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

September 25th, 2018

September is “Social Media” Month

This week’s stories:

- **Thousands of Canadians’ personal data from NCIX servers listed on Craigslist: cybersecurity expert** 🇨🇦
- **Federal workers cited 3,075 times for lapses in document security** 🇨🇦
- **BlackBerry CEO John Chen warns driverless cars could turn into fully loaded weapons if hacked**
- **Cyber security is changing, and so is the way it’s being sold**
- **Botnet-powered credential stuffing still a problem**
- **Full disclosure: Benchmarking data reveals the human error in privacy incidents**
- **Google still lets third-party apps scan your Gmail data**
- **Security Engineer Hacks Hotel WiFi, Fined for Exposing Admin Password**
- **Mirai’s architects avoid prison thanks to work for FBI**
- **Fitbit-based life insurance is a potential privacy and security nightmare**
- **Thousands of Breached Websites Turn Up On MagBo Black Market**
- **The Latest Cryptocurrency Exchange Hack Is a $60 Million Theft at Japan's Zaif**

Thousands of Canadians’ personal data from NCIX servers listed on Craigslist: cybersecurity expert 🇨🇦

https://globalnews.ca/news/4476625/ncix-server-data-breach/

Privacy advocates are raising the alarm after data potentially belonging to thousands of Canadians allegedly made its way onto buy-and-sell website Craigslist.

The information was contained on servers and hard drives formerly owned by Vancouver-based computer retailer NCIX.

The company went bankrupt last December, and its inventory was auctioned off.

Click link above to read more

Federal workers cited 3,075 times for lapses in document security 🇨🇦

https://www.cbc.ca/news/politics/security-sweep-pspc-privacy-1.4833551

Office workers at Public Services and Procurement Canada were cited 3,075 times last year for failing to lock up documents, USB keys and other storage devices containing sensitive information, says a new security report.

And six of those employees were found to be chronic offenders during a "security sweep" at the department in 2017-2018, with each of them leaving confidential material unsecured at least six times over the 12-month period.

"In 2017, we identified six employees who exceeded maximum offences and we are doing review for cause interviews," says a June 2018 briefing note, obtained by CBC News under the Access to Information Act.

Click link above to read more

BlackBerry CEO John Chen warns driverless cars could turn into fully loaded weapons if hacked

https://business.financialpost.com/technology/driverless-driverless-cars-could-be-fully-loaded-weapons-if-tech-i

Driverless cars could be hacked and deployed as “fully loaded weapons,” according to the chief executive of BlackBerry.

Best known for its smartphones, the company is developing software for driverless cars in partnership with Baidu, the Chinese web search giant.

John Chen, BlackBerry’s chief executive, said driverless cars were programmed with more lines of code than a typical fighter jet, offering enormous scope for hackers to exploit vulnerabilities to insert malware

Click link above to read more

Cyber security is changing, and so is the way it’s being sold

https://www.itworldcanada.com/article/cybersecurity-is-changing-and-so-is-the-way-its-being-sold/409213

Cyber security vendors still have sales targets to meet and their own products to glorify, but a “weird sales dynamic,” as Brian Krause describes, is also creeping its way into the market.

“Every single person in here is a salesperson, there’s no denying what we’re doing here … it’s our software first,” said the director of North American channels for Centrify, referring to a room full of cyber security vendors at Optiv Security‘s 2018 Toronto Enterprise Security Solutions Summit last week. “But we’re seeing more, especially in the software community, most of us are partnering with each other.”

Click link above to read more

Botnet-powered credential stuffing still a problem

https://www.itworldcanada.com/article/botnet-powered-credential-stuffing-still-a-problem-report/409268

Phishing is one of the most successful ways attackers get past an organization’s network defences. But credential stuffing –backed by the power of botnets and millions of stolen usernames and passwords — is still a potent weapon.

According to a report issued last week by Akamai, it’s network detected 8.3 million malicious login attempts between May and the end of June.

One botnet made 300,000 attempts an hour over a series of targets.

Click link above to read more

Full disclosure: Benchmarking data reveals the human error in privacy

https://iapp.org/news/a/full-disclosure

This month, we are returning to this topic to dig deeper into incident intent classifications and how they can be further broken down into specific scenarios. To level set, looking at data from January 2017 through July 2018, we can see that the vast majority of incidents fall into one intent classification:

- Intentional, malicious intent: 0.86 percent of incidents.
- Intentional, not malicious intent: 2.78 percent of all incidents.
- Unintentional or inadvertent intent: 96.33 percent of all incidents.

The numbers show that unintentional or inadvertent incidents — those typically caused by human error rather than malicious intent such as hacking — are by far the most common.

Click link above to read more

Google still lets third-party apps scan your Gmail data

https://money.cnn.com/2018/09/20/technology/google-gmail-scanning/index.html

Google is defending its policy to allow third-party apps to access and share data from Gmail accounts, according to a letter made public Thursday.

Gmail, which has over 1.4 billion users globally, lets third-party developers integrate services into its email platform, such as trip planners and custom relationship management systems.

"Developers may share data with third parties so long as they are transparent with the users about how they are using the data," Susan Molinari, VP of public policy and government affairs for the Americas at Google, said in the letter to Senators, which was obtained by CNNMoney.

Click link above to read more

Security Engineer Hacks Hotel WiFi, Fined for Exposing Admin Password

https://www.bleepingcomputer.com/news/security/security-engineer-hacks-hotel-wifi-fined-for-exposing-admin-password/

A security engineer from Chinese multinational company Tencent hacked into the WiFi system of a hotel in Singapore and received a fine for publicly disclosing administrator login passwords.

Zheng Dutao participated in the capture-the-flag competition during the Hack In The Box security conference in Singapore at the end of August and decided to test the WiFi defenses of the Fragrance Hotel he checked into.

Click link above to read more

Mirai’s architects avoid prison thanks to work for FBI

https://www.welivesecurity.com/2018/09/20/mirais-architects-avoid-prison-thanks-work-fbi/

A US court has slapped an unusually lenient sentence on three men who’ve pleaded guilty to developing and operating a powerful botnet known as Mirai that in its heyday comprised hundreds of thousands of Internet-of-Things (IoT) devices.

Paras Jha, Josiah White, and Dalton Norman, who are all 21-22 years old, were each sentenced by a court in Alaska to serve five years of probation according to a statement from the US Department of Justice. The three men, all of whom are US citizens, also gave up significant amounts of cryptocurrency seized during the investigation into their activities and were ordered to pay $127,000 in restitution. Additionally, they were given 2,500 hours of community service – which includes continued cooperation with law enforcement and security researchers.

Click link above to read more

Fitbit-based life insurance is a potential privacy and security nightmare

https://thenextweb.com/security/2018/09/20/fitbit-based-life-insurance-is-a-potential-privacy-and-security-nightmare/

John Hancock is one of the oldest and most established insurance companies in the United States. According to Reuters, it's also the first US insurance company to ditch traditional life insurance policies entirely in favor of "interactive life insurance."

What does this mean? Essentially, John Hancock is encouraging (but not mandating) that policyholders to share health and lifestyle data with the company. This data typically comes from wearable devices, like the Apple Watch or Fitbit.

Those who lead healthy, active lifestyles are likely to live longer than, say, an overweight chain-smoker that has never even stepped foot in a gym. Insurance companies want healthier customers, as it means they collect more premiums over the lifetime of the policy, and ultimately pay out less when the person dies.

Click link above to read more

Thousands of Breached Websites Turn Up On MagBo Black Market

https://threatpost.com/thousands-of-breached-websites-turn-up-magbo-black-market/137564/

A newly-discovered underground marketplace has been peddling access to more than 3,000 breached websites, catering to hackers hungry for valuable data and the ability to launch a range of attacks on unsuspecting site visitors.

Advertisements for the Russian-speaking marketplace called MagBo were first posted on a top-tier hacking forum in March, according to researchers at Flashpoint. Upon further investigation, the research team found that details for thousands of breached websites were for sale on MagBo.

Click link above to read more

The Latest Cryptocurrency Exchange Hack Is a $60 Million Theft at Japan's Zaif

http://fortune.com/2018/09/20/cryptocurrency-exchange-hack-zaif-japan-60-million/

Hackers stole $60 million of digital coins from a Japanese exchange, the latest in a string of thefts that have kept many institutional investors wary of putting their money in cryptocurrencies.

The theft of Bitcoin, Monacoin and Bitcoin Cash from Zaif, an exchange owned by Osaka-based Tech Bureau Corp., occurred last week and was disclosed by Tech Bureau in a statement on Thursday. About 2.2 billion yen ($19.6 million) of stolen coins belonged to the exchange and the rest was client money.

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