Security News Digest
Information Security Branch
British Columbia OCIO | Office of the Chief Information Officer

January 5th, 2021

Try our January "Resolutions" Quiz

This week's stories:

- 🇨🇦 Understanding Canadian Cybersecurity Laws: Measuring Up — Outlining Existing National Cybersecurity Legislation in Canada, the UK, Australia, and the US (Article 8)
- 🇨🇦 CISA Releases New Guidance on SolarWinds Patch
- 🇨🇦 Cyber Security Today – Make these cybersecurity New Year's Resolutions
- US Treasury warns of ransomware targeting COVID-19 vaccine research
- 12 Cybersecurity Predictions For 2021 Every Organization Must Consider
- The threats arising from the massive SolarWinds hack
- Explainers: How Intel's Homomorphic Encryption Can Process Ciphertext
- Google Discloses Poorly-Patched, Now Unpatched, Windows 0-Day Bug
- Mobile emulator steals millions from online bank accounts
- The Emotet botnet is back and hits 100K recipients per day

🇨🇦 Understanding Canadian Cybersecurity Laws: Measuring Up — Outlining Existing National Cybersecurity Legislation in Canada, the UK, Australia, and the US (Article 8)

https://www.itworldcanada.com/blog/understanding-canadian-cybersecurity-laws-measuring-up-outlining-existing-federal-cybersecurity-legislation-in-canada-the-uk-australia-and-the-us-article-8/440137

With 2020 being a year of rapid, unprecedented, large-scale global change, the many necessarily proposed alternations to our current cybersecurity-related laws have quickly shifted to the forefront of national security discussion. While the Privacy Act, the Access to Information Act, and PIPEDA have adequately covered our national personal privacy and granted provisions, and while the Criminal Code of Canada has done an adequate job of categorizing and detailing the legal provisions for criminal offences, there remains an increasingly ominous lack of comprehensive cybersecurity-specific legislation and cybercrime-specific Criminal Code provisions under our existing Canadian federal law. When so many features and daily facets of our lives are digitally connected to a larger network upon which our daily activities and interactions have become reliant, the idea that our national security and digital infrastructure may be at risk of exploitation or malicious interference is terrifying.

Click link above to read more

🇨🇦 CISA Releases New Guidance on SolarWinds Patch

https://www.inforisktoday.com/cisa-releases-new-guidance-on-solarwinds-patch-a-15684

The Cybersecurity and Infrastructure Security Agency has released an emergency directive requiring all federal organizations still running the vulnerable SolarWinds Orion software to immediately update to the latest version.

In an update released Wednesday, CISA says the organizations with a vulnerable version of the SolarWinds platform installed must update to version 2020.2.1HF2 by Dec. 31.

"The National Security Agency has examined this version and verified that it eliminates the previously identified malicious code," CISA says.

Click link above to read more

🇨🇦 Cyber Security Today – Make these cybersecurity New Year’s Resolutions

https://www.itworldcanada.com/article/cyber-security-today-make-these-cybersecurity-new-years-resolutions/440069

Make these cybersecurity New Year’s Resolutions

Welcome to Cyber Security Today. It’s Monday January 4th. I’m Howard Solomon, contributing reporter on cybersecurity for ITWorldCanada.com.

Now’s the time to think ahead about cybersecurity when the year is still fresh.

Click link above to read more

US Treasury warns of ransomware targeting COVID-19 vaccine research

https://www.bleepingcomputer.com/news/security/us-treasury-warns-of-ransomware-targeting-covid-19-vaccine-research/

The US Treasury Department's Financial Crimes Enforcement Network (FinCEN) warned financial institutions of ransomware actively targeting vaccine research organizations.

"FinCEN is aware of ransomware directly targeting vaccine research, and FinCEN asks financial institutions to stay alert to ransomware targeting vaccine delivery operations as well as the supply chains required to manufacture the vaccines," the US Treasury Department bureau warned [PDF].

The warning was published the same day the US Food and Drug Administration (FDA) issued two emergency use COVID-19 vaccine authorizations.

Click link above to read more

---

12 Cybersecurity Predictions For 2021 Every Organization Must Consider

https://www.entrepreneur.com/article/362641

Cybersecurity will remain a booming field in 2021, with almost 3.5 million posts that need to be filled. However, the landscape is set to undergo massive changes, and organizations need to have an idea about the future to take the necessary steps to adapt to the fast-changing threat landscape. The following twelve cybersecurity predictions will help organizations understand how COVID-19 has altered workplace habits and demand for cybersecurity solutions.

Larger cybersecurity budgets and more full-time cyber staff

PwC Global Digital Trust Insights 2021 found that more than half of all enterprises (55 per cent) state they will be increasing their cybersecurity budgets. Around 51 per cent of the executives in the survey said they would add full-time cybersecurity staff.

Click link above to read more

The threats arising from the massive SolarWinds hack

https://www.cbsnews.com/news/the-threats-arising-from-the-massive-solarwinds-hack/

Like the coronavirus, it came from overseas, arriving, initially, unnoticed. When it was finally, belatedly discovered, the outrage (for a few days at least) was epic.

"This is nothing short of a virtual invasion by the Russians into critical accounts of our federal government," said Democratic Senator Dick Durbin.

Republican Senator Mitt Romney called it "an extraordinary invasion of our cyberspace."

The Russians, it's believed, hacked into the software of a company called SolarWinds, causing them to push out malicious updates – call it a "cyber virus" – infecting the computer systems of more than 18,000 private and government customers. Almost a cyber pandemic.

Click link above to read more

Explainers: How Intel's Homomorphic Encryption Can Process Ciphertext

https://cisomag.eccouncil.org/homomorphic-encryption-standard/

Data Privacy is a big concern for governments and institutions. There are many debates about data residency, data stewardship, data ownership, and data privacy on the cloud. The introduction of acts/laws such as GDPR, CCPA, LGPD, and industry standards like HIPAA, have kept data privacy in check. Data custodians are bound by data privacy laws. That can be a real inhibitor to bringing larger data sets together, which in turn limits how much we can infer from that data. Data is encrypted at rest and in transit, but it must be decrypted to be processed on the cloud or elsewhere. So, there is a window of opportunity where data privacy can be compromised. Well, Intel Labs has been working on a homomorphic encryption standard to address this issue. However, there are some speed bumps to be tackled before the technology is ready for widespread adoption. *CISO MAG* had earlier reported on a related development called Federated Learning. Both are part of Intel's Confidential Computing mission, which aims to tackle the issue related to the restrictions around data privacy.

Click link above to read more

Google Discloses Poorly-Patched, Now Unpatched, Windows 0-Day Bug

https://thehackernews.com/2020/12/google-discloses-poorly-patched-now.html

Google's Project Zero team has made public details of an improperly patched zero-day security vulnerability in Windows print spooler API that could be leveraged by a bad actor to execute arbitrary code.

Details of the unpatched flaw were revealed publicly after Microsoft failed to rectify it within 90 days of responsible disclosure on September 24.

Originally tracked as CVE-2020-0986, the flaw concerns an elevation of privilege exploit in the GDI Print / Print Spooler API ("splwow64.exe") that was reported to Microsoft by an anonymous user working with Trend Micro's Zero Day Initiative (ZDI) back in late December 2019.

Click link above to read more

Mobile emulator steals millions from online bank accounts

http://www.digitaljournal.com/tech-and-science/technology/mobile-emulator-steals-millions-from-online-bank-accounts/article/583037

A new form of cyber-crime has seen cybercriminals siphoning off millions from compromised bank accounts using mobile device emulators. This requires a new approach to protecting personal and business accounts.

The latest cybersecurity issue has been identified by IBM Trusteer. Here researchers indicate they have uncovered a massive fraud operation. This operation has utilized network of mobile device emulators to drain millions of dollars from online bank accounts in a matter of days.

Click link above to read more

The Emotet botnet is back and hits 100K recipients per day

https://securityaffairs.co/wordpress/112650/malware/december-emotet-redacted.html

Emotet is back on Christmas Eve, after two months of silence, cybercrime operators are sending out spam messages to deliver the infamous Trickbot Trojan.

The recent Emotet campaign uses updated payloads and is targeting over 100,000 recipients per day.

"After a lull of nearly two months, the Emotet botnet has returned with updated payloads. The changes are likely meant to help Emotet avoid detection both by victims and network defenders." *reads* the post published by Cofense. "Apart from these updates, the campaigns' targeting, tactics and secondary payloads remain consistent with previous active periods."

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.

Security News Digest
Information Security Branch

BRITISH COLUMBIA OCIO | Office of the Chief Information Officer