







October 27th, 2020

Challenge yourself during Cyber Security Awareness Month

Try our October - 'Cyber Security Awareness Month' Quiz

This week's stories:

-  [Career caravan offers Canadian military veterans opportunity to learn skills in software, cyber security](#)
-  [Canadian steelmaker Stelco hit by cyberattack](#)
-  [Canada concerned by 'pattern of malicious cyber activity' by Russian military, GAC says](#)
-  [The most common online, email scams Canadians are falling for now](#)
- [NIST Publishes Technical Note on Predicting Botnet Attacks](#)
- [CISA Analysis Report - Federal Agency Compromised by Malicious Cyber Actor](#)
- [Massive Nitro data breach impacts Microsoft, Google, Apple, more](#)
- [Sopra Steria Hit by New Ryuk Variant](#)
- [Moving to the cloud with a security-first, zero trust approach](#)
- [Password managers: A cheat sheet for professionals](#)
- [The Week in Ransomware - October 23rd 2020 - From Russia with Love](#)

Career caravan offers Canadian military veterans opportunity to learn skills in software, cyber security

<https://globalnews.ca/news/7410307/career-caravan-military-veterans-canadian-software-cyber-security/>

A career fair in Toronto is offering the more than 7,000 military veterans, who leave the Canadian Forces every year, the opportunity to learn new skills in software and cyber security.

Click link above to read more

Canadian steelmaker Stelco hit by cyberattack

<https://www.itworldcanada.com/article/canadian-steelmaker-stelco-hit-by-cyberattack/437503>

One of Canada's oldest steel manufacturing firms says it has been hit with an undefined cyberattack.

In a statement released Sunday afternoon, Stelco said it was “subject to a criminal attack on its information systems.”

“In response, Stelco immediately implemented countermeasures in accordance with established cybersecurity procedures and policies that have been developed in collaboration with expert external advisors,” the statement reads. “The countermeasures taken were effective and limited the scope of the attack. Certain operations, including steel production, were temporarily suspended as a precautionary measure but have since resumed operations.”

[Click link above to read more](#)

Canada concerned by ‘pattern of malicious cyber activity’ by Russian military, GAC says

<https://globalnews.ca/news/7406404/canada-russian-cyber-activity/>

Canadian officials are expressing concern over what they say is a “pattern of malicious cyber activity” at the hands of Russian military intelligence.

In a statement Monday afternoon, Global Affairs Canada (GAC) and the Communications Security Establishment said the country is “concerned over reports of a series of global malicious cyber activities, as detailed in today’s statements by the United States and the United Kingdom.”

[Click link above to read more](#)

The most common online, email scams Canadians are falling for now

<https://ca.sports.yahoo.com/news/scams-canada-fraud-online-email-210636718.html>

October is Cyber Security Awareness Month and the Canadian Anti-Fraud Centre (CAFC) is reminding the public about the most common scams to be on the lookout for.

“With the ongoing pandemic, Canadians have increasingly relied on the internet to conduct everyday activities, such as, buying and selling goods or looking for a job,” the bulletin from the CAFC reads.

[Click link above to read more](#)

NIST Publishes Technical Note on Predicting Botnet Attacks

<https://www.jdsupra.com/legalnews/nist-publishes-technical-note-on-69446/>

The Cybersecurity and Infrastructure Security Agency (CISA) responded to a recent threat actor’s On October 22, 2020, the National Institute of Standards and Technology (“NIST”) published NIST Technical Note (TN) 2111, “An Empirical Study on Flow-based Botnet Attacks Prediction”. The note, authored by Mitsuhiro Hatada and Matthew Scholl of NIST’s Information Technology Laboratory, presents a method to predict botnet attacks, such as mass spam email and distributed denial-of-service attacks (“DDoS”). This is particularly timely as botnet threats continue to rise in the era of the Internet of Things (“IoT”), where the number, density, and connectivity of devices continue to increase.

[Click link above to read more](#)

CISA Analysis Report - Federal Agency Compromised by Malicious Cyber Actor

<https://us-cert.cisa.gov/ncas/analysis-reports/ar20-268a>

The Cybersecurity and Infrastructure Security Agency (CISA) responded to a recent threat actor’s cyberattack on a federal agency’s enterprise network. By leveraging compromised credentials, the cyber

threat actor implanted sophisticated malware—including multi-stage malware that evaded the affected agency's anti-malware protection—and gained persistent access through two reverse Socket Secure (SOCKS) proxies that exploited weaknesses in the agency's firewall.

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

Massive Nitro data breach impacts Microsoft, Google, Apple, more

<https://www.bleepingcomputer.com/news/security/massive-nitro-data-breach-impacts-microsoft-google-apple-more/>

A massive data breach suffered by the Nitro PDF service impacts many well-known organizations, including Google, Apple, Microsoft, Chase, and Citibank.

Claimed to be used by over 10 thousand business customers and 1.8 million licensed users, Nitro is an application used to create, edit, and sign PDFs and digital documents.

As part of their service offering, Nitro offers a cloud service used by customers to share documents with coworkers or other organizations involved in the document creation process.

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

Sopra Steria Hit by New Ryuk Variant

<https://www.infosecurity-magazine.com/news/sopra-steria-hit-by-new-ryuk/>

French IT services giant Sopra Steria has said it will take weeks to return to normal after a serious ransomware attack forced key systems offline.

The group posted a very brief message on its website last week claiming to have discovered the attack on Tuesday evening.

However, its fintech business Sopra Banking Software confirmed in an update today that the incident was a ransomware attack.

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

Moving to the cloud with a security-first, zero trust approach

<https://www.helpnetsecurity.com/2020/10/21/moving-to-the-cloud-security-first-zero-trust-approach/>

Many companies tend to jump into the cloud before thinking about security. They may think they've thought about security, but when moving to the cloud, the whole concept of security changes. The security model must transform as well.

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

Password managers: A cheat sheet for professionals

<https://www.techrepublic.com/article/password-managers-a-cheat-sheet-for-professionals/>

The sheer number of passwords the average person has can lead to confusion and tons of password retrieval emails. Simplify and secure your digital life by learning about password managers.

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

The Week in Ransomware - October 23rd 2020 - From Russia with Love

<https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-23rd-2020-from-russia-with-love/>

This week has been busy with ransomware related news, including new charges against Russian state-sponsored hackers and numerous attacks against well-known organizations.

In 2017, there was an attack utilizing the NotPetya ransomware to destroy data on systems worldwide. This week, the US govt indicted six Russian intelligence operatives, known to be part of the notorious 'Sandworm' group, for hacking operations, including NotPetya.

We also learned of numerous attacks against large organizations, such as Barnes & Noble, the Monreal public transit system (STM), Sopra Steria, and Boyne Resorts.

[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.

