Health-ISAC Daily Cyber Headlines

Daily Cyber Headlines **TLP:WHITE** **Alert Id: c79eb4d6** **2022-10-18 13:22:27**

Today's Headlines:

Leading Story

- Zoom for macOS Contains High-Risk Security Flaw

Data Breaches & Data Leaks

- Keystone Health Data Breach Impacts PHI of Thousands of Individuals
- Hackers Compromised Hong Kong Govt Org's Network for a Year

Cyber Crimes & Incidents

- Black Basta Ransomware Hackers Infiltrates Networks and Deploy Brute Ratel C4

Vulnerabilities & Exploits

- Critical RCE Vulnerability Discovered in Popular Cobalt Strike Hacking Software

Trends & Reports

- Fortinet Urges Admins to Patch Bug with public Exploit Immediately

Privacy, Legal & Regulatory

- Chinese Spyder Loader Malware Spotted Targeting Organizations in Hong Kong

Upcoming Health-ISAC Events

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

Leading Story

Zoom for macOS Contains High-Risk Security Flaw

Summary

- Zoom has rolled out a high-priority patch for macOS users alongside a warning that hackers could abuse the software flaw to connect to and control Zoom Apps.

Analysis & Action

The vulnerability was discovered by the company's internal security team as part of a routine assessment.

Zoom Client for Meetings for macOS (Standard and for IT Admin) is affected by a debugging port misconfiguration. The issue, tracked as CVE-2022-28762, received a CVSS severity score of 7.3.

When the camera mode rendering context is enabled as part of the Zoom App Layers API by running specific Zoom Apps, a local debugging port is opened by the client. A local malicious user can exploit the debugging port to connect to and control the Apps running in the Zoom client.

Data Breaches & Data Leaks

[Keystone Health Data Breach Impacts PHI of Thousands of Individuals]

Summary

- Keystone Health, a Pennsylvania-based team of primary care providers, disclosed a healthcare data breach that potentially impacted the protected health information (PHI) of 235,237 individuals.

Analysis & Action

Keystone Health discovered the security incident on August 19 and later determined that an unauthorized party had accessed files within its system between July 28 and August 19.

The files contained patient names, clinical information, and Social Security numbers. Keystone Health has notified impacted individuals.

Keystone Health is implementing new network security measures and providing additional training to our employees to ensure awareness and security.

Cyber Crimes & Incidents

[Black Basta Ransomware Hackers Infiltrates Networks and Deploy Brute Ratel C4]

Summary

- The Black Basta ransomware family have been observed using the Qakbot trojan to deploy the Brute Ratek C4 framework as a second-stage payload in recent attacks.

Analysis & Action

The intrusion, achieved using a phishing email containing a weaponized link pointing to a ZIP archive, further entailed the use of Cobalt Strike for lateral movement. Threat actors are using a cracked version of Brute Ratel C4 that began circulating last month across cybercriminal underground.

Qakbot, also called QBot and QuackBot, is an information stealer and banking trojan that's known to be active since 2007. But its modular design and its ability to act as a downloader has turned it into an attractive candidate for dropping additional malware.

While these legitimate utilities are designed for conducting penetration testing activities, their ability to offer remote access has made them a lucrative tool in the hands of attackers looking to stealthily probe the compromised environment without attracting attention for extended periods of time.

Vulnerabilities & Exploits

[Critical RCE Vulnerability Discovered in Popular Cobalt Strike Hacking Software]

Summary
- HelpSystems, the company behind the Cobalt Strike software platform, has released an out-of-band security update to address a remote code execution vulnerability that could allow an attacker to take control of targeted systems.

Analysis & Action
The issue, tracked as CVE-2022-42948, affects Cobalt Strike version 4.7.1, and stems from an incomplete patch released on September 20, 2022, to rectify a cross-site scripting (XSS) vulnerability (CVE-2022-39197) that could lead to remote code execution.

The findings come a little over a week after the U.S. Department of Health and Human Services (HHS) cautioned of the continued weaponization of legitimate tools such as Cobalt Strike in attacks aimed at the healthcare sector.

Trends & Reports

Fortinet Urges Admins to Patch Bug with public Exploit Immediately

Summary
- Fortinet urges customers to urgently patch their appliances against a critical authentication bypass FortiOS, FortiProxy, and FortiSwitchManager vulnerability exploited in attacks.

Analysis & Action
The company released security updates to address the flaw in CVE-2022-40684 and advised customers to disable remote management user interfaces on affected devices.

After many notifications from Fortinet over the past week, there were a significant number of devices that require mitigation.

Attackers started scanning for unpatched Fortinet devices as soon as the initial confidential notification was sent to customers on October 6, with Fortinet saying that it detected threat actors exploiting the vulnerability to create malicious administrator accounts.

Privacy, Legal & Regulatory

Chinese Spyder Loader Malware Spotted Targeting Organizations in Hong Kong

Summary
- The China-aligned espionage-focused actor dubbed Winnti has set its sights on government organizations in Hong Kong as part of an ongoing campaign dubbed Operation CuckooBees.

Analysis & Action
The threat actor's campaigns have targeted healthcare, telecoms, high-tech, media, agriculture, and education sectors, with infection chains primarily relying on spear-phishing emails with attachments to initially break into the victims' networks.

Spyder Loader is being used for targeted attacks on information storage systems, collecting information about corrupted devices, executing mischievous payloads, coordinating script execution, and C&C server communication.

The fact that this campaign has been ongoing for several years, with different variants of the Spyder Loader malware deployed in that time, indicates that the actors behind this activity are persistent and focused adversaries, with the ability to carry out stealthy operations on victim networks over a long period of time.

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): Security Week, Health IT Security, The Hacker News, The Hacker News, Bleeping Computer, The Hacker News

Tags: Brute Ratel, Daily Cyber Headlines, DCH, CobaltStrike, apt41, Fortinet

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