Daily Cyber Headlines

Daily Cyber Headlines | TLP:WHITE | Alert ID : 3e518781 | Oct 10, 2023, 07:39 AM

Today's Headlines:

Leading Story

- Hackers Join in on Israel-Hamas War with Disruptive Cyberattacks

Data Breaches & Data Leaks

- DC Board of Elections Discloses Data Breach

Cyber Crimes & Incidents

- The Source Code of the 2020 Variant of HelloKitty Ransomware Was Leaked on a Cybercrime Forum
- Vietnam Tried to Hack U.S. Officials, CNN With Posts on X, Probe Finds

Vulnerabilities & Exploits

- Coordinated Disclosure: 1-Click RCE on GNOME (CVE-2023-43641)
- Patch Now: Massive RCE Campaign Wrangles Routers into Botnet

Trends & Reports

- Nothing to Report

Privacy, Legal & Regulatory

- Nothing to Report

Cybersecurity Awareness Month

- The Daily Cyber Headlines are being shared during the month of October at **TLP:WHITE** for Cybersecurity Awareness Month.

Upcoming Health-ISAC Events

- Americas Hobby Exercise - October 25, 2023. Registration is available here.
- Health-ISAC Monthly Threat Brief – October 31, 2023, 12:00 PM Eastern

Additional Information

Leading Story

Hackers Join in on Israel-Hamas War with Disruptive Cyberattacks

Summary

- Escalated violence between Israel and Palestine has triggered a surge in cyber activity in the region.

Analysis & Action

Due to an escalation of conflict between Israel and Palestine, cyber-attacks against Israeli infrastructure have increased.

Aside from the involvement of state-sponsored players behind the scenes, various hacktivist organizations have launched attacks in what appears to be a coordinated effort. KillNet declared war on Israel, and Anonymous Sudan, their most prolific affiliate, had joined the fight. Furthermore, over 30 hacktivist groups are believed to have joined campaigns against Israeli critical infrastructure.

Hacktivists have announced attacks on emergency notification systems and electrical grids. Local healthcare organizations are likely to be affected directly by cyber-attacks as part of vital infrastructure, as well as indirectly since assaults on other components of critical infrastructure might increase casualties and injuries, resulting in an increase in patient intake.

Data Breaches & Data Leaks

DC Board of Elections Discloses Data Breach

Summary

- The District of Columbia Board of Elections (DCBOE) from Washington D.C., disclosed a data breach.

Analysis & Action

The District of Columbia Board of Elections (DCBOE), which oversees ballot access, elections, and voter registration, announced that voter data was breached due to a third-party vendor compromise.

The incident occurred at DataNet, a website hosting service used by the agency. Names, driver's license numbers, phone numbers, birth dates, residences, email addresses, partial Social Security numbers, voter IDs, registration dates, political party affiliation, and voting place are among the data that was stolen.

RansomedVC has claimed responsibility for the attack and intends to sell the data. As more organizations have their sensitive data hacked due to third-party compromise, we encourage members to pay special attention to vendor risk management and to keep their networks always segmented to decrease the chance of a successful supply chain attack.

Cyber Crimes & Incidents

The Source Code of the 2020 Variant of HelloKitty Ransomware Was Leaked on a Cybercrime Forum

Summary

- A threat actor, with an alias of Kapuchino, leaked the source code for HelloKitty ransomware.

Analysis & Action

The source code for HelloKitty ransomware is now available on the dark web. HelloKitty, a threat actor suspected to be operating from Ukraine, has been active since January 2021. They are known for hacking corporate networks and encrypting data, while their victims span across industries, including healthcare.

The leaked hellokitty.zip archive contains a Microsoft Visual Studio solution that builds the HelloKitty encryptor and decryptor, and the NTRUEncrypt library, which is used to encrypt files. The archive was leaked by a threat actor with the alias Kapuchino on the dark web.

HelloKitty was previously connected to an Oregon Anesthesiology Group data breach, that exposed data of 750.000 patients. The leak of the source means that other threat actors can use it to develop their own campaigns.

Vietnam Tried to Hack U.S. Officials, CNN With Posts on X, Probe Finds

Summary

- Vietnamese government allegedly targeted high-profile individuals from the United States (US) with spyware.

Analysis & Action

Vietnamese governments had allegedly targeted US politicians with spyware known as Predator. The campaign was supposedly launched as the Vietnamese and American diplomats were holding discussions on regional cooperation agreements between the two countries, with an aim to curb Chinese influence in the region. The said agreement ended up being signed in September.

The operation used the X (ex-Twitter) platform to try to lure high-profile individuals to land on malicious websites that were designed to infect devices with Predator software. Allegedly, however, the campaign was unsuccessful. Presumably, the operation was launched to give more insight into American views on Asia in China to the Vietnamese officials.

The US government has previously blacklisted companies that make and sell spyware software, such as Cytrox and Intellexa, but a more globally unified strategy to attack the spyware sector is required to accomplish the desired effect.

Vulnerabilities & Exploits

Coordinated Disclosure: 1-Click RCE on GNOME (CVE-2023-43641)

Summary

- GitHub Security Lab just disclosed a new vulnerability in the libcue library, a library for parsing cue sheet files.

Analysis & Action

The libcue library flaw, tracked as CVE-2023-43641, is affecting GNOME Linux systems.

The vulnerability is rooted in an out-of-bounds array access in the track_set_index function, allowing code execution by getting victims to download a .cue file from a malicious webpage.

The flaw comes two weeks after GitHub revealed details about a high-severity type confusion vulnerability in the Google Chrome V8 JavaScript engine. Users of GNOME Linux are advised to patch their devices immediately in order to mitigate the risk of exploitation.

Patch Now: Massive RCE Campaign Wrangles Routers into Botnet

Summary

- The campaign dubbed IZ1H9 is using vulnerabilities to create botnets and launch distributed denial-of-service (DDoS) cyberattacks against their targets.

Analysis & Action

Researchers from FortiGuard Labs have identified a campaign called IZ1H9, which has been rapidly developing malware to target unpatched routers and IoT devices. The campaign is using vulnerabilities to create botnets and launch distributed denial-of-service (DDoS) cyberattacks against their targets.

The campaign has been updated with 13 new payloads, exploiting vulnerabilities in D-Link devices; Netis wireless routers; Sunhillo SureLine; Geutebruck IP cameras; and Yealink Device Management, Zyxel devices, TP-Link Archer, Korenix Jetwave, and Totolink routers. A surge of attacks happened on September 6, when the attacks were ranging to tens of thousands.

Targeted vulnerabilities are not zero-day flaws which means most of them have patches readily available. Members are advised to patch their devices and regularly change default login credentials to mitigate the risks of successful attacks.

Trends & Reports

- Nothing to Report.

Privacy, Legal & Regulatory

- Nothing to Report.

Health-ISAC Cyber Threat Level

On September 20, 2023, 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) is due to threats from concerns regarding malvertising, rogue USB drives, Async RAT, MFA Bypass, and persistent credential stuffing/spraying.

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

Security Week
Washington Post
Health-ISAC
GitHub

Dark Reading
Security Affairs
Security Week
GitHub

Tags

HelloKitty, Israel-Hamas, GNOME

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