CENTRAL RESERVE POLICE FORCE

CYBER BYTE

- **Vultur Android Banking Trojan Returns with Upgraded Remote Control Capabilities.**
- **AI Calling—Scammers turn to AI voice cloning tools for a new breed of scam.**
- **Cisco warns customers of password-spraying attacks that have been targeting Remote Access VPN (RAVPN) services of Cisco Secure Firewall devices.**
- **AI worm that can steal private data: What is it, how it works, and how to stay safe.**

CYBER BYTE
MAY-2024
EDITION

- **Cyber fraud updates**

Report on portal:
https://cybercrime.gov.in

For cyber fraud crime reporting
Call helpline no 1930

1.CYBER GEEKS NEWS

A) Vultur Android Banking Trojan Returns with Upgraded Remote Control Capabilities

The Android banking trojan known as **Vultur** has resurfaced with a suite of new features and improved anti-analysis and detection evasion techniques, enabling its operators to remotely interact with a mobile device and harvest sensitive data. "**Vultur** has also started masquerading more of its malicious activity by encrypting its C2 communication, using multiple encrypted payloads that are decrypted on the fly, and using the guise of legitimate applications to carry out its malicious actions.

The malware has been observed to be distributed via trojanized dropper apps on the **Google Play Store**, masquerading as authenticator and productivity apps to trick unwitting users into installing them.

The first SMS message guides the victim to a phone call. When the victim calls the number, the fraudster provides the victim with a second SMS that includes the link to the dropper: a modified version of the [legitimate] **McAfee Security app."** Upon installation, the malicious dropper executes three related payloads (two APKs and one DEX file) that register the bot with the C2 server, obtain accessibility services permissions for remote access via AlphaVNC and ngrok, and run commands fetched from the C2 server. One of the prominent additions to Vultur is the ability to remotely interact with the infected device, including carrying out clicks, scrolls, and swipes, through Android's accessibility services, as well as download, upload, delete, install, and find files. In addition, the malware is equipped to prevent the victims from interacting with a predefined list of apps, display custom notifications in the status bar, and even disable Keyguard to bypass lock screen security measures.

Suggestion

- Keep Software Updated.
- Use Reliable Security Software.
- Download Apps from Official Sources Only.
- Review App Permissions.
- Enable Google Play Protect.
- Implement Device Locking Mechanisms.
- Exercise Caution with Links and Attachments.
- Educate Yourself and Others.
- Regularly Back Up Data.
- Monitor Account Activity.

B) AI Calling—Scammers turn to AI voice cloning tools for a new breed of scam.

Cybercriminals have taken up newly forged artificial intelligence (AI) voice cloning tools and created a new breed of scam. With a small sample of audio, they can clone the voice of nearly anyone and send bogus messages by voicemail or voice messaging texts. The aim, most often, is to trick people out of hundreds, if not thousands, of dollars. Three seconds of audio is all it takes. With a small sample of a person's voice and a script cooked up by a cybercriminal, these voice clone messages sound convincing, 70% of people in worldwide survey said they weren't confident they could tell the difference between a cloned voice and the real thing. Cybercriminals create the kind of messages you might expect. Ones full of urgency and distress. They will use the cloning tool to impersonate a victim's friend or family member with a voice message that says they've been in a car accident, or maybe that they've been robbed or injured. Either way, the bogus message often says they need money right away. In all, the approach has proven quite effective so far. One in ten of people surveyed in study said they received a message from an AI voice clone, and 77% of those victims said they lost money as a result. Consider that people post videos of themselves on YouTube, share reels on social media, and perhaps even participate in podcasts. Even by accessing relatively public sources, cybercriminals can stockpile their arsenals with powerful source material. Nearly half (45%) of survey respondents said they would reply to a voicemail or voice message purporting to be from a friend or loved one in need of money, particularly if they thought the request had come from their partner or spouse (40%), mother (24%), or child (20%).

Further, they reported they'd likely respond to one of these messages if the message sender said:

- They've been in a car accident (48%).
- They've been robbed (47%).
- They've lost their phone or wallet (43%).
- They needed help while traveling abroad (41%).

These messages are the latest examples of targeted "spear phishing" attacks, which target specific people with specific information that seems just credible enough to act on it. Cybercriminals will often source this information from

public social media profiles and other places online where people post about themselves, their families, their travels, and so on—and then attempt to cash in. Payment methods vary, yet cybercriminals often ask for forms that are difficult to trace or recover, such as gift cards, wire transfers, reloadable debit cards, and even cryptocurrency. As always, requests for these kinds of payments raise a major red flag. It could very well be a scam.

Suggestion

- Set a verbal codeword with kids, family members, or trusted close friends.
- Always question the source.
- Think before you click and share.
- Protect your identity.
- Clear your name from data broker sites.

C) Cisco warns customers of password-spraying attacks that have been targeting Remote Access VPN (RAVPN) services of Cisco Secure Firewall devices.

The company published a document containing recommendations against **password spray attacks** aimed at Remote Access VPN (RAVPN) services. The IT giant pointed out that the attacks are also targeting third-party VPN concentrators.

"Cisco was made aware of multiple reports related to password spraying attacks aimed at RAVPN services. It has been noted by Talos that these attacks are not limited to Cisco products but also third-party VPN concentrators." reads the report. "Depending on your environment, the attacks can cause accounts to be locked, resulting in Denial of Service (DoS)-like conditions."

Password spraying is a type of brute force attack. In this attack, an attacker will brute force logins based on list of usernames with default passwords on the application. For example, an attacker will use one password (say, Secure@123) against many different accounts on the application to avoid account lockouts that would normally occur when brute forcing a single account with many passwords.

Suggestion

- Implement Strong Password Policies.
- Enable Multi-Factor Authentication (MFA).
- Update and Patch Devices.
- Monitor and Analyze Logs.
- Implement Account Lockout Policies.
- Enable Intrusion Prevention Systems (IPS).
- Implement Geo-Location Blocking.
- Regular Security Audits.

D) AI worm that can steal private data: What is it, how it works, and how to stay safe.

The digital world is rapidly growing, and currently, the top rider of this evolution is generative AI-Chat GPT, Gemini, Copilot, and so on. We are surrounded by a web of artificial intelligence-powered platforms that offer solutions to most of our problems. Need a protective plan? You get a customized one. Struggling to write code? You will have the entire draft right before your eyes using AI. However, this growing dependence on and spreading of the AI ecosystem is also harboring new threats that can potentially harm you to a great extent. One such threat is the development of AI worms, which can steal your confidential data and break the security walls put up by generative AI systems.

How does the AI worm work?

You can imagine this Morris II like a sneaky computer worm. And its job is to mess with email assistants that use artificial intelligence (AI). At first, Morris II uses a sneaky trick called "adversarial self-replication." It bombards the email system with messages, making it go in circles by forwarding messages over and over. This makes the AI models behind the email assistant get confused. They end up accessing and changing data. This can lead to either stealing information or spreading harmful stuff (like malware).

According to researchers, Morris II has two ways to sneak in: Text-Based: It hides bad prompts inside emails, fooling the assistant's security. Image-Based: It uses images with secret prompts to make the worm spread even more. In simple words, Morris II is a sneaky computer worm that messes with email systems using tricky tactics and confuses the AI behind them.

Suggestions:

- Keep Software Updated.
- Deploy Antivirus/Anti-Malware Software.
- Implement Network Segmentation.
- Enable Intrusion Detection and Prevention Systems (IDPS).
- Practice Least Privilege.

- Educate Users.
- Monitor Network Traffic.
- Backup Data Regularly.
- Implement Behavioral Analysis.
- Collaborate with Security Experts.

2.CYBER FRAUDS

i) A 37-year-old man from Maharashtra lost Rs 10.13 lakh in an online task scam after being lured by promises of high returns.

A 37-year-old man from Navi Mumbai in Maharashtra has allegedly lost Rs 10.13 lakh after being lured with the promise of high returns for some online tasks. The cyber police station in Navi Mumbai has registered a case against four persons in this connection. The accused contacted the victim, a resident of Old Panvel area, between January 16 and 27 and offered him to undertake some online prepaid tasks. They forwarded him certain links, assigned the tasks and promised lucrative returns. Subsequently, the victim made payments totaling Rs 10,13,005 into the bank accounts and through UPI IDs as instructed, an official from cyber police station. However, after completing the tasks, the victim neither received the promised returns nor his money was refunded. When he asked the accused for payment, they gave evasive responses.

ii) Voice cloning scam: How cybercriminals are using kids' voices to dupe parents.

Suppose you get a call from someone threatening to implicate your child in a criminal case if you do not meet their demands. You grow wary, wondering if someone is trying to con you. The next minute, however, you hear your sobbing child over the phone and you fear it may be true after all. And so you pay up — only to realise later that it was, indeed, a scam. Your child was never on the phone, but their voice was cloned using sophisticated software. Victim, a resident of Mahagun Moderne apartments in Noida Sector 78, who works as a superintending engineer in the Municipal Corporation of Delhi, he went to drop his 18-year-old son off for his JEE mock test at a centre near Rajendra Nagar Metro station in Ghaziabad. He then left to take care of some work. An hour later, he got a call from a number with a +92- country code. Victim said, "The caller, scammer, who claimed he was a police inspector, said my son had been caught with a gang of rapists…; he demanded I pay Rs 30,000 through Paytm immediately to get his name cleared. They said I could even talk to my son… The next minute, I heard a voice saying 'Papa please pay him, they are real policemen, please save me'. I could not doubt even for a second that he was not my boy. The style of speaking, crying… everything was the same." Still suspicious, Victim asked the caller which police station he was posted at but the man didn't respond. "I told him I don't use online services but I had Rs 10,000 in cash and could give it to him in person. But he refused, insisting I seek a shopkeeper's help to transfer the money. I was afraid that he may be a kidnapper. So I asked my driver to pose as a shopkeeper and handed over the phone to him To send Rs 10,000.

3.TIP OF THE MONTH

Debit Card /Credit Card Safety Instructions:-

Keep your cards safe: Treat your cards like cash. Don't leave them lying around or lend them to anyone.
Memorize PINs and passwords: Don't write down your PINs or passwords anywhere. Memorize them instead.
Protect your personal information: Be cautious about sharing personal information, especially over the phone or online. Ensure you're on secure websites when making online purchases.
Regularly review your account statements: Check your account statements frequently to spot any unauthorized transactions.
Enable transaction alerts: Many banks offer the option to receive notifications for every transaction made with your card. Enable this feature to stay updated about your card usage.
Be cautious with ATM and card readers: Check for any suspicious devices attached to ATMs or card readers before using them.
Use secure ATMs: Prefer using ATMs located in well-lit, secure areas. Avoid ATMs in secluded or poorly lit places.
Sign up for fraud protection services: Some financial institutions offer fraud protection services that monitor your account for suspicious activity and alert you to potential fraud.
Report lost or stolen cards immediately: If you lose your card or suspect it has been stolen, contact your bank or credit card issuer immediately to have the card canceled and replaced.
Use secure online payment methods: When making online purchases, consider using secure payment methods like PayPal or virtual credit card numbers. Attacker has used Cobalt strike adversary simulation tool for sending payloads to compromised systems.

Recent Cyber threat to Indian Cyberspace.

Hacking Group of Indonesia **Genosec Team** issued a warning on their Telegram channel, announcing the return of Hacktivist Indonesia in response to PM Narendra Modi's remarks on Muslims being "Infiltrators" they are going to launch #OPINDIA to target the Indian Cyberspace.


केन्द्रीय रिजर्व पुलिस बल
वीरता पदक विजेता
एवं
असाधारण आसूचना कुशलता पदक
अलंकरण समारोह -2024


शौर्य दिवस
9 अप्रैल 2024
मन समर्पित, तन समर्पित, और यह जीवन समर्पित
चाहता हूँ देश की धरती तुझे कुछ और भी दूँ


Cyber
revolution summit
25-26 APRIL 2024
HOTEL VIVANTA DWARKA
NEW DELHI, INDIA