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

July 28th, 2020

Try our July - ‘Back to Basics’ Quiz

This week’s stories:

- **Canadian story publishing site acknowledges improper access to users’ personal information🇨🇦**
- **Russian group targeted COVID-19 vaccine research in Canada, U.S. and U.K., say intelligence agencies🇨🇦**
- **Garmin confirms ransomware attack, services coming back online**
- **Source code from big-name companies leaked online**
- **New ‘Meow’ attack has deleted almost 4,000 unsecured databases**
- **Twitter hackers read private messages of 36 high-profile accounts**
- **Researchers Warn of High-Severity Dell PowerEdge Server Flaw**
- **Thieves Are Emptying ATMs Using a New Form of Jackpotting**
- **US Offers $2mn Bounty For Ukrainian SEC Hackers**

Canadian story publishing site acknowledges improper access to users’ personal information🇨🇦

https://www.itworldcanada.com/article/canadian-story-publishing-site-acknowledges-improper-access-to-users-personal-information/433464

A Toronto-based story publishing site says someone may have “improperly accessed” personal information about its users, including their email addresses and dates of birth.

The statement made Monday by Wattpad Corp. was an update on the breach of security controls first announced July 14. At that time it said no financial information, private messages or phone numbers were accessed.

But the update gave more detail about the information that was gained. Some of it could be used for phishing and impersonation, and the person who accessed the data could have seen or copied the following.

Click link above to read more

Russian group targeted COVID-19 vaccine research in Canada, U.S. and U.K., say intelligence agencies🇨🇦

https://www.cbc.ca/news/politics/tunney-russia-alleged-attack-vaccine-canada-us-uk-1.5651697

A hacker group "almost certainly" backed by Russia is trying to steal COVID-19-related vaccine research in Canada, the U.K. and the U.S., according to intelligence agencies in all three countries.

The Communications Security Establishment (CSE), responsible for Canada's foreign signals intelligence, said APT29 — also known as Cozy Bear and the Dukes — is behind the malicious activity.

The group was accused of hacking the Democratic National Committee before the 2016 U.S. election.

APT29 "almost certainly operates as part of Russian intelligence services," the CSE said in a statement released Thursday morning in co-ordination with its international counterparts — an allegation the Kremlin immediately denied.

Click link above to read more

Garmin confirms ransomware attack, services coming back online

https://www.bleepingcomputer.com/news/security/garmin-confirms-ransomware-attack-services-coming-back-online/

Garmin has officially confirmed that they were victims of a ransomware attack as they slowly bring their Garmin Connect, Strava, and navigation services back online.

Last week, Garmin suffered a worldwide outage that affected their Garmin Connect, Strava, inReach, and flyGarmin navigation and fitness services.

Click link above to read more

Source code from big-name companies leaked online

https://www.itworldcanada.com/article/source-code-from-big-name-companies-leaked-online/433690

Several big-name companies haven’t been putting enough protection around some of their source code, according to news reports.

According to Bleeping Computer, a security researcher called Tillie Kottmann has assembled a GitLab repository of source code from dozens of companies including Microsoft, Adobe, Lenovo, AMD, Qualcomm, Motorola, Hisilicon (owned by Huawei), Mediatek, GE Appliances, Nintendo, Roblox, Disney and Johnson Controls because of misconfigurations in their infrastructure.

Click link above to read more

New ‘Meow’ attack has deleted almost 4,000 unsecured databases

https://www.bleepingcomputer.com/news/security/new-meow-attack-has-deleted-almost-4-000-unsecured-databases/

Hundreds of unsecured databases exposed on the public web are the target of an automated 'meow' attack that destroys data without any explanation.

The activity started recently by hitting Elasticsearch and MongoDB instances without leaving any explanation, or even a ransom note. Attacks then expanded to other database types and to file systems open on the web.

A quick search by BleepingComputer on the IoT search engine Shodan initially found dozens of databases that have been affected by this attack. Recently, the number of wiped databases increased to over 1,800.

Click link above to read more

Twitter hackers read private messages of 36 high-profile accounts

https://www.bleepingcomputer.com/news/security/twitter-hackers-read-private-messages-of-36-high-profile-accounts/

Twitter today admitted that the attackers behind last week's incident read the private messages of 36 out of a total of 130 high-profile accounts targeted in the attack.

Among these, the hackers also accessed the Twitter inbox of Geert Wilders, a Dutch elected official and the leader of the Party for Freedom (PVV).

Click link above to read more

Researchers Warn of High-Severity Dell PowerEdge Server Flaw

https://threatpost.com/researchers-warn-of-high-severity-dell-poweredge-server-flaw/157795/

A path traversal vulnerability in the iDRAC technology can allow remote attackers to take over control of server operations.

Researchers have disclosed details of a recently patched, high-severity Dell PowerEdge server flaw, which if exploited could allow an attacker to fully take over and control server operations.

The web vulnerability was found in the Dell EMC iDRAC remote access controller, technology embedded within the latest versions of Dell PowerEdge servers. While the vulnerability was fixed earlier in July, Georgy Kiguradze and Mark Ermolov, the researchers with Positive Technologies who discovered the flaw, published a detailed analysis, Tuesday.

Click link above to read more

Thieves Are Emptying ATMs Using a New Form of Jackpotting

https://www.wired.com/story/thieves-are-emptying-atms-using-a-new-form-of-jackpotting/

The new hardware-based attack, which has targeted machines across Europe, can yield a stream of cash for the attacker.Diebold Nixdorf, which made $3.3 billion from ATM sales and service last year, is warning stores, banks, and other customers of a new hardware-based form of “jackpotting,” the industry term for attacks that thieves use to quickly empty ATMs.

The new variation uses a device that runs parts of the company’s proprietary software stack. Attackers then connect the device to the ATM internals and issue commands. Successful attacks can result in a stream of cash, sometimes dispensed as fast as 40 bills every 23 seconds. The devices are attached either by gaining access to a key that unlocks the ATM chassis or by drilling holes or otherwise breaking the physical locks to gain access to the machine internals.

Click link above to read more

US Offers $2mn Bounty For Ukrainian SEC Hackers

https://www.barrons.com/news/us-offers-2mn-bounty-for-ukrainian-sec-hackers-01595427006?tesla=y

The US State Department and Secret Service offered $2 million in reward money Wednesday for help capturing two Ukrainians charged with hacking and selling valuable insider corporate information from the Securities and Exchange Commission.

The agencies offered a bounty of $1 million each for information leading to the arrest and/or conviction of Artem Viacheslavovich Radchenko and Oleksandr Vitalyevich Ieremenko on charges of international cybercrime.

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:

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