December 6, 2022

Challenge yourself with our Holiday Scam Security Quiz!

This past week's stories:

- **Maple Leaf Foods confirms cyberattack, will not pay ransomware gang**
- **Hackers leak another set of Medibank customer data on the dark web**
- **Hyundai app bugs allowed hackers to remotely unlock, start cars**
- **Australia will now fine firms up to AU$50 million for data breaches**
- **LastPass breach fallout spreads to expose customer data**
- **Encryption provider for Sony leaks data for over a year**
- **FBI, CISA say Cuba ransomware gang extorted $60M from victims this year**
- **Vatican shuts down its website amid hacking attempts**
- **Google rolls out new Chrome browser update to patch yet another zero-day vulnerability**
- **Hackers linked to Chinese government stole millions in Covid benefits, Secret Service says**
- **BlackProxies – A criminal proxy services selling a million access to hackers**
- **The top ten hacks and cyber security threats of 2022**
- **BeCyberAware.eu - launches the largest EU funded cyber security awareness campaign related to digital commerce**
- **Rackspace confirms outage was caused by ransomware attack**

Maple Leaf Foods confirms cyberattack, will not pay ransomware gang

Maple Leaf Foods has confirmed that it has been struck by ransomware, but it has also stated that it will not pay for any ransom to have the malware lifted from its systems.

The packaged meats company's confirmation comes after the Black Basta ransomware gang listed Maple Leaf Foods as one of its victims. A security industry source told IT World Canada that a listing on the gang's website appeared last week which contained multiple screenshots of different documents that were allegedly copied from Maple Leaf Foods. While copies of the stolen files were unveiled on the ransomware website, the exact amount of data stolen was not specified.

https://www.insurancebusinessmag.com/ca/news/cyber/maple-leaf-foods-confirms-cyberattack-will-not-pay-ransomware-gang-429218.aspx

Click above link to read more.

Back to top

Hackers leak another set of Medibank customer data on the dark web

Medibank on Thursday confirmed that the threat actors behind the devastating cyber attack have posted another dump of data stolen from its systems on the dark web after its refusal to pay a ransom.

"We are in the process of analyzing the data, but the data released appears to be the data we believed the criminal stole," the Australian health insurer said.

https://thehackernews.com/2022/12/hackers-leak-another-set-of-medibank.html

Click above link to read more.

Back to top

Hyundai app bugs allowed hackers to remotely unlock, start cars

Vulnerabilities in mobile apps exposed Hyundai and Genesis car models after 2012 to remote attacks that allowed unlocking and even starting the vehicles.

Security researchers at Yuga Labs found the issues and explored similar attack surfaces in the SiriusXM "smart vehicle" platform used in cars from other makers (Toyota, Honda, FCA, Nissan, Acura, and Infinity) that allowed them to "remotely unlock, start, locate, flash, and honk" them.

https://www.bleepingcomputer.com/news/security/hyundai-app-bugs-allowed-hackers-to-remotely-unlock-start-cars/

Click above link to read more.

Back to top

Australia will now fine firms up to AU$50 million for data breaches

The Australian parliament has approved a bill to amend the country's privacy legislation, significantly increasing the maximum penalties to AU$50 million for companies and data controllers who suffered large-scale data breaches.

The financial penalty introduced by the new bill is set to whichever is greater:

- AU$50 million,
- Three times the value of any benefit obtained through the misuse of information,
- 30% of a company's adjusted turnover in the relevant period.

https://www.bleepingcomputer.com/news/security/australia-will-now-fine-firms-up-to-au50-million-for-data-breaches/

Click above link to read more.

Back to top

LastPass breach fallout spreads to expose customer data

The aftermath from an August breach at LastPass has spread, compromising customer data, the password manager said in a Wednesday notice.

“We recently detected unusual activity within a third-party cloud storage service,” CEO Karim Toubba said in a blog post. “We have determined that an unauthorized party, using information obtained in the August 2022 incident, was able to gain access to certain elements of our customers’ information.”

https://www.cybersecuritydive.com/news/lastpass-breached-customers-data/637749/

Click above link to read more.

Back to top

Encryption provider for Sony leaks data for over a year

A server at encryption services company ENC Security, which serves more than 12 million customers including Sony and Lexar, has been leaking data since 2021.

An investigation by technology news site Cyber News into the Netherlands-based security provider has revealed a flaw in its software which has caused it to leak configuration and certificate files from May 27, 2021 to November 9, 2022.

https://www.cshub.com/data/news/encryption-provider-for-sony-leaks-data-for-over-a-year

Click above link to read more.

Back to top

FBI, CISA say Cuba ransomware gang extorted $60M from victims this year

The Cuba ransomware gang extorted more than $60 million in ransom payments from victims between December 2021 and August 2022, a joint advisory from CISA and the FBI has warned.

The latest advisory is a follow-up to a flash alert released by the FBI in December 2021, which revealed that the gang had earned close to $44 million in ransom payments after attacks on more than 49 entities in five critical infrastructure sectors in the United States. Since, the Cuba ransomware gang has brought in an additional $60 million from attacks against 100 organizations globally, almost half of the $145 million it demanded in ransom payments from these victims.

https://techcrunch.com/2022/12/02/fbi-cisa-cuba-ransomware/

Click above link to read more.

Back to top

Vatican shuts down its website amid hacking attempts

The Vatican was forced to take down its main vatican.va website on Wednesday and soon admitted it had detected apparent attempts to hack it.

“Technical investigations are ongoing due to abnormal attempts to access the site,” Vatican spokesman Matteo Bruni told Reuters on November 30, without elaboration.

https://cybernews.com/news/vatican-shuts-down-its-website-amid-hacking-attempts/

Click above link to read more.

Back to top

Google rolls out new Chrome browser update to patch yet another zero-day vulnerability

Search giant Google on Friday released an out-of-band security update to fix a new actively exploited zero-day flaw in its Chrome web browser.

The high-severity flaw, tracked as CVE-2022-4262, concerns a type confusion bug in the V8 JavaScript engine. Clement Lecigne of Google's Threat Analysis Group (TAG) has been credited with reporting the issue on November 29, 2022.

https://thehackernews.com/2022/12/google-rolls-out-new-chrome-browser.html

Click above link to read more.

Back to top

Hackers linked to Chinese government stole millions in Covid benefits, Secret Service says

Hackers linked to the Chinese government stole at least $20 million in U.S. Covid relief benefits, including Small Business Administration loans and unemployment insurance funds in over a dozen states, according to the Secret Service.

The theft of taxpayer funds by the Chengdu-based hacking group known as APT41 is the first instance of pandemic fraud tied to foreign, state-sponsored cybercriminals that the U.S. government has acknowledged publicly, but may just be the tip of the iceberg, according to U.S. law enforcement officials and cybersecurity experts.

https://www.nbcnews.com/tech/security/chinese-hackers-covid-fraud-millions-rcna59636

Click above link to read more.

Back to top

BlackProxies – A criminal proxy services selling a million access to hackers

DomainTools analysts have recently spotted a new residential proxy market which is dubbed “BlackProxies” that is aggressively gaining huge popularity among the following entities:

- Hackers
- Cybercriminals
- Phishers
- Scalpers
- Scammers

During the investigation of the market in question, it was discovered that the market is providing and selling access to more than one million purported proxy IP addresses across the world.

https://cybersecuritynews.com/blackproxies/

Click above link to read more.

Back to top

The top ten hacks and cyber security threats of 2022

Cyber crime is an ever-evolving problem, with an estimated cost of US$10trn by 2025. In 2021, there were more than 4,100 publicly disclosed data breaches, which equates to approximately 22 billion records being exposed. The figures for 2022 are expected to at least match this, if not exceed it by as much as five percent.

Cyber Security Hub is dedicated to delivering breaking news from the cyber security sector. With this in mind, here are the news stories detailing the threat vectors, cyber attacks and data breaches that had the biggest impact on its readers over the past 12 months.

https://www.cshub.com/attacks/news/the-top-10-hacks-and-cyber-security-threats-of-2022

Click above link to read more.

Back to top

BeCyberAware.eu - launches the largest EU funded cyber security awareness campaign related to digital commerce

BeCyberAware.eu is helping to level up the awareness of common scams to help safe guard the EU's digital commerce revolution and ensure people are safe to trade and use online services.

The Largest EU Funded Cyber Security Awareness BeCyberAware.eu is an EU funded awareness and training campaign designed to help educate people who live in the EU on cyber security, safety online and resilience to common scams.

https://www.einnews.com/pr_news/567463778/becyberaware-eu-launches-the-largest-eu-funded-cyber-security-awareness-campaign-related-to-digital-commerce

Click above link to read more.

Back to top

Rackspace confirms outage was caused by ransomware attack

Texas-based cloud computing provider Rackspace has confirmed today that a ransomware attack is behind an ongoing Hosted Exchange outage described as an "isolated disruption."

"As you know, on Friday, December 2nd, 2022, we became aware of suspicious activity and immediately took proactive measures to isolate the Hosted Exchange environment to contain the incident," the company said in an update to the initial incident report.

https://www.bleepingcomputer.com/news/security/rackspace-confirms-outage-was-caused-by-ransomware-attack/
Click above link to read more.

Back to top

Click unsubscribe to stop receiving the Digest.

****

For previous issues of Security News Digest, visit the current month archive page at:

http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/security-news-digest

To learn more about information security issues and best practices, visit us at:

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

OCIOSecurity@gov.bc.ca