Monthly Cybersecurity Newsletter

October 2023

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

'Secure Our World:' October is Cybersecurity Awareness Month

October ushers in the annual occurrence of Cybersecurity Awareness Month, a time when the public and corporate sectors, as well as tribal communities, spread awareness of the value of cybersecurity. This annual initiative was set in place to promote the importance of good online security practices and the need for appropriate cyber defense mechanisms.

This year's campaign theme – **Secure Our World** – focuses on four simple ways to help stay safe online:

- **Recognize and report phishing.** Avoid clicking links or opening attachments in suspicious messages. If there is any doubt, check with the sender first.
- **Use strong passwords and a password manager.** All passwords should be long, complex and unique. Never reuse passwords; use password managers to generate and store strong passwords.
- **Turn on multifactor authentication.** It requires you to enter more information than just a password, such as a text code or fingerprint.
- **Update software.** Make sure your devices are running the latest version of operating systems, software and web browsers.

Throughout October, various organizations, educational institutions and businesses will host events, workshops and training programs to educate people on varying cyberthreats, data protection methods and different ways to safeguard personal information online.

Not only is security an individual effort, but it is also a collective effort as well. During Cybersecurity Awareness Month, take the time to evaluate the different methods you and your organization use to secure your devices and online presence. Take the time to learn about cybersecurity threats, best practices and tools you can use to enhance your security.

Finally, remember, you are the first line of defense in true security.

Hacker Deepfakes Employee's Voice in Call to Breach IT Company

Last month, Retool, a business software development company, fell victim to a sophisticated cyberattack that compromised 27 of its cloud customers.

The attack was a toxic cocktail of social engineering, AI deepfake technology and a vulnerability in Google's Authenticator app.

The attacker initiated the breach by sending phishing SMS messages to Retool employees, posing as an IT team member addressing a payroll issue. While most employees ignored the message, one clicked on the URL, leading them to a fake login portal with multifactor authentication.

Here is where it gets eerie: the hacker then called the employee using an AI-generated deepfake of a familiar voice from the IT team. Despite growing suspicion, the employee gave away an additional MFA code. This suggests the attacker had prior knowledge of the company, possibly indicating an earlier infiltration.

Once the MFA code was surrendered, the hacker gained access to the employee's GSuite account. This was particularly damaging because Google Authenticator's new cloud-syncing feature allowed the attacker to view MFA codes on multiple devices. Retool emphasized that this Google feature was a significant vulnerability, as compromising a Google account now also exposes all synced MFA codes.

Retool has since revoked the hacker's access and is sharing its experience to alert other companies. The incident underscores the evolving threats in cybersecurity, highlighting the need for a strong security culture and updated security procedures. Retool also urged Google to reconsider the cloud-syncing feature in its Authenticator app.

Deepfakes on the Rise: How to Fortify Your Cyber Defenses Now

The Federal Bureau of Investigation, National Security Agency and U.S. Cybersecurity and Infrastructure Agency have released a joint report outlining the various social engineering threats posed by deepfakes.

“Threats from synthetic media, such as deepfakes, present a growing challenge for all users of modern technology and communications, including National Security Systems, the Department of Defense, the Defense Industrial Base and national critical infrastructure owners and operators,” the report says. “As with many technologies, synthetic media techniques can be used for both positive and malicious purposes. While there are limited indications of significant use of synthetic media techniques by malicious state-sponsored actors, the increasing availability and efficiency of synthetic media techniques available to less capable malicious cyber actors indicate these types of techniques will likely increase in frequency and sophistication.”

The agencies conclude that organizations should use a combination of techniques and technologies to defend themselves against these attacks. “Organizations can take a variety of steps to identify, defend against and respond to deepfake threats,” the report says.

“They should consider implementing a number of technologies to detect deepfakes and determine media provenance, including real-time verification capabilities, passive detection techniques and protection of high-priority officers and their communications. Organizations can also take steps to minimize the impact of malicious deepfake techniques, including information sharing, planning for and rehearsing responses to exploitation attempts, and personnel training.”

The report adds, “Every organization should incorporate an overview of deepfake techniques into their training program. This should include an overview of potential uses of deepfakes designed to cause reputational damage, executive targeting and BEC attempts for financial gain, and manipulated media used to undermine hiring or operational meetings for malicious purposes. Employees should be familiar with standard procedures for responding to suspected manipulated media and understand the mechanisms for reporting this activity within their organization.”

This article is redistributed with permission from KnowBe4.

The Emergence of WormGPT

In recent years, the world has witnessed an alarming rise in cyberattacks, with hackers continually evolving their techniques to breach security systems and gain unauthorized access to sensitive information. One disconcerting development in this realm is the emergence of WormGPT, an advanced artificial intelligence phenomenon that poses a significant threat to the cybersecurity landscape.

WormGPT is a variant of OpenAI’s GPT model designed to better understand and generate programming languages. This AI application is powered by a massive neural network. It uses deep learning algorithms to generate computer worms. Traditionally, cybercriminals have relied on programming skills to craft viruses and worms, but with WormGPT, the process becomes automated and more adaptable.

While most AIs have great potential for positive applications, there is a risk that they could be used to assist in cyberattacks, such as crafting sophisticated phishing emails or generating malicious code. WormGPT has reinvented the game in cyberattacks by producing massive amounts of data to reproduce human-like text mimicking human behavior.

Once in motion, this AI regenerates human-like text by predicting what comes next in a sequence of words. Being trained to comprehend grammar, context and semantics, this behavior enables it to produce coherent and contextually relevant responses. Now you can see why this is a dangerous tool.

If you feel as if you are infected with WormGPT, disconnect the infected system from the network or internet connection immediately. This will prevent the worm from spreading further or communicating with command-and-control servers. Once the worm is identified, you can try to locate target removal instructions or other tools specific to that variant of the worm. Removing infected files and keeping your antivirus software up to date can help prevent or slow WormGPT attacks.

MGM Suffers Ransomware Attack that Started with a Simple Helpdesk Call

As the aftermath unfolds, the details surrounding the recent attack on MGM Resorts provide crucial insight into the attack's impact, who is responsible and how it started.

On Sept. 11, Las Vegas-based MGM Resorts International reported a cybersecurity "issue" affecting many of the company's systems. A report with the Securities and Exchange Commission was filed on Sept. 12, denoting that the issue was severe enough to inform law enforcement and taking measures including "shutting down systems." It was later determined that a ransomware attack had occurred, affecting the company's website, reservation systems, key card systems and more.

According to the Wall Street Journal, half of a $30 million ransom was paid to those behind the attack. There is some confusion as to who is responsible for this attack. Early on, a tweet by vx-underground attributed the attack to the ALPHV ransomware gang. But others are attributing the attack to a cybercriminal group known as both Scattered Spider and UNC3944 – a group thought to be made up of teenagers operating from both the U.S. and the U.K. They reportedly encrypted more than 100 MGM ESXi hypervisors.

But the more immediate issues are how did this even happen, and, given that this is a ransomware attack, which likely includes data exfiltration and extortion, was there any data stolen?
According to the previously mentioned tweet by vx-underground, it is believed that simple social engineering and a password reset call to the helpdesk were the cornerstones of the attack. Compromising a single account is more than enough of a foothold to spread malware via email and potentially log onto a virtual, remote or even on-premises endpoint.

A second SEC filing by MGM Resorts parent company, Caesars Entertainment, provides some insight into what kind of data was accessed and potentially stolen.

The threat actors responsible "acquired a copy of, among other data, our loyalty program database, which includes driver's license numbers and/or Social Security numbers for a significant number of members in the database."

From the filing, it appears that the paid ransom was made to "ensure that the stolen data is deleted by the unauthorized actor."

Given that the individuals in the loyalty program are those that spend money (which includes high rollers), it is fairly likely that those individuals will become targets themselves of social engineering attacks in an attempt to get them to part with thousands or even millions of dollars themselves.
The complete outcome of this attack remains to be seen. In just three days, there is so much detail that paints a devastating picture for MGM. The next few weeks will provide more clarity on just how impactful this attack was.

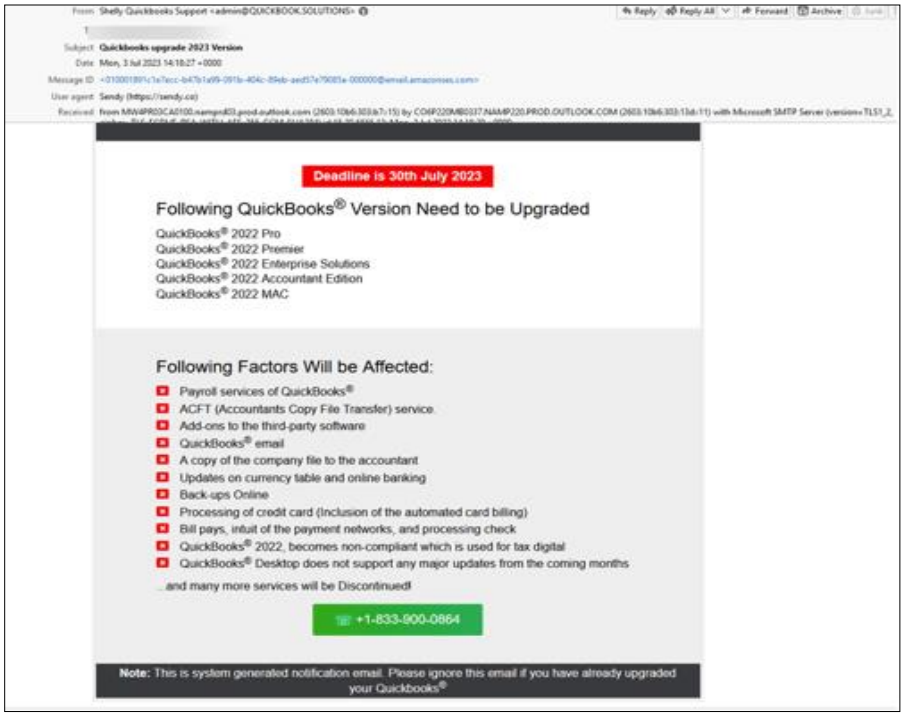
All it took to cost MGM millions was 10 minutes worth of rudimentary social engineering. Think about that for a moment. Putting strict processes in place around updating credentials as well as the use of multi-factor authentication for *every single user* are needed steps to significantly reduce the risk of a successful initial attack that will act as the foothold for a larger one like that of MGM Resorts.

This article is redistributed with permission from KnowBe4.

New Scam Impersonates QuickBooks to Steal Credentials, Extract Money

Establishing urgency through a false need to “upgrade” or lose services, this new attack takes advantage of the widespread use of the popular accounting app to attract victims.

Impersonation in phishing attacks only works if the target has an established rapport or relationship with the sender. And in the case of QuickBooks, there are about 8 million targets worldwide – large enough to send out mass emails and allow those that do not use the software to self-filter, leaving the customers to determine whether they are going to be victims or not.



Source: Avanan

This latest scam was identified by security researchers at Avanan. What is particularly interesting about this scam is the methods used to establish urgency. Take a look at the email used:

The email is about upgrading, and the tone is one of urgency. It quickly establishes that the recipient needs to upgrade or they will lose services like payroll or the account’s data. It also uses the color red, which naturally grabs our attention.

Lastly, in the example above, note how this email scam changes mediums, requiring the victim to call a phone number – a relatively recent tactic to remove the victim from an environment where security solutions can continue to assist in detecting malicious activity. The phone number is associated with a scam where callers are socially engineered into giving up their credit card details for the “upgrade."

This type of scam could just as easily be one that targets someone working in accounts payable, impersonating a vendor, making it important to educate all users of scams like these.

This article is redistributed with permission from KnowBe4.

Can Someone Guess My Password from the Wi-Fi Signal on My Phone?

Cybercriminals cannot ascertain your phone password just from a Wi-Fi signal, but they can come close, according to a method described in a recent research paper. Researchers have demonstrated a method that uses Wi-Fi signals to infer numerical passwords, and the mechanics behind it are nothing short of intriguing.

Side-channel attacks often reminiscent of James Bond-like espionage. So does a research paper that is to appear at ACM CCS later this year. The attack leverages something called Beamforming Information (BFI), which is essentially navigation instructions that guide your phone in sending data to an access point. These instructions are updated periodically to account for the phone moving or obstacles appearing.

Here is the kicker: when you type on your phone's screen, it directly affects the Wi-Fi antenna located behind the screen. It is the way you hold your phone. As a result, the BFI signal contains enough information that depends on your way of holding the phone and typing to capture your keystrokes. So, what is the best part? Attackers do not even need to hack into your Wi-Fi, which is increasingly protected by evolving hardware and software configurations.

Inferring passwords is not straightforward. Unlike natural languages, which have a linguistic structure that generative AI like ChatGPT can analyze, passwords lack such structure. The inference relies on independent keystroke features or transition features between two keystrokes (e.g., the time it took to move from one key to another). BFI signals are also sparse and sporadic, making the task even more challenging.

The Results

After extensive evaluations, the researchers found that their method, dubbed Wiki-Eve, achieves an 88.9% accuracy rate for identifying single numerical keys and an 85% top-100 accuracy for inferring a six-digit numerical password. While this may not be a realistic attack vector at the moment, it is worth noting that six-digit codes are often used in multifactor authentication.

This Wi-Fi-based attack is not an isolated case. Researchers are aware of other side channel attacks involving radio frequency, acoustic, vision, motion sensors and electromagnetic emissions. However, few are as covert and easily executable as this Wi-Fi-based method. Attackers could simply sit in a café somewhere near you and run the attack from their smartphone.

The Takeaway

Of course, a six-digit password is nothing people should be using. And your organization’s password policy should not allow these kinds of passwords in the first place. We recommend using passphrases, or preferably password managers that give you randomized passwords with at least eight characters. On top of that, you should also use phishing-resistant MFA.

This article is redistributed with permission from KnowBe4.

Training & 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/

Upcoming Events

- **Oct. 4:** SANS Webinar: Think Like a Hybrid Attacker Solutions Forum 2023
- **Oct. 4:** SANS Webinar: How to Get started with Cybersecurity
- **Oct. 11:** SANS Webinar: If Cybersecurity Is Too Difficult, You Might Be Doing It the Hard Way
- **Oct. 12:** SANS Webinar: Three Cloud Security Differentiators for Leaders
- **Oct. 12:** SANS Webinar: Enhance Security Investigations with ServiceNow Asset Data
- **Oct. 17:** SANS Webinar: Setting Up OSINT Watchdogs: Create Your Own Free Persistent Monitoring Tools with Python
- **Oct. 17:** SANS Webinar: Network Security in the Hybrid Cloud Era

View a list of upcoming SANS webcasts.

Be sure to follow the N.C. Department of Information Technology on 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.