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

June 11th, 2019

Try our June quiz – Smart Cities

Get Ready for Security Day - June 13, 2019

This years Security Day topic is “Smart Cities” To view the webcast follow this link at 8:30 am on June 13th, no registration is required, there will also be a major prize drawn!

This week’s stories:

- **DIACC releases first model of Canadian digital trust framework as companies show off solutions 🇨🇦**
- **National Research Council opens cyber security research hub at University of New Brunswick🇨🇦**
- **Keylogger, vulnerable server-led to Cathay Pacific Airlines breach**
- **Facebook won’t allow its apps to be pre-installed on Huawei devices**
- **New Spam Campaign Controlled by Attackers via DNS TXT Records**
- **Gaming Site Emuparadise Suffered Data Breach of 1.1M Accounts**
- **New Extortion Scam Threatens to Ruin a Website's Reputation**
- **GoldBrute Botnet Brute-Force Attacking 1.5M RDP Servers**
- **Traveler Photos Were Stolen And Exposed In A US Customs And Border Protection Database Breach**
- **Baltimore Ransomware Attack Costing City $18 Million**
- **Hospital to Pay $250,000 After Alleged False HITECH Claims**

DIACC releases first model of Canadian digital trust framework as companies show off solutions

https://www.itworldcanada.com/article/diac-releases-first-model-of-canadian-digital-trust-framework-as-companies-show-off-solutions/418769

Later this summer the Niagara Health regional authority will launch a mobile medical app which will eventually let area residents access their health records online.

Called Niagara Health Navigator, the launch version will have modest functionality: The ability to get current emergency room wait times, news and social media feeds from the Southern Ontario region’s 12 hospitals and clinics, and the ability to leave a thank-you to a health care worker.

Click link above to read more

National Research Council opens cyber security research hub at University of New Brunswick

https://www.itworldcanada.com/article/national-research-council-opens-cyber-security-research-hub-at-university-of-new-brunswick/418868

The University of New Brunswick's Canadian Institute for Cybersecurity has another partner: The National Research Council said Monday it has opened a new hub in its facility on the Fredericton campus to jointly work on research.

Called the Canadian Institute for Cybersecurity-NRC Cybersecurity Collaboration Consortium (CNCCC), the partners hope it will lead to discoveries and advances in cybersecurity including publications, patents, the commercialization of technology, as well as provide training opportunities for graduate students and post-doctoral fellows.

Click link above to read more

Keylogger, vulnerable server-led to Cathay Pacific Airlines breach

https://www.information-age.com/why-the-uk-must-invest-cyber-security-123483140/

Too many businesses consider security as the last stage of transformation. They build the castle and then add the moat. But security is not a distinct layer that can be dropped on top of existing operations. It is not a switch to flip. It needs to be woven into culture and processes as early as possible.

Click link above to read more

Facebook won't allow its apps to be pre-installed on Huawei devices

https://beta.theglobeandmail.com/business/technology/article-facebook-wont-allow-its-apps-to-be-pre-installed-on-huawei-devices/

Facebook Inc. is no longer allowing pre-installation of its apps on Huawei phones, the latest blow for the Chinese tech giant as it struggles to keep its business afloat in the face of a U.S. ban on its purchase of U.S. parts and software.

Customers who already have Huawei phones will still be able to use its apps and receive updates, Facebook told Reuters. But new Huawei phones will no longer be able to have Facebook, WhatsApp and Instagram apps pre-installed.

Click link above to read more

New Spam Campaign Controlled by Attackers via DNS TXT Records

https://www.bleepingcomputer.com/news/security/new-spam-campaign-controlled-by-attackers-via-dns-txt-records/

A new finance spam campaign with HTML attachments has been discovered that utilizes Google's public DNS resolver to retrieve JavaScript commands embedded in a domain's TXT record. These commands will then redirect a user's browser to an aggressive trading advertisement site, which has been reported as a scam.

According to MyOnlineSecurity.com, who discovered this campaign, it is being targeted at people in the United Kingdom and the associated IP addresses have previously been utilized by the Necurs botnet.

Click link above to read more

Gaming Site Emuparadise Suffered Data Breach of 1.1M Accounts

https://www.bleepingcomputer.com/news/security/gaming-site-emuparadise-suffered-data-breach-of-11m-accounts/

The Emuparadise retro gaming site has been reported to have suffered a data breach in April 2018. This breach exposed account information for approximately 1.1 million Emuparadise forum members.

Emuparadise is a retro gaming site that used to host ROMs for retro games that could be used in emulators. In August 2018, Emuparadise decided to no longer host game ROMs, but continued as a retro gaming database with community forums.

Click link above to read more

New Extortion Scam Threatens to Ruin a Website's Reputation

https://www.bleepingcomputer.com/news/security/new-extortion-scam-threatens-to-ruin-a-websites-reputation/

A new extortion scam campaign is underway that is targeting websites owners and stating that if they do not make a payment, the attacker will ruin their site's reputation and get them blacklisted for spam.

We all know, or should know, about the sextortion emails people are receiving where the sender states they have hacked the recipient's computer and taped them doing things while on adult sites. Since then, further extortion scams were created that pretend to be the CIA, bomb threats, and even from hitmen asking you to pay them to call off their hit.

Click link above to read more

GoldBrute Botnet Brute-Force Attacking 1.5M RDP Servers

https://www.databreachtoday.com/goldbrute-botnet-brute-force-attacking-15m-rdp-servers-a-12595

A new botnet dubbed GoldBrute is using brute-force or credential-stuffing methods to attack vulnerable Windows machines that have exposed Remote Desktop Protocol connections, according to new research from Morphus Labs.

While the end-goal of the group controlling the botnet is not clear, it appears that GoldBrute is currently using brute-force methods to attack about 1.5 million Remote Desktop Protocol servers that have exposed connections to the open internet, Renato Marinho, the chief research officer with Morphus, writes in blog published Thursday.

Click link above to read more.

Traveler Photos Were Stolen And Exposed In A US Customs And Border Protection Database Breach

https://www.buzzfeednews.com/article/daveyalba/the-us-governments-database-of-traveler-photos-has-been

A subcontractor with the US Customs and Border Protection agency has suffered a data breach that has exposed the photos of travelers and vehicles traveling in and out of the United States. The database, which could include passport and visa photos being used in an airport facial recognition program, also stores photos of people’s license plates.

In a Monday statement, the agency said that a copy of its database of traveler photos and license plate images had been "compromised by a malicious cyber-attack."

Click link above to read more

Baltimore Ransomware Attack Costing City $18 Million

https://www.databreachtoday.com/baltimore-ransomware-attack-costing-city-18-million-a-12584

A month after Baltimore's IT system was hit with ransomware, local officials expect the attack to cost the city $18 million in recovery costs and lost revenue, although that number could increase in the coming months as systems are brought back online and a federal investigation continues.

At a press conference this week, City Finance Director Henry Raymond offered some preliminary details about the cost to the city so far. In his estimate, Baltimore has spent about $10 million in recovery and forensic expenses, and the city is expected to lose about $8 million in revenue.

Click link above to read more

Hospital to Pay $250,000 After Alleged False HITECH Claims

https://www.databreachtoday.com/hospital-to-pay-250000-after-alleged-false-hitech-claims-a-12569

A Kansas hospital has agreed to pay $250,000 to settle allegations that it falsely attested to conducting a security risk analysis as required under the HITECH Act electronic health records financial incentives program. Two whistleblowers in the case - the hospital's former CIO and corporate compliance officer - who filed a lawsuit under the federal False Claims Act - will receive $50,000 of the settlement.

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:

Information Security Awareness Team - Information Security Branch

Office of the Chief Information Officer,

Ministry of Citizens' Services

4000 Seymour Place, Victoria, BC   V8X 4S8

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.