Monthly Cybersecurity Newsletter

January 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

IRS Warns of Expected Wave of Tax Scams

Urging taxpayers and tax professionals to be vigilant, the Internal Revenue Service provides simple guidance on how to spot new scams aimed at being able to file fake tax returns.

Apparently, there are actually three certainties in life: death, taxes and scams revolving around taxes. This reminder, according to the IRS, was part of its annual security summit. As with any major event that has the attention of millions of people simultaneously, tax season is no exception. In recent years, we've seen a consistent surge in tax-related scams during the months before taxes are due in the United States.

The IRS pointed out some very simple ways to spot scams around taxes. Given that many scams impersonate the IRS, the first recommendation is to scrutinize the method of communication. Most scams start with an email or a text — communication mediums the IRS almost never uses. Official IRS communication is most often handled through the mail.

It is not out of the realm of possibility for a scam to pretend to be a well-known tax preparation company or online service claiming to get you a refund … "guaranteed." If it hasn't already been done, we are sure to see it next year!

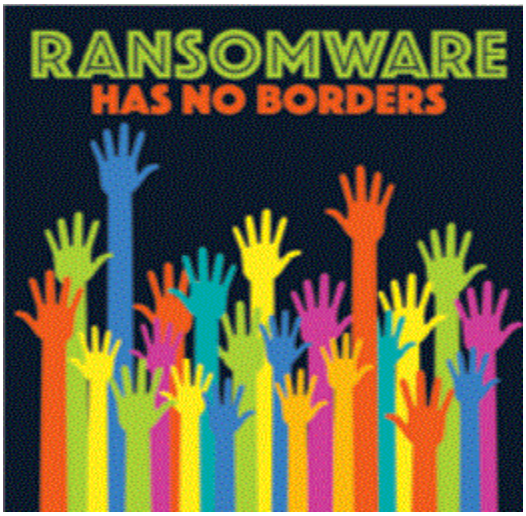
Those responsible for an organization's finances could also be targeted in an attempt to solicit payments. Be sure those individuals remain vigilant as we move into the months leading up to April 15.

This article is redistributed with permission from KnowBe4.

Virtual Hostage: The Unsettling Cyber Kidnapping of a Foreign Exchange Student

According to a recent article published by ABC News on 17-year-old Chinese exchange student Kai Zhuang, a new cyber-related scheme is emerging.

The idea of "cyber kidnapping" with the goal of extortion is taking on a new form. For most of us, our family is the most valuable thing that we possess, and we tend to protect them at all costs. This is exactly what cyber kidnappers rely on to make this scam successful.



To give a little background on this incident, Zhuang was reported missing five days before the start of the new year. In this scam, Zhuang was manipulated by cyber kidnappers into believing that his family in China was in danger. He was forced to isolate himself in a wooded area and provide pictures that made it appear he was being held captive. These photos were then sent to his family to extort the ransom, which we later found out was the whopping amount of $80,000. Zhuang complied with the kidnappers' demands and provided the photos under the belief that his family would otherwise be harmed.

On the other end of the scheme, the kidnappers contacted Zhuang's parents and provided them with the photos he was forced to take, making them believe that he was indeed in danger. His parents did not hesitate to send the kidnappers' asking price with the goal of saving their child's life. And just like that, the scam was successful.

The investigation, which involved analyzing bank records, purchases and phone ping records, led the police to believe Zhuang was isolating in a tent about 40 kilometers north of Riverdale, near Brigham City, Utah. He was found alive but in a distressed state, with no heat source in the tent and only a heat blanket, a sleeping bag, limited food and water and several phones assumed to be used in the cyber kidnapping.

The Riverdale Police Department, in collaboration with the FBI, the U.S. embassy in China and Chinese officials, played a crucial role in locating Zhuang. After his rescue, Zhuang expressed a desire to speak with his family, who had already paid the ransom during the scam.

This incident sheds light on how easy it is to pull off a cyber kidnapping scheme. Victims are typically instructed to isolate themselves and are coerced into taking pictures in distress, which are then used to demand money from their families. Authorities advise anyone who believes they have been targeted by cyber kidnappers to immediately cut all communications with them and contact law enforcement.

Russian Hackers Indicted for Phishing Attacks Against U.S., Allies

The U.S. Justice Department has indicted two individuals for launching spear phishing attacks against the U.S., the UK, Ukraine and various NATO member countries on behalf of the Russian government.

“The indictment … alleges the conspiracy targeted current and former employees of the U.S. Intelligence Community, Department of Defense, Department of State, defense contractors, and Department of Energy facilities between at least October 2016 and October 2022,” the Justice Department said in a press release.

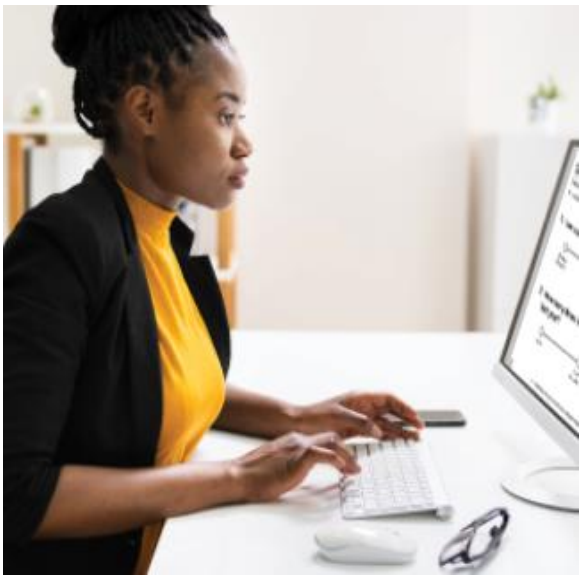
“In addition, the indictment alleges the conspirators – known publicly by the name ‘Callisto Group’ – targeted military and government officials, think tank researchers and staff, and journalists in the United Kingdom and elsewhere, and that information from certain of these targeted accounts was leaked to the press in Russia and the United Kingdom in advance of U.K. elections in 2019.”

The individuals allegedly crafted tailored phishing attacks to steal victims’ credentials.

“As a common example, the conspirators used ‘spoofed’ email accounts designed to look like personal and work-related email accounts of the group’s targets,” the Justice Department says. “The conspirators allegedly also sent sophisticated looking emails that appeared to be from email providers suggesting users had violated terms of service. These messages were designed to trick victims into providing their email account credentials to false login prompts. Once the conspirators fraudulently obtained the victims’ credentials, they were able to use those credentials to access the victims’ email accounts at will.”

Assistant Attorney General Matthew G. Olsen of the Justice Department’s National Security Division stated, “The Russian government continues to target the critical networks of the United States and our partners, as highlighted by the indictment unsealed today. Through this malign influence activity directed at the democratic processes of the United Kingdom, Russia again demonstrates its commitment to using weaponized campaigns of cyber espionage against such networks in unacceptable ways. The Department of Justice will respond to such behavior with an even more determined commitment to disrupt those activities and to hold accountable the individuals responsible.”

Undercover Threat: North Korean Operatives Infiltrate U.S. Companies Through Job Platforms



Researchers at Nisos warn that North Korean threat actors are impersonating skilled job seekers to obtain remote employment at U.S. companies.

“The identified personas claim to have highly sought-after technical skills and experience and often represent themselves as U.S.-based teleworkers, but Nisos investigators found indications that they are based abroad,” the researchers write.

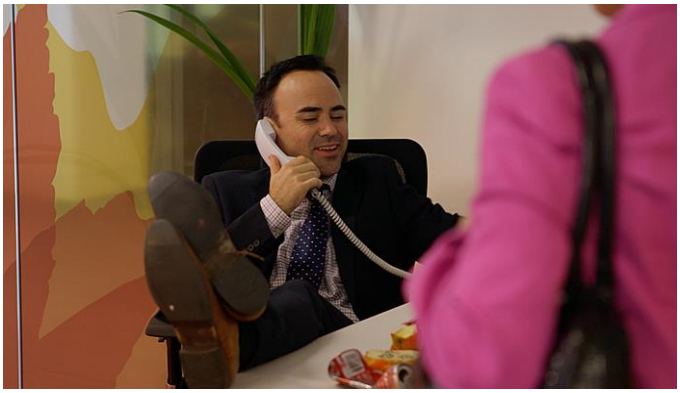
“Boasting expert-level skills in mobile and web-based applications as well as a number of programming languages, the personas also list significant remote work experience which can be difficult to verify. The personas further obfuscate their identities by impersonating U.S.-based individuals’ identities and/or copying resume content from publicly visible profiles of unassociated individuals, further increasing the difficulty of identifying the personas.”

The researchers note that the threat actors have crafted phony personas on job-seeking platforms.“Nisos investigators found that although the personas are often active on professional networking sites, IT industry-specific freelance contracting platforms, software development platforms and common messaging applications, they are usually not active on social media platforms,” the researchers write.

“Nisos assesses that the accounts were created solely for the purpose of acquiring employment. Investigators found instances of several accounts, associated with a persona, using the same picture but different names; other accounts lacked profile photos. Investigators also found that many of the accounts are only active for a short period of time before they are disabled. Nisos assesses the accounts remained active only for a short period of time because they were created in support of an application for a specific position or were flagged for fraudulent behavior and removed by the platform provider.”

Nisos explains that hiring these individuals is a violation of U.S. and UN sanctions since they “provide a critical stream of revenue that helps fund the DPRK regime’s highest economic and security priorities, such as its weapons development program, and may also leak intellectual property (IP) and other sensitive information to the DPRK.”

Who's Calling? Spam, Scams and Wasted Time



First-ever insights into annoying spam calls provide enlightening details into how many calls are there, where are they coming from and how much time is wasted dealing with them.

It's sort of the new normal — never answer your phone if you don't know the caller, and let it go to voicemail. Why? Because of the proliferation of spam calls that *nobody* wants to receive.

But just how bad is it? Global communications provider Truecaller released its first Monthly U.S. Spam and Scam Report, and there are some interesting bits of detail that give you an idea of just how much effort is being put into these calls that are riddled with scams:

- Americans receive 2.1 billion spam calls each month.
- The average American individually gets 5.6 spam calls a month.
- The average spam call is 3.36 minutes long.

What's interesting is where these come from: 90.66% of the calls originate from *within the U.S.*, but of the other nearly 10% of calls, the majority (84.5%) originates in India.

These spam calls are scams. Individuals need to be made aware of the types of scams, which will lower the effectiveness of these scams and thus undermine these cybercriminal organizations.

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/

Jan. 10: SANS Webinar: Identify, Evaluate & Prioritize Industrial Cyber Risk

Jan. 11: SANS Webinar: The ICS ATT&CK Map Series: Water Sector

Jan. 17: SANS Webinar: Hands-On Workshop | Least Privilege — An Adventure in Third-Party Cloud Account Access

Jan. 18: SANS Webinar: ICS/OT Cybersecurity Survey: 2023 AUS Insights

Jan. 18: SANS Webinar: Cloud Flight Simulator Part 2: Protecting Kubernetes Clusters with Admission

Jan. 24: SANS Webinar: Forensic Analysis of Apple IoT Devices (Apple TV, Watch, HomePod, HomeKit)

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.*