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

September 22nd, 2020

Try our September - ‘Passwords’ Quiz

This week’s stories:

- **SFU ransomware attack exposed data from 250,000 accounts, documents show** 🇨🇦
- **Suspicious activity found on 48,000 CRA accounts after cyberattacks: treasury board** 🇨🇦
- **The perils of privacy breaches by hospital employees** 🇨🇦
- **NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management (Preliminary Draft)**
- **“Zerologon” Continues to Reverberate, as Gov’t Scrambles to Patch**
- **SEC Issues New Risk Alert on “Credential Stuffing” Attacks**
- **Leading U.S. laser developer IPG Photonics hit with ransomware**
- **This Russian Facial Recognition Startup Plans To Take Its ‘Aggression Detection’ Tech Global With $15 Million Backing From Sovereign Wealth Funds**
- **Police Open Homicide Probe Into Hospital Hack After Woman Dies**
- **U.S. charges Chinese Winnti hackers for attacking 100+ companies**
- **Hacking Group Used Malware to Bypass 2FA on Android Devices**

SFU ransomware attack exposed data from 250,000 accounts, documents 🇨🇦

https://www.cbc.ca/news/canada/british-columbia/sfu-ransomware-attack-1.5732027

The Treasury Board of Canada says it has uncovered suspicious activities on more than 48,000 Canada Revenue Agency accounts following cyberattacks in July and August.

The treasury says the previously announced attacks targeted CRA accounts and GCKey, an online portal through which Canadians access employment insurance and immigration services.

.

Click link above to read more

Suspicious activity found on 48,000 CRA accounts after cyberattacks: treasury 🇨🇦

https://www.cbc.ca/news/politics/cyber-attack-cra-1.5729230

IPG Photonics, a leading U.S. developer of fiber lasers for cutting, welding, medical use, and laser weaponry has suffered a ransomware attack that is disrupting their operations.

Based out of Oxford, Massachusetts, IPG Photonics has locations worldwide where they employ over 4,000 people and have a $1.3 billion revenue in 2019.

Click link above to read more

The perils of privacy breaches by hospital employees 🇨🇦

https://hospitalnews.com/the-perils-of-privacy-breaches-by-hospital-employees/

Canadian privacy laws contain a basic safeguarding principle: access to personal information may only be granted on a need-to-know basis. Snooping violates that principle.

Several Ontario arbitrators have upheld a “zero tolerance” approach for #privacy breaches at hospitals, holding that summary dismissal is the appropriate remedy for deliberate breaches of confidentiality and workplace codes of conduct by hospital employees who snoop into patient records for their own reasons, rather than for any legitimate purpose.

Click link above to read more

NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management (Preliminary Draft)

https://csrc.nist.gov/publications/detail/white-paper/2019/09/09/nist-privacy-framework-preliminary-draft/draft

Announcement

NIST seeks comments on the Preliminary Draft of the "NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management" (“Preliminary Draft”). The Preliminary Draft was developed by NIST using information collected through the Request for Information (RFI) that was published in the Federal Register on November 14, 2018, and a series of open public workshops and webinars. NIST developed the Preliminary Draft in collaboration with public and private stakeholders.

Click link above to read more

“Zerologon” Continues to Reverberate, as Gov’t Scrambles to Patch

https://www.cbronline.com/news/windows-server-vulnerability-zerologon

The impact of a devastating Windows Server vulnerability dubbed “Zerologon” — ostensibly patched by Microsoft on August 11 — continues to reverberate, with the US Cybersecurity and Infrastructure Security Agency (CISA) warning US government agencies Friday that they have four-days to implement the patch.

That CISA feels it needs to do so — over a month after the CVSS 10-rated bug was fixed by Microsoft in a software update — is itself a worrying sign that critical patches are not being widely implemented across the government estate. (The patch is a temporary mitigation, with a full fix not due until early 2021. Several end-users have warned that the fix breaks other critical programmes, including VPNs).

Click link above to read more

SEC Issues New Risk Alert on “Credential Stuffing” Attacks

https://www.jdsupra.com/legalnews/sec-issues-new-risk-alert-on-credential-47285/

On September 15, 2020, the SEC's Office of Compliance Inspections and Examinations (OCIE) issued a Risk Alert highlighting the recent uptick in "credential stuffing" cyber-attacks against SEC-registered investment advisors and broker dealers.

Credential stuffing is an automated cyber-attack on Internet-based user accounts and firm networks. Attackers obtain usernames and passwords from the dark web and then employ automated scripts utilizing the compromised information to attempt to log in and gain unauthorized access to other customer accounts and firm networks. Credential stuffing has proven to be a more effective way for hackers to gain access to accounts and firm systems than traditional brute force password attacks have been. If the credential stuffing attack is successful, attackers can gain access to and control over customer assets and confidential information.

Click link above to read more

Leading U.S. laser developer IPG Photonics hit with ransomware

https://www.bleepingcomputer.com/news/security/leading-us-laser-developer-ipg-photonics-hit-with-ransomware/

IPG Photonics, a leading U.S. developer of fiber lasers for cutting, welding, medical use, and laser weaponry has suffered a ransomware attack that is disrupting their operations.

Based out of Oxford, Massachusetts, IPG Photonics has locations worldwide where they employ over 4,000 people and have a $1.3 billion revenue in 2019.

Click link above to read more

This Russian Facial Recognition Startup Plans To Take Its 'Aggression Detection' Tech Global With $15 Million Backing From Sovereign Wealth Funds

https://www.forbes.com/sites/thomasbrewster/2020/09/22/this-russian-facial-recognition-startup-plans-to-take-its-aggression-detection-tech-global-with-15-million-backing-from-sovereign-wealth-funds/#5f8564924b9e

Next year, in cities across the world, expect to have your face scanned for levels of aggression. NtechLab, a Russian facial recognition company best known for the FindFace app once labelled the harbinger for the end of online privacy, says it's currently testing "aggression detection" tech with plans for a full rollout to its surveillance partners and customers in 2021.

Click link above to read more

Police Open Homicide Probe Into Hospital Hack After Woman Dies

https://www.silicon.co.uk/workspace/ransomware-attack-hospital-347839

German police have opened a homicide investigation into a hacking incident that shut down the computer systems of a Düsseldorf hospital after a woman died.

Malware installed by hackers began affecting the systems of Düsseldorf University Hospital (UKD) in the early hours of 10 September, making the facility's IT systems largely unusable, UKD said in an advisory.

Click link above to read more

U.S. charges Chinese Winnti hackers for attacking 100+ companies

https://www.bleepingcomputer.com/news/security/us-charges-chinese-winnti-hackers-for-attacking-100-

plus-companies/

The U.S. Department of Justice announced today charges against five Chinese nationals fort cyberattacks on more than 100 companies, some of them being attributed to state-backed hacking group APT41.

APT41 is one of the oldest threat groups, known primarily for cyber-espionage operations against a variety of entities, including software developers, gaming companies, hardware manufacturers, think tanks, telcos, social, universities, or foreign governments.

Click link above to read more

Hacking Group Used Malware to Bypass 2FA on Android Devices

https://threatpost.com/google-play-bans-stalkerware/159328/

A recently uncovered hacking group that has targeted Iranian dissidents for several years has developed malware that can bypass two-factor authentication protection on Android devices to steal passwords, according to a paper published by Check Point Research on Friday.

The hacking group, which Check Point researchers call "Rampant Kitten," also has developed other malicious tools used to steal information and personal data from Windows devices and Telegram accounts, according to the report.

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