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

June 16th, 2020

Try our June - Connect with Care Quiz

This week's stories:

- **Restructuring of IT infrastructure to take 'several months' after ransomware attack, says eHealth Saskatchewan** 🇨🇦
- **Health sector: protect yourself from cyber threats**
- **Honda resumes production at plants hit by suspected cyber attack**
- **Obscure Indian cyber firm spied on politicians, investors worldwide**
- **Over 100,000 UK Security Cameras Could Be at Risk of Hacking**
- **Accessories giant Claire's hacked to steal credit card info**
- **Extortionists threaten to destroy sites in fake ransom attacks**
- **Expert says Huawei's cyber risks can't be mitigated in a 5G network**

Restructuring of IT infrastructure to take 'several months' after ransomware attack, says eHealth Saskatchewan

https://www.itworldcanada.com/article/restructuring-of-it-infrastructure-to-take-several-months-after-ransomware-attack-says-ehealth-saskatchewan/431942

Five months after a ransomware attack locked the computer systems storing confidential medical data of Saskatchewan residents, eHealth Saskatchewan says it's going to take a while to restructure its IT infrastructure, and that it's still unsure who stole the data or where it is.

The health agency's chief executive officer Jim Hornell confirmed in February that the virus first entered the eHealth system on December 20, 2019. Employees didn't discover there was a problem until they tried to open files on Jan. 6 and were asked to hand over bitcoin in exchange for the encrypted data.

Click link above to read more

Health sector: protect yourself from cyber threats

https://cyber.gc.ca/en/news/health-sector-protect-yourself-cyber-threats

The Cyber Centre recommends that health organizations working on the pandemic remain vigilant and ensure that they are engaged in cyber defence best practices, including increased monitoring of network logs, reminding employees to practice phishing awareness and ensuring that servers and critical systems are patched for all known security vulnerabilities.

Keep in mind that working from home presents more risk than working on an organization's network, especially when employees are using their own laptops, tablets and phones. Help your workers be aware of malicious messages and give them tips on how to protect themselves at home. One way to do that – and to take advantage of one of our services – is to use CIRA's Canadian Shield for your DNS provider. Following a few simple steps will ensure you aren't inadvertently sent to a website the Cyber Centre knows to be malicious.

Click link above to read more

Honda resumes production at plants hit by suspected cyber attack

https://www.thechronicleherald.ca/business/reuters/honda-resumes-production-at-plants-hit-by-suspected-cyber-attack-461283/

TOKYO (Reuters) - Japan's Honda Motor Co <7267.T> has resumed production at automobile and motorcycle plants in the United States and other countries after they were hit by a suspected cyber attack this week, a spokesman said on Friday.

The suspected attack comes less than a month after Honda reopened its North American vehicle assembly plants, following closure of factories in late March to comply with coronavirus-related, shelter-at-home rules in the United States and Canada.

The spokesman said the Japanese automaker had resumed vehicle output by Thursday at its main plant in the U.S. state of Ohio, which produces models such as the CR-V SUV crossover and the Accord sedan.

Click link above to read more

Obscure Indian cyber firm spied on politicians, investors worldwide

https://www.cbc.ca/news/technology/indian-cyber-firm-1.5604376

A little-known Indian information technology company offered its hacking services to help clients spy on more than 10,000 email accounts over a period of seven years.

New Delhi-based BellTroX InfoTech Services targeted government officials in Europe, gambling tycoons in the Bahamas, and well known investors in the United States, including private equity giant KKR and short seller Muddy Waters, according to three former employees, outside researchers, and a trail of online evidence.

Click link above to read more

Over 100,000 UK Security Cameras Could Be at Risk of Hacking

https://www.infosecurity-magazine.com/news/uk-security-cameras-risk-hacking/

More than 100,000 indoor security cameras across UK homes and businesses may have critical security flaws that make them vulnerable to hacking, an investigation by Which? has found. Owners of wireless cameras that use the CamHi app could be at risk of having their home or business spied upon by cyber-criminals, in addition to having data stolen or other devices targeted, according to the analysis.

Although many cameras have been removed from sale, many remain available from online marketplaces such as Amazon, eBay and Wish.com, and include popular brands like Accfly, ieGeek and SV3C. Over 12,000 were activated in UK homes in the last three months alone, and Which? believes there are around 3.5 million of these camera types in use around the world, mainly in Asia.

Click link above to read more

Accessories giant Claire's hacked to steal credit card info

https://www.bleepingcomputer.com/news/security/accessories-giant-claires-hacked-to-steal-credit-card-info/

The websites for U.S. based jewelry and accessory giant Claire's, and its subsidiary Icing, were compromised in April and may have allowed hackers to gain access to customer's credit cards.

Claire's is a very popular U.S. based jewelry and accessories store with over 2,000 locations in North America and Europe, and 6,794 concession locations and 546 franchised stores in other regions.

The Claire's stores are commonly found in shopping malls around the United States and are very popular among teenage girls and young women.

Click link above to read more

Extortionists threaten to destroy sites in fake ransom attacks

https://www.bleepingcomputer.com/news/security/extortionists-threaten-to-destroy-sites-in-fake-ransom-attacks/

Scammers are targeting website owners with blackmail messages asking them to pay ransoms between $1,500 and $3,000 in bitcoins to avoid having their sites' databases leaked and their reputation destroyed.

As the fraudsters falsely claim, they exfiltrate the databases to attacker-controlled servers using credentials harvested after exploiting a vulnerability found within the sites' software.

Click link above to read more

Expert says Huawei’s cyber risks can’t be mitigated in a 5G network

https://www.itworldcanada.com/article/expert-says-huaweis-cyber-risks-cant-be-mitigated-in-a-5g-network/432030

There’s no way to mitigate the possibility that network equipment from Huawei Technologies could be used by Chinese intelligence agencies for spying in Canada’s fledgling 5G networks, says a U.S. cyber expert.

“In my opinion, the risks cannot be mitigated,” Melissa Hathaway, president of a Virginia-based consultancy, a distinguished fellow at the Centre for International Governance Innovation based in Waterloo, Ont., and an advisor to two U.S. presidents said in an interview.

Click link above to read more

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

The information presented or referred to in SND is owned by third parties and protected by copyright law, as well as any terms of use associated with the sites on which the information is provided. The recipient is responsible for making itself aware of and abiding by all applicable laws, policies and agreements associated with this information.

We attempt to provide accurate Internet links to the information sources referenced. We are not responsible for broken or inaccurate Internet links to sites owned or operated by third parties, nor for the content, accuracy, performance or availability of any such third-party sites or any information contained on them.

Security News Digest
Information Security Branch

BRITISH COLUMBIA OCIO | Office of the Chief Information Officer