Health-ISAC Daily Cyber Headlines

Daily Cyber Headlines	○ TLP:WHITE	Alert ID : 0164c76c	Oct 22, 2021, 10:31 AM

Today's Headlines:

Leading Story

- Bulletproof Hosting Admins Sentenced for Helping Cybercrime Gangs

Data Breaches & Data Leaks

- Nothing to Report

Cyber Crimes & Incidents

- Evil Corp Demands $40 Million In New Macaw Ransomware Attacks
- DoJ Sues Robocaller to Pay Massive Fine

Vulnerabilities & Exploits

- Threat Actors Abusing Discord to Spread Malware
- CISA: GPS Software Bug May Cause Unexpected Behavior This Sunday

Trends & Reports

- 72% of Organizations Experienced a DNS Attack in the Last Year

Privacy, Legal & Regulatory

- Microsoft Now Defends Nonprofits Against Nation-State Attacks
- CISA Awards $2M to Cybersecurity Training Programs

Upcoming Health-ISAC Events

- Health-ISAC Monthly Threat Brief – October 26, 2021, 12:00 PM Eastern

Additional Info

Leading Story

Bulletproof Hosting Admins Sentenced for Helping Cybercrime Gangs

Summary

- Two Eastern European men were sentenced to prison on Racketeer Influenced Corrupt Organization (RICO) charges for bulletproof hosting services used by multiple cybercrime operations to target US organizations.

Analysis & Action

The duo provided cybercrime-affiliated clients with the infrastructure needed to host exploit kits and to run malicious campaigns distributing spam emails and malware for roughly seven years, between 2008 and 2015. The bulletproof hosting service helped cybercrime gangs register new infrastructure using stolen or false identities that allowed them to circumvent law enforcement efforts to block their attacks.

Malware hosted by the organization included Zeus, SpyEye, Citadel, and the Blackhole Exploit Kit, which attacked US companies and financial institutions between 2009 and 2015 and caused or attempted to cause millions of dollars in losses to US victims, the Department of Justice said in the sentencing memorandum.

The FBI investigated the case with assistance from law enforcement partners from the United Kingdom, Germany, and Estonia. The bulletproof hosting service was founded by Russian citizens Aleksandr Grichishkin and Andrei Skvortsov, who were also indicted in the same case. All four defendants pleaded guilty to one count of RICO conspiracy in February, March, and May 2021. The bulletproof hosting founders also face a maximum penalty of 20 years in prison.

Data Breaches & Data Leaks

Nothing to Report.

Cyber Crimes & Incidents

Evil Corp Demands $40 Million In New Macaw Ransomware Attacks

Summary

- Evil Corp has launched a new ransomware called Macaw Locker to evade United States sanctions that prevent victims from making ransom payments.
- Macaw Locker has been the ransomware behind the Sinclair Broadcast Group and Olympus.

Analysis & Action

The Evil Corp hacking group, also known as Indrik Spider and the Dridex Gang, launched a new ransomware called Macaw Locker in order to evade United States sanctions against them, preventing victims from making ransom payments.

The new malware has been used twice so far, in the weekend ransomware attacks against Olympus and Sinclair Broadcast Group early October 2021. The threat actors demanded a 450 bitcoin ransom, or $28 million, from one victim, and $40 million from the other.

The Macaw Locker ransomware encrypts victims' files and appends the .macaw extension to the file name when conducting attacks. The ransomware will also create ransom notes in each folder named macaw_recover.txt. For each attack, the ransom note contains a victim negotiation page on Macaw Locker's Tor site and an associated decryption ID. It also contains a brief description of what happened to the victim, a tool to decrypt three files for free, and a chatbox to negotiate with attackers.

DoJ Sues Robocaller to Pay Massive Fine

Summary

- The United States' Department of Justice (DoJ) is seeking to recover a financial penalty of nearly $10m that was imposed on Montanan man for operating malicious robocalling campaigns.

Analysis & Action

The Federal Communication Commission (FCC) fined Scott Rhodes $9,918,000 in January of 2021 after discovering that he had illegally used caller ID spoofing with the intent to cause harm. An investigation by the FCC found that between May 2018 and December 2018 Rhodes had made thousands of spoofed robocalls targeting specific communities with malicious pre-recorded xenophobic messages.

Earlier this week, the DOJ filed a complaint against Rhodes in the US District Court for the District of Montana that seeks to recover the financial penalty and obtain an injunction that would prevent Rhodes from committing any further violations of the Truth in Caller ID Act.

The complaint states that Rhodes harassed people in Florida and Georgia with spoofed robocalls that attacked gubernatorial candidates, while in Idaho, he robocalled residents of Sandpoint City, attacking the local newspaper and its publisher.

The department will work with its agency partners to vigorously enforce the telemarketing laws that prohibit these practices, the DoJ said in a statement.

Vulnerabilities & Exploits

Threat Actors Abusing Discord to Spread Malware

Summary

- Researchers have discovered new malware and threat actors abusing the core functions of popular group app platform Discord.

Analysis & Action

Check Point explained in a blog report that it found several malicious GitHub repositories featuring malware based on the Discord API and malicious bots. It included various features, including keylogging, taking screenshots and executing files. Discord bots help users automate tasks on the Discord server. However, they can also be used for malicious purposes, the researchers warned.

For example, the Discord Bot API can easily be manipulated to turn a bot into a simple Remote Access Trojan (RAT). This doesn’t even require the Discord app to be downloaded to a target’s machine.

As of now, any type of file, malicious or not, whose size is less than 8MB can be uploaded and sent via Discord. Because the file content isn’t analyzed, malware can be easily spread via Discord, the report concluded.

CISA: GPS Software Bug May Cause Unexpected Behavior This Sunday

Summary

- The cybersecurity and Infrastructure Security Agency (CISA) warned that GPS devices might experience issues over the weekend of October 22, 2021, due to a timing bug impacting Network Time Protocol (NTP) servers running the GPS Daemon (GPSD) software.

Analysis & Action

The cybersecurity and Infrastructure Security Agency (CISA) warned that GPS devices might experience issues over the weekend of October 22, 2021, due to a timing bug impacting Network Time Protocol (NTP) servers running the GPS Daemon (GPSD) software. The bug is set to trigger on October 24th, but they are unable to predict what the implications will be, as the systems may become unresponsive or unavailable.

On October 24, 2021, all NTP servers using GPSD versions 3.2 through 3.22 are going to jump back 1024 weeks in time, to March 3rd, 2002. The vulnerable versions were released between late December 2019 and early January 2021, so CISA urges all affected owners to update to GPSD version 3.23 (released August 2021) or newer to avoid all changes of facing problems.

Every 1024 weeks, a week number rollover phenomenon takes place in the system due to an integer overflow on the broadcasted ten-digit binary, causing the internal value of the week count to drop to zero. The last time it occurred was during April 2019, and caused flight cancellations, wireless network crashes, and functional problems on older smartphones.

Health-ISAC has produced an additional intelligence report on this issue, the link can be found here.

Trends & Reports

72% of Organizations Experienced a DNS Attack in the Last Year

Summary

- 72% of organizations have suffered a domain name system (DNS) attack in the last 12 months, according to a new data by the Neustar International Security Council (NISC).

Analysis & Action

The 302 security professionals from six EMEA and US markets included in the survey were also asked about the damage caused by these incidents. Among those organizations targeted, 58% saw their businesses disrupted for over an hour, 14% took several hours to recover. However, around one-third were able to recover within minutes.

While Neustar noted that DNS attacks are generally a lower concern for security pros than vectors like ransomware, distributed denial-of-service (DDoS), and targeted account hacking, they are becoming increasingly menacing to organizations. According to its latest study, 55% of security professionals consider DNS compromise an increasing threat, compared to 47% in October 2020.

The most common types of DNS attacks experienced were DNS hijacking, at 47%, DNS flood, reflection or amplification attacks that segued into DDoS at 46%, DNS tunneling, at 35%, and cache poisoning, at 33%.

Privacy, Legal & Regulatory

Microsoft Now Defends Nonprofits Against Nation-State Attacks

Summary

- Microsoft announced a new security program for nonprofit organizations to provide them with protection against nation-state attacks that have been increasingly targeting them in recent years.

Analysis & Action

Microsoft launched the program in response to the increasing cybercrime impacting industry sectors worldwide – especially nonprofits, due to their vulnerability of lack of adequate resources to build a suitable defense.

Through the new Security program for nonprofits, Microsoft aims to provide monitoring and notification in the case of a nation-state attack, assess organization and infrastructure rest to help nonprofits enhance their security posture based on environment, and streamline security training for IT professionals and end-users.

CISA Awards $2M to Cybersecurity Training Programs

Summary

- The United States' Cybersecurity and Infrastructure Security Agency (CISA) has awarded NPower and CyberWarrior $2M to develop their cybersecurity workforce training programs.

Analysis &Action

The awards are the first of their kind for the agency, and the recipients plan to use the cash to bring cybersecurity training to the unemployed and to underemployed communities. The programs will focus on training underserved communities in rural and urban areas and seek to recruit traditionally underrepresented groups in the cybersecurity industry, such as women, people of color, and military spouses.

CyberWarrior will host the program in the form of a 28-week bootcamp, and CISA's support will help NPower to expand the reach of its training program across the United States. The goal of the program is to help recruit and train individuals from all areas and backgrounds with the aptitude and attitude to succeed in the cybersecurity field. Additionally, CISA's other workplace developments include the CYBER.org initiative and the K-12 student and teacher oriented Cyber Education and Training Assistance Program.

Reference | References

Bleeping Computer
Bleeping Computer
Info Security Magazine
Bleeping Computer
Bleeping Computer
Bleeping Computer
Bleeping Computer
Health-ISAC

Info Security Magazine
Health-ISAC
Info Security Magazine
Info Security Magazine
Health-ISAC

Tags

Daily Cyber Headlines, DCH

TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.