Security Digest
Information Security Branch

BRITISH COLUMBIA

OCIO
Office of the Chief Information Officer

August 28th, 2018

August is "Wi-Fi" Month

This week's stories:

Canadian telcos could have been hacked by third party app flaw, says security firm

https://www.itworldcanada.com/article/canadian-telcos-could-have-been-hacked-by-third-party-app-flaw-says-security-firm/408288

A coding flaw in a cloud application aimed at helping people who have hearing or speech disorders place calls through an assistive telephone device could have been used to steal administration passwords at Canada's major telecom providers or any other provider using the service, according to researchers at a security firm.

The firm, Project Insecurity, said in a report that Soleo Communications — which provides a range of search and voice services for communications providers — fixed the bug in its IP Relay service Aug. 10th. But, the researchers added, a determined attacker could have leveraged the vulnerability before it was sealed to steal passwords from configuration files.

Click link above to read more

Russian trolls 'spreading discord' over vaccine safety online

https://www.theguardian.com/society/2018/aug/23/russian-trolls-spread-vaccine-misinformation-on-twitter

Bots and Russian trolls spread misinformation about vaccines on Twitter to sow division and distribute malicious content before and during the American presidential election, according to a new study.

Scientists at George Washington University, in Washington DC, made the discovery while trying to improve social media communications for public health workers, researchers said. Instead, they found trolls and bots skewing online debate and upending consensus about vaccine safety.

The study discovered several accounts, now known to belong to the same Russian trolls who interfered in the US election, as well as marketing and malware bots, tweeting about vaccines.

Click link above to read more

Kids at hacking conference show how easily US elections could be sabotaged

https://www.theguardian.com/technology/2018/aug/22/us-elections-hacking-voting-machines-def-con

Changing recorded votes would be difficult for bad actors. But at Def Con in Las Vegas, children had no trouble finding another point of entry.

At the world's largest hacking conference, there was good news and bad news for fans of free and fair elections.

The good news is that hacking the US midterms – actually changing the recorded votes to steal the election for a particular candidate – may be harder than it seems, and most of the political actors who could pose a threat to the validity of an election are hesitant to escalate their attacks that far.

The bad news is that it doesn't really matter. While the actual risk of a hacker seizing thousands of voting machines and altering their records may be remote, the risk of a hacker casting the validity of an election into question through one of any number of other entry points is huge, and the actual difficulty of such an attack is child's play. Literally.

Click link above to read more

Banking Malware Targets Mexico; Will It Spread?

https://www.databreachtoday.com/interviews/banking-malware-targets-mexico-will-spread-i-4082

Kaspersky Lab has discovered a new form of malware it calls Dark Tequila that has been targeting users in Mexico and stealing bank credentials and other personal and corporate data. The malware can move laterally through a computer while it's offline, says Dmitry Bestuzhev, head of Kaspersky Lab's global research and analysis team for Latin America.

The malware is designed for infiltration of systems even when networks have limited access to the internet, he explains in an interview with Information Security Media Group. "There are two known infection vectors: email and USB devices," Bestuzhev says.

While the malware apparently has been infecting computers in Mexico for about five years, it could potentially spread to other countries, Bestuzhev warns.

Click link above to read more

Google sued for tracking you, even when 'location history' is off

https://www.zdnet.com/article/google-sued-for-tracking-you-even-when-location-history-is-off/

Google now faces a potential class action lawsuit over the revelation that it continues to store users' location data even if they turn off Location History.

The lawsuit was filed on Friday, the day Google updated its help page to clarify that with Location History off it still stores some location data in other services such as Google Search and Maps.

Until then, Google's help page on Location History stated that "with Location History off, the places you go are no longer stored". However a report by the Associated Press found this statement wasn't true.

Click link above to read more

U.S. judge extends ban of online release of 3-D printed gun blueprints

https://globalnews.ca/news/4411819/u-s-3-d-printed-gun-blueprints-ban/

A U.S. judge on Monday extended a ban on the online distribution of 3-D printed gun blueprints, a win for a group of mainly Democratic-led states that said such a publication would violate their right to regulate firearms and endanger their citizens.

U.S. District Judge Robert Lasnik in Seattle issued the extension of a nationwide injunction, blocking a Texas-based group from disseminating files for printing plastic weapons on the internet.

Click link above to read more

UN hosts 'killer robots' panel to examine the future of warfare

https://globalnews.ca/news/4411808/killer-robots-united-nations/

Experts from scores of countries are meeting to discuss ways to define and deal with "killer robots" — futuristic weapons systems that could conduct war without human intervention.

The weeklong gathering that opened Monday is the second at UN offices in Geneva this year to focus on such lethal autonomous weapons systems and to explore possibilities for regulating them, among other issues.

Click link above to read more

Bulk to stealth security – covering all points of attack

https://www.itworldcanada.com/article/bulk-to-stealth-security-covering-all-points-of-attack/408317

When HPE National Strategist Garth Reid says cybercrime is getting worse, not better, he's not being alarmist; he's being realistic.

"Our biggest hacks might still be ahead of us, which is scary," he said during the ITWC webinar "Growing and Innovating at a Time of Rising Cybercrime" on August 21, 2018.

Tech Data Technology Consultant Robert LeRoy introduced a second point of concern: that hackers are casting a much wider net than ever before — going after even the most unlikely of targets.

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:

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

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.