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

# July 16th, 2019

**Try our July quiz – Summer Phishing**

## This week's stories:

- **Firms have to get back to cyber security basics, government expert tells Parliament** 🇨🇦
- **Public skeptical over privacy protection in Sidewalk Labs' Toronto waterfront plan** 🇨🇦
- **Cost of mounting an APT attack could be as low as US$15,000, says vendor**
- **Almost all of the world's biggest banks vulnerable to web or mobile attacks: Vendor study**
- **Australia's anti-encryption laws being used to bypass journalist protections, expert says**
- **An Amazon Phishing Scam Hits Just in Time For Prime Day**
- **Monroe College Hit With Ransomware, $2 Million Demanded**
- **25 Million Android Devices Infected by 'Agent Smith' Malware**
- **U.S. regulators approve $5 bln Facebook settlement over privacy issues – source**
- **$32m stolen from Tokyo cryptocurrency exchange in latest hack**
- **Google workers can listen to what people say to its AI home devices**
- **FBI Releases Master Decryption Keys for GandCrab Ransomware**

### Firms have to get back to cyber security basics, government expert tells Parliament 🇨🇦

https://www.itworldcanada.com/article/public-skeptical-over-privacy-protection-in-googles-toronto-waterfront-plan/419974

Investing in the basics of cyber security is the best way Canadian organizations can lower the risk of data breaches, a parliamentary committee looking into the recent huge data theft at Desjardins Group of credit unions.

"Ultimately there is no silver bullet when it comes to cyber security," Andre Boucher, deputy minister and director of operations at the Canadian Centre for Cyber Security told members of the House of Commons public safety committee on Monday. "We cannot be complacent."

**Click link above to read more**

### Public skeptical over privacy protection in Sidewalk Labs' Toronto waterfront plan 🇨🇦

https://www.itworldcanada.com/article/public-skeptical-over-privacy-protection-in-googles-toronto-waterfront-plan/419974

There's ample public skepticism in Toronto about the ability of Google's sister company Sidewalk Labs to oversee a proposed lakefront smart community that promises strong data privacy protection, if the first public meeting on the proposed draft master plan of the multi-million-dollar project is a yardstick.

"Databases get hacked again and again," complained one man at the meeting Monday night, "and nobody does anything. When I think of privacy I don't think of Google."

**Click link above to read more**

---

## Cost of mounting an APT attack could be as low as US$15,000, says vendor

https://www.itworldcanada.com/article/cost-of-mounting-an-apt-attack-could-be-as-low-as-us15000-says-vendor/419925

The cost of developing a package of tools for an advanced persistent threat (APT) attack could be as little as US$15,000, estimates a security vendor.

In a report released Thursday, Positive Technologies came to that conclusion after looking at the tools used by 29 APT groups used in attacks over the last two years from its own data — including postings on 190 dark web sites and sites selling APT tools — and public reports from other security companies.

**Click link above to read more**

---

## Almost all of the world's biggest banks vulnerable to web or mobile attacks: Vendor study

https://www.itworldcanada.com/article/almost-all-of-the-worlds-biggest-banks-vulnerable-to-web-or-mobile-attacks-vendor-study/419873

Banks are among the biggest profit-makers in the world and can afford the best in cybersecurity among private sector firms.

But security vendor ImmuniWeb says too many of the websites and mobile apps of the world's biggest financial institutions have vulnerabilities when measured by the free version of its tools.

**Click link above to read more**

---

## Australia's anti-encryption laws being used to bypass journalist protections, expert says

https://www.theguardian.com/australia-news/2019/jul/08/australias-anti-encryption-laws-being-used-to-bypass-journalist-protections-expert-says

The anti-encryption laws passed by the federal parliament last year have been used to bypass journalist protections in other national security laws, a cybersecurity researcher has said.

The parliamentary joint committee on intelligence and security has launched a review into the Telecommunications (Assistance and Access) Act, which passed into law at the end of 2018.

**Click link above to read more**

---

## An Amazon Phishing Scam Hits Just in Time For Prime Day

https://www.wired.com/story/amazon-prime-day-phishing-campaign/

Next week, Amazon will celebrate Prime Day, a bacchanal of modestly discounted ephemera. But amid the flurry of cheap TVs and ebooks and what else, maybe Instant Pots? Watch out for this clever phishing campaign that might hit your inbox.

Researchers from security company McAfee today have shared details of a so-called phishing kit, which contains the tools an aspiring hacker would need to kick off a phishing campaign, designed to target

Amazon customers. While McAfee discovered this particular kit in May, it appears to be a spinoff of one that had targeted Apple users in the US and Japan last November. The kit is called 16Shop; its author goes by the handle DevilScreaM.

**Click link above to read more**

---

## Monroe College Hit with Ransomware, $2 Million Demanded

https://www.bleepingcomputer.com/news/security/monroe-college-hit-with-ransomware-2-million-demanded/

A ransomware attack at New York City's Monroe College has shutdown the college's computer systems at campuses located in Manhattan, New Rochelle and St. Lucia.

According to the Daily News, Monroe College was hacked on Wednesday at 6:45 AM and ransomware was installed throughout the college's network. It is not known at this time what ransomware was installed on the system, but it is likely to be Ryuk, IEncrypt, or Sodinokibi, which are known to target enterprise networks.

**Click link above to read more**

---

## 25 Million Android Devices Infected by ‘Agent Smith’ Malware

https://www.bleepingcomputer.com/news/security/25-million-android-devices-infected-by-agent-smith-malware/

Malware researchers discovered a new malicious campaign for Android devices that replaces legitimate apps with tainted copies built to push advertisements or hijack valid ad events.

Around 25 million devices have already been infected with what researchers have dubbed "Agent Smith," after users installed an app from an unofficial Android store.

**Click link above to read more**

---

## U.S. regulators approve $5 bln Facebook settlement over privacy issues – source

https://vancouversun.com/pmn/business-pmn/u-s-regulators-approve-5-bln-facebook-settlement-over-privacy-issues-wsj/wcm/b36613ce-6c98-4a07-b64f-0ba2bdce95dd

The U.S. Federal Trade Commission approved a roughly $5 billion settlement with Facebook Inc this week over its investigation into the social media company’s handling of user data, a source familiar with the situation said on Friday.

The FTC has been investigating allegations Facebook inappropriately shared information belonging to 87 million users with the now-defunct British political consulting firm Cambridge Analytica. The probe has focused on whether the data sharing violated a 2011 consent agreement between Facebook and the regulator.

**Click link above to read more**

---

## $32m stolen from Tokyo cryptocurrency exchange in latest hack

https://www.theguardian.com/technology/2019/jul/12/tokyo-cryptocurrency-exchange-hack-bitpoint-bitcoin

A cryptocurrency exchange in Tokyo has halted services after it lost $32m (£25m) in the latest apparent hack on volatile virtual monies.

Remixpoint, which runs the Bitpoint Japan exchange, discovered that about ¥3.5bn in various digital currencies had gone missing from under its management.

The apparent hack emerged after an error appeared in the firm's outgoing funds transfer system on Thursday night. It said the cryptocurrency went missing from a so-called hot wallet, which is connected to the internet, but that currency held in cold wallets that are offline was not affected.

**Click link above to read more**

## Google workers can listen to what people say to its AI home devices

https://www.theguardian.com/technology/2019/jul/11/google-home-assistant-listen-recordings-users-privacy

Google acknowledged its contractors are able to listen to recordings of what people say to the company's artificial-intelligence system, Google Assistant.

The company admitted on Thursday that humans can access recordings made by the Assistant, after some of its Dutch language recordings were leaked. Google is investigating the breach.

**Click link above to read more**

## FBI Releases Master Decryption Keys for GandCrab Ransomware

https://www.bleepingcomputer.com/news/security/fbi-releases-master-decryption-keys-for-gandcrab-ransomware/

In an FBI Flash Alert, the FBI has released the master decryption keys for the Gandcrab Ransomware versions 4, 5, 5.0.4, 5.1, and 5.2. Using these keys, any individual or organization can create and release their very own GandCrab decryptor.

On June 1st, 2019, the developers behind the wildly successful GandCrab Ransomware announced that they were closing shop after allegedly amassing $2 billion in ransom payments and personally earning $150 million.

**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

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