June 15, 2021

Challenge yourself with our Phishing quiz!

Register for Security Day: June 23, 2021

This week's stories:

- Canada's border agency urgently developing biometric plans in response to COVID-19
- JBS CEO Says Company Paid $11M in Ransom
- Avaddon ransomware operation shuts down and releases decryption keys
- U.S. Water and Power Are Shockingly Vulnerable to Cyberhacks
- Ransomware gangs are increasingly going after SonicWall devices
- FBI seized Colonial Pipeline ransom using private key
- 26M passwords exposed in Botnet data leak
- Phished Account Credentials Mostly Verified in Hours
- Hackers can mess with HTTPS connections by sending data to your email server
- EA hacked and source code stolen
- Canada police broke law with facial recognition software, regulator finds

---

Canada's border agency urgently developing biometric plans in response to COVID-19

OTTAWA — Canada's border agency is urgently looking to hire a global technology firm to help develop a biometric strategy in response to rapidly evolving issues including COVID-19.

The Canada Border Services Agency issued a notice of procurement today inviting 15 firms to submit proposals for immediately setting up an Office of Biometrics and Identity Management.

The agency also wants a strategy and road map for digital solutions using biometric-related technologies to address issues flowing from the pandemic and other priorities.

https://www.canadiansecuritymag.com/canadas-border-agency-urgently-developing-biometric-plans-in-response-to-covid-19/

Click above link to read more.

Back to top

JBS CEO Says Company Paid $11M in Ransom

The decision to pay attackers was a difficult one, CEO Andre Nogueira said in a statement.

JBS USA, the meat producer recently hit with a ransomware attack, paid the equivalent of $11 million in ransom to attackers, its leadership has confirmed.

Andre Nogueira, CEO of JBS USA, said in a statement that the decision to pay was made after consulting with internal IT professionals and third-party cybersecurity experts. The company made the decision to "mitigate any unforeseen issues related to the attack and ensure no data was exfiltrated." At the time of payment, the vast majority of the company's facilities were operational.

https://www.darkreading.com/attacks-breaches/jbs-ceo-says-company-paid-$11m-in-ransom/d/d-id/1341270

Click above link to read more.

Back to top

Avaddon ransomware operation shuts down and releases decryption keys

The criminal group behind the Avaddon ransomware has shut down its operation today and released decryption keys for past victims.

The keys were made available earlier today via a private message sent to Bleeping Computer, a ransomware support forum and news site that has been covering the ransomware scene since 2016.

The keys have now been shared with Emsisoft, a security firm that has previously released tens of free decryption utilities for all kinds of ransomware strains.

The company expects to release a free decryptor over the weekend, Emsisoft security researcher Michael Gillespie has told The Record in an interview. [Update: Decryptor now live here.]

https://therecord.media/avaddon-ransomware-operation-shuts-down-and-releases-decryption-keys/

Click above link to read more.

Back to top

U.S. Water and Power Are Shockingly Vulnerable to Cyberhacks

When the Los Angeles Department of Water and Power was hacked in 2018, it took a mere six hours. Early this year, an intruder lurked in hundreds of computers related to water systems across the U.S. In Portland, Oregon, burglars installed malicious computers onto a grid providing power to a chunk of the Northwest.

Two of those cases -- L.A. and Portland -- were tests. The water threat was real, discovered by cybersecurity firm Dragos.

https://news.bloomberglaw.com/privacy-and-data-security/u-s-water-and-power-are-shockingly-vulnerable-to-cyberhacks-1

Click above link to read more.

Back to top

Ransomware gangs are increasingly going after SonicWall devices

Over the course of the last few months, cybercrime groups have increasingly targeted SonicWall devices in order to breach corporate networks and deploy ransomware.

The attacks come after enterprise-grade networking equipment from Citrix, F5, Pulse Secure, Fortinet, and Palo Alto Networks was abused in a similar manner across 2019 and 2020, with enterprise VPNs and network gateways representing a popular entry point for ransomware gangs.

https://therecord.media/ransomware-gangs-are-increasingly-going-after-sonicwall-devices/

Click above link to read more.

Back to top

FBI seized Colonial Pipeline ransom using private key

After Colonial Pipeline paid a $4.4 million ransom demand in last month's attack, the DOJ announced the majority of the funds have been retrieved by the FBI.

Using a bitcoin private key, the FBI recovered the majority of the ransom payment made by Colonial Pipeline Co. following a ransomware attack last month.

https://searchsecurity.techtarget.com/news/252502115/FBI-seized-Colonial-Pipeline-ransom-using-private-key

Click above link to read more.

Back to top

26M passwords exposed in Botnet data leak

There's such a surfeit of stolen data floating around on dark web forums that it's overwhelming. Passwords and other credentials collected are bought and sold on an industrial scale.

On Wednesday, a 1.2-terabyte batch of data was highlighted by NordLocker, which is part of the Nord family of security products. NordLocker says the data, which was for sale, was accidently revealed by a hacking group, according to a blog post. It was hosted on a cloud service, which was then notified, and the data was taken down.

https://www.bankinfosecurity.com/blogs/26m-passwords-exposed-in-botnet-data-leak-p-3054

Click above link to read more.

Back to top

Phished Account Credentials Mostly Verified in Hours

Almost two-thirds of all phished credentials are verified by attackers within a day and then used in a variety of schemes, including business email compromise and targeting other users with malicious code.

Attackers from 44 countries used look-alike cloud portals to collect users' credentials, verified the majority of username-password combination in hours, and used them to send malicious payloads and spam to other Internet users and to conduct business email compromise (BEC), email-security firm Agari states in a new report.

https://www.darkreading.com/threat-intelligence/phished-account-credentials-mostly-verified-in-hours/d/d-id/1341240

Click above link to read more.

Back to top

Hackers can mess with HTTPS connections by sending data to your email server

When you visit an HTTPS-protected website, your browser doesn't exchange data with the webserver until it has ensured that the site's digital certificate is valid. That prevents hackers with the ability to monitor or modify data passing between you and the site from obtaining authentication cookies or executing malicious code on the visiting device.

But what would happen if a man-in-the-middle attacker could confuse the browser into accidentally connecting to an email server or FTP server that uses a certificate that's compatible with the one used by the website?

https://arstechnica.com/gadgets/2021/06/hackers-can-mess-with-https-connections-by-sending-data-to-your-email-server/

Click above link to read more.

Back to top

EA hacked and source code stolen

Hackers have stolen valuable information from major game publisher Electronic Arts (EA), the company said.

The attackers claimed to have downloaded source code for games such as FIFA 21 and for the proprietary Frostbite game engine used as the base for many other high-profile games.

https://www.bbc.com/news/technology-57431987

Click above link to read more.

Back to top

Canada police broke law with facial recognition software, regulator finds

The Canadian federal police force broke the law when it used controversial facial recognition software, the country's top privacy regulator found in a report released on Thursday.

The Royal Canadian Mounted Police (RCMP) initially denied that it used Clearview AI, a U.S.-based facial recognition software that cross-references photos with a database of photos posted to social media. In February 2020, the agency said it had been using it for several months.

https://www.reuters.com/technology/canada-privacy-regulator-says-federal-police-broke-laws-using-facial-recognition-2021-06-10/

Click above link to read more.

Back to top