December 10th, 2019

Try our December quiz – Shopping Safety

Save the date - February 5th to 7th is the Privacy and Security Conference

This week's stories:

- **Tech companies are beyond government control, Edward Snowden tells Ontario college administrators**
- **Canada's cyber intelligence agency is helping the U.K. protect its election**
- **University of Ottawa to open cybersecurity research hub**
- **International crackdown on RAT spyware which takes total control of victims' PCs**
- **Millions of text messages from bulk service provider found open on the internet**
- **'Evil Corp': Feds charge Russians in massive $100 million bank hacking scheme**
- **The Great Cannon DDoS Tool Used Against Hong Kong Protestors' Forum**
- **Moscow Cops Sell Access to City CCTV, Facial Recognition Data**
- **These browsers actually protect your privacy**
- **University of Birmingham Finds Weakness in Intel's Processors**

Tech companies are beyond government control, Edward Snowden tells Ontario college administrators

https://www.itworldcanada.com/article/tech-companies-are-beyond-government-control-edward-snowden-tells-ontario-college-administrators/424673

Surveillance whistleblower Edward Snowden attacked global companies that collect large amounts of personal data for intruding on privacy, complaining they are beyond the control of most governments.

In a keynote address Monday to the annual Colleges Ontario conference for administrators via video feed from Moscow, where he has been forced to live since revealing in 2013 how Western governments had been scooping up masses of data on unsuspecting people, Snowden said not much has changed.

Click link above to read more

Canada's cyber intelligence agency is helping the U.K. protect its election

https://www.cbc.ca/news/politics/cse-uk-election-1.5385818

Canada's foreign signals intelligence agency is on the lookout for threats to Britain's election as the country heads into the final week of campaigning.

Communications Security Establishment spokesperson Evan Koronewski said the agency regularly shares information with its international allies "that has a significant impact on protecting our respective countries' safety and security."

Click link above to read more

University of Ottawa to open cybersecurity research hub

https://www.itworldcanada.com/article/university-of-ottawa-to-open-cybersecurity-research-hub/424802

The University of Ottawa will soon open what it calls a hub for research in cybersecurity and cyber safety, with IBM Canada as the first of what is expected to be several industry partners.

The two sides said this week that the hub — it doesn't have a physical space yet on campus — will officially open in the spring.

Click link above to read more

International crackdown on RAT spyware which takes total control of victims' PCs

https://www.europol.europa.eu/newsroom/news/international-crackdown-rat-spyware-which-takes-total-control-of-victims%E2%80%99-pcs

"A hacking tool that was able to give full remote control of a victim's computer to cybercriminals has been taken down as a result of an international law enforcement operation targeting the sellers and users of the Imminent Monitor Remote Access Trojan (IM-RAT).
The investigation, led by the Australian Federal Police (AFP), with international activity coordinated by Europol and Eurojust, resulted in an operation involving numerous judicial and law enforcement agencies in Europe, Colombia and Australia.

Coordinated law enforcement activity has now ended the availability of this tool, which was used across 124 countries and sold to more than 14 500 buyers. IM-RAT can no longer be used by those who bought it."

Click link above to read more

Millions of text messages from bulk service provider found open on the internet

https://www.itworldcanada.com/article/millions-of-text-messages-from-bulk-service-provider-found-open-on-the-internet/424640

Businesses and educational institutions around the world that use the TrueDialog SMS bulk texting service are scrambling to assess the potential damage to their communications after news that security researchers discovered a huge database of unprotected messages from the Texas-based provider.

Researchers at vpnMonitor, a news site that reviews VPN solutions, said Sunday that as part of an ongoing project to discover unprotected databases on the internet they found one belonging to TrueDialog, a cloud-based provider of mass texting solutions used by companies and colleges. Not only were customer messages open, so were texts of TrueDialog employees.

Click link above to read more

'Evil Corp': Feds charge Russians in massive $100 million bank hacking scheme

https://www.cnbc.com/2019/12/05/russian-malware-hackers-charged-in-massive-100-million-bank-scheme.html

The U.S. Justice and Treasury departments took action Thursday against a Russian hacking group known as “Evil Corp.,” which stole “at least” $100 million from banks using malicious software that swiped banking credentials, according to a joint press release.

“Evil Corp.,” a name reminiscent of the nickname for the key malevolent corporation in the popular television drama “Mr. Robot,” is “run by a group of individuals based in Moscow, Russia, who have years of experience and well-developed, trusted relationships with each other,” according to a Treasury Department press release.

Click link above to read more

The Great Cannon DDoS Tool Used Against Hong Kong Protestors’ Forum

https://www.bleepingcomputer.com/news/security/the-great-cannon-ddos-tool-used-against-hong-kong-protestors-forum/

The Great Cannon Distributed Denial of Service (DDoS) tool was deployed again to launch attacks against the LIHKG social media platform used by Hong Kong protesters to coordinate during this year's anti-extradition protests.

Attackers use the Great Cannon to consume the resources of a targeted website outside the Great Firewall of China (GFW) with superfluous web traffic coming from Chinese users who had their insecure HTTP connections injected with malicious JavaScript code when visiting insecure sites.

Click link above to read more

Moscow Cops Sell Access to City CCTV, Facial Recognition Data

https://www.bleepingcomputer.com/news/security/moscow-cops-sell-access-to-city-cctv-facial-recognition-data/

Anyone with a little money can buy access to Moscow's surveillance system of tens of thousands of cameras along and check footage stored over the previous five days.

Sellers on forums and messenger groups that trade illegal data also provide facial recognition lookup services.

Click link above to read more

These browsers actually protect your privacy

https://securityboulevard.com/2019/12/these-browsers-actually-protect-your-privacy/

Your web browser is the vehicle that carries you around the Internet to your desired websites. As such, it knows precisely what sites you have visited, how long you spent browsing them, and what you clicked on (or almost clicked on). Anyone who has access to your web browser can have a window into your income, your political leanings, and even your sexual preferences.

This is why it’s so important to only use browsers you know will protect and improve your internet privacy. In this article, we explain how browsers capture so much information and which web browsers in 2019 are best at keeping your browsing history safe from data-hungry tech companies and advertisers.

Click link above to read more

University of Birmingham Finds Weakness in Intel’s Processors

https://www.securitymagazine.com/articles/91390-university-of-birmingham-find-weakness-in-intels-processors

Researchers at the University of Birmingham say that they have identified a weakness in Intel's processors: by undervolting the CPU, Intel's secure enclave technology reportedly becomes vulnerable to attack.

"Modern processors are being pushed to perform faster than ever before – and with this comes increases in heat and power consumption. To manage this, many chip manufacturers allow frequency and voltage to be adjusted as and when needed – known as 'undervolting' or 'overvolting'. This is done through privileged software interfaces, such as a "model-specific register" in Intel Core processors," says the University of Birmingham.

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:

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