February 21, 2023

There has been an increase in fraudulent activity regarding the BC Services Card App. Please ensure that you only download BC Government documents and BC Services Card App from official sources (gov.bc.ca). The BC Services Card app is free and available for Android™ and iOS (iPhone® and iPad®).

Challenge yourself with our Raise Your Cyber Security Game Quiz!

This past week's stories:

- **Indigo website still offline nearly 1 week after cybersecurity incident**
- **Russian-linked malware was close to putting U.S. electric, gas facilities 'offline' last year**
- **RedEyes Hacking Group Uses Steganography Technique to Deploy Malware on PC & Mobile Phones**
- **Killnet claims cyberattack on Lufthansa was retaliation for Germany's support in Ukraine**
- **India-linked group used Telegram to mastermind cyberattacks across Asia, says analyst**
- **Experts Warn of 'Beep' - A New Evasive Malware That Can Fly Under the Radar**
- **UK surveillance watchdog issues warning over Chinese cameras**
- **Dark side of ChatGPT: it's aiding cybercrime**
- **Hackers using Google Ads to spread FatalRAT malware disguised as popular apps**
- **Student loan breach exposes 2.5 million records**
- **Royal Mail resumes overseas mail at post offices after cyber-attack**
- **Oakland Declares State of Emergency Due to Ransomware Attack**

Indigo website still offline nearly 1 week after cybersecurity incident

Almost a week after being hit with an apparent cyberattack, book retailer Indigo's website is still offline, leaving customers with more questions than answers.

The TSX-listed bookseller's website went dark on Wednesday, Feb. 8. Indigo's brick-and-mortar stores could not process any transactions that were not in cash, leaving anyone who wanted to return or buy an item using debit, credit or gift cards in the lurch.

https://www.cbc.ca/news/business/indigo-cyberattack-update-1.6747714

Click above link to read more.

Back to top

Russian-linked malware was close to putting U.S. electric, gas facilities 'offline' last year

Hackers linked to Russia got very close to being able to take a dozen U.S. electric and gas facilities offline in the first weeks of the war in Ukraine, the head of a top cybersecurity company warned Tuesday.

Robert M. Lee, the founder and CEO of Dragos, which helps companies respond to cyberattacks, said hackers with a group Dragos calls "Chernovite" were using a malicious software to try to take down "around a dozen" U.S. electric and liquid natural gas sites.

https://www.politico.com/news/2023/02/14/russia-malware-electric-gas-facilities-00082675

Click above link to read more.

Back to top

RedEyes Hacking Group Uses Steganography Technique to Deploy Malware on PC & Mobile Phones

RedEyes Hacking Group (aka APT37), a threat group known for its cyber espionage activities, has recently adopted a new tactic in its efforts to collect intelligence from targeted individuals.

This group is now using a sophisticated malware called "M2RAT," which is specifically designed to evade detection by security software.

In addition to using M2RAT, APT37 is also utilizing steganography, a technique that hides information within seemingly innocuous files or images, to further conceal their activities.

https://cybersecuritynews.com/redeyes-hacking-group/

Click above link to read more.

Back to top

Killnet claims cyberattack on Lufthansa was retaliation for Germany's support in Ukraine

Pro-Russian hacker group Killnet claimed responsibility for the IT failure of German carrier Lufthansa, adding that following a "rat experiment," it now knows how to stop navigation of any airport in the world.

Germany's flagship carrier Lufthansa experienced a severe IT fault on Wednesday, leaving thousands of passengers stranded. The company initially attributed the incident to the damage caused to several of Deutsche Telekom's glass-fiber cables during construction work in Frankfurt.

https://cybernews.com/news/killnet-claims-cyberattack-on-lufthansa-was-retaliation-for-germanys-support-in-ukraine/

Click above link to read more.

Back to top

India-linked group used Telegram to mastermind cyberattacks across Asia, says analyst

Previously undisclosed phishing operations attributed to a threat group believed to have links to Indian nationalists have been revealed by cyber analyst Group-IB. It says the attacks targeted government, military, and legal institutions across Asia.

The cybersecurity watchdog said it tracked SideWinder – also known as Hardcore Nationalist (HN2) – going after more than 60 organizations in Afghanistan, Bhutan, Myanmar, Nepal, and Sri Lanka in 2021.

https://cybernews.com/security/india-telegram-cyberattacks-asia/

Click above link to read more.

Back to top

Experts Warn of 'Beep' - A New Evasive Malware That Can Fly Under the Radar

Cybersecurity researchers have unearthed a new piece of evasive malware dubbed Beep that's designed to fly under the radar and drop additional payloads onto a compromised host.

"It seemed as if the authors of this malware were trying to implement as many anti-debugging and anti-VM (anti-sandbox) techniques as they could find," Minerva Labs researcher Natalie Zargarov said.

https://thehackernews.com/2023/02/experts-warn-of-beep-new-evasive.html

Click above link to read more.

Back to top

UK surveillance watchdog issues warning over Chinese cameras

Fraser Sampson, Biometrics and Surveillance Camera Commissioner, said in his annual report that most police forces in England and Wales still use camera equipment that is either made in China or contains Chinese components.

This is leaving the police open to spying by Beijing, Sampson warned. Moreover, the use of such equipment poses ethical concerns since some of the Chinese-made cameras are helping the Chinese government monitor notorious detainment camps for Uyghurs in Xinjiang province.

https://cybernews.com/news/uk-watchdog-warning-chinese-cameras/

Click above link to read more.

Back to top

Dark side of ChatGPT: it’s aiding cybercrime

The same technology promising to transform our lives is also making it easier for scammers to create everything from voice clones and deepfakes to convincing phishing emails. But will the arrival of ChatGPT make it even easier for cybercriminals?

https://cybernews.com/security/dark-side-of-chatgtp/

Click above link to read more.

Back to top

Hackers using Google Ads to spread FatalRAT malware disguised as popular apps

Chinese-speaking individuals in Southeast and East Asia are the targets of a new rogue Google Ads campaign that delivers remote access trojans such as FatalRAT to compromised machines.

https://thehackernews.com/2023/02/hackers-using-google-ads-to-spread.html?&web_view=true

Click above link to read more.

Back to top

Student loan breach exposes 2.5 million records

EdFinancial and the Oklahoma Student Loan Authority (OSLA) are notifying over 2.5 million loanees that their personal data was exposed in a data breach.

https://threatpost.com/student-loan-breach-exposes-2-5m-records/180492/

Click above link to read more.

Back to top

Royal Mail resumes overseas mail at post offices after cyber-attack

International mail services have finally been reinstated at UK post offices, more than a month after Royal Mail was hit by a cyber attack.

The breach on 10 January caused a backlog that led to long delays for consumers and businesses.

https://www.bbc.com/news/business-64718824

Click above link to read more.

Back to top

Oakland Declares State of Emergency Due to Ransomware Attack

Oakland Interim City Administrator G Harold Duffey on Tuesday issued a local state of emergency due to "ongoing impacts" of network outages caused by ransomware, the city announced on Twitter.

The declaration of the emergency will allow the city to expedite its attack on the malicious software.

https://www.nbcbayarea.com/news/local/east-bay/oakland-state-of-emergency-ransomware-attack/3158122/

Click above link to read more.

Back to top

Click unsubscribe to stop receiving the Digest.

****

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