# Daily Cyber Headlines

Daily Cyber Headlines | TLP:WHITE | Alert ID : d349b232 | Oct 17, 2024, 07:50 AM

**Today's Headlines:**

**Leading Story**

- Iranian Hackers Act As Brokers Selling Critical Infrastructure Access

**Data Breaches & Data Leaks**

- Varsity Brands Data Breach Impacts 65,000 People
- Hackers Target Ukraine's Potential Conscripts With MeduzaStealer Malware

**Cyber Crimes & Incidents**

- North Korean Threat Actors Use Newly Discovered Linux Malware To Raid ATMs

**Vulnerabilities & Exploits**

- Microsoft Patches Vulnerabilities in Power Platform, Imagine Cup Site
- North Korean ScarCruft Exploits Windows Zero-Day To Spread RokRAT Malware

**Trends & Reports**

- FIDO Alliance Proposes New Passkey Exchange Standard

**Privacy, Legal & Regulatory**

- Nothing to Report

**Upcoming Health-ISAC Events**

- Global Monthly Threat Brief
  - Americas – October 29, 2024, 12:00-01:00 PM ET

    - European – October 30, 2024, 03:00-04:00 PM CET
- T-SIG Webinar for SMB Members – November 14, 2024 at 11:30 AM ET
- European Summit, Athens, Greece - October 15-17, 2024
- Fall Americas Summit, Phoenix, Arizona - December 2-6, 2024

**Additional Information**

**Leading Story**

Iranian Hackers Act As Brokers Selling Critical Infrastructure Access

**Summary**

- Iranian threat actors are breaching critical infrastructure organizations to sell stolen credentials and network data on cybercrime forums.

**Analysis & Action**

On October 16, 2024, a joint Cybersecurity Advisory involving numerous authoring agencies was released. The advisory warned that Iranian threat actors were assessed to be acting as initial access brokers using brute force techniques to gain access to organizations across many sectors.

Citing observed activity from October 2023, the advisory informs that Iranian threat actors often press on in their effort to steal more credentials and identify other sensitive information that could be used to obtain additional points of access.

It is assessed that Iranian threat actors sell this information on cybercriminal forums to actors who may use it to conduct additional malicious operations.

Health-ISAC encourages organizations to implement the security measures in the mitigations section of the joint Cybersecurity Advisory for protection against the observed malicious activity, available here.

**Data Breaches & Data Leaks**

## Varsity Brands Data Breach Impacts 65,000 People

**Summary**

- The apparel company Varsity Brands notified individuals of a data breach that disclosed personal information.

**Analysis & Action**

Varsity Brands informed the Maine Attorney General's Office about unusual activity identified on their systems in May 2024. The apparel firm launched an investigation into the incident and discovered that an intruder obtained a subset of company files that contained personal information impacting over 65,000 people.

Varsity Brands' brief description of the incident suggests it may have been targeted in a ransomware attack; however, no credit has been taken by any ransomware group, and no ransom payments have been confirmed at the time of reporting.

Health-ISAC recommends that organizations implement strong access controls, regularly update software, and educate employees on cybersecurity best practices to prevent data breaches.

## Hackers Target Ukraine's Potential Conscripts With MeduzaStealer Malware

**Summary**

- MeduzaStealer malware is used to target draft-aged men's devices as malware spreads through Telegram.

**Analysis & Action**

Russian threat actors often took advantage of the MeduzaStealer malware, using it to obtain various information such as computer information, browsing history, password manager data, and login credentials. In the last year, UAC-500, a threat actor, deployed the malware to work maliciously on its Polish and Ukrainian targets.

MeduzaStealer malware has been deployed by an unidentified threat actor, using Telegram accounts masked as technical support bots. The threat actors used a Ukrainian government app by the name of Reserve+, which launched earlier in the year. After posing as customer support for the app, actors would upload ZIP archives with instructions on updating personal data that is under requirements

by military officials in Ukraine. These files then target any device that has MeduzaStealer, incrementally stealing documents and then self-deleting to avoid detection. Though the threat actor has yet to be identified, this is a common tactic used by threat actors linked to Russia, previously exploiting messengers and mobile apps, including Telegram.

Attacks utilizing messaging services to distribute malicious malware are a common practice used by threat actors, putting importance on the need for the security of one's data. Health-ISAC recommends its members to enable spam filters and list identifiable points of contact on Do Not Call Registries to prevent similar instances from taking place.

## Cyber Crimes & Incidents

### North Korean Threat Actors Use Newly Discovered Linus Malware To Raid ATMs

**Summary**

- North Korean threat actors have compromised Windows infrastructure and are now expanding to include Linux systems.

**Analysis & Action**

Research has identified that the malware is being tracked as FASTCash. The banking infrastructure that the threat actors compromised ran IBM's proprietary version of Unix, which goes by the name AIX.

The malware used by North Korean threat actors is a remote access tool. The tool is able to exploit compromised networks and retrieve payments that have been installed on payment switches handling card transactions on payments. Warnings of AIX were first brought to light in 2018 within an advisory regarding payment networks in retail stores. Research has since found two samples of the malware running on Linux. The first sample was on Ubuntu Linux 20.04, while the other sample has shown no evidence of being used at this time. Additionally, the Linux version of the malware was uploaded to VirusTotal in June 2023.

Health-ISAC recommends using SSH key authentication and keeping security enhancement and enforcement mode enabled on any susceptible Linux devices to mitigate the risk of similar attacks on vulnerable systems.

## Vulnerabilities & Exploits

### Microsoft Patches Vulnerabilities in Power Platform, Imagine Cup Site

**Summary**

- Microsoft recently patched vulnerabilities affecting Power Platform, Dataverse, and the Imagine Cup website.

**Analysis & Action**

Microsoft patched a critical vulnerability, tracked as CVE-2024-38190, in their Power Platform. The low-code platform for managing apps, workflows, and AI tools had a missing authorization flaw that could have exposed sensitive information to unauthenticated threat actors.

Additionally, Microsoft released updates for CVE-2024-38139, which impacts the Dataverse platform. Dataverse, a component of the Power Platform, allows users to store and manage data securely. The security flaw is caused by an improper authentication issue that could allow authenticated threat actors to elevate privileges.

Lastly, Microsoft addressed CVE-2024-38204 which affects their Imagine Cup website. Imagine Cup is a competition for student startup founders using AI technologies. Prior to the fix, the vulnerability allowed for an improper access control issue that threat actors could use to gain elevated privileges.

Health-ISAC encourages organizations to implement robust vulnerability management programs that identify and assess weaknesses efficiently to help bolster their security apparatus.

### North Korean ScarCruft Exploits Windows Zero-Day to Spread RokRAT Malware

**Summary**

- Links have been identified to recently patched zero-day exploitation security flaws and ScarCruft, a North Korean threat actor.

**Analysis & Action**

The threat actor, ScarCruft, is based in North Korea, where recent events have seen it deploy its malware, RokRAT. Though the security flaw has since been patched as of August 2024, intel on the threat actor continues to emerge as investigations continue.

The previously attacked vulnerability was marked as CVE-2024-38178 and has additionally received a CVS score of 7.5. This vulnerability involved a bug causing corruption in the engine's scripting. This bug could lead to remote code execution when one is using Microsoft's Edge browser, specifically in Internet Explorer mode. The attack generated from convincing users to click on URLs, successful instances would then execute malicious code. A pop-up notification advertisement program that tandems with free software is what has since been characterized by the zero-day attack. In the attacks, PCs were infected, and vulnerable toast (pop-up notifications) were installed, subjecting victims to remote access and other malicious activities. RokRAT, the threat actor malware, terminates processes, issues remote code execution, enumerates files and gathers data from a number of browsers. In the past, the threat actor has also been known to exploit other vulnerabilities like CVE-2020-1380, and CVE-2022-41128, bringing attention to the threat actor's history and experience.

Health-ISAC recommends that its members utilize trusted antivirus software and pop-up blocking services to mitigate the risks of falling victim to similar attacks.

## Trends & Reports

### FIDO Alliance Proposes New Passkey Exchange Standard

**Summary**

- The FIDO Alliance proposed a new passkey initiative allowing users to securely move them across devices.

**Analysis & Action**

With the rapid and widespread adoption of passkeys by users seen for major services, including Apple, Google, and Microsoft, the Fast Identity Online (FIDO) Alliance wants to make the login option less siloed across different providers.

Passkeys are assessed to be a safer authentication method as they cannot be stolen in data breaches, phishing attacks, or by malware, like usual credentials. However, one downside regarding using passkeys is that they currently do not allow users to transfer them across different platforms and password managers.

As a result, the FIDO Alliance has drafted specifications that include the Credential Exchange Protocol (CXP) and the Credential Exchange Format (CXF). These initiatives provide a standard format for transferring credentials in a password manager, including passwords and passkeys, to another provider in a secure manner. Health-ISAC recommends implementing the latest security protections to ensure organizations remain resilient to risks associated with the threat landscape.

**Privacy, Legal & Regulatory**

- Nothing to Report

**Health-ISAC Cyber Threat Level**

On September 19, 2024, 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:

The Threat Level of Blue (Guarded) is due to threats from DPRK IT fraud, elections-induced cyber activity, potential repercussions of recent activity in the Middle East, potential Ivanti Endpoint Manager exploitation, and ongoing observances of infostealer's logs being posted on Telegram.

**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.**

**Report Source(s)**

Health-ISAC

**Incident Date**

Oct 17, 2024, 11:59 PM

**Reference | References**

**cisa**
**Infosecurity Magazine**
**Bleeping Computer**
**Security Week**
**Security Week**
**The Record**
**Red Packet Security**
**Ars Technica**

**Tags**

FIDO, StarCruft, MeduzaStealer

**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 HTIP, please visit the Knowledge Base article "HTIP - Share Threat Intel" here.

The "Share Threat Intel" feature allows for attributed or anonymous sharing across ISACs and other cybersecurity-related entities.

**Turn off Categories:**

For guidance on disabling alert categories, please visit the Knowledge Base article "HTIP Alert Categories" here.

**Access the Health-ISAC Threat 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 Health-ISAC Threat Intelligence Portal (HTIP).

**For Questions or Comments:**

Please email us at toc@h-isac.org