September 13, 2022

Challenge yourself with our Ransomware Quiz!

This past week's stories:

- **North Vancouver RCMP warn of rash of 'brazen' scams targeting seniors**
- **Charlottetown Police warn about scam text urging Islanders to pay fines from city**
- **Holiday Inn hotels hit by cyber-attack**
- **Albania is the first known country to sever diplomatic ties over a cyberattack**
- **Dutch cyber security organisations to join forces**
- **Researchers warn older D-Link routers are under threat from Mirai malware variant**
- **Huge Los Angeles Unified School district hit by cyberattack**
- **Healthcare fintechs targeted by cybercriminals**
- **North Korean Lazarus hackers targeting energy providers around the world**
- **New vulnerabilities reported in Baxter's internet-connected infusion pumps**
- **Ukraine dismantles more bot farms spreading Russian disinformation**
- **Montenegro wrestles with massive cyberattack, Russia blamed**

North Vancouver RCMP warn of rash of 'brazen' scams targeting seniors

Mounties in North Vancouver are warning about recent rash of increasingly 'brazen' scams targeting seniors.

In a two-day period, the detachment received six reports of so-call grandparent scams, a spokesperson told CTV news in an email. The ruse involves contacting a senior pretending to be the police, saying a grandchild has been arrested and demanding money for bail.

https://bc.ctvnews.ca/north-vancouver-rcmp-warn-of-rash-of-brazen-scams-targeting-seniors-1.6064416

Click above link to read more.

Back to top

Charlottetown Police warn about scam text urging Islanders to pay fines from city

Several Islanders say they've been receiving scam texts asking them to pay fines linked to a website impersonating the City of Charlottetown.

Beth Claron lives in Charlottetown and got the text while studying on Saturday. She didn't click the link, but when she loaded up the site on her computer, she had second thoughts.

https://www.cbc.ca/news/canada/prince-edward-island/pei-rext-scam-spet-2022-1.6579388

Click above link to read more.

Back to top

Holiday Inn hotels hit by cyber-attack

Holiday Inn owner, Intercontinental Hotels Group (IHG), has confirmed the company has been hit by a cyber-attack.

IHG, which has some of the world's largest hotel chains, issued a statement saying it was investigating "unauthorised access" to a number of its technology systems.

https://www.bbc.com/news/technology-62814943

Click above link to read more.

Back to top

Albania is the first known country to sever diplomatic ties over a cyberattack

NATO member Albania cut off diplomatic relations with Iran on Wednesday over a cyberattack that destroyed government data and shut down services.

It’s the first known time a nation has taken such an aggressive step in response to a cyberattack, and it generated support from several other nations, including the United States.

https://www.washingtonpost.com/politics/2022/09/08/albania-is-first-known-country-sever-diplomatic-ties-over-cyberattack/

Click above link to read more.

Back to top

Dutch cyber security organisations to join forces

The Netherlands' National Cyber Security Centre (NCSC), Digital Trust Centre (DTC) and Cyber Security Incident Response Team for Digital Service Providers (CSIRT-DSP) are to merge into a single central expertise centre and information hub.

Combining knowledge and information on cyber security, legal tasks and services in the event of major incidents increases the country's digital resilience.

https://www.computerweekly.com/news/252524711/Dutch-cyber-security-organisations-to-join-forces

Click above link to read more.

Back to top

Researchers warn older D-Link routers are under threat from Mirai malware variant

Threat actors are exploiting vulnerabilities in D-Link routers to spread a variant of Mirai malware called MooBot, which targets exposed networking devices running Linux, according to research released Tuesday from Palo Alto Networks' Unit 42.

Though the manufacturer has published security bulletins for the vulnerabilities, users may be running older or unpatched versions of D-Link devices, according to the report.

https://www.cybersecuritydive.com/news/d-link-routers-mirai-malware-palo-alto-research/631421/

Click above link to read more.

Back to top

Huge Los Angeles Unified School district hit by cyberattack

A ransomware attack targeting the huge Los Angeles school district prompted an unprecedented shutdown of its computer systems as schools increasingly find themselves vulnerable to cyber breaches at the start of a new year.

The attack on the Los Angeles Unified School District sounded alarms across the country, from urgent talks with the White House and the National Security Council after the first signs of ransomware were discovered late Saturday night to mandated password changes for 540,000 students and 70,000 district employees.

https://apnews.com/article/technology-los-angeles-us-department-of-education-007f5c48d88536b623c1803ec88a6f08

Click above link to read more.

Back to top

Healthcare fintechs targeted by cybercriminals

Companies that process payments for physician groups, hospitals and other healthcare providers are more vulnerable to hacks, information system breaches and ransom demands than their peers in other segments of the industry, cybersecurity professionals warn.

In a report last month, cybersecurity firm Critical Insight noted that two fintech firms were hit with ransomware attacks since July 1, exposing financial and healthcare data from almost three million patients.

https://www.cybersecuritydive.com/news/healthcare-payments-fintechs-cybersecurity-breaches-ransom/631440/

Click above link to read more.

Back to top

North Korean Lazarus hackers targeting energy providers around the world

A malicious campaign mounted by the North Korea-linked Lazarus Group targeted energy providers around the world, including those based in the United States, Canada, and Japan, between February and July 2022.

"The campaign is meant to infiltrate organizations around the world for establishing long-term access and subsequently exfiltrating data of interest to the adversary's nation-state," Cisco Talos said in a report shared with The Hacker News.

https://thehackernews.com/2022/09/north-korean-lazarus-hackers-targeting.html

Click above link to read more.

Back to top

New vulnerabilities reported in Baxter's internet-connected infusion pumps

Multiple security vulnerabilities have been disclosed in Baxter's internet-connected infusion pumps used by healthcare professionals in clinical environments to dispense medication to patients.

"Successful exploitation of these vulnerabilities could result in access to sensitive data and alteration of system configuration," the U.S. Cybersecurity and Infrastructure Security Agency (CISA) said in a coordinated advisory.

https://thehackernews.com/2022/09/new-vulnerabilities-reported-in-baxters.html

Click above link to read more.

Back to top

Ukraine dismantles more bot farms spreading Russian disinformation

The Cyber Department of the Ukrainian Security Service (SSU) dismantled two more bot farms that spread Russian disinformation on social networks and messaging platforms via thousands of fake accounts.

As the SSU discovered, this bot army "of almost 7,000 accounts" was used to push content discrediting the Defence Forces of Ukraine, justify Russia's armed aggression, and destabilize Ukraine's social and political situation.

https://www.bleepingcomputer.com/news/security/ukraine-dismantles-more-bot-farms-spreading-russian-disinformation/

Click above link to read more.

Back to top

Montenegro wrestles with massive cyberattack, Russia blamed

At the government headquarters in NATO-member Montenegro, the computers are unplugged, the internet is switched off and the state’s main websites are down. The blackout comes amid a massive cyberattack against the small Balkan state which officials say bears the hallmark of pro-Russian hackers and its security services.

The coordinated attack that started around Aug. 20 crippled online government information platforms and put Montenegro’s essential infrastructure, including banking, water and electricity power systems, at high risk.

https://www.nbcnews.com/tech/security/montenegro-wrestles-massive-cyberattack-russia-blamed-rcna47277

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