# Daily Cyber Headlines

Daily Cyber Headlines | TLP:WHITE | Alert ID : 89fe021c | Oct 16, 2024, 07:26 AM

**Today's Headlines:**

**Leading Story**

- CISA Warns of Active Exploitation in SolarWinds Help Desk Software Vulnerability

**Data Breaches & Data Leaks**

- Volkswagen Says IT Infrastructure Not Affected After Ransomware Gang Claims Data Theft

**Cyber Crimes & Incidents**

- SideWinder APT Hackers Added New Post-Exploitation Toolkit To Their Arsenal
- ExoneraTor Tool Detects IP Address Linked With Tor Network, Uncovers Volt Typhoon

**Vulnerabilities & Exploits**

- Splunk Enterprise Update Patches Remote Code Execution Vulnerabilities

**Trends & Reports**

- Amazon Says 175 Million Customers Now Use Passkeys to Log in

**Privacy, Legal & Regulatory**

- Finland Seizes Servers of Sipultie Dark Web Drug Market

**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**

CISA Warns of Active Exploitation in SolarWinds Help Desk Software Vulnerability

**Summary**

- CISA added a critical SolarWinds Web Help Desk (WHD) vulnerability to its known exploited vulnerabilities catalog.

**Analysis & Action**

The Cybersecurity and Infrastructure Security Agency (CISA) added a critical security flaw, tracked as CVE-2024-28987, to its known exploited vulnerabilities catalog due to evidence of active exploitation.

The vulnerability has a CVSS score of 9.1 and stems from hard-coded credentials that could be abused by a threat actor to gain unauthorized access and make modifications. Initially disclosed in late August 2024, security researchers at Horizon3.ai also provided additional technical details regarding CVE-2024-28987.

After successfully exploiting the vulnerability, a threat actor can remotely read and modify help desk ticket details which typically contain sensitive data. Health-ISAC released a vulnerability bulletin titled Critical Hardcoded Credential Vulnerability (CVE-2024-28987) in SolarWinds Web Help Desk.

Organizations should patch vulnerable SolarWinds Web Help Desk instances to prevent any potential exploitation activity. For additional information, including recommendations, see the full alert here.

**Data Breaches & Data Leaks**

## Volkswagen Says IT Infrastructure Not Affected After Ransomware Gang Claims Data Theft

**Summary**

- Volkswagen advises that their IT infrastructure has remained unaffected after the 8Base ransomware threat actor claimed to have stolen data.

**Analysis & Action**

Volkswagen recently released a public statement advising that its IT systems were not affected after the 8Base ransomware threat actor claimed to have stolen data. The Volkswagen Group advises that it will continue to monitor the situation closely.

The ransomware gang claims to have stolen invoices, receipts, accounting documents, personal data, certificates, employment contracts, personnel files, and a substantial amount of sensitive information.

The 8Base ransomware gang has seasoned operators active since early 2023, claiming more than 400 victims on its data leak site. Health-ISAC recommends that organizations implement robust security controls and efficiently identify gaps or vulnerabilities that must be resolved to minimize their attack surface.

## Cyber Crimes & Incidents

## SideWinder APT Hackers Added New Post-Exploitation Toolkit To Their Arsenal

**Summary**

- Researchers have observed a large expansion to SideWinders capabilities with a new StealerBot toolkit.

**Analysis & Action**

Security researchers discovered a new toolkit for post-exploitation, which allows the SideWinder threat actor to conduct stronger espionage activities.

SideWinder, which is also identified as Rattlesnake or T-APT-04, has been active since 2012 and is believed to be state-sponsored in India. The main targets of the threat actors are those of government entities or military units in Southeast Asian countries. Their new toolkit, named StealerBot, contains various capabilities, including installing malware, logging keystrokes, stealing passwords, exfiltrating files, executing bypasses, and intercepting remote desktop credentials.

The threat actor's chain of infection often originates with a phishing email containing malicious ZIP archives of Microsoft Office documents. These infections exploit vulnerabilities like CVE-2017-11882, for example, in which JavaScript stages are deployed along with .NET downloaders, allowing StealerBot to be downloaded.

Developing new toolkits like this brings attention to the need for proper security practices to protect data. Health-ISAC recommends deploying multi-factor authentication and adding spam filters within emails to mitigate the risks of phishing.

## ExoneraTor Tool Detects IP Address Linked With TorNetwork, Uncovers Volt Typhoon

**Summary**

- A tool named ExoneraTor has uncovered Chinese state-sponsored threat actor Volt Typhoon activity via detecting IP addresses.

**Analysis & Action**

The tool ExoneraTor specializes in verifying IP addresses and their association with the Tor network for specific dates. With this tool, Volt Typhoon was uncovered, providing greater visibility to researchers and law enforcement to investigate Tor-involved online activities.

The tool's functionality revolves around querying historical data for Tor relays. These could be middle relays, entry guards, or exit nodes, to name a few. Users can input an IP address and date into the system and determine if the traffic involved a Tor relay.

Health-ISAC recommends considering implementations of behavioral analysis of systems, and advanced detection of anomalies to mitigate risks of these threats to network environments.

## Vulnerabilities & Exploits

### Splunk Enterprise Update Patches Remote Code Execution Vulnerabilities

**Summary**

- Splunk recently released updates for several vulnerabilities affecting Splunk Enterprise.

**Analysis & Action**

Of the eleven vulnerabilities, the most severe is CVE-2024-45733, which has a CVSS score of 8.8. This vulnerability is an insecure session storage configuration flaw that allows users without appropriate roles to execute code remotely. Those who do not run Splunk Web are not impacted.

Versions 9.2.3 and 9.1.6 provide fixes for CVE-2024-45733, an arbitrary file write security flaw that can allow remote code execution (RCE). Splunk Enterprise version 9.3.1 also includes patches for this flaw.

Splunk identified several other vulnerabilities and released detections for most. Health-ISAC recommends updating affected infrastructure related to the Splunk vulnerabilities and reviewing their security advisories page for additional information.

## Trends & Reports

### Amazon Says 175 Million Customers Now Use Passkeys to Log in

**Summary**

- Amazon announced observing a large increase in the adoption of passkeys since their release and implementation a year ago.

**Analysis & Action**

After rolling out passkeys as a login option, Amazon reported that over 175 million customers have adopted the security feature. Passkeys are digital credentials tied to biometric controls or PINs and stored on devices such as phones, computers, and USB security keys.

The authentication feature uses cryptographic keys, both public and private, to act as credentials tied to a biometric feature or PIN when logging into a service. Private keys are stored securely on a device's secure chip while the online service receives only the public key. The implementation of passkeys is assessed to be a safer authentication method as they cannot be stolen in data breaches, phishing attacks, or by malware, like usual credentials.

Passkeys are not portable to other devices; however, the Fast Identity Online (FIDO) alliance announced a new specification that makes them transferable across different platforms and password managers. Health-ISAC recommends that organizations routinely assess and identify what layered security approaches are feasible for their business objectives and resiliency to potential threats.

## Privacy, Legal & Regulatory

### Finland Seizes Servers of Sipultie Dark Web Drugs Market

**Summary**

- The Finnish Customs office took down and seized the servers for a darknet marketplace site used for selling illegal narcotics anonymously.

**Analysis & Action**

An illicit narcotics darknet marketplace known as Sipulitie was recently taken down, and the Finnish Customs Office seized its servers. According to its operator, the site churned out 1.3 million Euros (approximately $1.42 million) and was frequented by both Finnish and English-speaking users.

The international operation was successful due to collaborative efforts by the Finnish Customs, Europol, the Swedish police, Polish law enforcement authorities, and researchers at Bitdefender.

The takedown of Sipultie comes almost four years after its predecessor, Sipulimarket, was brought down in December 2020. Sipulimarket also generated large monetary value and was created by the same administrator. The Finnish Customs Office has identified the main operators, moderators, and users of the marketplaces, and arrests will be announced soon.

**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 16, 2024, 11:59 PM

**Reference | References**

**Bleeping Computer**
**Bleeping Computer**
**The Hacker News**
**cybersecuritynews**
**cybersecuritynews**
**Security Week**
**Health-ISAC Threat Advisory System**

**Tags**

Splunk, SideWinder, SolarWinds

**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