DAILY CYBER HEADLINES

Health-ISAC Daily Cyber Headlines

TLP:GREEN

Feb 11, 2022

Today's Headlines:

Leading Story

- FritzFrog Botnet Grows 10x, Hits Healthcare, Edu, and Govt Systems

Data Breaches & Data Leaks

- Hacking Incidents Reported by AccelHealth and Pace Center for Girls

Cyber Crimes & Incidents

- Nothing to Report

Vulnerabilities & Exploits

- Microsoft Fixes Defender Flaw Letting Hackers Bypass Antivirus Scans

Trends & Reports

- Importance of API Security in Healthcare Grows as Cyberattacks Increase
- Hacking Group ModifiedElephant Evaded Discovery for a Decade
- $1.3 Billion Lost to Romance Scams in the Past Five Years

Privacy, Legal & Regulatory

- Former NFL Player Gets Five Years for Healthcare Fraud

Upcoming Health-ISAC Events

- Health-ISAC Monthly Threat Brief – February 22, 2022, 12:00 PM Eastern

Leading Story

FritzFrog Botnet Grows 10x, Hits Healthcare, Edu, and Govt Systems

Summary

- The FritzFrog botnet that has been active for more than two years has resurfaced with an alarming infection rate, growing ten times in a month of hitting healthcare, education, and government systems with an exposed SSH server.

Analysis & Action

FritzFrog malware is written in Golang and relies on custom code. The malware is primarily run-in memory and is decentralized, so it does not need a central management server. Researchers at Akami, a security company, observed a new version of FritzFrog malware

utilizing a Tor proxy chain and indicates that more capabilities are coming that would allow the targeting of WordPress servers.

The operators of the FritzFrog malware have previously hit systems in China, a TV network in Europe, various East Asian universities, and a Russian healthcare firm, suggesting that all of these industries are susceptible to further attacks.

Akami's security recommendations include enabling system login auditing with alerting capabilities, monitoring the authorized_hosts file on Linux, and others.

Akami's full report can be found here.

Data Breaches & Data Leaks

Hacking Incidents Reported by AccelHealth and Pace Center for Girls

Summary

- AccelHealth and Pace Center for Girls have discovered security breaches that have led to the compromise of protected health information

Analysis & Action

AccelHealth suffered a ransomware attack on December 15, 2021, which prevented the Federally Qualified Health Center from accessing certain files and folders on its network. Investigators discovered that unauthorized individuals had gained access to the network on December 9th and may have viewed or acquired files containing patient information. 48,126 patients were impacted, though no evidence of data exfiltration or misuse has been found.

Pace Center for Girls has discovered certain infrastructure systems were accessed by unauthorized individuals who may have viewed or acquired the sensitive data of current and former students. The breach was detected in the week of December 13, 2021, and it was confirmed that the compromise had first occurred in January of 2021. A third-party cybersecurity firm was hired to help secure its network and physical computer access and assess its data protection and gateway security systems.

Cyber Crimes & Incidents

There is nothing to report.

Vulnerabilities & Exploits

Microsoft Fixes Defender Flaw Letting Hackers Bypass Antivirus Scans

Summary

- Microsoft has recently addressed a weakness in the Microsoft Defender Antivirus on Windows that allowed attackers to plant and execute malicious payloads without triggering Defender's malware detection engine.

Analysis & Action

The flaw resulted from lax security settings for the Windows Defender Exclusions registry key and has affected the latest Windows 10 versions. Exploiting the weakness was possible because the registry key was accessible by the Everyone group, making it possible for local users to access it through the command line.

After installing the February 2022 Patch Tuesday Windows updates, the flaw can no longer be accessed.

Trends & Reports

Importance of API Security in Healthcare Grows as Cyberattacks Increase

Summary

- As more organizations rely on APIs to run critical functions, ensuring API security in healthcare is crucial to preventing cyberattacks, according to security firm Gartner.

Analysis & Action

API security is essential to healthcare cybersecurity as threat actors increasingly turn to APIs as an easy network entry point. Cequence, an API security firm, analyzed API usage patterns from June to

December 2021 and found that health monitoring API usage rose by 941%.

APIs can increase productivity, cut costs, and allow innovation and collaboration. However, there have been significant increases in account scraping, account takeovers, and malicious traffic surrounding API use. Developers must prioritize API security and data privacy to prevent threat actors from easily manipulating APIs.

The full report issued by Gartner can be found here.

More information on proper API security measures can be found here.

Hacking Group ModifiedElephant Evaded Discovery for a Decade

Summary

- Researchers at SentinelLabs detailed the tactics of ModifiedElephant explaining how recently published evidence helped them attribute previously orphan attacks.

Analysis & Action

The most reliable evidence is overlapping infrastructure observed in multiple campaigns between 2013 and 2019, as well as consistency in the malware deployed. The group employees readily available trojans through spear phishing, and has been targeting human rights activists, free speech defenders, academics, and lawyers in India since 2012. The malicious emails push keyloggers and remote access trojans.

The primary malware deployed on the campaigns are NetWire and DarkComet, two remote access trojans that are publicly available and widely used by lower-tier cybercriminals.

The full report issued by SentinelLabs can be found here.

$1.3 Billion Lost to Romance Scams in the Past Five Years

Summary

- According to the US Federal Trade Commission (FTC), romance-based fraud and scams have reached a record high, with $547 million in losses reported in 2021 in the US.

Analysis & Action

In total, consumers have lost at least $1.3 billion. Data collected reveals that losses were up almost 80% last year in comparison to 2020 and overall, the trend continues to surge upward. The average victim can lose around $2,400.

A new vector for these scams includes cryptocurrency, where the scammer will gain the trust of the victim, then offer them a lucrative and time-sensitive business opportunity, which leads to the theft of funds and in some cases, sensitive data.

The full report published by the FTC can be found here.

Privacy, Legal & Regulatory

Former NFL Player Gets Five Years for Healthcare Fraud

Summary

- A former player for the National Football League (NFL) has been jailed for five years for his part in a major fraud scheme involving over 50 other players.

Analysis & Action

Robert McCune has pleaded guilty to one count of conspiracy to commit health care fraud and wire fraud, 10 counts of wire fraud, 12 counts of healthcare fraud, and three counts of aggravated identity theft.

Between June 2017 and April 2019, McCune submitted false documents on behalf of dozens of former players and himself, seeking reimbursement for non-existent medical treatment and equipment. McCune and his co-conspirators are said to have submitted around $2.9 million in fraudulent claims in this way.

As telemedicine continues to grow, it is important to remain wary of healthcare fraud, which can be triggered through phishing attacks or identity theft. Telemedicine has become an easy route for those

seeking non-legitimate reimbursement of fake medical treatments and equipment.

Health-ISAC Cyber Threat Level

On February 3, 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) due to Russian aggression towards Ukraine; ongoing cleanup operations for the Log4j vulnerability; increased instances of ransomware; actors releasing fraudulent job applications online, and new, sophisticated phishing techniques using reverse-proxy tools to bypass multi-factor authentication.

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(s)	gartner, Health-ISAC, Info Security Magazine, Health IT Security, ZDNet, HIPAA Journal, Bleeping Computer, Sentinel One, FTC, Bleeping Computer, Akamai, Health-ISAC, Health IT Security, Bleeping Computer

Alert ID c9fc4d4b

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**