# Daily Cyber Headlines

Daily Cyber Headlines | TLP:WHITE | Alert ID : f52d7585 | Oct 21, 2024, 06:40 AM

**Today's Headlines:**

**Leading Story**

- Omni Family Health Data Breach Impacts 468,344 Individuals

**Data Breaches & Data Leaks**

- Tech Giant Nidec Confirms Data Breach Following Ransomware Attack

**Cyber Crimes & Incidents**

- Microsoft Lost Some Customers' Cloud Security Logs

**Vulnerabilities & Exploits**

- Microsoft Reveals macOS Vulnerability That Bypasses Privacy Controls In Safari Browser
- Severe Flaws in E2EE Cloud Storage Platforms Used by Millions

**Trends & Reports**

- 68% of Healthcare Workers Experienced A Supply Chain Attack
- Microsoft Creates Fake Azure Tenants to Pull Phishers Into Honeypots

**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
- Fall Americas Summit, Phoenix, Arizona - December 2-6, 2024

**Additional Information**

**Leading Story**

Omni Family Health Data Breach Impacts 468,344 Individuals

**Summary**

- California-based Omni Family Health notified individuals that their personal information was compromised in a data breach.

**Analysis & Action**

On August 7, 2024, Omni Family Health discovered the security breach after claiming that information was stolen from its systems and leaked on the dark web. The organization is a healthcare provider that offers many services, including primary care, dental care, behavioral health, and preventative services.

According to the data breach notification, the healthcare provider launched an investigation into the matter shortly after being informed about the claims. The investigation revealed that the data breach may have exposed various information types for current and former patients. These include names, addresses, Social Security numbers, dates of birth, health insurance details, and medical information.

Omni Family Health informed the US Department of Health and Human Services that 468,344 individuals were impacted. The Hunters International ransomware gang claimed responsibility for the incident and stated they stole 2.7 terabytes of data upon listing the organization on their data leak site. The stolen information was later released on August 23, 2024. Health-ISAC recommends that organizations implement strong access controls, regularly update software, and educate employees on cybersecurity best practices to prevent data breaches.

**Data Breaches & Data Leaks**

## Tech Giant Nidec Confirms Data Breach Following Ransomware Attack

**Summary**

- Nidec Corporation disclosed data stolen in a ransomware attack suffered earlier this year was leaked on the dark web.

**Analysis & Action**

Earlier this year, the Japanese tech giant Nidec Corporation suffered a ransomware attack that compromised sensitive data. According to Nidec, the threat actors attempted to extort them, but they did not pay any ransom. Subsequently, the sensitive data stolen during the ransomware attack was leaked to the dark web.

The cyberattack targeted the Nidec Precision division in Vietnam, which specializes in manufacturing optical, electronic, and mechanical equipment for the photography industry. According to an internal investigation, the threat actors retrieved an employee's valid VPN account credentials and accessed a server containing confidential information.

The investigation also revealed that the threat actors stole 50,694 files, including internal documents, letters from business partners, green procurement, labor safety and health policies, business documents, and contracts. Cyberattacks can be extremely damaging, requiring organizations and their partners to act quickly to remediate the issue. Health-ISAC recommends implementing comprehensive incident response plans that enable organizations to act in a timely manner to eradicate existing threats.

## Cyber Crimes & Incidents

## Microsoft Lost Some Customers' Cloud Security Logs

**Summary**

- Cloud security logs for multiple weeks, relied on by customers to spot possible cyber intrusions, have been lost in recent Microsoft reports.

**Analysis & Action**

Microsoft has lost customer-utilized cloud security logs. The company notified all affected earlier in the month. Reports from the company claim that a security compromise was not a cause of the incident.

Rather, the company stated that the cause of the incident was the internal monitoring agent and a bug within it. This bug was triggered, and a fix was implemented within the log collection according to a post-incident review. The bug, however, created a malfunction within several agents once log data was uploaded to the internal logging platform. The issue was then temporarily resolved with a periodical restart of the server or agent and restarting the collection process of logs. Though this fix has been acted on, some of the affected log data is unrecoverable and lost for good. Several services were affected, creating incomplete logs for Azure Logic Apps, Healthcare APIs, Monitor, Trusted Signing, Microsoft Sentinel and Entra, and Power Platform.

Complete logs remain crucial as they are needed for incident responders to do their jobs. Health-ISAC recommends addressing data inventories and sensitive data locations to weaken the potential of being affected by similar events in the future.

## U.S. and Allies Warn of Iranian Cyberattacks on Critical Infrastructure In Year-Long Campaign

**Summary**

- A cyberattack campaign spanning a year in length has been warned about by Canada, Australia, and the United States for its brute-force attacks.

**Analysis & Action**

Iranian threat actors have helmed the campaign, using password spraying and brute force to gain access to the accounts of users and organizations in various fields.

Fields targeted in these attacks include government, engineering, information technology, healthcare, and energy sectors. Additionally, the threat actors have utilized prompt bombing with multi-factor authentication to gain access to networks of their interest. These methods would flood users with MFA push notifications, prompting the user to approve the requests due to annoyance, a process known as MFA fatigue. Information and credentials are being sold as the end goal of the attacks, giving access to other threat actors. After access is gained through means of reconnaissance of the network and systems, a vulnerability marked CVE-2020-1472 with a CVSS score of 5.5 can be used to increase privileges. Certain cases pertaining to the attacks use msedge.exe, in which an outbound connection will be established to Cobalt Strike C2 infrastructure.

Health-ISAC recommends its members consider using phishing resistant MFA as a mechanism to prevent methods of push bombing going forward. Additionally, setting limits on account login attempts can prevent brute force attacks from transpiring, locking out threat actors after several failed attempts.

## Vulnerabilities & Exploits

### Microsoft Reveals macOS Vulnerability That Bypasses Privacy Controls In Safari Browser

**Summary**

- Recent Microsoft announcements detail a prior security flaw within the Apple TCC framework that has likely been exploited.

**Analysis & Action**

The security flaw disclosed by Microsoft has since been patched in macOS Sequoia 15.

The vulnerability, tracked as CVE-2024-44133, was given the codename HM Surf by Microsoft. HM Surf malicious activity involved removing Transparency, Consent, and Control (TCC) protections within Safari's browser directories. From here, the vulnerability would alter a configuration file within the directory, receiving information including user data. This data included locations, microphone activity, browsed pages, and even the camera of the user's device. Further research addresses macOS adware by the name of AdLoad as a likely proponent of the exploit of the vulnerability.

The commonality of these methods used by threat actors highlights the need for security measures against attacks utilizing similar techniques.

Health-ISAC recommends that its members use trusted antivirus software to scan future downloads for malware.

### Severe Flaws in E2EE Cloud Storage Platforms Used by Millions

**Summary**

- Researchers reveal vulnerabilities affecting multiple end-to-end encrypted (E2EE) cloud storage instances.

**Analysis & Action**

Researchers from ETH Zurich discovered via cryptographic analysis that end-to-end encrypted (E2EE) cloud storage instances, including Sync, pCloud, Icedrive, Seafile, and Tresorit services, were vulnerable.

The analysis focused on a threat actor who could manipulate data from a malicious server to read, modify, and inject data arbitrarily.

ETH Zurich contacted the cloud storage providers about the vulnerabilities that had been discovered. Sync, pCloud, Seafile, and Icedrive were notified on April 23, 2024, while Tresorit was contacted on September 27, 2024.

Each of the cloud storage providers addressed the disclosures differently, as some informed that they have taken appropriate action while others have not. Health-ISAC recommends that organizations utilize vendor risk assessments to evaluate third-party vendors and suppliers. This will help ensure that the third party meets the organization's security standards and mitigate potential risks.

## Trends & Reports

### 68% of Healthcare Workers Experienced A Supply Chain Attack

**Summary**

- After analysis and survey were conducted, concerns were put into play regarding cyberattacks' effects on healthcare organizations.

**Analysis & Action**

A recent report from Proofpoint found that 92% of organizations experienced cyberattacks in the last 12 months, a 4% increase from the year prior. Additionally, 69% of incidents were reported to disrupt patient care.

Common cyberattacks like supply chain attacks, cloud compromises, ransomware, and email compromise have created struggles within healthcare organizations in the past years, with 56% reporting poor patient outcomes due to an attack. Amongst concerns by medical staff are those of insecure mobile apps and a means for stronger posture to their cybersecurity teams. However, organizations have begun to address these issues by administering employee training programs. Additionally, 54% of survey respondents' organizations utilize AI within their patient care systems and cybersecurity. With numerous data losses/exfiltrations, ransomware attacks, and other forms of malicious acts by threat actors, this recent push to bolster protection will likely improve both physical and network security in healthcare organizations in the coming years.

Health-ISAC recommends using encryption methods to prevent threat actors from following through with means of data exfiltration and protecting sensitive data. Additionally, the use of firewalls and trusted antivirus software can weaken the chances of ransomware attacks, detecting and scanning malicious cyber threats.

## Microsoft Creates Fake Azure Tenants to Pull Phishers Into Honeypots

**Summary**

- Microsoft is implementing fake Azure tenants as honeypots to lure threat actors.

**Analysis & Action**

A Microsoft principal security software engineer created a hybrid high-interaction honeypot using decommissioned infrastructure to collect threat intelligence spanning from novice cybercriminals to sophisticated threat groups targeting Microsoft.

Microsoft is taking a proactive approach by visiting active phishing sites identified by Defender and typing in credentials from the honeypot tenants. The accounts purposely do not have two-factor authentication enabled and contain seemingly authentic information.

Microsoft intends to leverage the collected data to analyze malicious infrastructure, analyze phishing operations in depth, disrupt campaigns, identify threat actors, and throttle their activity. Leveraging honeypots as a defensive measure can provide several benefits.

Health-ISAC recommends using them to observe threat actor behavior and tactics while keeping critical production systems secure.

**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 21, 2024, 11:59 PM

**Reference | References**

**The Hacker News**
**Bleeping Computer**
**Bleeping Computer**
**Bleeping Computer**
**Security Magazine**
**Help Net Security**

**Security Affairs**
**feedly**

**Tags**

Honeypots, macOS, 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 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