Community Institution & Associations Risk Summary Report

Week of 22 May | 2023 Edition | Vol. 178

Follow Us

TLP GREEN | Americas Cyber Threat Level: Guarded | DHS Terrorism Threat Level: Elevated

In This Issue

Threats of the Week

News and Risk Information

Summary

Below are some of the top news and risks that the Financial Services Information Sharing Analysis Center (FS-ISAC) has observed this week for community institutions (CIs).

Backup repositories targeted 93% of ransomware attacks. The ransomware threat is still very much alive, with 85% of organizations having suffered from at least one such attack over the past 12 months, according to Veeam's *2023 Ransomware Trends Report*. Veeam also found that in 93% of ransomware incidents, the threat actors target the backup repositories, resulting in 75% of victims losing at least some of their backups during the attack, and more than one-third (39%) of backup repositories being completely lost. The report showed that organizations are still ill-prepared to face this threat. Sheltered Harbor is an affordable option to protect your customer records and prevent disruption. (Info Security Magazine)

DarkBERT could help automate dark web mining for cyber threat intelligence. Researchers have developed DarkBERT, a language model pre-trained on dark web data, to help cybersecurity pros extract cyber threat intelligence (CTI) from the Internet's virtual underbelly. (HelpNet Security)

IT security budgets are shifting as companies target risk reduction. Organizations are designing their security spending around keeping the business secure and operations running smoothly. Despite the impact that cyber incidents have on an organization's overall business operations, security spending remains within the purview of the IT budget, albeit a small part. In 2022, IT security made up just 5.2% of IT budgets, according to research from Gartner. Yet, as small as that percentage looks, it is an improvement from the year before. Risk reduction is a driver for this increase, Gartner found. (Cybersecurity Dive)

Cloned CapCut websites push information-stealing malware. A new malware distribution campaign is underway impersonating the CapCut video editing tool to push various malware strains to unsuspecting victims. CapCut is ByteDance's official video editor and maker for TikTok, supporting music mixing, color filters, animation, slow-mo effects, picture-in-picture, stabilization, and more. It has over 500 million downloads on Google Play alone, and its website receives over 30 million hits monthly. (Bleeping Computer)

KeePass password manager flaw detailed; patch coming. The KeePass password manager has a vulnerability that allows an attacker to retrieve master passwords via a memory dump. A patch for the 2.x versions on Windows, macOS, and Linux is expected next month. (The Hacker News)

Millions of mobile phones come pre-infected with malware. A recently fixed command injection vulnerability (CVE-2023-28771) affecting a variety of Zyxel firewalls may soon be exploited in the wild, Rapid7 researchers have warned, after publishing a technical analysis and a PoC script that triggers the vulnerability and achieves a reverse root shell. Discovered and reported by TRAPA Security researchers, the vulnerability has been fixed by Zyxel in April 2023, with the release of ZLD v5.36 and ZLD v4.73 Patch 1. Admins of vulnerable devices are advised to upgrade to the latest firmware update as quickly as possible. Enabling automatic firmware updates is also generally a good idea. (HelpNet Security)

This Week's Top Risks

Security is Everyone's Responsibility

Threats, Malware, Cybercampaigns, and Adversaries

- Agent Tesla
- ASTAROTH
- BrutePrint
- BUMBLEBEE
- Business email compromise and impersonation use of texts; credential capture, pharming, harvesting, and validation scams
- CageyChameleon (New variant)
- GootLoader (SEO Poisoning)
- IceID
- JsOutProx RAT
- Lokibot
- NanoCore
- NetSupport
- Qbot/QakBot
- PDFUnfolder Downloader
- PikaBot Malware
- Remcos (DBatLoader, GuLoader)
- Snake malware
- SOCGHOLISH
- STRRAT Malware
- Typosquatting attack
- Ursnif

Hardware & System Vulnerabilities (multiple)

- Amazon, Apache, Apple, Aruba, Brocade Fabric OS, Cisco, Citrix, Cygwin, Debian, Dell, HP, Hitachi. IBM, Lenovo, Linux, Microsoft, Mozilla, Oracle, Red Hat, RSA, SAP, Sophos, SUSE, Trendmicro Apex, Ubuntu, VMware, WireShark, and Xerox.

Themed Phishing Campaigns

Please see the Phishing Daily Digest for all activity. Use keywords for AV black lists.

Subject Keywords: 1295185895, 5050, Advance Payment, Amazon, Arrival Notice, DHL, Diversion, Drake Software, Form A – PT, Google, HELOC PO, Invoice, MFA, New Sign, New ZixCorp, O365, Order #, Payment Confirmation, PayPal, PROFORMA, Purchase Order, SP24, SWIFT, Your identity, and Your Package.

Threats of the Week

BrutePrint fingerprint vulnerability and the Lemon Group highlight this week's risks

New BrutePrint Attack Brute-Forces Fingerprints on Android Devices

Summary

Bleeping Computer reports, Chinese researchers discovered a new type of attack targeting smartphones. BrutePrint is a brute-force attack to defeat fingerprint authentication. Brute-force attacks use numerous trial-and-error attempts to decipher a key, or password to obtain access to accounts without authorization. Smartphones typically have attempt limits (locking and preventing new attempts after a certain number of failures) and liveness detection (differentiating between an actual fingerprint and a picture of a fingerprint) to defend against brute-force attacks. However, the researchers explained that they exploited two zero-day vulnerabilities in this attack: Cancel-After-Match-Fail (CAMF) and Match-After-Lock (MAL) that forced the device to ignore failed attempts and allowed them to continue making login attempts during the "lockout" period, respectively. The final component of the BrutePrint attack uses a "neural style transfer" system to make all fingerprint images in the database look like the target device's sensor scanned them. This makes the images appear valid and thus have better chances of success. Additionally, the Serial Peripheral Interface (SPI) of the fingerprint sensors' biometric data was insufficiently safeguarded, making it possible for a man-in-the-middle (MITM) attack to steal fingerprint images. Experts tested the new method on ten smartphone models. These tests resulted in unlimited login attempts on all Android and HarmonyOS (Huawei) phones and ten additional attempts on iOS devices. The main goal of this type of brute-force attack is to allow intruders an unlimited number of attempts to unlock a device using a fingerprint match. For a BrutePrint attack, hackers need proximity to the target device, a fingerprint database, and $15 worth of equipment.

Risk

The techniques described by the researchers greatly decrease the amount of time required to brute-force a device protected with fingerprint authentication, making such attacks more practical for threat actors. Compromised devices containing sensitive information can be retrieved and potentially lead to compliance, financial, legal, regulatory, and reputation risks.

Remediation

Specialists tested the attack method on Android and iOS devices. The results show that all of them had at least one weakness that made them vulnerable. Apply security updates to devices if vendors release them to address these vulnerabilities.

Android devices permit an endless number of fingerprint trials, making it practically viable to brute-force the user's fingerprint and unlock the device. However, the authentication security on iOS is significantly stronger and can efficiently thwart brute-force attacks.

Allowing one device to be unlocked with multiple fingerprints exponentially decreased the amount of time to successfully brute-force. Where practical, only allow a single fingerprint to be used to unlock a device.

Lemon Group's Business of Pre-infected Devices

Summary

Cyware reports the Lemon Group gained control over millions of smartphones distributed around the world via preinstalled malware. According to Trend Micro, the actors behind the campaign are known as Lemon Group, and they preloaded Guerrilla malware on the devices. The campaign has been active since 2018, and the attacker changed the name of its operation from Lemon to Durian Cloud SMS after Trend Micro detailed its operations last year.

Lemon Group conducts business for marketing and advertising companies and utilizes big data. This enables the threat actor to monitor customers who can be infected with other apps to build on - such as displaying advertisements to app users from specific regions. The security firm analyzed the Guerrilla malware by acquiring a phone and extracting its ROM image. Trend Micro found over 490,000 active services from Durian Cloud SMS across 180 countries, with the top 10 being Mexico, the US, Indonesia, Russia, South Africa, Thailand, India, the Philippines, Argentina, and Angola.

Durian Cloud SMS uses an implant that loads a downloader, which serves as the main plugin for fetching and running other plugins. The secondary plugins capture SMS messages (OTPs for WhatsApp/Facebook) and set up a reverse proxy. Furthermore, it collects application data, delivers ads when launching official apps, and hijacks WhatsApp to send messages.

The large-scale infection can be profitable for Durian Cloud SMS in the long run, as it could compromise critical infrastructure. This also highlights the risk to users' privacy posed by copycat brands of premium devices. To mitigate this risk, users should always purchase smartphones from genuine brands instead of copycats.

Build The Muscle Memory For Strong Incident Response

The registration for the 2023 CAPS exercise for community institutions is now open on the FS-ISAC Intelligence Exchange, within the Member Services application. You'll register for the 2023 CAPS season, 4 September – 13 October, then conduct the exercise with your team over a day or two when best for your schedules. The CAPS virtual tabletop exercise challenges your incident response team to overcome a simulated attack against securities systems and processes. Participants practice mobilizing quickly, working under pressure, critically appraising information as it becomes available, and connecting the dots to defend against a cyber-attack on a fictional insurance company. One individual registers and leads your internal team through a two-part virtual exercise. The exercise follows a realistic, timely scenario involving a fictional organization.

Hijacked Job Ads Pose Risks to Consumers and Financial Institutions

Check fraud finding new victims through bogus job ads

Summary

Scammers are taking outdated ads from real employers, changing them, and posting them on employment websites and career-oriented platforms like Indeed or LinkedIn. The modified ads seem to be real job offers with legitimate companies. They're not. Their goal is to trick job seekers into sharing personal information. So how do you know if you're dealing with a scammer?

Some of the hijacked job postings are offers to work from home as a personal assistant or customer service representative. The cybercriminals ask job seekers for information, such as their Social Security and their bank account numbers, so they can (supposedly) deposit their salary. Sometimes, they tell job seekers they got the job and will send the job seeker a check to "buy needed equipment." But in desperate times, good judgment may be lessened in the hope of work. Your customers need to be aware of these scams – but so do tellers in "branchland."

Consumer Tips

Verify job openings before you apply. Visit the official website of the organization or company for which the job seeker is applying. Most include a "career opportunities" or "jobs" section.

See what others are saying. Look up the name of the company along with words like "scam," "review," or "complaint." The results may include the experiences of others who've lost money.

Never deposit a check from someone you don't know. An honest employer will never send a person a check and then tell the person to send them part of the money. That's a scam.

Teller Tips

Know Your Customer. Knowing your customer is more than verification, it's understanding their account activity and history. Has your customer been out of work and suddenly deposited a large check? Do you have recourse in the event of fraud?

Adhere to teller check cashing guidelines. If the check falls outside of teller guidelines, take a partner. Elevate the approval to a supervisor or manager.

Inspect the deposited check. Does the presented check appear to be altered, or counterfeit? Does it qualify for a Reg C hold?

Security Tips

Provide teller fraud training. Teach tellers to identify common check fraud types. Teach them what they should do if they detect a suspicious deposit item at a teller window.

Provide an internal fraud hotline. Having an internal line to report suspicious activity enables you to contact the issuing bank to determine if the item is legitimate or not.

Remember!

If you are a community institution, chances are that any loss is a big loss. If you have been a fraud victim… Build your case by collecting evidence such as a digital closed circuit television video, an affidavit of fraud, identifying other victim banks to aggregate the loss and complete a comprehensive narrative, and then contact law enforcement.

ChatGPT Uses For Security Threats

We continue our second article discussing AI threats - ChatGPT

Summary

In the 15 May, Issue 177 report, we began talking about how Artificial Intelligence could be used to assess credit risks and fraud reduction. Dark Reading recently reported some of the problems that could increase the sale of pain relievers for security practitioners. The article provides 3 areas of concern:

Mass Phishing. Because ChatGPT is so powerful, it can reduce the amount of time it takes to create handcrafted, personalized emails to a list of people from a few days to just minutes. And with just the click of a button, ChatGPT can answer very specific questions and use its knowledge to impersonate both security and non-security personnel experts.

Reverse Engineering. ChatGPT is amazing at understanding code, or even machine code. By providing either binary code or obfuscated code of a system, ChatGPT can explain how the code works and what it does in a way that makes it easy for hackers to manipulate the piece of software and enable them to gain access to the company's servers. Reverse engineering used to be a very rare and highly lucrative skill; historically, only nation-states could incorporate it into their operations. This is now something that can be done by the most basic hackers.

Smart Malware. With ChatGPT, the malware can make decisions autonomously so it understands where the interesting data is, where passwords might be stored locally, and even how to connect to the data sources and extract the data automatically. Since it is completely autonomous — there's no longer a need for a hacker to control the malware and manually direct it to the right place — it is not only more dangerous, but it could be more common. This means more companies are at risk of being sporadically attacked, instead of being specifically targeted.