Security Digest
Information Security Branch

BRITISH COLUMBIA
OCIO
Office of the Chief Information Officer

November 20th, 2018

November is "Online Shopping" Month

This week's stories:

- BlackBerry makes largest acquisition ever in $1.4B purchase of AI firm Cylance
- Why a seemingly insignificant financial merger triggered huge wave of Canadian phishing attacks
- VisionDirect Data Breach Caused by MageCart Attack
- New Gmail Bug Allows Sending Messages Anonymously
- Make-A-Wish Website Compromised for Cryptojacking Operation
- Speech Synthesis API Being Restricted in Chrome 71 Due to Abuse
- Azure, Office 365 go super-secure: Multi-factor auth borked in Europe, Asia, USA
- Blackout for thousands of dark web pages
- Russians impersonating US State Dept aide in hacking campaign: researchers
- Database leak exposes millions of two-factor codes and reset links sent by SMS
- Police decrypt 258,000 messages after breaking pricey IronChat crypto app

---

BlackBerry makes largest acquisition ever in $1.4B purchase of AI firm Cylance

https://www.itworldcanada.com/article/blackberry-makes-largest-acquisition-ever-in-1-4b-purchase-of-ai-firm-cylance/411937

Waterloo, Ont.-based BlackBerry Ltd. is making its largest acquisition ever in acquiring Irvine, Calif.-based Cylance for $1.4 billion, the firms announced Friday.

Founded in 2012, Cylance is known for its artificial intelligence software that aims to intercept security breaches before they occur. It's one of several firms that are touting new AI capabilities to help enterprises stay one step ahead of hackers. This space has been a hot one this year, attracting venture capital investments and acquisitions.

BlackBerry will wholly acquire Cylance, according to a press release, for $1.4 billion in cash, plus the assumption on unvested employee incentive awards. The deal is expected to close before the end of BlackBerry's next fiscal year, which arrives in February 2019.

Click link above to read more

Why a seemingly insignificant financial merger triggered huge wave of Canadian phishing attacks

https://www.itworldcanada.com/article/why-a-seemingly-insignificant-financial-merger-triggered-huge-wave-of-canadian-phishing-attacks/411929

In February two Canadian bank-owned co-operatives, Interac Association – which runs the inter-bank debit card network – and Acxsys Corp. – which among other things runs Interac's e-transfer and Online service – announced they were merging to form Interac Corp.

Missed that breathtaking news, did you? Well, cyber criminals didn't.

According to security vendor RSA, a gang or gangs used that information to launch a wave of phishing attacks against residents here, hoping to sucker them into giving up their usernames and passwords by pretending to from Interac or the Canada Revenue Agency and asking for confirmation of transactions.

Click link above to read more

VisionDirect Data Breach Caused by MageCart Attack

https://www.bleepingcomputer.com/news/security/visiondirect-data-breach-caused-by-magecart-attack/

VisionDirect, a popular contact lens online merchant in Europe, has posted an advisory stating that their web site had a data breach that led to the theft of credit card and account information.

According to the notification, account and payment information entered on the site between November 3rd and November 8th could have been captured and sent to attackers. This data includes all account information such as billing addresses, phone numbers, and credit card information.

Click link above to read more

New Gmail Bug Allows Sending Messages Anonymously

https://www.bleepingcomputer.com/news/security/new-gmail-bug-allows-sending-messages-anonymously/

A new bug discovered in Gmail affects the web app's user experience by hiding the source address of an email, a situation that comes with an obvious potential for abuse.

Tampering with the 'From:' header by replacing some text with an <object>, <script> or <img> tag causes the interface to show a blank space instead of the sender's address.

Click link above to read more

Make-A-Wish Website Compromised for Cryptojacking Operation

https://www.bleepingcomputer.com/news/security/make-a-wish-website-compromised-for-cryptojacking-operation/

Crooks have no scruples when it comes to making money. Any high-traffic website is a good target for setting up a cryptocurrency mining operation, and the one handled by the Make-A-Wish charitable organization makes no exception.

Operators of a known campaign that compromises websites still vulnerable to the Drupalgeddon 2 security bug targeted 'worldwish.org' and planted a script that uses the computing resources of the visitor's systems to mine for cryptocurrency.

Click link above to read more

Speech Synthesis API Being Restricted in Chrome 71 Due to Abuse

https://www.bleepingcomputer.com/news/google/speech-synthesis-api-being-restricted-in-chrome-71-due-to-abuse/

Web developers can use the SpeechSynthesis API to convert text on a web page into synthesized audio speech. While this feature is great for accessibility and audio queues, it is being abused by advertisements and low quality/scammy web sites.

As this method is one of the last remaining ways for a site to autoplay audio without user interaction, is being abused by sites and advertisements, and does not adhere to Google's autoplay policies, Google has decided to restrict its use starting in Chrome 71.

Click link above to read more

Azure, Office 365 go super-secure: Multi-factor auth borked in Europe, Asia, USA

https://www.theregister.co.uk/2018/11/19/azure_down/

Azure Multi-Factor Authentication is struggling, meaning that some users with the functionality enabled are now super secure. And, er, locked out.

Microsoft confirmed that there were problems from 04:39 UTC with a subset of customers in Europe, the Americas, and Asia-Pacific experiencing "difficulties signing into Azure resources" such as the, er, little used Azure Active Directory, when Multi-Factor Authentication (MFA) is enabled.

Click link above to read more

Blackout for thousands of dark web pages

https://www.bbc.com/news/technology-46263995

Hackers have deleted more than 6,500 sites being held on a popular dark web server.

Called Daniel's Hosting, the site was sitting on the hidden Tor network and many people used it to host pages they did not want to publish on the wider web.

Administrator Daniel Winzen said no back-ups were kept of the pages it hosted.

He said the site should be back in service in December.

Click link above to read more

Russians impersonating US State Dept aide in hacking campaign: researchers

https://www.channelnewsasia.com/news/technology/russians-impersonating-us-state-dept-aide-in-hacking-campaign--researchers-10940008

Hackers linked to the Russian government are impersonating U.S. State Department employees in an operation aimed at infecting computers of U.S. government agencies, think tanks and businesses, two cybersecurity firms told Reuters.

The operation, which began on Wednesday, suggests Russia is keen to resume an aggressive campaign of attacks on U.S. targets after a lull going into the Nov. 6 U.S. midterm election, in which Republicans lost control of the House of Representatives, according to CrowdStrike and FireEye Inc .

Click link above to read more

Database leak exposes millions of two-factor codes and reset links sent by SMS

https://arstechnica.com/information-technology/2018/11/millions-of-sms-texts-in-unsecured-database-expose-2fa-codes-and-reset-links/

Millions of SMS text messages—many containing one-time passcodes, password reset links, and plaintext passwords—were exposed in an Internet-accessible database that could be read or monitored by anyone who knew where to look.

The discovery comes after years of rebukes from security practitioners that text messages are a woefully unsuitable medium for transmitting two-factor authentication (2FA) data. Despite those rebukes, SMS-

based 2FA continues to be offered by banks such as Bank of America, cellular carriers such as T-Mobile, and a host of other businesses.

Click link above to read more

Police decrypt 258,000 messages after breaking pricey IronChat crypto app

https://arstechnica.com/information-technology/2018/11/police-decrypt-258000-messages-after-breaking-pricey-ironchat-crypto-app/?utm_source=The+Parallax+View&utm_campaign=c3640c8146-EMAIL_CAMPAIGN_2018_11_16&utm_medium=email&utm_term=0_7d4de369d8-c3640c8146-223502857

Police in the Netherlands said they decrypted more than 258,000 messages sent using IronChat, an app billed as providing end-to-end encryption that was endorsed by National Security Agency leaker Edward Snowden. Through a representative at the American Civil Liberties Union, Snowden said he had never heard of the app until recently and has never endorsed it.

In a statement published Tuesday, Dutch police said officers achieved a “breakthrough in the interception and decryption of encrypted communication” in an investigation into money laundering. The encrypted messages, according to the statement, were sent by IronChat, an app that runs on a device that cost thousands of dollars and could send only text messages.

Click link above to read more