



December 1st, 2020

Try our December - [“Shopping Online” Quiz](#)

This week's stories:

- [Auditor general says N.S. slow to act on cybersecurity amid increasing risk](#) 
- [Home Depot to pay U.S. states \\$17.5 million for 2014 data breach](#)
- [Egregor RaaS Continues the Chaos with Cobalt Strike and Rclone](#)
- [FBI warns of BEC scammers using email auto-forwarding in attacks](#)
- [Android app still exposing messages of 100M users despite bug fix](#)
- [Ransomware Attack Targets Baltimore County Public Schools](#)
- [Fake VPN add-ons hit Microsoft Edge browser store](#)
- [Updated Trickbot Malware Is More Resilient](#)

Auditor general says N.S. slow to act on cybersecurity amid increasing risk 

<https://www.thestar.com/news/canada/2020/12/01/auditor-general-says-ns-slow-to-act-on-cybersecurity-amid-increasing-risk.html>

Nova Scotia's auditor general says the COVID-19 pandemic is highlighting the need for more robust cybersecurity and anti-fraud measures as government employees are forced to work remotely.

However, he says the provincial government isn't working fast enough to manage those risks.

Acting auditor general Terry Spicer notes in a report released today that the federal government's Canadian Centre for Cybersecurity has warned of an increase in attempts to access and attack networks used by remote workers.

[Click link above to read more](#)

Home Depot to pay U.S. states \$17.5 million for 2014 data breach

<https://www.itworldcanada.com/article/home-depot-to-pay-u-s-states-17-5-million-for-2014-data-breach/438785>

It's taken six years but a number of U.S. states have finally come to an agreement on financial penalties and other remedies against The Home Depot for a huge data breach in 2014.

Home Depot will have to pay 46 states and the District of Columbia \$17.5 million and implement a series of data security practices designed to strengthen its information security program and safeguard the personal information of consumers.

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

Egregor RaaS Continues the Chaos with Cobalt Strike and Rclone

<https://labs.sentinelone.com/egregor-raas-continues-the-chaos-with-cobalt-strike-and-rclone/>

Egregor ransomware is an offshoot of the Sekhmet malware family that has been active since mid-September 2020. The ransomware operates by compromising organizations, stealing sensitive user data, encrypting said data, and demanding a ransom to exchange encrypted documents. Egregor is ransomware associated with the cyberattacks against GEFCO and Barnes & Noble, Ubisoft, and numerous others.

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

FBI warns of BEC scammers using email auto-forwarding in attacks

<https://www.bleepingcomputer.com/news/security/fbi-warns-of-bec-scammers-using-email-auto-forwarding-in-attacks/>

The FBI is warning US companies about scammers actively abusing auto-forwarding rules on web-based email clients to increase the likelihood of successful Business Email Compromise (BEC) attacks.

This warning was issued through a joint Private Industry Notification (PIN) sent on November 25 and coordinated with DHS-CISA.

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

Android app still exposing messages of 100M users despite bug fix

<https://www.bleepingcomputer.com/news/security/android-app-still-exposing-messages-of-100m-users-despite-bug-fix/>

GO SMS Pro, an Android instant messaging app with more than 100 million installs, is still exposing the privately shared messages of millions of users even though the developer has been working on a fix for the flaw behind the data leak for almost two weeks.

The flaw, discovered by Trustwave researchers three months ago and publicly disclosed on November 19, enabled unauthenticated attackers to gain unrestricted access to voice messages, videos, and photos privately shared by GO SMS Pro users.

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

Ransomware Attack Targets Baltimore County Public Schools

<https://www.bankinfosecurity.com/ransomware-attack-targets-baltimore-county-public-schools-a-15467>

Officials with the Baltimore County Public Schools are investigating a ransomware attack that disrupted virtual learning for students on Wednesday. Now, the district has been forced to call-off its virtual classes until next Monday, when children return from the Thanksgiving holiday break.

On Wednesday, Mychael Dickerson, the district's chief of staff, confirmed via Twitter that several schools in Baltimore were affected after ransomware attackers targeted its IT systems and caused network interruption.

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

Fake VPN add-ons hit Microsoft Edge browser store

<https://www.techradar.com/news/fake-vpn-add-ons-hit-microsoft-edge-browser-store>

Reports are emerging of fake VPN extensions cropping up on the Microsoft Edge store. The malicious add-ons were found to be injecting suspicious ads into search results or redirecting users to entirely unwanted search engines altogether.

Users first started noticing that something wasn't right when they found that their Google searches were being redirected to a site called 'OKSearch'. Closer inspection identified that the extension had some code relating to the obscure search portal in the sources tab of its developer tools.

[Click link above to read more](#)

Updated Trickbot Malware Is More Resilient

<https://www.databreachtoday.com/updated-trickbot-malware-more-resilient-a-15449>

The gang operating Trickbot is continuing its activities despite recent takedown efforts, rolling out two updates that make the malware more difficult to kill, according to the security firm Bitdefender.

The latest Trickbot versions - 2000016 and 100003 - were rolled out on Nov. 3 and Nov. 18, respectively, with changes that include using a new command-and-control infrastructure based on MikroTik routers and only using packed modules. The malware was last updated in August, the researchers say.

[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.

