April 20, 2021

Try our April Working Remotely Quiz

This week's stories:

Everything you need to know about the Microsoft Exchange Server hack

Four zero-day vulnerabilities in Microsoft Exchange Server are being actively exploited by state-sponsored threat groups and others to deploy backdoors and malware in widespread attacks.

While in no way believed to be connected to the SolarWinds supply chain attack that has impacted an estimated 18,000 organizations worldwide -- so far -- there is concern that lags in patching vulnerable servers could have a similar impact, or worse, on businesses.

Here is everything you need to know about the security issues and our guide will be updated as the story develops.

WHAT HAPPENED?

Microsoft told security expert Brian Krebs that the company was made aware of four zero-day bugs in "early" January.

https://www.zdnet.com/article/everything-you-need-to-know-about-microsoft-exchange-server-hack/

Click link above to read more

Update to REvil ransomware changes Windows passwords to automate file encryption via Safe Mode

The hackers behind the REvil ransomware have released an updated version of the malware that allows them to change Windows passwords and automate file encryption through Safe Mode, according to a recent report from Bleeping Computer. Researcher R3MRUN also released a detailed breakdown of the attack method on his Twitter account, highlighting that attackers can now use the command-line "smode" to essentially put a device into Safe Mode, allowing them to execute the encryption of the files on a device.

The ransomware then changes the device password to "DTrump4ever" and forces the device to log in automatically after being rebooted.

Bryan Embrey, director of product marketing at Zentry Security, explained that REvil uses three primary attack vectors to penetrate a network: phishing emails with malicious attachments, Remote Desktop Protocol vulnerabilities and software vulnerabilities.

https://www.techrepublic.com/article/update-to-revil-ransomware-changes-windows-passwords-to-automate-file-encryption-via-safe-mode/

Click link above to read more

Geico discloses website bug that exposed driver's license numbers

US car insurer Geico said it plugged a bug on one of its official websites that allowed threat actors to obtain customer driver’s license numbers for more than a month.

In a data breach notification filed with the California Office of Attorney General last week, the car insurer said that between January 21 and March 1, 2021, it detected exploitation attempts against its website’s online sales system.

Geico said threat actors used information about its users that was already made public elsewhere to exploit a bug in its website and match the public data with that user’s driver’s license number that Geico had stored inside its internal database.

While the incident might look insignificant since only driver’s license numbers were exposed, the auto insurer said the data could be abused by attackers to apply for unemployment benefits in the name of some of its customers.

https://therecord.media/geico-discloses-website-bug-that-exposed-drivers-license-numbers/

Click link above to read more

Patch now! NSA, CISA, and FBI warn of Russian intelligence exploiting 5 vulnerabilities

The National Security Agency (NSA), the Cybersecurity and Infrastructure Security Agency (CISA), and the Federal Bureau of Investigation (FBI) have jointly released a Cybersecurity Advisory called Russian SVR Targets U.S. and Allied Networks, to expose ongoing Russian Foreign Intelligence Service (SVR) exploitation of five publicly known vulnerabilities. The advisories’ executive summary reads:

Russian Foreign Intelligence Service (SVR) actors, who are also known under the names APT29, Cozy Bear, and The Dukes frequently use publicly known vulnerabilities to conduct widespread scanning and exploitation against vulnerable systems in an effort to obtain authentication credentials and use those to gain further access. This targeting and exploitation encompasses US and allied networks, including national security and government related systems.

Remarkable mentions in the cybersecurity advisory

Released alongside the advisory is the US Government's formal attribution of the SolarWinds supply chain compromise, and the cyber espionage campaign related to it, to Russia.

Mentioned are recent SVR activities that include targeting COVID-19 research facilities via WellMess malware and targeting networks through a VMware vulnerability disclosed by NSA.

https://blog.malwarebytes.com/malwarebytes-news/2021/04/patch-now-nsa-cisa-and-fbi-warn-of-russian-intelligence-exploiting-5-vulnerabilities/

Click link above to read more

'High-level' organiser of FIN7 hacking group sentenced to ten years in prison

A "high-level manager" of the FIN7 hacking group has been sentenced to ten years in prison.

The US Department of Justice described Ukranian national Fedir Hladyr, 35, as a systems administrator for the FIN7 hacking group.

He was arrested in Germany, in 2018 at the request of U.S. law enforcement and was extradited to Seattle. In September 2019, he pleaded guilty to conspiracy to commit wire fraud and one count of conspiracy to commit computer hacking.

Hladyr served as FIN7's systems administrator and played a central role in aggregating stolen payment card information, supervising FIN7's hackers, and maintaining the elaborate network of servers that the group used to attack and control victims' computers, according to the Department of Justice. He also controlled the organization's encrypted channels of communication, it said.

https://www.zdnet.com/article/high-level-organiser-of-fin7-hacking-group-sentenced-to-ten-years-in-prison/

Click link above to read more

WordPress may automatically disable Google FLoC on websites

WordPress announced today that they are treating Google's new FLoC tracking technology as a security concern and may block it by default on WordPress sites.

For some time, browsers have begun to increasingly block third-party browser cookies [1, 2, 3] used by advertisers for interest-based advertising.

In response, Google introduced a new ad tracking technology called Federated Learning of Cohorts, or FLoC, that uses a web browser to anonymously place users into interest or behavioral buckets based on how they browse the web.

After Google began testing FLoC this month in Google Chrome, there has been a consensus among privacy advocates that Google's FLoC implementation just replaces one privacy risk with another one.

https://www.bleepingcomputer.com/news/security/wordpress-may-automatically-disable-google-floc-on-websites/

Click link above to read more

Not just ransomware: Schools and universities are increasingly targeted by impersonation scams

Last August, the IT security staff at the University of Maryland, Baltimore County noticed a phishing email that was unusually intricate.

nlike obvious scams that ask for gift cards using typo-laden text, the email was a fake job application allegedly sent by someone working for a real investor relations executive at Paylocity. The email asked interested candidates to send basic information, including a phone number and email address, as well as "a little about you and why you think you should be considered" for an executive assistant role. Students who went through with the application process eventually received a follow-up email that appeared to come from the Paylocity executive, confirming their appointment as his personal assistant and asking them to fill out hiring paperwork.

The scam was similar to legitimate emails that came from companies in the past, said UMBC's chief information security officer Mark Cather. "We actually do see emails that are almost the same—an executive looking for an assistant—but when we contact them, they're legitimate," he said. "The scammers have been getting better at their craft… They're going after universities and individual departments because it's a smaller, more trusted network."

https://therecord.media/not-just-ransomware-schools-and-universities-are-increasingly-targeted-by-impersonation-scams/

Click link above to read more

Concerns grow over digital threats faced from former employees

Security experts said the recent upheaval in the job market makes it imperative to bolster separation protocols further.

The COVID-19 pandemic has caused unprecedented turmoil in the job market over the last year, with millions across the world losing or leaving jobs due to economic disruption. An unfortunate byproduct of the employee turnover is the cybersecurity threat that comes with having a significant number of former employees.

Darren Guccione, CEO and co-founder of Keeper Security, and other cybersecurity experts spoke to TechRepublic about how to protect an enterprise from those who have knowledge or access to their former employer's confidential information, keeping the door open for looming hackers.

"A lot of companies fail to have clear policies or a checklist that employers use for post-employee separation. This is extremely important because failing to do so is going to involve a lot of things but the most important thing is that you want to make sure that the former employee or even a subcontractor that previously had access to the organization's technologies and systems is completely locked out," Guccione said in an interview.

https://www.techrepublic.com/article/concerns-grow-over-digital-threats-faced-from-former-employees/

Click link above to read more

Malvertisers hacked 120 ad servers to load malicious ads

A malvertising operation known under the codename of Tag Barnakle has breached more than 120 ad servers over the past year and inserted malicious code into legitimate ads that redirected website visitors to sites promoting scams and malware.

Security firm Confiant first reported on this campaign last year, in April 2020, when it said it found 60 ad servers that were left unpatched and compromised by the Tag Barnakle gang.

One year later, Confiant said that despite exposing the group's tactics and raising an alarm in the online advertising industry, the Tag Barnakle group has continued to operate unchecked and has doubled the number of servers it breached.

https://therecord.media/malvertisers-hacked-120-ad-servers-to-load-malicious-ads/c

Click link above to read more

Covid-19 themed threats surge: McAfee sees cyber-attack detections increase by 114% in Q4 2020

As businesses the world over adapted to unprecedented numbers of employees working from home, cybercriminals worked feverishly to launch Covid-19-themed attacks on a workforce coping with pandemic restrictions and the potential vulnerabilities of remote device and bandwidth security. As the pandemic began to surge around the world, IT security firm McAfee saw a 605% increase in Q2 2020. These attacks again increased by 240% in Q3 and 114% in Q4.

Recently, McAfee released its Threats Report: April 2021, examining cybercriminal activity related to malware and the evolution of cyber threats in the third and fourth quarters of 2020. In Q4, McAfee Labs observed an average of 648 threats per minute, an increase of 60 threats per minute (10%) over Q3. The two quarters also saw Covid-19-related cyber-attack detections increase by 240% in Q3 and 114% in Q4, while Powershell threats again surged 208% due to continued increases in Donoff malware activity.

https://www.financialexpress.com/industry/technology/covid-19-themed-threats-surge-mcafee-sees-cyber-attack-detections-increase-by-114-in-q4-2020/2235817/

Click link above to read more

Cyber attacks: How bad can they get and how do you fight a cyberwar?

On the morning of June 27, 2017, it seemed as if Ukraine had slipped back in time and into the wrong century – almost nothing worked. Not the ATMs, the trains, the airports, the television stations. Even the radiation monitors at the old Chernobyl nuclear plant were down.

Ukraine, in the midst of a long and undeclared war with Russia, had been hit by mysterious blackouts before but this was eating through computer networks at a terrifying pace, turning screens dark across the country. And it seemed to be spreading further than intended, out through Europe and around the globe, paralysing hospitals and companies from London to Denver, even the Cadbury chocolate factory in Tasmania, and bringing swathes of the world's shipping to a halt. By the time the culprit – a wild variant of malicious computer code (or worm) known as NotPetya – was stopped hours later, it had looped back into Russia, where it originated, and racked up about $US10 billion ($12.9 billion) in damage worldwide, making it the most expensive cyber attack to date.

https://www.smh.com.au/national/robots-worms-and-satellites-how-do-you-fight-a-cyberwar-20210407-p57ha5.html

Click link above to read more

Google's Project Zero updates vulnerability disclosure rules to add patch cushion

The Google Project Zero security team has updated its vulnerability disclosure guidelines today to add a cushion of 30 days to some security bug disclosures, so end-users have enough time to patch software and prevent attackers from weaponizing bugs.

Today's changes are of particular importance because a large part of the cybersecurity community has adopted Project Zero's rules as the unofficial methodology for disclosing a security bug to software vendors and then to the general public.

Prior to today, Google Project Zero researchers would give software vendors 90 days to fix a security bug. When the bug was patched, or at the end of the 90 days time window, Google researchers would publish details about the bug online (on their bug tracker).

Starting today, Project Zero says it will wait 30 days before publishing any details about the bug.

https://therecord.media/googles-project-zero-updates-vulnerability-disclosure-rules-to-add-patch-cushion/

Click link above to read more

NitroRansomware Asks for $9.99 Discord Gift Codes, Steals Access Tokens | Threatpost

The malware seems like a silly coding lark at first, but further exploration shows it can wreak serious damage in follow-on attacks.

The NitroRansomware malware strain is shaking up the ransomware norm by demanding Discord Nitro gift codes from victims instead of actual money.

Discord is a VoIP, instant messaging and digital-distribution platform designed for creating communities. Users communicate with voice calls, video calls, text messaging, media and files in private chats or as part of communities called "servers.

While it's free, users can purchase an upgraded "Nitro" subscription for $9.99 that allows larger upload sizes, HD video streaming, better emoji options and the ability to "stand out" via promotions on servers.

https://threatpost.com/nitroransomware-discord-gift-codes/165488/

Click link above to read more

Malware That Spreads Via Xcode Projects Now Targeting Apple's M1-based Macs

A Mac malware campaign targeting Xcode developers has been retooled to add support for Apple's new M1 chips and expand its features to steal confidential information from cryptocurrency apps.

XCSSET came into the spotlight in August 2020 after it was found to spread via modified Xcode IDE projects, which, upon the building, were configured to execute the payload. The malware repackages payload modules to imitate legitimate Mac apps, which are ultimately responsible for infecting local Xcode projects and injecting the main payload to execute when the compromised project builds.

https://thehackernews.com/2021/04/malware-spreads-via-xcode-projects-now.html

Click link above to read more

FireEye: More than 1,900 distinct hacking groups are active today

US cybersecurity firm FireEye says that based on its internal data, there are currently more than 1,900 distinct hacking groups that are active today, a number that grew from 1,800 groups recorded at the end of 2019.

In its yearly cybercrime report, the company said it discovered 650 new threat actors during 2020, but new evidence also allowed it to remove 500 groups from its threat actor tracker due to overlaps in activity and hacking infrastructure with previously-known clusters.

The 1,900 figure includes nation-state-sponsored threat actors (known as APTs), financially motivated groups (known as FINs), and uncategorized groups (known as UNCs) about which information is still scarce to place them in either of the first two categories.

https://therecord.media/fireeye-more-than-1900-distinct-hacking-groups-are-active-today/

Click link above to read more

---

100 million more IoT devices are exposed—and they won't be the last

Over the last few years, researchers have found a shocking number of vulnerabilities in seemingly basic code that underpins how devices communicate with the Internet. Now, a new set of nine such vulnerabilities are exposing an estimated 100 million devices worldwide, including an array of Internet-of-things products and IT management servers. The larger question researchers are scrambling to answer, though, is how to spur substantive changes—and implement effective defenses—as more and more of these types of vulnerabilities pile up.

Dubbed Name:Wreck, the newly disclosed flaws are in four ubiquitous TCP/IP stacks, code that integrates network communication protocols to establish connections between devices and the Internet. The vulnerabilities, present in operating systems like the open source project FreeBSD, as well as Nucleus NET from the industrial control firm Siemens, all relate to how these stacks implement the "Domain Name System" Internet phone book. They all would allow an attacker to either crash a device and take it offline or gain control of it remotely. Both of these attacks could potentially wreak havoc in a network, especially in critical infrastructure, health care, or manufacturing settings where infiltrating a connected device or IT server can disrupt a whole system or serve as a valuable jumping-off point for burrowing deeper into a victim's network.

https://arstechnica.com/information-technology/2021/04/100-million-more-iot-devices-are-exposed-and-they-wont-be-the-last/

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:

https://www.gov.bc.ca/informationsecurity

OCIOSecurity@gov.bc.ca