Health-ISAC Daily Cyber Headlines

Daily Cyber Headlines | TLP:WHITE | Alert ID : 165d20c3 | Oct 12, 2021, 04:01 PM

Today's Headlines:

Leading Story

- Microsoft: Azure Customer Hit by Record DDoS Attack in August

Data Breaches & Data Leaks

- Hospital Hacker Steals Patients' Data

Cyber Crimes & Incidents

- Euro Police Disrupt $17m Fake Investment Scheme
- Banking Insider Accused of Role in $1m BEC Scheme

Vulnerabilities & Exploits

- Nothing to Report

Trends & Reports

- UK Firms Hit by One Attack Every 47 Seconds Over Summer
- Over 90% of Firms Suffered Supply Chain Breaches Last Year

Privacy, Legal & Regulatory

- Most Insurers Mandate MFA, But Premiums Are Still Soaring

Upcoming Health-ISAC Events

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

Additional Info

Leading Story

Microsoft: Azure Customer Hit by Record DDoS Attack in August

Summary

- Microsoft has mitigated a record 2.4 terabytes per second (Tbps) Distributed Denial-of-Service (DDoS) attack targeting a European Azure customer during the last week of August.

Analysis & Action

This is 140 percent higher than a 2020 1 Tbps attack and higher than any network volumetric event previously detected on Azure, said a Senior Program Manager for Azure Networking, describing the attack as a User Datagram Protocol (UDP) reflection attack. The attack was launched using roughly 70,000 bots, mainly across the Asia-Pacific region. The attackers hit Azure's infrastructure in terse bursts over a 10-minute timeframe, each of these bursts reaching terabit volumes.

The attack came after Microsoft reported a 25 percent increase in attacks compared to 2020 Q4, with a decline in maximum volumetric throughput, from 1Tbps in 2020 Q3 to 625 Megabits per second in the first half of 2021.

Data Breaches & Data Leaks

Hospital Hacker Steals Patients' Data

Summary

- An unknown cyber-attacker has deleted data belonging to patients of a hospital in New Mexico.

Analysis & Action

An unauthorized individual breached the IT network of San Juan Regional Medical Center (SJRMC) in Farmington in September last year. The attack was reported to the United States Department of Health and Human Services' Office for Civil Rights on June 4, 2021 as a network server security incident impacting 68,792 individuals.

In a statement released on October 7, 2021, the hospital said it had launched an investigation after identifying unauthorized access to its network on September 8, 2020. SJRMC has not found any evidence to suggest that the compromised data has been misused. The hospital said that the attack did not involve ransomware. Individuals whose Social Security numbers were in the files removed during the cyber-attack are being offered complimentary credit monitoring services.

Cyber Crimes & Incidents

Euro Police Disrupt $17m Fake Investment Scheme

Summary

- European police have disrupted a financial crime organization said to have made at least €15m by tricking investors.

Analysis & Action

Between May 2019 and September 2021, the criminal network reportedly lured German investors via adverts on social media and elsewhere, supported by over 250 newly registered domain names. As part of the scam, two call centers were reportedly set up where around 100 employees were required to pose as financial advisors and try to sell fake financial options for investing.

The criminal gang behind the scam took the money invested by clients and pocketed the funds so that they didn't receive any payment of winnings or credit balance updates following their investment.

It's unclear where the scam's ringleaders were based, but the criminal network is said to have been connected to a Ukrainian company. The investigation has also so far led to 246 criminal proceedings across 15 German federal states.

Banking Insider Accused of Role in $1m BEC Scheme

Summary

- Three men including one former bank employee have been indicted by a federal grand jury for their alleged role in a business email compromise (BEC) conspiracy.

Analysis & Action

Onyewuchi Ibeh, Jason Joyner, and Mouaaz Elkhebri were charged with money laundering and aggravated identity theft, according to a superseding indictment late last week. According to the court documents, the trio targeted firms of all sizes across the globe between January 2018 and March 2020.

After phishing their way into employee accounts, they would allegedly conduct months-long reconnaissance before stepping in when a supplier invoice was expected by the victim company by substituting their own highly convincing request for payment.

Faked domains mimicking those of the supplier were employed to add legitimacy to their communications with the victim organization. At least five businesses lost over $1.1m in total over the period, with the co-conspirators laundering the funds through dozens of bank accounts, according to the Department of Justice. Each faces a maximum penalty of 20 years in prison.

Vulnerabilities & Exploits

Nothing to Report.

Trends & Reports

UK Firms Hit by One Attack Every 47 Seconds Over Summer

Summary

- Cyber-attacks targeting UK firms are increasing, reaching a rate of one incident every 47 seconds over the summer, according to new data from Beaming.

Analysis & Action

Beaming noted a 9% year-on-year drop in the second quarter, but it now appears that was a temporary blip. Attacks increased 4% between July and September over the same period last year. IoT applications and systems attracted the most compromise attempts, amounting to 162 per day, while attempts to breach web applications increased by 21% to reach 48 per day on average.

Beaming has been recording attack traffic patterns since 2016, and Q2's decline was the first since 2018. However, that now seems to have been merely a slight interruption of the general upward trend in attacks. Beaming's managing director urged companies to remain vigilant as they transition to new hybrid working practices.

Over 90% of Firms Suffered Supply Chain Breaches Last Year

Summary

- 93% of global organizations have suffered a direct breach due to weaknesses in their supply chains over the past year, according to new data from BlueVoyant.

Analysis & Action

BlueVoyant polled 1200 IT and procurement leaders responsible for supply chain and cyber-risk management from global companies with 1,000+ employees to compile its report titled Managing Cyber Risk Across the Extended Vendor Ecosystem.

The report revealed the average number of breaches experienced in the past 12 months grew from 2.7 in 2020 to 3.7 in 2021, a 37% year-on-year increase.

Although the percentage of companies that don't consider third-party risk a priority has fallen from 31% last year to 13% in 2021, the number who admit they have no way of knowing if an incident has occurred in their supply chain rose from 31% to 38%.

The full BlueVoyant report can be accessed here.

Privacy, Legal & Regulatory

Most Insurers Mandate MFA, But Premiums Are Still Soaring

Summary

- US cyber-insurers are increasing premiums and lowering coverage limits despite mandating stricter security controls as a pre-requisite for coverage, according to a new report from Risk Placement Services (RPS).

Analysis & Action

The US Cyber Market Outlook report warns that providers have been battered by higher-than-anticipated recent losses and are now generally charging much more for less coverage. Over the past year, we've seen the challenges of the COVID-19 pandemic and increasing frequency and severity of ransomware attacks put pressure on the US cyber liability market, said an RPS representative.

Sectors hit hard over the past year, including education, government, healthcare, construction, and manufacturing, have seen premiums increase by 300% or more at renewal time. This is even if corporate policyholders have the right set of security controls in place. Such controls are becoming increasingly widespread, according to RPS. Multi-factor authentication (MFA) is now described as a must-have to even qualify for coverage.

The full RPS report can be accessed here.

Reference | References

Info Security Magazine
Info Security Magazine
Info Security Magazine
Info Security Magazine
Info Security Magazine

bluevoyant
rpsins
Info Security Magazine
Bleeping Computer

Tags

Daily Cyber Headlines, DCH

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

For Questions or Comments: Please email us at toc@h-isac.org