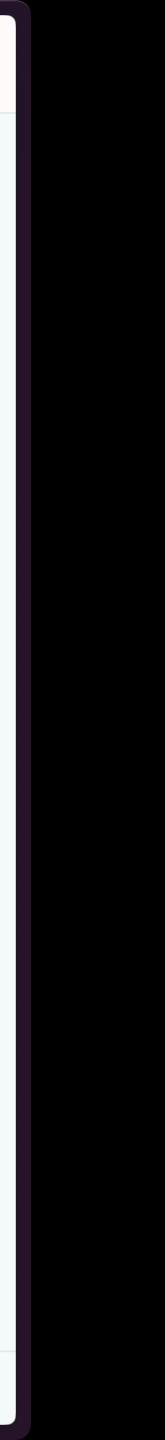






Impact Projects Appium Appium is an open-source, Node.js server used for automating native, mobile web, and hybrid... \bigcirc ▲ Download Learn more ▲ Contribute jQuery jQuery is a fast, small, and feature-rich JavaScript library. It makes things like HTML document traversal... \bigcirc ▲ Contribute Learn more ▲ Download webpack webpack is a bundler for modules and is primarily used to bundle JavaScript files for usage in a browser. It is... \bigcirc ▲ Contribute Learn more ▲ Download

ng ↗	Blog Commu	nity 🗸	Become a member
	0	n is a framework to build o apps with JavaScript, H ⁻	
	Learn more	Download	
		s ® is a JavaScript runtime ript engine.	built on Chrome's V8
	Learn more	Download	Contribute





STORMATCH

CYBERSECURITY NEWS

	_	_		_	_	_		
								Ş
								P
								K
								Z
								4
								1
								т
								' 5
								0
								N
								C
								F
								K
								0
								F
								E
								S
								Ι
								I E
								I E R
			D = S B					I E R
								I R C

ma pedia

Library

Families Actors

https://ma

Click here to download all references as Bib-File. • 🔊

Search...

Enter keywords to filter the library entries below or Propose new Entry

2024-04-12 · Volexity · Volexity Threat Research Zero-Day Exploitation of Unauthenticated Remote Code **永** UPSTYLE

2024-04-12 · Palo Alto Networks Unit 42 · Unit 42 Threat Brief: Operation MidnightEclipse, Post-Exploit **永** UPSTYLE

2024-04-11 · Twitter (@embee_research) · Embee_research Tracking Malicious Infrastructure With DNS Records -🟦 Vultur

2024-04-11 · Github (jeFF0Falltrades) · Jeff Archer **Rat King Configuration Parser**

兼 AsyncRAT 兼 DCRat 兼 Quasar RAT 兼 Venom RAT

2024-04-10 · IWcommunityFR Leak of Epsilon Stealer's source code 🟦 Epsilon Stealer

2024-04-10 · 2024-04-10 · Antonio Pirozzi, Sarthak Misraa XZ Utils Backdoor | Threat Actor Planned to Inject Further Vulnerabilities 🕱 xzbot

2024-04-10 · Offset Blog · Daniel Bunce Recolving Stack Strings with Canstone Disassembler & Unicorn in Puthon

Fraunhofer
Inventory Statistics Usage ApiVector Login
alpedia.caad.fkie.fraunhofer.de/library
<pre>« 1 2 3 »</pre>
S ✓ Execution Vulnerability in GlobalProtect (CVE-2024-3400)
ා 🖍
ා 🖍 Vultur Banking Trojan
S 🖍
D 🖍
IJrther Vulnerabilities



ma pedia

Library

Families

Actors

Search...

Enter keywords to filter the families below

	OS	Common Name
1	•	Vultur
2		Epsilon Stealer
3		Nova Stealer
4		Zloader
5		Amadey
6	\bigtriangleup	xzbot
7		Vidar
8		AsyncRAT
9	=	Quasar RAT
10		DCRat
11		Venom RAT
12		SystemBC
13		RedLine Stealer
14	ţ	LaZagne
15	=	Drokbk



Inventory Statistics Usage ApiVector Login

« 1 2 3 »

Last Updated	Status
2024-04-15	
2024-04-15	★ 🗉
2024-04-11	★ 🗉
2024-02-16	💷 🗣
2024-02-05	🛧 📼 🗣
2024-04-15	2
2024-04-15	🗙 🖬 🗣
2024-04-15	💷 🗣
2024-04-15	💷 🗣
2024-04-15	💷 🗣
2024-04-15	
2024-01-22	💷 🗣
2024-04-15	💷 🗣
2024-04-15	2
2024-04-15	🛨 🖂



ma pedia

Library

Families Actors

The following table provides a mapping of the actor groups tracked by the MISP Galaxy Project, augmented with the families covered in Malpedia.

Search...

Enter keywords to filter the actors below

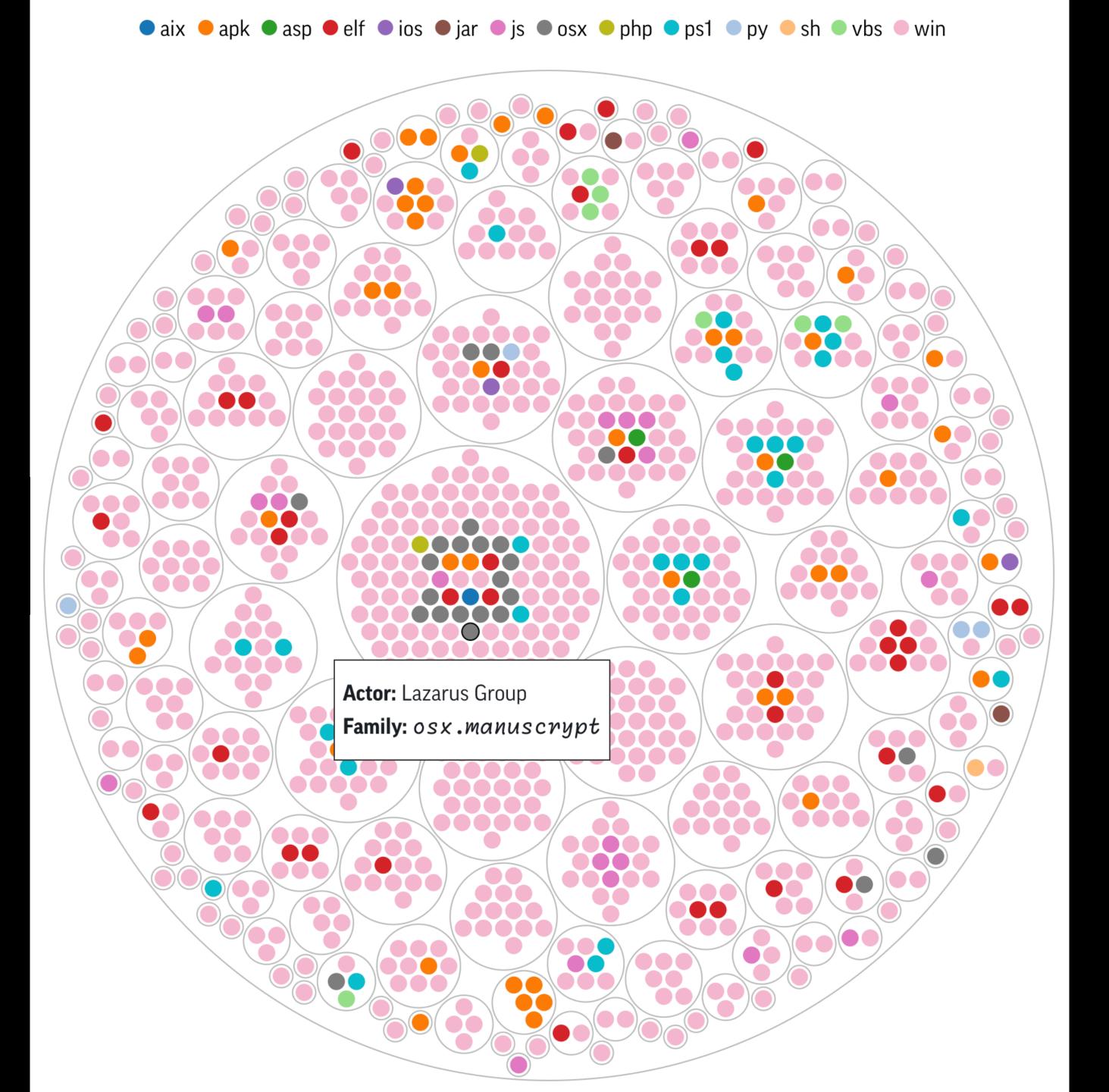
		Common Name	Coverage
1	•	Lazarus Group	ૠ 129
2		Cleaver	ज़ी 36
3	* `	APT1	∄i € 35
4	= 6	Turla	ज़ी 33
5	= 6	APT28	流 32
6	= 6	UNC2452	,îk 30
7	G	CHRYSENE	jîk 28
8	*	APT41	π̂ 27
9	÷	OilRig	जी 27
10	= 6	APT29	ñ t 24
11	* 6	APT40	jît 20
12	•	Silent Chollima	jît 20
13	*	APT32) ग्रि 18
14	•	APT37	,îk 15
15	6	FIN11)îk 15



Inventory Statistics Usage ApiVector Login



https://observablehq.com/ @hrbrmstr/2024-30-day-mapchallenge-day-12relationships-family



SHAMELESS F-PROMOTI

STORMATCH

CYBERSECURITY NEWS

	_	_		_	_	_		
								Ş
								P
								K
								Z
								4
								1
								т
								' 5
								0
								N
								C
								F
								K
								0
								F
								E
								S
								Ι
								I E
								I E R
			D = S B					I E R
								I R C



Join Censys for a Thrunting Workshop & Happy Hour! https://go.censys.com/threat-hunting-workshop-philadelphia-2024.html

April 17, 2024 | City Winery | Philadelphia

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





Products 🔻 Request a Demo Company 🔻 Solutions 🔻 Federal Search Now Q Resources 🔻 BLOGS

CVE-2024-3272 & CVE-2024-3273: D-Link NAS



https://censys.com/cve-2024-3272-and-2024-3273/



Products 💌	Solutions 🔻	Federal	Resources 💌	Company

BLOGS

Sisense: A Look at Industry and Geography

https://censys.com/sisense-a-look-at-industry-and-geography/

Search Now Q

Request a Demo

https://www.greynoise.io/blog/netnoisecon-amplifying-the-future-of-infosec

COMPANY

NetNoiseCon: Amplifying the Future of InfoSec

Sam Houston | April 2, 2024





VULNERABILITIES LABS

CVE-2024-3400: Command Injection Vulnerability in Palo Alto Networks PAN-OS

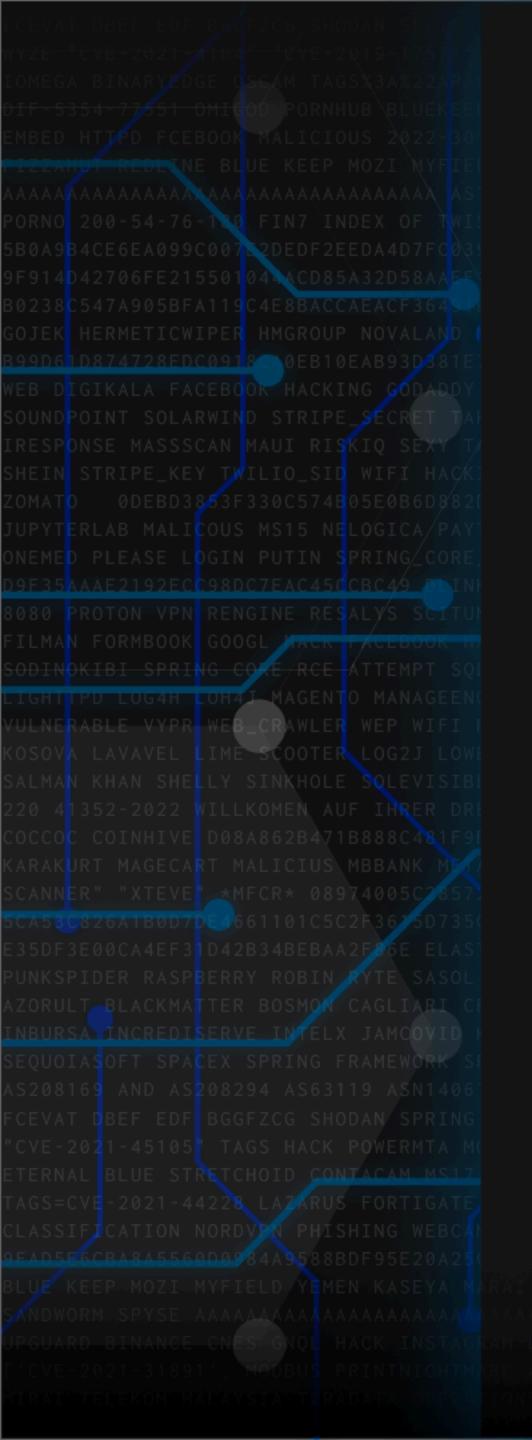
The GreyNoise Labs Team | April 15, 2024



https://www.greynoise.io/blog/cve-2024-3400-command-injection-vulnerability-palo-alto-networks-pan-os

https://viz.greynoise.io/tags/palo-alto-pan-os-cve-2024-3400-rce-attempt?days=30





ROI

CYBERSECURITY NEWS

STORMATCH

	_	_		_	_	_		
								Ş
								P
								K
								Z
								4
								1
								т
								' 5
								0
								N
								C
								F
								K
								0
								F
								E
								S
								Ι
								I E
								I E R
			D = S B					I E R
								I R C

elFinder 2.1.58 RCE CVE-2021-32682 Attempt (CVE-2021-32682) elFinder 2.1.58 RCE CVE-2021-32682 Check (CVE-2021-32682) Joomla! ProDesk 1.0/1.2 LFI CVE-2008-6222 Attempt (CVE-2008-6222) DbGate Web Client RCE Attempt Citrix StoreFront XSS CVE-2023-5914 Attempt (CVE-2023-5914)

۲

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

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

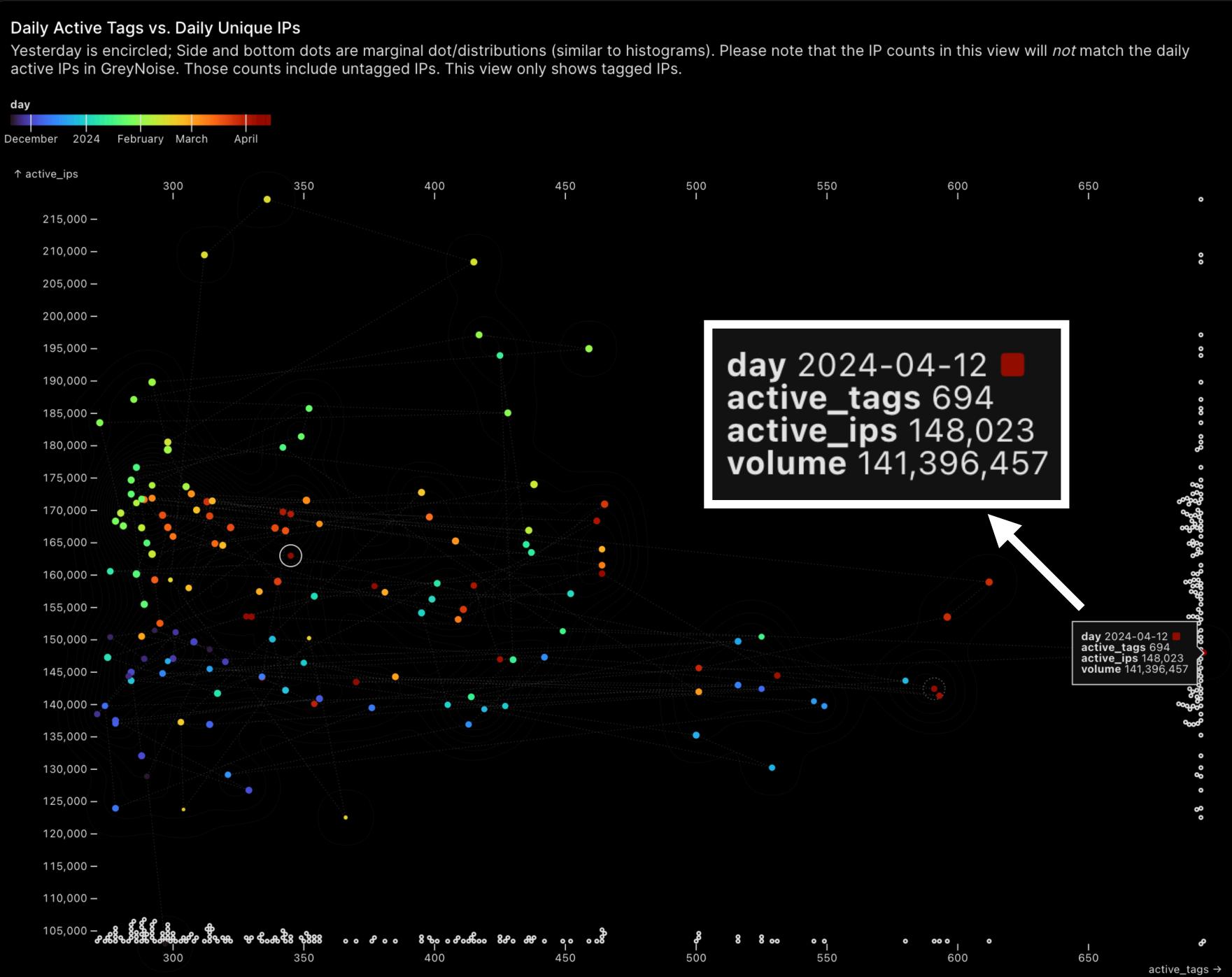
```
Telesquare TLR-2005KSH CVE-2024-29269 RCE Attempt (CVE-2024-29269)
```

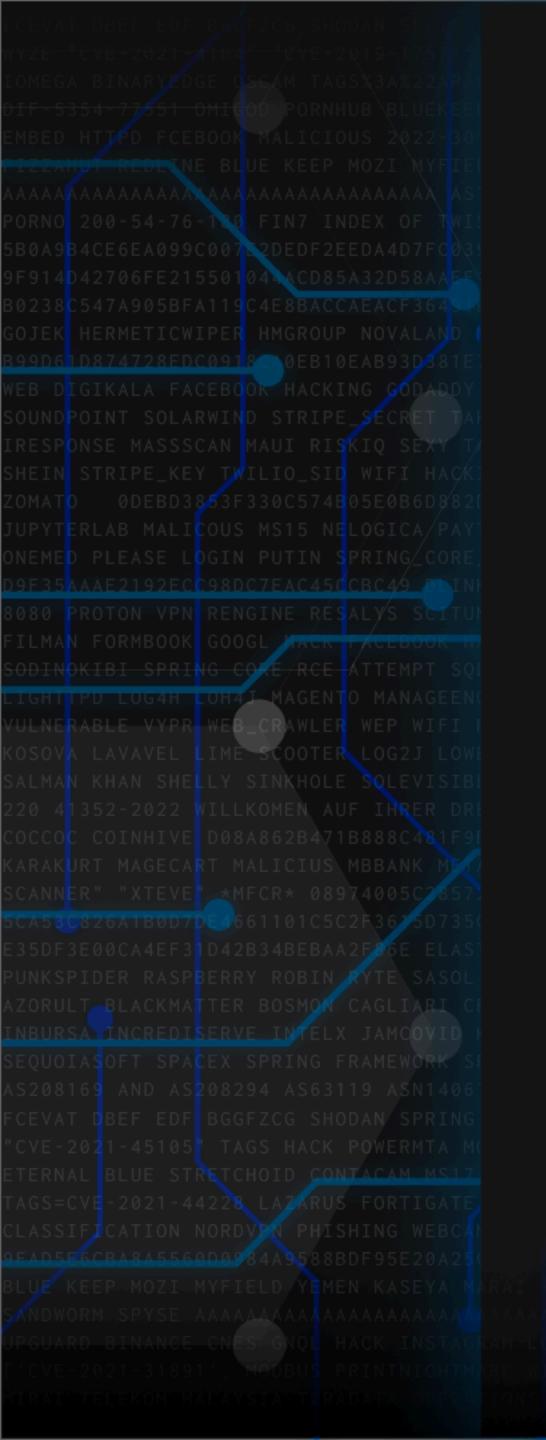
```
Wordpress Popup-Maker CVE-2019-17574 Auth Bypass Attempt (CVE-2019-17574)
LearnPress SQL Injection CVE-2023-6567 Attempt (CVE-2023-6567)
```

• • ColumbiaSoft DocumentLocator SSRF CVE-2023-5830 Attempt (CVE-2023-5830) • ZZZCMD zzzphp CVE-2019-9041 RCE Attempt (CVE-2019-9041) • WordPress Automatic Plugin CVE-2024-27954 Attempt (CVE-2024-27354) • Adobe ColdFusion Arbitrary File Read CVE-2024-20767 Attempt (CVE-2024-20767) • ESAFENET CDG Arbitrary File Download CVE-2019-9632 Attempt (CVE-2019-9632) • Nexus Repository Manager CVE-2020-10199 RCE Attempt (CVE-2020-10199) • NotificationX SQL Injection CVE-2024-1698 Attempt (CVE-2024-1698) • Apache Tika CVE-2018-1335 Command Injection RCE Attempt (CVE-2018-1335) • • • Joomla! Component RWCards 3.0.11 LFI CVE-2008-6172 Attempt (CVE-2008-6172) • Palo Alto PAN-OS CVE-2024-3400 RCE Attempt (CVE-2024-3400) • • • • • Inspur ClusterEngine CVE-2020-21224 RCE Attempt (CVE-2020-21224) •

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

```
Duplicator Unauthenticated Data Exposure CVE-2023-6114 Attempt (CVE-2023-6114)
PrestaShop AtributeWizardPro CVE-2018-10942 Arbitrary File Upload Attempt (CVE-2018-10942)
```





ABOUT

KEV



	_	_		_	_	_		
								Ş
								P
								K
								Z
								4
								1
								т
								' 5
								0
								N
								C
								F
								K
								0
								F
								E
								S
								Ι
								I E
								I E R
			D = S B					I E R
								I R C

CCYAI DOEF DJF BOG 226, SHODAN SI WYZE CVE-2021 100 100 PORNHUB BLU EMBED HITTPD FCEBOOR MALICIOUS 202 FIZEARDI REDITNE BLUE KEEP MOZI AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA		
DIF -5354 -7755 OMICOD PORNHUB BLU EMBED HTTED FCEBOOR MALICIOUS 202 LICANUL HEDEINE BLUE KEEP MOZI M AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA		
DIF -5354 -7755 OMICOD PORNHUB BLU EMBED HTTED FCEBOOR MALICIOUS 202 LICANUL HEDEINE BLUE KEEP MOZI M AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA		
EMBED HTTPD FCEBOOR MALICIOUS 202 LEARDY REDEINE BLUE KEEP MOZI M AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA		
LECANDI REDEINE BLUE KEEP MOZI M AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA		
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA		
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA		
5B0A9 B4CEGEA099C007 2DEDF2E 9F914 D4270GFE215501 04 ACD857 B0238 C547A905BFA119 C488BACC G0JEK HERMETICWIPER HMGROUP B99D61D874728EDC0918 00EB108 WEB DIGIKALA FACEBOOK HACKIN SOUND POINT SOLARWIND STRIPE. IRESP ONSE MASSSCAN MAUI RIST SHEIN STRIPE_KEY TVILIO_SID ZOMAT 0 0DEBD38357330C574B6 JUPYTERLAB MALICOUS MS15 NEI ONEMED PLEASE LOGIN PUTIN ST D9535 AAE2192ECC98DC7EAC4560 8080 PROTON VPN RENGINE REST FILMAN FORMBOOK GOOGL 7ACK SODIN PKIBI SPRING COLE RCE 7 LIGHT PD LOGAH LOHAL MAGENTO VULNE RABLE VYPR WEB_CRAWLER KOSOVA LAVAVEL IME SCOOTER SALMAN KHAN SHELLY SINKHOLE 220 41352-2022 VILLKOMEN AUT COCCOC COINHIVE D08A862B4718 KARAKURT MAGECART MALICIUS F SCANDER" "XTEVE * *MFCR* 089 SCASSCS26A1B0D7 12.3661101C5C E35DF3E00CA4EF3 D42B34BEBAA3 PUNKSPIDER RASPBERRY ROBIN AZORULT BLACKMA TER BOSMON O INBURSA INCREDISERVE IDTELX SEQUOIASOFT SPACEX SPRING FF AS208165 AND AS208294 AS631 FCEVAT DBEF EDF BGGFZCG SHOT "CVE-2021-45105 TAGS HACK F ETERNAL BLUE STRICTCHOID CONT TAGS=CVE-2021 - 44223 LAZARUS CLASSIFICATION NORDY 6 PHISF SEAD5FCEBASA55COD0384A9588BI BLUE KEEP MOZI MYFIELD YEMET SANDWORM SPYSE AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA		
9F914042706FE21550104450857 B0238C547A905BFA119C448BACC GOJEK HERMETICWIPER HMGROUP B990610874728EDC0918000ED108 WEB DIGIKALA FACEBOOK HACKIN SOUND POINT SOLARWIND STRIPE, IRESPONSE MASSSCAN MAUI RIST SHEIN STRIPE,KEY TVILIO_SID ZOMATO 0DEBD38357330C57486 JUPYTERLAB MALICOUS MS15 NEI ONEMED PLEASE LOGIN PUTIN ST D95354AAE2192EC598DC7EAC4560 8080 PROTON VPN RENGINE REST FILMAN FORMBOOK GOOGL 7ACK SODIN KIBI SPRING COLE, RCE 7 LIGHT PD LOGAH COMAL MAGENTO VULNE RABLE VYPR WEB_CRAWLER KOSOVA LAVAVEL TIME SCOOTER SALMAN KHAN SHELLY SINKHOLE 220 41352-2022 VILLKOMEN AUT COCCOC COINHIVE D08A862B4715 KARAKURT MAGECART MALICIUS F SCANDER" "XTEVE * *MFCR* 089 SCASSCS26A1B0D7 120661101C5C E35DF3E00CA4EF3 D42B34BEBAA3 PUNKSPIDER RASPBERRY ROBIN AZORULT BLACKMA TER BOSMON (INBURSA INCREDISERVE IDTELX SEQUOIASOFT SPACEX SPRING FF AS208165 AND AS208294 AS631 FCEVAT DBEF EDF BGGFZCG SHOT "CVE-2021-45105 TAGS HACK F ETERNAL BLUE STRICTCHOID CON TAGS=CVE-2021-44223 LAZARUS CLASSIFICATION NORDY 6 PHISF SEAD5F5CBASA55500D0384A9588BI BLUE KEEP MOZI MYFIELD YEMEF SANDWORM SPYSE AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA		
B0238 C547A905BFA119 C4E8BACC G0JEK HERMETICWIPER HMGROUP B99D61D874728EDC0918) 0EB106 WEB DIGIKALA FACEBOOK HACKIN SOUND POINT SOLARWIN D STRIPE, IRESPONSE MASSSCAN MAUI RIS SHEIN STRIPE_KEY TVILIO_SID ZOMATO 0DEBD3853F330C574B6 JUPYTERLAB MALICOUS MS15 NEU ONEMED PLEASE LOGIN PUTIN SO D9F35AAAE2192EC 98DC7EAC450 8080 PROTON VPN RENGINE RES FILMAN FORMBOOK GOOGL MACK SODINOKIBI SPRING CORE RES CODINOKIBI SPRING CORE RES SALMAN KHAN SHELLY SINKHOLE 220 41352-2022 WILLKOMEN AU COCCOC COINHIVE D08A862B4716 KARAKURT MAGECART MALICIUS I SCANDER" "XTEVE" *MFCR* 089 SCASS 0826ATB0070E 661101C5C E35DF3E00CA4EF3 ID42B34BEBAA3 PUNKSPIDER RASPBERRY ROBIN AZORULT BLACKMATTER BOSMCH O TNBURSA INCREDISERVE INTELX SEQUOIASOFT SPACEX SPRING FF AS208169 AND AS208294 AS631 FCEVAT DBEF EDF BGGFZCG SHOT "CVE-2021-45105 TAGS HACK I ETERNAL BLUE STRITCHOID CONT TAGS=CVE-2021 A4222 LA7KUS CLASSIFICATION NORDYNA PHIS PEADEFCEARA5560D078 AA35886 BLUE KEEP MOZI MYFIELD YEMEP		
GOJEK HERMETICWIPER HMGROUP B99DGTD874728EDC0918 0EB100 WEB DIGIKALA FACEBOOK HACKIN SOUNDPOINT SOLARWIN D STRIPE, IRESPONSE MASSSCAN MAUI RISS SHEIN STRIPE_KEY TVILIO_SID ZOMATO ODEBD3853F330C574B6 JUPYTERLAB MALICOUS MS15 NED ONEMED PLEASE LOGIN PUTIN SO D9F35AAAF2192EC 98DC7FAC4507 8080 PROTON VPN RENGINE RÉS FILMAN FORMBOOK GOOGL MACKI SODINOKIBI SPRING CORE/RCE LIGHT PD LOGAH LOHAT MAGENTO VULNE RABLE VYPR WEB_CRAWLER KOSOVA LAVAVEL LIME SCOTER SALMAN KHAN SHELLY SINKHOLE 220 41352-2022 WILLKOMEN AUI COCCOC COINHIVE D08A862B4716 KARAKURT MAGECART MALICIUS O SCASSOS2GATBOD7DL3661101C5C E35DF3E00CA4EF3 ID42B34BEBAA3 PUNKSPIDER RASPBERRY ROBIN AZORULT BLACKMATTER BOSMCH O TNBURSA TNCREDTSERVE TVIELX SEQUOIASOFT SPACEX SPRING FF AS208169 AND AS208294 AS631 FCEVAT DBEF EDF BGGFZCG SHOT "CVE-2021-45105 TAGS HACK O ETERNAL BLUE STRETCHOID CONT TAGS=CVE-2021 A4223 LA7KUS CLASSIFICATION NORDVIA PHISP PEADEFECEARA5560D0784A3588B0 BLUE KEEP MOZI MYFIELD YEMEP SANDWORM SPYSE AAAAAAAAAAAA	9F914 <mark>D</mark> 42706FE215	
B9906 D874728EDC09 B OEB10 WEB DIGIKALA FACEBOOK HACKIN SOUNDPOINT SOLARWIN D STRIPE, IRESPONSE MASSSCAN MAUI RISS SHEIN STRIPE_KEY TVILIO_SID ZOMATO ODEBD3853F330C574B6 JUPYTERLAB MALICOUS MS15 NEL ONEMED PLEASE LOGIN PUTIN SO D9F35AAAE2192ECC98DC7FAC4507 S080 PROTON VPN RENGINE RESS FILMAN FORMBOOK GOOGL MACK SODINOKIBI SPRING CCLE ACE UIGHT PD LOG4H OHAT MAGENTO VULNERABLE VYPR WEB_CRAWLER KOSOVA LAVAVEL IME SCOOTER SALMAN KHAN SHELLY SINKHOLE 220 41352-2022 WILLKOMEN AU COCCOC COINHIVE D08A862B4718 KARAKURT MAGECART MALICIUS O SCASSC326ATBOD764661101C5C E35DF3E00CA4EF3 D42B34BEBAA3 PUNKSPIDER RASPBERRY ROBIN AZORULT BLACKMATTER BOSMON O INBURSA INCREDISERVE INTELX SEQUOIAS OFT SPACEX SPRING FI AS208169 AND AS208294 AS631 FCEVAT DBEF EDF BGGFZCG SHOI "CVE-2021-45105 TAGS HACK I ETERNAL BLUE STRETCHOID CON TAGS=CVE-2021-44228 LATARUS CLASSIFICATION NORDVAR PHIS PEADSFCBA8A55560D0384A3588BI BLUE KEEP MOZI MYFIELD YEMEI SANDWORM SPYSE AAAAAAAAAAAA	B 0 2 3 8 <mark>C</mark> 5 4 7 A 9 0 5 B F A	
WEB DIGIKALA FACEBOOK HACKIN SOUNDPOINT SOLARWIND STRIPE, IRESPONSE MASSSCAN MAUI RISE SHEIN STRIPE_KEY TVILIO_SID ZOMATO ØDEBD3853F330C57486 JUPYTERLAB MALICOUS MS15 NEU ONEMED PLEASE LOGIN PUTIN SE D9F35AAAE2192EC 98DC7EAC4507 8080 PROTON VPN RENGINE RES FILMAN FORMBOOK GOOGL MACK SODINOKIBI SPRING COLE.RCE LIGHT PD LOG4H OHAT MAGENTO VULNERABLE VYPR WEB_CRAWLER KOSOVA LAVAVEL IME SCOOTER SALMAN KHAN SHELLY SINKHOLE 220 41352-2022 VILLKOMEN AUF COCCOC COINHIVE D08A862B4718 KARAKURT MAGECART MALICIUS N SCASSCS2GATBOD70L3661101C5C E35DF3E00CA4EF3 D42B34BEBAA3 PUNKSPIDER RASPBERRY ROBIN AZORULT BLACKMATTER BOSMON O INBURSA INCREDISERVE INTELX SEQUOIAS OFT SPACEX SPRING FF AS208169 AND AS 208294 AS631 FCEVAT DBEF EDF BGGFZCG SHOU "CVE-2021-45105 TAGS HACK I ETERNAL BLUE STRETCHOID CON TAGS=CVE-2021-44228 LATARUS CLASSIFICATION NORDVAL PHIS SEADSECBA8A5550D0984A3588BE BLUE KEEP MOZI MYFIELD YEMEN SANDWORM SPYSE AAAAAAAAAAAAAAA	GOJEK HERMETICWI	
SOUND POINT SOLARWIND STRIPE, IRESPONSE MASSSCAN MAUI RIS SHEIN STRIPE_KEY TVILIO_SID ZOMATO ØDEBD3853F330C57480 JUPYTERLAB MALICOUS MS15 NEL ONEMED PLEASE LOGIN PUTIN SE D9F35 AAAF2192EC 988DC7FAC4500 8080 PROTON VPN RENGINE RES FILMAN FORMBOOK GOOGL FACK T SODINOKIBI SPRING COLE, RCE T LIGHT PD LOG4H LOHAT MAGENTO VULNE RABLE VYPR WEB_CRAWLER KOSOVA LAVAVEL TIME SCOOTER SALMAN KHAN SHELLY SINKHOLE 220 4 1352-2022 WILLKOMEN AUF COCCOC COINHIVE D08A862B4718 KARAKURT MAGECART MALICIUS N SCASOCS26ATB0D7DE S61101C5C2 E35DF3E00CA4EF31D42B34BEBAA2 PUNKSPIDER RASPBERRY ROBIN AZORULT BLACKMATTER BOSMON O TNBURSA INCREDISERVE TVIELX SEQUOIASOFT SPACEX SPRING FF AS208169 AND AS 208294 AS6317 FCEVAT DBEF EDF BGGFZCG SHOU "CVE-2021-45105 TAGS HACK F ETERNAL BLUE STRETCHOID CON TAGS=CVE-2021-44228 LAZARUS CLASSIFICATION NORDVO PHIS PEADEFSCBA8A5560D0784A3588BI BLUE KEEP MOZI MYFIELD YEMEI SANDWORM SPYSE AAAAAAAAAAAAA	<u>B 9 9 D 6 <mark>1 D 8 7 4 7 2 8 E D 0</mark></u>	
IRESPONSE MASSSCAN MAUI RIS SHEIN STRIPE_KEY TVILIO_SID ZOMATO ØDEBD3803F330C57480 JUPYTERLAB MALICOUS MS15 NEL ONEMED PLEASE LOGIN PUTIN SE D9F35AAAF2192ECC98DC7FAC4500 8080 PROTON VPN RENGINE RES FILMAN FORMBOOK GOOGL FACK F SODINOKIBI SPRING COLE REE LIGHT PD LUG4H OH41 MAGENTO VULNERABLE VYPR WEB_CRAWLER KOSOVA LAVAVEL LIME SCOOTER SALMAN KHAN SHELLY SINKHOLE 220 4 1352-2022 WILLKOMEN AUF COCCOC COINHIVE D08A862B471E KARAKURT MAGECART MALICIUS N SCANNER" "XTEVE *MFCR* 0895 SCASSC826ATB0D7DE3661101C5C5 E35DF3E00CA4EF3ID42B34BEBAA5 PUNKSPIDER RASPBERRY ROBIN AZORULT BLACKMATTER BOSMON O INBURSA INCREDISERVE INTELX SEQUOIASOFT SPACEX SPRING FF AS208165 AND AS208294 AS6315 FCEVAT DBEF EDF BGGFZCG SHOU "CVE-2021-45105 TAGS HACK F ETERNAL BLUE STRITCHOID CONT TAGS=CVE-2021-44228 LA7ARUS CLASSIFICATION NORDVIA PHIS SEADSFECEA8A5550000584A3588BI BLUE KEEP_MOZI_MYFIELD YEMEP SANDWORM SPYSE AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	WEB D <mark>IGIKALA FAC</mark>	
SHEIN STRIPE_KEY TVILIO_SID ZOMATO ODEBD3363F330C57486 JUPYTERLAB MALICOUS MS15 NEL ONEMED PLEASE LOGIN PUTIN SE D9F35 AAAE2192ECC98DC7EAC450 8080 PROTON VPN RENGINE RÉS FILMAN FORMBOOK GOOGL FACE F CODINOKIBI SPRING COLE, RCE F LIGHT PU LUG4H LOHTI MAGENTO VULNERABLE VYPR WEB_CRAWLER KOSOVA LAVAVEL LIME SCOOTER SALMAN KHAN SHELLY SINKHOLE 220 41352-2022 WILLKOMEN AUF COCCOC COINHIVE D08A862B4718 KARAKURT MAGECART MALICIUS M SCANNER" "XTEVE" *MFCR* 0893 SCA53C326ATB0D7DE 3661101C5C3 E35DF3E00CA4EF31D42B34BEBAA3 PUNKSPIDER RASPSERRY ROBIN AZORULT BLACKMATTER BOSMON O INBURSA INCREDISERVE INTELX SEQUOIASOFT SPACEX SPRING FF AS208169 AND AS208294 AS6317 FCEVAT DEF EDF BGGFZCG SHOU "CVE-2021-45105 TAGS HACK F ETERNAL BLUE STRITCHOID CON TAGS=CVE-2021-44228 LA7ARUS CLASSIFICATION NORDY M PHISP SEADSFECEASA5550000584A3588B0 BLUE KEEP MOZI MYFIELD YEMEN SANDWORM SPYSE AAAAAAAAAAAAAAAAAAAA	SOUNDPOINT SOLAR	
ZOMATO ODEBD3853F330C57486 JUPYTERLAB MALICOUS MS15 NEL ONEMED PLEASE LOGIN PUTIN SE D9F35AAAE2192ECC98DC7FAC450 8080 PROTON VPN RENGINE RÉS FILMAN FORMBOOK GOOGL MACK T SODINOKIBI SPRING CCAE/RCE F LIGHT PD LOG4H LOHAT MAGENTO VULNERABLE VYPR WEB_CRAWLER KOSOVA LAVAVEL LIME SCOOTER SALMAN KHAN SHELLY SINKHOLE 220 41352-2022 WILLKOMEN AUF COCCOC COINHIVE D08A862B471E KARAKURT MAGECART MALICIUS F SCASSC826ATB0D7DE 661101C5C2 E35DF3E00CA4EF3 D42B34BEBAA2 PUNKSPIDER RASPBERRY ROBIN AZORULT BLACKMATTER BOSMON O INBURSA INCREDISERVE INTELX SEQUOIASOFT SPACEX SPRING FF AS208169 AND AS208294 AS631 FCEVAT DBEF EDF BGGFZCG SHOE "CVE-2021-45105 TAGS HACK F ETERNAL BLUE STRETCHOID CONT TAGS=CVE-2021-44228 LAZARUS CLASSIFICATION NORDVO PHISE SFAD5E6CBASA5560DC684A9588BE BLUE KEEP-MOZI MYFIELD YEMEP SANDWORM SPYSE AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	IRESPONSE MASSSO	
JUPYTERLAB MALI COUS MS15 NEL ONEMED PLEASE LOGIN PUTIN SE D9F35AAAE2192EC 98DC7EAC4500 8080 PROTON VPN RENGINE RES FILMAN FORMBOOK GOOGL MACK I SODINOKIBI SPRING COLE RE UIGHT PD LOG4H LOHAT MAGENTO VULNE RABLE VYPR WEB_CRAWLER KOSOVA LAVAVEL IME SCOOTER SALMAN KHAN SHELLY SINKHOLE 220 41352-2022 WILLKOMEN AUF COCCOC COINHIVE D08A862B471E KARAKURT MAGECART MALICIUS N SCANNER" "XTEVE" *MFCR* 0895 SCA53C826ATB0D70E 661101C5C3 E35DF3E00CA4EF31D42B34BEBAA3 PUNKSPIDER RASPBERRY ROBIN AZORULT BLACKMATTER BOSMON O INBURSA TINCREDISERVE INTELX SEQUOIAS OFT SPACEX SPRING FF AS208169 AND AS208294 AS6315 FCEVAT DBEF EDF BGGFZCG SHOU "CVE-2021-45105' TAGS HACK F ETERNAL BLUE STRETCHOID CON TAGS=CVE -2021-44228 LATARUS CLASSIFICATION NORDVX PHISE SEAD55CBASA555CODOS84A9588BE BLUE KEEP MOZI MYFTELD YEMEP SANDWORM SPYSE AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	SHEIN STRIPE_KEY	
ONEMED PLEASE LOGIN PUTIN SE D9F35AAAE2192ECC98DC7EAC4500 8080 PROTON VPN RENGINE RÉSA FILMAN FORMBOOK GOOGL DACK D SODINDKIBI SPRING COLE RCE A LIGHT PD LOG4H LOHAT MAGENTO VULNE RABLE VYPR WEB_CRAWLER KOSOVA LAVAVEL IME SCOOTER SALMAN KHAN SHELLY SINKHOLE 220 4 1352-2022 VILLKOMEN AUF COCCOC COINHIVE D08A862B471E KARAK URT MAGECART MALICIUS N SCANNER" "XTEVE" *MFCR* 0893 SCASSC826ATB0D70E2661101C5C2 E35DF3E00CA4EF3 D42B34BEBAA3 PUNKSPIDER RASPBERRY ROBIN D AZORULT BLACKMATTER BOSMON O INBURSA INCREDISERVE INTELX SEQUOIAS OFT SPACEX SPRING FF AS208169 AND AS208294 AS6317 FCEVAT DBEF EDF BGGFZCG SHOT "CVE-2021-45105" TAGS HACK F ETERNAL BLUE STRETCHOID CONT TAGS=CVE-2021-44228 LA7ARUS CLASSIFICATION NORDVIA PHISF 9EAD556CBA8A5560D0784A9588BT BLUE KEEP MOZI MYFIELD Y MEP SANDWORM SPYSE AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	ZOMAT <mark>O 0DEBD38</mark>	
D9F35AAAF2192EC C98DC7FAC45CC 8080 PROTON VPN RENGINE RÉSA FILMAN FORMBOOK GOOGL FACK SODIN DKIBI SPRING CCAE RCE A LIGHT PD LOG4H LOH41 MAGENTO VULNE RABLE VYPR WEB_CRAWLER KOSOVA LAVAVEL IME SCOOTER SALMAN KHAN SHE LLY SINKHOLE 220 41352-2022 WILLKOMEN AUF COCCOC COINHIVE D08A862B471E KARAKURT MAGECART MALICIUS P SCANNER" "XTEVE *MFCR* 0893 SCASSC826A1B0D77E 0661101C5C2 E35DF3E00CA4EF3 D42B34BEBAA3 PUNKSPIDER RASP BERRY ROBIN AZORULT BLACKMATTER BOSMON O TNBURSA TNCREDISERVE IM ELX SEQUOIAS OFT SPACEX SPRING FF AS208169 AND AS 208294 AS6317 FCEVAT DBEF EDF BGGFZCG SHOT "CVE-2021-45105 TAGS HACK F ETERNAL BLUE STRETCHOID CON TAGS=CVE - 2021-44228 LA7ARUS CLASSIFICATION NORDVIA PHISF PEAD5FC BASA556 0D078 4A9588BT BLUE KEEP MOZI MYFIELD Y MEP SANDWORM SPYSE AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	JUPYTERLAB MALI	
8080 PROTON VPN RENGINE RÉS FILMAN FORMBOOK GOOGL LACK SODINOKIBI SPRING COLE/RCE LIGHT PD LOGAH LOHAI MAGENT VULNERABLE VYPR WEB_CRAWLER KOSOVA LAVAVEL IME SCOOTER SALMAN KHAN SHELLY SINKHOLE 220 41352-2022 WILLKOMEN AU COCCOC COINHIVE D08A862B4716 KARAKURT MAGECART MALICIUS N SCANSC82GATBOD7DE 0661101C5C E35DF3E00CA4EF31D42B34BEBAA3 PUNKSPIDER RASPBERRY ROBIN AZORULT BLACKMATTER BOSMON INBURSA INCREDISERVE INTELX SEQUOIASOFT SPACEX SPRING FR AS208169 AND AS208294 AS631 FCEVAT DBEF EDF BGGFZCG SHOU "CVE-2021-45105" TAGS HACK F ETERNAL BLUE STRETCHOID CON TAGS=CVE-2021-44228 LA7ARUS CLASSIFICATION NORDY A PHIS SEADSDCBA8A55560D0384A3588BE BLUE KEEP MOZI MYFIELD YEMEP SANDWORM SPYSE AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	ONEMED PLEASE LC	
FILMAN FORMBOOK GOOGL FACE SODINOKIBI SPRING COLE RCE LIGHT PD LOGAH LOHAI MAGENTO VULNE RABLE VYPR WEB_CRAWLER KOSOVA LAVAVEL LIME SCOOTER SALMAN KHAN SHELLY SINKHOLE 220 41352-2022 VILLKOMEN AU COCCOC COINHIVE D08A862B4718 KARAKURT MAGECART MALICIUS N SCANNER" "XTEVE" *MFCR* 0893 SCASSC826A1B0D7DE1661101C5C3 E35DF3E00CA4EF31D42B34BEBAA3 PUNKSPIDER RASPBERRY ROBIN AZORULT BLACKMATTER BOSMON TNBURSA INCREDISERVE INTELX SEQUOIASOFT SPACEX SPRING FR AS208169 AND AS208294 AS631 FCEVAT DBEF EDF BGGFZCG SHOU "CVE-2021-45105" TAGS HACK F ETERNAL BLUE STRETCHOID CONT TAGS=CVE-2021-44228 LA7ARUS CLASSIFICATION NORDVON PHISE SFAD5F6CBA8A55560D0584A9588BI BLUE KEEP-MOZI MYFIELD YEMEN SINDWORM SPYSE AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	D9F35AAAE2192EC	
FILMAN FORMBOOK GOOGL FACE SODINOKIBI SPRING COLE RCE LIGHT PD LOGAH LOHAI MAGENTO VULNE RABLE VYPR WEB_CRAWLER KOSOVA LAVAVEL LIME SCOOTER SALMAN KHAN SHELLY SINKHOLE 220 41352-2022 VILLKOMEN AU COCCOC COINHIVE D08A862B4718 KARAKURT MAGECART MALICIUS N SCANNER" "XTEVE" *MFCR* 0893 SCASSC826A1B0D7DE1661101C5C3 E35DF3E00CA4EF31D42B34BEBAA3 PUNKSPIDER RASPBERRY ROBIN AZORULT BLACKMATTER BOSMON TNBURSA INCREDISERVE INTELX SEQUOIASOFT SPACEX SPRING FR AS208169 AND AS208294 AS631 FCEVAT DBEF EDF BGGFZCG SHOU "CVE-2021-45105" TAGS HACK F ETERNAL BLUE STRETCHOID CONT TAGS=CVE-2021-44228 LA7ARUS CLASSIFICATION NORDVON PHISE SFAD5F6CBA8A55560D0584A9588BI BLUE KEEP-MOZI MYFIELD YEMEN SINDWORM SPYSE AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	8080 PROTON VPN	
SODINOKIBI SPRING COLE/RCE / LIGHT PD LOG4H LOH41 MAGENTO VULNERABLE VYPR WEB_CRAWLER KOSOVA LAVAVEL IME SCOOTER SALMAN KHAN SHELLY SINKHOLE 220 41352-2022 WILLKOMEN AU COCCOC COINHIVE D08A862B4718 KARAKURT MAGECART MALICIUS M SCANNER" "XTEVE" *MFCR* 089 SCASSC826ATB0D7DE 0661101C5C3 E35DF3E00CA4EF31D42B34BEBAA3 PUNKSPIDER RASPBERRY ROBIN AZORULT BLACKMATTER BOSMON SEQUOIASOFT SPACEX SPRING FF AS208169 AND AS208294 AS631 FCEVAT DBEF EDF BGGFZCG SHOU "CVE-2021-45105" TAGS HACK F ETERNAL BLUE STRETCHOID CONT TAGS=CVE-2021-44228 LA7ARUS CLASSIFICATION NORDVIA PHISP 9FAD5E6CBA8A5560D0584A35880 BLUE KEEP_MOZI_MYFIELD YEMEP SINDWORM_SPYSE_AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA		
VULNERABLE VYPR WEB_CRAWLER KOSOVA LAVAVEL IME SCOOTER SALMAN KHAN SHELLY SINKHOLE 220 41352-2022 WILLKOMEN AUF COCCOC COINHIVE D08A862B4718 KARAKURT MAGECART MALICIUS N SCANNER" "XTEVE" *MFCR* 0893 SCA53C826ATB0D7DE 0661101C5C2 E35DF3E00CA4EF31D42B34BEBAA2 PUNKSPIDER RASPBERRY ROBIN AZORULT BLACKMATTER BOSMON O INBURSA INCREDISERVE INTELX SEQUOIASOFT SPACEX SPRING FF AS208169 AND AS208294 AS631 FCEVAT DBEF EDF BGGFZCG SHOU "CVE-2021-45105" TAGS HACK F ETERNAL BLUE STRETCHOID CONT TAGS=CVE-2021-44228 LAZARUS CLASSIFICATION NORDVIN PHISP SEAD555CBA8A55560D0284A3588B0 BLUE KEEP MOZI MYFIELD YEMEN SINDWORM SPYSE AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA		
KOSOVA LAVAVEL LIME SCOOTER SALMAN KHAN SHELLY SINKHOLE 220 41352-2022 WILLKOMEN AUE COCCOC COINHIVE D08A862B471E KARAKURT MAGECART MALICIUS F SCANNER" "XTEVE' *MFCR* 0895 SCA53C826A1B0D7DE 661101C5C2 E35DF3E00CA4EF31D42B34BEBAA2 PUNKSPIDER RASPBERRY ROBIN AZORULT BLACKMATTER BOSMON (INBURSA INCREDISERVE INTELX SEQUOIASOFT SPACEX SPRING FF AS208169 AND AS208294 AS6315 FCEVAT DBEF EDF BGGFZCG SHOT "CVE-2021-45105" TAGS HACK F ETERNAL BLUE STRETCHOID CONT TAGS=CVE-2021-44228 LAZARUS CLASSIFICATION NORDV & PHISF 9FAD5F6CBA8A55560D0584A3588BI BLUE KEEP-MOZI MYFIELD YEMEP SINDWORM SPYSE AAAAAAAAAAAAAAAAA	LIGHTIPD LOG4H	OH4I MAGENT
SALMAN KHAN SHELLY SINKHOLE 220 41352-2022 WILLKOMEN AUF COCCOC COINHIVE D08A862B471F KARAKURT MAGECART MALICIUS N SCANNER" "XTEVE" *MFCR* 0893 5CA53C826A1B0D7DE1661101C5C3 E35DF3E00CA4EF31D42B34BEBAA3 PUNKSPIDER RASPBERRY ROBIN AZORULT BLACKMATTER BOSMON (INBURSA INCREDISERVE INTELX SEQUOIASOFT SPACEX SPRING FF AS208169 AND AS208294 AS6311 FCEVAT DBEF EDF BGGFZCG SHOT "CVE-2021-45105" TAGS HACK F ETERNAL BLUE STRETCHOID CONT TAGS=CVE-2021-44228 LA7ARUS CLASSIFICATION NORDV & PHISE SEAD5F5CBA8A55560D0984A9588BE BLUE KEEP-MOZI_MYFIELD YEMEP SINDWORM_SPYSE_AAAAAAAAAAAAAAA	VULNERABLE VYPR	WEB_CRAWLER
220 41352-2022 WILLKOMEN AUG COCCOC COINHIVE D08A862B4718 KARAKURT MAGECART MALICIUS N SCANNER" "XTEVE" *MFCR* 0893 SCA53C826ATB0D7DE 0661101C5C3 E35DF3E00CA4EF31D42B34BEBAA3 PUNKSPIDER RASPBERRY ROBIN AZORULT BLACKMATTER BOSMON O INBURSA INCREDISERVE INTELX SEQUOIASOFT SPACEX SPRING FF AS208169 AND AS208294 AS6313 FCEVAT DBEF EDF BGGFZCG SHOU "CVE-2021-45105" TAGS HACK F ETERNAL BLUE STRETCHOID CONT TAGS=CVE-2021-44228 LAZARUS CLASSIFICATION NORDVIN PHISP 9EAD5E5CBA8A5560D0934A3588BI BLUE KEEP-MOZI MYFIELD YEMEP SANDWORM SPYSE AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA		
COCCOC COINHIVE D08A862B4716 KARAKURT MAGECART MALICIUS F SCANNER" "XTEVE" *MFCR* 089 5CA53C826A1B0D7DE1661101C5C3 E35DF3E00CA4EF31D42B34BEBAA3 PUNKSPIDER RASPBERRY ROBIN AZORULT BLACKMATTER BOSMON C INBURSA INCREDISERVE INTELX SEQUOIASOFT SPACEX SPRING FF AS208169 AND AS208294 AS6311 FCEVAT DBEF EDF BGGFZCG SHOT "CVE-2021-45105" TAGS HACK F ETERNAL BLUE STRETCHOID CONT TAGS=CVE-2021-44228 LAZARUS CLASSIFICATION NORDVIA PHISF 9FAD5F5CBA8A5560D0284A3588B5 BLUE KEER-MOZI-MYFIELD YEMEP SANDWORM SPYSE AAAAAAAAAAAAAAAA	SALMAN KHAN SHEL	
KARAKURT MAGECART MALICIUS N SCANNER" "XTEVE" *MFCR* 0895 SCASSC826A1B0D7DE 661101C5C2 E35DF3E00CA4EF31D42B34BEBAA2 PUNKSPIDER RASPBERRY ROBIN J AZORULT BLACKMATTER BOSMON (INBURSA INCREDISERVE INTELX SEQUOIASOFT SPACEX SPRING FF AS208169 AND AS208294 AS6315 FCEVAT DBEF EDF BGGFZCG SHOT "CVE-2021-45105" TAGS HACK F ETERNAL BLUE STRETCHOID CONT TAGS=CVE-2021-44228 LAZARUS CLASSIFJCATION NORDVIN PHISF 9FAD5F5CBA8A5560D0284A9588BI BLUE KEEP. MOZI MYFIELD YEMEN SANDWORM SPYSE AAAAAAAAAAAAAA UPGUARD BINANCE CNES GNOL HACK IN		
SCANNER" "XTEVE" *MFCR* 0895 SCA53C826A1B0D7DE 0661101C5C5 E35DF3E00CA4EF31D42B34BEBAA5 PUNKSPIDER RASPBERRY ROBIN AZORULT BLACKMATTER BOSMON (INBURSA INCREDISERVE INTELX SEQUOIASOFT SPACEX SPRING FF AS208169 AND AS208294 AS631 FCEVAT DBEF EDF BGGFZCG SHOT "CVE-2021-45105" TAGS HACK F ETERNAL BLUE STRETCHOID CONT TAGS=CVE-2021-44228 LAZARUS CLASSIFICATION NORDVDN PHISF 9FAD5F6CBA8A5560D0584A9588BT BLUE KEEP MOZI MYFIELD YEMET SANDWORM SPLYSE AAAAAAAAAAAAAAA UPGUARD BINANCE CNES GNOL HACK IN	COCCO <mark>C COINHIVE</mark>	
SCASSC826A1B0D7DE 0661101C5C2 E35DF3E00CA4EF31D42B34BEBAA2 PUNKSPIDER RASPBERRY ROBIN 0 AZORULT BLACKMATTER BOSMON 0 INBURSA INCREDISERVE INTELX SEQUOIASOFT SPACEX SPRING FF AS208169 AND AS208294 AS6311 FCEVAT DBEF EDF BGGFZCG SHOT "CVE-2021-45105" TAGS HACK F ETERNAL BLUE STRETCHOID CONT TAGS=CVE-2021-44228 LAZARUS CLASSIFICATION NORDVDN PHISF 9FAD5F5CBA8A5560D0984A9588BI BLUE KEEP MOZI MYFIELD YEMEP SANDWORM SPYSE AAAAAAAAAAAAAA UPGUARD-BINANCE-CNES GVOL HACK IN		
SCASSC826A1B0D7DE 0661101C5C2 E35DF3E00CA4EF31D42B34BEBAA2 PUNKSPIDER RASPBERRY ROBIN 0 AZORULT BLACKMATTER BOSMON 0 INBURSA INCREDISERVE INTELX SEQUOIASOFT SPACEX SPRING FF AS208169 AND AS208294 AS6311 FCEVAT DBEF EDF BGGFZCG SHOT "CVE-2021-45105" TAGS HACK F ETERNAL BLUE STRETCHOID CONT TAGS=CVE-2021-44228 LAZARUS CLASSIFICATION NORDVDN PHISF 9FAD5F5CBA8A5560D0984A9588BI BLUE KEEP MOZI MYFIELD YEMEP SANDWORM SPYSE AAAAAAAAAAAAAA UPGUARD-BINANCE-CNES GVOL HACK IN	SCANN <mark>ER" "XTEVE</mark>	
PUNKSPIDER RASP BERRY ROBIN (AZORULT BLACKMATTER BOSMON (INBURSA INCREDISERVE INTELX SEQUOIASOFT SPACEX SPRING FF AS208169 AND AS 208294 AS631 FCEVAT DBEF EDF BGGFZCG SHOT "CVE-2021-45105" TAGS HACK F ETERNAL BLUE STRETCHOID CON TAGS=CVE-2021-44228 LATARUS CLASSIFICATION NORDVIN PHISF 9FAD5F5CBA8A55560D0984A9588BT BLUE KEEP MOZI MYFIELD YEMEP SANDWORM SPYSE AAAAAAAAAAAAAA UPGUARD BINANCE CNES GNOL HACK IN		
		ERRY ROBIN
	AZORULT <u>B</u> LACKMA	
	INBURSA INCREDIS	
	SEQUOIAS <mark>OFT SPAC</mark>	
	AS208169 AND AS <mark>2</mark>	
	FCEVAT D <mark>BEF EDF</mark>	
	CLASSIF CATION N	
	THE PARTY OF THE PAR	

Days Since The Last KEV Release

https://kev.hrbrmstr.app



It Has Been

	_	_		_	_	_		
								Ş
								P
								K
								Z
								4
								1
								т
								' 5
								0
								N
								C
								F
								K
								0
								F
								E
								S
								Ι
								I E
								I E R
			D = S B					I E R
								I R C

CVE-2024-3273: D-Link Multiple NAS Devices Command Injection CVE-2024-3400: Palo Alto Networks PAN-OS Command Injection

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

- CVE-2024-3272: D-Link Multiple NAS Devices Use of Hard-Coded Credentials