Security News Digest
Information Security Branch

BRITISH COLUMBIA OCIO Office of the Chief Information Officer

August 18th, 2020

Try our August - 'Summer social media' Quiz

This week's stories:

- Government denies successful cyber attack shows failure of systems
- Ontario's privacy consultation could lead to new private sector data protection laws, but not everyone is thrilled about it
- NSA and FBI warn that new Linux malware threatens national security
- Secret Service buys location data that would otherwise need a warrant
- Over 25% of all UK universities were attacked by ransomware
- U.S. spirits and wine giant hit by cyberattack, 1TB of data stolen
- Amazon Alexa flaws could have revealed home address and other personal data
- NIST releases Zero Trust Architecture

Government denies successful cyber attack shows failure of systems

https://www.itworldcanada.com/article/government-denies-successful-cyber-attack-shows-failure-of-systems/434641

The federal government's top IT officer says that last week's credentials stuffing hack of 11,000 tax and service accounts of Canadians does not mean its systems failed to protect people's information.

"I would argue, no," Marc Brouillard, acting chief information officer, told reporters during a press briefing this morning. "Quite the opposite. The system worked. We were able to identify these fraudulent actions coming in through some pretty sophisticated analytics that detected [suspicious] behaviours. From a systems perspective, this is a person trying to log into the system and our tools were able to detect those patterns that were suspicious and identify those that were not valid.

Click link above to read more

Ontario's privacy consultation could lead to new private sector data protection laws, but not everyone is thrilled about it

https://www.itworldcanada.com/article/will-ontarios-privacy-consultation-lead-to-a-private-sector-data-protection-law/434596

With its announcement last week about a public consultation to “improving provincial privacy laws,” Ontario is signalling it’s willing to pass its own private sector privacy law, joining Quebec, B.C. and Alberta.

Other than those three, the other provinces and territories accept the federal Personal Information Privacy and Electronic Documents Act (PIPEDA), which covers federally-registered businesses, as their law for overseeing data privacy in provincially-registered businesses. However, non-profits and charities aren’t covered, nor are Ontario provincial political parties.

Ontario’s existing privacy laws only cover the health, municipal and provincial public sectors (including universities and colleges).

Click link above to read more

NSA and FBI warn that new Linux malware threatens national security

https://arstechnica.com/information-technology/2020/08/nsa-and-fbi-warn-that-new-linux-malware-threatens-national-security/

The FBI and NSA have issued a joint report warning that Russian state hackers are using a previously unknown piece of Linux malware to stealthily infiltrate sensitive networks, steal confidential information, and execute malicious commands.

In a report that’s unusual for the depth of technical detail from a government agency, officials said the Drovorub malware is a full-featured tool kit that has gone undetected until recently. The malware connects to command and control servers operated by a hacking group that works for the GRU, Russia’s military intelligence agency that has been tied to more than a decade of brazen and advanced campaigns, many of which have inflicted serious damage to national security.

Click link above to read more

Secret Service buys location data that would otherwise need a warrant

https://arstechnica.com/tech-policy/2020/08/secret-service-other-agencies-buy-access-to-mobile-phone-location-data/

An increasing number of law enforcement agencies, including the US Secret Service, are simply buying their way into data that would ordinarily require a warrant, a new report has found, and at least one US senator wants to put a stop to it.

The Secret Service paid about $2 million in 2017-2018 to a firm called Babel Street to use its service Locate X, according to a document (PDF) Vice Motherboard obtained. The contract outlines what kind of content, training, and customer support Babel Street is required to provide to the Secret Service.

Click link above to read more

Over 25% of all UK universities were attacked by ransomware

https://www.bleepingcomputer.com/news/security/over-25-percent-of-all-uk-universities-were-attacked-by-ransomware/

A third of the universities in the United Kingdom responding to a freedom of information (FOI) request admitted to being a victim of a ransomware attack. These represent more than 25% of the universities and colleges in the country.

The incidents occurred in the past decade, most of them between 2015 and 2017. Several educational institutions suffered at least two file-encrypting attacks over the past decade, one of them recording more than 40 since 2013.

Click link above to read more

U.S. spirits and wine giant hit by cyberattack, 1TB of data stolen

https://www.bleepingcomputer.com/news/security/us-spirits-and-wine-giant-hit-by-cyberattack-1tb-of-data-stolen/

Brown-Forman, one of the largest U.S. companies in the spirits and wine business, suffered a cyber attack. The intruders allegedly copied 1TB of confidential data; they plan on selling to the highest bidder the most important info and leak the rest.

Headquartered in Louisville, Kentucky, the company holds world-known whiskey and scotch brands like Jack Daniel's, Woodford, Old Forester, Collingwood, Glenglassaugh, and Glendronach; Herradura, El Jimador, and Pepe Lopez tequila; Finlandia vodka, and Sonoma-Cutrer wines.

Click link above to read more

Amazon Alexa flaws could have revealed home address and other personal data

https://www.techrepublic.com/article/amazon-alexa-flaws-could-have-revealed-home-address-and-other-personal-data/?ftag=TREa988f1c&bhid=42420269&mid=12989596&cid=2176068089

Smart devices and their voice assistants have become a pervasive and popular way for us to find information, control our surroundings, communicate with others, and tap into a host of skills from business to entertainment. But as we share certain personal requests and details with our smart devices, concerns have arisen over the security and privacy of our data.

A report released Thursday by intelligence provider Check Point Research highlights recent security vulnerabilities found in Amazon Alexa, which could have given attackers access to the confidential information of users.

Click link above to read more

NIST releases Zero Trust Architecture

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

The U.S. National Institute of Standards and Technology's Computer Security Resource Center published its Zero Trust Architecture, which outlines a road map for cybersecurity measures across an organization. NIST explained the security concept was established to "move defenses from static, network-based perimeters to focus on users, assets, and resources." The architecture focuses on "enterprise network trends," including bring your own device, remote users and cloud-based assets.

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