Security News Digest
Information Security Branch

OCIO Office of the Chief Information Officer

November 30, 2021

Challenge yourself with our Online Shopping quiz!

This week's stories:

- How to stay safe during the pandemic spike in cyberattacks
- New standard brings clarity on cyber security SMEs
- Bureau Veritas is latest target of attack
- Maritime giant Swire Pacific Offshore suffers data breach following cyber-attack
- Eavesdropping bugs in MediaTek chips affect 37% of all smartphones and IoT globally
- Apple sues NSO group for hacking Apple users using state-sponsored software
- Attackers actively target Windows Installer zero-day
- Cybersecurity ETFs to consider amidst increasing threat from internet crimes
- Disruptive impact of emerging technologies on cyber security
- What Avengers movies can teach us about cybersecurity
- CyberCube warns underwriters after GoDaddy attack
- IKEA email systems hit by ongoing cyberattack
- Phishing Remains the Most Common Cause of Data Breaches, Survey Says
- Panasonic confirms data breach after hackers access internal network

---

How to stay safe during the pandemic spike in cyberattacks

The hospital in Kemptville. The transit network in Gatineau. The municipal government in Clarence-Rockland.

Those are just a few of the Ottawa-area organizations victimized in recent weeks by cybercriminals, emboldened as the COVID-19 pandemic forces people to work from home and more and more business gets conducted online.

https://www.cbc.ca/news/canada/ottawa/covid-19-cyberattacks-ottawa-five-big-questions-1.6256205

Click above link to read more.

Back to top

New standard brings clarity on cyber security SMEs

With 2021 expected to be the worst year on record for cyberattacks, the CIO Strategy Council has published a new standard that will help smaller businesses protect their systems from intruders.

The new standard, supported by the Standards Council of Canada (SCC), will form part of the requirements for CyberSecure Canada, a voluntary certification program established by Innovation, Science and Economic Development (ISED) and the Communications Security Establishment (CSE) to help SMEs achieve a reasonable level of cybersecurity.

https://www.globenewswire.com/news-release/2021/11/24/2340693/0/en/New-standard-brings-clarity-on-cybersecurity-to-SMEs.html

Click above link to read more.

Back to top

Bureau Veritas is latest target of attack

Bureau Veritas, the classification and inspection services company has become the latest global company to detect a cyber attack on its systems. The company, which has sought to become a thought leader in cybersecurity, reported that last weekend its security systems detected the attack and that the company immediately took precautionary measures.

“In response, all the group's cybersecurity procedures were immediately activated,” BV said in a prepared statement. “A preventive decision has been made to temporarily take our servers and data offline to protect our clients and the company while further investigations and corrective measures are in progress.”

https://www.maritime-executive.com/article/bureau-veritas-is-latest-target-of-cyber-attack

Click above link to read more.

Back to top

Maritime giant Swire Pacific Offshore suffers data breach following cyber-attack

Shipping giant Swire Pacific Offshore (SPO) has announced a data breach after it fell victim to a cyber-attack.

The maritime organization, which is headquartered in Singapore, said in a press release that it had suffered “unauthorized access to its IT systems”.

https://portswigger.net/daily-swig/maritime-giant-swire-pacific-offshore-suffers-data-breach-following-cyber-attack

Click above link to read more.

Back to top

Eavesdropping bugs in MediaTek chips affect 37% of all smartphones and IoT globally

Multiple security weaknesses have been disclosed in MediaTek system-on-chips (SoCs) that could have enabled a threat actor to elevate privileges and execute arbitrary code in the firmware of the audio processor, effectively allowing the attackers to carry out a "massive eavesdrop campaign" without the users' knowledge.

The discovery of the flaws is the result of reverse-engineering the Taiwanese company's audio digital signal processor (DSP) unit by Israeli cybersecurity firm Check Point Research, ultimately finding that by stringing them together with other flaws present in a smartphone manufacturer's libraries, the issues uncovered in the chip could lead to local privilege escalation from an Android application.

https://thehackernews.com/2021/11/eavesdropping-bugs-in-mediatek-chips.html

Click above link to read more.

Back to top

Apple sues NSO group for hacking Apple users using state-sponsored spyware

Apple sued NSO Group for exploiting Pegasus to hack devices and spy on innocent victims. Apple has registered a lawsuit against the Israeli manufacturer of commercial spyware NSO Group.

The NSO Group was sued earlier by Facebook for creating and using an exploit for a zero-day vulnerability in WhatsApp in May of that year. And now it has been sued by Apple, well it is the second major technology company to sue the NSO Group in the United States.

https://cybersecuritynews.com/apple-sues-nso-group-for-hacking-apple-users/

Click above link to read more.

Back to top

Attackers actively target Windows Installer zero-day

Attackers are actively exploiting a Windows Installer zero-day vulnerability that was discovered when a patch Microsoft issued for another security hole inadequately fixed the original and unrelated problem.

Over the weekend, security researcher Abdelhamid Naceri discovered a Windows Installer elevation-of-privilege vulnerability tracked as CVE-2021-41379 that Microsoft patched a couple of weeks ago as part of its November Patch Tuesday updates.

https://threatpost.com/attackers-target-windows-installer-bug/176558/

Click above link to read more.

Back to top

Cybersecurity ETFs to consider amidst increasing threat from internet crimes

Investing in the stocks of a specific industry or a particular theme may be highly rewarding, but can be an equally risky proposition. The volatility in such stocks may be high in the short to medium term as they are more prone to the news flow impacting their fortunes. One is related to cyber security and those looking to invest in the stocks of companies in the sector may consider buying cybersecurity-related exchange-traded funds (ETFs). Cyber security ETFs are expected to thrive in the virus-hit economy worldwide.

According to the Internet Crime Complaint Center (IC3), a record number of complaints from the American public in 2020: 791,790 were received, with reported losses exceeding $4.1 billion. This represents a 69% increase in total complaints from 2019.

https://www.financialexpress.com/investing-abroad/featured-stories/cybersecurity-etfs-to-consider-amidst-increasing-threat-from-internet-crimes/2376573/

Click above link to read more.

Back to top

Disruptive impact of emerging technologies on cyber security

Banking and telecom industries are racing to adopt technologies to keep up with the influx of digital disruption caused by— artificial intelligence (AI), extended reality (XR), machine learning (ML) and the internet of things (IoT). However, growing legacy systems, trends in advancement and demand for multi-channel customer-centric solutions are posing their own set of cyber challenges.

The cyber security market is projected to reach a marker valuation of around $245 billion by 2023 globally, as highlighted in— Analytics Insight Report, March 17, 2019.

https://cio.economictimes.indiatimes.com/news/digital-security/disruptive-impact-of-emerging-technologies-on-cyber-security/87922311

Click above link to read more.

Back to top

What Avengers movies can teach us about cybersecurity

Marvel has been entertaining us for the last 20 years. We have seen gods, super-soldiers, magicians, and other irradiated heroes fight baddies at galactic scales. The eternal fight of good versus evil. A little bit like in cybersecurity, goods guys fighting cybercriminals.

If we choose to go with this fun analogy, is there anything useful we can learn from those movies?

https://thehackernews.com/2021/11/what-avengers-movies-can-teach-us-about.html

Click above link to read more.

Back to top

CyberCube warns underwriters after GoDaddy attack

New research has highlighted how a Single Point of Failure (SPoF) cyber attack represents one of the most likely ways the world could experience its first systemic cyber event, according to analytics company, CyberCube.

The GoDaddy breach is the latest in a series of cyber attacks on SPoFs including the SolarWinds attack of 2020 and, more recently, an attack on Microsoft Exchange servers.

https://www.reinsurancene.ws/cybercube-warns-underwriters-after-godaddy-attack/

Click above link to read more.

Back to top

IKEA email systems hit by ongoing cyberattack

IKEA is battling an ongoing cyberattack where threat actors are targeting employees in internal phishing attacks using stolen reply-chain emails.

A reply-chain email attack is when threat actors steal legitimate corporate email and then reply to them with links to malicious documents that install malware on recipients' devices.

https://www.bleepingcomputer.com/news/security/ikea-email-systems-hit-by-ongoing-cyberattack/

Click above link to read more.

Back to top

Phishing Remains the Most Common Cause of Data Breaches, Survey Says

Phishing, malware, and denial-of-service attacks remained the most common causes for data breaches in 2021. Data from Dark Reading's latest Strategic Security Survey shows that more companies experienced a data breach over the past year because of phishing than any other cause. The percentage of organizations reporting a phishing-related breach is slightly higher in the 2021 survey (53%) than in the 2020 survey (51%). The survey found that malware was the second biggest cause of data breaches over the past year, as 41% of the respondents said they experienced a data breach where malware was the primary vector.

Even though there have been a number of high-profile ransomware attacks over the past year, the number of organizations in the survey who experienced a breach as a result of ransomware is relatively low. Just 13% of organizations in the survey reported a ransomware-related breach in the past 12 months, compared to 17% in the 2020 survey.

https://www.darkreading.com/edge-threat-monitor/phishing-remains-the-most-common-cause-of-data-breaches-survey-says

Click above link to read more.

Back to top

Panasonic confirms data breach after hackers access internal network

Japanese tech giant Panasonic has confirmed a data breach after hackers gained access to its internal network.

Panasonic said in a press release dated November 26 that its network was “illegally accessed by a third party” on November 11 and that “some data on a file server had been accessed during the intrusion.” However, when reached, Panasonic spokesperson Dannea DeLisser confirmed that the breach began on June 22 and ended on November 3 — and that the unauthorized access was first detected on November 11.

https://techcrunch.com/2021/11/29/panasonic-data-breach/

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

Security News Digest
Information Security Branch
BRITISH COLUMBIA OCIO Office of the Chief Information Officer