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

September 7, 2021

Challenge yourself with our ABCs of Cyber Security quiz!

This week's stories:

🍁 **New hacking group emerges, claims two Canadian victims**

Twitter tests safety mode feature to silence abuse

WhatsApp photo filter bug could have exposed your data to remote attackers

Around 1 million people potentially affected by suspected breach in Indonesia's COVID-19 app: report

Microsoft warns of credential phishing attack abusing open redirect links

T-Mobile data breach and SIM-swap scam: How to protect your identity

Traffic exchange networks distributing malware disguised as cracked software

9 notable government security initiatives of 2021

Free car, load of cash among schemes as phishing scams explode, report says

Criminal's wish list: Who's their ideal ransomware victim?

Translated ransomware playbook gives rare insight into gang's operation

---

New hacking group emerges, claims two Canadian victims

A new criminal hacking group has appeared, claiming to have stolen data from firms in a number of countries including Canada and the U.S.

CoomingProject alleges its Canadian victims are a horse-breeding association and a women's fashionware business. The U.S. site appears to be a work in progress for reading Japanese Manga graphic comics.

https://www.itworldcanada.com/article/new-hacking-group-emerges-claims-two-canadian-victims/457918

Click above link to read more.

Back to top

Twitter tests safety mode feature to silence abuse

Twitter is launching a feature that it hopes will help crack down on abuse and trolling, both of which have become huge issues for the platform.

Safety Mode will flag accounts using hateful remarks, or those bombarding people with uninvited comments, and block them for seven days.

The feature will work automatically once enabled, taking the burden off users to deal with unwelcome tweets.

https://www.bbc.com/news/technology-58408781

Click above link to read more.

Back to top

WhatsApp photo filter bug could have exposed your data to remote attackers

A now-patched high-severity security vulnerability in WhatApp's image filter feature could have been abused to send a malicious image over the messaging app to read sensitive information from the app's memory.

Tracked as CVE-2020-1910 (CVSS score: 7.8), the flaw concerns an out-of-bounds read/write and stems from applying specific image filters to a rogue image and sending the altered image to an unwitting recipient, thereby enabling an attacker to access valuable data stored the app's memory.

https://thehackernews.com/2021/09/whatsapp-photo-filter-bug-could-have.html

Click above link to read more.

Back to top

Around 1 million people potentially affected by suspected breach in Indonesia's COVID-19 app: report

An independent report has revealed a data breach in the Indonesian government's COVID-19 test-and-trace mobile app, potentially affecting records of around 1.3 million users.

Launched this year, the electronic Health Alert Card (eHAC) is a mandatory requirement for travellers entering Indonesia. It stores users' health status, personal data, contact details, COVID-19 test results, among others.

https://www.healthcareitnews.com/news/asia/around-1-million-people-potentially-affected-suspected-breach-indonesias-covid-19-app

Click above link to read more.

Back to top

Microsoft warns of credential phishing attack abusing open redirect links

Microsoft has warned about a new widespread phishing campaign in which scammers are abusing open redirect links to divert users to malicious websites and steal MS Office 365 credentials.

In a detailed report, the IT security researchers at Microsoft wrote that this campaign is widespread but didn’t clarify the number of attacks they detected. It is suspected that some phishing emails sent in this campaign had January dates, while researchers claim the campaign is still active.

https://www.hackread.com/microsoft-credential-phishing-attack-open-redirect-links/

Click above link to read more.

Back to top

T-Mobile data breach and SIM-swap scam: How to protect your identity

Just when you think the massive T-Mobile hack can't get any worse, on Friday the carrier announced that over 50 million people, including current and former customers as well as prepaid customers, were affected by the breach. Information like Social Security numbers, driver's licenses and account PINs were exposed. Here are some steps you can take right now to protect your financial information.

Regardless whether you're a T-Mobile user, the exposure of account PINs is a major danger. That's the password that you're asked to give to a T-Mobile employee before any changes can be made to your account. A scammer who knows your account password can call customer care and ask to have the SIM card linked to your phone number changed to a new SIM card and device, effectively taking over your phone number. If you've moved on from T-Mobile to another carrier and used the same passcode, you should change it immediately.

https://www.cnet.com/tech/mobile/t-mobile-data-breach-and-sim-swap-scam-how-to-protect-your-identity/

Click above link to read more.

Back to top

Traffic exchange networks distributing malware disguised as cracked software

An ongoing campaign has been found to leverage a network of websites acting as a "dropper as a service" to deliver a bundle of malware payloads to victims looking for "cracked" versions of popular business and consumer applications.

"These malware included an assortment of click fraud bots, other information stealers, and even ransomware," researchers from cybersecurity firm Sophos said in a report published last week.

https://thehackernews.com/2021/09/traffic-exchange-networks-distributing.html

Click above link to read more.

Back to top

---

9 notable government security initiatives of 2021

Cybersecurity has steadily crept up the agenda of governments across the globe. This has led to initiatives designed to address cybersecurity issues that threaten individuals and organizations.

“Government-led cybersecurity initiatives are critical to addressing cybersecurity issues such as destructive attacks, massive data breaches, poor security posture, and attacks on critical infrastructure,” Steve Turner, security and risk analyst at Forrester, tells CSO. “These initiatives provide consistent guidance on how organizations and consumers can protect themselves, provide services to companies that don’t have the knowledge or monetary means to protect themselves, legislative levers that can be utilized, means of taking offensive actions against nation state adversaries, and most of all investigation of significant cyber incidents paired with critical information sharing during or after those incidents.”

https://www.csoonline.com/article/3630632/9-notable-government-cybersecurity-initiatives-of-2021.html

Click above link to read more.

Back to top

Free car, load of cash among schemes as phishing scams explode, reports say

There’s been a dramatic increase in scams during the past year where con artists send out emails and texts hoping to reel in victims. It’s called phishing.

Now there’s a warning about one phishing scam that uses a new car and promises of free cash to reel you in. The scam is pretty blatant about what it wants from you if you know what to look for.

Who wouldn’t want a new car and a load of cash to boot?

https://www.wnct.com/on-your-side/consumer-watch/free-car-load-of-cash-among-schemes-as-phishing-scams-explode-report-says/

Click above link to read more.

Back to top

Criminal’s wish list: Who’s their ideal ransomware victim?

The most sought-after type of victim for ransomware-wielding attackers is a large, U.S.-based business with at least $100 million in revenue, not operating in the healthcare or education sector, for which remote access is available via remote desktop protocol or VPN credentials.

So says Israeli threat intelligence firm Kela in a new report, rounding up dozens of active discussion threads it tracked on cybercrime forums during July that were devoted to buying initial access to networks. About half of the threads it found had been created the same month, suggesting that the market for supplying such access continues to thrive, it says.

https://www.bankinfosecurity.com/blogs/criminals-wish-list-whos-their-ideal-ransomware-victim-p-3110

Click above link to read more.

Back to top

Translated ransomware playbook gives rare insight into gang’s operation

A leak of a purported tutorial from the Conti ransomware gang for turning compromised machines into ransomware beachheads provides a rare look inside the operations of a popular cybercriminal syndicate and highlights the tenuous relationships between groups in the cybercriminal ecosystem.

Threat experts at Cisco Talos this week provided a full English translation of the playbook, which came to light last month, allegedly after a disgruntled "affiliate" leaked the location of the server controlling compromised machines and more than 100MB of tools and documents. The playbook focuses on a number of popular tools — such as Cobalt Strike, Mimikatz, and PowerShell — and tells affiliates, low-level cybercriminals who infect systems for a cut of the profits, how to find exploits for common vulnerabilities.

https://www.darkreading.com/attacks-breaches/translated-ransomware-playbook-gives-insight-into-gang-operations

Click above link to read more.

Back to top

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