November 29, 2022

Challenge yourself with our Online Shopping Security Quiz

This past week's stories:

- **Canada to boost defence, cyber security in Indo-Pacific policy, focus on 'disruptive' China**
- **Durham school board systems down after 'cyber-incident'**
- **SLGA investigation states cybersecurity attack compromised 40,000 people**
- **Ontario secondary school teachers' union notifies victims of ransomware attack**
- **Microsoft says attackers are hacking energy grids by exploiting decades-old software**
- **European Parliament website affected by hacking attack**
- **U.K. Police Arrest 142 in global crackdown on 'iSpoof' phone spoofing service**
- **New ransomware attacks in Ukraine linked to Russian Sandworm hackers**
- **The new iPhone 14 and iOS upgrade include some big cybersecurity changes**
- **Black Basta ransomware gang actively infiltrating U.S. companies with Qakbot malware**
- **Whatsapp data of over 500 million users phone numbers around the globe up for sale**
- **5.4 million Twitter users' stolen data leaked online — more shared privately**
- **Holiday DDoS cyberattacks can hurt e-commerce, lack legal remedy**

Canada to boost defence, cyber security in Indo-Pacific policy, focus on 'disruptive' China

Canada launched its long-awaited Indo-Pacific strategy on Sunday, outlining spending of C$2.3 billion ($1.7 billion) to boost military and cyber security in the region and vowed to deal with a "disruptive" China while working with it on climate change and trade.

The plan, detailed in a 26-page document, said Canada would tighten foreign investment rules to protect intellectual property and prevent Chinese state-owned enterprises from snapping up critical mineral supplies.

https://www.reuters.com/world/americas/canada-launches-new-indo-pacific-strategy-focus-disruptive-china-2022-11-27/

Click above link to read more.

Back to top

Durham school board systems down after 'cyber-incident'

Schools in Durham Region were subjected to a cyber security incident, discovered on Friday, the local school board says.

The Durham District School Board said it was made aware of a "cyber-incident" on Friday. As a result, school phones and email services are not working, while staff may not have access to emergency contact information.

https://globalnews.ca/news/9308341/durham-school-board-systems-down-after-cyber-incident/

Click above link to read more.

Back to top

SLGA investigation states cybersecurity attack compromised 40,000 people

The Saskatchewan Information and Privacy Commissioner released an investigation report into the SLGA Nov. 10, detailing a cyberattack that happened late last year.

According to the report, the personal information of roughly 40,000 individuals was compromised during a privacy breach of the Saskatchewan Liquor and Gaming Authority (SLGA) in December 2021.

https://globalnews.ca/news/9302790/slga-cyberattack-investigation-report-recommendations/

Click above link to read more.

Back to top

Ontario secondary school teachers' union notifies victims of ransomware attack

Some Ontario current and retired public high school teachers and related staff are being notified that their personal information was copied by a hacker as part of a ransomware attack on their union's IT systems last spring.

The Ontario Secondary School Teachers Federation (OSSTF) said Wednesday it realized on May 30th that an unauthorized third party had accessed and encrypted some of the union's systems. The systems were compromised around five days earlier.

https://www.itworldcanada.com/article/ontario-secondary-school-teachers-union-notifies-victims-of-ransomware-attack/514978

Click above link to read more.

Back to top

Microsoft says attackers are hacking energy grids by exploiting decades-old software

Microsoft has warned that malicious hackers are exploiting a discontinued web server found in common Internet of Things (IoT) devices to target organizations in the energy sector.

In an analysis published on Tuesday, Microsoft researchers said they had discovered a vulnerable open-source component in the Boa web server, which is still widely used in a range of routers and security cameras, as well as popular software development kits (SDKs), despite the software's retirement in 2005. The technology giant identified the component while investigating a suspected Indian electric grid intrusion first detailed by Recorded Future in April, where Chinese state-sponsored attackers used IoT devices to gain a foothold on operational technology (OT) networks, used to monitor and control physical industrial systems.

https://techcrunch.com/2022/11/23/microsoft-boa-server-energy-grids/

Click above link to read more.

Back to top

European Parliament website affected by hacking attack

The European Parliament website was affected because of a hacking attack Wednesday, officials said.

European Parliament spokesman Jaume Duch said the website “is currently impacted from outside due to high levels of external network traffic.” He added that “this traffic is related to a DDOS attack (Distributed Denial of Service) event.”

https://www.theglobeandmail.com/world/article-european-parliament-website-affected-by-hacking-attack-2/

Click above link to read more.

Back to top

U.K. Police Arrest 142 in global crackdown on 'iSpoof' phone spoofing service

A coordinated law enforcement effort has dismantled an online phone number spoofing service called iSpoof and arrested 142 individuals linked to the operation.

The websites, ispoof[.]me and ispoof[.]cc, allowed the crooks to "impersonate trusted corporations or contacts to access sensitive information from victims," Europol said in a press statement.

https://thehackernews.com/2022/11/uk-police-arrest-142-in-global.html

Click above link to read more.

Back to top

New ransomware attacks in Ukraine linked to Russian Sandworm hackers

New ransomware attacks targeting organizations in Ukraine first detected this Monday have been linked to the notorious Russian military threat group Sandworm.

Slovak software company ESET who first spotted this wave of attacks, says the ransomware they named RansomBoggs has been found on the networks of multiple Ukrainian organizations.

https://www.bleepingcomputer.com/news/security/new-ransomware-attacks-in-ukraine-linked-to-russian-sandworm-hackers/

Click above link to read more.

Back to top

The new iPhone 14 and iOS upgrade include some big cybersecurity changes

It’s Black Friday and the official start of the holiday shopping season, and there’s a new iPhone 14 for consumers in the market looking to upgrade their Apple device. From better cameras and longer battery life to faster chips, there are plenty of features consumers will consider when buying a new iPhone — that is, if you can find one amid what’s looking like a season short on supply of some of Cupertino’s newest models.

One new safety feature that has been getting a lot of attention is emergency satellite connectivity. Cybersecurity may not be among the top selling points, but the new iPhone and iOS16 do have some significant security upgrades, too.

https://www.cnbc.com/2022/11/25/buying-new-iphone-here-are-new-features-designed-for-your-security.html

Click above link to read more.

Back to top

Black Basta ransomware gang actively infiltrating U.S. companies with Qakbot malware

Companies based in the U.S. have been at the receiving end of an "aggressive" Qakbot malware campaign that leads to Black Basta ransomware infections on compromised networks.

"In this latest campaign, the Black Basta ransomware gang is using QakBot malware to create an initial point of entry and move laterally within an organization's network," Cybereason researchers Joakim Kandefelt and Danielle Frankel said in a report shared with The Hacker News.

https://thehackernews.com/2022/11/black-basta-ransomware-gang-actively.html

Click above link to read more.

Back to top

WhatsApp data of over 500 million users phone numbers around the globe up for sale

In a recent data security breach, a threat actor posted over 500 million active WhatsApp users’ phone numbers for sale on a well-known hacker platform. The database reportedly includes information from WhatsApp users in 84 different countries.

The Cybernews report says the database holds phone numbers of more than 32 million US user records, 45 million from Egypt, 5 million from Italy, 29 million from Saudi Arabia, 20 million (each) from France and Turkey, 10 million phone numbers from Russian users, and over 11 million numbers are from the UK.

https://cybersecuritynews.com/whatsapp-users/

Click above link to read more.

Back to top

5.4 million Twitter users' stolen data leaked online — more shared privately

Over 5.4 million Twitter user records containing non-public information stolen using an API vulnerability fixed in January have been shared for free on a hacker forum.

Another massive, potentially more significant, data dump of millions of Twitter records has also been disclosed by a security researcher, demonstrating how widely abused this bug was by threat actors.

https://www.bleepingcomputer.com/news/security/54-million-twitter-users-stolen-data-leaked-online-more-shared-privately/

Click above link to read more.

Back to top

Holiday DDoS cyberattacks can hurt e-commerce, lack legal remedy

Cyberattacks that knock internet platforms offline temporarily—a particular concern on Cyber Monday—are likely to spike this holiday season, but victims have few legal avenues to seek recovery, attorneys and industry professionals say.

Ransomware attacks that take control of victims' systems garner more media attention, but distributed denial-of-service attacks are one of the most common cybersecurity incidents to disrupt a company's business operations.

https://news.bloomberglaw.com/privacy-and-data-security/holiday-ddos-cyberattacks-can-hurt-e-commerce-lack-legal-remedy

Click above link to read more.

Back to top

The Security News Digest (SND) is a collection of articles published by others that have been compiled by the Information Security Branch (ISB) from various sources. The intention of the SND is simply to make its recipients aware of recent articles pertaining to information security in order to increase their knowledge of information security issues. The views and opinions displayed in these articles are strictly those of the articles' writers and editors and are not intended to reflect the views or opinions of the ISB. Readers are expected to conduct their own assessment on the validity and objectivity of each article and to apply their own judgment when using or referring to this information. The ISB is not responsible for the manner in which the information presented is used or interpreted by its recipients.

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