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

September 24th, 2019

Try our September quiz – Back to School

This week's stories:

- **Scotiabank source code, credentials found open on GitHub: news report** 🇨🇦
- **TD launches self-serve block features for credit cards** 🇨🇦
- **Botnet takes advantage of weak passwords, poorly-patched systems: report**
- **Smart TVs, smart-home devices found to be leaking sensitive user data, researchers find**
- **Twitter Removes State-backed Actors Conducting Information Campaigns**
- **Selfie Android Apps with 1.5M+ Installs Push Ads, Can Record Audio**
- **400 Million Medical Radiological Images Exposed on the Internet**
- **2020 campaigns get Trump administration help on cybersecurity, counterintelligence**
- **Payment card thieves hack Click2Gov bill paying portals in 8 cities**
- **Ring Provided a Map of Its Customers to Police**
- **A report from a former NSA operative says countries across the world are still adjusting to the new reality of sophisticated cyberwarfare.**

Scotiabank source code, credentials found open on GitHub: news report 🇨🇦

https://www.itworldcanada.com/article/scotiabank-source-code-credentials-found-open-on-github-news-report/421992

A researcher has accused one of Canada's biggest banks of "muppet-grade security" after discovering application source code and private login keys to backend systems on GitHub repositories.

The accusation comes from IT pro Jason Coulls, who, according to the online news service *The Register,* recently discovered the unprotected folders of data belonging to Scotiabank.

"These repositories featured, among other things, software blueprints and access keys for a foreign exchange rate system, mobile application code, and login credentials for services and database instances," the news story says. It describes the files as "a potential gold mine of vulnerabilities for criminals and hackers to exploit."

Click link above to read more

TD launches self-serve block features for credit cards 🇨🇦

https://www.itworldcanada.com/article/td-launches-self-serve-block-features-for-credit-cards/422007

The Toronto-Dominion Bank (TD) has announced a new set of control features for all TD Visa consumer credit cards in Canada, including the ability to temporarily block all access to the account and the ability to block in-person international charges.

To block access to the account, users must be logged on to the TD mobile banking app. In the case of a lost card, users can ease the stress of the situation by disabling the card until it can be located or replaced, depending on the end result. When the feature is enabled, no new purchases can be made with the card or a digital wallet; although pre-authorized payments and deposits will still go through. Once the situation has been resolved, the feature can simply be turned off, restoring the card to its normal functionality.

Click link above to read more

Botnet takes advantage of weak passwords, poorly-patched systems: report

https://www.itworldcanada.com/article/botnet-takes-advantage-of-weak-passwords-poorly-patched-systems-report/421987

There are money-saving advantages to running computers with older operating systems that aren’t carefully patched. But it may come at a price: being infected with malware that makes machines part of a global botnet for harvesting credentials and spreading cryptomining software.

That’s the takeaway from a report this week by security vendor Guardicore into what some researchers are calling the Smominru botnet. Guardicore estimates in August alone August, Smominru infected 90,000 machines around the world, with an infection rate of 4,700 machines per day.

Click link above to read more

Smart TVs, smart-home devices found to be leaking sensitive user data, researchers find

https://www.nbcnews.com/tech/tech-news/smart-tvs-smart-home-devices-found-be-leaking-sensitive-user-n1055796

Smart-home devices, such as televisions and streaming boxes, are collecting reams of data — including sensitive information such as device locations — that is then being sent to third parties like advertisers and major tech companies, researchers said Tuesday.

Click link above to read more

Twitter Removes State-backed Actors Conducting Information Campaigns

https://www.bleepingcomputer.com/news/technology/twitter-removes-state-backed-actors-conducting-information-campaigns/

Twitter has removed another batch of state-sponsored actors performing information campaigns on Twitter. The detected operations announced today involved Qatar, Iran, Yemen, Ecuador, Saudi Arabia, Spain, China, and Hong Kong.

Starting in October 2018, Twitter began disclosing state-backed information operations detected on their service and that were subsequently removed.

Click link above to read more

Selfie Android Apps with 1.5M+ Installs Push Ads, Can Record Audio

https://www.bleepingcomputer.com/news/security/selfie-android-apps-with-15m-installs-push-ads-can-record-audio/

A couple of Android apps found in Google Play included functionality that stealthy recording audio without user consent. The apps posed as selfie camera filters and had been installed over 1.5 million times.

The main activity of the two apps was not spying on users but aggressively pushing adware that covered the entire screen of the Android device.

Click link above to read more

---

400 Million Medical Radiological Images Exposed on the Internet

https://www.bleepingcomputer.com/news/security/400-million-medical-radiological-images-exposed-on-the-internet/

An analysis of medical image storage systems exposed to the public web reveals that almost 600 servers in 52 countries are completely unprotected against unauthorized access.

Audited systems were unpatched against thousands of vulnerabilities, more than 500 of them having the highest severity score.

Click link above to read more

2020 campaigns get Trump administration help on cybersecurity, counterintelligence

https://www.nbcnews.com/politics/2020-election/2020-campaigns-get-trump-administration-help-cybersecurity-counterintelligence-n1057366

WASHINGTON — Perched behind government computers at a site in Northern Virginia, hacking experts are scanning the networks of Democratic presidential campaigns, searching for vulnerabilities and openings to inject malicious code. For weeks at a time, they're hitting campaign officials with phishing emails not unlike those that Russian hackers used to infiltrate the Democratic National Committee in 2016.

Click link above to read more

Payment card thieves hack Click2Gov bill paying portals in 8 cities

https://arstechnica.com/information-technology/2019/09/payment-card-thieves-hack-click2gov-bill-paying-portals-in-8-cities/

In 2017 and 2018, hackers compromised systems running the Click2Gov self-service bill-payment portal in dozens of cities across the United States, a feat that compromised 300,000 payment cards and generated nearly $2 million of revenue. Now, Click2Gov systems have been hit by a second wave of attacks that's dumping tens of thousands of records onto the Dark Web, researchers said on Thursday.

Click link above to read more

Ring Provided a Map of Its Customers to Police

https://www.extremetech.com/internet/298031-ring-provided-a-map-of-its-customers-to-police

Ring was one of the first companies to make video doorbells and has since expanded to other home security products. As part of its aggressive strategy after the Amazon acquisition, Ring has partnered with hundreds of police departments across the US. This program has proven controversial, and it becomes more so with each new report. According to a new leak, Ring's pitch to police sometimes includes a map of active Ring customers, something it previously said it would not do.

Click link above to read more

A report from a former NSA operative says countries across the world are still adjusting to the new reality of sophisticated cyberwarfare.

https://www.techrepublic.com/article/governments-still-struggling-to-contend-with-weaponized-social-media-platforms/?ftag=CMG-01-10aaa1b

Since the 2016 US Presidential Election, social media platforms have been more proactive about addressing security gaps and stopping the kind of state-run psychological operations that were endemic over the last decade.

Despite their efforts to focus on security, experts say these kinds of digital psychological operations by governments are evolving in ways that will require sophisticated, multi-pronged security efforts.

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.

Security News Digest
Information Security Branch

BRITISH COLUMBIA OCIO Office of the Chief Information Officer