Security Digest
Information Security Branch

BRITISH COLUMBIA

OCIO
Office of the Chief Information Officer

December 4th, 2018

December is Mobile Month

This week's stories:

- **Starwood Hotels hack of 500 million customers over four years confirmed**
- **Google, Twitter object to proposed Canadian online political ad registries**
- **'Butter' attack still victimizing Linux servers**
- **A Dunkin' Donuts Hack**
- **Watch Out for a Cleaver Tough ID Scam Hitting the App Store**
- **DOJ Indicts Hackers From Atlanta Who Installed Ransomware**
- **Healthcare Organizations Falling Behind on Cyber Risk Management**
- **Retailers Achieve Record Email Trustworthiness Leading into Holiday Shopping Season**
- **Mass router hack exposes millions of devices to potent NSA exploit**
- **Moscow's New Cable Car System Infected with Ransomware the Day After it Opens**

Starwood Hotels hack of 500 million customers over four years confirmed

https://www.itworldcanada.com/article/breaking-news-hotel-hack-of-500-million-customers/412535

Mariott Hotels this morning admitted encrypted and unencrypted personal information on 500 million customers who made reservations at one of its Starwood Hotels has been copied over four years from one of its databases.

In a release the company said that for approximately 327 million of these guests the stolen information includes some combination of name, mailing address, phone number, email address, passport number, Starwood Preferred Guest ("SPG") account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences.

Click link above to read more

Google, Twitter object to proposed Canadian online political ad registries

https://www.itworldcanada.com/article/google-twitter-object-to-proposed-canadian-online-political-ad-registries/412504

The biggest social media companies in Canada are split on a proposed law that would force online content platforms to create a registry of domestic and foreign political advertisers during federal elections.

At a meeting Thursday of the Senate legal affairs committee considering Bill C-76, which would update the Elections Act, Facebook sent in a letter that it supports the proposed legislation.

Click link above to read more

‘Butter’ attack still victimizing Linux servers

https://www.itworldcanada.com/article/butter-attack-still-victimizing-linux-servers-report/412454

To many people, butter is a basic food that is used widely in cooking and eating. It’s also the username an attack group has been using after breaking into Linux servers.

Which is why GuardiCore Labs has dubbed an attack campaign that has been going on for several years “Butter.” And like its namesake, simplicity is the key to its success.

Click link above to read more

A Dunkin’ Donuts Hack

https://www.zdnet.com/article/dunkin-donuts-accounts-may-have-been-hacked-in-credential-stuffing-attack/

Dunkin', the company behind the Dunkin' Donuts franchise, has notified owners of DD Perks rewards accounts that a hacker might have accessed their profiles and personal data last month.

The company said it didn't suffer an actual breach of its backend systems but only fell victim to an automated attack known in the cyber-security field as a credential stuffing attack.

Click link above to read more

Watch Out For Cleaver Tough ID Scam Hitting the Network

HTTPS://WWW.WIRED.COM/STORY/IPHONE-TOUCH-ID-SCAM-APPS/

One of the joys of Touch ID is how seamlessly it works. It rarely takes more than an instant to unlock your iPhone or approve a purchase. But recently a handful of scam apps have turned that ease of use against anyone unlucky enough to download them.

Click link above to read more

DOJ Indicts Hackers From Atlanta Who Installed Ransomware

https://www.wired.com/story/doj-indicts-hackers-samsam-ransomware/

The city of Atlanta. Kansas Heart Hospital. Those are just a few of the more than 200 municipalities, universities, hospitals, and other targets that have fallen victim to SamSam, a pernicious strain of ransomware that has spent the past three years rampaging throughout the US. On Wednesday, the Justice Department indicted two Iranian men allegedly behind the attacks.

The six-count indictment (embedded in full below) alleges that Faramarz Shahi Savandi and Mohammad Mehdi Shah Mansouri, both Iranian nationals, created SamSam and deployed it to devastating effect. In all, the Justice Department estimates that the hackers collected around $6 million in ransom payments from victims, while causing $30 million of damage.

Click link above to read more

Healthcare Organizations Falling Behind on Cyber Risk Management

https://www.securitymagazine.com/articles/89645-healthcare-organizations-falling-behind-on-cyber-risk-management

Only 29 percent of healthcare organizations reporting having a comprehensive security program in place, and among those that do not have such a program, 31 percent are either not meeting with their executive committee or are meeting less than once a year to give security updates.

Click link above to read more

Global Cybersecurity Workforce Gap Expands to 2.9 Million

https://www.securitymagazine.com/articles/89642-global-cybersecurity-workforce-gap-expands-to-29-million

The global cybersecurity workforce gap has increased to more than 2.9 million, according to (ISC)2. Fifty-nine percent of cybersecurity professionals say that the widening workforce gap puts their organizations at risk.

Across the U.S., there are currently 313,735 total cybersecurity job openings nationally, and the supply of cybersecurity workers is very low. The national average cybersecurity workforce supply/demand ratio is 2.3, according to CyberSeek's Cybersecurity Supply/Demand Heat Map.

Click link above to read more

Retailers Achieve Record Email Trustworthiness Leading into Holiday Shopping Season

https://www.securitymagazine.com/articles/89634-retailers-achieve-record-email-trustworthiness-leading-into-holiday-shopping-season

Two hundred of the largest online retailers are taking consumer email protection and convenience seriously, according to analysis by the Internet Society's Online Trust Alliance.

"Although email unsubscribe and security practices may not win any retail customers, it can certainly lose them, and retailers appear to be paying attention," said the Technical Director of the Internet Society's Online Trust Alliance, Jeff Wilbur. "Our research shows that retailers are working hard to eliminate email compromise and impersonation, while generally making it easier than ever for consumers to unsubscribe from marketing emails. We've noted there's still plenty of room for improvement and one or two worrying trends, but overall this shows a serious commitment to improving the online shopping experience."

Click link above to read more

Mass router hack exposes millions of devices to potent NSA exploit

https://arstechnica.com/information-technology/2018/11/mass-router-hack-exposes-millions-of-devices-to-potent-nsa-exploit/

More than 45,000 Internet routers have been compromised by a newly discovered campaign that's designed to open networks to attacks by EternalBlue, the potent exploit that was developed by, and then stolen from, the National Security Agency and leaked to the Internet at large, researchers said Wednesday.

The new attack exploits routers with vulnerable implementations of Universal Plug and Play to force connected devices to open ports 139 and 445, content delivery network Akamai said in a blog post. As a result, almost 2 million computers, phones, and other network devices connected to the routers are reachable to the Internet on those ports. While Internet scans don't reveal precisely what happens to the connected devices once they're exposed, Akamai said the ports—which are instrumental for the spread of EternalBlue and its Linux cousin EternalRed—provide a strong hint of the attackers' intentions.

Click link above to read more

Moscow's New Cable Car System Infected with Ransomware the Day After it Opens

https://www.bleepingcomputer.com/news/security/moscows-new-cable-car-system-infected-with-ransomware-the-day-after-it-opens/

Moscow recently opened its first cable-car service and promised free rides for the first month. Unfortunately, only days after after the service was made available, attackers reportedly hacked into the cable car systems and infected them with ransomware.

With eager passengers waiting to take their free ride, police officers were explaining that the cable car was shut down due to technical reasons according to a report from the TheMoscowTimes.

Click link above to read more

Click Unsubscribe to stop receiving the Digest.

****

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