Monthly Cybersecurity Newsletter

March 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

Cellphone Outage Highlights Importance of Resiliency, Change Management

A recent power outage that disrupted calls and text messages for more than 70,000 customers of a major U.S. telecommunications provider highlights the importance of critical infrastructure resilience and a regularly monitored change management program – both of which serve as a crucial component of operational security.

Crippling one's ability to communicate can have a grave impact on national security as well as our supply chain, making us more vulnerable to attacks.

The outage was attributed to an incorrect process applied during the expansion of the cellphone provider's network. It was not an adversarial attack, but one that is worth noting. In an actual cyber-related incident, how quickly we can recover and restore would be a factor. This incident tested that ability.

Although the incident was not cyber-related, the Federal Communications Commission and other federal agencies are further investigating.

Meanwhile, the cellphone company is taking measures to help prevent such outages from happening again and has offered impacted customers a $5 credit to accommodate for the disruption.

Advanced AI Tops Concerns This Election Season

With election underway, there is a need to consider the possibility of Election Day scams. This can encompass a wide array of potential threats – ranging from AI-generated disinformation to cyberbullying – threatening the integrity of the entire electoral system.

A key concern is the disruption of election cycles using advanced AI tools, which have made creating and disseminating deepfakes and disinformation more accessible. These technologies can fabricate convincing

photos, video, and audio, making it challenging for voters to discern truth from manipulation.

Hackers use a variety of tactics to gain unauthorized access or cause disruption. From exploiting software vulnerabilities to ransomware with denial-of-service attacks to disrupting the supply chain, there are no limits to what could be done.

Corrupting vendors who supply election services, such as voter registration databases, electronic poll books or voting machine software, is also an area of concern. Compromising these systems can give hackers access to a broader range of election infrastructure, allowing them to control election results or shut down the system.

We also should think about the security of the election workers at election sites. Those looking to disrupt the election process or altar election results could consider social engineering tactics to manipulate poll workers.

This could inolve quid pro quo tactics, in which workers are offered something in exchange for information or location access. For example, an imposter posing as an IT worker called to fix a technical issue might require a worker's login credentials or direct access to election systems.

Tailgating behind an authorized user is also a way to gain unauthorized access. Hackers will even go as far as finding sensitive information about the worker, threatening to expose it if the worker refuses to follow through with orders. To defend against these tactics, poll workers and election officials will have to be trained to recognize social engineering attempts.

Another aspect of concern is the potential impact of a government shutdown during the election preparation process, which focuses on security. A shutdown could interrupt critical federal certification processes for voting systems and hinder the partnership between local, state and federal officials in ensuring election security. This scenario underscores the importance of timely federal assistance and support in safeguarding the electoral process against various threats, including foreign interference.

These threats, and many others, require vigilance and proactive measures from both officials and the public to protect the integrity of elections and ensure a fair and secure voting process.

Americans Lose a Record $10 Billion to Fraud in 2023; Mostly Due to Investment Scams

The U.S. Federal Trade Commission has disclosed that people in the United States lost a record $10 billion to fraud in 2023, a 14% increase from 2022.
Nearly half of the losses were due to investment scams.

Consumers reported losing more money to investment scams – more than $4.6 billion – than any other category in 2023. That amount represents a 21% increase over 2022," says the FTC. "The second highest reported loss amount came from imposter scams, with losses of nearly $2.7 billion reported."

In 2023, consumers reported losing more money to bank transfers and cryptocurrency than all other methods combined.

The median loss from a scam in 2023 was $7,000, compared to $3,000 in 2019. The five most common fraud techniques involved imposters, online shopping, phony sweepstakes or prizes, investments and fake job opportunities.

“The FTC received fraud reports from 2.6 million consumers last year, nearly the same amount as in 2022. The most commonly reported scam category was imposter scams, which saw significant increases in reports of both business and government impersonators,” the FTC says.

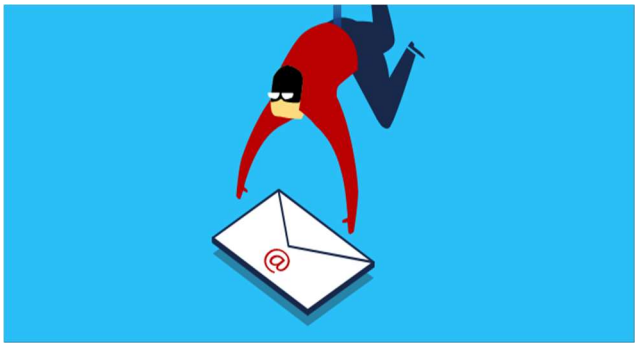
“Online shopping issues were the second most commonly reported in the fraud category, followed by prizes, sweepstakes, and lotteries; investment-related reports; and business and job opportunity scams.”

Notably, email was the most common medium used by scammers to target victims in 2023.

“Another first is the method scammers reportedly used to reach consumers most commonly in 2023: email,” the FTC says. “Email displaced text messages, which held the top spot in 2022 after decades of phone calls being the most common. Phone calls are the second most commonly reported contact method for fraud in 2023, followed by text messages.”

This article is redistributed with permission from KnowBe4.

Phishing Campaign Exploits Remote Desktop Software



A phishing campaign is attempting to trick users into downloading remote-monitoring and management (RMM) software, according to researchers at Malwarebytes.

While these tools are legitimate, they can be exploited by threat actors to carry out many of the same functions as malware. These tools may also be less likely to be flagged as malicious by antivirus software.

“The modus operandi of these threat actors involves deceiving employees through sophisticated scams and deceptive online advertisements,” the researchers write. “Unsuspecting employees, misled by these tactics, may inadvertently invite these criminals into their systems. By convincing employees to download and run these seemingly benign RMM applications under the guise of fixing non-existent issues, these fraudsters gain unfettered access to the company’s network.”

The scammers trick users into visiting a phishing site that impersonates the user’s bank.

“We believe victims are first targeted and then contacted via phishing emails or text messages (smishing) based on their position in the company,” the researchers write.

“Attackers could trick them by sending them to a typical phishing page or making them download malware, all of which are good options. However, they are instead playing the long game where they can interact with their victims. Users are directed to newly registered websites that mimic their financial institution. To get support, they need to download remote desktop software disguised as a ‘live chat application.’"

The phony live chat application is actually remote desktop software.

“In this instance, they are using a legitimate (although outdated) executable file, which would not be detected as malicious by security products,” Malwarebytes says. “Running the program will show a code that you can give to the person trying to assist you. This can allow an attacker to gain control of the machine and perform actions that look like they came directly from the user.”

This article is redistributed with permission from KnowBe4.

Synthetic Data: The New Frontier in Cyber Extortion

Organizations are increasingly facing cyberattacks resulting in data breaches, and part of their post-incident responsibilities include adhering to mandatory reporting requirements.

Notably, the infamous BlackCat ransomware group has been exploiting these requirements for their own benefit. They apply pressure on victims by threatening to inform the Securities and Exchange Commission about the company's supposed failure to report significant data breaches. The validity of the breach claim becomes inconsequential in the face of such extortion tactics, as the mere suggestion of regulatory non-compliance can be damaging enough.

Cybercriminals are using new tools like deepfakes and voice-fakes to their advantage, exploiting even the small gaps in knowledge and awareness amongst their targets. Advancements in artificial intelligence are escalating the difficulty of distinguishing between authentic and manipulated information. Deepfakes and voice-fakes are becoming so convincing that they can easily mislead the public, complicating the fight against the spread of misinformation and disinformation.

Ransomware groups are evolving their methodologies, moving away from encrypting data to simply threatening to leak stolen data on the dark web. This shift emphasizes the significance of the data breach itself over the disruption of operations. Some groups are even contemplating fabricating data breaches altogether. While claiming false breaches is not new, profiting from such deceptions is a relatively untapped strategy.

A case involving a European car rental company illustrates this emerging threat. A data set was published by an individual claiming to have hacked company, but the company was quick to refute the claim, stating that the data did not match its records. Despite the inaccuracy, such synthetic data sets can still cause harm by appearing credible, forcing organizations to invest resources in unnecessary investigations and dealing with potential reputational damage.

This situation underscores the need for organizations to prioritize their ability to manage what has become more of a public relations challenge than a technical one. Public disinformation and compliance with reporting obligations require a joint effort between public relations departments and cybersecurity teams. Organizations must therefore cultivate security awareness not only internally but also among their customers and other stakeholders. In response to these emerging threats, it's essential that PR experts and security professionals combine their expertise to present a unified front.

This article is redistributed with permission from KnowBe4.

Face-off: New Banking Trojan Steals Biometrics to Access Victims' Bank Accounts

Venturebeat had the scoop on a fresh Group-IB report. They discovered the first banking trojan that steals people's faces. Unsuspecting users are tricked into giving up personal IDs and phone numbers and are prompted to perform face scans. These images are then swapped out with AI-generated deepfakes that can easily bypass security checkpoints.

The method – developed by a Chinese-based hacking family – is believed to have been used in Vietnam last month, when attackers lured a victim into a malicious app, tricked them into face scanning, then withdrew the equivalent of $40,000 from their bank account.

These hackers “have introduced a new category of malware families that specialize in harvesting facial recognition data,” Sharmine Low, malware analyst in Group-IB’s Asia-Pacific APAC threat intelligence team, wrote in a blog post. “They have also developed a tool that facilitates direct communication between victims and cybercriminals posing as legitimate bank call centers.”

A Whole New Fraud Technique

These hackers “have introduced a new category of malware families that specialize in harvesting facial recognition data,” Low said.

Face swap deepfake attacks increased by 704% between the first and second halves of 2023, according to a new iProov Threat Intelligence Report. The biometric authentication company also discovered a 672% increase in the use of deepfake media being used alongside spoofing tools and a 353% increase in the use of emulators (which mimic user devices) and spoofing to launch digital injection attacks.

Furthermore, “cybercriminals are becoming increasingly creative and adept at social engineering,” Low writes. “By exploiting human psychology and trust, bad actors construct intricate schemes that can deceive even the most vigilant users.”

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 Training & Events

- **Mar. 4:** SANS Webinar: Detecting AI in OSINT Investigations
- **Mar. 6:** SANS Webinar: Why Do We Do What We Do? A Motivational Talk
- **Mar. 20**: SANS Webinar: SANS 2024 Threat Hunting Survey: Hunting for Normal Within Chaos
- **Mar. 21**: SANS Webinar: Azure Recon and Password Guessing
- **Mar. 25**: SANS Webinar: SANS 2024: SANS@Night - Cracking the Code: The Role of Programming in Information Security
- **Mar. 26**: SANS Webinar: Securely Moving to the Government Cloud
- 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.*