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

March 10th, 2020

Try our March Quiz – Protecting Mobile Devices

This week's stories:

- Canada's cyber intelligence agency working on 'Holy Grail' of encryption 🇨🇦
- Canada, allies must scrutinize military equipment for cyber weaknesses: experts say 🇨🇦
- Android security alert: 1 billion devices will no longer get updates
- Brave to generate random browser fingerprints to preserve user privacy
- Multiple nation-state groups are hacking Microsoft Exchange servers
- Zoho zero-day published on Twitter
- Microsoft: 99.9% of compromised accounts did not use multi-factor authentication
- Next-Gen Ransomware Packs a 'Human' Punch, Microsoft Warns
- Researchers Expose New, Hidden Techniques to Target Mobile and Gaming Users Worldwide

Canada's cyber intelligence agency working on 'Holy Grail' of encryption 🇨🇦

https://www.cbc.ca/news/politics/cse-homomorphic-encryption-1.5468400

Canada's cyber intelligence agency says it's working on what it calls the "Holy Grail" of data encryption to protect government information as the number of reports of privacy breaches, malware attempts and ransomware hits continues to grow.

Encryption mainly works in transit — which protects data when it's being sent — or "at rest", which guards information when it's being stored. But in order to be processed and understood, that information needs to be decrypted, potentially putting it at risk.

Click link above to read more

Canada, allies must scrutinize military equipment for cyber weaknesses: experts say 🇨🇦

https://globalnews.ca/news/6636756/cyber-security-military-equipment/

A top U.S. Defense Department official says her country is working on cyber weaknesses in its vast array of military equipment and will shut down anything that isn't brought up to standards.

The comments on Thursday by Ellen Lord, the U.S. undersecretary of defense for acquisition and sustainment, raise the question of what Canada is doing to protect its own military equipment from cyberattacks.

Click link above to read more

Android security alert: 1 billion devices will no longer get updates

https://cntechpost.com/2020/03/09/1-billion-android-devices-will-no-longer-get-updates/

If you are still running Android 6.0 or earlier, you are vulnerable to malware. Currently, more than one billion Android devices worldwide are no longer supported by security updates, and they are all very vulnerable.

According to the policy in Android Security Bulletins, no security patches for Android systems below 7.0 (Nougat) have been released in 2019.

This means that more than 1 billion phones and tablets are active worldwide but will no longer receive security updates.

Click link above to read more

Brave to generate random browser fingerprints to preserve user privacy

https://www.zdnet.com/article/brave-to-generate-random-browser-fingerprints-to-preserve-user-privacy/

"Brave's new approach aims to make every browser look completely unique, both between websites and between browsing sessions."

The Brave browser is working on a feature that will randomize its "fingerprint" every time a user visits a website in an attempt to preserve the user's privacy.

Brave's decision comes as online advertisers and analytics firms are moving away from tracking users via cookies to using fingerprints.

Click link above to read more

Multiple nation-state groups are hacking Microsoft Exchange servers

https://www.zdnet.com/article/multiple-nation-state-groups-are-hacking-microsoft-exchange-servers/

Multiple government-backed hacking groups are exploiting a recently-patched vulnerability in Microsoft Exchange email servers.

The exploitation attempts were first spotted by UK cyber-security firm Volexity on Friday and confirmed today to ZDNet by a source in the DOD.

Volexity did not share the names of the hacking groups exploiting this Exchange vulnerability. Volexity did not return a request for comment for additional details.

Click link above to read more

Zoho zero-day published on Twitter

https://www.zdnet.com/article/zoho-zero-day-published-on-twitter/

A security researcher published yesterday details on Twitter about a zero-day vulnerability in a Zoho enterprise product.

Cyber-security experts who have reviewed the vulnerability have told *ZDNet* that the zero-day could spell trouble for companies around the world, as it could be an entry point for ransomware gangs to infect corporate networks and ransom their data.

The vulnerability impacts the Zoho ManageEngine Desktop Central. According to the Zoho website, this is an endpoint management solution. Companies use the product to control their fleets of devices -- such as Android smartphones, Linux servers, or Mac and Windows workstations.

Click link above to read more

Microsoft: 99.9% of compromised accounts did not use multi-factor authentication

https://www.msn.com/en-us/finance/other/microsoft-999-25-of-compromised-accounts-did-not-use-multi-factor-authentication/ar-BB10OHBA

Speaking at the RSA security conference last week, Microsoft engineers said that 99.9% of the compromised accounts they track every month don't use multi-factor authentication, a solution that stops most automated account attacks.

The cloud giant said it tracks more than 30 billion login events per day and more than one billion monthly active users.

Click link above to read more

Next-Gen Ransomware Packs a 'Human' Punch, Microsoft Warns

https://threatpost.com/next-gen-ransomware-packs-a-human-punch-microsoft-warns/153501/

Ryuk, DoppelPaymer, Parinacota and other ransomware groups are getting more sophisticated, Microsoft warns.

Researchers are warning that "human operated" ransomware campaigns are growing more sophisticated, adopting new infection tactics and lateral movement techniques that traditional defense teams aren't equipped to handle.

Click link above to read more

Researchers Expose New, Hidden Techniques to Target Mobile and Gaming Users Worldwide

https://cyware.com/news/researchers-expose-new-hidden-techniques-to-target-mobile-and-gaming-users-worldwide-bbda1fc5m

- It was found that hackers use popular gamer chat apps and cheat videos as bait.
- Attackers would hide by hacking the original developer's Google Play account.

A computer security firm reported that modern hackers are using hidden mobile apps, third-party login, and counterfeit gaming videos as bait to target potential victims.

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.