Monthly Cybersecurity Newsletter

June 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

New Nasty Android Malware Can Steal Your 2FA Codes — Is Your Phone Affected?

Check Point Research, a cybersecurity investigative team, discovered a *gnarly* Android malware called FluHorse. This sickening, malicious software can mimic legitimate apps, luring unsuspecting victims to its deceptive lair.

Making matters worse, FluHorse can lie dormant in your device for months, remaining undetected and flying under your radar. Check Point Research investigators called the threat "persistent, dangerous and hard-to-spot."

What Can FluHorse Do?

FluHorse's *modus operandi* is mimicking genuine applications to mislead victims into its deceitful den. For example, investigators discovered that the malware masqueraded as a popular Taiwan-based toll collection app in Google Play.

According to Check Point Research , the attackers behind FluHorse often imitated major banking and transportation apps, but the report did not disclose the names of these malicious apps. Most of these FluHorse-infected apps have more than **1,000,000** installs.

"The malware operators made an effort to carefully mimic all the key interface details to avoid raising any suspicions," the Check Point Research report said.

Once FluHorse wiggles its way into a victim's device, it can steal their credentials and two-factor authentication (2FA) codes. How? Firstly, once the imposter app is installed, it asks victims to allow it to send and view SMS messages.

Next, quarries are prompted to input their credentials (e.g., password and credit card details). At some point, a command-and-control server intercepts any incoming SMS traffic to snatch 2FA codes.

How do these FluHorse-infected apps end up on users' phones? A sophisticated phishing campaign lures victims to install apps as an APK.

"We traced infection chains for different types of malicious applications and discovered multiple high-profile entities among the recipient of these emails," the report said.

Check Point Research noted that the framework that underpins these malicious apps is Flutter, a Google-created open-source software development kit. The Eastern Asian markets, according to the team, were the main targets of FluHorse, but that doesn't mean you're off the hook if you're outside of that region.

As always, the moral of the story is to avoid installing Android apps from non-reputable third-party app stores, suspicious emails and other risky channels. The Google Play Store has its drawbacks, but it's a far safer platform than the aforementioned sources.

*This article is redistributed with permission from K*imberly Gedeon of Laptop Magazine

---

Attackers Are Now Using GhostTouch Attacks to Hack Your Phone

It comes as no surprise that threat actors and hackers have always used malware and phishing attacks to infiltrate devices and gain unauthorized access. However, according to new research from China's Zhejiang University and Germany's Technical University of Darmstadt, threat actors are now using a new technique called GhostTouch, which exploits electromagnetic signals to mimic gestures like swiping and tapping on the targeted device.

This new technique eliminates the need to install malware and allows threat actors to gain unauthorized access to smartphones, potentially compromising sensitive data, including passwords and banking applications.

As of now, nine smartphone models, including the iPhone SE (2020), Samsung Galaxy S20 FE 5G, Redmi 8 and Nokia 7.2, have been identified as vulnerable to this exploit.

Public Places Prone to GhostTouch Attacks

While the idea of attackers remotely hacking your phone might sound alarming, it is important to note that threat actors need to be near their victims to carry out the attack. As a result, public places like libraries, cafes or conference lobbies become the prime targets for such attacks.

Additionally, given that people keep their phones face down in quiet environments, such as the library, threat actors can take advantage of this situation by placing their hacking equipment nearby and emitting electromagnetic signals within a range of 40 mm.

However, it is important to note that these attacks are not inconspicuous. In fact, users will observe their phones seemingly operating on their own. But unfortunately, since the occurrences of glitches where the phone registers false touches are relatively common, many users may not even realize that a hacking attempt has taken place.

How to Stay Protected

While there is no foolproof solution to safeguard against GhostTouch attacks, users can take several steps to prevent hackers from gaining access. These include implementing robust security mechanisms like PIN codes, swipe patterns or biometric authentication and refraining from placing their phones face down on tables.

This article is redistributed with permission from Hisan Kidwai of Android Headlines.

FTC Warns of MetaMask and PayPal Phishing Campaigns

The U.S. Federal Trade Commission has issued an alert warning of phishing campaigns that are impersonating PayPal and the MetaMask cryptowallet.

"If you got an email that seems to be from MetaMask or PayPal, stop," the FTC says. "They're phishing scams. The MetaMask fake says your cryptocurrency wallet is blocked. And, if you don't act fast, click a link, and update your wallet, they say your crypto will be lost. The phony PayPal message says BNC Billing canceled your payment to Binance — and it gives you a phone number to reach PayPal…except that's a scam, too. If you get one of the messages, delete it."

The FTC explains that many phishing attacks attempt to convey a sense of urgency to make users act without thinking:

"Most unexpected emails saying to act quickly, click a link, or call a number are phishing scams," the alert says. "They may look like they come from companies you know, but they're from scammers who want you to think the message is real. That way, scammers think you'll click into a fake website or call an actual scammer — all to solve a fake problem. If you click or call, the scammers will steal your financial or personal information, and that could lead to identity theft."

The FTC offers the following advice for users:

- “Slow down. Ask yourself: Do I have an account with the company? Do I know whoever sent the email? If ‘no,’ it’s a phishing attempt. If ‘yes,’ still check it out. Contact the company using a number or website you know is real. And, if you own a cryptocurrency wallet and have a concern, contact the cryptocurrency exchange that holds your wallet.

- “Don’t click on any links. Links in unexpected texts or emails could lead to identity theft or let scammers install malware.

- “Update your security software. This will protect your phone and computer from security threats, which could expose your personal or financial information to scammers.”

This article is redistributed with permission from KnowBe4.

Number of Ransomware Victim Organizations Nearly Doubles in March

New data shows a resurgence in successful ransomware attacks with organizations in specific industries, countries and revenue bands being the target.

While every organization should always operate under the premise that they may be a ransomware target on any given day, it’s always good to see industry trends to paint a picture of where cybercriminals are currently focusing their efforts. This gives organizations the ability to either shore up security measures today (if they’re a current target) or shore up security measures today anyways (so they’re ready for when they do become the target).

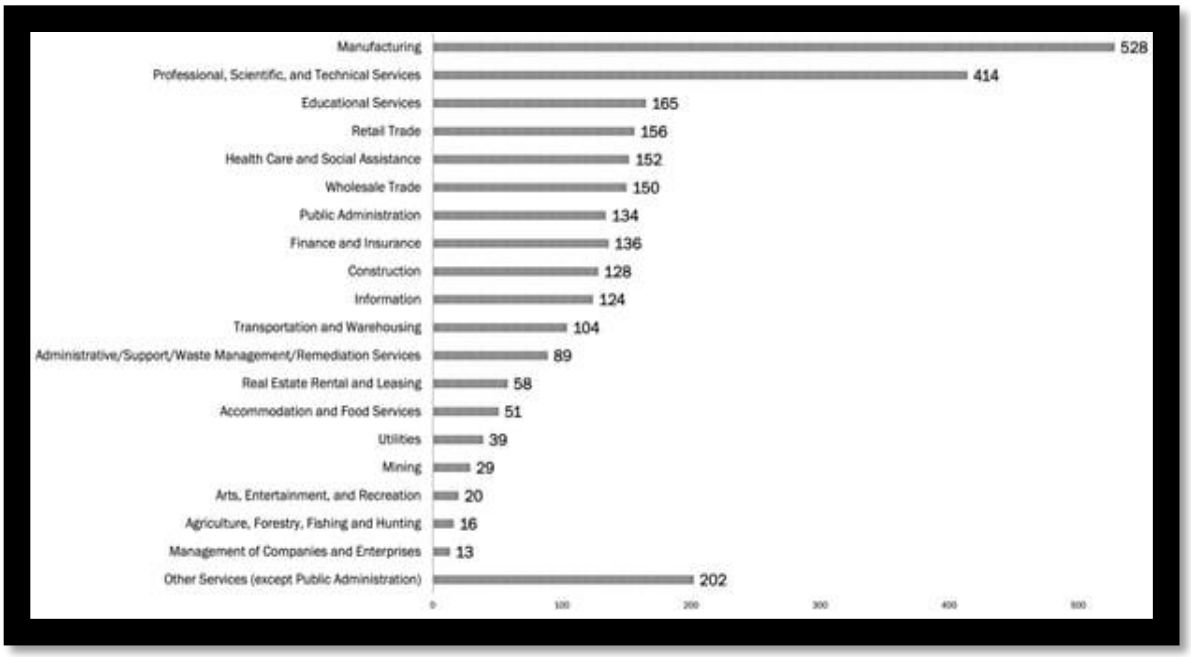
In third-party risk vendor Black Kite’s 2023 Ransomware Threat Landscape Report, we see some interesting trends around successful ransomware attacks today:

- March of this year saw 410 ransomware victim organizations – nearly double that of April of last year, with only 208.

- The U.S. dominated as the primary focus, with 1171 victim organizations representing 43% of the total victims reported, with the UK, Germany, France, Italy, and Spain combined making up around 20% of victim orgs.

- The largest group of victim organizations by revenue resided in the $50-60m range, with the next two groupings in the $40-50 million and $60-70 million ranges, respectively.

- Manufacturing topped the list of industries, with “Professional, Scientific, and Technical Services” coming in second, representing nearly 35% of all victim organizations.



Source: Black Kite

In summary, it appears like cybercriminals are focused on mid-market, U.S.-based organizations that likely have a material amount of intellectual property and/or sensitive data.

This, of course, doesn't mean if you're not in that specific demographic you're off the hook; nothing could be further from the truth. The Black Kite data shows where the focus is *today*. But there's always a new player looking for a niche victim demographic they can nestle themselves into, making it necessary to shore up all security – including your user's vigilance against phishing and social engineering attacks.

For additional information, please refer to the CISA and MS-ISAC Ransomware Guide.

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/

Jun. 1: SANS Webinar: **A Journey of Vulnerability Hunting in a Third-Party Plugin in Adobe Acrobat Through Fuzzing**

Jun. 6: SANS Webinar: **Exposed Industrial Control System Remote Services: A Threat to Critical Infrastructure**

Jun. 9: SANS Webinar: **2023 Cyber Solutions Fest | Spring: Insider Threat, Phishing & Malware**

Jun. 15: SANS Webinar: **Achieve Cloud Security at Scale**

Jun. 20: SANS Webinar: **The Future of Risk-Based Detection**

Jun. 27: SANS Webinar: **Hands-On Workshop: Multi Cloud Data Security**

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.*