Monthly Cybersecurity Newsletter

August 2023 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

Nearly One-Quarter of All Emails Are Considered to Be Malicious

The quantity of emails involved in scams and cyberattacks continues to grow as credential theft and response-based phishing persist as top attack variants.

The ripple effect from cybercrime-as-a-service launching a few years back has reached critical mass, where we're seeing significant increases in the percentage of emails that are clearly determined to be malicious (7.7%) as well as those suspicious enough that users are recommended to not engage with (15.9%). This is according to Fortra's latest quarterly update, Phishing Trends and Tactics: Q1 of 2023.

Of those deemed malicious, 58% of them were related to credential theft attacks, with 40% of the emails involved in response-based phishing attacks. These details about the massive percentage of emails considered to be harmful to users and their organizations gives you a clear idea of what's important to cybercriminals: they either want your credentials outright or are wanting to engage users with social engineering for purposes of digital fraud, access to social media and crypto wallets.

Also, thinking about the "one-quarter" stat and merge it with the fact that 1 in 8 malicious emails get past security solutions, you can do some quick math and determine that literally *1 out of 32 emails sent gets to an inbox* – making your users the last line of defense. Only those users that are able to interact with email and the web with a sense of cyber-vigilance will be able to distinguish malice and suspicion quickly and avoid engaging with such content.

This article is redistributed with permission from KnowBe4.

Child Hackers: How Do Young People Inadvertently Develop into Proficient Online Criminals?

Numerous young people are battling to control their motivations on the web, in a scramble for fast excitement and the ability to move past restrictions to advance via gaming and other online activities, while possibly expanding their potential of inadvertently becoming a digital criminal. It is the thrill of the chase that empowers them to push past their limits.

A child's passion for gaming may trigger them to naturally develop advanced computing skills to include the understanding of programming, networking and system architecture. These skills can be beneficial for ethical purposes but can also be misused for hacking.

Today's gaming platforms are set up to encourage online interactions. These social interactions may connect the child to more experienced hackers who will in turn introduce them to more advanced hacking techniques possibly supplying them with malicious software in the process. Kids who download cheat programs, modifications or unofficial add-ons for games can inadvertently introduce malware or hacking tools onto their computers exposing them to other unknown hacking activities. These platforms also build trust between the hacker and the child whereas the child will divulge personal information about themselves or their household, making them vulnerable for other attacks.

Different online communities and forms dedicated to gaming can also be a hub for sharing hacking knowledge and tools. Here, children can learn about hacking techniques, engage in discussion and potentially be influenced by more experienced individuals.

It is best to teach your children how to protect themselves online to ensure their safety and their privacy. Talk to your child about the risks and teach them to keep their personal information private especially when dealing with strangers and potential online predators. It is also important for them to understand password security and not to share that information with others. Monitor your child's activities and let them know that all downloads are not safe.

Google Play Apps with Over 1.5M Installs Used as Spybots for China

In recent years, the rise of smartphones and mobile applications have transformed the way we live, work and communicate. However, this rapid growth has also opened doors to potential security risks, as malicious actors find new avenues to exploit vulnerabilities in app marketplaces like Google Play. One particular concern that has alarmed security researchers is the presence of China spybots hiding within seemingly harmless apps.

China spybots, as the name suggests, are malicious software created by entities with ties to China. These bots are designed to infiltrate devices by disguising themselves as legitimate apps, often found within the Google Play store. Unsuspecting users download these applications unaware of the hidden dangers lurking within.

The scale of this infiltration is vast and concerning. Recent revelations have unveiled instances where certain applications such as, File Recovery and Data Recovery (used as file management applications), were found sharing sensitive information with servers located in China, raising serious questions regarding the data privacy and security for millions of users. An even bigger revelation is that more than 1.5 million users have installed these applications under the disguise that their data was being protected.

This shocking discovery has alarmed both users and privacy advocates alike. Research has discovered that certain Android applications were transmitting sensitive and personal data to include emails, text messages and location information without the user's knowledge or consent. This revelation has brought to light serious concerns about data sovereignty. Data sovereignty works under the concept that data is subject to the laws and governance of the country in which it is located or where it originates. The bigger question here is how do we handle stolen cross-border data flows beyond our country's jurisdiction.

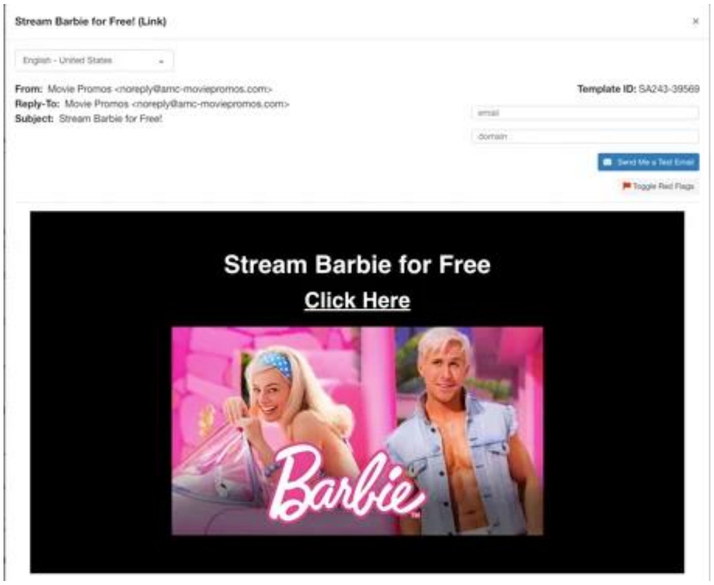
As an update, Google has since removed the infected applications from Google Play that listed the developer as Wang Tom and has implemented additional safeguards to contain and/or identify this type of malware. Please understand that any app in the app store could be infiltrated by bad actors and may go undetected. It is important to stay vigilant for any of us at anytime can fall victim to these attacks.

Barbie-Related Scams Emerge After Recent Movie Release

Scammers are taking advantage of the popularity of the Barbie movie, according to researchers at McAfee.

“In the last three weeks, we’ve seen 100 new instances of malware that have Barbie-related filenames,” the researchers write. “Once again, this shows how attackers have latched onto the movie’s hype, hoping the people will click the malicious files because the Barbie name is trending.

“The types of files varied but included typical types such as .html and .exe. By and large, attackers focused on the U.S., yet other countries have found themselves targeted as well.”



Stream Barbie for Free! (Link)

From: Movie Promos <noreply@amc-moviepromos.com>
Reply-To: Movie Promos <noreply@amc-moviepromos.com>
Subject: Stream Barbie for Free!

Template ID: SA243-39569

Steve Grobman, McAfee’s chief technology officer, notes that criminals often exploit popular topics to distribute scams.

“As Barbie makes her debut on the big screen, scammers are aiming to cash in on the summer blockbuster,” Grobman says. “A rash of scams have cropped up online, including bogus downloads of the film that install malware, Barbie-related viruses and fake videos that point people to free tickets – but lead to links that steal personal information with spyware instead.

“Cybercriminals are always on the lookout for opportunities to make phishing and other scams more attractive and believable. They often leverage popular and well-publicized events, such as movie premieres, concerts or sporting events to trick users into clicking on malicious links.”

McAfee offers several recommendations to help users avoid falling for these scams:

- **Stick with trusted retailers and streamers.** Keeping your shopping and viewing to known, reputable brands remain your safest bet online. Trusted retailers carry legitimate merchandise. And if counterfeit and knockoff goods do slip into their marketplaces, refund policies give you a way to recover your loss. Moreover, trusted streamers will only carry shows and events that they have the rights to. If you find an offer to stream something that’s heavily discounted, free or not available on known media outlets, it’s likely a scam. At the very least, it might be pirated content, which could carry malware threats along with it.

- **Purchase tickets from the theater chain or a reputable ticketing app**. Another way scammers like to cash in on a hot ticket is to open a bogus online box office that charges for tickets. Of course, they won’t deliver. They’ll simply take your money and your card number to boot. You can avoid this by purchasing your tickets online directly from the theater or with a reputable online movie ticketing app that you can find in Apple's App Store or Google Play.

- **Watch out for shoddy-looking sites**. Online scammers have various levels of sophistication when it comes to building and designing scam sites. Some can look quite legitimate, yet others look rather slapped together. In either case, keep a sharp eye out for poor web design, typos and grammatical errors, however small. These often indicate a scam site, as reputable companies make every effort to provide a clean and professional-looking experience.

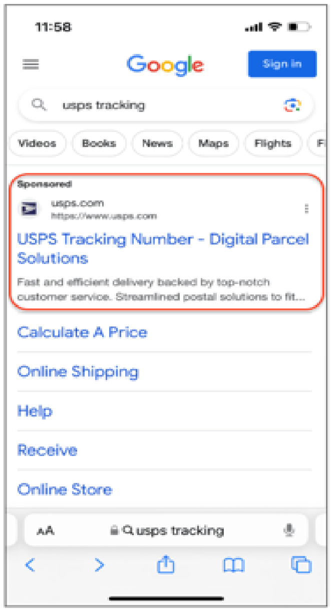
This article is redistributed with permission from KnowBe4.

Banking Detail Malvertising Attack Disguises Itself as a Foolproof USPS Google Ad

A new scam aimed at stealing your credit card and banking information has reared its ugly head as a completely legitimate ad that is likely to be clicked based on the corresponding search term.

If you type in "USPS Tracking" in Google, you probably want to enter a U.S. Postal Service tracking number so you can see where your package is, right?

So, if you saw the following result, would you give it a second thought?



Sponsored

usps.com
https://www.usps.com

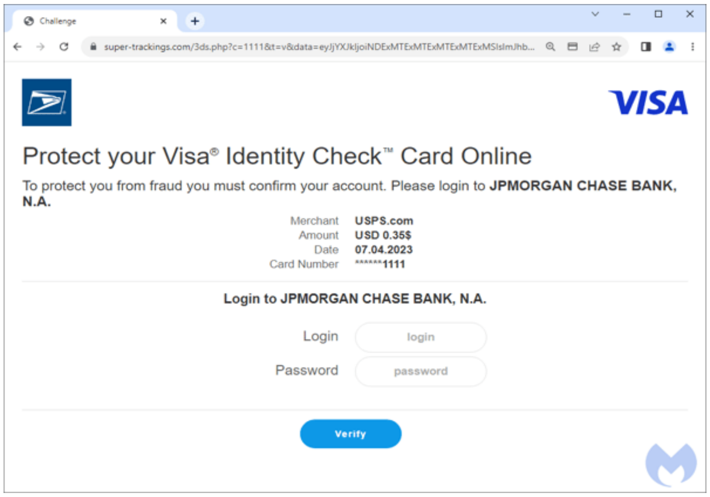
USPS Tracking Number - Digital Parcel Solutions

Fast and efficient delivery backed by top-notch customer service. Streamlined postal solutions to fit...

You wouldn't and neither would most of us. This is perfect malvertising execution on the part of Ukrainian cybercriminals, according to security researchers at Malwarebytes.

What initially seems like a legitimate tracking experience, suddenly changes tone, as the website tells the victim user they must pay a 35-cent fee and asks for credit card information. This alone should raise a red flag. But since 35 cents isn't much, let's assume you go with it – your credit card details will likely be sold off on the dark web.

The real goal of this attack comes next. In an attempt to "verify" your card (under a second brand impersonation of Visa's "Identity Check," which one can only assume is trying to appear like their cardholder verification service), the scammers ask the victim to provide their logon credentials to their bank.



Challenge
super-trackings.com/3ds.php?c=1111&t=v&data=eyJjYXJkIjoiNDExMTExMTExMTExMTExMSIsImJhb...
VISA

Protect your Visa® Identity Check™ Card Online

To protect you from fraud you must confirm your account. Please login to **JPMORGAN CHASE BANK, N.A.**

Merchant **USPS.com**
Amount **USD 0.35$**
Date **07.04.2023**
Card Number ********1111**

Login to JPMORGAN CHASE BANK, N.A.

Login: login
Password: password

Note that the bank and credit card name changes based on the information provided by the victim. It's a slick attack. But it's also one that includes unexpected requests that users should instantly recognize with the right training.

Images source: Malwarebytes

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/

Aug. 4: SANS Webinar: **2023 Digital Forensics and Incident Response Summit Solutions Track**

Aug. 16: SANS Webinar: **Hands-On Workshop: Protecting Cloud Assets and Improving Security**

Aug. 16: SANS Webinar: **Hands-on Malicious Script Analysis for Ransomware Response**

Aug. 17: SANS Webinar: **How to Use Zero Trust to Secure Workloads in the Public Cloud**

Aug. 18: SANS Webinar: **Cloud Security Exchange 2023**

Aug. 23: SANS Webinar: **Threat Detection Trends 2023**

View a list of upcoming SANS webcasts.

Important Reminders: ESRMO Updates

September: National Preparedness Month

Upcoming Business Continuity Training Events

The classes that require registration is as follows:

- **Aug. 29: 9 a.m. to 4 p.m. -** Riskonnect In-Person Formal Training (New Users)
- **Aug. 30: 9 a.m. to noon -** Riskonnect In-Person Formal Training (Intermediate and Advanced Users)
- **Aug. 30: 1 p.m. to 4 p.m. -** Riskonnect In-Person Formal Training (Intermediate and Advanced Users)

- **Sept. 14: 1 p.m. to 4 p.m. -** Repeat of Riskonnect Formal Training Virtual (Intermediate and Advanced Users)
- **Sept. 19: 10 a.m. to 4 p.m. -** Repeat of Riskonnect Formal Training Virtual (New Users)

The registration link is https://it.nc.gov/support/training-user-resources/assurance-cm-training

---

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.*