April 6, 2021

Try our April Working Remotely Quiz

This week's stories:

U.S. looks to keep critical sectors safe from cyberattacks

A top Biden administration official says the government is undertaking a new effort to help electric utilities, water districts and other critical industries protect against potentially damaging cyberattacks.

"Our aim is to ensure that control systems serving 50,000 or more Americans have the core technology to detect and block malicious cyber activity," Anne Neuberger, deputy national security adviser, said in an interview with The Associated Press on Thursday. "That's it in a sentence. Clear, clean goal, but it's going to take a lot of work to get there."

The public-private partnership reflects the administration's concerns about the vulnerability of vital systems, including the electric grid and water treatment plants, to hacks that could cause catastrophic consequences to American life. Though there is a history of government working with utilities, officials believe the threat has increased as more utility systems are connected to the Internet, and the Biden administration wants to make fast progress in blocking any attacks.

The administration, meanwhile, has grappled in its first 60 days with responses to two major cyber intrusions. In the first, Russian hackers snuck malicious code into a software update pushed out to thousands of government agencies and private companies. The second even more widespread hack affected untold thousands of Microsoft Exchange email servers, a breach the company says was carried out by Chinese state hackers.

https://www.canadiansecuritymag.com/u-s-looks-to-keep-critical-sectors-safe-from-cyberattacks/

Click link above to read more

Stolen Data of 533 Million Facebook Users Leaked Online

A user in a low-level hacking forum on Saturday published the phone numbers and personal data of hundreds of millions of Facebook users for free.

The exposed data includes the personal information of over 533 million Facebook users from 106 countries, including over 32 million records on users in the US, 11 million on users in the UK, and 6 million on users in India. It includes their phone numbers, Facebook IDs, full names, locations, birthdates, bios, and, in some cases, email addresses.

Insider reviewed a sample of the leaked data and verified several records by matching known Facebook users' phone numbers with the IDs listed in the data set. We also verified records by testing email addresses from the data set in Facebook's password-reset feature, which can be used to partially reveal a user's phone number.

https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4

Click link above to read more

Facebook takes down troll farm linked to Iranian opposition group

Facebook on Tuesday announced it had removed 14 networks in 11 countries for using fake accounts to amplify deceptive campaigns, including one linked to an exiled militant Iranian group operating a troll farm out of Albania.

The social media giant took down 1,167 Facebook accounts, 290 Instagram accounts, 255 Pages, and 34 Groups in the month of March for their connections to these "coordinated inauthentic behavior" campaigns, which targeted a range of countries including Israel, Mexico, Benin, and Georgia.

Facebook also highlighted in its report that three groups it took action against were using profile photos likely generated by machine learning technologies. It had removed four other groups using similar techniques since September 2019. The company said it can often easily recognize these photos through telltale errors, like unnaturally distorted backdrops or facial features—one image the company included showed glasses that had asymmetrical frames with different legs, hinges, and connections on each side. Although theses images can be automatically spotted, they show how malicious actors are adopting new tactics and techniques to try to improve their campaigns.

https://therecord.media/facebook-takes-down-troll-farm-linked-to-iranian-opposition-group/

Click link above to read more

Data scraped from 500 million LinkedIn users found for sale online

IDs, names, email addresses and more personal details are part of the massive database of stolen data, which could be used to launch additional attacks on LinkedIn and its users.

A massive trove of LinkedIn account data has been found for sale online, containing 500 million user records including email addresses, phone numbers, links to other social media profiles and professional details.

Reported by CyberNews researchers, the leak was posted to a forum popular with hackers by a user asking for a "four-digit $$$$ minimum price" for access to the full database of stolen account information.

To prove the legitimacy of the info, the leaker included two million records as a sample that users on the form can view for $2 worth of forum-specific credits. CyberNews researchers were able to confirm that the data contained in the sample was legitimate, but added that " it's unclear whether the threat actor is selling up-to-date LinkedIn profiles, or if the data has been taken or aggregated from a previous breach suffered by LinkedIn or other companies."

https://www.techrepublic.com/article/data-scraped-from-500-million-linkedin-users-found-for-sale-online/

Click link above to read more

Hackers From China Target Vietnamese Military and Government

A hacking group related to a Chinese-speaking threat actor has been linked to an advanced cyberespionage campaign targeting government and military organizations in Vietnam.

The attacks have been attributed with low confidence to the advanced persistent threat (APT) called Cycldek (or Goblin Panda, Hellsing, APT 27, and Conimes), which is known for using spear-phishing techniques to compromise diplomatic targets in Southeast Asia, India, and the U.S. at least since 2013.

According to researchers from Kaspersky, the offensive, which was observed between June 2020 and January 2021, leverages a method called DLL side-loading to execute shellcode that decrypts a final payload dubbed "FoundCore."

https://thehackernews.com/2021/04/hackers-from-china-target-vietnamese.html

Click link above to read more

Conti Gang Demands $40M Ransom from Florida School District

New details of negotiation between attackers and officials from Broward County Public Schools emerge after a ransomware attack early last month.

The Conti Gang has demanded a $40 million ransom from a Fort Lauderdale, Fla., school district after a ransomware attack last month. Attackers stole personal information from students and teachers, disrupted the district's networks, and caused some services to be unavailable.

The incident that was discovered on March 7 at Broward County Public Schools drew limited attention at the time of attack. However, new details have emerged on DataBreaches.net, which recently posted a screenshot of a chat between attackers and a school district official about the sum of money attackers demanded. That has shed new light on the incident, given the exorbitant nature of the ransom demands.

During the conversation, attackers — who claim to be from the "ContiLocker Team" — informed the official that they had not only encrypted files, but also had downloaded "more than 1 terabyte of personal data, including financial, contracts, database and other documents" containing Social Security numbers and other personal information about teachers and students.

https://threatpost.com/conti-40m-ransom-florida-school/165258/

Click link above to read more

UC Berkeley confirms data breach, becomes latest victim of Accellion cyber-attack

The University of California, Berkeley (UC Berkeley) has confirmed it suffered a data breach, becoming the latest victim of the Accellion cyber-attack.

On Monday (March 29), "multiple" employees at UC Berkeley received an email from an unknown actor stating that their data had been stolen and would be released.

The emails contained a link that displayed a sample of personal details from UC employees, a statement from UC Berkeley reads.

UC Berkeley said that the data breach was due to an earlier intrusion suffered by third-party provider Accellion, a secure file transfer service, which was used by the university.

Third-party failure

The University of California Office of the President (UCOP) confirmed last night (March 31) that attackers exploited a vulnerability in Accellion to gain access to its data.

https://portswigger.net/daily-swig/uc-berkeley-confirms-data-breach-becomes-latest-victim-of-accellion-cyber-attack

Click link above to read more

GitHub investigating crypto-mining campaign abusing its server infrastructure

Code-hosting service GitHub is actively investigating a series of attacks against its cloud infrastructure that allowed cybercriminals to implant and abuse the company's servers for illicit crypto-mining operations, a spokesperson told The Record today.

The attacks have been going on since the fall of 2020 and have abused a GitHub feature called GitHub Actions, which allows users to automatically execute tasks and workflows once a certain event happens inside one of their GitHub repositories.

In a phone call today, Dutch security engineer Justin Perdok told The Record that at least one threat actor is targeting GitHub repositories where GitHub Actions might be enabled.

The attack involves forking a legitimate repository, adding malicious GitHub Actions to the original code, and then filing a Pull Request with the original repository in order to merge the code back into the original.

https://therecord.media/github-investigating-crypto-mining-campaign-abusing-its-server-infrastructure/

Click link above to read more

How the quick shift to the cloud has led to more security risks

The coronavirus pandemic forced many organizations to put their cloud migration projects into overdrive. Such a fast and unexpected transition to the cloud inevitably opened the door to more security threats. A report released Tuesday by Palo Alto Networks threat intelligence team Unit 42 examines how the cloud migration has affected security and what organizations can do to better protect themselves.

Based on internal data, Unit 42's latest "Cloud Threat Report" found that organizations increased their cloud workloads by more than 20% between December 2019 and June 2020. Along the way, cloud security incidents rose by 188% just in the second quarter of 2020.

Industries that are vital in the effort to combat the pandemic have been hit especially hard. Over last year's second quarter, cloud security incidents for the retail, manufacturing and government sectors rose by 402%, 230% and 205%, respectively.

https://www.techrepublic.com/article/how-the-quick-shift-to-the-cloud-has-led-to-more-security-risks/

Click link above to read more

How To Defend the Extended Network Against Web Risks

Aamir Lakhani, cybersecurity researcher for Fortinet's FortiGuard Labs, discusses criminals flocking to web server and browser attacks, and what to do about it.

Smart cybercriminals are going after web servers and browsers, more so than after individuals. Unfortunately, these types of attacks often go ignored, as they're harder to test for (in terms of pen-testing).

With much of the world now working remotely, this threat has intensified. Attackers use email, instant messages, SMS messages and links on social networking to trick at-home workers into installing malware

that leads to identity theft, loss of property and, possibly, entry into the corporate network. Phishing attacks may lead users to fake sites or landing pages, with the same intent.

What are the latest risks organizations are facing, and what can be done now to defend against them?

Web-Based Phishing On the Rise

The cybersecurity industry is seeing a significant spike in web-based phishing, starting with the HTML/phishing cyber-threat family. Similar HTML cousins – /ScrInject (browser script injection attacks) and /REDIR (browser redirection schemes) – have also contributed to the increase in phishing attempts in 2020. Web-based malware tends to override or bypass most common antivirus (AV) programs, giving it a greater chance of survival and successful infection.

https://threatpost.com/how-to-defend-the-extended-network-against-web-risks/165236/

Click link above to read more

Hackers Targeting professionals With 'more_eggs' Malware via LinkedIn Job Offers

A new spear-phishing campaign is targeting professionals on LinkedIn with weaponized job offers in an attempt to infect targets with a sophisticated backdoor trojan called "more_eggs."

To increase the odds of success, the phishing lures take advantage of malicious ZIP archive files that have the same name as that of the victims' job titles taken from their LinkedIn profiles.

"For example, if the LinkedIn member's job is listed as Senior Account Executive—International Freight the malicious zip file would be titled Senior Account Executive—International Freight position (note the 'position' added to the end)," cybersecurity firm eSentire's Threat Response Unit (TRU) said in an analysis. "Upon opening the fake job offer, the victim unwittingly initiates the stealthy installation of the fileless backdoor, more_eggs."

https://thehackernews.com/2021/04/hackers-targeting-professionals-with.html

Click link above to read more

Sensitive Student Data leaked online by Ransomware Gang

In recent months, several universities were hit by the Clop ransomware gang, specialists think all the attacks are linked to Accellion File Transfer Appliance (FTA) software, a third-party vendor, which was used by students and staff to transfer encrypted files.

Staff and students at the University of Maryland had their private information, such as passports, names, addresses, financial information, and Social Security numbers posted online following a ransomware attack in December.

https://heimdalsecurity.com/blog/attackers-disclose-data-of-students-in-cyberattack/

Click link above to read more

In a rare step, Activision warns CoD players of malware hidden in cheat apps

In a rare step for a company that seldomly issues security warnings, gaming giant Activision published research yesterday detailing how cybercriminals are hiding malware inside Call of Duty: Warzone cheats, warning users to stay away from such offers.

The Activision report walks users through a step-by-step scenario of how these cheats start out as tutorials on hacking forums (screenshot #1), how the cheat software is mass-built, malware is added, and then the final package is advertised on gaming forums (screenshot #2) and via YouTube videos (screenshot #3) to players looking to get an edge.

https://therecord.media/in-a-rare-step-activision-warns-cod-players-of-malware-hidden-in-cheat-apps/

Click link above to read more

North Korean Group Targets Security Researchers - Again

Google: Attackers Leverage Social Media Accounts

A North Korean government-backed threat group that was detected targeting security researchers in January is once again staging a campaign against cybersecurity professionals using advanced social engineering techniques, Google reports.

Google attributed the latest campaign to an unnamed North Korean-linked group, which the company says was behind a similar campaign that targeted security researchers by posing as bug hunters in January. In that campaign, the attackers shared malicious Visual Basic software with a backdoor to exfiltrate data from their victims.

In Wednesday's update, Google notes the North Korean group revived the campaign yet again, this time targeting security researchers using a hoax website that is promoted by the attackers using fake LinkedIn accounts.

https://www.bankinfosecurity.com/north-korean-group-targets-security-researchers-again-a-16322

Click link above to read more