
# March 16th, 2021

**Try our March Fraud Prevention Quiz**

This week's stories:

**Cybercriminals using Google Search as the latest trick to snare unsuspecting victims for malware attacks**

**How malware is targeting the new Apple Macs**

**2021 Hacker Report: Hackers are not just driven by money**

**Molson Coors discloses cyberattack disrupting its brewery operations**

**Malicious Actors Target Crypto Wallets of Coinbase Users in New Phishing Campaign**

**Exchange servers first compromised by Chinese hackers hit with ransomware**

**Security agencies leak sensitive data by failing to sanitize PDF files**

**White House Weighs New Cybersecurity Approach After Failure to Detect Hacks**

**Windows 10 Ransomware Protection In 2021: Some Surprises, Says Report**

**U.S. Indicts CEO of Encrypted Phone Firm 'Sky'**

**Netflix is trying to crack down on password sharing with new test**

**Hackers target NFT craze by stealing from Nifty Gateway users**

**Flaw in Million Times Downloaded iPhone Call Recording app**

**Cyberattacks See Fundamental Changes, A Year into COVID-19**

---

## Cybercriminals using Google Search as the latest trick to snare unsuspecting victims for malware attacks

*Malware from SEO poisoning such as the Gootkit RAT is a new way for companies to be hit with ransomware.*

It was only a matter of time before cybercriminals turned their attention to one of the most common activities on the internet— a Google search. The latest trick is using long-tail search terms and legitimate websites to deliver the Gootkit remote access trojan.

This latest iteration of the Gootkit RAT uses "malicious search engine optimization techniques to squirm into Google search results," as Sophos analysts describe it in a blog post. The cybersecurity firm reports that criminals are using this new variation they call Gootloader to deliver malware payloads in North America, South Korea, Germany and France. The Sophos research found that bad actors are not targeting other search engines as frequently or as successfully.

Chris Rodgers, CEO and founder of Colorado SEO Pros, said that this new tactic uses Google as a gateway and SEO knowledge, particularly about long-tail searches.

"They had to go in and find topics that are low competition and low search volume and they have to be doing this at massive volume for it to be lucrative," he said.

https://www.techrepublic.com/article/hackers-update-gootkit-rat-to-use-google-searches-and-discussion-forums-to-deliver-malware/

***Click link above to read more***

---

## How malware is targeting the new Apple Macs

*As the new kid on the block, the M1 chip-based Mac is already on the radar of malware writers, says Kaspersky.*

Cybercriminals often like to attack any technology that's new in hopes of catching potential victims off guard. And that's proved true of the latest Macs. Unveiled in November 2020, the latest MacBook Air, 13-inch MacBook Pro and Mac mini are powered by Apple's M1 chip as a shift away from Intel-based architecture. Beyond attracting buyers, the new platform is attracting malware writers eager to expand their range of targets.

In a report released Friday, security provider Kaspersky describes three malware threats to the M1 Mac—XCSSET malware, Silver Sparrow and Pirrit adware.

https://www.techrepublic.com/article/how-malware-is-targeting-the-new-apple-macs/?ftag=TREe01923b&bhid=19662319145962710268575546540229&mid=13300035&cid=712327807

***Click link above to read more***

---

## 2021 Hacker Report: Hackers are not just driven by money

*HackerOne released its 2021 Hacker Report that reveals a 63% increase in the number of hackers submitting vulnerabilities in 2020.*

As organizations' attack surfaces have shifted due to pandemic led digital transformation, hackers have adapted and zeroed in on emerging threats. Reports for vulnerabilities caused by trends like moving to the cloud have proliferated in the past year, with misconfiguration vulnerabilities rising by 310%.

Other key findings

- 38% of hackers spent more time hacking since the COVID-19 pandemic started
- Top hackers, on average, are reporting bugs across 20 different vulnerability categories, with a 53% rise in submissions for both Improper Access Control and Privilege Escalation
- Half the hackers surveyed have not reported a bug because of a lack of a clear reporting process, or a previous negative experience
- Hackers are not just driven by money, 85% of hackers do it to learn and 62% do it to advance their career
- Hackers are expanding their experience of different technologies with more specialising in IoT, APIs and Android apps than ever before

"This year's Hacker Report demonstrates the depth of vulnerability insights that hackers bring to a security program," said HackerOne co-founder, Jobert Abma.

https://www.helpnetsecurity.com/2021/03/10/2021-hacker-report/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29

***Click link above to read more***

---

## Molson Coors discloses cyberattack disrupting its brewery operations

Brewing giant Molson Coors disclosed Thursday that it has experienced a "cybersecurity incident" that has disrupted operations and beer production. In a Form-8K filed with the SEC today, Miller Coors said it's bringing in an outside forensic IT firm to investigate the breach, but that delays in shipments were likely as it works to bring its systems back online.

"The Company is working around the clock to get its systems back up as quickly as possible," Miller Coors wrote in the filing. "Although the Company is actively managing this cybersecurity incident, it has caused and may continue to cause a delay or disruption to parts of the Company's business, including its brewery operations, production, and shipments."

Molson Coors operates a huge portfolio of beer brands, including the iconic Coors and Miller brands, as well as Molson Canadian, Blue Moon, Peroni, Grolsch, Killian's, and Foster's.

The company has not provided additional details of the cyberattack, but some security experts are calling the incident a ransomware attack. In November, Campari Group, the famed Italian beverage vendor behind brands like Campari, Cinzano, and Appleton, was hit with a ransomware attack that took down a large part of its IT network.

https://www.zdnet.com/article/molson-coors-discloses-cyberattack-disrupting-its-brewery-operations/

***Click link above to read more***

---

## Malicious Actors Target Crypto Wallets of Coinbase Users in New Phishing Campaign

Cybercriminals are targeting Coinbase platform users with phishing campaigns in an attempt to steal their account credentials and drain their cryptocurrency wallets, Bitdefender Antispam Lab has learned.

According to our latest telemetry, the phishing campaign was noticed since mid-February, targeting over 25,000 users. Sixty-nine percent of the fraudulent correspondence originated from India, 13.73 percent from Brazil, 10 percent from the US and 2.33 percent from Japan.

When analyzing the final destination of the phishing emails, we noticed the following:

- 54.72 percent reached users from South Korea
- 12.53 percent reached users from Sweden
- 7 percent reached users from Ireland
- 6.78 percent reached users from Japan
- 5.12 percent reached users from the United States
- 2.81 percent reached users from Great Britain
- 2.16 percent reached users from Canada

https://hotforsecurity.bitdefender.com/blog/malicious-actors-target-crypto-wallets-of-coinbase-users-in-new-phishing-campaign-25445.html?web_view=true

***Click link above to read more***

---

## Exchange servers first compromised by Chinese hackers hit with ransomware

As if Exchange users didn't already have enough to worry about, they have this.

Organizations using Microsoft Exchange now have a new security headache: never-before-seen ransomware that's being installed on servers that were already infected by state-sponsored hackers in China.

Microsoft reported the new family of ransomware deployment late Thursday, saying that it was being deployed after the initial compromise of servers. Microsoft's name for the new family is Ransom:Win32/DoejoCrypt.A. The more common name is DearCry.

Security firm Kryptos Logic said Friday afternoon that it has detected Hafnium-compromised Exchange servers that were later infected with ransomware. Kryptos Logic security researcher Marcus Hutchins told Ars that the ransomware is DearCry.

"We've just discovered 6970 exposed webshells which are publicly exposed and were placed by actors exploiting the Exchange vulnerability," Kryptos Logic said. "These shells are being used to deploy ransomware." Webshells are backdoors that allow attackers to use a browser-based interface to run commands and execute malicious code on infected servers.

https://arstechnica.com/gadgets/2021/03/ransomware-gangs-hijack-7000-exchange-servers-first-hit-by-chinese-hackers/

***Click link above to read more***

---

## Security agencies leak sensitive data by failing to sanitize PDF files

Security agencies are doing a poor job at sanitizing PDF documents they publish on their official websites and are leaking troves of sensitive information that could be collected and weaponized in malware attacks.

In a research paper published this month, the French National Institute for Research in Computer Science and Automation (INRIA) said it collected and analyzed 39,664 PDF files published on the websites of 75 security agencies from 47 countries.

INRIA researchers Supriya Adhatarao and Cédric Lauradoux said they were able to recover sensitive data from 76% of the files they analyzed. This included data such as:

- Name of the author
- Name of the PDF app
- Operating system
- Device details
- Author email
- File path information
- Comments and annotations

**19 security agencies didn't update software for 2+ years**

The researchers warn that threat groups could collect documents from an agency's website over time and build profiles on the agency's software policy and individual employee machines.

https://therecord.media/security-agencies-leak-sensitive-data-by-failing-to-sanitize-pdf-files/

***Click link above to read more***

---

## White House Weighs New Cybersecurity Approach After Failure to Detect Hacks

*The intelligence agencies missed massive intrusions by Russia and China, forcing the administration and Congress to look for solutions, including closer partnership with private industry.*

The sophisticated hacks pulled off by Russia and China against a broad array of government and industrial targets in the United States — and the failure of the intelligence agencies to detect them — are driving the Biden administration and Congress to rethink how the nation should protect itself from growing cyberthreats.

Both hacks exploited the same gaping vulnerability in the existing system: They were launched from inside the United States — on servers run by Amazon, GoDaddy and smaller domestic providers — putting them out of reach of the early warning system run by the National Security Agency.

The agency, like the C.I.A. and other American intelligence agencies, is prohibited by law from conducting surveillance inside the United States, to protect the privacy of American citizens.

But the F.B.I. and Department of Homeland Security — the two agencies that can legally operate inside the United States — were also blind to what happened, raising additional concerns about the nation's capacity to defend itself from both rival governments and nonstate attackers like criminal and terrorist groups.

https://www.nytimes.com/2021/03/14/us/politics/us-hacks-china-russia.html

***Click link above to read more***

---

## Windows 10 Ransomware Protection In 2021: Some Surprises, Says Report

Windows 10 ransomware protection remains the first and only line of defense for the majority of consumers using Windows in 2021.

Ransomware is one of the most dangerous kinds of malware because it not only denies access to your data but demands a ransom be paid.

And the amount of ransom demanded keeps going up. The average ransom payment jumped 31 percent to $233,817 in the third quarter of 2020 from $110,532 in the second quarter, according to statistics posted by Coveware.

Are you protected? Windows ransomware protection basics

Unbeknownst to many consumer users of Windows, Microsoft offers built-in ransomware protection as part of Windows Defender, found under Virus & Threat Protection.

The basics for turning it on aren't complicated: type in "Ransomware Protection" in the Windows 10 Cortana search bar (typically in the bottom lower left of the screen) then go to the "Ransomware Protection" screen.

https://www.forbes.com/sites/brookecrothers/2021/03/14/state-of-windows-10-ransomware-protection-2021-some-surprises-says-report/?sh=70e76f7d7d2f

***Click link above to read more***

## U.S. Indicts CEO of Encrypted Phone Firm 'Sky'

*"The indictment alleges that Sky Global generated hundreds of millions of dollars providing a service that allowed criminal networks around the world to hide their international drug trafficking activity from law enforcement."*

The U.S. the Department of Justice announced an indictment against the chief executive officer of Sky Global and an associate for allegedly selling their devices to help international drug traffickers avoid law enforcement on Friday.

The indictment is rare in that it marks only the second time the DOJ has filed charges against an encrypted phone company, and signals that the DOJ will continue to prosecute the heads and associates of companies that they say cater deliberately to facilitating criminal acts. The move also comes just days after the company, responding to law enforcement action against the firm in Europe, vehemently denied being a preferred choice for criminals, and Jean-Francois Eap, Sky's CEO, specifically told Motherboard that his product exists for the prevention of identity theft, hacking, and other privacy issues.

https://www.vice.com/en/article/4adzdj/sky-secure-global-indictment

***Click link above to read more***

## Netflix is trying to crack down on password sharing with new test

Netflix has more than 200 million subscribers around the world, and now the company is looking at ways to curb password sharing for both business and security reasons.

A new feature, first spotted by GammaWire, prevents people who are not authorized to use the account from accessing it. A Netflix spokesperson told The Verge, “This test is designed to help ensure that people using Netflix accounts are authorized to do so.” If Netflix detects that someone is trying to use the account without being an account owner, they’ll be asked to verify later or verify being an account owner through an email code or text code.

If someone is unable to verify account ownership within a certain timeframe, they won’t be able to stream any Netflix content. Instead, they’ll be asked to make their own account. While this may not prevent all password sharing — hypothetically, an account owner could send their friend the code as it comes through — the idea is that it will prevent some password sharing.

https://www.theverge.com/2021/3/11/22325831/netflix-password-sharing-test-feature-piracy-security-streaming-video

***Click link above to read more***

## Hackers target NFT craze by stealing from Nifty Gateway users

It was the digital art heist everyone in the cybersecurity world saw coming.

Over the last couple days, multiple users of Nifty Gateway, a marketplace for buying and selling non-fungible tokens (NFTs), reported on Twitter that their accounts had been hacked and then drained of thousands of dollars worth of digital art.

The theft marks one of the first known incidents of digital art theft, but the rapid adoption of NFTs suggests it will not be the last. According to NFT Report 2020, the NFT market grew almost 300% last year and is now valued at roughly $250 million, making it an attractive target for hackers.

NFTs have been hailed as a way to help artists profit from their work, but the fast-growing market has left many onlookers incredulous, seeing as the images or objects can be easily copied or redistributed online.

https://therecord.media/hackers-target-nft-craze-by-stealing-from-nifty-gateway-users/

***Click link above to read more***

## Flaw in Million Times Downloaded iPhone Call Recording app

The “Automatic call recorder” application is one of the popular applications used by iPhone users to record their calls. The app is among top-grossing in the Business category of App Store currently #15 in the downloads in the Business Category worldwide.

PingSafe AI, a security company that monitors multiple breaches in real-time, has uncovered a critical vulnerability in the iPhone automatic call recorder application that exposed thousands of users' recorded calls.

The Call Recorder app-enabled third-parties to access a user's entire library of recordings, just by knowing their phone number. Apple doesn't offer call recording as a stock feature on the iPhone, so those wishing to do so easily need an app to facilitate the function.

https://cybersecuritynews.com/automatic-call-recorder-flaw/

***Click link above to read more***

---

## Cyberattacks See Fundamental Changes, A Year into COVID-19

A year after COVID-19 was officially determined to be a pandemic, the methods and tactics used by cybercriminals have drastically changed.

COVID-19-related phishing emails, brute-force attacks on remote workers, and a focus on exploiting or abusing collaboration platforms are the hallmarks of cybercriminal enterprise as the coronavirus marks its first anniversary of going global.

A year after the COVID-19 crisis was officially determined to be a pandemic, the way people live and work has radically changed – and so have "the methods and tactics used by criminals on the internet looking to exploit the massive increase in online traffic," according to a report from Kaspersky, issued on Monday.

https://threatpost.com/cyberattacks-fundamental-changes-covid-19/164775/

***Click link above to read more***

---