DAILY CYBER HEADLINES

Daily Cyber Headlines

TLP:WHITE

Oct 20, 2025

Today's Headlines:

Leading Story

- Threat Actors Exploit Cisco SNMP Flaw to Deploy Rootkit on Switches

Data Breaches & Data Leaks

- Marketing and Email Platform Exposed Over 40 Billion Records Online

Cyber Crimes & Incidents

- Beware of Fake LastPass Hack Emails Trying To Trick Users Into Installing Malware
- Threat Actors Leveraging ClickFake Interview Attack to Deploy OtterCandy Malware

Vulnerabilities & Exploits

- Critical ConnectWise Vulnerabilities Allow Attackers To Inject Malicious Updates

Trends & Reports

- Open Source Malware Surges 140% in Q3 2025
- Ransomware Hits Record Highs: Healthcare, Government, Tech Sectors Top Targets in BlackFog Q3 2025 Analysis

Privacy, Legal & Regulatory

- Italy's Comprehensive New AI Law

Upcoming Health-ISAC Events

- Global Monthly Threat Brief
  - Americas - October 28, 2025, 12:00-01:00 PM ET
  - European – October 29, 2025, 03:00-04:00 PM CET
- Fall Americas Summit – Carlsbad, California – December 1-5, 2025

Leading Story

Threat Actors Exploit Cisco SNMP Flaw to Deploy Rootkit on Switches

Summary

- Cisco disclosed that threat actors recently exploited a zero-day vulnerability in the IOS and IOS XE software's Simple Network Management Protocol subsystem to deploy a rootkit on vulnerable devices.

Analysis & Action

Cisco disclosed that a vulnerability in the IOS and IOS XE software with Simple Network Management Protocol (SNMP) enabled was recently observed being exploited in the wild.

The flaw, tracked as CVE-2025-20352 and patched in September 2025, stems from a stack overflow condition. The vulnerability enables authenticated threat actors to cause denial-of-service (DoS) conditions or, more critically, gain full system compromise through command execution. The recent attack targeted Linux systems running Cisco 9400, 9300, and the legacy 3750G series, and deployed a rootkit with extensive UDP controller capabilities on systems without endpoint detection response (EDR) solutions. According to Trend Micro, who tracked the attack, the threat actors also attempted to exploit CVE-2017-3881, a Cluster Management Protocol code flaw.

Health-ISAC encourages its members to patch vulnerable software promptly, deploy EDR solutions, and disable the vulnerable object IDs as mitigation measures.

Data Breaches & Data Leaks

Marketing and Email Data Platform Exposed Over 40 Billion Records Online

Summary

- Approximately 40 billion Netcore Cloud Pvt records were exposed after an unencrypted and non-password-protected database was discovered. An unencrypted and unsecured database belonging to Netcore Cloud Pvt has been found, exposing its records.

Analysis & Action

Netcore Cloud Pvt, a leading marketing and email data platform, has exposed approximately 40 billion records (13 terabytes) after the discovery of an unencrypted and non-password-protected database.

The information compromised in this database includes sensitive data such as health sector notifications, banking alerts, employment-related communications, account verification emails, and marketing messages. It is essential to clarify that it remains uncertain whether the database was under the management of Netcore Cloud Pvt or a third-party contractor. Nonetheless, this exposure presents significant risks, including potential targeted phishing attempts, spoofing, and the likelihood of entire systems being compromised due to detailed internal and infrastructural data availability.

Health-ISAC strongly recommends that its members adopt proactive strategies to mitigate the risk of data breaches. These include encrypting all sensitive data, creating regular offline backups, and diligently verifying configuration settings to ensure accuracy. Implementing these measures is essential for safeguarding data integrity and security.

Cyber Crimes & Incidents

Beware Of Fake LastPass Hack Emails Trying To Trick Users Into Installing Malware

Summary

- Cybersecurity professionals warn of fake LastPass phishing emails masquerading as breach notifications.

Analysis & Action

Cybersecurity experts have raised alarms about a new wave of phishing emails masked as LastPass breach notifications.

The scheme has seen activity since early October, impacting several enterprise users. Messages within the malicious phishing emails warn recipients of account compromise, using LastPass branding such as the company logos and links with manipulated URLs to urge them to download fake security patches that will supposedly restore access. The included downloadable file instead consists of a sophisticated malware loader, capable of keylogging, capturing screenshots, and laterally moving throughout corporate networks, harvesting credentials and deploying payloads.

Health-ISAC advises its members to remain wary of links or attachments coming from foreign senders, confirming validity before interaction as proactive mitigations to phishing campaigns.

Threat Actors Leveraging ClickFake Interview Attack to Deploy OtterCandy Malware

Summary

- North Korean threat group WaterPlum has leveraged a new malware strain, known as OtterCandy, in its ongoing ClickFake interview campaigns targeting the blockchain industry.

Analysis & Action

The North Korean threat group WaterPlum, also known as Famous Chollima and PurpleBravo, has implemented a new malware strain into its ClickFake Interview campaign.

The social engineering campaign leverages fake job applications and interview processes that lure victims into downloading malicious payloads disguised as driver updates or camera setup instructions. The new malware, identified as OtterCandy, targets Windows, macOS, and Linux systems. It combines features from the previously used RATatouille and OtterCookie families for stealthier information-stealing capabilities and long-term persistence. OtterCandy incorporates an independent backup mechanism that enables continuity in the event of an interruption and has a trace deletion feature that helps erase evidence of intrusion.

Health-ISAC recommends that its members educate staff on social engineering campaigns, avoid downloading attachments from unknown sources, and deploy endpoint detection solutions to mitigate similar threats.

Vulnerabilities & Exploits

Critical ConnectWise Vulnerabilities Allow Attackers To Inject Malicious Updates

Summary

- Two critical ConnectWise vulnerabilities within its agent communications permit threat actors to intercept sensitive data and/or push malicious updates.

Analysis & Action

ConnectWise has released a security update regarding two critical flaws. These flaws permit threat actors to intercept sensitive data and/or push malicious updates to software.

The matter stems from environments reliant on encrypted HTTP traffic or outdated protocols for encryption, impacting all versions before 2025.9. The first flaw, CVE-2025-11492 (CVSS 9.6), involves transmitting sensitive agent data into plain text, while the second, CVE-2025-11493 (CVSS 8.8), allows for code downloads without verifying their integrity. These flaws enable threat actors nearby or on the same local network to eavesdrop on transmissions or tamper with update downloads, possibly resulting in data breaches or complete system compromise. ConnectWise has since released a critical security update in its patched version 2025.9 addressing the issue.

Health-ISAC advises its members to consider auditing their configurations and to monitor for malicious traffic regularly.

Trends & Reports

Open Source Malware Surges 140% in Q3 2025

Summary

- New data from the Open Source Malware Index Q3 2025 indicates a significant growth in open source malware, allowing threat actors to target developers with data exfiltration and dropper malware.

Analysis & Action

Following the release of new data as part of the Open Source Malware Index Q3 2025, a large escalation in software supply chain attacks has been identified.

The reports detail 34,319 new malicious open source packages identified in Q3 alone, a 140% increase from Q2. This growth indicates cybercriminals' increased focus on gathering intelligence and establishing persistence within networks. The threats primarily highlight methods such as data exfiltration, accounting for 37% of the malicious packages found, and the use of droppers, representing 38% of threats. Furthermore, the use of backdoors by threat actors saw a growth of 143%, further highlighting that threat actors focus on maintaining long-term access to compromised environments. At this time, financial service organizations (47%) faced the most attacks, followed by business services (14%), and energy and utilities (8%).

Health-ISAC advises its members to consider continuously monitoring dependencies and implementing regulatory checks to verify component integrity as mitigation strategies.

Ransomware Hits Record Highs: Healthcare, Government, Tech Sectors Top Targets in BlackFog Q3 2025 Analysis

Summary

- BlackFog’s latest Q3 report reveals an increase in ransomware attacks, with the majority targeting the health sector, government entities, and technology industries.

Analysis & Action

BlackFog's analysis for Q3 2025 reveals a significant increase in ransomware attacks targeting critical infrastructure globally, with the healthcare sector remaining one of the most affected.

The report indicates that approximately 270 attacks were publicly disclosed, representing a 36% increase compared to last year. Additionally, 1,510 undisclosed incidents were identified, marking a 21% rise from last year. The healthcare sector experienced 86 publicly disclosed attacks, which account for 32% of all incidents in this category. The technology industry and government entities followed as the next most targeted sectors. The report also identified Qilin as the most active threat group, noting the emergence of 18 new threat groups during the quarter.

Health-ISAC encourages its members to encrypt all data, establish regular backup schedules, and deploy endpoint detection and response solutions as precautionary measures against ransomware attacks.

Privacy, Legal & Regulatory

Italy’s Comprehensive New AI Law

Summary

- Italy’s new AI Law integrates the European Union’s framework and defines artificial intelligence's role in better preparing and protecting critical sectors, including healthcare.

Analysis & Action

Italy implemented new artificial intelligence (AI) legislation on October 10. This law aligns with the European Union's AI regulatory framework (EU AI Act) for critical sectors operating within the country, including healthcare.

The Italian AI Law outlines the requirements and roles of AI tools across various industries, strongly emphasizing privacy protection and the need for transparency regarding their usage. In the healthcare sector, AI can be utilized for diagnostics and prevention, but it is crucial to maintain complete transparency with patients about its application. Furthermore, the law defines the responsibilities of national authorities and initiatives aimed at promoting the responsible use and development of AI. It references key organizations, including the Agency for Digitalization of Italy (AgID), the National Cybersecurity Authority (ACN), the Data Protection Authority, and the Communications Regulatory Authority (AGCOM). Additionally, the legislation proposes an increase in funding for AI, cybersecurity, and quantum computing innovation.

Health-ISAC encourages its members to adhere to local and federal guidelines on cybersecurity and related tools to ensure legal compliance and address the evolving threat landscape.

Health-ISAC Cyber Threat Level

On September 18, 2025, the Health-ISAC Threat Intelligence Committee (TIC) evaluated the current Cyber Threat Level and collectively decided to maintain the Cyber Threat Level to **Blue (Guarded)**. The Threat Level of **Blue (Guarded)** is due to threats from:

NPM Worm Impact, QR Code Phishing, Typosquatting Campaigns, Remote IT Worker Fraud, and **Job Posting Scams.**

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

Alert ID 318ffee2

View Alert

Share Feedback

was this helpful? |

Tags AI Law, Cisco SNMP Flaw, ClickFake Interview, LastPass Password Manager, Malware, ConnectWise, Data Breaches, Ransomware

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

Download Health-ISAC's Information Sharing App.

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**