September 21, 2021

Challenge yourself with our ABCs of Cyber Security quiz!

This week's stories:

A 'digital spy in your pocket': Zero-click hack blocked by Apple, but what is it?

Apple users are being asked to install a security update after researchers found a flaw that hackers could use to access devices without any user action.

The researchers from Citizen Lab at the University of Toronto said in a report on Monday that a "zero-click exploit" was found in iMessage on a Saudi activist's iPhone. Apple released a software patch on Monday in response to the exploit.

https://globalnews.ca/news/8189561/digital-spy-zero-click-hack-apple-explained/

Click above link to read more.

Back to top

Why auto industry has seen a massive increase in fraud

Despite the popular perception of identity theft as a major cause of fraud, it accounts for only 20% of auto loan fraud risk while income and employment misrepresentation account for 60% of loan losses, says Justin Davis, fraud consultant at Point Predictive.

"Income misrepresentation is hard to catch without really causing friction for consumers. In the auto industry, you have lenders but you also have to worry about the dealership. A lot of dealers have also started committing fraud," says Davis.

https://www.bankinfosecurity.com/auto-industry-has-seen-massive-increase-in-fraud-a-17537

Click above link to read more.

Back to top

FBI: $113 million lost to online romance scams this year

"The FBI warns of a rising trend in which scammers are defrauding victims via online romance scams, persuading individuals to send money to allegedly invest or trade cryptocurrency," the federal law enforcement agency said in a PSA published today on the Internet Crime Complaint Center (IC3) site.

"From January 1, 2021 — July 31, 2021, the FBI Internet Crime Complaint Center (IC3) received over 1,800 complaints, related to online romance scams, resulting in losses of approximately $133,400,000."

https://www.bleepingcomputer.com/news/security/fbi-113-million-lost-to-online-romance-scams-this-year/

Click above link to read more.

Back to top

Universal decryptor released for past ransomware victims

Romanian cybersecurity firm Bitdefender has published today a universal decryption utility that will be able to help past victims of the REvil (Sodinokibi) ransomware gang recover their encrypted files — if they still have them.

Made available through the company's research blog, Bitdefender said the decryptor was developed **"**in collaboration with a trusted law enforcement partner**."**

The company said it couldn't elaborate more, citing an ongoing law enforcement investigation.

https://therecord.media/universal-decryptor-released-for-past-revil-ransomware-victims/

Click above link to read more.

Back to top

Cryptocurrency launchpad hit by $3 million supply attack

SushiSwap's chief technology officer says the company's MISO platform has been hit by a software supply chain attack. SushiSwap is a community-driven decentralized finance (DeFi) platform that lets users swap, earn, lend, borrow, and leverage cryptocurrency assets all from one place. Launched earlier this year, Sushi's newest offering, Minimal Initial SushiSwap Offering (MISO), is a token launchpad that lets projects launch their own tokens on the Sushi network.

Unlike cryptocurrency coins that need a native blockchain and substantive groundwork, DeFi tokens are an easier alternative to implement, as they can function on an existing blockchain. For example, anybody can create their own "digital tokens" on top of the Ethereum blockchain without having to recreate a new cryptocurrency altogether.

https://arstechnica.com/information-technology/2021/09/cryptocurrency-launchpad-hit-by-3-million-supply-chain-attack/

Click above link to read more.

Back to top

Europol busts major crime ring, arrests over 100 online fraudsters

Law enforcement agencies in Italy and Spain have dismantled an organized crime group linked to the Italian Mafia that was involved in online fraud, money laundering, drug trafficking, and property crime, netting the gang about €10 million ($11.7 million) in illegal proceeds in just a year.

"The suspects defrauded hundreds of victims through phishing attacks and other types of online fraud such as SIM swapping and business email compromise before laundering the money through a wide network of money mules and shell companies," Europol said in a statement published today.

https://thehackernews.com/2021/09/europol-busts-major-cybercrime-ring.html

Click above link to read more.

Back to top

Skills gap in healthcare IT industry causes security threats, according to new report

Research from European provider of cloud infrastructure and cloud services, IONOS Cloud, has found that 37% of healthcare IT decision-makers say their organisation is at risk of security threats due to skills gaps.

Additionally, four in 10 (39%) are facing a skills gap in data protection, with a quarter (25%) saying it means they are not adhering to necessary legislation or following the correct data protection procedures (21%).

https://www.healthcareitnews.com/news/emea/skills-gap-healthcare-it-industry-cause-security-threats-according-new-report

Click above link to read more.

Back to top

AT&T phone-unlocking malware ring costs carrier $200M

The ringleader of a seven-year phone-unlocking and malware scheme will head to the clink for 12 years, according to the Department of Justice, after effectively compromising AT&T's internal networks to install credential-thieving malware.

The perp, one Muhammad Fahd of Pakistan and Grenada, was convicted of grooming AT&T employees at a Bothell, Wash. call center to take part in the scam. He and his now-deceased co-conspirator bribed employees to first use their AT&T credentials to sever phones from the AT&T network for customers who were still under contract — meaning those customers could take their newly independent phones to another service. And then later, Fahd asked his accomplices in the call center to install custom malware and "hacking tools that allowed him to unlock phones remotely from Pakistan," according to court documents.

https://threatpost.com/att-phone-unlocking-malware/174787/

Click above link to read more.

Back to top

Ransomware accounted for a quarter of all cyber insurance claims in Europe between 2016 and 2020

Almost a quarter of all cyber insurance claims filed between 2016 and 2020 across continental Europe have been related to ransomware attacks, according to insurance giant Marsh.

The numbers are even higher when 2020 is analyzed alone, with almost a third (32%) of all cyber insurance claims filed last year being related to a ransomware incident, the company said in "The Changing Face of Cyber Claims 2021," a report that reviewed the Marsh cyber insurance business from the past half-decade.

https://therecord.media/ransomware-accounted-for-a-quarter-of-all-cyber-insurance-claims-in-europe-between-2016-and-2020/

Click above link to read more.

Back to top

How to see who is trying to break into your Office 365 and what they're trying to hack

We've all had spam and phish from compromised Office 365 systems. They're a prime target for bad actors, as mail from Exchange Online is highly trusted, and with the automation tools Microsoft has developed hackers can use the Microsoft Graph APIs to programmatically send messages in the background, while the owner of the compromised account carries on working without knowing that their email address is hard at work for someone else.

https://www.techrepublic.com/article/how-to-see-who-is-trying-to-break-into-your-office-365-and-what-theyre-trying-to-hack/

Click above link to read more.

Back to top

Hacker makes off with $12 million in latest DeFi breach

In the latest security incident involving a decentralized finance protocol, cross-chain project pNetwork announced Sunday it had been hacked for 277 pBTC, a form of wrapped bitcoin, with losses worth over $12 million at current value.

In a series of tweets announcing the incident, pNetwork said, "We're sorry to inform the community that an attacker was able to leverage a bug in our codebase and attack pBTC on BSC, stealing 277 BTC (most of its collateral). The other bridges were not affected. All other funds in the pNetwork are safe."

https://www.bankinfosecurity.com/hacker-makes-off-12-million-in-latest-defi-breach-a-17580

Click above link to read more.

Back to top

$5.9 million ransomware attack on farming co-op may cause food shortage

Iowa-based provider of agriculture services NEW Cooperative Inc. has been hit by a ransomware attack, forcing it to take its systems offline. The BlackMatter group that is behind the attack has put forth a $5.9 million ransom demand. The farming cooperative is seen stating the attack could significantly impact the public supply of grain, pork, and chicken if it cannot bring its systems back online.

Ransomware group BlackMatter has hit NEW Cooperative and is demanding $5.9 million to provide a decryptor, according to screenshots shared online by threat intel analysts.

https://arstechnica.com/information-technology/2021/09/5-9-million-ransomware-attack-on-farming-co-op-may-cause-food-shortage/

Click above link to read more.

Back to top

---

https://www.gov.bc.ca/informationsecurity

OCIOSecurity@gov.bc.ca