# Daily Cyber Headlines

**Daily Cyber Headlines** **TLP:WHITE** **Alert Id: 47c3e419** **2023-10-02 10:32:30**

**Today's Headlines:**

**Leading Story**
- Microsoft Breach Led to Theft of 60,000 US State Department Emails

**Data Breaches & Data Leaks**
- Nothing to Report

**Cyber Crimes & Incidents**
- Novel ZenRAT Scurries Onto Systems via Fake Password Manager Tool
- ShinyHunters Member Pleads Guilty to $6 Million in Data Theft Damages

**Vulnerabilities & Exploits**
- Millions of Exim Mail Servers Exposed to Zero-Day RCE Attacks
- Hackers Set Sights on Apache NiFi Flaw That Exposes Many Organizations to Attacks

**Trends & Reports**
- FBI Warns Energy Sector of Likely Increase in Targeting by Chinese, Russian Hackers

**Privacy, Legal & Regulatory**
- US National Security Agency Unveils Artificial Intelligence Security Center

**Upcoming Health-ISAC Events**
- Americas Hobby Exercise - October 25, 2023. Registration is available here.
- Health-ISAC Monthly Threat Brief – October 31, 2023, 12:00 PM Eastern

## Leading Story

Microsoft Breach Led to Theft of 60,000 US State Dept Emails

**Summary**
- The United States State Department has suffered a data breach that resulted in the theft of tens of thousands of emails.

**Analysis & Action**

The United States State Department has suffered a massive breach in Microsoft's Exchange email platform. Approximately 60,000 unclassified emails primarily focusing on Indo-Pacific diplomacy efforts have been stolen, including a list containing all the department's email accounts.

No classified systems were breached. According to Microsoft, the company has attributed these attacks to a Chinese cyber-espionage group known as Storm-0558. Threat actors were able to breach the Microsoft accounts by exploiting a previously patched zero-day validation vulnerability.

Members are encouraged to familiarize themselves with the tactics, techniques, and procedures (TTPs) of Storm-0558 to avoid becoming the victim of cyber espionage activity.

## Data Breaches & Data Leaks

- Nothing to Report.

## Cyber Crimes & Incidents

### Novel ZenRAT Scurries Onto Systems via Fake Password Manager Tool

**Summary**

- Windows users are being targeted by information-stealing malware.

**Analysis & Action**

According to Dark Reading, information-stealing malware called ZenRAT has been exclusively targeting Windows users by hiding behind fake installation packages of the password manager, Bitwarden.

Threat actors used a very convincing lookalike domain to mimic Bitwarden's authentic domain to distribute packages of hidden ZenRAT malware to Windows users. The malware itself collects system identification data, installed applications data, and steals passwords from browsers to send back to threat actors through a command-and-control (C2) server.

Members are encouraged to only download software through trusted third parties or validated sources to reduce the risk of inadvertently installing information-stealing malware on corporate devices.

### ShinyHunters Member Pleads Guilty to $6 Million in Data Theft Damages

**Summary**

- 22-year-old Sebastien Raoult has been arrested for his participation in the ShinyHunters cybercriminal group.

**Analysis & Action**

A 22-year-old named Sebastien Raoult was apprehended last year in Morocco and has pleaded guilty to conspiracy to commit wire fraud and aggravated identity theft. Raoult and his other co-conspirators, under the ShinyHunters alias, would steal corporate and consumer data and would sell it on various cybercriminal forums, marketplaces, and Telegram channels.

ShinyHunters was observed ransoming private data for up to $425,000. Raoult and his group used a wide range of tactics, techniques, and procedures (TTPs) to gain access to private corporate information. One such tactic was creating phishing sites that mimicked login sites of legitimate businesses. There, the threat actors were able to steal login credentials and use them to gain access to other private corporate information in the same network.

Members are encouraged to employ multifactor authentication (MFA) to reduce the risk of threat actors gaining access via obtaining login credentials to access private information.

## Vulnerabilities & Exploits

### Millions of Exim Mail Servers Exposed to Zero-Day RCE Attacks

**Summary**

- A new critical zero-day vulnerability was recently discovered affecting all versions of the Exim mail transfer agent (MTA).

**Analysis & Action**

The newly found remote code execution (RCE) flaw affects all versions of the Exim mail transfer agent (MTA).

The vulnerability, tracked as CVE-2023-42115, could allow unauthenticated attackers to gain remote code execution (RCE) on Internet-exposed servers. The flaw is a result of out-of-bounds write weaknesses found in the SMTP service. Exim is a highly vulnerable target because of its internet exposure and can be an easy entry point for attackers into a network.

The NSA (National Security Agency) has previously reported on Russian military threat actor Sandworm exploiting one of Exim's flaws.

A patch is currently not available for the said flaw; however, users are advised to restrict remote access from the internet to prevent exploitation as a temporary workaround.

### Hackers Set Sights on Apache NiFi Flaw That Exposes Many Organizations to Attacks

**Summary**

- Researchers have uncovered a high-severity flaw affecting Apache NiFi, with available public exploit code.

**Analysis & Action**

Apache NiFi, an open-source data integration and automation tool is affected by a remote code execution (RCE) vulnerability.

The vulnerability tracked as CVE-2023-34468 has a CVSS (Common Vulnerability Scoring System) score of 8.8 and, could allow authenticated users to configure a database URL to be vulnerable to custom code execution. In the event of a successful attack, the threat actor could gain access to sensitive files and could execute code remotely.

The flaw is affecting NiFi versions 0.0.2 through 1.21.0 and was addressed in the newest NiFi version 1.22.0. Security experts have discovered a discussion among threat actors on dark web forums about plans to exploit the vulnerability. While there have been no recorded exploitations to date, publicly shared exploit code is available.

## Trends & Reports

FBI Warns Energy Sector of Likely Increase in Targeting by Chinese, Russian Hackers

**Summary**

- The FBI issued a warning about the probable increase in energy sector targeting by Chinese and Russian state-backed entities.

**Analysis & Action**

Chinese and Russian state actors are expected to intensify their attacks on critical energy infrastructure in the United States.

This is expected as a result of certain geopolitical developments and resulting changes in the global energy supply chain, such as an increase in US liquefied natural gas exports, changes in the global crude oil supply chain favoring the US, ongoing Western sanctions on Russia affecting its energy revenues, and China's reliance on oil imports. The warning does not identify any specific APT but rather is the consequence of trends detected over time, as well as ongoing efforts by Chinese and Russian hackers to analyze important systems and gaps in networks.

We recommend that members have an offline data backup as well as generators to ensure that critical equipment such as ventilators or incubators can continue to operate even if a local power system is successfully attacked.

**Privacy, Legal & Regulatory**

US National Security Agency Unveils Artificial Intelligence Security Center

**Summary**

- The United States National Security Agency (NSA) has announced the creation of an artificial intelligence security center to monitor AI capabilities in U.S. defense and intelligence services.

**Analysis & Action**

On Thursday, the NSA announced that it was aware of the increasing importance of AI in the national security landscape and the new center will help to maintain the advantage the U.S. has in AI development.

The new AI center will be incorporated into the NSA’s Cybersecurity and Collaboration Center and will promote the secure adoption of new AI capabilities across the national security and defense industry base. Cybersecurity researchers claim that China has recently stepped up cyber operations focused on US and allied institutions that may disrupt military communications.

As the US continues to tackle the emerging benefits and disadvantages of AI, members should be on the lookout for new rules and regulations regarding the use of AI.

## Health-ISAC Cyber Threat Level

On September 20, 2023, the Health-ISAC Threat Intelligence Committee (TIC) evaluated the current Cyber Threat Level and collectively decided to maintain the Cyber Threat Level at Blue (Guarded).

The Threat Level of Blue (Guarded) is due to threats from concerns regarding malvertising, rogue USB drives, Async RAT, MFA Bypass, and persistent credential stuffing/spraying.

**For more information about the Health-ISAC Cyber Threat Level, including definitions and response guidelines for each of the alert levels, please review the Threat Advisory System.**

**You must have Cyware Access to reach the Threat Advisory System document. Contact membership@h-isac.org for access to Cyware.**

**Reference(s):** Al Jazeera, Bleeping Computer, Bleeping Computer, Security Week, The Record, Health-ISAC , Bleeping Computer, Dark Reading

**Tags:** ZenRAT, ShinyHunters, Microsoft

**TLP:WHITE:** Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

### Share Threat Intel:

For guidance on sharing indicators with Health-ISAC via CSAP, please visit the Knowledge Base article CSAP ■Share Threat Intel■ Documentation at the link address provided here: https://health-isac.cyware.com/webapp/user/knowledge-base Additionally, this collaborative medium provides opportunities for attributed or anonymous sharing across ISACs and other cybersecurity-related entities.

### Turn off Categories:

For guidance on disabling this alert category, please visit the Knowledge Base article CSAP "Alert Categories" Toggle Documentation at the link address provided here: https://health-isac.cyware.com/webapp/user/knowledge-base

### Access the Health-ISAC Intelligence Portal:

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.

### For Questions or Comments:

Please email us at toc@h-isac.org