Monthly Cybersecurity Newsletter

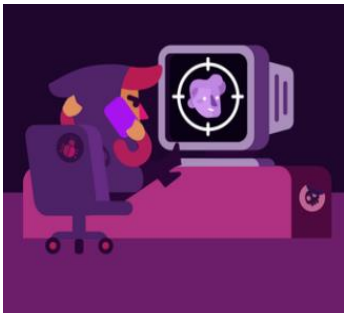
February 2024 Issue

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

Russian Hackers Win Big: Microsoft's Senior Executive Team Emails Breached



In a recent regulatory filing, Microsoft reported that its corporate email accounts were compromised by a Russian state-sponsored hacking group known as Midnight Blizzard, also identified as Nobelium or APT29.

Microsoft's disclosure aligns with new U.S. requirements for reporting cybersecurity incidents. The attack was detected Jan. 12, but it appears to have started in November 2023.

The Breach and Attack

The attack involved Russian hackers using a password spray attack to access a legacy non-production test tenant account at Microsoft. Password spraying is a brute-force technique where attackers attempt to log in using a list of potential usernames and passwords.

This indicates that the breached account did not have two-factor authentication – or multifactor authentication – enabled. Once the hackers gained access to the test account, they used it to access a "small percentage" of Microsoft's corporate email accounts over the course of a month.

Notably, the targeted email accounts included members of Microsoft's leadership team as well as employees in their cybersecurity and legal departments. Microsoft emphasized that this breach was due to a brute-force password attack and not a vulnerability in its products or services.

About Nobelium (aka Midnight Blizzard, APT29)

Nobelium is a Russian state-sponsored hacking group believed to be associated with Russia's Foreign Intelligence Service. It gained notoriety for its involvement in the 2020 SolarWinds supply chain attack, which impacted both Microsoft and several U.S. government agencies. Nobelium is known for conducting cyber espionage, data theft and developing custom malware for its attacks.

Microsoft stated that the breach did not result in the theft of customer data, access to production systems or proprietary source code.

Response and Impact

Microsoft is actively investigating the breach and will provide additional details as appropriate. The company has affirmed that the breach did not have a material impact on its operations. The Cybersecurity & Infrastructure Security Agency is working closely with Microsoft to assess the incident's impact and protect potential victims. There is no evidence of hackers accessing customer data or critical systems.

This article is redistributed with permission from KnowBe4.

Social Engineering Attacks Are Rising in the Trucking Industry

Spear phishing and voice phishing (vishing) are on the rise in the trucking industry, according to a new report from the National Motor Freight Traffic Association.

“Spear phishing is still one of the most effective tools attackers have to breach networks,” the report says.

“Also expected is an increase in vishing, which is when a scammer calls a person pretending to be a reputable company or organization, or even a co-worker (or someone’s boss), and urges the person to provide personal or sensitive data or send money to a fraudulent account.”

The report also predicts a rise in phishing attacks that use QR codes to trick users into clicking on malicious links. “The convenience of QR codes is training people to unthinkingly do the very thing that cybersecurity professionals say they should never do, which is to click on random links without knowing where they go,” the report says.

“Not only do QR codes encourage poor security practices, but they also obscure some of the techniques many would use to verify if a typical URL or hyperlink is safe to click on. With QR codes, attackers or scammers can trick users into visiting malicious sites or fool them by showing them things they can monetize, such as gift cards, discount coupons or cryptocurrency.”

The report notes that most ransomware attacks are preceded by phishing or other social engineering tactics.

“Hackers frequently use phishing scams to gain access to a carrier’s enterprise system,” the report says. “Once they can access the system, they use that access to launch ransomware attacks. Phishing attacks generally take the form of deceptive communications that trick people into clicking links or opening attachments. Trucking companies’ best preparation for and defense against these attacks is to thoroughly train their people to spot a phishing attack.”

This article is redistributed with permission from KnowBe4.

Facebook Phishing Scams Target Concerned Friends and Family

BleepingComputer describes a phishing scam that's been running rampant on Facebook for the past several months, in which threat actors use hacked accounts to post links to phony articles implying that someone has been killed in an accident.

The Facebook posts have captions like "I can't believe he is gone," accompanied by thumbnails of news articles involving car accidents or crime scenes. Users are more likely to click on the links since they've been posted by a friend's account. The links lead to phishing sites that ask users to enter their Facebook credentials to view the videos.

"To entice a visitor to enter their password, they show what appears to be a blurred-out video in the background, which is simply an image downloaded from Discord," BleepingComputer says.

"If you enter your Facebook credentials, the threat actors will steal them, and the site will redirect you to Google. While it is not known what the stolen credentials are used for, the threat actors are likely to use them further to promote the same phishing posts through the hacked accounts. This phishing scam is widely spread, with BleepingComputer seeing numerous posts created each day by friends and family who unwittingly had their accounts hacked through the same scam."

BleepingComputer notes that enabling multifactor authentication will give your Facebook account an extra layer of protection against phishing attacks.

"As this phishing attack does not attempt to steal two-factor authentication (2FA, also known as MFA) tokens, it is strongly advised that Facebook users enable 2FA to prevent their accounts from being accessed if they fall for a phishing scam," BleepingComputer says. "Once enabled, Facebook will prompt you to enter a unique one-time passcode each time your credentials are used to log in to the site from an unknown location. As only you will have access to these codes, even if your credentials are stolen, they cannot log in."

It's worth keeping in mind, however, that some phishing attacks will attempt to trick you into entering a 2FA code as well.

The Hidden Threat of Juice Jacking in Cybersecurity

If you have ever been in a public location with a low phone battery, your first instinct is to find a charging station to charge your phone, right?

In the world of cybersecurity, there is a lesser known but equally sinister threat lurking in public charging stations, better known as “juice jacking.” This cyberattack may sound benign, but it poses a significant risk to unsuspecting users who plug their devices into compromised charging ports.

Let’s first define juice jacking and why it is a threat.

Juice jacking is a cyberattack method where malicious actors exploit USB charging ports to install malware or conduct data theft from connected devices. These compromised USB ports can be found in public locations, such as airports, hotels, cafes or any public charging stations designed to offer convenience to users on the go.

How does it work?

The mechanics of juice jacking are relatively straightforward but alarmingly effective. A USB port is not solely for charging; it also facilitates data transfer. This dual functionality is where the vulnerability lies. When a device is connected to a tampered USB charging port, it becomes susceptible to unauthorized access. Attackers can exploit this connection to inject malware into the device or extract sensitive information, ranging from personal photos and emails to passwords and banking details.

What are the risks involved?

The risks associated with juice jacking are profound. Beyond the immediate threat of malware infection and data theft, the implications can extend to identity theft, financial loss and long-term privacy breaches. The stealthy nature of juice jacking means that victims may remain unaware of the compromise for an extended period, allowing attackers to exploit their information or device functionalities, such as the camera and microphone, without detection.

How do you protect yourself from juice jacking? There are a few things that you can do to help protect yourself:

- Using a personal charger. Plug your personal charger directly into an electrical outlet and avoid USB charging stations altogether.
- Carry a portable power bank to eliminate the need to use public USB ports.
- Use small, portable data blocking devices that can be plugged into a USB charging cable, allowing electricity to flow for charging while blocking data transfer pins to prevent unauthorized data exchange.
- Exercise caution when charging devices in public areas. If a charging station or the surrounding area looks tampered with or suspicious, it's safer to avoid using it.
- Always keep your device locked while charging in a public space. This may not prevent juice jacking, but it adds an extra layer of security against direct file access.

As awareness of juice jacking grows, so do the efforts to combat it. Manufacturers and software developers are continually working on enhancing USB security features to prevent unauthorized data transfers. Meanwhile, public charging station providers are also improving security measures to protect users from such threats. The key to staying safe, however, lies in individual awareness and cautious practices.

Juice jacking highlights a critical aspect of cybersecurity: the constant need for vigilance, even in seemingly mundane activities like charging a device. By understanding the risks and adopting simple preventive measures, individuals can significantly reduce their vulnerability to this surreptitious form of cyberattack. As technology evolves, so do the tactics of cybercriminals, making continuous education and precautionary practices essential components of digital security in the modern world.

Work-From-Home Job-Posting Scam Goes the Extra Mile to Trick Victims

A new job posting scam found by IT security company Qualysys is focused on capturing the victim's identity details, accessing the victim's Facebook accounts and committing fraud.

In this new scam, legitimate Facebook advertising is used to post fake work-from-home job ads from several companies. As with most of these scams, victims are directed to a third-party messaging app and are asked to sign a realistic-looking employment contract.

This type of scam has been seen everywhere, including LinkedIn and legitimate career sites, attempting to do everything from infect victims with malware to stealing personal information.

What makes this case particularly notable is the incorporation of an authentic-looking contract, which is a new tactic. This particular scam aims not to infect any devices but to acquire personal information. The inclusion of a contract lends a sense of credibility, leading victims to willingly submit photos of both sides of their driver's license and to digitally transfer a check from the fraudulent employer for procuring job-necessary software.

In the end, the victim has lost control over their identity and potentially some of the funds in their bank account. This is only because these bad actors' intent is not about gaining access to a corporate network; this scam could just as easily taken a turn to infect the victim's computer with malware.

Regardless of the malicious outcome, staying vigilant against scams like this is imperative so they understand that even when it's the victim themselves that seems to have initiated the interaction, it really was the scammer that posted the job ad in the first place.

This article is redistributed with permission from KnowBe4.

New Cyber and Privacy Training Courses Available in February

The Office of State and Human Resources has released new training to bolster cybersecurity and privacy education among state employees. The training was released Feb. 2 with a scheduled completion date of March 3, giving employees approximately 30 days to complete the material. The courses aim to equip employees with the latest tools, knowledge and practices to protect sensitive information and navigate through the ongoing landscape of digital threats.

The new training initiative underscores the state of North Carolina's commitment to enhancing the cybersecurity posture of the state. Cyberthreats are becoming more frequent and continue to evolve in sophistication. The need for up-to-date training has never been more critical. This training was developed in efforts to close the gap.

Here are the links for state employees to access the material through the North Carolina Learning Center.

- Privacy: The Value of Data
- Privacy: The What, Why and How of Data Privacy (2024)
- Privacy: Security Bytes: PII
- Privacy: Privacy vs Security - What's the Difference?
- Cybersecurity: How to Behave: Protecting Sensitive Information

Protecting our personal privacy and the privacy of others is hard work, but with the right amount of vigilance and attention to detail, employees can play a key role in mitigating potential threats and ensuring the integrity of our sensitive information.

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

Feb. 15: SANS Webinar: Cloud Flight Simulator Part 4: Least Privileged Pods with Kubernetes Workloads

Feb. 19: SANS Webinar: Enhancing Threat Hunting Efficiency with AI and Machine Learning

Feb. 20: SANS Webinar: SANS Security East 2024: Keynote - Cybersecurity Controls For ICS and Critical Infrastructure in Times of Warfare

Feb. 21: SANS Webinar: Promoting Your Path: From Engineer to CISO

Feb. 21: SANS Webinar: From Pentest to Red Team: Overview of The Necessary Skills and Breakdown of Frameworks

Feb. 26: SANS Webinar: OT Penetration Testing - Lessons Learned from Penetration Testing Operational Environments

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.*