Monthly Cybersecurity Newsletter

April 2024
Issue

NCDIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Enterprise Security and Risk Management Office (ESRMO)

**From the Desk of the State Chief Risk Officer – Torry Crass**

# Apple Users Become the Latest Targets of MFA Attacks

A new string of multifactor authentication (MFA) attacks targeting the reset of Apple IDs seem to be popping up in a likely attempt to steal the victim's digital identity and more.

A recent post on Twitter/X from entrepreneur Parth Patel outlines his experience when his phone became inundated with requests to reset his Apple ID password – to the tune of over 100.

Similar to the MFA fatigue attacks we've seen last year, this attack sought to use the same technique to get the victim to either answer "yes" to make the prompts stop or to make a mistake and accidentally allow the password reset.

While this kind of attack may not seem mainstream enough to pay attention on terms of warning users about it, etc., it does demonstrate how the cybercrime economy is growing enough that threat actors are looking for ways to fit into the economy by establishing a niche victim set for them to go after – digital identity theft via Apple IDs.

These attacks aren't unique, as Krebs on Security covered this and another similar attack on an IT professional, demonstrating it's more than a one-off experience.

What can be taken from this specific attack is something taught in security awareness training – if something looks suspicious, vigilance should immediately go up, a slowing of the response should be the status quo, and meticulously either disengaging or responding (as in the case of the prompt bomb attacks, where you'd need to at least deny each attack prompt) to ensure malicious intentions aren't enabled by the victim-user's actions.

*This article is redistributed with permission from KnowBe4.*

# Malicious App Impersonates McAfee to Distribute Malware via Text and Phone Calls

A trojanized version of the McAfee Security app is installing the Android banking Trojan “Vultur,” according to researchers at Fox-IT. The attackers are spreading links to the malicious app via text messages and phone calls.

“In order to deceive unsuspecting individuals into installing malware, the threat actors employ a hybrid attack using two SMS messages and a phone call,” the researchers write. “First, the victim receives an SMS message that instructs them to call a number if they did not authorize a transaction involving a large amount of money. In reality, this transaction never occurred, but it creates a false sense of urgency to trick the victim into acting quickly.”

If a victim calls the phone number, they’ll receive another text with a link to a malicious version of the McAfee Security app, which will install the Vultur malware.

“A second SMS is sent during the phone call, where the victim is instructed to install a trojanized version of the McAfee Security app from a link,” Fox-IT says.

“This application is actually Brunhilda Dropper, which looks benign to the victim as it contains functionality that the original McAfee Security app would have. As illustrated below, this dropper decrypts and executes a total of 3 Vultur-related payloads, giving the threat actors total control over the victim’s mobile device.”

The researchers note that this version of Vultur has new features that make it harder to detect.
“The most intriguing addition is the malware’s ability to remotely interact with the infected device through the use of Android’s Accessibility Services,” the researchers write.

“The malware operator can now send commands in-order-to perform clicks, scrolls, swipe gestures, and more. Firebase Cloud Messaging (FCM), a messaging service provided by Google, is used for sending messages from the C2 server to the infected device. The message sent by the malware operator through FCM can contain a command, which, upon receipt, triggers the execution of corresponding functionality within the malware. This eliminates the need for an ongoing connection with the device.”

*This article is redistributed with permission from KnowBe4.*

# IT Leaders Can't Stop AI and Deepfake Scams as They Top the List of Most Frequent Attacks

New data shows that the attacks IT feels most inadequate to stop are the ones they're experiencing the most.

According to Keeper Security's latest report, The Future of Defense: IT Leaders Brace for Unprecedented Cyber Threats, the most serious emerging types of technologies being used in modern cyber attacks lead with AI-powered attacks and deepfake technology.  By itself, this information wouldn't be that damning.
But when you also find that the two types of attacks IT leaders don't feel like they can stop are also AI-powered attacks and deepfake technology we suddenly have a problem.

Despite security solutions evolving to leverage AI, it doesn't translate into stopping AI-generated attacks. We know this because Keeper also point out in their report that 61% of organizations are still battling phishing as an attack vector, with 51% of orgs saying phishing use in cyberattacks is increasing.

In other words, it's time to engage and empower the one part of your cybersecurity defenses you haven't utilized yet – the user. By enrolling users in security awareness training, you elevate their vigilance and reduce the likelihood that even the best written or most convincing sounding piece of content will be just assumed to be valid.

And when you get users to jump in and immediately suspect email and web content where "something's just off about it," the likelihood of even the most sophisticated attacks falling users into clicking on links or attachments dwindles.

*This article is redistributed with permission from KnowBe4.*

# New Malware Loader Delivers Agent Tesla Remote Access Trojan Via Phishing

A new malware loader is delivering the Agent Tesla remote access Trojan (RAT), according to researchers at Trustwave SpiderLabs. The malware is distributed by phishing emails with malicious attachments.

“The threat begins with a fake bank payment email designed to deceive recipients,” the researchers write. “Concealed within this email is an attachment named ‘Bank Handlowy w Warszawie - dowód wpłaty_pdf.tar.gz’ masquerading as a legitimate payment receipt from a bank.

"This filename implies a harmless document, but it actually contains a malicious loader disguised within the tar.gz archive. This tactic is commonly employed in phishing attacks to trick recipients into unwittingly activating the malware and initiating nefarious activities.”

If a user falls for the phishing attack, the malware will be downloaded and installed.

“The infection chain begins with a phishing email posing as a bank payment notification in which a disguised loader was attached as an archive file,” the researchers write.

“This loader then used obfuscation to evade detection and leveraged polymorphic behavior with complex decryption methods. The loader also exhibited the capability to bypass antivirus defenses and retrieved its payload using specific URLs and user agents leveraging proxies for further obfuscate traffic. The payload itself, the Agent Tesla infostealer, is then executed entirely in memory, capturing and exfiltrating data via SMTP using compromised email accounts for discreet communication.”

Using compromised email accounts to exfiltrate the stolen data helps the malware avoid detection.

“Threat actors often hijack compromised email accounts to carry out the exfiltration process,” the researchers explain. “This method has several strategic benefits. First, it exploits the trust people have in regular email communication, making it less likely to raise suspicion. Second, it provides anonymity and makes it harder to trace the attack back to the threat actors. Finally, using existing email systems means they don't have to set up new communication channels, saving time and resources.”

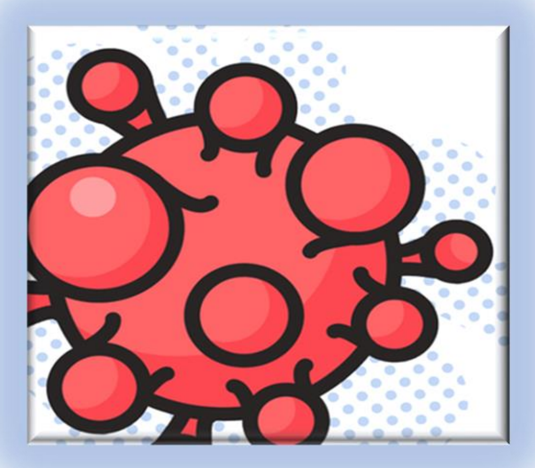
*This article is redistributed with permission from KnowBe4.*

# The Number of New Pieces of Malware Per Minute Has Quadrupled in Just One Year

The threat of novel malware is growing exponentially, making it more difficult for security solutions to identify attachments and links to files as being malware.
According to BlackBerry’s new Global Threat Intelligence Report, the problem of novel malware has been continually growing over the last year.

At the beginning of last year, BlackBerry was detecting new malware at a rate of just one per minute. By the next month, it was 1.5, 2.9 pieces per minute by August of last year. By Q4 of last year, it rose to 3.7 pieces per minute.

That’s a staggering jump in a single year, and even ransomware hasn’t rose that quickly. The likely culprit is the affiliate cybercrime models that have arisen; with one “vendor” producing malware that may be used by hundreds or thousands of would-be threat actors, a viable way to make malware look unique for each one becomes a marketable “feature.”



According to BlackBerry, despite critical infrastructure organizations being attacked the most (they represented 64% of all attacked stopped), 53% of attacks targeted the commercial enterprise sector (which BlackBerry sees as the culmination of retail, capital goods, wholesale trade and other related industries) used unique malware last year.

This problem of malware being unique won’t necessarily stop security solutions from detecting it early. Since covering how one in eight email threats make it past security solutions, it stands to reason this may become a larger problem, with the organization needing to rely on the user to spot and stop the attack based purely on the social engineering cues in an email.

*This article is redistributed with permission from KnowBe4.*

## Training and Continued Learning Resources

- FedVTE: Free Online Training Environment: https://fedvte.usalearning.gov/
- TEEX: Texas Engineering Extension Service: https://teex.org/
- NICCS: National Initiative for Cybersecurity Careers & Studies: https://niccs.cisa.gov/
- ICS-CERT Training: https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT

## CYBERSECURITY NEWSLETTERS

**SAC Security Awareness Newsletter:** Monthly security awareness newsletter provided for all state employees by KnowBe4. Access the newsletter. ***Note**: You must have a valid state employee Microsoft 365 account*.

**CIS Security Tips Newsletter:** Free monthly cybersecurity resource from the Center for Internet Security. https://www.cisecurity.org/insights/newsletter

**SANS OUCH! Newsletter:** Free monthly cybersecurity awareness newsletter provided by the SANS Institute. https://www.sans.org/newsletters/ouch/

**April 16:** SANS Webinar: Introduction to AI and Leveraging it in Cybersecurity

**April 16:** SANS Webinar: Making Mistakes Publicly: Cloud Edition – Aviata Solo Flight Challenge Chapter 1

**April 17**: SANS Webinar: Spring Cyber Solutions Fest 2024: Emerging Technologies Track

**April 18**: SANS Webinar: Spring Cyber Solutions Fest 2024: Insider Threat & Identity Access Management Track

**April 19**: SANS Webinar: Spring Cyber Solutions Fest 2024: DevSecOps & Application Security Track

**April 20**: SANS Webinar: Spring Cyber Solutions Fest 2024: Attack Surface & Vulnerability Track

View a list of upcoming SANS webcasts.

Be sure to follow the N.C. Department of Information Technology on X (Formerly Known as Twitter), Facebook and LinkedIn for more tips. Also visit it.nc.gov/CyberSecureNC or Stay Safe Online for additional information and resources on cybersecurity awareness. *Remember … Stop. Think. Connect.*

***Disclaimer****: Vendors, references and links in this newsletter are for informational purposes only, and their inclusion should, in no way, be considered an endorsement from the N.C. Department of Information Technology.*