Security Digest
Information Security Branch

BRITISH COLUMBIA

OCIO
Office of the Chief Information Officer

June 26th, 2018

June is IoT (Internet of Things) Month

Take our monthly quiz and test your knowledge

This week's stories:

Rhode Island woman's selfie shows up on stranger's phone due to possible iPhone glitch

https://globalnews.ca/news/4293086/iphone-glitch-selfie-strangers-phone-rhode-island/

Providence, R.I.-based Alicia White was stumped this week when six photos of her and her fiance stored in her iPhone account wound up on a Connecticut-based stranger's phone.

According to reporting from Eyewitness news, White took the photos about three weeks ago, but on Wednesday received a text from a friend with a screenshot from a Snapchat video.

"Help, does anyone know who these people are and why six pictures of them randomly appeared on my camera roll this morning?" the caption on the snap read.

Click link above to read more

Facebook brings its messaging app for kids to Canada despite experts' concerns

http://www.cbc.ca/news/technology/facebook-messenger-kids-launches-canada-1.4717944

A version of Facebook's popular text and video messaging app aimed at children under the age of 13 is now available in Canada, Facebook said on Friday, despite concerns from advocates that children are ill-equipped to use social media at such a young age.

Messenger Kids was first made available in the United States at the end of last year, and has been pitched as a means for parents to let their kids chat with close friends and family in a safer and more controlled environment than other messaging apps.

However, Messenger Kids has attracted criticism from some experts who argue that young children are not yet able to navigate the complexities of privacy and social etiquette online, and that an increase in screen time could interfere with the development of healthy relationship skills that otherwise come from face-to-face interactions.

Click link above to read more

U.S. adopts digital-era privacy rules to regulate how phone companies track

https://globalnews.ca/news/4293007/privacy-rules-regulate-phone-company-tracking/

Police generally need a warrant to look at records that reveal where cellphone users have been, the Supreme Court ruled Friday in a big victory for privacy interests in the digital age.

The justices' 5-4 decision marks a big change in how police may obtain information that phone companies collect from the ubiquitous cellphone towers that allow people to make and receive calls, and transmit data. The information has become an important tool in criminal investigations.

Click link above to read more

Micro-targeting: How Facebook is selling you to advertisers

https://globalnews.ca/news/4293050/micro-targeting-facebook-selling-you/

The U.K.'s Information Commissioner, Canadian Elizabeth Denham, issued a warning earlier this year to anyone with a social media account: You are what you click.

Denham warned of the rise of online "micro-targeting," a marketing strategy that involves turning a social media profile into a psychological profile, in order to create specifically targeted advertisements.

Micro-targeting has become a popular tool for both businesses and political campaigns to sell products and win votes. And psychologists say the information gleaned from someone's online profile can allow advertisers to know someone better than their own spouse.

Click link above to read more

Alexa, I can trust you with my checkbook, right?

https://www.canadiansecuritymag.com/news/data-security/alexa-i-can-trust-you-with-my-checkbook-right

Big banks and financial companies have started to offer banking through virtual assistants — Amazon's Alexa, Apple's Siri, and Google's Assistant — in a way that will allow customers to check their balances, pay bills and, in the near future, send money just with their voice. And with the rapid adoption of Zelle, a bank-to-bank transfer system, it soon could be possible to send money to friends or family instantly with voice commands.

But the potential to do such sensitive tasks through a smart speaker raises security concerns. Virtual assistants and smart speakers are still relatively new technologies, and potentially susceptible to being exploited by cyber criminals.

Regional banking giant U.S. Bank is the first bank to be on all three services — Alexa, Siri and Assistant. The company did a soft launch of its Siri and Assistant services in early March and this month started marketing the option to customers.

Click link above to read more

Apple strikes blow to Facebook as it clamps down on data harvesting

https://www.theguardian.com/technology/2018/jun/13/apple-facebook-privacy-data-harvesting-onavo-app-store

Apple has updated its rules to restrict app developers' ability to harvest data from mobile phones, which could be bad news for a Facebook-owned data security app called Onavo Protect.

Onavo ostensibly provides users with a free virtual private network (VPN) which, it claims, helps "keep you and your data safe when you browse and share information on the web". What is not immediately obvious is that it feeds information to Facebook about what other apps you are using and how much you are using them back to the social networking giant.

"The problem with Onavo is that it talks about being a VPN that keeps your data private, but behind the scenes it's harvesting your data for Facebook," said Ryan Dochuk, CEO of the paid-for VPN TunnelBear. "It goes against what people generally expect when they use a VPN."

Onavo has been a Trojan horse for Facebook (in the classical sense, not as malware), allowing it to gather intelligence on the apps people use on tens of millions of devices outside its empire. This real-time market research highlights which apps are becoming popular and which are struggling. Such competitive intelligence can inform acquisition targets and negotiations as well as identify popular features it could copy in rival apps.

Click link above to read more

Thousands of Apps Leak Sensitive Data via Misconfigured Firebase Backends

https://www.bleepingcomputer.com/news/security/thousands-of-apps-leak-sensitive-data-via-misconfigured-firebase-backends/

Thousands of iOS and Android mobile applications are exposing over 113 GBs of data via over 2,271 misconfigured Firebase databases, according to a report released this week by mobile security firm Appthority.

Firebase is a Backend-as-a-Service offering from Google that contains a vast collection of services that mobile developers can use in the creation of mobile and web-based apps.

The service is insanely popular with top Android devs, providing cloud messaging, push notifications, database, analytics, advertising, and a bunch more of other backends and APIs that they can easily plug into their projects and benefit from Google's large-scale and high-performance systems within their apps.

Click link above to read more

Someone Is Taking Over Insecure Cameras and Spying on Device Owners

https://www.bleepingcomputer.com/news/security/someone-is-taking-over-insecure-cameras-and-spying-on-device-owners/

Many brands of webcams, security cameras, pet and baby monitors, use a woefully insecure cloud-based remote control system that can allow hackers to take over devices by performing Internet scans, modifying the device ID parameter, and using a default password to gain control over the user's equipment and its video stream.

In the last nine months, two security firms have published research on the matter. Both pieces of research detail how the camera vendor lets customers use a mobile app to control their device from remote locations and view its video stream

Click link above to read more

Widely used D-Link modem/router under mass attack by potent IoT botnet

https://arstechnica.com/information-technology/2018/06/widely-used-d-link-modemrouter-under-mass-attack-by-potent-iot-botnet/

Malicious hackers are mass exploiting a critical vulnerability in D-Link DSL routers in an attempt to make them part of Satori, the potent Internet-of-things botnet that is used to take down websites and mine digital coins, researchers said.

Since making its debut late last year, Satori has proven to be a particularly versatile and sophisticated botnet. It made a name for itself in December when it infected more than 100,000 Internet-connected devices in just 12 hours by exploiting remote code-execution vulnerabilities in Huawei and RealTek routers. A month later, Satori operators released a new version that infected devices used to mine digital coins, proving that the IoT botnet could also take control of more traditional computing devices. In February, Satori resurfaced when it infected tens of thousands of routers manufactured by Dasan Networks.

Click link above to read more

Hackers who sabotaged the Olympic games return for more mischief

https://arstechnica.com/information-technology/2018/06/hackers-who-sabotaged-the-olympic-games-return-for-more-mischief/

The advanced hacking group that sabotaged the Pyeongchang Winter Olympics in February has struck again, this time in attacks that targeted financial institutions in Russia and chemical- and biological-threat prevention labs in France, Switzerland, the Netherlands, and Ukraine, researchers said.

The new campaigns began last month with spear-phishing emails that were designed to infect targeted companies with malware that collected detailed information about their computers and networks. One of the malicious Word documents referred to Spiez Convergence, a biochemical threat conference that's organized by the Spiez Laboratory, which played a key role in the investigation of the poisoning in March of a former Russian spy in the UK. UK government officials have said Russia was behind the poisoning. A second document targeted health and veterinary control authorities in Ukraine.

Researchers from Moscow-based Kaspersky Lab said that documents in the phishing emails closely resemble those used to infect organizers, suppliers, and partners of the Winter Olympic Games in the months preceding the February Pyeongchang attack. These initial infections allowed the attackers to spend months developing detailed knowledge of the networks supporting the games. One of the key reasons the malware dubbed Olympic Destroyer was so successful in disrupting the Olympics was that it used this knowledge to sabotage the networks. The discovery of a new phishing campaign by the same group raises the possibility that they are intended to support new sabotage hacks.

Click link above to read more

Med Associates breach leaves 270,000 patient records at risk

https://hotforsecurity.bitdefender.com/blog/med-associates-breach-leaves-270000-patient-records-at-risk-20052.html

Med Associates has suffered a data breach that may have directed patient names and insurance information into the wrong hands. Hackers could use the data for medical fraud, the company said.

On its About page, Med Associates Inc. describes itself as a manufacturer, software developer, and supplier of products for behavioral psychology, pharmacology, neuroscience, and related fields of research.

On March 22, the company's staff noticed "unusual activity" at an employee's workstation, so Med Associates began investigating with its IT vendor and a third-party forensics firm.

"It was determined that the unauthorized party accessed the workstation and through that, may have had access to certain personal and protected information," reads the press release.

The group said they found no evidence that any patient information was specifically accessed or used in any way, but if an attacker did obtain any information through the privileges assigned to that terminal, it would include patient names, dates of birth, addresses, dates of service, diagnosis codes, procedure codes and insurance information (including insurance ID Number). Med Associates acknowledges that a bad actor could use this data for fraud.

Times Union, a New York-based publication, reports impacted patients number 270,000.

The company has since implemented higher security standards and has increased staff training on data privacy and security. While the group doesn't say it was human error that led to the breach, the wording certainly implies it.

Click link above to read more

Black River Medical Center employee falls for phishing scam; breach ensues

https://hotforsecurity.bitdefender.com/blog/black-river-medical-center-employee-falls-for-phishing-scam-breach-ensues-20049.html

Black River Medical Center has issued a notice informing customers that the healthcare provider has learned of a data security lapse that may have resulted in the exposure of some patients' personal information.

An affiliate of Saint Francis Healthcare System, Black River is a community-owned, not-for-profit hospital in Missouri, US. On April 23, the hospital discovered that a staffer fell for a phishing scam and had his / her email account compromised. From there, the attacker could use those credentials to access sensitive patient information.

"The investigation determined that an unknown, unauthorized third party gained access to the employee's email account and could have viewed or accessed the information contained therein, which included patients' names, addresses and phone numbers, and in certain instances, limited treatment information," the notice reads.

Click link above to read more

Evasive MyloBot botnet can take over enterprise devices to steal data, spread ransomware

https://securityledger.com/2018/06/highly-evasive-new-botnet-can-take-over-enterprise-

A new, extremely evasive botnet has been discovered that takes unique leverage of command and control servers and can completely take over an enterprise device to execute any type of code it wishes, from ransomware to trojans to data extraction, according to researchers at endpoint and mobile security firm Deep Instinct.

The malware–which is complex in nature and has the potential to cause extreme damage to enterprises by spreading ransomware and stealing data–also is evidence of how hackers are using dark markets to spread malicious software and carry out other types of cyber crime, Tom Nipravsky, Deep Instinct security researcher, said in a blog post revealing the botnet, called MyloBot.

About two and a half months ago, Deep Instinct researchers discovered the botnet on one of their client's devices, which they didn't identify specifically but said is from a "top data communication and telecommunication equipment manufacturer."

Click link above to read more

Smart home devices are being used in domestic abuse, report finds

https://www.digitaltrends.com/home/smart-home-domestic-abuse/

The New York Times conducted more than 30 interviews with domestic abuse victims, lawyers, shelter workers, and emergency responders, who noted that Internet of Things devices were leveraged for purposes beyond the manufacturers' intentions. For example, abusers would reportedly control objects in their or their victim's home, watching and listening to conversations and comings and goings, or in some cases, using them to "scare of show power."

In some cases, the abusers would cause loud bursts of music to suddenly play, change the lighting, turn on or off heating or cooling units, or otherwise make a home seemingly act of its own accord.

Much of the challenge in addressing this new cycle of abuse, the Times notes, is that there is still a lack of knowledge generally speaking when it comes to how to operate many of these IoT devices.

"People have started to raise their hands in trainings and ask what to do about this," Erica Olsen, director of the Safety Net Project at the National Network to End Domestic Violence, told the Times. She further noted that she was reticent to discuss the abuse of smart technology because "we don't want to introduce the idea to the world, but now that it's become so prevalent, the cat's out of the bag."

Even within a single household, it's often the case that only one individual installs and otherwise controls the smart home device, creating a power dynamic that can be exploited if things turn sour.

Click link above to read more

Click Unsubscribe to stop receiving the Digest.

****

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:
Information Security Awareness Team - Information Security Branch
Office of the Chief Information Officer,
Ministry of Citizens' Services
4000 Seymour Place, Victoria, BC V8X 4S8
http://gov.bc.ca/informationsecurity
OCIOSecurity@gov.bc.ca