






September 29th, 2020
Try our September - 'Passwords' Quiz

This week's stories:

- [Canadian cybersecurity poll finds 84 per cent rethink doing businesses hit by data breach](#) 
- [Leaders must do more to reassure Canadians on COVID Alert app, says tech lawyer](#) 
- ['Netwalker' ransomware attacks pose challenge for businesses, organizations in Canada](#) 
- ["Joker"—the malware that signs you up for pricey services—floods Android markets](#)
- [CISA warns of notable increase in LokiBot malware](#)
- [APT28 Delivers Zebrocy Malware Campaign using NATO Theme as Lure](#)
- [eBay Execs to Plead Guilty to Cyber-Stalking](#)
- [Microsoft: Ransomware & Nation-State Attacks Rise, Get More Sophisticated](#)
- ['ZeroLogon' hackers scan for unpatched servers](#)
- [Ring's latest security camera is a drone that flies around inside your house](#)

Canadian cybersecurity poll finds 84 per cent rethink doing businesses hit by data breach 

<https://www.ctvnews.ca/business/canadian-cybersecurity-poll-finds-84-per-cent-rethink-doing-businesses-hit-by-data-breach-1.5122991>

TORONTO -- A large majority of Canadians are reluctant to do business with companies that suffer a data breach, according to a new study released Monday by KPMG.

The report also says about one-quarter of the people surveyed for the report have had their login credentials stolen from a trusted site.

[Click link above to read more](#)

Leaders must do more to reassure Canadians on COVID Alert app, says tech lawyer 

<https://www.itworldcanada.com/article/leaders-must-do-more-to-reassure-canadians-on-covid-alert-app-says-tech-lawyer/436288>

The country's leaders must do more to convince skeptical Canadians that the national COVID Alert app protects their privacy and is worth downloading, says a leading technology lawyer.

“Even the very best of apps — and we have a good one in Canada — won’t achieve the level of success we need unless there is a vigorous effort to make sure people are aware of it and as many as people as possible install it,” Michael Geist, Canada Research Chair in Internet and E-Commerce Law at the University of Ottawa, told an online panel discussion on COVID apps Sept. 25.

[Click link above to read more](#)

‘Netwalker’ ransomware attacks pose challenge for businesses, organizations in Canada

<https://globalnews.ca/news/7362769/netwalker-ransomware-attacks-canada/>

TORONTO — A shadowy group of cyber criminals that attacked a prominent nursing organization and Canadian Tire store has successfully targeted other companies with clients in governments, health care, insurance and other sectors.

Posts on their NetWalker “blog” indicate the recent infiltration of cloud-services company Accreon and document company Xpertdoc, although only the College of Nurses of Ontario has publicly acknowledged being victimized.

[Click link above to read more](#)

“Joker”—the malware that signs you up for pricey services—floods Android markets

<https://arstechnica.com/information-technology/2020/09/joker-the-malware-that-signs-you-up-for-pricey-services-floods-android-markets/>

September has been a busy month for malicious Android apps, with dozens of them from a single malware family alone flooding either Google Play or third-party markets, researchers from security companies said.

[Click link above to read more](#)

CISA warns of notable increase in LokiBot malware

<https://www.securityweek.com/cisa-warns-increased-use-lokibot-malware>

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) is warning of a significant increase in the use of LokiBot malware over the past couple of months.

Initially detailed in 2016 as a piece of malware targeting Android devices, LokiBot arrived on Windows in 2018 and has evolved into a prevalent threat, targeting corporate mailboxes and employing innovative distribution methods.

[Click link above to read more](#)

APT28 Delivers Zebrocy Malware Campaign using NATO Theme as Lure

<https://quointelligence.eu/2020/09/apt28-zebrocy-malware-campaign-nato-theme/>

On 9 August, QuoIntelligence disseminated a Warning to its government customers about a new APT28 (aka Sofacy, Sednit, Fancy Bear, STRONTIUM, etc.) campaign targeting government bodies of NATO members (or countries cooperating with NATO). In particular, we found a malicious file uploaded to VirusTotal, which ultimately drops a Zebrocy malware and communicates with a C2 in France. After our discovery, we reported the malicious C2 to the French law enforcement as part of our responsible disclosure process.

[*Click link above to read more*](#)

eBay Execs to Plead Guilty to Cyber-Stalking

<https://www.infosecurity-magazine.com/news/ebay-execs-to-plead-guilty-to/>

Four former eBay executives accused of cyber-stalking and intimidating a Massachusetts couple are to admit their guilt before a court next month.

The married couple, an editor and a publisher residing in Natick, were targeted with a series of terrifying deliveries after they criticized eBay in an online newsletter.

Horrific parcels sent to the couple included a bloody pig mask, live spiders and cockroaches, a book on surviving the death of a spouse, and a wreath of funeral flowers. In addition, pornographic magazines addressed to the husband were received by one of the couple's neighbors.

[*Click link above to read more*](#)

Microsoft: Ransomware & Nation-State Attacks Rise, Get More Sophisticated

<https://www.darkreading.com/threat-intelligence/microsoft-ransomware-and-nation-state-attacks-rise-get-more-sophisticated/d/d-id/1339037>

Attackers continue to improve their tactics and tools, demonstrating growing sophistication, including the creation of one-off web addresses to foil blocklists, a jump in ransomware infections, a focus on reconnaissance and credential harvesting, and an uptick in targeting connected devices, according to Microsoft's annual "Digital Defense Report," published on Sept. 29.

[*Click link above to read more*](#)

'ZeroLogon' hackers scan for unpatched servers

<https://www.itnews.com.au/news/zerologon-hackers-scan-for-unpatched-servers-553942>

Unknown attackers are scanning the internet and attempting to exploit the "ZeroLogon" privilege escalation bug in Microsoft's Netlogon Remote Control Protocol for Domain Controllers, which has a full 10.0 out of 10 severity rating on the Common Vulnerability Scoring System (CVSS).

Microsoft security researcher Kevin Beaumont noted over the weekend that someone had sent hundreds of login attempts that match the exploit chain for ZeroLogon.

[*Click link above to read more*](#)

Ring's latest security camera is a drone that flies around inside your house

<https://www.theverge.com/2020/9/24/21453709/ring-always-home-cam-indoor-drone-security-camera-price-specs-features-amazon>

Ring latest home security camera is taking flight — literally. The new Always Home Cam is an autonomous drone that can fly around inside your home to give you a perspective of any room you want when you're not home. Once it's done flying, the Always Home Cam returns to its dock to charge its battery. It is expected to cost \$249.99 when it starts shipping next year.

[*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.

