Security News Digest
Information Security Branch

BRITISH COLUMBIA OCIO | Office of the Chief Information Officer

October 20th, 2020

Challenge yourself during Cyber Security Awareness Month

Try our October - 'Cyber Security Awareness Month' Quiz

This week's stories:

- **Waze Vulnerability Lets Attackers Track and Identify Users**
- **Barnes & Noble hit by Egregor ransomware, strange data leaked**
- **Darkside ransomware donates $20K of extortion money to charities**
- **Hackers Claim to Have Access to 50,000 Home Security Cameras**
- **Six Russian military officers indicted by U.S. grand jury for huge cyber attacks**
- **Software AG Hit by Data-Stealing Ransomware Attack**
- **Twitter slammed by U.S. regulator over bitcoin scam**

Waze Vulnerability Lets Attackers Track and Identify Users

https://www.infosecurity-magazine.com/news/waze-vulnerability-identifies-users/

A vulnerability has been discovered in Google's GPS navigation software app Waze that lets hackers identify and track users.

Autoevolution.com reports that the flaw was discovered by security engineer Peter Gasper. When using the app's web interface, Gasper discovered that he could request the Waze API to display not only his coordinates, but also those of other drivers traveling nearby.

Click link above to read more

Barnes & Noble hit by Egregor ransomware, strange data leaked

https://www.bleepingcomputer.com/news/security/barnes-and-noble-hit-by-egregor-ransomware-strange-data-leaked/

The Egregor ransomware gang is claiming responsibility for the cyberattack on U.S. Bookstore giant Barnes & Noble on October 10th, 2020. The attackers state that they stole unencrypted files as part of the attack.

Barnes & Noble is the largest brick-and-mortar bookseller in the United States, with over 600 bookstores in fifty states. The bookseller also operated the Nook Digital, which is their eBook and e-Reader platform.

Click link above to read more

Darkside ransomware donates $20K of extortion money to charities

https://www.bleepingcomputer.com/news/security/darkside-ransomware-donates-20k-of-extortion-money-to-charities/

The operators of Darkside ransomware have donated some of the money they made extorting victims to non-profits Children International and The Water Project.

They explain this Robin Hood move as an effort to make the world a better place and plan to make more donations in the future, but anonymously.

Click link above to read more

Hackers Claim to Have Access to 50,000 Home Security Cameras

https://www.infosecurity-magazine.com/news/hackers-access-50000-home-security

A hacking group is selling access to more than 50,000 hacked home security cameras, including footage of children in various states of undress, it has emerged.

The group, which has over 1000 global members, has been using messaging platform Discord to advertise its wares, according to a report on AsiaOne.

Click link above to read more

Six Russian military officers indicted by U.S. grand jury for huge cyber attacks

https://www.itworldcanada.com/article/six-russian-military-officers-indicted-by-u-s-grand-jury-for-huge-cyber-attacks/437264

Six members of Russia’s military intelligence unit have been accused of being behind some of the biggest known cyberattacks, including the NotPetya wiper, which caused over $1 billion in losses around the world, and malware that twice knocked out power to large parts of Ukraine.

The U.S. Justice Department said Monday that a federal grand jury in Pittsburg returned an indictment accusing the hackers and their co-conspirators of conspiracy, computer hacking, wire fraud, aggravated identity theft, and false registration of a domain name.

Click link above to read more

Software AG Hit by Data-Stealing Ransomware Attack

https://www.infosecurity-magazine.com/news/software-ag-datastealing

A major German enterprise software company has become the latest tech name to suffer a likely ransomware attack featuring information theft.

IoT specialist Software AG, which claims to have over 10,000 customers and annual revenue exceeding €800m, revealed the news in a brief update late last week.

Click link above to read more

Twitter slammed by U.S. regulator over bitcoin scam

https://www.itworldcanada.com/article/twitter-slammed-by-u-s-regulator-over-bitcoin-scam/437278

A New York state regulator has slammed Twitter for poor cybersecurity protection that allowed young hackers to seize control of several celebrities’ accounts in July to run a “double your bitcoin” scam.

“Given that Twitter is a publicly-traded, US$37 billion technology company, it was surprising how easily the hackers were able to penetrate Twitter’s network and gain access to internal tools allowing them to take over any Twitter user’s account,” said the report by the Department of Financial Services.

Click link above to read more

Click Unsubscribe to stop receiving the Digest.

****

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

Security News Digest
Information Security Branch

BRITISH COLUMBIA OCIO | Office of the Chief Information Officer