Health-ISAC Daily Cyber Headlines

Daily Cyber Headlines **TLP:WHITE** **Alert Id: bc54ac47** **2022-10-14 12:42:02**

Today’s Headlines:

Leading Story

- A Quarter of Healthcare Ransomware Victims Forced to Halt Operations

Data Breaches & Data Leaks

- RansomEXX Leaks 52GB of Barcelona Health Centers’ Data
- LockBit Identified as Responsible for Forcing NHS Tech Supplier to Shut Down

Cyber Crimes & Incidents

- Feature-Rich Alchimist Cyberattack Framework Targets Windows, Mac, Linux Environments
- Magniber Ransomware Now Infects Windows User Via Java Scripts Files

Vulnerabilities & Exploits

- PoC Exploit Released for Critical Fortinet Authorization Bypass Bug Under Active Attacks

Trends & Reports

- Surge in Dark Data Represents Growing Danger for Corporations

Privacy, Legal & Regulatory

- Nothing to Report

Upcoming Health-ISAC Events

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

Leading Story

A Quarter of Healthcare Ransomware Victims Forced to Halt Operations

Summary

- New research developed by Trend Micro has shown alarming results regarding operations disruptions due to ransomware campaigns against healthcare organizations.

Analysis & Action

The new report released by Trend Micro has demonstrated that ransomware attacks against healthcare organizations have a detrimental effect on the organization's operations.

According to Trend Micro, 86% of global healthcare organizations that have been compromised by ransomware suffered operational outages. Additionally, it was possible to determine that 25% of the targeted organizations were forced to halt their operations completely. Also, 56% of ransomware victims required days to restore their operations while 24% needed several weeks to recover from the attacks.

Although ransomware is the main threat, attackers' intent is to exfiltrate data, therefore, 60% of responding organizations experienced data leaks as a consequence of the ransomware attacks.

Data Breaches & Data Leaks

RansomEXX Leaks 52GB of Barcelona Health Centers' Data

Summary

- RansomEXX has been observed leaking 52GB of a healthcare organization on its dark web data leak sites.

Analysis & Action

The threat actor RansomEXX has been actively targeting various companies in multiple industries including healthcare and automotive.

This week security researchers observed that the threat actor published confidential information about a Barcelona Hospital system, which provides medical and social services. It was assessed that the compromised information included personally identifiable information and private health information as medical test results and identity cards have been stolen.

The data was directly obtained from the Consorci Sanitari Integral organization, and the leaked data could expose the affected individuals to cybercriminal-related activity such as extortion, phishing, as well as identity theft. The organization stated that a speedy recovery plan has been established and that it is expected it will enhance the organization's current cybersecurity practices.

LockBit Identified as Responsible for Forcing NHS Tech Supplier to Shut Down

Summary

- An NHS technology supplier has admitted that customer data was exfiltrated during an August ransomware attack and it was assessed that LockBit is behind the attack.

Analysis & Action

A ransomware attack directed at Advanced, an NHS technology provider, took place in August 2022 and disrupted the operations of NHS 111 medical services.

The affected organization established that after discovering the incident it was necessary to pull a portion of its infrastructure offline to prevent the spread of the attack. Apart from the operational disruptions caused at the NHS, it was possible to determine that the threat actors behind the attack were financially motivated and that they were able to access confidential information.

The compromised information was obtained from Advanced environment pertaining to 16 Staffplan and Caresys customers. At the moment of writing the organization has stated that the impact on individuals' data is minimal, however, the tech provider is also monitoring the dark web to prevent any additional damage to individuals.

Cyber Crimes & Incidents

Feature-Rich Alchimist Cyberattack Framework Targets Windows, Mac, Linux Environments

Summary

- A new cyberattack framework has been identified by security researchers that is currently targeting Windows, Linux, and Mac systems.

Analysis & Action

Security researchers were able to identify a new and potentially dangerous cyberattack framework targeting Windows, Linux, and Mac operating systems.

The new cyberattack framework includes many different features such as a new remote access trojan called Insekt, a standalone command and control tool dubbed Alchemist, and a custom backdoor and malware used to exploit macOS. The researchers from Cisco Talos that discovered the new framework have stated that it is used as an alternative to Cobalt Strike and Silver, and the threat actor behind the new framework is likely a China-based threat group.

The researchers assessed with confidence that the framework is already being used in the wild. The development of the new cyberattack framework is another strategy employed by threat actors to use alternative solutions to widely employed attack frameworks.

Magniber Ransomware Now Infects Windows User Via Java Scripts Files

Summary

- A new campaign has been identified which was observed to deliver Magniber ransomware to Windows home users.

Analysis & Action

Security researchers have identified a new malicious campaign that is currently targeting Windows home users. The users are lured with fake antivirus and security updates for Windows 10, which will then download malicious files in ZIP format, that contain JavaScript commands.

Then, the encrypting malware would be delivered to compromise the users' data. Researchers at HP's threat intelligence team observed that the victims of Magniber ransomware were asked to pay $2,500 for the decryption tool that will allow them to recover their information.

Also, it was possible to determine that Magniber is employing a new infection chain and that it limits the encryption to specific file types. It is advised to home users to regularly back up their data on an offline storage device, so they are not exposed to the extortion techniques used by threat actors.

Vulnerabilities & Exploits

PoC Exploit Released for Critical Fortinet Authorization Bypass Bug Under Active Attacks

Summary

- A proof-of-concept exploit has been released by security researchers regarding a critical security flaw affecting multiple Fortinet products.

Analysis & Action

A proof-of-concept exploit code that is now available for the critical security flaw affecting Fortinet FortiOS, FortiProxy, and FortiSwitchManager highlights the need for a rapid and effective patch management strategy.

The vulnerability found in Fortinet products is tracked as CVE-2022-40684 and has a CVSS score of 9.6 out of 10, which could allow an attacker to perform malicious operations on the administrative interface via specially crafted HTTP requests.

Fortinet has already patched the vulnerability and it has urged CISA to issue an advisory for federal agencies to patch the issue by November 1, 2022.

Trends & Reports

Surge in Dark Data Represents Growing Danger for Corporations

Summary

- The increase in dark data has raised concerns for many organizations as storing and securing data typically incurs more expense than value.

Analysis & Action

Researchers have concluded that dark data represents the biggest potential cybersecurity exposure for U.S. and U.K. businesses. Dark data is the information assets organizations collect, process and store during regular business activities, but generally fail to use for other purposes. This data is often used for compliance purposes only.

Dark data can be unstructured, sensitive, personal, regulated, vulnerable or high-risk information an organization has collected and stored over time. Many senior executives are concerned about storing dark data could pose more risk than value.

Dark data is often forgotten and unprotected by corporations, which creates substantial liabilities and can lead to tempting targets for cyber criminals. IT departments should deploy technologies to better find, secure and redact dark data.

Privacy, Legal & Regulatory

Nothing to Report

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, Healthcareinfosecurity, The Register, Dark Reading, Bleeping Computer, The Hacker News, The Hacker News

Tags: Dark web data, Alchimist, Barcelona Hospital, Daily Cyber Headlines, Magniber Ransomware, Lockbit, DCH, Fortinet, Ransomware, Data Breach

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