Daily Cyber Headlines

Daily Cyber Headlines | TLP:WHITE | Alert ID : 7adbb2fc | Oct 30, 2023, 08:24 AM

Today's Headlines:

Leading Story

- New Hunters International Ransomware Possible Rebrand of Hive

Data Breaches & Data Leaks

- California City Warns of Data Breach After Ransomware Attack Claims
- Michael Garron Hospital Under Code Grey Following Data Security Incident

Cyber Crimes & Incidents

- Iran APT Targets the Mediterranean with Watering-Hole Attacks

Vulnerabilities & Exploits

- Urgent: New Security Flaws Discovered in NGINX Ingress Controller for Kubernetes

Trends & Reports

- Feds Warn Healthcare Sector of AI-Augmented Phishing Threats

Privacy, Legal & Regulatory

- King Charles III Signs Off on UK Online Safety Act, With Unenforceable Spying Clause

Cybersecurity Awareness Month

- The Daily Cyber Headlines are shared during October at TLP: WHITE for Cybersecurity Awareness Month.

Upcoming Health-ISAC Events

- Health-ISAC Monthly Threat Brief – October 31, 2023, 12:00 PM Eastern

Additional Information

Leading Story

New Hunters International Ransomware Possible Rebrand of Hive

Summary

- Hunters International is a new ransomware-as-a-service brand that is allegedly using code from the Hive ransomware operation.

Analysis & Action

The group claims to have purchased the source code from the Hive developers and has fixed some of the mistakes in the code.

This theory is supported by analysis of the new encryptor revealing multiple code overlaps between the two ransomware gangs. Hive ransomware's operations came to a sudden stop in January after its Tor payment and data leak site were seized in an international operation.

The new group says that encryption is not the main goal of their operation, instead they are focusing on stealing data as leverage when extorting victims into paying a ransom demand.

Data Breaches & Data Leaks

California City Warns of Data Breach After Ransomware Attack Claims

Summary

- The security of personal data and information of residents in Victorville, CA were compromised during a ransomware attack against government systems in California.

Analysis & Action

Personal data and information on the citizens of Victorville have been accessed by the NoEscape ransomware group. Citizens' names, social security numbers, driver's license number or state identification card numbers, medical information, and health insurance policy numbers were among the files that were accessed by threat actors.

The NoEscape ransomware group has stolen 200GB of data from Victorville's government systems. The ransomware attack had an impact on phone and website

systems, such as paying online bills and submitting online forms. These attacks led to limited action within government services. According to current sources, specifics about the incident have not been disclosed.

While details about how the ransomware attack occurred are unknown, previous attacks from the NoEscape ransomware group point toward phishing operation involving malicious emails and attachments. Members are encouraged to identify suspicious emails and verify their sources before engaging.

Michael Garron Hospital Under Code Grey Following Data Security Incident

Summary

- A Toronto based Michael Garron Hospital has reported a data security incident.

Analysis & Action

Major Toronto healthcare organization, Michael Garron Hospital, part of the Toronto East Health Network, is investigating a security incident.

While the hospital did not state what exactly occurred, they have allegedly used Code Grey, which is used in cases where there is a loss of key infrastructure of the hospital, indicating a possibility of a serious incident at hand. According to the statement made by the Hospital, there is currently an investigation ongoing, and necessary measures have been taken to keep data and information systems safe.

Hospitals keep being targeted by ransomware groups. Members are advised to keep being vigilant in monitoring their networks for suspicious activities and maintaining diligent patching of vulnerable devices to reduce weak points that could be used as entry points for threat actors.

Cyber Crimes & Incidents

Iran APT Targets the Mediterranean with Watering-Hole Attacks

Summary

- Mediterranean organizations are being targeted by Iranian advanced persistent threat (APT) actors utilizing a new malware downloader.

Analysis & Action

The threat actor sponsored by the Islamic Republic of Iran, which is known as Tortoiseshell, Imperial Kitten, TA456, Crimson Sandstorm, or Yellow Liderc, has been spotted targeting Mediterranean organizations, specifically those within the maritime, shipping, and logistics sectors.

The APT has been reported utilizing watering holes, phishing domains, highly targeted emails, fake social media accounts, and more to forward their espionage campaign. Yellow Liderc has also utilized open-source software to insert malicious links into fake newsletters that impersonate organizations. Automotive, defense, IT, healthcare, and nuclear industries are also at risk of cyberattacks conducted by Yellow Liderc.

Members are encouraged to observe any unusual network traffic, such as identifying suspicious emails and downloads. Verification of the sources of unprompted emails is also highly encouraged to reduce the possibility of more cyberattacks.

Vulnerabilities & Exploits

Urgent: New Security Flaws Discovered in NGINX Ingress Controller for Kubernetes

Summary

- Three new security vulnerabilities affecting Kubernetes NGINX Ingress Controller were just disclosed.

Analysis & Action

Three new security flaws tracked as CVE-2022-4886, CVE-2023-5043 and CVE-2023-5044 were disclosed affecting Kubernetes NGINX Ingress Controller.

CVE-2022-4886 is a path sanitization bug and can be bypassed to obtain the credentials of the ingress-nginx controller, with CVSS (Common Vulnerability Scoring System) score of 8.8. CVE-2023-5043 is an Ingress-nginx annotation injection that could allow arbitrary command execution and has a CVSS score of 7.6. CVE-2023-5044 is a code injection bug via nginx.ingress.kubernetes.io/permanent-redirect annotation, also with a CVSS score of 7.6. In the event of a successful exploitation of the vulnerabilities, the attacker could inject arbitrary code into the ingress controller process, and consequently gain access to sensitive data.

Currently there are no patches available, however certain actions like enabling the "strict-validate-path-type" option and setting the --enable-annotation-validation flag, could mitigate the risk of exploitation.

Trends & Reports

Feds Warn Healthcare Sector of AI-Augmented Phishing Threats

Summary

- HSHC3 published a new advisory warning healthcare organization about AI-powered phishing operations.

Analysis & Action

The Health Sector Cybersecurity Coordination Center (HSHC3) has warned healthcare organizations about the increased threat of AI-powered phishing operations.

Phishing is one of the most popular attack vectors in the healthcare industry, and healthcare employees are especially vulnerable to phishing attempts due to the urgency of their profession and the necessity to reply to potentially vital correspondence in relation to patient condition. Furthermore, AI technology could allow even less experienced attackers to launch sophisticated attacks, potentially increasing influx of the attacks, while also enabling more convincing and targeted phishing campaigns.

Some of the recommended mitigation strategies for the healthcare organizations are configuration of email scanning tools to improve filtering of spam email, application of endpoint security software and multifactor (MFA) authentication measures. Furthermore, healthcare organizations are advised to continuously educate their staff on phishing operations.

Full advisory can be accessed here.

Privacy, Legal & Regulatory

King Charles III Signs Off on UK Online Safety Act, With Unenforceable Spying Clause

Summary

- The United Kingdom has signed the Online Safety Act into law, but it poses the risk of being difficult to enforce.

Analysis & Action

The Online Safety Act, signed into law by King Charles III, is the newest legislation attempting to keep the internet safe. The law requires tech companies to identify and remove all illegal content from their platforms, which includes harmful material that children could see. While fines would be the main punishment, it also includes the possibility of imprisonment for company executives who do not comply.

The biggest issue is that the Office of Communications is given the power to demand, from online service providers, scans of all online communications, via an improved software, disallowing encryption. This could also run the risk of threat actors exploiting this new backdoor scanning system and gain access to personal identifiable information since the system can scan everything from pictures to files and messages.

Members in the UK are urged to read further into the law and ensure they follow all the requirements it sets up. Where applicable, members should also look into an alternative approach to encryption, like a public key to protect their internal communications.

On October 19, 2023, the Health-ISAC Threat Intelligence Committee (TIC) evaluated the current Cyber Threat Level and collectively decided to raise the Cyber Threat Level to Yellow (Elevated). The Threat Level of Yellow (Elevated) is due to threats from concerns regarding hacktivist activity related to the conflict in the Middle East, an uptick in LinkedIn profile impersonations, MFA Bypass, QR code phishing, and the actively exploited Cisco IOS XE bug.

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 | References

The Register
cp24
Bleeping Computer
HHS
The Hacker News
The Record
Dark Reading
Bank Info Security

Tags

Hunters International, Hive Ransomware, Kubernetes, 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