# DAILY CYBER HEADLINES

## Health-ISAC Daily Cyber Headlines

TLP:WHITE

Oct 12, 2022

**Today's Headlines:**

**Leading Story**

- Microsoft October 2022 Patch Tuesday Fixes Zero-Day Used in Attacks, 84 Flaws

**Data Breaches & Data Leaks**

- High-Value Targets: String of Aussie Telco Breaches Continues

**Cyber Crimes & Incidents**

- Experts Analyzed the Evolution of the Emotet Supply Chain
- BazarCall Callback Phishing Attacks Constantly Evolving Its Social Engineering Tactics

**Vulnerabilities & Exploits**

- Hacking Group POLONIUM Uses 'Creepy' Malware Against Israel

**Trends & Reports**

- Abuse of Legitimate Tools Threatens Healthcare Cybersecurity

**Privacy, Legal & Regulatory**

- India Rolls Out Nationwide Tele-Mental Health Service

**Upcoming Health-ISAC Events**

- Health-ISAC Monthly Threat Brief – October 25, 2022, 12:00 PM Eastern

## Leading Story

Microsoft October 2022 Patch Tuesday Fixes Zero-Day Used in Attacks, 84 Flaws

**Summary**

- Tuesday, October 11, 2022, was Microsoft's Patch Tuesday for the month of October 2022.

**Analysis & Action**

In this iteration of patch Tuesday, Microsoft patched a total of 84 vulnerabilities within the Windows operating system.

13 of the 84 patches made fixed critical vulnerabilities, indicating a common vulnerability scoring system (CVSS) score between 9.0-10. These vulnerabilities allowed for privilege escalation, spoofing, or remote code execution.

With all the recent patches, two known zero-day vulnerabilities, CVE-2022-41040 and CVE-2022-41082 have not been fixed. To see the full list of patches made, see the table within the article here.

## Data Breaches & Data Leaks

High-Value Targets: String of Aussie Telco Breaches Continues

**Summary**

- In the weeks after the Optus breach, two other Australian telecommunications providers have been hit by threat actors.

**Analysis & Action**

Security researchers have seen an increase in Australian telecommunications providers being attacked by malicious cyber actors. These attacks have been in quick succession hitting multiple companies with data exfiltration followed by extortion efforts.

These threat actors have made their intentions known by releasing parts of the stolen data on the dark web.

Historically, telecommunications providers are sought-after targets in threat actor circles. This is due to the size of their customer base, which indicates a high likelihood of paying ransoms. This string of extortion attacks are proving the effectiveness of data exfiltration attacks as opposed to standard ransomware.

**Cyber Crimes & Incidents**

Experts Analyzed the Evolution of the Emotet Supply Chain

**Summary**

- Security researchers have been tracking the supply chain of the Emotet banking trojan and botnet to monitor its evolution.

**Analysis & Action**

Security researchers have been observing the continual evolution of the Emotet trojan. The threat actors behind this malware have been tracked as group TA542. In the retroactive review of their activities, experts observed adaptations to new Microsoft security defaults.

This adaptation is notable because the main things being changed are the tactics, techniques, and procedures (TTPs) themselves. In the pyramid of pain, aa hierarchy of changes a threat actor may make ranked by difficulty; the TTPs are labeled as the hardest thing to change. This shows true dedication.

Particularly, TA542 has been observed diversifying its attack vectors, thus making attribution harder for victims. In summary, TA542 has undergone these changes to keep their attacks effective and evade detection via diversifying their attack vectors.

BazarCall Callback Phishing Attacks Constantly Evolving Its Social Engineering Tactics

**Summary**

- BazaCall, a threat actor infamous for targeting the healthcare sector has been observed evolving its social engineering strategies.

**Analysis & Action**

The threat actors behind the Bazacall callback campaign have been observed sending fraudulent emails to victims that entice them to call a certain phone number. When the number is called, the threat actors walk the victim through installing a backdoor under the guise of an existing software upgrade.

They have also been known to use this number to pretend to be PayPal incident responders, informing the victim that their account has been the subject of anomalous login activity. The threat actors then encourage the victim to click on a URL that will download and execute malicious payloads that grant the threat actors access to the victim's system.

This group is known to heavily target the healthcare sector in the US and abroad. Members are recommended to refresh their call-center employees on this particular vishing campaign to avoid falling victim to it.

## Vulnerabilities & Exploits

Hacking Group POLONIUM Uses 'Creepy' Malware Against Israel

**Summary**

- Security researchers have observed an increase in the targeting of Israeli companies by a threat actor known as POLONIUM to conduct cyber espionage activities.

**Analysis & Action**

This threat actor group has been observed utilizing a wide variety of tools to conduct espionage against Israeli companies. They have not been observed partaking in any destructive activities such as data wiping or deploying ransomware.

It has been deduced that their main objective is data exfiltration. This group has been speculated to be a part of the Iranian Ministry of Intelligence and Security (MOIS). The capabilities exhibited by POLONIUM back up the tentative nation-state attribution.

This group has been observed using seven different backdoors. Once a backdoor is in place, the group opens communication with a command and control (C2) server to exfiltrate files to a file transfer protocol (FTP) server.

## Trends & Reports

Abuse of Legitimate Tools Threatens Healthcare Cybersecurity

**Summary**

- Threat actors have repeatedly abused legitimate tools like Cobalt Strike and PowerShell to threaten healthcare cybersecurity.

**Analysis & Action**

Threat actors are continuously leveraging legitimate tools such as Cobalt Strike, Mimikatz, and PowerShell to conduct cyberattacks that pose threats to healthcare cybersecurity, the HHS Health Sector Cybersecurity Coordination Council (HC3) warned in a recent brief.

Cobalt Strike has been used in multiple high-profile cyberattacks, from as early as 2016. In December 2020, threat actors used Cobalt Strike to deploy a large-scale supply chain attack on SolarWinds. These tools can bring significant risk to healthcare organizations, and each organization should weigh the risks and benefits accordingly.

A link to the HC3 threat brief can be found here.

## Privacy, Legal & Regulatory

India Rolls Out Nationwide Tele-Mental Health Service

**Summary**

- The Union Ministry of Health & Family Welfare of India is officially releasing its national tele-mental health program this week.

**Analysis & Action**

The COVID-19 pandemic and subsequent quarantine sent mental health consequences rippling through the Indian populace at an unprecedented rate. To combat this, the Indian government has elected to begin a nationwide tele-mental health service.

This is a testament to the effectiveness and desirability of telehealth services. India has the second largest population in the world at an astonishing 1.38 billion people. A national telehealth service for this population is a massive undertaking.

As telehealth gains more relevance and popularity, the cybersecurity risks facing telecommunications services become intertwined with healthcare risks. Members should be aware of the large-scale telehealth implementation efforts worldwide and plan accordingly for risks to this emerging network.

**Health-ISAC Cyber Threat Level**

On September 15, 2022, 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) was chosen in response to credential thieving and social engineering attempts with CEO Impersonation, fraudulent payment processing, EU energy crisis, Russia-Ukraine ongoing conflict, railroad strike and supply chain Issues, and IcedID and Qbot reemergence.

**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)** | Dark Reading, Bleeping Computer, Security Affairs, Bleeping Computer, The Hacker News, Health IT Security, Healthcare IT News |

**Alert ID** 973c6896

This Alert has 1 attachment(s). To view or download the attachment(s), click "View Alert" to login to the web portal.

## View Alert

**Tags** POLONIUM, Daily Cyber Headlines, BazaCall, Telehealth, DCH, Emotet Trojan, Patch Tuesday, Telecommunications, Australia, India, Cobalt Strike

**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

Download Health-ISAC's Information Sharing App.

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