Security Digest
Information Security Branch

BRITISH COLUMBIA

OCIO
Office of the Chief Information Officer

September 4th, 2018

August is "Social Media" Month

This week's stories:

- **Air Canada: Attack Exposed 20,000 Mobile App Users' Data**
- **Preparing for Windows 7 'doomsday'**
- **Testing Apple's new Screen Time parental controls: First came tears, then frustration**
- **Executive compromise attacks don't always have malicious links**
- **Card-Skimming Malware Campaign Hits Dozens of Sites Daily**
- **Police Probe Sale of 130 Million Chinese Hotel-Goers' Data**
- **Election Security: FBI Combats Information Operations**
- **Remote Access Phone Scams Bilk Australians of AU$4.4 Million Stolen So Far in 2018**
- **2.3 Million T-Mobile Customers Exposed Following Data Breach**

Air Canada: Attack Exposed 20,000 Mobile App Users' Data

https://www.databreachtoday.com/air-canada-attack-exposed-20000-mobile-app-users-data-a-11441

Air Canada is forcing 1.7 million mobile app accountholders to reset their passwords after it detected unusual login behavior that it says may have exposed 20,000 accounts, including customers' passport details. But the airline has been forced to battle ongoing technical problems as well as hordes of angry users.

Click link above to read more

Preparing for Windows 7 'doomsday'

https://www.itworldcanada.com/article/is-your-company-ready-for-windows-7-doomsday/408549

The countdown has started, Saturday marks only 500 days until Microsoft stops supporting the world's most popular operating system, Windows 7 according to a new study.

This could cause major security concerns for companies as Microsoft will stop providing vital security updates to the Windows 7 system by Janruary 2020, according to a study from Kollective, a content delivery company

However, many corporate IT departments, 66 per cent in fact, don't see moving away from Windows 7 as a priority, the report stated.

Click link above to read more

Testing Apple's new Screen Time parental controls: First came tears, then frustration

https://business.financialpost.com/technology/personal-tech/testing-apples-new-screen-time-parental-controls-first-came-tears-then-frustration

“Don’t set the time limit. I can be reasonable!” pleads 9-year-old Tazio, looking up from his iPad.

It’s not always fun owning an iPad that a parent can remotely shut off. Also not easy: Trying to parent via new digital “Screen Time” controls.

Coming soon to an iPad or iPhone near you, Apple’s iOS 12 adds menus, buttons and bar charts to help monitor and control what kids (and adults) do with their devices. It’s a good thing that Apple, along with Amazon and Google, now acknowledge tech can be disruptive, if not addictive.

But anyone looking for help from this software may be in for a surprise. It might make parenting more difficult. One example: Apple’s bad default settings give kids access to NC-17 movies, explicit books and the entire web — even when it knows their exact age.

Click link above to read more

Executive compromise attacks don’t always have malicious links

https://www.itworldcanada.com/article/executive-compromise-attacks-dont-always-have-malicious-links-report/408569

For an attacker, spear phishing is an efficient way of getting work done. Business Email Compromise (BEC) schemes (sometimes also called business executive compromise), which specifically target executives or mid-level finance officials, can be particularly useful: Get an official to click on a link, infect the target and there’s high-level access to an organization. Or, get the official to wire money to a link and rake in the cash.

To counter this, security awareness defensive techniques include training employees to watch out for suspicious links in email, text or social media messages.

Click link above to read more

Card-Skimming Malware Campaign Hits Dozens of Sites Daily

https://www.databreachtoday.com/card-skimming-malware-campaign-hits-dozens-sites-daily-a-11451

More than 7,000 e-commerce sites in the past six months have been infected with harmful JavaScript designed to harvest customers' payment card details as they finalize their orders.

So warns Willem de Groot, a security consultant and researcher based in the Netherlands, who says that online card-skimming software that communicates with a domain hosted in Moscow, magentocore[dot]net, is being used to infect 50 to 60 e-commerce sites a day.

"The victim list contains multimillion-dollar, publicly traded companies, which suggests the malware operators make a handsome profit," de Groot writes in a blog post, noting that the malicious code is designed to work with legitimate Magento e-commerce software. "But the real victims are eventually the customers who have their card and identity stolen."

Click link above to read more

Police Probe Sale of 130 Million Chinese Hotel-Goers' Data

https://www.databreachtoday.com/police-probe-sale-130-million-chinese-hotel-goers-data-a-11442

Police in China are investigating the apparent loss of 130 million customers' personal details from Huazhu Hotels Group. The data exposure may trace to a Huazhu production database for which access credentials were accidentally uploaded to GitHub, the web-based code sharing and development platform.

Click link above to read more

Election Security: FBI Combats Information Operations

https://www.databreachtoday.com/blogs/election-security-fbi-combats-information-operations-p-2657

With the U.S. midterm election primaries already well underway, the FBI this week launched an informational website that describes the bureau's actions to counter propaganda and influence operations being run by foreign governments

Click link above to read more

Remote Access Phone Scams Bilk Australians of AU$4.4 Million Stolen So Far in 2018

https://hotforsecurity.bitdefender.com/blog/remote-access-phone-scams-bilk-australians-of-au4-4-million-stolen-so-far-in-2018-20279.html

The Australian Competition and Consumer Commission (ACCC) reported that 8,000 scam attempts that have taken place by mid-2018 have resulted in AU$4.4 million being lost to scammers.

While traditional phone scams trick victims into believing their computers are riddled with malware and promise to clean them by instructing them to purchase fictive security software, they now claim to be investigating hacking attempts.

Pretending to be calling on behalf of Telstra, the National Broadband Network (NBN) company, Microsoft, or the police, they tap into victims' internet backing accounts by using popular remote desktop tools and transfer money to attacker-controlled bank accounts.

Click link above to read more

2.3 Million T-Mobile Customers Exposed Following Data Breach

https://hotforsecurity.bitdefender.com/blog/2-3-million-t-mobile-customers-exposed-following-data-breach-20282.html

The personal data of 2.3 million T-Mobile customers may have been exposed and could be up for sale following a data breach on Aug. 20. While the company did say it successfully blocked the attack and no credit card information, social security numbers, or passwords were compromised, other personal data may have been accessed.

The type of information believed to have been exfiltrated by the hacker ranges from customers' names, phone numbers, zip codes, and email addresses to account numbers and whether or not the accounts were prepaid or postpaid.

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.