Security News Digest
Information Security Branch
BRITISH COLUMBIA OCIO | Office of the Chief Information Officer

July 7th, 2020

Try our July - 'Back to Basics' Quiz

This week's stories:

- **Clearview AI cancels contract with RCMP, says it's no longer offering its facial recognition tech in Canada** 🇨🇦
- **Security cameras can tell burglars when you're not home, study shows**
- **Schools urged to ensure students' security and privacy when conducting classes online** 🇨🇦
- **First reported Russian BEC scam gang targets Fortune 500 firms**
- **EDP energy giant confirms Ragnar Locker ransomware attack**
- **FBI nabs Nigerian business scammer who allegedly cost victims millions**
- **US Cyber Command urges F5 customers to patch critical BIG-IP flaw**

Clearview AI cancels contract with RCMP, says it's no longer offering its facial recognition tech in Canada

https://www.itworldcanada.com/article/clearview-ai-says-its-cancelling-contract-with-rcmp-and-no-longer-offering-its-facial-recognition-tech-in-canada/432730

Bowing to months of pressure from Canadian privacy regulators, American facial recognition provider Clearview AI has stopped trying to sell its services to law enforcement agencies in Canada while it is under investigation for the way it collects images from the internet.

The Office of the Privacy Commissioner of Canada (OPC) announced July 6 that Clearview AI will cease offering its facial recognition services in Canada and that it's cancelled its contract with the Royal Canadian Mounted Police, which was the firm's last client in the country.

Click link above to read more

Security cameras can tell burglars when you're not home, study shows

https://www.cnn.com/2020/07/06/tech/home-security-cameras-risks-scli-intl-scn/index.html

Some popular home security cameras could allow would-be burglars to work out when you've left the building, according to a study published Monday.

Researchers found they could tell if someone was in, and even what they were doing in the home, just by looking at data uploaded by the camera and without monitoring the video footage itself.

Click link above to read more

Schools urged to ensure students' security and privacy when conducting classes online 🇨🇦

https://www.cbc.ca/news/technology/schools-virtual-learning-privacy-1.5615999

As most parts of Canada are gradually reopening their economies following months of lockdown due to the COVID-19 pandemic, some provinces — including Ontario, Manitoba, Alberta and New Brunswick — have released plans on how they aim to allow students to return to the classroom in September.

But those school boards continuing with partial or fully virtual learning need to ensure measures are in place to protect students' privacy and safety when using video-conferencing platforms for online classes, a cybersecurity expert says.

Click link above to read more

First reported Russian BEC scam gang targets Fortune 500 firms

https://www.bleepingcomputer.com/news/security/first-reported-russian-bec-scam-gang-targets-fortune-500-firms/

Over the past year, a new group of fraudsters believed to be from the Russian cybercriminal space has elevated Business Email Compromise (BEC) scams to a new level.

Most BEC attacks are from Nigerian actors, who target companies of any size. Cosmic Lynx is a different breed that focuses on multinational corporations and tries to score big, asking for large sums (hundreds of thousands or even millions of USD) to be transferred to mule accounts in Hong Kong.

Researchers at email prevention company Agari tracking Cosmic Lynx say that the group is responsible for more than 200 BEC attacks since July 2019 and show operational complexity not seen before with other BEC actors.

Click link above to read more

EDP energy giant confirms Ragnar Locker ransomware attack

https://www.bleepingcomputer.com/news/security/edp-energy-giant-confirms-ragnar-locker-ransomware-attack/

EDP Renewables North America (EDPR NA) confirmed a Ragnar Locker ransomware attack that affected its parent corporation's systems, the Portuguese multinational energy giant Energias de Portugal (EDP).

EDP Group's activities are focused on electric power generation and distribution, as well as on the information technology industry sectors.

At the moment, it has over 11,500 employees, delivers energy to over 11 million customers, and is the world's 4th largest producer of wind energy and one of the largest energy sector operators (both gas and electricity) in Europe.

Click link above to read more

FBI nabs Nigerian business scammer who allegedly cost victims millions

https://arstechnica.com/tech-policy/2020/07/fbi-nabs-nigerian-business-scammer-who-allegedly-cost-victims-millions/

The US government has gained custody of a Nigerian man who is accused of participating in a massive fraud and money laundering operation. The defendant, Ray "Hushpuppi" Abbas, has amassed 2.4 million followers on Instagram, where he flaunts his access to luxury cars, designer clothing, and private jets. The feds say that he gained this wealth by defrauding banks, law firms, and other businesses out of millions of dollars. He was arrested last month by authorities in the United Arab Emirates, where he had been living.

The FBI's criminal complaint details how the government obtained a wealth of information tying Abbas to his alleged crimes. Abbas was an avid user of American technology platforms, including Instagram, Gmail, iCloud, and Snapchat. Accounts on these platforms were all registered using a handful of common email addresses and phone numbers. Abbas's main email account—rayhushpuppi@gmail.com—included a copy of Abbas' lease at a luxury hotel in Dubai and scans of various government-issued photo IDs under Abbas' name.

Click link above to read more

US Cyber Command urges F5 customers to patch critical BIG-IP flaw

https://www.bleepingcomputer.com/news/security/us-cyber-command-urges-f5-customers-to-patch-critical-big-ip-flaw/

F5 Networks (F5) patched a critical remote code execution (RCE) vulnerability found in undisclosed pages of Traffic Management User Interface (TMUI) of the BIG-IP application delivery controller (ADC).

F5 customers using BIG-IP software and hardware solutions include enterprise governments, Fortune 500 firms, banks, service providers, and consumer brands (including Microsoft, Oracle, and Facebook), with the company's website saying that "48 of the Fortune 50 rely on F5."

F5's Big-IP ADC is used by Fortune 500 firms, governments, and banks all around the world, and, last month, more than 8,000 such devices were found to be vulnerable to attacks designed to exploit this vulnerability.

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:

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.

Security News Digest
Information Security Branch

BRITISH COLUMBIA OCIO | Office of the Chief Information Officer