CENTRAL RESERVE POLICE FORCE

CYBER BYTE

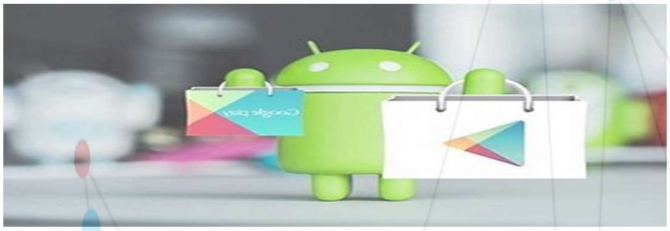
CYBER BYTE
APRIL-2024
EDITION

- **Patchwork Using "Romance Scam" Lures to Infect Android Devices with VajraSpy Malware.**
- **New Python-Based Snake Info Stealer Spreading Through Facebook Messages.**
- **AndroxGh0st Malware Targets Laravel Apps to Steal Cloud Credentials.**

- **Cyber frauds updates**

1.CYBER GEEKS NEWS

A) Patchwork Using "Romance Scam" Lures to Infect Android Devices with VajraSpy Malware.

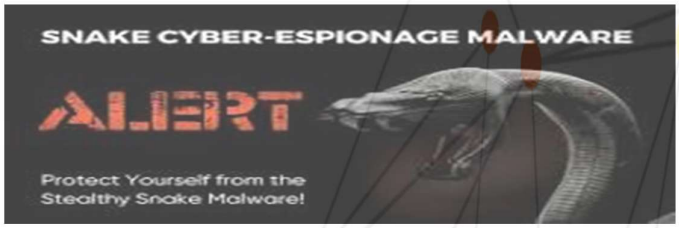


The threat actor known as **Patchwork** likely used "**romance scam"** to lures and trap victims in Pakistan and India, and infect their Android devices with a **remote access trojan** called **VajraSpy**. VajraSpy has a range of espionage functionalities that can be expanded based on the permissions granted to the app bundled with its code. It steals contacts, files, call logs, and SMS messages, but some of its implementations can even extract WhatsApp and Signal messages, record phone calls, and take pictures with the camera. The malicious app is distributed via **Google Play and other sources primarily masqueraded as messaging applications.**

- **Privee Talk (com.priv.talk)**
- **MeetMe (com.meeete.org)**
- **Let's Chat (com.letsm.chat)**
- **Quick Chat (com.qqc.chat)**
- **Rafaqat رفاق (com.rafaqat.news)**
- **Chit Chat (com.chit.chat)**
- **YohooTalk (com.yoho.talk)**
- **TikTalk (com.tik.talk)**
- **Hello Chat (com.hello.chat)**
- **Nidus (com.nidus.no or com.nionio.org)**
- **GlowChat (com.glow.glow)**
- **Wave Chat (com.wave.chat)**

Android users with a fake loan app (Moneyfine or "com.moneyfine.fine") as part of an extortion scam that manipulates the selfie uploaded as part of a know your customer (KYC) process to create a nude image and threatens victims to make a payment or risk getting the doctored photos distributed to their contacts. These unknown, financially motivated threat actors make enticing promises of quick loans with minimal formalities, deliver malware to compromise their devices, and employ threats to extort money. It also comes amid a broader trend of people falling prey to predatory loan apps, which are known to harvest sensitive information from infected devices, and employ blackmail and harassment tactics to pressure victims into making the payments.

B) New Python-Based "Snake Info Stealer" Spreading through Facebook Messages.



Facebook messages are being used by threat actors to distribute a Python-based information stealer dubbed Snake that's designed to capture credentials and other sensitive data.

"The credentials harvested from unsuspecting users are transmitted to different platforms such as Discord, GitHub, and Telegram,". The attacks entail sending prospective users seemingly innocuous RAR or ZIP archive files that, upon opening, activate the infection sequence.

The collected information, which comprises credentials and cookies, is then exfiltrated in the form of a ZIP archive via the Telegram Bot API. The stealer is also designed to dump cookie information specific to Facebook, an indication that the threat actor is likely looking to hijack the accounts for their own purposes.

Multiple information stealers targeting Facebook cookies have appeared in the wild, counting S1deload Stealer, MrTonyScam, NodeStealer, and VietCredCare. It also follows a discovery that threat actors are "using a cloned game cheat website, SEO poisoning, and a bug in GitHub to trick would-be-game-hackers into running Lua malware,"

C)AndroxGh0st Malware Targets Laravel Apps to Steal Cloud Credentials.

Cybersecurity researchers have shed light on a tool referred to as AndroxGh0st that's used to target Laravel applications and steal sensitive data. "It works by scanning and taking out important information from .env files, revealing login details linked to AWS and Twilio,". AndroxGh0st has been detected in the wild since at least 2022, with threat actors leveraging it to access Laravel environment files and steal credentials for various **cloud-based applications like Amazon Web Services (AWS), SendGrid, and Twilio**.

Attack chains involving the Python malware are known to exploit known security flaws in Apache HTTP Server, Laravel Framework, and PHP Unit to gain initial access and for privilege escalation and persistence. Androxgh0st first gains entry through a weakness in Apache, identified as CVE-2021-41773, allowing it to access vulnerable systems. Following this, it exploits additional vulnerabilities, specifically CVE-2017-9841 and CVE-2018-15133, to execute code and establish persistent control, essentially taking over the targeted systems.

Androxgh0st is designed to exfiltrate sensitive data from various sources, including .env files, databases, and cloud credentials. This allows threat actors to deliver additional payloads to compromised systems. A majority of the attack attempts targeting its honeypot infrastructure originated from the U.S., U.K., China, the Netherlands, Germany, Bulgaria, Kuwait, Russia, Estonia, and India, it added.

With cloud environments increasingly becoming a lucrative target for threat actors, it is critical to **keep software up to date and monitor for suspicious activity.** Threat intelligence firm has also released a tool called **CloudGrappler**, that's built on top of the foundations of cloud grep and scans AWS and Azure for flagging malicious events related to well-known threat actors.

Suggestions:

- Be cautious of unknown links.
- Keep software updated.
- Use strong passwords.
- Enable two-factor authentication.
- Educate yourself and others.
- Use reputable security software.
- Verify messages and attachments.
- Report suspicious activity.

2.CYBER FRAUDS

Noida woman duped of Rs 3.7 lakh over 7-hour Skype call in latest 'digital arrest' scam.

A 32-year-old woman IT engineer based in Noida was allegedly duped of Rs 3.75 lakh by cyber criminals who held her "hostage" over a Skype call for around seven hours, gradually withdrawing money from her account in a planned manner. The police said the fraudsters claimed to be police personnel and accused her of supplying drugs in a purported parcel sent from Mumbai to Taiwan. Victim's husband have filed a complaint in which he had told that his wife had received a call from a courier company from a number and then she was cheated through a Skype call. Necessary legal action is being taken by registering a case," said Additional DCP, Noida. "They said that a courier was going from Mumbai to Taiwan, which was seized by the customs officials and objectionable items were found in it. Then the call was transferred to a police officer who asked for my wife's account details and family details. They threatened and intimidated her and forced her to give them money.

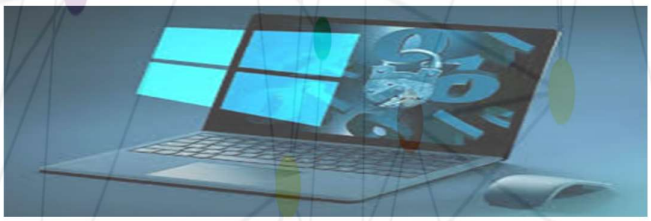
Gujarati businessman scammed of Rs 95 lakh after accepting Facebook friend request.

Cyber scams are becoming more widespread, with a growing number of individuals falling victim to them. A man claimed that he lost lakhs of rupees after befriending a woman on Facebook. The Gujarati businessman reportedly lost Rs 95 lakh in total to a scam. A resident of Alkapuri, victim complained to the Cyber Crime Police Station after falling victim to a scam, as reported by the Times of India (TOI). He explained to the police that he had received a friend request from a woman fraudster on Facebook last year in October, which he accepted. They later moved their conversations to WhatsApp. According to the outlet, victims friend suggested that he purchase herbal goods from India for Rs 1 lakh apiece and sell them to fraudsters firm for Rs 2 lakh. Once victim consented, she urged him to get in touch with some friend to obtain the items. Friend and victim communicated by email. He paid Rs 1 lakh and received a sample packet following their online chat. The box came on schedule, but victim did not open it.

As the publication stated, he instead ordered more orders.

Victim allegedly continued to give money to Friend even after that, in several accounts as per his instructions. When Friend persisted in requesting more money under fictitious pretences, he became sceptical. According to TOI, when he didn't get the promised sum, victim urged his friend to call off the agreement and give him his money back. But since then, neither friend nor the woman have been in contact.

3.TIP OF THE MONTH



Windows Security Tips: -

Keep Your System Updated: Ensure that your Windows operating system, as well as all installed software and drivers, are up to date with the latest security patches and updates. Regularly check for and install Windows updates to protect against known vulnerabilities.

Use Strong Passwords: Create strong, unique passwords for your user accounts, and consider using a password manager to securely store and manage your passwords. Enable multi-factor authentication (MFA) wherever possible for an added layer of security.

Enable Windows Defender Antivirus: Windows Defender Antivirus is built info Windows and provides real-time protection against viruses, malware, and other threats. Ensure that it is enabled and regularly updated to help safeguard your system.

Enable Windows Firewall: Turn on Windows Firewall or use a third-party firewall to monitor and control incoming and outgoing network traffic. Configure firewall settings to block

unauthorized access and only allow necessary connections.

Be Cautious of Email Attachments and Links: Exercise caution when opening email attachments or clicking on links, especially if they are from unknown or suspicious sources. Be wary of phishing emails and scams designed to trick you into disclosing sensitive information.

Use Secure Browsing Practices: Use a secure web browser, such as Microsoft Edge or Google Chrome, and keep it up to date with the latest security updates. Be cautious when visiting unfamiliar websites and avoid downloading software from untrusted sources.

Encrypt Your Data: Use built-in encryption tools like BitLocker to encrypt your hard drive and sensitive data. Encrypting your data helps protect it from unauthorized access, in case your device is lost or stolen.

Backup Your Data Regularly: Perform regular backups of your important files and data to an external hard drive, cloud storage service, or network drive. In the event of a security incident or system failure, you can restore your data from backups without losing valuable information.

Use Account Types Appropriately: Avoid using an administrator account for everyday tasks. Instead, use a standard user account for regular use, and only switch to an administrator account when necessary. This can help prevent unauthorized changes to your system.

Stay Informed and Educated: Stay informed about the latest security threats and best practices by following reputable security blogs, news sources, and forums. Educate yourself and others in your household or organization about common security risks and how to mitigate them.

Enable BitLocker: If you're using Windows 10 Pro or Enterprise, consider encrypting your system drive with BitLocker to protect your data in case your device is lost or stolen. BitLocker provides full-disk encryption, ensuring that only authorized users can access your data.

Use Windows "Hello" for Biometric Authentication: If your device supports it, consider using Windows Hello for biometric authentication, such as facial recognition or fingerprint scanning, to log in to your system securely without relying solely on passwords.

Enable Controlled Folder Access: Controlled Folder Access is a feature in Windows Security that helps protect your important files and folders from unauthorized changes by malicious applications. Enable this feature to add an extra layer of security to your sensitive data.

SmartScreen: SmartScreen is a feature in Windows that helps protect against phishing attacks and malicious software downloads. It checks websites and files against a list of known threats and warns users if they encounter potentially harmful content.

Device Guard: Device Guard is a security feature in Windows 10 Enterprise and Windows Server 2016 that helps protect against malware by allowing only trusted applications to run on the system. It uses hardware-based security features to ensure that only signed and trusted code is executed.

Credential Guard: Credential Guard is a security feature in Windows 10 Enterprise and Windows Server 2016 that helps protect against Pass-the-Hash (PtH) attacks by storing user credentials securely in a virtualized environment.

Windows Defender Application Guard: This feature in Windows 10 Enterprise provides hardware-based isolation for Microsoft Edge browser sessions, protecting the rest of the system from potential malware and zero-day attacks that may originate from the internet.

Security Baselines: Microsoft provides security baselines that are a set of recommended security settings for Windows systems to help organizations improve their security posture. These baselines are regularly updated to address emerging threats and vulnerabilities.

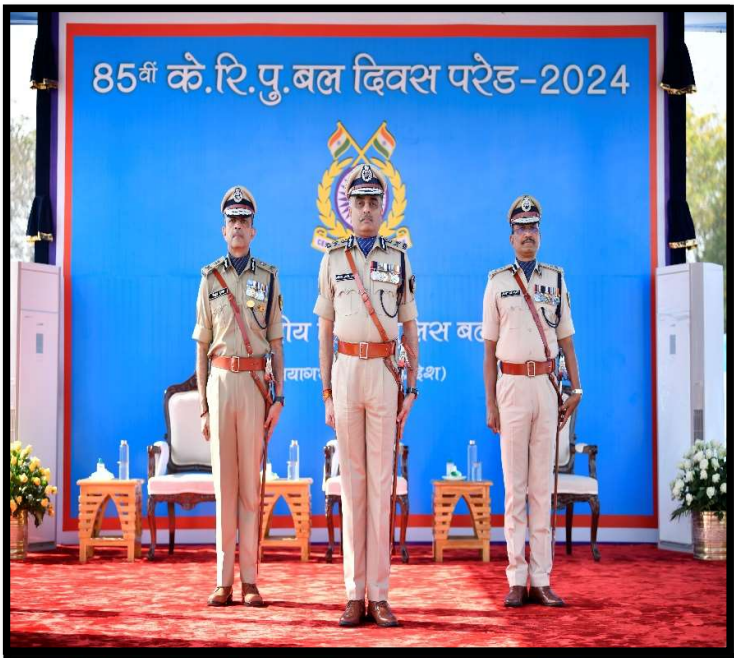
Microsoft Security Blog: Microsoft regularly publishes updates and announcements related to Windows Security on its official Security Blog. You can visit the blog to stay informed about the latest security features, best practices, and threat intelligence from Microsoft.

Windows Security Center: Check the Windows Security Center on your system for any alerts, notifications, or recommendations related to security. Windows Security provides insights into the overall security status of your system and offers recommendations to enhance security.

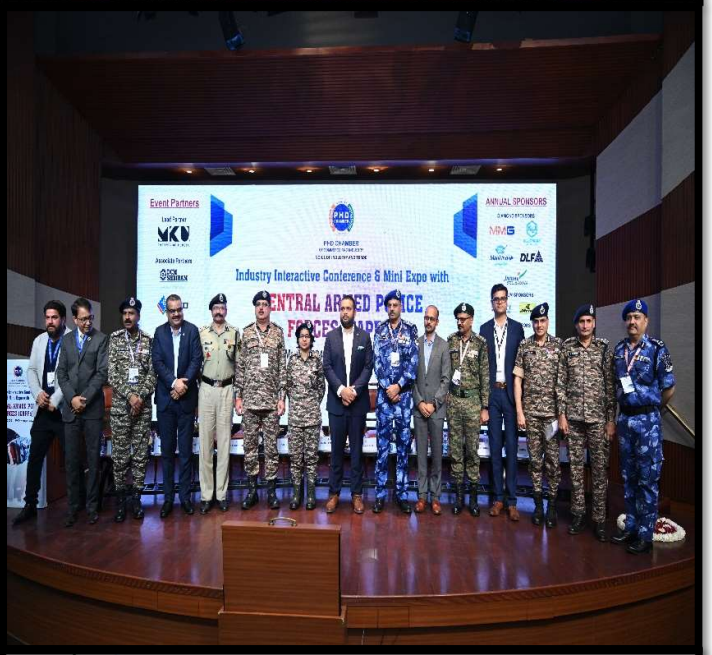
Microsoft Security Response Center (MSRC): The MSRC is Microsoft's primary security information portal for security researchers, professionals, and customers. It provides information about security vulnerabilities, patches, and advisories related to Microsoft products, including Windows Security.

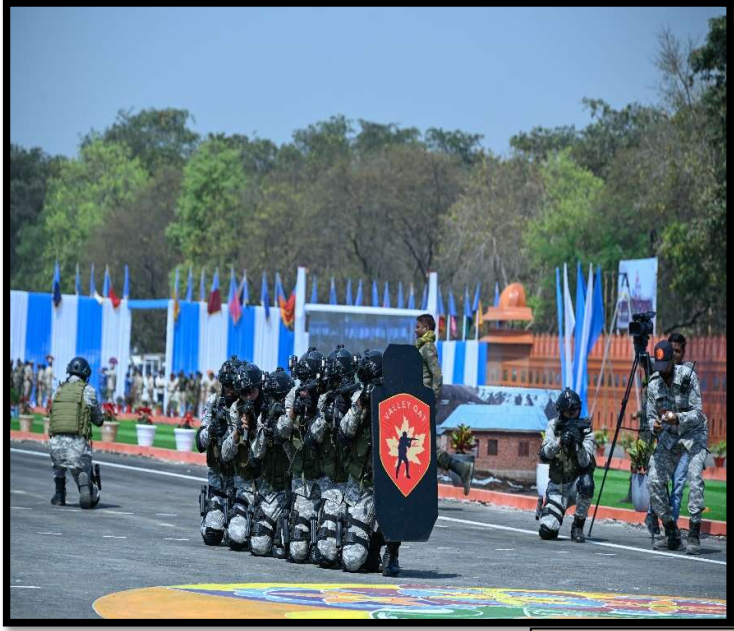
Security Conferences and Events: Keep an eye on security conferences, webinars, and events where Microsoft representatives or security experts may discuss the latest security trends, threats, and best practices related to Windows Security.

Security Communities and Forums: Engage with security communities, forums, and discussion groups where professionals and enthusiasts shard insights, tips, and news about Windows Security and related topics.


85वीं के.रि.पु.बल दिवस परेड-2024


होली उत्सव


Event Partners
ANNUAL SPONSORS
Industry Interactive Conference & Mini Expo with




सेवा निष्ठा
85वें के.रि.पु.बल दिवस परेड-2024