May 18, 2021

Challenge yourself with our Spotting a Fake quiz!

This week's stories:

- Cybersecurity experts say Canadian businesses can learn from U.S. pipeline attack

Exploit released for wormable Windows HTTP vulnerability

Nearly all wi-fi devices are vulnerable to new FragAttacks

Ransomware world in 2021: who, how and why

7 modern-day cybersecurity realities

Defending the castle: how world history can teach cybersecurity a lesson

TeaBot – a new malware that stealing victim's credentials and intercepting SMS messages

SSO explained: How single sign-on improves security and the user experience

DarkSide ransomware explained: How it works and who is behind it

Five critical password security rules your employees are ignoring

Cybersecurity: what is truly essential?

Phishers using Zix to "legitimize" emails in the eyes of Office 365 users

Cyber attack 'most significant' on Irish state

FBI warns of cybercriminals abusing search ads to promote phishing sites

Ransomware crooks post cops' psych evaluations after talks with DC police stall

U.S. Intelligence Agencies Warn about 5G

Victim of Elon Musk bitcoin scam loses home deposit

Thousands of patient records exposed after ransomware attack on CaptureRx

Cybersecurity experts say Canadian businesses can learn from U.S. pipeline attack

Canada's two largest pipeline companies say they have taken a proactive approach to avoid the type of cyberattack that has disrupted gasoline supplies in the U.S. Southeast and contributed to higher retail gasoline prices across North America.

Hackers were able to seize control of computer systems for the Colonial Pipeline, locking access, and demanding a ransom to release them. Partial service was restored manually late Monday but a full recovery isn't expected to be complete until the weekend.

TC Energy and Enbridge, both based in Calgary, say they regularly take precautions including technology and training to protect their operations from cyberattacks.
https://www.canadiansecuritymag.com/cybersecurity-experts-say-canadian-businesses-can-learn-from-u-s-pipeline-attack/

Click above link to read more.

Back to top

Exploit released for Windows HTTP vulnerability

Proof-of-concept exploit code has been released over the weekend for a critical wormable vulnerability in the latest Windows 10 and Windows Server versions.

The bug, tracked as CVE-2021-31166, was found in the HTTP Protocol Stack (HTTP.sys) used by the Windows Internet Information Services (IIS) web server as a protocol listener for processing HTTP requests.
https://www.bleepingcomputer.com/news/security/exploit-released-for-wormable-windows-http-vulnerability/

Click above link to read more.

Back to top

Nearly all wi-fi devices are vulnerable to new FragAttacks

Three design and multiple implementation flaws have been disclosed in IEEE 802.11 technical standard that undergirds Wi-Fi, potentially enabling an adversary to take control over a system and plunder confidential data.

Called FragAttacks (short for FRgmentation and AGgregation attacks), the weaknesses impact all Wi-Fi security protocols, from Wired Equivalent Privacy (WEP) all the way to Wi-Fi Protected Access 3 (WPA3), thus virtually putting almost every wireless-enabled device at risk of attack.

"An adversary that is within radio range of a victim can abuse these vulnerabilities to steal user information or attack devices," Mathy Vanhoef, a security academic at New York University Abu Dhabi, said. "Experiments indicate that every Wi-Fi product is affected by at least one vulnerability and that most products are affected by several vulnerabilities."
https://thehackernews.com/2021/05/nearly-all-wifi-devices-are-vulnerable.html

Click above link to read more.

Back to top

Ransomware world in 2021: who, how and why

As the world marks the second Anti-Ransomware Day, there's no way to deny it: ransomware has become *the* buzzword in the security community. And not without good reason. The threat may have been around a long time, but it's changed. Year after year, the attackers have grown bolder, methodologies have been refined and, of course, systems have been breached. Yet, much of the media attention ransomware gets is focused on chronicling which companies fall prey to it. In this report, we take a step back from the day-to-day ransomware news cycle and follow the ripples back into the heart of the ecosystem to understand how it is organized.

First, we will debunk three preconceived ideas that obstruct proper thinking on the ransomware threat. Next, we dive deep into the darknet to demonstrate how cybercriminals interact with each other and the types of services they provide. And finally, we conclude with a look at two high-profile ransomware brands: REvil and Babuk.
https://securelist.com/ransomware-world-in-2021/102169/

Click above link to read more.

Back to top

---

7 modern-day cybersecurity realities

Move to the cloud. Shift left. Buy the latest XDR and deception tools. The technology and cybersecurity industry has always been susceptible to marketing hype, but do these moves actually make their organizations more secure? Or do they just add more complexity?

With all the major hacks, from SolarWinds to the issues with Microsoft Exchange, how can security pros sleep at night? They may think they are doing the right thing, but are they operating with a false sense of security?

Michael Isbitski, technology evangelist at Salt Security, says security pros have to focus more on securing the application programming interfaces (APIs) that power many of these tech strategies. From hosting internal cloud apps to relying on gateways and traditional patch management tools, the old methods don't focus enough on API security – and the APIs are susceptible to attackers.
https://www.darkreading.com/cloud/7-modern-day-cybersecurity-realities/d/d-id/1340826

Click above link to read more.

Back to top

Defending the castle: how world history can teach cybersecurity a lesson

Cybersecurity attackers follow the same principles practiced in warfare for millennia. They show up in unexpected places, seeking out portions of an organization's attack surface that are largely unmonitored and undefended.

Attackers strike where defenders least expect it — in cybersecurity, certainly, but in the world of physical warfare as well. As a former military officer, I think it's particularly instructive to look at military battles from the cybersecurity defender's perspective. Military battles bring direct lessons and, I find, often serve as a

reminder that attack surface blind spots have been an Achilles' heel for defenders for a long time. They remind us that we have to rethink our assumptions, habits, and biases to operate at our best.

One notable example occurred in 1204 at Château Gaillard. The château provided the English a seemingly impenetrable stronghold from which to defend their claim in the Normandy countryside. The base of the keep was built out of natural rock, and all possible approaches were guarded by impressive towers and walls. Undaunted, the French laid siege, and for eight months, continued their constant frontal attack, despite the heavy toll to their forces.
https://www.darkreading.com/vulnerabilities---threats/defending-the-castle-how-world-history-can-teach-cybersecurity-a-lesson/a/d-id/1340944

Click above link to read more.

Back to top

TeaBot – a new malware that stealing victim's credentials and intercepting SMS messages

A new trendy and massive android banking trojan was discovered and analyzed by Cleafy called TeaBot. This Teabot steals the victim's credentials and SMS messages for enabling fraud scenarios against a predefined list of banks.

TeaBot is featured with the following potential:

- Ability to perform Overlay Attacks against multiple banks applications to steal login credentials and credit card information
- Ability to send / intercept / hide SMS messages
- Enable keylogging functionalities
- Ability to steal Google Authentication codes
- Ability to obtain full remote control of an Android device (via Accessibility Services and real-time screen-sharing).

https://cybersecuritynews.com/teabot-malware/

Click above link to read more.

Back to top

SSO explained: How single sign-on improves security and the user experience

Single sign-on (SSO) is a centralized session and user authentication service in which one set of login credentials can be used to access multiple applications. Its beauty is in its simplicity; the service authenticates you on one designated platform, enabling you to then use a plethora of services without having to log in and out each time.

Implemented correctly, SSO can be great for productivity, IT monitoring and management, and security control. With one security token (a username and password pair), an administrator can enable and disable user access to multiple systems, platforms, apps, and other resources. SSO also reduces the risk of lost, forgotten or weak passwords.
https://www.csoonline.com/article/2115776/sso-explained-how-single-sign-on-improves-security-and-the-user-experience.html

Click above link to read more.

Back to top

DarkSide ransomware explained: How it works and who is behind it

DarkSide is a ransomware threat that has been in operation since at least August 2020 and was used in a cyberattack against Georgia-based Colonial Pipeline, leading to a major fuel supply disruption along the East Coast of the US. The malware is offered as a service to different cybercriminals through an affiliate program and, like other prolific ransomware threats, employs double extortion that combines file encryption with data theft and is deployed on compromised networks using manual hacking techniques.
https://www.csoonline.com/article/3618688/darkside-ransomware-explained-how-it-works-and-who-is-behind-it.html

Click above link to read more.

Back to top

Five critical password security rules your employees are ignoring

According to Keeper Security's Workplace Password Malpractice Report, many remote workers aren't following best practices for password security.

Password security was a problem even before the advent of widespread remote work. So, what happened post-pandemic? Keeper Security's Workplace Password Malpractice Report sought to find out. In February 2021, Keeper surveyed 1,000 employees in the U.S. about their work-related password habits — and discovered that a lot of remote workers are letting password security go by the wayside.
https://threatpost.com/5-password-security-rules-employees-ignoring/165686/

Click above link to read more.

Back to top

Cybersecurity: what is truly essential?

My wife and I recently became homeowners. In the weeks leading up to the move, we spent a lot of time going through our belongings to decide what to keep, what to give away, and what to throw away or recycle.

During this process, it struck me that despite the fact I'm organized and don't like to accumulate "stuff," I could probably eliminate 50% to 75% of what I have and never even notice. I bet that's true for many of us. It got me thinking about what's important in life, and for me that's health, happiness, family, friends, and freedom.

And because security is such a big part of my life, I quickly realized how the moving exercise related, too. As security professionals, we should ask ourselves: "What is truly essential?"
https://www.darkreading.com/edge/theedge/cybersecurity-what-is-truly-essential/b/d-id/1340971

Click above link to read more.

Back to top

Phishers using Zix to "legitimize" emails in the eyes of Office 365 users

A phishing campaign aimed at harvesting Office 365 account credentials is employing a variety of tricks to fool both email security sistems and recipients: the phishing emails come from a compromised enterprise account, through the secure email system Zix, to make recipients believe that the offered link isn't malicious.

The phishing emails are sent from a compromised email account belonging to a real estate services provider (Authentic Title, LLC), and ostensibly contain a closing settlement counter offer. To view it, the recipients are asked to follow a link included in the email.

As the emails are sent via Zix, they sport a header and a footer proclaiming that "This message was sent securely using Zix" and "This message was secured by Zix" – which might be enough for some users to decide the email is legitimate and they can safely follow the provided link.
https://www.helpnetsecurity.com/2021/05/12/phishers-using-zix/

Click above link to read more.

Back to top

Cyber attack 'most significant' on Irish state

A cyber attack on Irish health service computer systems is "possibly the most significant cybercrime attack on the Irish state", a minister has said.

Speaking on broadcaster RTÉ, Ossian Smyth said the attack "goes right to the core of the [health] system".

However, he also said that it was "not espionage".

The health service has temporarily shut down its IT system to protect it after the attack.
Mr. Smyth, who is minister for public procurement and eGovernment, said it was an international attack.

He added: "These are cyber criminal gangs, looking for money. "What they're attempting to do is to encrypt and lock away our data, and then to try to ransom it back to us for money."
https://www.bbc.com/news/world-europe-57111615

Click above link to read more.

Back to top

FBI warns of cybercriminals abusing search ads to promote phishing sites

The Federal Bureau of Investigation says that cybercrime gangs are using search results and search engine ads to lure victims on phishing sites for financial institutions in order to collect their login credentials.

"The schemes resulted in illicit ACH transfers amounting to hundreds of thousands of dollars in financial losses," the FBI said in a private industry notification (PIN) send to the US private sector on Tuesday.

The PIN alert, which *The Record* cannot share due to TLP sharing restrictions, describes a particular phishing campaign mimicking the brand of an unnamed US-based financial institution.

"The cyber actors conducted two versions of the scheme," the FBI said.

https://therecord.media/fbi-warns-of-cybercriminals-abusing-search-ads-to-promote-phishing-sites/

Click above link to read more.

Back to top

Ransomware crooks post cops' psych evaluations after talks with DC police stall

A ransomware gang that hacked the District of Columbia's Metropolitan Police Department (MPD) in April posted personnel records on Tuesday that revealed highly sensitive details for almost two dozen officers, including the results of psychological assessments and polygraph tests; driver's license images; fingerprints; social security numbers; dates of birth; and residential, financial, and marriage histories.

The data, included in a 161MB download from a website on the dark web, was made available after negotiations broke down between members of the Babuk ransomware group and MPD officials, according to screenshots purporting to be chat transcripts between the two organizations. After earlier threatening to leak the names of confidential informants to crime gangs, the operators agreed to remove the data while they carried out the now-aborted negotiations, the transcripts showed.

The operators demanded $4 million in exchange for a promise not to publish any more information and provide a decryption key that would restore the data.
https://arstechnica.com/gadgets/2021/05/ransomware-crooks-post-cops-psych-evaluations-after-talks-with-dc-police-stall/

Click above link to read more.

Back to top

U.S. Intelligence Agencies Warn about 5G

Inadequate implementation of telecom standards, supply chain threats, and weaknesses in systems architecture could pose major cybersecurity risks to 5G networks, potentially making them a lucrative target for cybercriminals and nation-state adversaries to exploit for valuable intelligence.

The analysis, which aims to identify and assess risks and vulnerabilities introduced by 5G adoption, was published on Monday by the U.S. National Security Agency (NSA), in partnership with the Office of the Director of National Intelligence (ODNI) and the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA).

"As new 5G policies and standards are released, there remains the potential for threats that impact the end-user," the report said. "For example, nation states may attempt to exert undue influence on standards that benefit their proprietary technologies and limit customers' choices to use other equipment or software."
https://thehackernews.com/2021/05/us-intelligence-agencies-warn-about-5g.html

Click above link to read more.

Back to top

Victim of Elon Musk bitcoin scam loses home deposit

Julie Bushnell said she felt ashamed and embarrassed after falling for a Bitcoin fraud that cost her £9,000.

It used the name of entrepreneur Elon Musk and a story on a fake BBC website suggesting she could double her money in a giveaway of the cryptocurrency.

The Brighton teacher said: "I think about it every minute of every day."

Ms. Bushnell, an investor in cryptocurrency, spotted an item on a website that appeared to use BBC News branding, claiming Mr. Musk, the billionaire boss of the Tesla car firm, would pay back double the sum of any Bitcoin deposit.
https://www.bbc.com/news/uk-england-sussex-57102038

Click above link to read more.

Back to top

Thousands of patient records exposed after ransomware attack on CaptureRx

A ransomware attack on the healthcare administrative-service provider CaptureRx has exposed patient information from multiple provider systems.

According to reporting from *HIPAA Journal*, tens of thousands of patients from at least five health systems had their data stolen in the incident.

"The investigation determined that, at the time of the incident, the relevant files contained first name, last name, date of birth, and prescription information," said CaptureRx in a press statement.
https://www.healthcareitnews.com/news/thousands-patient-records-exposed-after-ransomware-attack-capturerx

Click above link to read more.

Back to top