June 9th, 2020

Try our June - Connect with Care Quiz

This week's stories:

- CPA Canada breach put 329,000 accounting pros at risk
- Canadian organizations lag global firms in cybersecurity maturity, finds EY
- B.C. health data privacy exemptions extended to December 31
- Don't fall for this VPN scam, huge attacks on WordPress sites …
- Android: Why this photo is bricking some phones
- China and Iran Tried to Hack the Biden and Trump Campaigns
- TrickBot Adds BazarBackdoor to Malware Arsenal
- Cisco Confirms 5 Serious Security Threats To 'Tens Of Millions' Of Network Devices
- Can Governments Defeat Nation-State Attacks on Critical Infrastructures?
- Vulnerabilities in popular open source projects doubled in 2019
- Office 365 users: Beware of fake company emails delivering a new VPN configuration
- New ransomware trends spotted: Auctioning stolen files, cybergangs joining forces
- Honda's global operations hit by cyber-attack

CPA Canada breach put 329,000 accounting pros at risk

https://www.scmagazine.com/home/security-news/data-breach/cpa-canada-breach-put-329000-accounting-pros-at-risk/

A breach at Charter Professional Accountants of Canada (CPA Canada) by an unauthorized third party exposed the personal information of 329,000 individuals.

"329,000 professionals are now at risk of sustained attacks, and therefore their clients are at risk," said Colin Bastable, CEO of Lucy Security. "Accounting firms' numbers of clients can range from the tens to the hundreds – these clients are where the money is. Expect to see multiple CEO fraud, business email compromise (BEC) fraud, ransomware attacks and ongoing phishing attacks against the accountants and, subsequently, their clients."

Click link above to read more

Canadian organizations lag global firms in cybersecurity maturity, finds EY

https://www.consulting.ca/news/1695/canadian-organizations-lag-global-firms-in-cybersecurity-maturity-finds-ey

Canadian organizations trail global firms in cybersecurity maturity, according to EY's Global Information Security Survey (GISS). Thirty-four percent of Canadian businesses said they have not articulated their cybersecurity risks, compared to only 16% of global respondents, the survey of 1,300 C-suite and IT leaders found.

In order for Canadian companies to catch up to their global peers and thrive amid disruption – including a huge shift to digital infrastructure and remote work in the pandemic era – EY recommends embracing "security by design," which integrates risk thinking at the initiation of any new product, service, or project.

Click link above to read more

B.C. health data privacy exemptions extended to December 31

https://biv.com/article/2020/06/bc-health-data-privacy-exemptions-extended-december-31

Minister of Citizens Services Anna Kang initially ordered that people's health information might be shared with others inside and outside of Canada. Kang extended that to December 31 in an order issued June 3.

For B.C.'s Information and Privacy Commissioner, however, the situation presents a problem in that his office does not have the legislated power to fine companies handling such data should it be misused.

Click link above to read more

Don't fall for this VPN scam, huge attacks on WordPress sites …

https://www.itworldcanada.com/article/cyber-security-today-dont-fall-for-this-vpn-scam-huge-attacks-on-wordpress-sites-and-lessons-from-a-data-breach/431729

Criminals are taking advantage of the increasing use of virtual private network software by people working at home to spread malware. A VPN may be required by employers for safely logging into company applications. Knowing that, hackers are sending targeted email to people pretending to be from the IT department of their employer. The message suggests the included link is for a VPN software update. To get it the victim is asked to click on the link and log in. But according to a security firm called Abnormal Security, which discovered the scam, the link goes to an Office 365 website that captures the victim's username and password. Some 15,000 fake update messages have gone to Office 365 users.

Click link above to read more

Android: Why this photo is bricking some phones

https://www.bbc.com/news/technology-52891650

Several brands seem to be affected, including Samsung and Google's Pixel.
The bug makes the screen turn on and off continuously. In some cases, a factory reset is required.

The BBC does not recommend trying it out.

Samsung is due to roll out a maintenance update on 11 June. The BBC has contacted Google for comment but not yet had a response.

Click link above to read more

China and Iran Tried to Hack the Biden and Trump Campaigns

https://searchsecurity.techtarget.com/news/252484260/Chinese-Iranian-hackers-targeted-Trump-and-Biden-campaigns

Google announced Thursday that state-sponsored Chinese and Iranian hackers targeted campaign staff of both Joe Biden and President Donald Trump in recent election attacks.

In a series of posts on Twitter, Shane Huntley, director of Google's Threat Analysis Group (TAG), detailed the recent attempts by advanced persistent threat (APT) groups to compromise both presidential campaigns through phishing attacks, which he said were unsuccessful.

Click link above to read more

TrickBot Adds BazarBackdoor to Malware Arsenal

https://threatpost.com/trickbot-bazarbackdoor-malware-arsenal/156243/

A new module for the infamous trojan known as TrickBot has been deployed: A stealthy backdoor that researchers call “BazarBackdoor.”

The binary was first spotted being delivered as part of a phishing campaign that began in March, according to an analysis from Panda Security this week. The campaign used the legitimate marketing platform Sendgrid

to reach targets in a mass-mailing fashion; however, the emails were well-crafted, with the operators making an effort to make the phishing links inside the emails look legitimate. The link addresses also corresponded to the emails’ lures, researchers said

Click link above to read more

Cisco Confirms 5 Serious Security Threats To ‘Tens of Millions’ Of Network Devices

https://www.forbes.com/sites/daveywinder/2020/02/05/cisco-confirms-5-serious-security-threats-to-tens-of-millions-of-network-devices/#2d775f0e13e8

A total of five high-rated Cisco vulnerabilities, dubbed collectively as CDPwn, have been confirmed today. With Cisco network devices everywhere from the trading floor to the boardroom, this is one security alert you can't afford to ignore.

Let’s face it, the last few weeks have been pretty depressing from the security perspective. The travel industry got caught in the ransomware crosshairs, a threat which returned to haunt those businesses which hadn’t patched their systems against a widely discussed Citrix vulnerability.

Click link above to read more

Can Governments Defeat Nation-State Attacks on Critical Infrastructures?

https://threatpost.com/can-governments-defeat-nation-state-attacks-on-critical-infrastructures/156338/

The one cyber risk that governments are much better at controlling than we are is insider threats. Governments have been dealing with people threats for centuries and have powerful tools at their disposal for such investigations.

For physical conflicts, we expect our government to protect us from nation-state adversaries. It turns out, though, that industrial enterprises are much better positioned to defeat most nation-state attacks on power plants, pipelines, and other critical infrastructures than governments are.

Click link above to read more

Vulnerabilities in popular open source projects doubled in 2019

https://www.zdnet.com/article/vulnerabilities-in-popular-open-source-projects-doubled-in-2019/

A study that analyzed the top 54 open source projects found that security vulnerabilities in these tools doubled in 2019, going from 421 bugs reported in 2018 to 968 last year.

According to RiskSense's "The Dark Reality of Open Source" report, released today, the company found 2,694 bugs reported in popular open source projects between 2015 and March 2020.

Click link above to read more

Office 365 users: Beware of fake company emails delivering a new VPN configuration

https://www.helpnetsecurity.com/2020/06/04/office-365-users-beware-of-fake-company-emails-delivering-a-new-vpn-configuration/

Yet another Office 365 phishing campaign.

“The sender email address is spoofed to impersonate the domain of the targets’ respective organizations. The link provided in the email allegedly directs to a new VPN configuration for home access. Though the link appears to be related to the target’s company, the hyperlink actually directs to an Office 365 credential phishing website,” Abnormal Security explained.

Click link above to read more

New ransomware trends spotted: Auctioning stolen files, cybergangs joining forces

https://www.scmagazine.com/home/security-news/ransomware/new-ransomware-trends-spotted-auctioning-stolen-files-cybergangs-joining-forces/

The tactics of human-operated ransomware campaigns continue to escalate. Victims who previously feared having their systems disrupted, their files encrypted and their data stolen and published online may now face another ultimatum: Pay up or have your data auctioned off to the highest bidder.

Click link above to read more

Honda's global operations hit by cyber-attack

https://www.bbc.com/news/technology-52982427

Honda has said it is dealing with a cyber-attack that is impacting its operations around the world. "Honda can confirm that a cyber-attack has taken place on the Honda network," the Japanese car-maker said in a statement.

It added that the problem was affecting its ability to access its computer servers, use email and otherwise make use of its internal systems.

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