Security Digest
Information Security Branch
British Columbia
OCIO
Office of the Chief Information Officer

September 11th, 2018

September is “Social Media” Month

This week’s stories:

- **Controversy erupts over Five Eyes countries’ statement on encryption** 🇨🇦
- **Digital Payments Security: Lessons From Canada** 🇨🇦
- **Facebook, Twitter try to limit U.S. regulation at hearing**
- **Apple Removes Top Security App For Stealing Data and Sending it to China**
- **Tesla Will Restore Car Firmware/OS When Hacking Goes Wrong**
- **Vodafone Tells Hacked Customers with "1234" Password to Pay Back Money**
- **Feds Charge North Korean With Devastating Cyberattacks**
- **Teenage hacker admits making hoax bomb threats against schools and airlines**
- **Russian Charged in JPMorgan Chase Hack Extradited to US**
- **Cyber Insurance Market to Double by 2020, Says Munich Re**
- **Trend Micro Apps Leak User Data, Removed from Mac App Store**
- **Postmortem: Multiple Failures Behind the Equifax Breach**

Controversy erupts over Five Eyes countries’ statement on encryption 🇨🇦

https://www.itworldcanada.com/article/controversy-erupts-over-five-eyes-countries-statement-on-encryption/408738

Are Canada, the U.S. and other members of the Five Eyes intelligence alliance preparing to sacrifice online privacy to increase security? Are the five countries about to increase pressure on telecom and software companies to install ways of defeating encryption?

Yes, if you believe privacy advocates after seeing a communique issued last week by security and public safety ministers following their annual meeting in Australia.

They are alarmed the statement says the five countries – including the U.K., Australia and New Zealand – “agreed to the urgent need for law enforcement to gain targeted access to data, subject to strict safeguards, legal limitations, and respective domestic consultations.”

Click link above to read more

Digital Payments Security: Lessons From Canada 🇨🇦

https://www.databreachtoday.com/interviews/digital-payments-security-lessons-from-canada-i-4108

Canada, which has a head start on the adoption of digital payments, has learned some valuable security lessons that could be beneficial to the U.S., says Gord Jamieson of Visa.

"If we look at Canada itself as a market, we're probably one of the leading countries when it comes to the adoption and usage of digital payments," says Jamieson, head of payment system risk for Visa Canada. "Seventy percent of our Canadian personal consumption expenditure is conducted using digital payments."

Click link above to read more

Facebook, Twitter try to limit U.S. regulation at hearing

https://www.itworldcanada.com/article/facebook-twitter-try-to-limit-u-s-regulation-at-hearing/408633

Senior executives of Facebook and Twitter faced a Congressional committee Wednesday morning trying to limit the amount of regulation the U.S. government might impose on social media companies in the wake of increasing evidence that foreign organizations are using them for disinformation campaigns there and in other countries.

“Actions taken show how determined we are to do everything we can do to stop this from happening,” said Facebook COO Sheryl Sandberg.

She noted the company has more than doubled the number of people working in its safety and security divisions to 20,000, reviewing reports in 50 languages. With the use of machine learning Facebook is more proactive in finding abuse, she said. In the first three months of this year over 85 per cent of violent content was either taken down or added warning labels before they were reported.

“We are now blocking millions of attempts to register false accounts each and every day,” she added.

Click link above to read more

Apple Removes Top Security App For Stealing Data and Sending it to China

https://www.bleepingcomputer.com/news/security/apple-removes-top-security-app-for-stealing-data-and-sending-it-to-china/

Apple removed today a very popular anti-malware app called Adware Doctor from the Mac App Store because it was gathering browsing history and other sensitive information without a user's permission and then uploading it to someone in China.

Adware Doctor is promoted as an anti-malware and adware protection program that claims to be able to protect your Mac from malicious files and browser from adware. This program was the #1 paid utility in the Mac App Store with a 4.8 star rating and over 7,000 reviews.

Click link above to read more

Tesla Will Restore Car Firmware/OS When Hacking Goes Wrong

https://www.bleepingcomputer.com/news/security/tesla-will-restore-car-firmware-os-when-hacking-goes-wrong/

Tesla recently added to its responsible disclosure guidelines with clarifications that welcome researchers to probe software in its cars for security bugs.

Well-known for its security-aware attitude, the company is now spelling it out to security researchers that they can hack Tesla cars without fear of ending up with a non-running automobile, of voiding the warranty, or of legal liability.

Click link above to read more

Vodafone Tells Hacked Customers with "1234" Password to Pay Back Money

https://www.bleepingcomputer.com/news/security/vodafone-tells-hacked-customers-with-1234-password-to-pay-back-money/

A Czech court recently sentenced two hackers to three years in prison for accessing Vodafone customer's mobile accounts and using them to purchase 600,000 Czech Koruna worth of gambling services. Vodafone reportedly wants the hacked victim's to pay for these charges as they were using an easy password of "1234".

According to reporting from Czech news site idnes.cz, the hackers accessed mobile customer's accounts by using the password 1234. Once they were able to gain access, they ordered new SIM cards that they picked up from various branches. As they knew the phone number and password they were able to pick up the SIM card and install it in their phones without any other verification.

This allowed the attackers to charge over 600,000 Czech Koruna, or approximately 30K USD, for gambling services.

Click link above to read more

Feds Charge North Korean With Devastating Cyberattacks

https://www.databreachtoday.com/feds-charge-north-korean-devastating-cyberattacks-a-11473

U.S. prosecutors have accused a 34-year-old North Korean man of involvement in some of the most destructive and profitable cyberattacks ever seen, including the WannaCry ransomware outbreak, the Sony Pictures Entertainment breach as well as the theft of $81 million from Bangladesh Bank.

Click link above to read more

Teenage hacker admits making hoax bomb threats against schools and airlines

https://hotforsecurity.bitdefender.com/blog/teenage-hacker-admits-making-hoax-bomb-threats-against-schools-and-airlines-20309.html

British police have announced that they have arrested a 19-year-old man in connection with a series of hoax bomb threats and distributed denial-of-service (DDoS) attacks.

George Duke-Cohan (who goes by online aliases such as “7R1D3N7”, “DoubleParallax”, and “optcz1”) is also reported to be a member of the Apophis Squad hacking gang, which has launched denial-of-service attacks against secure email provider ProtonMail, and cybersecurity blogger Brian Krebs.

Click link above to read more

Russian Charged in JPMorgan Chase Hack Extradited to US

https://www.databreachtoday.com/russian-charged-in-jpmorgan-chase-hack-extradited-to-us-a-11476

A Russian national who's been accused of hacking into JPMorgan Chase's network in 2014 and stealing personal information on more than 83 million customers has been extradited to the United States to face hacking, wire fraud and other charges.

The U.S. Department of Justice says Andrei Tyurin, 35, was extradited from the Eastern European country of Georgia. He appeared in Manhattan federal court on Friday and pleaded not guilty, Bloomberg reported.

Click link above to read more

Cyber Insurance Market to Double by 2020, Says Munich Re

https://www.securityweek.com/cyber-insurance-market-double-2020-says-munich-re

"Cyber risks are one of the biggest threats to the networked economy," Munich Re board member Torsten Jeworrek said in a statement on the first day of an annual meeting of reinsurers in the Mediterranean principality.

Munich Re estimated that companies could more than double their spending on cyber insurance from $3.4-$4 billion (3-3.4 billion euros) in 2017 to $8-$9 billion by 2020.

Click link above to read more

Trend Micro Apps Leak User Data, Removed from Mac App Store

https://www.bleepingcomputer.com/news/security/trend-micro-apps-leak-user-data-removed-from-mac-app-store/

Multiple apps developed by Trend Micro are no longer available in the Mac App Store after researchers showed they were collecting browser history and information about users' computers.

On Friday, Apple removed Adware Doctor, a top security app, from its store, on the exact same grounds.

The apps are Dr. Antivirus, Dr. Cleaner, and Dr. Unarchiver, all under the developer account Trend Micro, Incorporated. Until removal, all products were top-sellers, with thousands of positive reviews that averaged their ratings between 4.6 and 4.9.

Click link above to read more

Postmortem: Multiple Failures Behind the Equifax Breach

https://www.databreachtoday.com/postmortem-multiple-failures-behind-equifax-breach-a-11480

A newly released report on the Equifax breach from the U.S. Government Accountability Office, titled "Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach," provides new details into how the breach occurred and what Equifax could have done to have helped prevent or more rapidly mitigate it, centering on failures involving detection, segmentation and data governance.

Equifax's latest count of breach victims includes at least 145.5 million U.S. consumers for whom PII was compromised. The credit bureau has also said that 15.2 million records pertaining to U.K. residents were exposed, putting 860,000 British consumers at risk, and said that 8,000 Canadian residents' personal details were also exposed.

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.

Information Security Branch
www.gov.bc.ca/informationsecurity

BRITISH COLUMBIA

OCIO
Office of the Chief Information Officer