DAILY CYBER HEADLINES

Health-ISAC Daily Cyber Headlines

TLP:WHITE

Oct 17, 2022

Today's Headlines:

Leading Story

- Venus Ransomware Targets Publicly Exposed Remote Desktop Services

Data Breaches & Data Leaks

- Phishing Incident May Have Exposed Seton Patient Names, Clinical Information

Cyber Crimes & Incidents

- Prestige Ransomware Targeting Polish and Ukrainian Organizations

Vulnerabilities & Exploits

- Zimbra Releases Patch for Actively Exploited Vulnerability in its Collaboration Suite

- Microsoft Office 365 Uses Broken Email Encryption to Secure Messages

Trends & Reports

- Phishing Works So Well Criminals Won't Bother with Deepfakes

Privacy, Legal & Regulatory

- Nothing to Report

Upcoming Health-ISAC Events

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

Leading Story

Venus Ransomware Targets Publicly Exposed Remote Desktop Services

Summary

- Threat actors behind the relatively new Venus Ransomware are hacking into publicly exposed Remote Desktop services to encrypt Windows devices.

Analysis & Action

Venus Ransomware appears to have begun operating in the middle of August 2022 and has since encrypted victims worldwide.

When executed, the Venus ransomware will attempt to terminate thirty-nine processes associated with database servers and Microsoft Office applications.

As the ransomware appears to be targeting publicly-exposed Remote Desktop services, even those running on non-standard TCP ports, it is vital to put these services behind a firewall.

Health-ISAC recommenders ensuring Remote Desktop Services are not publicly exposed on the Internet. Remote Desktop Services should only be accessible via a VPN.

Data Breaches & Data Leaks

Phishing Incident May Have Exposed Seton Patient Names, Clinical Information

Summary

- A vendor associated with Seton Medical Center in Harker Heights was recently the victim of a phishing incident, according to a news release from the hospital late Friday afternoon.

Analysis & Action

According to the center, an unauthorized agent accessed the email accounts of two of the vendor's employees. An investigation from the vendor told Seton that the following types of patient information may have been exposed:

- First and last name
- Date of birth
- Medical record number
- Certain clinical information.

Information including patients' Social Security numbers, addresses and financial information was not accessed, the release said.

The vendor does not indicate that any protected health information has been misused.

Regardless, Seton Medical Center Harker Heights encourages individuals to take precautions to protect the security of their information.

Cyber Crimes & Incidents

Prestige Ransomware Targeting Polish and Ukrainian Organizations

Summary

- A new ransomware campaign targeted the transportation and logistics sectors in Ukraine and Poland on October 11 with a previously unknown payload dubbed Prestige.

Analysis & Action

This new ransomware was first used in the wild on October 11, in attacks detected within an hour of each other.

The method of initial access remains unknown. The threat actor obtained privileged access to the compromised environment to deploy the ransomware using three different methods.

The activity shares victimology with recent Russian state-aligned activity, specifically on affected geographies and countries, and overlaps with previous victims of the HermeticWiper malware.

Vulnerabilities & Exploits

Zimbra Releases Patch for Actively Exploited Vulnerability in its Collaboration Suite

Summary

- Zimbra has released patches to contain an actively exploited security flaw in its enterprise collaboration suite that could be leveraged to upload arbitrary files to vulnerable instances.

Analysis & Action

Unknown APT groups have actively been taking advantage of the flaw in the wild, with one of the actors systematically infecting all vulnerable servers in Central Asia.

Approximately 1,600 Zimbra servers are estimated to have been infected in a mix of targeted and opportunistic attacks.

The attacks, which unfolded over two attack waves in early and late September, primarily targeted government entities in the region, abusing the initial foothold to drop web shells on the compromised servers for follow-on activities.

Microsoft Office 365 Uses Broken Email Encryption to Secure Messages

Summary

- A security vulnerability has been in Microsoft 365 that could be exploited to infer message contents due to the use of a broken cryptographic algorithm.

Analysis & Action

Researchers observed the messages are encrypted in insecure Electronic Codebook (ECB) mode of operation. Office 365 Message Encryption (OME) is a security mechanism used to send and receive encrypted email messages between users inside and outside an organization without revealing anything about the communications themselves.

A concern with cybersecurity professionals is third party suppliers gaining access to encrypted email messages that could be used to decipher the messages, effectively breaking confidentiality protections.

The National Institute of Standards and Technology (NIST) acknowledged earlier this year that ECB mode encrypts plaintext blocks independently, without randomization; therefore, the inspection of any two ciphertext blocks reveals whether the corresponding plaintext blocks are equal.

Trends & Reports

Phishing Works So Well Criminals Won't Bother with Deepfakes

Summary

- Researchers are noting that the frequency of incidents associated with deepfakes is unremarkable.

Analysis & Action

Traditional attacks involving phishing are effective enough that cybercriminals are not dedicating a significant amount of energy to deepfakes. Instead, phishing campaigns remain the most effective approach to compromising machines.

Researchers at Sophos noted that phishing and other forms of social engineering are simpler and cheaper to operationalize for threat actors than developing deepfakes.

One area in which Sophos does see deepfakes becoming prevalent is romance scams. It takes a hefty amount of devotion, time and energy to craft believable fake personas, and the additional effort to add a deepfake is not huge.

Researchers at Trend Micro warned last month that deepfakes may not always be a scammer's main tool but are often used to enhance other techniques. The lifelike digital images have lately shown up in job seeker scams, bogus business meetings and web ads.

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.

Alert ID a7edf961

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 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

Download Health-ISAC's Information Sharing App.  

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