Security News Digest

Information Security Branch

BRITISH COLUMBIA OCIO Office of the Chief Information Officer

May 7th, 2019

Try our May quiz - Security By The Numbers

This week's stories:

- **Public Safety Canada issues guide to lowering insider cyber risk** 🇨🇦
- **Canada distant on 5G security guidelines issued from international meeting** 🇨🇦
- **World Password Day: Time for CISOs to re-think login strategies**
- **Darknet Disruption: 'Wall Street Market' Closed for Business**
- **Drug Lab Cyberattack Puts Spotlight on IP Theft Threat**
- **Trump Order Aims to Boost Federal Cybersecurity Workforce**
- **Mystery Database Exposed Info on 80 Million US Households**
- **Israel Bombs Building as Retaliation for Hamas Cyber Attack**
- **Someone Is Hacking GitHub Repositories and Holding Code Ransom**
- **The Cybersecurity 202: A cyberattack just disrupted grid operations in the U.S. But it could have been far worse.**

Public Safety Canada issues guide to lowering insider cyber risk 🇨🇦

https://www.itworldcanada.com/article/public-safety-canada-issues-guide-to-lowering-insider-cyber-risk/417562

The odds are an organization will be attacked by an external threat actor, according to most studies. Over the years, Verizon's annual international data breach investigations report has shown on average two-thirds of data breaches come from nation-states, criminals or activists.

That means about one-third of breaches are blamed on insiders — defined as employees, contractors and partners — who have access to sensitive data.

Click link above to read more

Canada distant on 5G security guidelines issued from international meeting 🇨🇦

https://www.itworldcanada.com/article/canada-distant-on-5g-security-guidelines-issued-from-international-meeting/417716

The rule of law and the security environment in the country where telecommunications equipment is made are factors nations can consider when deciding whether to allow the purchase of 5G wireless network gear from a vendor, according to a summary of discussions at an international closed-door meeting.

It's one of 20 proposals issued Friday by the meeting chair as a summary after a two-day private meeting of government officials and experts from 32 countries — including Canada, the U.S., the European Union, Japan and Israel — at the Prague 5G Security Conference.

Click link above to read more

World Password Day: Time for CISOs to re-think login strategies

https://www.itworldcanada.com/article/world-password-day-time-for-cisos-to-re-think-login-strategies/417572

Today is World Password Day, which is usually aimed at encouraging consumers to strengthen or change their passwords.

However, CISOs can also take the day to re-think their identity and access management strategies focussing on several issues:

- Do you have a well-defined yet clear password strategy for employees?
- Do you have a mechanism to check whether staff passwords can be found on common stolen credentials lists used by attackers?
- Do you ensure the principle of least privilege applies across the enterprise — that is, only those who need access to a resource get it?

Click link above to read more

Darknet Disruption: 'Wall Street Market' Closed for Business

https://www.bankinfosecurity.com/darknet-disruption-wall-street-market-closed-for-business-a-12446

Two of the world's most notorious darknet markets have been disrupted as part of coordinated, international law enforcement operations. The markets sold illegal narcotics, counterfeit currency, malware, stolen jewelry and more.

Authorities officially announced the takedowns of the Wall Street Market as well as the Silkkitie - aka Valhalla Marketplace - on Friday.

The Wall Street Market was formerly the world's second-largest illegal darknet market.

Click link above to read more.

Drug Lab Cyberattack Puts Spotlight on IP Theft Threat

https://www.bankinfosecurity.com/drug-lab-cyberattack-puts-spotlight-on-ip-theft-threat-a-12448

In what may be a case of industrial espionage, Massachusetts-based drug development company Charles River Laboratories has reported unauthorized access to portions of its information systems and the copying of data by an intruder.

In an April 30 8K filing with the Securities and Exchange Commission, Charles River Laboratories says it has notified clients of the incident.

Click link above to read more

Trump Order Aims to Boost Federal Cybersecurity Workforce

https://www.bankinfosecurity.com/trump-order-aims-to-boost-federal-cybersecurity-workforce-a-12447

The White House is hoping a mix of new incentives and programs can bolster the federal government's cybersecurity workforce.

On Thursday, President Donald Trump signed an executive order that offers a mix of incentives and new guidelines aimed at hiring and retaining more security pros to work within the federal government. The order creates a President's Cup Cybersecurity Competition as a way to reward top professionals. It also enables federal employees to take on temporary assignments at other agencies to gain knowledge of cybersecurity issues.

There are more than 300,000 open cybersecurity position the U.S., and the administration believes that a public-private sector initiative can help bridge that gap, Trump said in a statement.

Click link above to read more

Mystery Database Exposed Info on 80 Million US Households

https://www.bankinfosecurity.com/mystery-database-exposed-info-on-80-million-us-households-a-12432

A mysterious, unsecured database hosted on Microsoft's cloud platform contained personal information on nearly 80 million U.S. households, according to two researchers who found it.

In a blog posted Monday, Noam Rotem and Ran Locar, self-described security researchers and hacktivists, describe finding the exposed 24 GB database that contained information pertaining to 80 million U.S. households, including the full names of residents, age, marital status, income bracket and other details.

Click link above to read more

Israel Bombs Building as Retaliation for Hamas Cyber Attack

https://www.bleepingcomputer.com/news/security/israel-bombs-building-as-retaliation-for-hamas-cyber-attack/

The Israel Defense Forces (IDF) announced that a building used by Hamas cyber operatives was bombed on Saturday as part of a joint retaliation operation with the Israel Security Agency (Shin Bet) and Unit 8200 of Military Intelligence, following a failed cyber attack against Israel.

IDF's attack on the Hamas cyber operations center came during intensive fire exchanges between Israel and the Palestinians, which led to the exchange of roughly 900 rockets and, eventually, with an Egyptian-mediated cease-fire that began Monday 4:30 A.M.

Click link above to read more

Someone Is Hacking GitHub Repositories and Holding Code Ransom

https://www.vice.com/en_us/article/vb9v33/github-bitbucket-repositories-ransomware

Hackers are breaking into private code repositories, wiping them, and asking their owners for a ransom to restore their projects.

Ransomware, a type of attack where hackers infect computers, encrypt their content, and ask for money in exchange for a decryption key that will restore their data, has been around for decades. This new attack is a little different, but it’s unclear how successful it will be since one victim has claimed to have found a way to recover their code without paying the ransom.

Click link above to read more

The Cybersecurity 202: A cyberattack just disrupted grid operations in the U.S. But it could have been far worse.

https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/05/06/the-cybersecurity-202-a-cyberattack-just-disrupted-grid-operations-in-the-u-s-but-it-could-have-been-far-worse/5ccf61eda7a0a46cfe152c3e/?noredirect=on&utm_term=.f1fc1c5efb01

A recently disclosed hack at an electric utility in the western United States crosses a disturbing new line.

It’s the first time a digital attack is known to have interfered with electrical grid operations in the United States. And it was due to a relatively basic hack, raising the specter of what might happen if a sophisticated bad actor chose to launch a far more powerful attack, say, with the intent of shuting off electricity for millions of people.

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:

Information Security Awareness Team - Information Security Branch
Office of the Chief Information Officer,
Ministry of Citizens’ Services
4000 Seymour Place, Victoria, BC   V8X 4S8
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