Security News Digest
Information Security Branch

BRITISH COLUMBIA OCIO Office of the Chief Information Officer

September 1st, 2020
Try our September - 'Passwords' Quiz

This week's stories:

- **Victims of CRA hackers vulnerable to other cyberattacks: experts**
- **Inside the Chinese military attack on Nortel**
- **Royal Bank among the top victims of cybersquatting, says report**
- **New Zealand bourse website hit by fresh cyberattack, but keeps trading**
- **How phishing attacks have exploited Amazon Web Services accounts**
- **Phishing Attack Used Box to Land in Victim Inboxes**
- **American Payroll Association discloses credit card theft incident**
- **Elon Musk confirmed Russian's plans to extort Tesla**

Victims of CRA hackers vulnerable to other cyberattacks: experts

https://www.cbc.ca/news/politics/cra-cyber-attack-privacy-1.5689928

Thousands of Canadians affected by recent cyberattacks on the Canada Revenue Agency and federal government computer systems could be vulnerable to other attacks, warn cybersecurity and privacy experts.

"They have to be very scared if they have another account with the same password," said Ali Ghorbani, director of the Canadian Institute for Cybersecurity at the University of New Brunswick. "If it doesn't happen now, it would happen tomorrow."

Former Ontario privacy commissioner Ann Cavoukian said the risk to those whose accounts were breached shouldn't be underestimated.

Click link above to read more

Inside the Chinese military attack on Nortel

https://globalnews.ca/news/7275588/inside-the-chinese-military-attack-on-nortel/

In 2004 Nortel cyber-security advisor Brian Shields investigated a serious breach in the telecom giant's network. At the time Nortel's fibre optics equipment was the world's envy, with 70 per cent of all internet traffic running on Canadian technology.

And someone wanted Nortel's secrets.

Shields found that a computer in Shanghai had hacked into the email account of an Ottawa-based Nortel executive. Using passwords stolen from the executive the intruder downloaded more than 450 documents from “Live Link” — a Nortel server used to warehouse sensitive intellectual property.

Click link above to read more

Royal Bank among the top victims of cybersquatting, says report

https://www.itworldcanada.com/article/royal-bank-among-the-top-victims-of-cybersquatting-says-report/435254

Royal Bank of Canada is among the top worldwide brands whose domains are mimicked by cybercriminals to make fake websites look more real, according to a new study.

In a report released this morning, Palo Alto Networks says RBC was the third most common brand and domain abused by crooks in a survey done last December, behind PayPal and Apple and slightly ahead of Netflix, LinkedIn and Amazon.

Others in the top 10 that month included Dropbox, Trip Advisor and Bank of America.

Click link above to read more

New Zealand bourse website hit by fresh cyberattack, but keeps trading

https://ca.news.yahoo.com/zealands-stock-market-website-goes-000225284.html

The New Zealand stock market was hit by a fifth day of cyber attacks on Monday, crashing its website, but maintained trading after switching to a contingency plan for the release of market announcements.

NZX Ltd <NZX.NZ> was halted for most of last week due to the attacks, which authorities have said originated offshore.

Monday's attack came shortly after NZX said it had agreed with the Financial Markets Authority (FMA) on a back-up plan for the release of market announcements.

Click link above to read more

How phishing attacks have exploited Amazon Web Services accounts

https://www.techrepublic.com/article/how-phishing-attacks-have-exploited-amazon-web-services-accounts/?ftag=TREa988f1c&bhid=19662319145962710268575546540229&mid=13008079&cid=712327807

Amazon is a target ripe for exploitation in phishing campaigns because the company has such a huge presence across so many different areas. Most phishing emails that impersonate Amazon are aimed at consumers who use the company on a retail level. But some are designed to spoof Amazon on a business level. A series of recent phishing attacks tried to take advantage of organizations that use Amazon Web Services (AWS). In a blog post published Monday, security trainer KnowBe4 describes how these phishing emails proved quite convincing.

Click link above to read more

Phishing Attack Used Box to Land in Victim Inboxes

https://www.darkreading.com/attacks-breaches/phishing-attack-used-box-to-land-in-victim-inboxes/d/d-id/1338754?_mc=rss_x_drr_edt_aud_dr_x_x-rss-simple&utm_medium=email&_hsmi=93958163&_hsenc=p2ANqtz-9CiORceEEaaQIgCQQoPt2F91c9BJ18CdDcs9x61ar_-wy48pEXCiyfLQw-

MelZG0DhXMJGz3Ep02060hyyGsSBTy0hxVfJI1uBVGvbj02mHCZmZBk&utm_content=93958163&utm_source=hs_email

A phishing attack targeting government and security organizations used a legitimate Box page with Microsoft 365 branding to trick victims.

A newly discovered credential phishing campaign used a legitimate Box webpage and exploited widespread trust in Microsoft 365 to capture victims' credentials in a convoluted attack chain.

The team at Armorblox discovered this threat back in June and say it affected city officials, as well as government and cybersecurity organizations. Attackers chose to host the phishing site on a legitimate Box page, which security experts say helped the emails land in victims' inboxes.

Click link above to read more

American Payroll Association discloses credit card theft incident

https://www.bleepingcomputer.com/news/security/american-payroll-association-discloses-credit-card-theft-incident/

The American Payroll Association (APA) disclosed a data breach affecting members and customers after attackers successfully planted a web skimmer on the organization's website login and online store checkout pages.

APA discovered around July 23, 2020, that its website and online store were breached by unknown threat actors who deployed a skimmer designed to collect and exfiltrate sensitive information to attacker-controlled servers.

The attackers used a security vulnerability in the organization's content management system (CMS) to hack into APA's site and online store according to a data breach notification sent to affected individuals by Robert Wagner, APA's Senior Director of Govt. and Public Relations, Certification, and IT.

Click link above to read more

Elon Musk confirmed Russian's plans to extort Tesla

https://www.bleepingcomputer.com/news/security/elon-musk-confirmed-russians-plans-to-extort-tesla/

The FBI thwarted the plans of 27-year-old Russian national Egor Igorevich Kriuchkov to recruit an insider within Tesla's Nevada Gigafactory, persuade him to plant malware on the company's network, and then ransom Tesla under threat that he would leak data stolen from their systems.

Kriuchkov was arrested on August 22, 2020, in Los Angeles after he got a phone call from an FBI agent and tried to leave the U.S.

Click link above to read more

---

https://www.gov.bc.ca/informationsecurity
OCIOSecurity@gov.bc.ca