DAILY CYBER HEADLINES

Health-ISAC Daily Cyber Headlines

TLP:GREEN

Apr 15, 2022

Today's Headlines:

Leading Story

- Microsoft Zero-Days, Wormable Bugs Spark Concern

Data Breaches & Data Leaks

- Nothing to Report

Cyber Crimes & Incidents

- Continuation of Operation Dream Job Sees North Korea-Linked APT Target Orgs in Espionage Campaign
- OldGremlin Ransomware Group Uses New Malware to Target Russian Businesses

Vulnerabilities & Exploits

- Critical Vulnerability in Elementor Plugin Impacts Millions of WordPress Sites
- EnemyBot DDoS Botnet Borrows Exploit Code from Mirai and Gafgyt

Trends & Reports

- Preparing for Armageddon: How Ukraine Battles Russian Hackers

Privacy, Legal & Regulatory

- Ethereum Developer Jailed 63 Months for Helping North Korea Evade Sanctions

Upcoming Health-ISAC Events

- Health-ISAC Monthly Threat Brief – April 26, 2022, 12:00 PM Eastern

Leading Story

Microsoft Zero-Days, Wormable Bugs Spark Concern

Summary

- Microsoft addressed a zero-day under active attack and several critical security vulnerabilities
- Three of the patched vulnerabilities allowed self-propagating exploits

Analysis & Action

Microsoft released patches for 128 security vulnerabilities for the April 2022 Patch Tuesday monthly scheduled update.

Most notably, an actively exploited privilege escalation bug designated CVE-2022-2452, has a patch now available. Microsoft received a report from the National Security Agency (NSA) that the flaw is under active attack.

Health-ISAC joined Microsoft for a Monthly Microsoft Patch Tuesday Podcast which is available for playback here.

The Microsoft April 2022 Security Updates are available for review.

Data Breaches & Data Leaks

Nothing to Report

Cyber Crimes & Incidents

Continuation of Operation Dream Job Sees North Korea-Linked APT Target Orgs in Espionage Campaign

Summary

- Symantec has observed the North Korea-linked Lazarus APT operating a campaign that appears to be a continuation of Operation Dream Job

Analysis & Action

Operation Dream Job involves Lazarus using fake job offers as a means of luring victims into clicking on malicious links or opening malicious attachments that eventually lead to the installation of malware used for espionage.

Past Dream Job campaigns targeted individuals back in August 2020 and July 2021.

A detailed analysis is available from the Symantec blog.

OldGremlin Ransomware Group Uses New Malware to Target Russian Businesses

Summary

- Researchers have disclosed that a small ransomware group named OldGremlin has recently become active again.
- The group, which was inactive for over a year, is using custom backdoors to target businesses based in Russia.

Analysis & Action

OldGremlin prepares its phishing emails with great care and monitors the news agenda closely.

The OldGremlin group was responsible for two phishing campaigns in March 2022, which took advantage of trending news topics.

After the backdoor is in place, the attacker starts collecting information from the compromised system. It can be months before the final payload is deployed, which is TinyCrypt or TinyCryptor; a custom ransomware payload of the OldGremlin group.

The full report is available from Group-IB here.

Vulnerabilities & Exploits

Critical Vulnerability in Elementor Plugin Impacts Millions of WordPress Sites

Summary

- A critical vulnerability addressed in the Elementor WordPress plugin could allow authenticated users to upload arbitrary files to affected websites, potentially leading to code execution.
- Roughly one-third of websites were running a vulnerable version when the bug was found.

Analysis & Action

Elementor is a drag-and-drop website builder for WordPress that has more than 5 million installations.

The newly addressed vulnerability was introduced in version 3.6.0 of the plugin.

The issue was addressed with the release of Elementor version 3.6.3.

WordPress administrators are advised to update to a patched version of the plugin as soon as possible.

Additional details are available from the Elementor changelog.

EnemyBot DDoS Botnet Borrows Exploit Code from Mirai and Gafgyt

Summary

- A threat group that pursues crypto mining and distributed denial-of-service (DDoS) attacks has been linked to a new botnet called Enemybot
- The botnet has been compromising routers and Internet of Things (IoT) devices since last month.

Analysis & Action

The botnet has been attributed to an actor named Keksec and appears to be mainly derived from Gafgyt source code along with borrowing several modules from Mirai's original source code.

The botnet uses the following vulnerabilities:

- CVE-2020-17456

- CVE-2018-10823
- CVE-2022-27226

A detailed analysis is available from the Fortinet blog.

Trends & Reports

Preparing for Armageddon: How Ukraine Battles Russian Hackers

Summary

- Ukrainian IT experts, intelligence officers, and a criminal prosecutor have observed Russian hackers based in Ukraine following the 2014 invasion of Crimea
- The group of hackers was nicknamed Armageddon

Analysis & Action

The hackers have resided in Crimea following the 2014 invasion. Ukraine studied the hackers cyber weapons for several years preceding the recent invasion of Ukraine. This research prepared Ukraine for the tactics, techniques, and procedures orchestrated by Armageddon.

Tracking Armageddon enabled Ukraine to fend of cyberattacks levied in recent weeks.

Health-ISAC will continue to monitor the evolving threatscape in Ukraine as a means of understanding Russian threat actors and the cybercriminal underground that orchestrates aggressive cyber tactics.

Privacy, Legal & Regulatory

Ethereum Developer Jailed 63 Months for Helping North Korea Evade Sanctions

Summary

- A U.S. court has sentenced former Ethereum developer Virgil Griffith to five years and three months in prison.
- The developer must also pay a $100,000 fine for conspiring with North Korea to help use cryptocurrencies to circumvent sanctions imposed on the country.

Analysis & Action

The press release stated Griffith conspired to provide services to North Korea including advice on using cryptocurrency and blockchain technology to avoid sanctions. Griffith admitted in court to taking actions to evade

sanctions, which are in place to prevent North Korea from building a nuclear weapon.

Griffith previously traveled to North Korea to attend and present at the 2019 Pyongyang Blockchain and Cryptocurrency Conference. His presentations included using blockchain smart contracts for nuclear weapon negotiations.

Griffith pleaded guilty and was sentenced to 63 months in jail.

The full press release is available for review.

Health-ISAC Cyber Threat Level

On April 7, 2022, the Health-ISAC Threat Intelligence Committee (TIC) evaluated the current Cyber Threat Level and collectively decided to maintain the Cyber Threat Level at Yellow (Elevated). The Threat Level of Yellow (Elevated) was maintained due to the ongoing Ukrainian – Russian conflict and its subsequent conflict-oriented hacktivism; evolving OFAC-related list and sanctions; a continuous surge in employment scams; and the ongoing phishing lures related to Ukraine.

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 Cywa

Reference(s)	Health-ISAC, Microsoft, Security, Security, Bleeping Computer, group-ib, Security Week, elementor, The Hacker News, NIST-NVD, NIST-NVD, NIST-NVD, Fortinet, Ars Technica, The Hacker News, US Department of Justice, Threat Post

Alert ID 824f96f9

View Alert

Tags Daily Cyber Headlines, DCH

TLP:GREEN Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.

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**