News from Wednesday, March 22, 2023. Reported on Thursday, March 23, 2023.

Live links are embedded throughout today's briefing. To see the actual URL, hover your mouse over the link for a moment before clicking. These links were copied directly from the web site of the source article. Tyler Cybersecurity has not performed any testing on the sites / links for security.

| Sources | Articles |
|---|---|
| Bleeping Computer | **Hackers inject credit card stealers into payment processing modules**<br>A new credit card stealing hacking campaign is doing things differently than we have seen in the past by hiding their malicious code inside the 'Authorize.net' payment gateway module for WooCommcerce, allowing the breach to evade detection by security scans.<br><br>Historically, when threat actors breach a commerce site like Magenta or WordPress running WooCommerce, they inject malicious JavaScript into the HTML of the store or customer checkout pages.<br><br>These scripts will then steal inputted customer information on checkout, such as credit card numbers, expiration dates, CVV numbers, addresses, phone numbers, and email addresses.<br><br>However, many online merchants now work with security software companies that scan the HTML of public-facing eCommerce sites to find malicious scripts, making it harder for threat actors to stay hidden.<br><br>To evade detection, the threat actors are now injecting malicious scripts directly into the site's payment gateway modules used to process credit card payments on checkout.<br><br>As these extensions are usually only called after a user submits their credit card details and checks out at the store, it may be harder to detect by cybersecurity solutions.<br><br>The campaign was discovered by website security experts at Sucuri after being called in to investigate an unusual infection on one of their client's systems.<br><br>**PoC exploits released for Netgear Orbi router vulnerabilities**<br>Proof-of-concept exploits for vulnerabilities in Netgear's Orbi 750 series router and extender satellites have been released, with one flaw a critical severity remote command execution bug.<br><br>Netgear Orbi is a popular network mesh system for home users, providing strong coverage and high throughput on up to 40 simultaneously connected devices across spaces between 5,000 and 12,500 square feet.<br><br>The flaws in Netgear's system were discovered by the Cisco Talos team and reported to the vendor on August 30, 2022. Cisco urges users to update their firmware to the latest version, 4.6.14.3, released on January 19, 2023.<br><br>At the time of the disclosure, Cisco wasn't aware of any cases of active exploitation of the above flaws. However, considering the availability of a PoC for CVE-2022-37337, threat actors could attempt to find misconfigured, publicly accessible routers to exploit.<br><br>The good news is that these exploits require local access, valid login credentials, or the admin console to be publicly accessible, making it much harder to exploit the vulnerabilities.<br><br>However, a quick search using Shodan found almost 10,000 Orbi devices publicly accessible from the Internet, with the majority located in the United States. If any use the default admin credentials, they could potentially be vulnerable to attackers.<br><br>While Orbi does support the automatic installation of updates, on an Orbi seen by BleepingComputer, new firmware did not automatically install, and it was running software released in August 2022. |

| Sources | Articles |
|---|---|
| | Therefore, owners of Netgear Orbi 750 devices should manually check to see if they are running the latest version, and if not, upgrade their firmware as soon as possible.<br><br>**Dole discloses employee data breach after ransomware attack**<br>Fresh produce giant Dole Food Company has confirmed threat actors behind a February ransomware attack have accessed the information of an undisclosed number of employees.<br><br>Dole employs around 38,000 people worldwide, providing fresh fruits and vegetables to customers in more than 75 countries.<br><br>The company revealed that last month's cyberattack directly impacted its employees' information in the annual report filed with the U.S. Securities and Exchange Commission (SEC) on Wednesday.<br><br>"All our businesses are implementing our Crisis Management Protocol to resume 'business as usual' post haste, inclusive of our Manual Backup Program if needed. Please bear with us as we navigate our way and hopefully, we will minimize this event," Dole said.<br><br>While the company said the ransomware attack had limited impact, it was forced at the time to shut down production plants across North America.<br><br>"Dole Food Company is in the midst of a cyberattack, and [we] have subsequently shut down our systems throughout North America. Our plants are shut down for the day, and all shipments are on hold," the memo reads.<br><br>**Windows 11, Tesla, Ubuntu, and macOS hacked at Pwn2Own 2023**<br>On the first day of Pwn2Own Vancouver 2023, security researchers successfully demoed Tesla Model 3, Windows 11, and macOS zero-day exploits and exploit chains to win $375,000 and a Tesla Model 3.<br><br>The first to fall was Adobe Reader in the enterprise applications category after Haboob SA's Abdul Aziz Hariri (@abdhariri) used an exploit chain targeting a 6-bug logic chain abusing multiple failed patches which escaped the sandbox and bypassed a banned API list on macOS to earn $50,000.<br><br>The STAR Labs team (@starlabs_sg) demoed a zero-day exploit chain targeting Microsoft's SharePoint team collaboration platform that brought them a $100,000 reward and successfully hacked Ubuntu Desktop with a previously known exploit for $15,000.<br><br>During last year's Vancouver Pwn2Own contest, security researchers earned $1,155,000 after hacking Windows 11 six times, Ubuntu Desktop four times, and successfully demonstrating three Microsoft Teams zero-days.<br><br>They also reported several zero-days in Apple Safari, Oracle Virtualbox, and Mozilla Firefox and hacked the Tesla Model 3 Infotainment System. |
| The Hacker News | **Nexus: A New Rising Android Banking Trojan Targeting 450 Financial Apps**<br>An emerging Android banking trojan dubbed Nexus has already been adopted by several threat actors to target 450 financial applications and conduct fraud.<br><br>"Nexus appears to be in its early stages of development," Italian cybersecurity firm Cleafy said in a report published this week.<br><br>"Nexus provides all the main features to perform ATO attacks (Account Takeover) against banking portals and cryptocurrency services, such as credentials stealing and SMS interception."<br>The trojan, which appeared in various hacking forums at the start of the year, is advertised as a subscription service to its clientele for a monthly fee of $3,000. Details of the malware were first documented by Cyble earlier this month. |

| Sources | Articles |
|---|---|
| | Some new additions to the list of functionalities are its ability to remove received SMS messages, activate or stop the 2FA stealer module, and update itself by periodically pinging a command-and-control (C2) server.<br><br>"The [Malware-as-a-Service] model allows criminals to monetize their malware more efficiently by providing a ready-made infrastructure to their customers, who can then use the malware to attack their targets," the researchers said. |
| Information Security Magazine | **Malicious ChatGPT Chrome Extension Hijacks Facebook Accounts**<br>Security researchers have warned of yet another security threat using public interest in ChatGPT to propagate – this time under the guise of a Chrome extension.<br><br>Guardio claimed in a blog post that threat actors forked a legitimate open source "ChatGPT for Google" extension and added malicious code designed to steal Facebook session cookies.<br><br>Users were then directed to the extension by malicious sponsored search engine results.<br><br>"So, you search for 'Chat GPT 4,' eager to test out the new algorithm, ending up clicking on a sponsored search result promising you just that," Guardio explained.<br><br>"This redirects you to a landing page offering you ChatGPT right inside your search results page – all that's left is to install the extension from the official Chrome Store. This will give you access to ChatGPT from the search results but will also compromise your Facebook account in an instant."<br><br>The malicious extension is particularly difficult to tell apart from the legitimate version on which it's based, as the code differs in just one respect.<br><br>"Looking at the "OnInstalled" handler function that is triggered once the extension is installed, we see the genuine extension just using it to make sure you see the options screen (to log in to your OpenAI account)," Guardio said. |
| HIPAA Journal | **FBI: Losses to Cybercrime Increased by 49% in 2022 to $10.3 Billion**<br>The Federal Bureau of Investigation (FBI) has published its 2022 Internet Crime Report, which shows at least $10.3 billion was lost to cybercrime in 2022, up 49% ($3.4 billion) from 2021, despite a 5% reduction in complaints (800,944). Over the past 5 years, the FBI Internet Crime Complaint Center (IC3) has received reports of losses of more than $27.6 billion across 3.26 million complaints to IC3.<br><br>FBI data show a 36% year-over-year decrease in ransomware attacks, which fell from 3,729 complaints in 2021 to 2,385 complaints in 2022. Despite this decrease, the FBI says ransomware still poses a significant threat, especially to the healthcare sector which ranked top out of 16 critical infrastructure sectors for ransomware attacks in 2022 and actually saw an increase in complaints. 210 ransomware complaints were filed with IC3 in 2022 by healthcare organizations compared to 148 in 2021. The FBI has observed an increase in double extortion tactics in ransomware attacks, where data are stolen in addition to file encryption and payment is required to obtain the decryption keys and to prevent the publication or sale of stolen data. LockBit was the most prolific ransomware actor with 149 reported attacks, ALPHV/BlackCat was second with 114 attacks, and Hive was 3rd with 87 attacks.<br><br>Several cybercriminal groups that have historically used ransomware in their attacks have switched to extortion-only attacks, involving data theft and ransom demands but no file encryption. The FBI's data shows extortion attacks have remained flat, increasing only slightly from 39,360 complaints in 2021 to 39,416 complaints in 2022.<br><br>Phishing remains one of the most common attack vectors, although reported phishing attacks fell by 7% year over year to 300,497 incidents. Even with that decrease, phishing is still the most common crime type in terms of victim count ahead of personal data breaches with 58,859 complaints and non-payment/non-delivery with 51,679 complaints. |

| Source | Long Form Article |
|---|---|
| Krebs on Security by Brian Krebs | **Google Suspends Chinese E-Commerce App Pinduoduo Over Malware**<br>Google says it has suspended the app for the Chinese e-commerce giant Pinduoduo after malware was found in versions of the software. The move comes just weeks after Chinese security researchers published an analysis suggesting the popular e-commerce app sought to seize total control over affected devices by exploiting multiple security vulnerabilities in a variety of Android-based smartphones.<br><br>In November 2022, researchers at Google's Project Zero warned about active attacks on Samsung mobile phones which chained together three security vulnerabilities that Samsung patched in March 2021, and which would have allowed an app to add or read any files on the device.<br><br>Google said it believes the exploit chain for Samsung devices belonged to a "commercial surveillance vendor," without elaborating further. The highly technical writeup also did not name the malicious app in question.<br><br>On Feb. 28, 2023, researchers at the Chinese security firm DarkNavy published a blog post purporting to show evidence that a major Chinese ecommerce company's app was using this same three-exploit chain to read user data stored by other apps on the affected device, and to make its app nearly impossible to remove.<br><br>DarkNavy likewise did not name the app they said was responsible for the attacks. In fact, the researchers took care to redact the name of the app from multiple code screenshots published in their writeup. DarkNavy did not respond to requests for clarification.<br><br>"At present, a large number of end users have complained on multiple social platforms," reads a translated version of the DarkNavy blog post. "The app has problems such as inexplicable installation, privacy leakage, and inability to uninstall."<br><br>On March 3, 2023, a denizen of the now-defunct cybercrime community BreachForums posted a thread which noted that a unique component of the malicious app code highlighted by DarkNavy also was found in the ecommerce application whose name was apparently redacted from the DarkNavy analysis: Pinduoduo.<br><br>On March 4, 2023, e-commerce expert Liu Huafang posted on the Chinese social media network Weibo that Pinduoduo's app was using security vulnerabilities to gain market share by stealing user data from its competitors. That Weibo post has since been deleted.<br><br>On March 7, the newly created Github account Davinci1010 published a technical analysis claiming that until recently Pinduoduo's source code included a "backdoor," a hacking term used to describe code that allows an adversary to connect to a compromised system remotely and secretly at will.<br><br>That analysis includes links to archived versions of Pinduoduo's app released before March 5 (version 6.50 and lower), which is when Davinci1010 says a new version of the app removed the malicious code.<br><br>Pinduoduo has not yet responded to requests for comment. Pinduoduo parent company PDD Holdings told Reuters Google has not shared details about why it suspended the app.<br><br>The company told CNN that it strongly rejects "the speculation and accusation that Pinduoduo app is malicious just from a generic and non-conclusive response from Google," and said there were "several apps that have been suspended from Google Play at the same time."<br><br>Pinduoduo is among China's most popular e-commerce platforms, boasting approximately 900 million monthly active users.<br><br>Most of the news coverage of Google's move against Pinduoduo emphasizes that the malware was found in versions of the Pinduoduo app available outside of Google's app store — Google Play. |

| Source | Long Form Article |
|---|---|
| | "Off-Play versions of this app that have been found to contain malware have been enforced on via Google Play Protect," a Google spokesperson said in a statement to Reuters, adding that the Play version of the app has been suspended for security concerns.<br><br>However, Google Play is not available to consumers in China. As a result, the app will still be available via other mobile app stores catering to the Chinese market — including those operated by Huawei, Oppo, Tencent and VIVO.<br><br>Google said its ban did not affect the PDD Holdings app Temu, which is an online shopping platform in the United States. According to The Washington Post, four of the Apple App Store's 10 most-downloaded free apps are owned by Chinese companies, including Temu and the social media network TikTok.<br><br>The Pinduoduo suspension comes as lawmakers in Congress this week are gearing up to grill the CEO of TikTok over national security concerns. TikTok, which is owned by Beijing-based ByteDance, said last month that it now has roughly 150 million monthly active users in the United States.<br>A new cybersecurity strategy released earlier this month by the Biden administration singled out China as the greatest cyber threat to the U.S. and Western interests. The strategy says China now presents the "broadest, most active, and most persistent threat to both government and private sector networks," and says China is "the only country with both the intent to reshape the international order and, increasingly, the economic, diplomatic, military, and technological power to do so." |