Health-ISAC Daily Cyber Headlines

Daily Cyber Headlines	○ TLP:WHITE	Alert ID : 388a87cf	Oct 21, 2021, 10:17 AM

Today's Headlines:

Leading Story

- CISA Leader Backs 24-Hour Timeline for Incident Reporting

Data Breaches & Data Leaks

- Nothing to Report.

Cyber Crimes & Incidents

- Google Disrupts Massive Phishing and Malware Campaign

Vulnerabilities & Exploits

- Political-Themed Actor Using Old MS Office Flaw to Drop Multiple RATs

Trends & Reports

- 81% of UK Healthcare Organizations Hit by Ransomware in Last Year
- CISOs Call for Healthcare Cybersecurity Federal Assistance

Privacy, Legal & Regulatory

- US Govt to Ban Export of Hacking Tools to Authoritarian Regimes
- CMS Selects 4 States for ACO-Based Rural Telehealth Delivery Model

Upcoming Health-ISAC Events

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

Additional Info

Leading Story

CISA Leader Backs 24-Hour Timeline for Incident Reporting

Summary

- The Executive Director of the U.S. Cybersecurity and Infrastructure Security Agency (CISA) has voiced support for a 24-hour timeline for cyber incident reporting involving critical infrastructure.

Analysis & Action

Bandon Wales, the executive director of CISA, said that the U.S. government has argued that 24 hours is the right amount of time for a company to determine whether cyber incidents are real or not, while still being early enough to use all the information. The goal is to focus on rapid information sharing, which will help target areas where threats are currently existing and provide CISA with data to help prioritize resources without disseminating information to the private sector operators of critical infrastructure.

The support for the 25-hour timeline aligns with the Cyber Incident Notification Act of 2021, a bill that would require federal agencies, contractors, and organizations that are considered critical to U.S. national security to report security incidents to CISA within 24 hours. Companies that do not report an incident within 24 hours could face a maximum financial penalty equal to 0.5% of the previous year's gross revenue, but the measure allows for exceptions.

Data Breaches & Data Leaks

Nothing to report.

Cyber Crimes & Incidents

Google Disrupts Massive Phishing and Malware Campaign

Summary

- Google has blocked 1.6 million phishing emails since May 2021 that were part of a malware campaign run by Russian subcontractors to hijack YouTube accounts and promote cryptocurrency scams.

Analysis & Action

Google's threat Analysis Group (TAG) announced that since late 2019 it has been disrupting phishing campaigns run by a network of Russian hacker subcontractors who have been targeting YouTubers with highly customized phishing emails and cookie-stealing malware. The main goal of the group has been to hijack YouTube accounts to live-stream scams that offer free cryptocurrency in exchange for initial contribution. The other main revenue source was selling those hijacked channels from $3 to $4,000, depending on how many subscribers a channel has.

Google says that as of May, it has blocked 1.6 million messages to targets, displayed 62,000 Safe Browsing phishing alerts, and restored around 4,000 hijacked accounts. It has also identified 1,011 domains that were created for malware delivery, impersonating well-known tech sites like Luminar, Cisco VPN, and games on Steam.

Vulnerabilities & Exploits

Political-Themed Actor Using Old MS Office Flaw to Drop Multiple RATs

Summary

- A threat actor with political motives is running a campaign delivering multiple Windows and Android RATs (remote access tools) through the exploitation of CVE-2017-11882.

Analysis & Action

The unknown threat actor was spotted by researchers at Cisco Talos, who didn’t find any strong links to a particular nation, apart from a Pakistani IT front company named Bunse Technologies.

The four-years-old Microsoft Office Equation Editor bug was addressed in a November 2017 patch, but it appears that it's still exploitable for leverage, especially in India and Afghanistan where the targets of this campaign are based. The actor has registered multiple domains that feature political themes such as diplomatic and humanitarian efforts and uses them to deliver malware payloads to the victims.

Although the actor is generally using commodity malware in this campaign, the appearance of custom downloaders and CVE-2017-11882 is a sign that they are looking to shift away from using detectable tools.

Trends & Reports

81% of UK Healthcare Organizations Hit by Ransomware in Last Year

Summary

- More than 81% of United Kingdom (UK) healthcare organizations suffered a ransomware attack in 2020, with 38% electing to pay the ransom to have their files returned and 44% refusing and having their data destroyed as a result.

Analysis & Action

A survey of 100 cybersecurity managers in the UK’s health sector revealed that 38% of organizations have been attacked by ransomware and paid the demand, and 44% of organizations have refused to pay the demand and suffered the loss of their healthcare data because of it. Of these attacks, 64% of victims have had to cancel in person appointments because of them, and 65% of organizations believe that a cyber-attack on their systems could lead to loss of life.

In 2021, there has been a 30% increase in attacks on healthcare industry IT infrastructure between Quarter three and Quarter two of the fiscal year. This rise was observed across multiple attack vectors, including email security threats, insider attacks, and perimeter breaches.

George Patsis, the CEO of Obrela, commented that the security community and the UK government should use this data as a call to action to step in and assist.

CISOs Call for Healthcare Cybersecurity Federal Assistance

Summary

- A survey of CISOs and other healthcare IT leaders has revealed that healthcare cybersecurity is lacking in federal assistance and resources needed to combat cyber threats.

Analysis & Action

The survey, which was funded by the College of Healthcare Information Management Executives (CHIME) and Association for Executives in Healthcare Information Security (AEHIS), revealed that over 80 percent of respondents reported increased cyber insurance costs over the past year as healthcare cybersecurity incidents continue to multiply. One in six respondents saw a 100 percent cost increase, and more than 20 percent of respondents saw a 50 percent cost increase in the last year.

Over 65 percent of respondents indicated that their organizations had experienced a cybersecurity incident in the last 12 months. Phishing, malware, ransomware, hacking, and insider threats were identified as the most common security exploits. Approximately 40 percent of respondents reported needing help in terms of grants and federal assistance, and a third of respondents said they would appreciate having regional extension centers (RECs) with cyber experts on hand who could provide guidance and expertise. The full CHIME and AEHIS survey can be accessed here.

Privacy, Legal & Regulatory

US Govt to Ban Export of Hacking Tools to Authoritarian Regimes

Summary

- The United States Commerce Department's Bureau of Industry and Security (BIS) has announced new controls that would ban US companies from exporting and reselling software and hardware tools that could be used to support authoritarian practices through malicious hacking activities and human rights abuse.

Analysis & Action

The rule will become effective in 90 days and will effectively ban the export of cybersecurity tools for national security and anti-terrorism reasons. BIS' new rule says that these items warrant controls because they could be leveraged to conduct malicious cyber activities, including but not limited to surveillance, espionage, or other actions that would disrupt, deny or degrade access to network devices.

The United States Government opposes the misuse of technology to abuse human rights or conduct other malicious cyber activities, and these new rules will help ensure that U.S. companies are not fueling authoritarian practices, the BIS said in a public statement.

CMS Selects 4 States for ACO-Based Rural Telehealth Delivery Model

Summary

- Four US states will receive federal funding to expand telehealth and other services in rural areas through an accountable care organization (ACO) model of care.

Analysis & Action

The Centers for Medicare & Medicare Services (CMS) will provide funding to the University of Alabama at Birmingham (UAB), South Dakota’s Department of Social Services, Texas’ Health and Human Services Commission and the Washington State Healthcare Authority to implement the Community Health Access and Rural Transformation (CHART) model. Those organizations will develop telehealth and other services through an ACO transformation tracks that leverages value-based payment models. This CHART funding will help test whether improving access to telehealth services and access to adequate transportation for those living in rural areas can maintain or improve care quality and lower health care costs.

The organization will spend the next 15 months convening an advisory council, establishing partnerships, recruiting hospitals and developing a plan with those hospitals and their surrounding communities to improve healthcare access.

Reference | References

Info Security Magazine
Bleeping Computer
Gov Info Security
Health-ISAC
Bleeping Computer
chimecentral
mhealthintelligence
Health-ISAC
Health IT Security
ZDNet

Tags

Daily Cyber Headlines, DCH

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