Security Digest
Information Security Branch

BRITISH COLUMBIA

OCIO
Office of the Chief Information Officer

November 6th, 2018

November is "Online Shopping" Month

This week's stories:

- Amid growing cybercrime, tech companies hire teams of hackers to exploit flaws in their own software
- Canadian firms now must report serious data breaches; get ready for more victim lawsuits
- How can we stop being cyber idiots?
- New data shows China has "taken the gloves off" in hacking attacks on US
- Private Messages for 81k Hacked Facebook Accounts Being Sold Online
- Majority of Top 30 Sites Don't Offer Wide Range of 2FA Options
- Georgia Election Further Complicated by Hacking Accusation
- Ransomware Keeps Ringing in Profits for Cybercrime Rings
- Australian Shipbuilder Hacked, Refuses to Pay Ransom
- Eye Clinic Sees Quick Recovery from Ransomware Attack
- Data leak affects thousands of wealthy Moscow residents
- Lloyds replacing some debit cards after cyber-attacks

Amid growing cybercrime, tech companies hire teams of hackers to exploit flaws in their own software

https://business.financialpost.com/technology/personal-tech/amid-growing-cybercrime-tech-companies-hire-teams-of-hackers-to-exploit-flaws-in-their-own-software

There is a team of seven people bunkered down in Redmond, Wash., trying to hack and infiltrate the latest Microsoft Corp. software that's used by more than a billion devices around the world.

From Twitter to Reddit, the group was recruited from various corners of the internet to identify software vulnerabilities that can be exploited to steal personal data that can then be sold to the highest bidder, break inside networks or infiltrate devices.

They are good at what they do. Fortunately, they aren't malicious. They are Microsoft's in-house Red Team, and they are constantly trying to identify and fix security vulnerabilities in the company's products before real-world hackers ever get a crack at them.

Click link above to read more

Canadian firms now must report serious data breaches; get ready for more victim lawsuits

https://www.itworldcanada.com/article/canadian-firms-now-must-report-serious-data-beaches-get-ready-for-more-victim-lawsuits/411272

Canada's new mandatory data breach notification law takes effect today.

It forces companies that come under the federal data protection act to report serious violations of personal data safeguards to tell victims and the federal privacy commissioner. Violations could result in fines of up to $100,000.

Whether companies will try to skirt the law, which says only breaches that could result in "real risk of significant harm" – forever shortened now as RRSH – have to be reported, is open. Some feel the definition is loose enough that a few firms may say, in effect, 'we didn't think it was that serious.'

Click link above to read more

How can we stop being cyber idiots?

https://www.bbc.com/news/technology-45953238

Humans are often the weakest link in the chain when it comes to computer security. So how can we stop doing silly things that play into the hands of cyber criminals?

When you ring IT support, you know the geek on the other end of the line thinks you're an idiot. It's the heavy sigh and patronising tone that give it away.

In fact, they have an acronym for us - PEBKAC. It stands for Problem Exists Between Keyboard And Chair. That's you and me.

And before you get on your high horse full of indignation, ask yourself: when did I last back up my data? How many online accounts do I use the same password for? How many times have I clicked on a link in an email without really knowing who sent it?

Click link above to read more

New data shows China has "taken the gloves off" in hacking attacks on US

https://arstechnica.com/information-technology/2018/11/new-data-shows-china-has-taken-the-gloves-off-in-hacking-attacks-on-us/

Remember the good old days, when the US and China were supposedly working out new norms for the cybers, and China was going to stop all that hacking of US companies to steal intellectual property? It turns out the Chinese were just upping their hacking game, improving their operational security and penetration skills—learning from the methods of their Russian counterparts.

A recent example of that "island hopping" tactic is the "Cloud Hopper" hacking campaign, active since at least May of 2016. In October, DHS issued a new alert on the campaign, warning of a surge in activity by the campaign over the past few months. Cloud Hopper has been attributed to the threat group known as APT 10, aka Stone Panda—a hacking group that has been tied to the Chinese Ministry of State Security's Tianjin Bureau.

Click link above to read more

Private Messages for 81k Hacked Facebook Accounts Being Sold Online

https://www.bleepingcomputer.com/news/security/private-messages-for-81k-hacked-facebook-accounts-being-sold-online/

Criminals are selling the private messages of 81,000 hacked Facebook accounts for 10 cents per account.

According to research conducted by the BBC, a seller going by the name "FBSaler" began posting on underground criminal forums about having access to the information of 120 million Facebook users as well as access to the private messages of 81,000 profiles. These accounts are being sold for 10 cents each.

Click link above to read more

Majority of Top 30 Sites Don't Offer Wide Range of 2FA Options

https://www.bleepingcomputer.com/news/security/majority-of-top-30-sites-dont-offer-wide-range-of-2fa-options/

The Dashlane password management company has released research showing that the majority of the top 30 consumer sites do not offer a complete range of two factor authentication (2FA) options for login authentication. Of the top 30 sites, only 8 offered all of the tested for 2FA options.

Two Factor Authentication (2FA) provides extra security for a login procedure by not only requiring a password to login, but also some sort of 3rd party authentication code or mechanism. For example, sites can be configured to use 2FA that would require you to login with your password and then further enter a code that is texted to your mobile device or displayed on authentication software, before allowing you to fully login.

Click link above to read more

Georgia Election Further Complicated by Hacking Accusation

https://www.databreachtoday.com/georgia-election-further-complicated-by-hacking-accusation-a-11666

The Republican gubernatorial candidate in Georgia has accused the state's Democratic Party of attempting to hack the state's voter registration database. But his charge has triggered skepticism and a fierce rebuttal from the accused.

The accusation, from Brian Kemp, is further complicated because he is also the state's current secretary of state, who supervises election infrastructure and procedures.

On Sunday, Kemp's office released a two paragraph statement saying he'd ordered his office to open an investigation into the Democratic Party of Georgia "after a failed attempt to hack the state's voter registration system."

Click link above to read more

Ransomware Keeps Ringing in Profits for Cybercrime Rings

https://www.databreachtoday.com/ransomware-keeps-ringing-in-profits-for-cybercrime-rings-a-11667

Criminals continue to earn an illicit payday - at victims' expense - thanks to crypto-locking ransomware, security experts and cyber insurance firms warn.

One insurer says it's seen the number of cyber insurance claims for ransomware increase in recent months.

"In September, our insureds were hit particularly hard, with notifications to Beazley of ransomware attacks more than doubling relative to August," Beazley Breach Response Services, which is part of London-based insurance business Beazley, says in a blog posted on Thursday. "It is unclear if this spike will continue, as up until September the overall number of ransomware incidents in 2018 have been holding steady with 2017 numbers."

Click link above to read more

Australian Shipbuilder Hacked, Refuses to Pay Ransom

https://www.databreachtoday.com/australian-shipbuilder-hacked-refuses-to-pay-ransom-a-11662

Australia's largest defense exporter says it hasn't responded to an extortion attempt after ship design schematics were stolen by a hacker.

Austal, which is based in Henderson, Western Australia, is one of the country's largest shipbuilders; it has built vessels for the U.S. Navy.

The company, which is listed on Australia's ASX stock exchange, announced the breach late Thursday. The announcement came just a day after a security researcher in France posted screenshots on Twitter of the purported stolen data.

Click link above to read more

Eye Clinic Sees Quick Recovery from Ransomware Attack

https://www.databreachtoday.com/eye-clinic-sees-quick-recovery-from-ransomware-attack-a-11665

An Iowa eye clinic and its affiliated surgery center recently recovered from a ransomware attack on their common systems within one day and without paying a ransom. This case offers important reminders to other healthcare entities and their vendors.

Experts say that well thought-out and carefully implemented advance planning was likely helpful in the quick recovery.

"See? It *can* be done," says Rebecca Herold, president of Simbus, a privacy and cloud security services firm, and CEO of The Privacy Professor consultancy.

"With pre-planning, up-to-date backups, trained response and recovery teams, and documented policies and procedures, responding to ransomware attacks can be handled efficiently, consistently and with minimal disruption to services," she says.

Click link above to read more

Data leak affects thousands of wealthy Moscow residents

https://ca.news.yahoo.com/data-leak-affects-thousands-wealthy-moscow-residents-133957347.html

Thousands of wealthy Moscow residents who subscribed to a regional internet provider have had personal data including names, home addresses and mobile numbers posted online.

People affected by the high-profile data leak are all clients of Moscow-based internet provider Akado Telecom, a large telecommunications network owned by billionaire businessman Viktor Vekselberg, which said it had opened an inquiry into the incident.

Click link above to read more

Lloyds replacing some debit cards after cyber-attacks

https://www.bbc.com/news/business-46075090?intlink_from_url=https://www.bbc.com/news/topics/cz4pr2gd85qt/cyber-security&link_location=live-reporting-story

The bank has reissued debit cards to all customers that have made purchases on Ticketmaster's website.

It is also working with BA to establish which customers have had their details compromised during two cyber-attacks.

Lloyds said it had a "range of approaches" designed to protect customers from fraud.

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