

CISO-Share Office Weekly Newsletter

A very warm welcome to all of you from all of us at the CISO-Share Office.

Here are a few of the articles which caught the attention of the CISO-Share team this week.

Contents

CISO-Share Office Weekly Newsletter	1
Google Warns of Chrome Browser Zero-Day Being Exploited.....	1
The exploited zero-day, tagged as CVE-2024-0519, is described as an out-of-bounds memory access issue in the V8 JavaScript engine.	1
SC3 Daily Threat Summaries and Weekly Report.....	2
CREW Notice	2
Russian APT Known for Phishing Attacks Is Also Developing Malware, Google Warns.....	3
45% of critical CVEs left unpatched in 2023.....	4
Tech Giant HP Enterprise Hacked by Russian Hackers Linked to DNC Breach	5

If you have any questions or comments, please contact us via CISO-Office@hefestis.ac.uk



Google Warns of Chrome Browser Zero-Day Being Exploited

The exploited zero-day, tagged as CVE-2024-0519, is described as an out-of-bounds memory access issue in the V8 JavaScript engine.

Main Article

Google has pushed out an urgent Chrome browser update to fix a trio of high-severity security defects and warned that one of the bugs is already being exploited in the wild.

The exploited zero-day, tagged as **CVE-2024-0519**, is described as an out-of-bounds memory access issue in the V8 JavaScript engine.

As is customary, Google did not provide any additional details on scope of the observed attacks or share telemetry to help defenders hunt for signs of compromise.

Action Point:

The latest [Chrome browser refresh](#) mitigates this exploit and also provides cover for two additional memory safety issues in V8 that are rated high-risk. Google said the update also includes multiple fixes found internally from audits, fuzzing and other initiatives.



SC3 Daily Threat Summaries, CREW Notice and Weekly Report

Please find SC3's daily threat summaries for w/c 22/01/2024 and the vulnerability report for this week, for those who do not receive this information directly.

CREW Notice

Exploitation of vulnerability in Apple products

To draw your attention to a critical vulnerability in the following Apple products that may have come under exploitation by threat actors:

- [iOS 17.3 and iPadOS 17.3](#) - iPhone XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, and iPad mini 5th generation and later
- [iOS 16.7.5 and iPadOS 16.7.5](#) - iPhone 8, iPhone 8 Plus, iPhone X, iPad 5th generation, iPad Pro 9.7-inch, and iPad Pro 12.9-inch 1st generation
- [macOS Sonoma 14.3](#) - Macs running macOS Sonoma
- [macOS Ventura 13.6.4](#) - Macs running macOS Ventura
- [macOS Monterey 12.7.3](#) - Macs running macOS Monterey
- [tvOS 17.3](#) - Apple TV HD and Apple TV 4K (all models)
- [Safari 17.3](#) - Macs running macOS Monterey and macOS Ventura

[CVE-2024-23222](#) is a WebKit confusion issue that attackers could exploit to gain code execution on targeted devices. Successful exploitation enables threat actors to execute arbitrary malicious code on devices running vulnerable iOS, macOS, and tvOS versions after opening a malicious web page. Apple commented that they are "aware of a report that this issue may have been exploited".

These issues are addressed by updating devices to iOS 17.3. Users are encouraged to apply this update immediately.



SC3 - Weekly
vulnerability report - summary



SC3 - Daily threat
summary - 22 January



SC3 - Daily threat
summary - 23 January



SC3 - Daily threat
summary - 24 January



SC3 - Daily threat
summary - 25 January



SC3 - Daily threat
summary - 26 January

Action Point:

A single point of reference for SC3 intelligence each week.



Russian APT Known for Phishing Attacks Is Also Developing Malware, Google Warns

A Russian threat group named ColdRiver, which is known for its phishing attacks, has also been developing custom malware, Google warned on Thursday.

[Main Article](#)

The internet giant has shared [indicators of compromise \(IoCs\) and YARA rules](#) to help defenders detect and analyze the threat.

ColdRiver is tracked by other companies as Star Blizzard, Callisto Group, BlueCharlie, TA446, and Dancing Salome. The group has been linked to a unit of Russia's FSB security service and is known for conducting both cyberespionage operations and influence campaigns.

The hackers typically target organizations in the academia, defense, government, NGO and think tank sectors in the US, the UK and other NATO countries.

Action Point: As always - stay clear of using links and downloads from untrusted sources.

Named **Spica**, the malware has been described as a backdoor written in Rust that uses JSON over websockets for command and control (C&C). Spica can be used to execute arbitrary shell commands, steal web browser cookies, upload and download files, obtain filesystem contents, and exfiltrate documents.

The malware has been delivered by sending targets benign PDFs that appear to be encrypted. When the victim informs the sender that the PDF is encrypted, they are provided an executable that can allegedly be used to decrypt the document. This executable deploys the malware.



45% of critical CVEs left unpatched in 2023

According to a report by Armis, global attack attempts increased by 104% in 2023, targeting various industries and devices.

[Main Article](#)

The report also found that 45% of critical CVEs remained unpatched, exposing organizations to potential exploits. Older Windows server OS versions, end-of-life or end-of-support OSs, and high-profile vulnerabilities like Log4Shell were among the main risk factors.

The report revealed that Chinese and Russian actors were behind many of the attack attempts, especially on manufacturing, educational services and public administration sectors.

The report suggested that organizations should use intelligence to prioritize and remediate critical vulnerabilities, segment legacy technology, and leverage AI-driven technologies to defend and manage the attack surface in real-time.

Action Point:

Ensure that you have a clear and effective process for identifying, testing and applying patches for critical CVEs and other vulnerabilities in a timely manner.

Identify and inventory all the devices and assets connected to your network, and determine which ones are running on outdated or unsupported OSs. Consider upgrading, replacing or isolating these devices to minimize the attack surface.

Implement advanced threat detection and response capabilities to identify and block malicious activities from foreign adversaries. Educate your staff on how to recognize and report phishing and social engineering attempts.

Explore how AI and ML can help you automate and enhance your cybersecurity operations, such as by providing real-time visibility, risk assessment, anomaly detection and incident response.



Tech Giant HP Enterprise Hacked by Russian Hackers Linked to DNC Breach

Hewlett Packard Enterprise (HPE) disclosed that its cloud email environment was breached by a Russian state-sponsored group known as APT29, which exfiltrated data from some of its mailboxes and SharePoint files since May 2023.

Main Article

Microsoft revealed that the same threat actor accessed its corporate systems in November 2023 and stole emails and attachments from its cybersecurity and legal departments. APT29, also called Cozy Bear, BlueBravo, or Nobelium, is believed to be behind the 2016 attack on the Democratic National Committee and the 2020 SolarWinds supply chain compromise.

APT29 is a sophisticated and persistent adversary that poses a serious threat to any organization.

Action Point:

To protect against such attacks, it is recommended to:

- Implement strong identity and access management policies and practices, such as multi-factor authentication, password rotation, and least-privilege principle.

- Monitor and audit network activity and logs for any suspicious or anomalous behaviour, such as unusual login attempts, data transfers, or file modifications.

- Update and patch systems and applications regularly to fix any known vulnerabilities that could be exploited by attackers.

All the best from all of us at **HEFESTIS** and look out for our next **ThreatScape** update next week.

CISO-Share Office Weekly Newsletter

A very warm welcome to all of you from all of us at the CISO-Share Office.



10 Security Metrics Categories CISOs Should Present to the Board

Data security, resilience, and continuity

Financial asset risks and losses

People risks and performance

Supplier risks and performance

IT infrastructure risks and performance

User-controlled device risks and performance

IoT device risks and performance

Application risks and performance

Security validation and testing

Incident detection and response

Action Point:



What Are Ghost Students, and How Do They Operate?

Action Point:



Microsoft Exchange Server Flaw Exploited as a Zero-Day Bug

Action Point:

Extended Protection for Authentication (EPA)



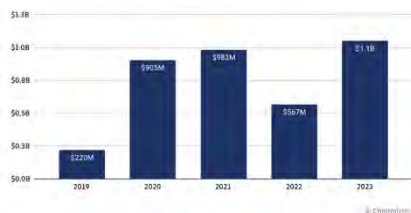
U.S. Government Disrupts Russian-Linked Botnet Engaged in Cyber Espionage

Action Point:



Cybersecurity sectors adjust as DDoS attacks reach new heights

Action Point:



Ransomware Payments Surpassed \$1 Billion in 2023: Analysis

The payments made by victims in response to ransomware attacks doubled in 2023 compared to 2022, according to Chainalysis.

The payments made by victims of ransomware attacks doubled in 2023 compared to the previous year, exceeding \$1 billion, according to blockchain analysis firm Chainalysis.

Action Point:

All the best from all of us at [HEFESTIS](#) and look out for our next [Threatscape](#) update next week.

From: [Lisa Clark](#)
To: [Roddy Mackenzie](#); [Janet Carroll](#)
Subject: FW: Steve McIntosh shared "Threatscape" with you
Date: 19 February 2024 10:48:32
Attachments: [AttachedImage](#)
[AttachedImage](#)
[AttachedImage](#)
[AttachedImage](#)
[AttachedImage](#)
[AttachedImage](#)
[AttachedImage](#)
[AttachedImage](#)
[AttachedImage](#)
[AttachedImage](#)
[AttachedImage](#)
[image001.png](#)

For RMC – thanks.

From: CISO Shared Service - HEFESTIS <CISO-SHARE@JISCMail.AC.UK> **On Behalf Of** Steve McIntosh
Sent: Friday, February 16, 2024 9:52 AM
To: CISO-SHARE@JISCMail.AC.UK
Subject: Steve McIntosh shared "Threatscape" with you



CISO Share

Threatscape

A very warm welcome to all of you from all of us at the CISO-Share Office.

Here are a few of the articles which caught the attention of the CISO-Share team this week.

If you have any questions or comments, please feel free to contact us via CISO-Office@hefestis.ac.uk.

[Weekly digest for w/c 12/02/2024](#)

Main body of text Action Point: Our Weekly Threat Intelligence from SC3



Scottish
Cyber
Coordination
Centre

Steve McIntosh
2/16/2024



[10 Security Metrics Categories CISOs Should Present to the Board](#)

Boards of directors don't care about a security program's minute technical details. They want to see how key performance indicators are tracked and used. Here are the 10 metric areas outlined in the article: Data security, resilience, and continuity...

Steve McIntosh
2/16/2024



[What Are Ghost Students, and How Do They Operate?](#)

Many colleges in the US are facing a problem of fake applicants and enrollees, known as ghost students. These are scammers who use false or stolen identities to get accepted and enrolled in a college, but not for the purpose of learning. They may us...

Steve McIntosh
2/16/2024



[Microsoft Exchange Server Flaw Exploited as a Zero-Day Bug](#)

Microsoft has discovered that a critical vulnerability in Exchange Server, which it fixed in February's Patch Tuesday update, is actually being exploited by attackers in the wild. The flaw, CVE-2024-21410, allows attackers to steal and relay Windows...

Steve McIntosh
2/16/2024



[U.S. Government Disrupts Russian-Linked Botnet Engaged in Cyber Espionage](#)

The U.S. government has disrupted a botnet used by Russian hackers to spy on targets of intelligence interest. The botnet, called MooBot, infected hundreds of routers in the U.S. and allowed the hackers to hide their true location and steal credenti...

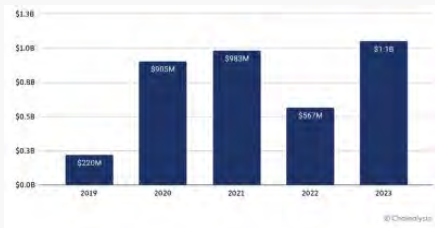
Steve McIntosh
2/16/2024



[Cybersecurity sectors adjust as DDoS attacks reach new heights](#)

In this Help Net Security video, Andrey Slastenov, Head of Security Department at Gcore , discusses the findings of their latest report that provide insights into the current state of the DDoS protection market and cybersecurity trends. Key highligh...

Steve McIntosh
2/16/2024



[Ransomware Payments Surpassed \\$1 Billion in 2023: Analysis](#)

The payments made by victims in response to ransomware attacks doubled in 2023 compared to 2022, according to Chainalysis. Main Article The payments made by victims of ransomware attacks doubled in 2023 compared to the previous year, exceeding \$1 bi...

David Robertson
2/12/2024

[Go To Site](#)

[!\[\]\(1a0ecb0f44016aa353f6ecdd79a3699d_img.jpg\) Get the SharePoint Mobile App](#)

CISO-Share Office Weekly Newsletter

A very warm welcome to all of you from all of us at the CISO-Share Office.

Rise of deepfake threats means biometric security measures won't be enough



Action Point:



3 new ways the Microsoft Intune Suite offers security, simplification, and savings

Enterprise App Management

Advanced Analytics

Cloud PKI

Action Point:



CISA Warns of Active Exploitation Apple iOS and macOS Vulnerability

Action Point:



Ransomware's Impact Could Include Heart Attacks, Strokes & PTSD

First-order harms:

Second-order harms:

Third-order harms:

Action Point:



Juniper Networks Releases Urgent Junos OS Updates for High-Severity Flaws

Action Point:



In Other News: Secure Use of AI, HHS Hacking, CISA Director Swatting

Threat actor selling the data of 15 million Trello members

SecurityWeek

CISA director Jen Easterly target of swatting

Browser-based phishing attacks increase

Ransomware reports

Action Point:

All the best from all of us at **HEFESTIS** and look out for our next **Threatscape** update next week.

CISO-Share Office Weekly Newsletter

A very warm welcome to all of you from all of us at the CISO-Share Office.

Here are a few of the articles which caught the attention of the CISO-Share team this week.

Contents

CISO-Share Office Weekly Newsletter	1
Microsoft Adds Face Check to Entra Verified ID.....	1
SC3 Daily Threat Summaries, CREW Notice and Weekly Report	2
Finance worker pays out \$25 million after video call with deepfake 'chief financial officer'	4
Botnet Attack Targeted Routers: A Wake-Up Call for Securing Remote Employees' Hardware	5
University of Manchester's CISO on Managing Major Cyber Incidents.....	6

If you have any questions or comments, please contact us via CISO-Office@hefestis.ac.uk



Microsoft Adds Face Check to Entra Verified ID

Microsoft has launched a new feature for its Entra Verified ID service, which allows users to prove their identity with verifiable credentials. The feature, called Face Check, uses facial recognition to match a user's live selfie with a trusted identity document, such as a driver's license or a passport. The user's identity is then verified with a confidence score, which is sent to the requesting party.

Main Article

Face Check is designed to enhance the security and privacy of digital identity verification, by preventing account takeover and impersonation attacks. The feature does not store or retain any biometric data or images, and uses Microsoft's Azure AI Face API to perform the facial matching. Face Check is currently available as a free public preview, and will be commercially released later this year.

Entra Verified ID is a decentralized identity (DID) system that leverages standards-based interoperability with other platforms, such as IBM, Workday, Ping, and Mattr. The service enables users to create and issue verifiable credentials for various claims, such as employment, education, certifications, and residence. Microsoft plans to extend the service to support more identity attributes, such as work history and legal entity verification.

Action Points:

Try out Face Check: Users can test the new feature with the Microsoft Authenticator app and see how it works with verifiable credentials.

Learn more about Entra Verified ID: Users can explore the benefits and use cases of the service, and how it integrates with Azure AD and other platforms.

Stay tuned for updates: Users can follow the latest news and developments on Face Check and Entra Verified ID, and provide feedback to Microsoft.



SC3 Daily Threat Summaries, CREW Notice and Weekly Report

Please find SC3's daily threat summaries for w/c 05/02/2024 and the vulnerability report for this week, for those who do not receive this information directly.

CREW Notice - Ivanti Policy Secure (IPS) gateways (CVE-2023-46805, CVE-2024-21887, CVE-2024-21888 and CVE-2024-21893)

With thanks to colleagues at GC3 we are circulating the following update and advice for your information and action where appropriate.

Ivanti had published an updated advisory regarding the vulnerabilities:

Ivanti Connect Secure (ICS) and Ivanti Policy Secure (IPS) gateways (CVE-2023-46805, CVE-2024-21887, CVE-2024-21888 and CVE-2024-21893)

Following on from this update, [NCSC published updated guidance](#) to highlight the key steps to follow. **It is important to note the requirement to perform a factory reset before installing the update.**

SC3 ask that organisations using the affected products, perform the following priority actions:

Action

1. Check for compromise using the detection steps and indicators of compromise (IoCs) detailed in the [Ivanti KB article](#), the [Volexity blog](#) and the [Mandiant blog](#).
2. If you believe you have been compromised and are in the UK, you should [report it to the NCSC](#) and notify us at SC3 (SC3@gov.scot)
3. If an update for your version is not currently available, install the [vendor temporary workaround](#).
4. Monitor the [Ivanti KB article](#) and install the security update once it is available for your version. **You must perform a factory reset before installing the update.**
5. Perform [continuous monitoring and threat hunting](#) activities.

We encourage those potentially affected to [subscribe to Ivanti security bulletins](#) to ensure you are made aware of future updates. If you are unable to adequately protect any Ivanti device, you should consider disconnecting it until it has been reset and updated.

SC3 ask that organisations notify us of the following:

1. If you have found any evidence of compromise (you should also [report to the NCSC](#)).
2. you have successfully performed a factory reset.
3. you have successfully installed the update.
4. If an update is currently unavailable for your version (please also provide the version)
5. We would be grateful if you could confirm to us at SC3 (SC3@gov.scot) once these actions have been implemented.

Negative returns are not required.

Summaries on next page.

Please see below for the critical vulnerabilities reported today:

CVE-2023-34992, CVE-2024-23108 and CVE-2024-23109 – **Fortinet**

FortiSIEM. [More information](#).

CVE-2024-20252 and CVE-2024-20254 - **Cisco Expressway Series** collaboration gateways. [Vendor advisory](#).

CVE-2023-22527 - **Atlassian Confluence**. [Vendor advisory](#)

CVE-2023-40547 – Linux shim, a small piece of code that many major Linux distributors use during the secure boot process. [Advisory](#).

There is also interesting reading about state-sponsored threat actors targeting the Dutch MoD using a remote access trojan (RAT), tracked as **COATHANGER**, which is specifically designed to target Fortigate appliances, and warnings of **Volt Typhoon's** activities in preparing destructive attacks against US critical infrastructure. Please read the [CISA advisory](#) for more details.

Please note the following critical vulnerabilities:

CVE-2024-21762 – an out-of-bounds write vulnerability in **Fortinet FortiOS** that allows unauthenticated attackers to gain remote code execution (RCE) via maliciously crafted requests. Yesterday, Fortinet disclosed that Chinese state-sponsored threat actors known as Volt Typhoon targeted FortiOS vulnerabilities to deploy custom malware known as COATHANGER. [Vendor advisory](#).

CISA also warns of CVE-2023-28654 - a critical vulnerability in Industrial Control System vendor, **ProPump and Controls, Inc.** in equipment, **Osprey Pump Controller**. [CISA advisory](#).

This weeks reports



SC3 - Weekly
vulnerability report - (summary - 5 February)



SC3 - Daily threat
summary - 6 February



SC3 - Daily threat
summary - 7 February



SC3 - Daily threat
summary - 8 February



SC3 - Daily threat
summary - 9 February



SC3 - Daily threat
summary - 9 February

Action Point:

A single point of reference for SC3 intelligence each week.



Finance worker pays out \$25 million after video call with deepfake 'chief financial officer'

What happened: A finance worker at a multinational firm was tricked into paying out \$25 million to fraudsters using deepfake technology to pose as the company's chief financial officer in a video conference call, according to Hong Kong police. The worker

thought he was talking to his colleagues, but they were all fake. The scam was discovered when he checked with the head office.

Main Article

What is deepfake: Deepfake is a technology that uses artificial intelligence to modify or create realistic images and videos of people. It can be used for entertainment, education, or malicious purposes. Deepfake can fool facial recognition programs and human eyes.

What are the risks: Deepfake can be used to impersonate, blackmail, or defame anyone, especially celebrities, politicians, and business leaders. It can also spread misinformation, propaganda, or fake news. Deepfake can erode trust and security in the digital world.

What are the solutions: There are some ways to detect or prevent deepfake, such as looking for inconsistencies, verifying the source, using watermarking, or developing counter-technology. However, these methods are not foolproof and may lag behind the advances of deepfake.

Action Point:

Be vigilant and cautious when dealing with online transactions, especially involving large sums of money or sensitive information.

Do not rely on visual or audio cues alone to verify someone's identity or authenticity. Use other methods, such as passwords, codes, or personal questions.

Report any suspicious or fraudulent activities to the authorities and the relevant platforms or organizations.

Educate yourself and others about the potential and dangers of deepfake. Do not share or spread deepfake content without proper verification or consent.



Botnet Attack Targeted Routers: A Wake-Up Call for Securing Remote Employees' Hardware

The FBI spotted this state-sponsored attack that highlights how home office setups can be overlooked when it comes to employees' cybersecurity.

[Main Article](#)

State-sponsored hackers affiliated with China have targeted small office/home office routers in the U.S. in a wide-ranging botnet attack, Federal Bureau of Investigation Director Christopher Wray [announced](#) on Wednesday, Jan. 31. Most of the affected routers were manufactured by Cisco and NetGear and had reached end-of-life status.

Department of Justice investigators said on Jan. 31, 2024, that the malware has been deleted from affected routers. The investigators also cut the routers off from other devices used in the botnet.

IT teams need to know how to reduce cybersecurity risks that could stem from remote workers using outdated technology.

Action Points: How to reduce cybersecurity risks from botnets for remote workers

The fact that the targeted routers are privately owned highlights a security risk for IT pros trying to keep remote workers safe. With IT members not overseeing the routers used at home, it is difficult to know whether employers may be using old or even end-of-life routers.

[Botnets](#) are often used to launch distributed denial of service attacks or to distribute malware, so defenses against those are important components of a complete defense against botnets. Botnets are typically led by a centralized command and control server.

Organizations should ensure they have good endpoint protection and proactive defenses, such as:

- [security information and event management](#) solutions;

- security orchestration, automation and response solutions (with or without generative AI components), and;

- cybersecurity policies for remote employees.

Software and hardware should be kept up to date, since end-of-life devices are particularly vulnerable. In order to harden devices against being used in botnet attacks, run regular security scans, institute multifactor authentication and keep employees informed about [cybersecurity best practices](#).

"Proactively conducting thorough tech inventories of assets beyond the traditional office is essential," said Demi Ben-Ari, chief technology officer of third-party risk management technology firm Panorays, in an email to TechRepublic. "This approach assists in identifying outdated technology, ensuring that remote workers have up-to-date and secure equipment."

"While remote work introduces potential vulnerabilities due to varied environments, it is important to note that similar attacks could occur in an office setting," Ben-Ari said.



University of Manchester's CISO on Managing Major Cyber Incidents

In June 2023, the University of Manchester became a [victim of a cyber incident](#) in which systems were accessed by an unauthorized party and data compromised. The institution's CISO, Heather Lowrie, had joined as the University's cybersecurity lead just weeks before the cyber-attack and was faced with her first challenge.

[Main Article](#)

With the incident now closed, Lowrie spoke to *Infosecurity* to discuss her main learnings around the response, how to enhance the resiliency of the higher education sector and advice for cyber professionals on fostering collaboration across the industry.

Action Point:

Hopefully this is the precursor to a more in depth case study from UoM who report that the incident is now closed.

All the best from all of us at **HEFESTIS** and look out for our next **ThreatScape** update next week.

CISO-Share Office Weekly Newsletter

A very warm welcome to all of you from all of us at the CISO-Share Office.

Here are a few of the articles which caught the attention of the CISO-Share team this week.

If you have any questions or comments, please contact us via CISO-Office@hefestis.ac.uk

Table of Contents

CISO-Share Office Weekly Newsletter	1
SC3 Daily Threat Summaries and Weekly Report	1
We Are Receiving Reports Of Business Email Compromise (BEC) Attack Attempts Across The HE/FE Sector	2
How Decentralized Identity Is Shaping The Future Of Data Protection	4
LockBit Ransomware's Darknet Domains Seized in Global Law Enforcement Raid	5
Volt Typhoon Disrupts US Organizations, CISA Issues Alerts	6
Recent Zero-Day Could Impact Up to 97,000 Microsoft Exchange Servers	7
The Week in Cyber Security and Data Privacy: 12 – 18 February 2024.....	8



SC3 Daily Threat Summaries and Weekly Report

Please find SC3's daily threat summaries for w/c 19/02/2024 and the vulnerability report for this week, for those who do not receive this information directly.

This weeks reports

				
SC3 - Weekly vulnerability report - summary - 19 Febru	SC3 - Daily threat summary - 19 Febru	SC3 - Daily threat summary - 20 Febru	Daily threat summary-2024-02-2	Daily threat summary-2024-02-

Action Point:

A single point of reference for SC3 intelligence each week.



We Are Receiving Reports Of Business Email Compromise (BEC) Attack Attempts Across The HE/FE Sector

So far there have been no significant incidents from BEC, and all reported events have been appropriately contained, we would like to inform that this type of attack is on the rise. We include an example in the Action Point section from one of our members as to how they have addressed a recent reported BEC event.

***Although the following is not an endorsement of any individual supplier, this advisory information from proofpoint may be helpful in mitigating against this type of attack.**

Main Article

Business email compromise (BEC) is a type of email [cyber crime](#) scam in which an attacker targets a business to defraud the company. Business email compromise is a large and growing problem that targets organisations of all sizes across every industry around the world. BEC scams have exposed organisations to billions of dollars in potential losses.

[Email account compromise](#) (EAC), or email account takeover, is a related threat that is accelerating in an era of cloud-based infrastructure. EAC is often associated with BEC because [compromised accounts](#) are used in a growing number of BEC-like scams (though EAC is also the basis of other kinds of cyber attacks).

BEC and EAC are difficult to detect and prevent, especially with legacy tools, point products and native cloud platform defences.

We Are Receiving Reports Of Business Email Compromise (BEC) Attack Attempts Across The HE/FE Sector (Continued)

Action Point: Although reported incidents appear to be carrying a relatively benign payload, more sophisticated versions of this particular style of phishing/impersonation may be potentially more dangerous.

Here is a recent example from one of our members:

We've seen several cases of BEC style phishing.

IOC:

Sender Address: ****mail066@gmail.com

Subject: Available ?

Context:

Users are emailed from a Gmail address with same name as the person's line manager asking for iTunes/Apple giftcards.

Mitigation steps:

We added the email to the block list

We removed the delivered emails

We added the impersonated user to the "Phishing Impersonation protection policy"

Sample email below:





How Decentralized Identity Is Shaping The Future Of Data Protection

Decentralized identity (DCI) is a new way of managing identity information that gives users more control and privacy. It involves three parties: issuers, holders, and verifiers. Issuers create digital credentials that contain claims about users' attributes, such as date of birth, address, or credit score. Holders store these credentials in their own wallets and choose which claims to share with verifiers. Verifiers check the validity of the credentials and provide access to services based on the claims.

Main Article

DCI has many benefits for cybersecurity, such as reducing the risk of data breaches, fraud, and account takeovers. It also aligns with regulatory frameworks like GDPR and CCPA that aim to protect users' personal data. However, DCI also faces some challenges, such as the impact of AI on authentication, the user experience, and the interoperability of different systems and standards.

Patrick Harding, Chief Architect at Ping Identity, discusses these issues and more in this interview. He explains how DCI is changing the landscape of cybersecurity practices and what organizations need to do to adapt. He also shares his insights on how DCI can enable a sustainable, clean-energy future by leveraging nuclear fusion.

Action Points:

DCI is an evolving field that is influenced by regulatory frameworks, cybersecurity practices, and user expectations. Organizations need to be aware of the opportunities and risks involved in adopting DCI.



LockBit Ransomware's Darknet Domains Seized in Global Law Enforcement Raid

A joint operation by law enforcement agencies from 11 countries, along with Europol, has resulted in the seizure of several darknet domains used by LockBit, a notorious ransomware group. The operation, dubbed Operation Cronos, took advantage of a critical vulnerability in PHP to take over the group's .onion website and its affiliate panel, where they left a message warning the ransomware operators that they have access to their source code, victim data, chat logs, and other evidence.

Main Article

LockBit is one of the most active and dangerous ransomware groups, having claimed more than 2,000 victims and extorted at least \$91 million from U.S. organizations alone. It also topped the list of ransomware groups with the most victims listed on their data leak portal in the last quarter of 2023, according to ReliaQuest.

The seizure of LockBit's domains is a major blow to its operations and follows the disruption of the BlackCat ransomware group by the U.S. government two months ago. It also coincides with the arrest of a Ukrainian hacker who sold access to Google and online bank accounts of American and Canadian users on the dark web. These actions demonstrate the increasing efforts of international law enforcement to combat the growing threat of ransomware and cybercrime.

Action Point:

LockBit exploits known vulnerabilities in Windows systems, so it is important to keep your software up to date and apply security patches regularly.

LockBit often infiltrates networks through phishing emails or compromised credentials. You should train your staff to recognize and avoid suspicious emails and links, and to use strong and unique passwords for their accounts.



Volt Typhoon Disrupts US Organizations, CISA Issues Alerts

Volt Typhoon, a notorious cyber group linked to the People's Republic of China, has expanded its operations beyond illegal access and data theft. This state-backed hacker collective, also known as Vanguard Panda, BRONZE SILHOUETTE, Dev-0391, UNC3236, Voltzite, and Insidious Taurus, has infiltrated the networks of critical infrastructure sectors ranging from aviation to maritime in a strategic bid for future catastrophic cyberattacks.

Main Article

With a [joint advisory](#) from the Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), and Federal Bureau of Investigation (FBI) published on February 7, 2024, exposing their tactics, international collaboration sponsored by these agencies emphasizes the importance of worldwide vigilance against the harmful cyberthreats targeting key systems.

Action Point: Mitigations

Mickey Bresman, CEO of the Active Directory security and recovery platform Semperis, emphasizes the significance of adopting an “assume breach mindset” and establishing strong mitigations to improve the resilience of important systems. He also points out that the ease and frequency with which Volt Typhoon hackers infiltrate and exit networks should raise alarms.

To combat the [network security threats](#) brought by Volt Typhoon, Bresman proposes several critical mitigations:

Assess critical systems: Organizations must identify and prioritize critical systems, including infrastructure such as [Active Directory \(AD\)](#), which is a common target for cyberattacks.

Assume breach mindset: If one compromised environment or malware is detected, there are certainly more to come.

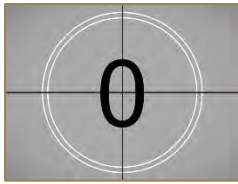
Monitor unauthorized changes: Set up real-time monitoring of AD infrastructure, particularly elevated network accounts and groups.

Perform clean recovery: Back up systems on a regular basis and carry out clean recoveries after any security issues. This entails doing extensive forensics and inspections to guarantee that the environment is clear of compromise.

Conduct forensics investigation: Save the compromised environment for a thorough forensics investigation to determine the scope of the breach and any [vulnerabilities](#).

From Semperis' incident response experiences, state-sponsored actors from nations like China and Russia are relentless in their attempts to compromise networks. There's a growing threat caused by cyber adversaries such as Volt Typhoon. Despite countless warnings over the years, malicious actors have operated with no consequence, emphasizing that organizations should operate under the assumption that their security will be compromised.

The intricate techniques deployed by Volt Typhoon serve as an alarming indicator of the ongoing cybersecurity dangers to our network infrastructures. To keep ahead of harmful actors, stakeholders must remain watchful and constantly improve their security measures while enhancing their [threat intelligence](#).



Recent Zero-Day Could Impact Up to 97,000 Microsoft Exchange Servers

There are more than 28,000 internet-accessible Microsoft Exchange servers affected by a recently disclosed zero-day vulnerability, non-profit cybersecurity organization The Shadowserver Foundation

warned on Monday.

[Main Article](#)

Approximately 68,000 other Exchange instances are considered 'possibly' vulnerable, meaning that they have mitigations installed, which brings the total of potentially exploitable servers to roughly 97,000, Shadowserver says.

The vulnerability, tracked as CVE-2024-21410 (CVSS score of 9.8), is a privilege escalation flaw leading to pass-the-hash attacks, allowing an attacker to relay a user's Net-NTLMv2 hash against a vulnerable server and authenticate as that user.

According to Microsoft, the issue exists because Exchange Server 2019 did not have NTLM credential relay protection, or Extended Protection for Authentication (EPA), enabled by default.

Action Point: Regardless of the actual number of vulnerable Exchange servers, CVE-2024-21410's active exploitation calls for urgent action from organizations, which starts with identifying potentially affected systems and applying the available mitigations and patches as soon as possible.

"Without complete asset inventory visibility, even the most responsive security teams can't patch a vulnerability for an asset they don't know is connected to their network. An accurate, up-to-date asset inventory at the foundation of your security program is essential to mitigating these types of risks," Sevco Security CSO Brian Contos points out in an emailed comment.



The Week in Cyber Security and Data Privacy: 12 – 18 February 2024

ITGovernance report: 402,437,094 known records breached in 240 publicly disclosed incidents.

Main Article

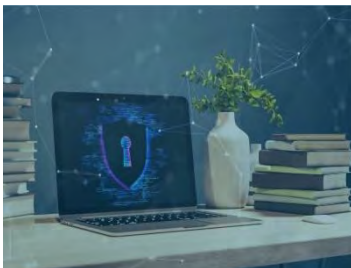
Publicly disclosed data breaches and cyber attacks: full list included within the body of this report.

Action Point: A useful source of information pertaining to the latest cyber attacks and data breaches in one place.

All the best from all of us at **HEFESTIS** and look out for our next **ThreatScape** update next week.

CISO-Share Office Weekly Newsletter

A very warm welcome to all of you from all of us at the CISO-Share Office.



Why Higher Education Is So Vulnerable to Cyber Attacks — And What to Do

Action Point:



Member update: Raised brute force activity against student accounts from Russian sources.

Advisory:

Implement Strong Authentication Mechanisms:

Enforce Strong Password Policies:

Implement Account Lockout Mechanisms:

Monitor and Analyze Login Attempts:

Implement Rate Limiting:

Use CAPTCHA or Human Verification:

Regularly Update and Patch Systems:

Educate Users About Security Best Practices:

Action Point:
Member experience.



NIST CSF 2.0 released, to help all organizations, not just those in critical infrastructure

Action Point:



WordPress Plugin Alert - Critical SQLi Vulnerability Threatens 200K+ Websites

Action Point:



How to Achieve the Best Risk-Based Alerting (Bye-Bye SIEM)

Action Point:

All the best from all of us at **HEFESTIS** and look out for our next **Threatscape** update next week.

From: [Lisa Clark](#)
To: [Roddy Mackenzie](#); [Janet Carroll](#)
Subject: FW: Steve McIntosh shared "Threatscape" with you
Date: 01 March 2024 10:01:24
Attachments: [AttachedImage](#)
[AttachedImage](#)
[AttachedImage](#)
[AttachedImage](#)
[AttachedImage](#)
[AttachedImage](#)
[AttachedImage](#)
[AttachedImage](#)
[AttachedImage](#)
[AttachedImage](#)
[image001.png](#)

For RMC – thanks.

Lisa

From: CISO Shared Service - HEFESTIS <CISO-SHARE@JISCMail.AC.UK> **On Behalf Of** Steve McIntosh
Sent: Friday, March 1, 2024 9:20 AM
To: CISO-SHARE@JISCMail.AC.UK
Subject: Steve McIntosh shared "Threatscape" with you



SharePoint



CISO Share

Threatscape

A very warm welcome to all of you from all of us at the CISO-Share Office.

Here are a few of the articles which caught the attention of the CISO-Share team this week.

If you have any questions or comments, please feel free to contact us via CISO-Office@hefestis.ac.uk.

[Why Higher Education Is So Vulnerable to Cyber Attacks — And What to Do](#)



Cyberattacks pose a serious threat to higher education institutions, which store a lot of sensitive and valuable data. Hackers target schools for various reasons, such as stealing personal information, selling research data, or exploiting outdated s...

Steve McIntosh
3/1/2024



[SC3 Weekly digest for w/c 26/02/2024](#)

Action Point: A single point of reference for SC3 intelligence each week.

Steve McIntosh
2/29/2024



[Member update: Raised brute force activity against student accounts from Russian sources.](#)

Reported by one of our members, there has been raised brute force activity against student accounts from Russian sources. So far all activity has been confidently contained and additionally blocked from spreading by comprehensive MFA. However, vulne...

David Robertson
2/29/2024



[NIST CSF 2.0 released, to help all organizations, not just those in critical infrastructure](#)

The Cybersecurity Framework (CSF) is a guide for managing cybersecurity risks, created by the National Institute of Standards and Technology (NIST). The latest version, 2.0, is suitable for all types of organizations, regardless of their size, secto...

Steve McIntosh
2/27/2024



[WordPress Plugin Alert - Critical SQLi Vulnerability Threatens 200K+ Websites](#)

A popular WordPress plugin called Ultimate Member has a critical security flaw that could expose more than 200,000 websites to SQL injection attacks. The flaw, CVE-2024-1071, has a CVSS score of 9.8 out of 10 and affects versions 2.1.3 to 2.8.2 of t...

Steve McIntosh
2/27/2024



[How to Achieve the Best Risk-Based Alerting \(Bye-Bye SIEM\)](#)

Cybersecurity is a complex and dynamic field that requires constant vigilance and adaptation. One of the most effective ways to enhance your security is to use risk-based alerting, a method that prioritizes alerts based on their potential impact on ...

Steve McIntosh
2/27/2024

[Go To Site](#)

 [Get the SharePoint Mobile App](#)

CISO-Share Office Weekly Newsletter

A very warm welcome to all of you from all of us at the CISO-Share Office.

Here are a few of the articles which caught the attention of the CISO-Share team this week.

If you have any questions or comments, please contact us via CISO-Office@hefestis.ac.uk

Table of Contents

CISO-Share Office Weekly Newsletter	1
SC3 Daily Threat Summaries and Weekly Report.....	1
Anatomy of a BlackCat Attack Through the Eyes of Incident Response	2
Threat Actors Exploit Multiple Vulnerabilities in Ivanti Connect Secure and Policy Secure Gateways.....	3
Apple Fixes Two New iOS Zero-Days Exploited In Attacks On iPhones.....	4
Linux Malware Campaign Targets Misconfigured Cloud Servers	5



SC3 Daily Threat Summaries and Weekly Report

Please find SC3's daily threat summaries for w/c 04/03/2024 for those who do not receive this information directly.

This weeks reports

				
SC3 Daily threat summary-2024-03-01	Daily threat summary-2024-03-01	Daily threat summary-2024-03-01	Daily threat summary-2024-03-01	SC3 Daily threat summary-2024-03-01

Action Point:

A single point of reference for SC3 intelligence each week.



Anatomy of a BlackCat Attack Through the Eyes of Incident Response

Incident response experts at Sygnia provide a detailed blow-by-blow of a BlackCat ransomware attack and share tips for survival. A Supplementary article is included exemplifying a pernicious exit scam tactic also being used by this malicious

group.

[Main Article](#)

[Supplementary Information](#)

Incident response firm Sygnia was contacted by a company to investigate suspect activity on its network. Sygnia rapidly concluded the company was experiencing a ransomware attack and was in imminent danger of having its entire environment encrypted. It recommended immediate and bold action — disconnect from the internet.

The company (which we'll now call the victim) complied. The attack was blocked, and the attacker could neither continue to the encryption phase nor delete its trail. The attacker was BlackCat, and Sygnia now had access to the detailed history and progress of the attack – and has [reported](#) on its analysis.

It was a supply chain attack. The supplier (which we'll now call the vendor) provided technical assistance to the victim — and the entry route for BlackCat. For reasons of customer confidentiality, Sygnia's CEO Ram Elboim declined to give *SecurityWeek* the name of either the victim or the vendor. It has, however, now published a detailed analysis of the progress and outcome of the BlackCat attack.

Action Point:

There are numerous takeaways from this case. Early and expert incident response is always advisable – but in the end, decisiveness and the courage to take drastic steps can save the day, even very late in the day. It is questionable whether the victim would have succumbed to the double extortion of system encryption and more expansive data theft, but if an attack that cannot be prevented can at least be limited to a questionable single extortion attack, survival is more likely.



Threat Actors Exploit Multiple Vulnerabilities in Ivanti Connect Secure and Policy Secure Gateways

The Cybersecurity and Infrastructure Security Agency (CISA) and the following partners (hereafter referred to as the authoring organizations) are releasing this joint Cybersecurity Advisory to warn that cyber threat actors are exploiting previously identified vulnerabilities in Ivanti Connect Secure and Ivanti Policy Secure gateways.

Main Article

CISA and authoring organizations appreciate the cooperation of Volexity, Ivanti, Mandiant and other industry partners in the development of this advisory and ongoing incident response activities. Authoring organizations:

Federal Bureau of Investigation (FBI)

Multi-State Information Sharing & Analysis Center (MS-ISAC)

Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC)

United Kingdom National Cyber Security Centre (NCSC-UK)

Canadian Centre for Cyber Security (Cyber Centre), a part of the Communications Security Establishment

New Zealand National Cyber Security Centre (NCSC-NZ)

CERT-New Zealand (CERT NZ)

Of particular concern, the authoring organizations and industry partners have determined that cyber threat actors are able to deceive Ivanti's internal and external Integrity Checker Tool (ICT), resulting in a failure to detect compromise.

Action Point: Based upon the authoring organizations' observations during incident response activities and available industry reporting, as supplemented by CISA's research findings, the authoring organizations recommend that the safest course of action for network defenders is to assume a sophisticated threat actor may deploy rootkit level persistence on a device that has been reset and lay dormant for an arbitrary amount of time. For example, as outlined in [PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure](#), sophisticated actors may remain silent on compromised networks for long periods.

The authoring organizations strongly urge all organizations to **consider the significant risk** of adversary access to, and persistence on, Ivanti Connect Secure and Ivanti Policy Secure gateways when **determining whether to continue operating** these devices in an enterprise environment.



Apple Fixes Two New iOS Zero-Days Exploited In Attacks On iPhones

Apple has issued emergency security updates to patch two iOS vulnerabilities that were being exploited by attackers. The company said it was aware of a report that the flaws may have been used in attacks.

Main Article

The vulnerabilities affect the iOS Kernel and RTKit, which are components of the operating system that manage memory and audio processing. The bugs could allow attackers to bypass kernel memory protections and gain arbitrary kernel read and write access.

The patches are available for devices running iOS 17.4 , iPadOS 17.4 , iOS 16.76, and iPad 16.7.6. The list of impacted devices includes iPhone XS and later, iPhone 8, iPhone 8 Plus, iPhone X, iPad 5th generation and later, iPad Pro 9.7-inch and later, iPad Air 3rd generation and later, and iPad mini 5th generation and later.

Apple did not disclose who found or exploited the vulnerabilities, or how they were used in attacks. However, iOS zero-days are often used by state-sponsored hackers to target high-profile individuals, such as journalists, politicians, and activists.

This is the third zero-day that Apple has fixed in 2024, after patching one in January. In 2023, the company fixed 20 zero-days that were exploited in the wild.

Action Point:

Apple advises users to install the security updates as soon as possible to protect their devices from potential attacks.



Linux Malware Campaign Targets Misconfigured Cloud Servers

A cryptojacking campaign involving Linux malware is targeting misconfigured Apache Hadoop, Confluence, Docker, and Redis instances with new and unique malicious payloads, cybersecurity firm Cado Security warns.

Main Article

As part of [the campaign](#), the attackers employ four new Golang payloads to automate the discovery and exploitation of vulnerable hosts, as well as a reverse shell and multiple user-mode rootkits to hide their presence.

In attacks targeting Docker, the threat actors used a command to spawn a new container and created a bind mount for the server's root directory that allowed them to write an executable used to establish a connection to the attackers' command-and-control (C&C) and to retrieve a first-stage payload from it.

Action Point:

In attacks targeting Confluence servers, the threat actors were seen exploiting CVE-2022-26134, a critical remote code execution flaw [patched in June 2022](#), when it was already [exploited as a zero-day](#).

"This extensive attack demonstrates the variety in initial access techniques available to cloud and Linux malware developers. It's clear that attackers are investing significant time into understanding the types of web-facing services deployed in cloud environments, keeping abreast of reported vulnerabilities in those services and using this knowledge to gain a foothold in target environments," Cado notes.

All the best from all of us at **HEFESTIS** and look out for our next **ThreatScape** update next week.

From: [CISO Shared Service - HEFESTIS](#) on behalf of [David Robertson](#)
To: CISO-SHARE@JISCMAIL.AC.UK
Subject: David Robertson shared "ThreatScape Newsletter" with you
Date: 08 March 2024 09:19:11
Attachments: [AttachedImage](#)
[AttachedImage](#)
[AttachedImage](#)
[AttachedImage](#)
[AttachedImage](#)
[AttachedImage](#)
[AttachedImage](#)
[AttachedImage](#)
[AttachedImage](#)



CISO Share

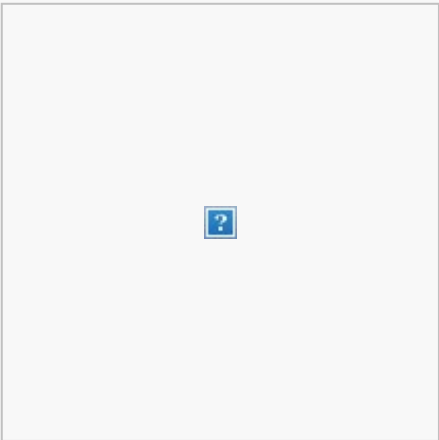
ThreatScape Newsletter

CISO-Share Office Weekly Newsletter

A very warm welcome to all of you from all of us at the CISO-Share Office.

Here are a few of the articles which caught the attention of the CISO-Share team this week.

If you have any questions or comments, please contact us via CISO-Office@hefestis.ac.uk



SC3 Weekly digest for w/c 04/03/2024

SC3 Daily Threat Summaries Action Point: A single point of reference for SC3 intelligence each week.

David Robertson
3/8/2024
2 views

Anatomy of a BlackCat Attack Through the



Eyes of Incident Response

Incident response experts at Sygnia provide a detailed blow-by-blow of a BlackCat ransomware attack and share tips for survival. Main Article Supplementary Information Incident response firm Sygnia was contacted by a company to investigate suspect a...

David Robertson

3/7/2024

2 views



Threat Actors Exploit Multiple Vulnerabilities in Ivanti Connect Secure and Policy Secure Gateways

The Cybersecurity and Infrastructure Security Agency (CISA) and the following partners (hereafter referred to as the authoring organizations) are releasing this joint Cybersecurity Advisory to warn that cyber threat actors are exploiting previously ...

David Robertson

3/7/2024

2 views



Apple fixes two new iOS zero-days exploited in attacks on iPhones

Apple has issued emergency security updates to patch two iOS vulnerabilities that were being exploited by attackers. The company said it was aware of a report that the flaws may have been used in attacks. The vulnerabilities affect the iOS Kernel an...

Steve McIntosh

3/6/2024

2 views

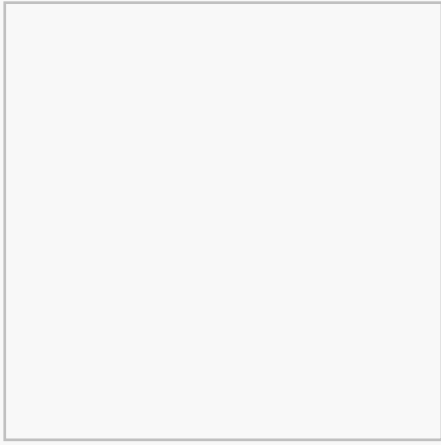
Linux Malware Campaign Targets Misconfigured Cloud Servers

A cryptojacking campaign involving Linux malware is targeting misconfigured Apache Hadoop, Confluence, Docker, and Redis instances with new and unique malicious payloads, cybersecurity firm Cado Security warns. Main Article As part of the campaign ,...

David Robertson

3/7/2024

2 views



[Go To Site](#)



[Get the SharePoint Mobile App](#)



CISO-Share Office Weekly Newsletter

A very warm welcome to all of you from all of us at the CISO-Share Office.



Key MITRE ATT&CK techniques used by cyber attackers

Cloud Account Compromises:

Email Forwarding Rules:

Persistent Threats:

Identity Attacks:

Emerging Techniques:

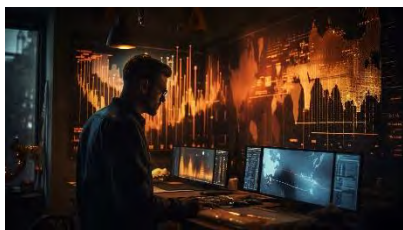
Industry-Specific Targets:

Action Point:



Human risk factors remain outside of cybersecurity pros' control

Action Point:



IT leaders think immutable data storage is an insurance policy against ransomware

Action Point:



Lessons Identified from the British Libraries Cyber Attack

- 1. Enhance network monitoring capabilities**
- 2. Retain on-call external security expertise**
- 3. Fully implement multi-factor authentication:**
- 4. Enhance intrusion response processes**
- 5. Implement network segmentation**
- 6. Practice comprehensive business continuity plans**
- 7. Maintain a holistic overview of cyber-risk:**
- 8. Manage systems lifecycles to eliminate legacy technology**

9. Prioritise remediation of issues arising from legacy technology:

10. Prioritise recovery alongside security

11. Cyber-risk awareness and expertise at senior level

12. Regularly train all staff in evolving risks:

13. Proactively manage staff and user wellbeing:

14. Review acceptable personal use of IT:

15. Collaborate with sector peers:

16. Implement Government standards, review and audit policies and processes regularly

Action Point:

Stanford University failed to detect ransomware intruders for 4 months



Stanford University ransomware attack

27,000 individuals

GB of data Akira 430

Action Point:

Credit Monitoring

ID Theft Recovery



Microsoft's Security Copilot Enters General Availability

Action Point:



17 potential costs of shadow IT

Dealing with Suspected Users:

Legal Expertise:

Employee Prosecution:

Disrupted IT Operations:

Mission-Critical Systems:

Risk Management:

Lost Productivity:

External Tech Support:

Compliance Irregularities:

Higher Insurance Premiums:

Reputational Damage:

Software Incompatibility:

Increased Resource Demand:

Specialized Hardware and Software:

Third-Party Assistance:

Cloud Access Security Broker (CASB):

Infrastructure Reconfiguration:

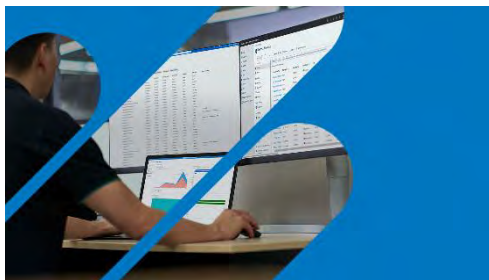
Action Point:

All the best from all of us at **HEFESTIS** and look out for our next **Threatscape** update next week.

*HEFESTIS Limited, Registered Office: Unit 27, Stirling Business Centre, Wellgreen, Stirling
FK8 2DZ
Incorporated in Scotland SC603511*

CISO-Share Office Weekly Newsletter

A very warm welcome to all of you from all of us at the CISO-Share Office.



How Microsoft Incident Response and Microsoft Defender for Identity work together

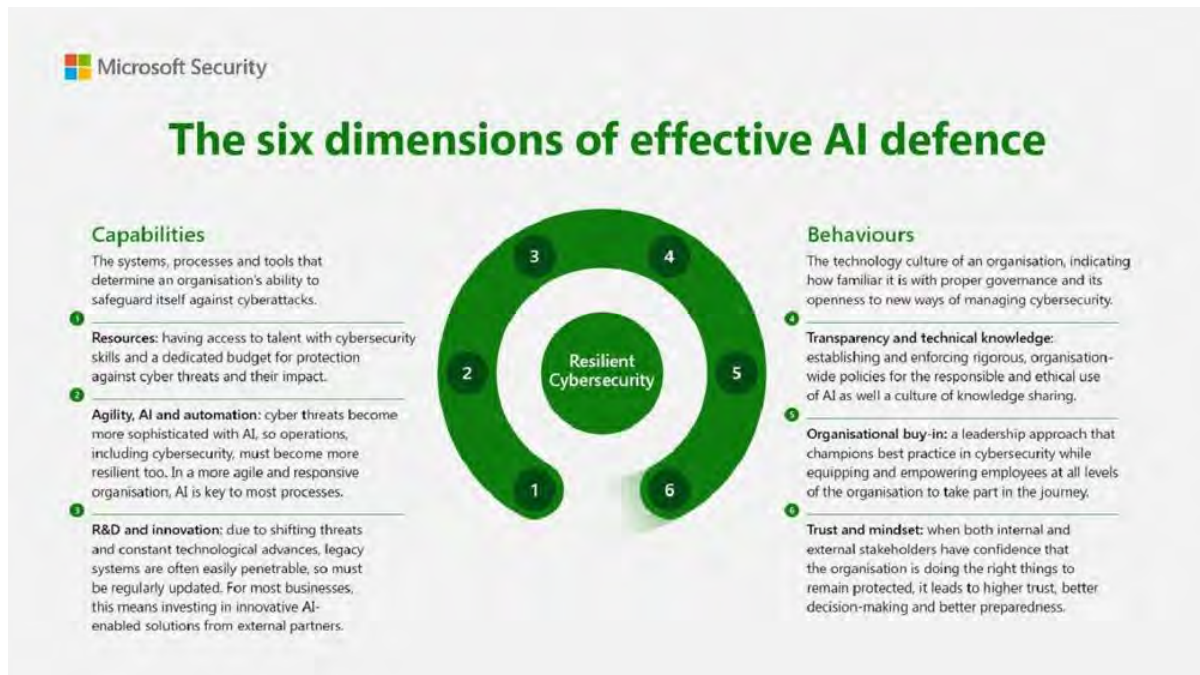


Action Point:



Microsoft: 87% of UK Businesses Are Unprepared for Cyberattacks

Highlights from the Microsoft and Goldsmiths research



Action Point:

Support widespread adoption of AI in cybersecurity:

Target investment:

Cultivate talent:

Foster research and knowledge sharing:

Support simple, safe adoption:



CISA Alerts on Active Exploitation of Flaws in Fortinet, Ivanti, and Nice Products

Action Point:



How New-Age Hackers Are Ditching Old Ethics

Action Point:

maintain vigilance and stay informed

All the best from all of us at **HEFESTIS** and look out for our next **Threatscape** update next week.

*HEFESTIS Limited, Registered Office: Unit 27, Stirling Business Centre, Wellgreen, Stirling
FK8 2DZ
Incorporated in Scotland SC603511*

From: [Lisa Clark](#)
To: [Roddy Mackenzie](#); [Janet Carroll](#)
Subject: FW: Steve McIntosh shared "Threatscape" with you
Date: 28 March 2024 15:08:15
Attachments: [AttachedImage](#)
[AttachedImage](#)
[AttachedImage](#)
[AttachedImage](#)
[AttachedImage](#)
[AttachedImage](#)
[AttachedImage](#)
[AttachedImage](#)
[AttachedImage](#)
[image001.png](#)

For next RMC – thanks.

From: CISO Shared Service - HEFESTIS <CISO-SHARE@JISCMail.AC.UK> **On Behalf Of** Steve McIntosh
Sent: Thursday, March 28, 2024 2:51 PM
To: CISO-SHARE@JISCMail.AC.UK
Subject: Steve McIntosh shared "Threatscape" with you



SharePoint



CISO Share

Threatscape

A very warm welcome to all of you from all of us at the CISO-Share Office.

Here are a few of the articles which caught the attention of the CISO-Share team this week.

If you have any questions or comments, please feel free to contact us via CISO-Office@hefestis.ac.uk.

[How Microsoft Incident Response and Microsoft Defender for Identity work together](#)

Identity-based cyberthreats are on the rise. 2023 saw a tenfold increase in threats including phishing,



ransomware, and more. 50% of Microsoft cybersecurity recovery engagements relate to ransomware, and 61% of all breaches involve credentials. One ...

Steve McIntosh
3/26/2024



[Microsoft: 87% of UK Businesses Are Unprepared for Cyberattacks](#)

A report from Microsoft and Goldsmiths, University of London has found that just 13% of U.K. businesses are resilient to cyberattacks, with 48% deemed vulnerable and the remaining 39% facing high risk. Highlights from the Microsoft and Goldsmiths re...

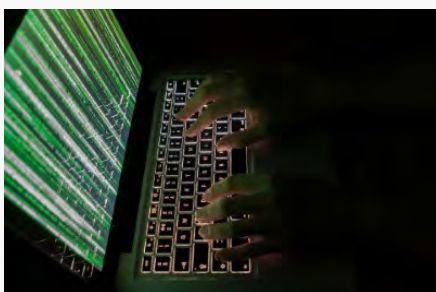
Steve McIntosh
3/26/2024



[CISA Alerts on Active Exploitation of Flaws in Fortinet, Ivanti, and Nice Products](#)

The U.S. Cybersecurity and Infrastructure Security Agency's (CISA) recently added three security flaws to its Known Exploited Vulnerabilities catalog. These vulnerabilities, actively exploited, affect products from Fortinet, Ivanti, and Nice. The fi...

Steve McIntosh
3/26/2024



[How New-Age Hackers Are Ditching Old Ethics](#)

The article discusses the shift in hacker ethics from the original code that respected certain boundaries to a new era where profit is prioritized, leading to more aggressive and unethical cyberattacks. It highlights the changing dynamics of ransomw...

Steve McIntosh
3/26/2024

[SC3 Weekly digest for w/c 25/03/2024](#)

Action Point: A single point of reference for SC3 intelligence each week.



Scottish
Cyber
Coordination
Centre

Steve McIntosh
3/26/2024

Go To Site



[Get the SharePoint Mobile App](#)

CISO-Share Office Weekly Newsletter

A very warm welcome to all of you from all of us at the CISO-Share Office.

Here are a few of the articles which caught the attention of the CISO-Share team this week.

If you have any questions or comments, please contact us via CISO-Office@hefestis.ac.uk

Table of Contents

CISO-Share Office Weekly Newsletter	1
SC3 Daily Threat Summaries and Weekly Report	2
Updated phishing awareness guidance	4
AI: Congress bans staff use of Microsoft's AI Copilot.....	5
XZ backdoor discovery reveals Linux supply chain attack	6
Number of Chinese Devices in US Networks Growing Despite Bans	7
Scathing Federal Report Rips Microsoft for Shoddy Security, Insincerity in Response to Chinese Hack.....	8



SC3 Daily Threat Summaries and Weekly Report

Please find SC3's daily threat summaries for w/c 02/04/2024 for those who do not receive this information directly.

This email has been sent out blind copy to those signed up to receive Cyber Resilience Early Warning Notices (CREW).

Dear all,

We'd like to alert you to a backdoor written into an update in **XZ Utils**, labelled as [CVE-2024-3094](#).

XZ Utils is nearly ubiquitous in Linux. It provides lossless data compression on virtually all Unix-like operating systems, including Linux. XZ Utils provides critical functions for compressing and decompressing data during all kinds of operations. XZ Utils also supports the legacy .lzma format. Malicious code added to XZ Utils versions 5.6.0 and 5.6.1 modified the way the software functions when performing operations related to .lzma compression or decompression. When these functions involved SSH, they allowed for malicious code to be executed with root privileges. This code allowed someone in possession of a predetermined encryption key to log in to the backdoored system over SSH. From then on, that person would have the same level of control as any authorized administrator. The backdoor can allow someone with the right private key to hijack sshd, the executable file responsible for making SSH connections, and from there to execute malicious commands.

The following Linux distributions are affected by the vulnerability:



Fedora Rawhide	https://www.redhat.com/en/blog/urgent-security-alert-fedora-41-and-rawhide-users
Fedora 41	https://www.redhat.com/en/blog/urgent-security-alert-fedora-41-and-rawhide-users
Debian testing, unstable and experimental distributions versions 5.5.1 alpha-0.1 to 5.6.1-1.	https://lists.debian.org/debian-security-announce/2024/msg00057.html
openSUSE Tumbleweed and openSUSE MicroOS	https://news.opensuse.org/2024/03/29/xz-backdoor/
Kali Linux (Discovery supported)	https://www.kali.org/blog/about-the-xz-backdoor/

To check whether your Linux system is affected by the vulnerability:

1. Run the command `xz --version` in your terminal to check the version of XZ Utils installed on your system. If the output shows a version equal to 5.6.0 or 5.6.1, your system may be vulnerable.
2. If your system is running a vulnerable version of XZ Utils, it is crucial to take immediate action by updating your system, especially if you are using a .deb or .rpm-based distribution with glibc. Prioritize updating systems using systemd on publicly accessible SSH ports to mitigate immediate risks.
3. If you suspect your system might have been compromised, you can also review audit logs for any anomalies that could indicate unauthorized access or unusual activities.

Sources:

[CVE-2024-3094- Red Hat Customer Portal](#)

[The XZ Backdoor: Everything You Need to Know | WIRED](#)

[Microsoft releases detailed FAQs about XZ Utils vulnerability in Linux systems - Neowin](#)

[Supply Chain Attack: Major Linux Distributions Impacted by XZ Utils Backdoor - SecurityWeek](#)

This weeks reports



SC3 - Daily threat bulletin - 3 April 2024



SC3 - Daily threat bulletin - 4 April 2024



SC3 - Daily threat bulletin - 5 April 2024

Action Point:

A single point of reference for SC3 intelligence each week.



Updated phishing awareness guidance

We are in the most challenging of times. The evolution of social engineering and phishing styled cyber-attacks is a rising threat enforcing change and inevitably risks disruption to maintaining Higher and Further Education services to staff students and partners, indeed all organisations and individuals in the UK and globally. We

at HEFESTIS hope you are all safe and well.



One area which is booming, however, is cyber-criminal activity. With more of us working from home and relying more than ever on remote working, the opportunity for hackers to unconscionably exploit individuals and organisations via the internet has proven too easy a temptation to resist.

No-one wants to have the disruption of a successful cyber-attack added to already challenging new working restrictions and conditions.

This paper is designed to raise awareness of this insidious and opportunistic form of exploitation during a national emergency and focus on the preferred cyber-attacks of choice phishing and its related partner in cyber-crime social engineering.

Action Point: Viewed through the lens of COVID related methodologies, updates include AI empowered email and phishing information and tips on running an effective anti-phishing campaign.



AI: Congress bans staff use of Microsoft's AI Copilot

The U.S. House has set a strict ban on congressional staffers' use of [Microsoft Copilot](#), the company's AI-based chatbot, Axios has learned.

[Main Article](#)

[More AI news](#)

Why it matters: It's the latest example of the federal government [trying to navigate its internal use of AI](#) while simultaneously attempting to craft regulations for the burgeoning technology.

The House last June [restricted staffers' use](#) of ChatGPT, allowing limited use of the paid subscription version while banning the free version.

Driving the news: The House's Chief Administrative Officer Catherine Szpindor, in guidance to congressional offices obtained by Axios, said Microsoft Copilot is "unauthorized for House use."

"The Microsoft Copilot application has been deemed by the Office of Cybersecurity to be a risk to users due to the threat of leaking House data to non-House approved cloud services," it said.

The guidance added that Copilot "will be removed from and blocked on all House Windows devices."

Action Point: The issue facing the House parallels concerns that [companies have faced](#), with many opting to block access to consumer chatbots like ChatGPT for fear of data leakage.

Many businesses are eyeing or purchasing business versions that come with guarantees that data won't be used to train future models — which opens the risk of data leakage.



XZ backdoor discovery reveals Linux supply chain attack

A maintainer for XZ, a popular open source compression library for Linux distributions, compromised the open source project over the course of two years.

[Main Article](#)

[Additional Information](#)

A backdoor was discovered in a widely used compression library for Linux distributions that could give unauthorized users access to infected systems.

On March 29 Andres Freund, a PostgreSQL developer at Microsoft, revealed he had discovered a backdoor hidden in the open source liblzma package for XZ, a popular compression library used in many Linux distributions. In a disclosure on the Open Source Security Mailing List, Freund wrote that he observed odd behavior in liblzma running on [Debian](#) in recent weeks, such as slow logins via SSH and surprisingly high CPU usage for SSHD processes. After further investigation, he concluded that the upstream XZ repository was compromised in a [supply chain attack](#).

Freund traced the malicious code and discovered the backdoor was committed to the open source project through legitimate-looking updates by an XZ maintainer, later identified as Jia Tan. "Given the activity over several weeks, the committer is either directly involved or there was some quite severe compromise of their system," he wrote in [the disclosure](#). "Unfortunately, the latter looks like the less likely explanation, given they communicated on various lists about the 'fixes' mentioned above."

Freund also found that the backdoor, which is present in XZ Utils versions 5.6.0 and 5.6.1, was contained in only the archived download packages, known as "tarballs," that are released upstream. The malicious code was not present in [Git](#) distributions.

Red Hat noted in a security advisory Friday that the backdoor, which is tracked as CVE-2024-3094 with a CVSS score of 10, is two stages. "The Git distribution lacks the M4 macro that triggers the build of the malicious code," the advisory said. "The second-stage artifacts are present in the Git repository for the injection during the build time, in case the malicious M4 macro is present. Without the merge into the build, the 2nd-stage file is innocuous."

Action Point: Arasaratnam told TechTarget Editorial that for open source security, there are no perfect sets of tools, practices that would have prevented this type of supply chain attack. "We may one day get to a point where we do have open source security capabilities to help secure open source software," he said. "I think that will require an all-hands approach using a tapestry of technologies and processes to help maintainers and consumers stay secure when producing and using digital public goods like open source software."



Number of Chinese Devices in US Networks Growing Despite Bans

An analysis conducted recently by cybersecurity firm Forescout shows that the number of Chinese-manufactured devices present in US networks has been increasing over the past year, despite efforts to prevent the use of such products due to security concerns.

[Main Article](#)

Over the past years, the United States government has taken action to reduce the potential risks posed by the use of products made in China, [banning the sale](#) of communications equipment and [allocating significant amounts of money](#) to help organizations replace Chinese gear in their networks.

A recent executive order focusing on the cybersecurity of US ports highlighted the risks associated with the use of [Chinese cranes](#), with other initiatives targeting [energy-storage batteries](#), and [cars](#) made in China.

Despite these efforts, Forescout's [analysis](#) found that the number of China-made devices in US networks has increased by more than 40% in the past year, from 185,000 in February 2023 to nearly 300,000 in February 2024. The 300,000 devices came from 473 different manufacturers.

This represents close to 4% of the total number of 7.5 million US-located devices currently in Forescout's repository of connected enterprise devices, which includes data on 19 million IT, IoT, OT and IoMT (medical) products from its customers' networks.

Roughly 88% of the Chinese-manufactured devices located in the United States are IT products, followed by IoT (9%), OT (2%) and IoMT (1%). A vast majority of devices are computers, followed at a distance by mobile devices, and surveillance products. The most widely encountered manufacturer is Lenovo, followed by Hikvision.

Forescout warned that critical infrastructure sectors such as healthcare, manufacturing and government are the most impacted. In the case of the government, the most commonly found Chinese devices are surveillance cameras made by Honeywell Security China and VoIP phones from Yealink.

Action Point: As for other countries, Forescout saw an increase from 10,000 China-made devices to 20,000 in the UK over the past year. An increase of 37% was seen in Australia and an increase of 67% was observed in Singapore. A drop of 14% has been seen in Canada, and a drop of 25% was seen in Germany over the past year.



Scathing Federal Report Rips Microsoft for Shoddy Security, Insincerity in Response to Chinese Hack

In a scathing indictment of Microsoft corporate security and transparency, a Biden administration-appointed review board issued a report Tuesday saying “a cascade of errors” by the tech giant let state-backed Chinese cyber operators break into email accounts of senior U.S. officials including Commerce Secretary Gina Raimondo.

Main Article

The [Cyber Safety Review Board](#), created in 2021 [by executive order](#), describes shoddy cybersecurity practices, a lax corporate culture and a lack of sincerity about the company’s knowledge of the targeted breach, which affected multiple U.S. agencies that deal with China.

In all, the state-backed [Chinese hackers broke into](#) the Microsoft Exchange Online email of 22 organizations and more than 500 individuals around the world including the U.S. ambassador to China, Nicholas Burns — accessing some cloud-based email boxes for at least six weeks and downloading some 60,000 emails from the State Department alone, the 34-page report said. Three think tanks and four foreign government entities, including Britain’s National Cyber Security Center, were among those compromised, it said.

Action Point: It concluded that “Microsoft’s security culture was inadequate and requires an overhaul” given the company’s ubiquity and critical role in the global technology ecosystem. Microsoft products “underpin essential services that support national security, the foundations of our economy, and public health and safety.”

All the best from all of us at **HEFESTIS** and look out for our next **ThreatScape** update next week.

CISO-Share Office Weekly Newsletter

A very warm welcome to all of you from all of us at the CISO-Share Office.

Here are a few of the articles which caught the attention of the CISO-Share team this week.

If you have any questions or comments, please contact us via CISO-Office@hefestis.ac.uk

Table of Contents

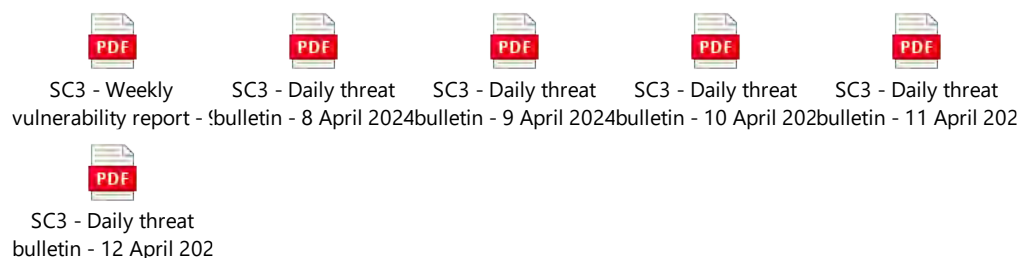
CISO-Share Office Weekly Newsletter	1
SC3 Daily Threat Summaries and Weekly Report.....	1
Microsoft's Security Chickens Have Come Home to Roost.....	2
Thousands of Ivanti VPN Appliances Impacted by Recent Vulnerability.....	3
U.K. and U.S. Agree to Collaborate on the Development of Safety Tests for AI Models	4
Member Article.....	5
In Other News: 100,000 Affected by CISA Breach, Microsoft AI Copilot Ban, Nuclear Site Prosecution.....	6



SC3 Daily Threat Summaries and Weekly Report

Please find SC3's daily threat summaries for w/c 08/04/2024 for those who do not receive this information directly.

This weeks reports



Action Point:

A single point of reference for SC3 intelligence each week.



Microsoft's Security Chickens Have Come Home to Roost

The US government's public documentation of Microsoft's shoddy cybersecurity practices, lax corporate culture and untruthfulness in public communications should come as no surprise to anyone.

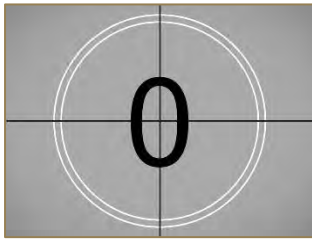
[Main Article](#)

There were dark patterns everywhere. For years, we collectively [groaned and rolled our eyes](#) as Microsoft shipped [faulty](#) and [incomplete patches](#), gutted its Patch Tuesday bulletins into irrelevance, [fought with hackers](#) reporting security problems, and made [baffling trade-offs](#) around cybersecurity transparency.

Even the ['/security'](#) page, for years used as a place to simplify the distribution of security warnings, mitigation guidance and software patches, morphed into a landing page to hawk Microsoft's newly "AI-powered" cybersecurity products.

Action Point: For those deeply entrenched in Microsoft's world, security costs can add up significantly, especially for granular logging to help with security incident detection, investigation, and response. "This course of business should stop," the CSRB notes, arguing that security-related logging should be a core element of cloud offerings.

The CSRB report is a remarkable document providing a blow-by-blow into one of the most daring APT attacks in history against a company that somehow blew a decade's worth of goodwill and completely lost its way in security.



Thousands of Ivanti VPN Appliances Impacted by Recent Vulnerability

Researchers at the Shadowserver Foundation have identified thousands of internet-exposed Ivanti VPN appliances likely impacted by a recently disclosed vulnerability leading to remote code execution.

[Main Article](#)

The vulnerability, tracked as CVE-2024-21894 (CVSS 8.2), is described as a heap overflow bug in the IPSec component of Ivanti Connect Secure (formerly Pulse Connect Secure) and Policy Secure that could be exploited by remote, unauthenticated attackers to cause a denial-of-service (DoS) condition or execute arbitrary code.

On April 2, Ivanti [released](#) software updates to address this flaw and three other vulnerabilities in its two VPN appliances, including CVE-2024-22053, another high-severity heap overflow bug leading to DoS.

The issue impact all supported versions of Connect Secure and Policy Secure and Ivanti has urged all users to update their instances, albeit noting that it was not aware of these bugs being exploited at the time of disclosure.

Action Point:

Ivanti has found itself reeling from a spate of zero-day attacks that recently threw its security response teams into disarray and forced the US government to issue disconnection instructions. The company says it is now [embarking on a makeover](#) of the entire cybersecurity organization.



U.K. and U.S. Agree to Collaborate on the Development of Safety Tests for AI Models

The U.K. government has formally agreed to work with the U.S. in developing safety tests for advanced AI models.

The U.K. government has formally agreed to work with the U.S. in [developing tests for advanced artificial intelligence models](#). A [Memorandum of Understanding](#), which is a non-legally binding agreement, was signed on April 1, 2024 by the U.K. Technology Secretary Michelle Donelan and U.S. Commerce Secretary Gina Raimondo.

Main Article

Both countries will now “align their scientific approaches” and work together to “accelerate and rapidly iterate robust suites of evaluations for AI models, systems, and agents.” This action is being taken to uphold the commitments established at the first global [AI Safety Summit](#) last November, where governments from around the world accepted their role in safety testing the next generation of AI models.

Action Point:

With the MoU, the U.K. and U.S. have agreed how they will build a common approach to AI safety testing and share their developments with each other. Specifically, this will involve:

- Developing a shared process to evaluate the safety of AI models.
- Performing at least one joint testing exercise on a publicly accessible model.
- Collaborating on technical AI safety research, both to advance the collective knowledge of AI models and to ensure any new policies are aligned.
- Exchanging personnel between respective institutes.
- Sharing information on all activities undertaken at the respective institutes.
- Working with other governments on developing AI standards, including safety.



Member Article

We want to bring to your attention an incident involving an [.]is domain within email signatures.

An incident involving a compromised domain within email signatures, such as "[.]is," could potentially be indicative of various types of cyberattacks, including:

1. **Phishing Attack:** Cybercriminals may have compromised the domain to host phishing pages or distribute phishing emails through the compromised email signatures. Phishing attacks typically involve tricking users into divulging sensitive information or credentials by impersonating legitimate entities.
2. **Malware Distribution:** The compromised domain could be used to distribute malware, such as ransomware, trojans, or spyware, via malicious links or attachments embedded in the email signatures. Malware distribution attacks aim to infect users' devices and compromise their security.
3. **Credential Harvesting:** Attackers may utilize the compromised domain to host fake login pages or forms designed to steal users' credentials. This type of attack, known as credential harvesting or credential theft, can lead to unauthorized access to users' accounts and sensitive information.
4. **Watering Hole Attack:** In a watering hole attack, attackers compromise websites frequented by their target audience, such as a specific organization or industry group. By compromising the domain within email signatures, attackers may attempt to lure targeted individuals or organizations to the compromised site, where they could be exposed to further exploitation.
5. **Domain Spoofing:** The incident involving the compromised domain within email signatures could also be a result of domain spoofing, where attackers impersonate legitimate domains to deceive recipients and gain their trust. Domain spoofing attacks are commonly used in phishing campaigns to make malicious emails appear legitimate.

Actions taken.

Due to a potential compromise, emails containing this domain were flagged as phishing by Microsoft and subsequently deleted as part of automated remediation measures.

Further incoming emails with this domain were also quarantined as a precautionary measure.

To address this issue, the organisation took immediate action to block the domain using defender IOC and FortiGate, limiting access as much as possible while ensuring continued mail flow. Subsequently, all deleted emails were restored.

While there remains a residual risk, particularly for users accessing the link on unmanaged or external devices, this risk assessed and accepted as low given the nature of the link not being a typical phishing call to action.

Action Point:

Please note that the current status of the (anonymised) domain suggests that it may have been recovered by the owner or a third party, but it is not yet operational.



In Other News: 100,000 Affected by CISA Breach, Microsoft AI Copilot Ban, Nuclear Site Prosecution

Here are this week's stories:

[Main Article](#)

100,000 people affected by CISA breach

The cybersecurity agency CISA told lawmakers that the recent breach involving its Chemical Security Assessment Tool (CSAT) could affect [over 100,000 individuals](#). The incident involved exploitation of an Ivanti product vulnerability. While the incident is 'major' based on FISMA's definition, CISA found no evidence that the hackers actually stole data, and the agency said the incident did not have any operational impact, despite forcing it to shut down some systems.

US House bans use of Microsoft AI Copilot

The US House has [banned](#) the use of Microsoft's Copilot AI chatbot by congressional staffers due to it potentially leaking data to non-approved cloud services. Microsoft is working on a suite of AI tools designed for government use, which the tech giant hopes will address data exposure concerns.

UK nuclear waste site to be prosecuted over cybersecurity failures

The UK's Office for Nuclear Regulation (ONR) has informed the Sellafield nuclear waste and decommissioning site that it will be [prosecuted](#) over alleged IT security offenses that occurred between 2019 and early 2023. The move comes a few months after it was reported that threat actors linked to Russia and China had [hacked](#) into Sellafield systems. The ONR said there was no indication that public safety was compromised as a result of the issues.

Action Point: Lessons learned from electrical grid security exercise and more in the full article.

All the best from all of us at **HEFESTIS** and look out for our next **ThreatScape** update next week.
