Security Digest
Information Security Branch

BRITISH COLUMBIA

OCIO
Office of the Chief Information Officer

September 18th, 2018

September is "Social Media" Month

This week's stories:

- **Federal employee reports theft of device with personal data**
- **Ransomware attack shuts down small Canadian town; officials pay ransom**
- **California bill regulates IoT for first time in US**
- **Misconfigured MongoDB database exposed customer data: Researcher**
- **New CSS Attack Restarts an iPhone or Freezes a Mac**
- **Cold-Boot Attack Steals Passwords In Under Two Minutes**
- **FreshMenu Hid Data Breach Affecting 110,000 Users**
- **Police in Europe Tie Card Fraud to People-Smuggling Gang**
- **Wielding EternalBlue, Hackers Hit Major US Business**
- **Why Cybercrime Remains Impossible to Eradicate**
- **UK Airport Won't Negotiate With Ransomware Attackers; Falls Back to Whiteboards**
- **Health Department blasted for 'disappointing' response to pharmacist snooping case**

Federal employee reports theft of device with personal data

https://www.itworldcanada.com/article/federal-employee-reports-theft-of-device-with-personal-data/408977

A device with personal information on 227 employees of Infrastructure Canada was reported stolen last month.

News of the theft was first revealed Thursday by Global News and confirmed this morning by a spokesperson for Public Services and Procurement Canada (PSPC).

A PSPC employee notified Ottawa police of the theft August 20, and then told their government supervisor the next day, Rania Haddad, a PSPC spokesperson said in an email today. The statement didn't detail what was on the device, but according to Global News, PSPC's Deputy Minister Marie Lemay sent an email Sept. 7 to affected staff that "no banking or social insurance information was affected. However, your name, person record identifier (PRI), date of birth, home address and salary range may have been on the stolen device."

Click link above to read more

Ransomware attack shuts down small Canadian town; officials pay ransom

https://hotforsecurity.bitdefender.com/blog/ransomware-attack-shuts-down-small-canadian-town-officials-pay-ransom-20331.html

The small Canadian town of Midland, Ontario, was hit by ransomware, and the municipality seems to be negotiating with hackers to pay ransom, reports Canadian news station CTV News.

The attack on September 1 completely shut down the computer system, leaving the municipality unable to use its financial processing system. During the shutdown, debit and credit card payments were not accepted.

Click link above to read more

California bill regulates IoT for first time in US

https://nakedsecurity.sophos.com/2018/09/13/california-bill-regulates-iot-for-first-time-in-us/

California looks set to regulate IoT devices, becoming the first US state to do so and beating the Federal Government to the post.

The State legislature approved 'SB-327 Information privacy: connected devices' last Thursday and handed it over to the Governor to sign. The legislation introduces security requirements for connected devices sold in the US. It defines them as any device that connects directly or indirectly to the internet and has an IP or Bluetooth address. That covers an awful lot of devices.

Click link above to read more

Misconfigured MongoDB database exposed customer data: Researcher

https://www.itworldcanada.com/article/misconfigured-mongodb-database-exposed-customer-data-researcher/408971

Criminals, activists and nation states are snooping around your organization looking for security vulnerabilities, and if it's not them then you have to worry about disgruntled insiders with an axe to grind. But the truth is one of the biggest threats are well-meaning employees who don't follow — or know — security rules.

Another example came to light this week with the discovery by security researcher and reporter Bob Diachenko of a misconfigured MongoDB server on Amazon apparently used by staff of data management company Veeam Software. Using the Shodan search engine Diachenko came across the database on Sept. 5. It was "publicly searchable and wide open" until Sept. 9th, when, after several notification attempts to Veeam by him and a reporter from TechCrunch, it was secured.

Click link above to read more

New CSS Attack Restarts an iPhone or Freezes a Mac

https://www.bleepingcomputer.com/news/security/new-css-attack-restarts-an-iphone-or-freezes-a-mac/

A new attack has been discovered that will cause iOS to restart or respring and macOS to freeze simply by visiting a web page that contains certain CSS & HTML. Windows and Linux users are not affected by this bug.

This new attack was discovered by Sabri Haddouche, a security researcher at Wire, who was able to devise a way to quickly use up an Apple device's resources so that it crashes when visiting a web page.

"The attack uses a weakness in the -webkit-backdrop-filter CSS property," Haddouche told BleepingComputer. "By using nested divs with that property, we can quickly consume all graphic resources and crash or freeze the OS. The attack does not require Javascript to be enabled therefore it also works in Mail. On macOS, the UI freeze. On iOS, the device restart."

Click link above to read more

Cold-Boot Attack Steals Passwords In Under Two Minutes

https://www.bleepingcomputer.com/news/security/cold-boot-attack-steals-passwords-in-under-two-minutes/

Relying on computer memory's remanence behavior, security researchers figured out a way to extract sensitive data from RAM, such as encryption keys, even after the loss of power.

The attack subscribes to the cold-boot category and exploits a weakness in how the computers protect the low-level software responsible for interacting with the RAM.

Known for its volatility in data retention when out of power, RAM (Random Access Memory) can preserve information for a longer time - even minutes, under low-temperature conditions.

Click link above to read more

FreshMenu Hid Data Breach Affecting 110,000 Users

https://www.databreachtoday.com/freshmenu-hid-data-breach-affecting-110000-users-a-11514

FreshMenu, a food delivery provider based in India, has come under social media attack for keeping under wraps a data breach two years ago that exposed the personal information of over 110,000 users.

The incident originally was brought to light in 2016 by data breach tracker HaveIBeenPwned, which discovered that the breach exposed names, email addresses, phone numbers, home addresses, and order histories, the Times of India reported on Wednesday. That news report led to the strong response on social media.

Click link above to read more

Police in Europe Tie Card Fraud to People-Smuggling Gang

https://www.databreachtoday.com/police-in-europe-tie-card-fraud-to-people-smuggling-gang-a-11518

Coordinated police raids in Germany and Sweden have resulted in the arrest of two individuals suspected of running a cyber fraud gang that used stolen payment card data to book hundreds of airline and train tickets to help smuggle people from the Middle East into Europe.

The EU's law enforcement intelligence agency Europol, which helped coordinate the raids, says they were launched after a private sector tip-off. Europol's European Cybercrime Center subsequently helped police identify suspects, leading to the arrest of two individuals last week.

Click link above to read more

Wielding EternalBlue, Hackers Hit Major US Business

http://www.databreachtoday.com/

Attack code known as EternalBlue, designed to exploit a Windows SMB flaw, continues to work for attackers despite Microsoft having issued patches more than a year ago. One major U.S. business was a recent victim as part of a cryptocurrency-mining malware campaign, a researcher reports.

Click link above to read more

Why Cybercrime Remains Impossible to Eradicate

https://www.databreachtoday.com/blogs/cybercrime-remains-impossible-to-eradicate-p-2662

More evidence that running cybercrime schemes remains inexpensive and accessible to anyone with criminal intent: To send spam emails, admitted botnet herder Peter Levashov quoted customers $500 for 1 million emails, $750 for 2 million emails, or $1,000 for 3 million emails, according to court documents.

And that was just his 2016 pricing. By 2017, Levashov was quoting customer's rates that began at $300 for 1 million spam emails, payable in bitcoin, according to court documents. But he allegedly charged more if those emails were to be used in phishing, ransomware or other more complicated types of campaigns.

Click link above to read more

UK Airport Won't Negotiate With Ransomware Attackers; Falls Back to Whiteboards

https://hotforsecurity.bitdefender.com/blog/uk-airport-wont-negotiate-with-ransomware-attackers-falls-back-to-whiteboards-20339.html

UK's Bristol Airport computers that displayed flight departure and arrival information were taken offline by a ransomware infection, causing officials to fall back to whiteboards and paper posters.

The airport's TV screens started displaying a ransom note early Friday morning, prompting airport officials to issue a warning over the weekend for passengers to arrive earlier than usual for check in. Using whiteboard and paper posters to constantly update flight information, passengers took to Twitter to offer snappy remarks, vent, or simply make fun of the situation.

Refusing to give in to the ransom note, Bristol Airport officials announced they will start restoring affected systems over the weekend. Early Sunday morning all systems were officially online, with all TV screens displaying flight departure and arrival information.

Click link above to read more

Health Department blasted for 'disappointing' response to pharmacist snooping case

https://www.cbc.ca/news/canada/nova-scotia

Nova Scotia's privacy commissioner says the confidential drug records of Nova Scotians are still not as secure as they should be, and she blames a lack of action by the Department of Health.

On Monday, Catherine Tully called the department's response to two reports she released last month "very disappointing."

The reports, one aimed at Sobeys, the other at the department, chronicled the actions of a Greenwood, N.S., pharmacist who worked for Sobeys and over a two-year period accessed the confidential drug records of 46 people.

Click link above to read more

Click Unsubscribe to stop receiving the Digest.

****

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