ENTRAL RESERVE POLICE FORCE

CYBER BYTE

- Stealing Malware
- “SOGU or PlugX” malware family.

CYBER BYTE MARCH-2024 EDITION

- Cyber frauds updates

- Android Security
- Case Study

1.CYBER GEEKS NEWS

A) Stealing Malware (i) RedLine (ii) Raccoon (iii) Vidar.

(i) RedLine: - A relatively new type of malware, RedLine Stealer has made security enthusiasts on their toes. It's evasive and hard to detect by various security tools. RedLine Stealer is a malicious information-stealing software that uses a customizable file-grabber to collect victims' sensitive data from web browsers, applications, emailing and messaging apps, and cryptocurrency wallets. This malware can gather detailed information about the infected device, such as its programs, antivirus products, and running processes, and proceed to elaborate ransomware attacks.

In essence, RedLine Stealer works as a remote access trojan that exfiltrates data and transfers sensitive user information to hackers who sell it on dark web forums afterward. Threat actors can make use of RedLine Stealer relatively easily because it works on a malware-as-a-service (MaaS) model.

How does RedLine Stealer infect a computer?

RedLine Stealer can infect a victim's device in a number of ways. The most common methods used by threat actors to distribute RedLine Stealer, includes-

Phishing emails: - Infecting devices through social engineering schemes is a technique favored by hackers, and RedLine Stealer is no exception. Using phishing emails, threat actors can send malicious attachments or links to a large number of recipients all at once.

Compromised websites: - Web users can be redirected to compromised websites through malicious ads or when hacker's typo squat well-known domain names. It only takes a visit to an infected website to get tricked into downloading legitimate-looking software from a seemingly official website but getting RedLine Stealer instead.

Legitimate-looking applications: - Being a trojan, RedLine Stealer malware can disguise itself as a legitimate-looking app or software program that is actually cracked and hides malware. In the most bizarre cases, victims can download malware thinking they are getting new antivirus software for their device or an update for their operating system.

(ii) Raccoon: - Raccoon malware comes with fairly basic info stealer functions like RedLine and by itself lacks any kind of antivirus protection. There are no functions that would complicate the analysis of the malware. However, Raccoon developers do suggest using a third-party crypter (a type of malware).

When it comes to the core functionality this virus depending on the configuration enabled by an attacker, can check system settings, capture screenshots, collect basic information like OS version, IP and username and steal passwords and logins from a variety of browsers. On top of that, the stealer can retrieve information from Microsoft Outlook as well as steal cryptocurrency wallets. When the data collection process ends the data is packed into a .ZIP archive that is then sent to the attackers' server.

(iii) Vidar: - Vidar is a type of information-stealing malware, specifically designed for stealing sensitive personal and financial information from infected systems. The Vidar malware is typically delivered via email, recently, in many campaigns as an ISO file, which is a disk image file format commonly used by malware authors to package their malware. In Vidar's case, the malicious ISO has been embedded in fake installers for legitimate software such as Adobe Photoshop and Microsoft Teams, delivered via the Fallout exploit hit, and sent as an attachment to phishing emails.

Vidar is an info stealer and frequently uses social media as part of its command and control (C2) infrastructure. The IP address of the C2 infrastructure will be embedded in a user profile on platforms like Mastodon or Twitter. The malware can access this profile, contact the indicated IP address, and download configuration files, instructions, and additional malware.

The Threat Vidar is primarily an info stealer, meaning that it is designed to collect a variety of sensitive information from an infected computer and exfiltrate this data to an attacker. Some examples of the information that Vidar collects from infected computers, browsers, and digital wallets include the following: OS data, Account credentials, Credit card data, Browser history.

Suggestions:

Keep Software Updated: Regularly update your operating system, antivirus software, and all applications to patch known vulnerabilities.

Use Reputable Security Software: Install reputable antivirus and anti-malware software to detect and prevent potential threats.

Exercise Caution with Emails: Avoid opening email attachments or clicking on links from unknown or suspicious sources. Be vigilant about phishing attempts.

Strong Passwords and Multi-Factor Authentication (MFA): Use complex passwords and enable MFA where possible to enhance account security.

Regular Backups: Perform regular backups of your important data and ensure they are stored securely. This helps mitigate the impact of potential attacks like ransomware.

Network Security Measures: Configure firewalls and intrusion detection/prevention systems to help safeguard your network.

Network Segmentation: Implement network segmentation to limit the potential spread of malware within your network.

Monitor System Activity: Regularly monitor system logs and network traffic for any unusual or suspicious activities.

Stay Informed: Stay updated with the latest cybersecurity news and advisories to remain informed about potential threats and vulnerabilities.

(B) "SOGU or PlugX" malware family : -

SOGU or PlugX refers to a type of malware that is known for its advanced and sophisticated capabilities. PlugX is the original name, while SOGU is often used as an alias for this malware. Here are key characteristics associated with SOGU/PlugX:

Remote Access Trojan (RAT): SOGU/PlugX is a Remote Access Trojan, or RAT, which means it is designed to provide attackers with unauthorized remote access to infected systems.

Espionage and Targeted Attacks: SOGU/PlugX is often associated with targeted cyber-espionage campaigns. It has been used by advanced persistent threat (APT) groups to compromise specific targets, including government organizations, military entities, and critical infrastructure.

Modular Design: SOGU/PlugX has a modular architecture, allowing attackers to customize its functionality based on their objectives. This modular design makes it adaptable and enables the malware to evolve in response to changing security measures.

Command and Control (C2) Servers: The malware establishes communication with command and control servers operated by attackers. This communication channel is used for sending instructions to the infected systems and exfiltrating sensitive data.

Persistence: SOGU/PlugX often employs various techniques to maintain persistence on infected systems. This may involve creating registry entries, scheduled tasks, or other mechanisms that ensure the malware remains active after system reboots.

Anti-Analysis Techniques: To avoid detection and analysis by security researchers, SOGU/PlugX incorporates anti-analysis techniques. This can include code obfuscation, encryption, and polymorphic elements to make it more difficult to identify and understand its behavior.

Delivery Methods: The malware is typically delivered through spear-phishing emails containing malicious attachments or links. Once a user interacts with the malicious content, the malware is executed on the target system.

Information Theft: SOGU/PlugX is capable of stealing sensitive information from infected systems. This can include login credentials, intellectual property, and other confidential data.

Suggestions:

- Update system, applications and software to the latest version and download the latest security patches.
- Install anti-virus/anti-malware software and keep the software (and its definition files) updated.
- Perform a scan of the system and networks regularly and scan all received files.
- Use complex passwords and strong methods of authentication.
- Be careful while clicking on links from untrusted sources.
- Don't trust pop-up windows that ask you to download software.
- Regularly monitor all user accounts and disable inactive accounts.
- Enforce password updates for account owners that may have their credentials leaked.

2.CYBER FRAUDS

Online trading scam: Gurugram doctor falls victim, loses Rs 2.5 crore.

Online trading scams are becoming a growing concern across the country. In the past few weeks, tens of individuals have fallen victim, losing lakhs. More recently, a doctor from Gurugram has become the victim of this cyber scam, losing a staggering Rs 2.5 crore to unidentified cybercriminals. According to a case reported by The Tribune, the victim a resident of Kendriya Vihar Society in Sector 56, came across a tempting advertisement on the internet on January 4, 2024. The advertisement offered a stock marketing investment plan, promising significant profits through online stock and initial public offering (IPO) investments. Enticed by the source of easy gains, victim contacted the number provided in the advertisement. Upon his inquiry, the caller sent him a link via WhatsApp, through which he was asked to download a share buying app which the victim felt legitimate. Further trusting the app's functionality, victim started making investments, initially investing Rs 50,000 to purchase shares. While his initial investment appeared to pay off, victim was soon persuaded to participate in an IPO. The app deceptively inflated his account balance, showing a substantial profit of Rs 3.19 crore. However, when he attempted to withdraw his profits, he was denied withdrawals. Unable to access his funds, victim contacted the scammers, but they further manipulated him. They convinced him to deposit additional money under the guise of "security deposits" to facilitate the withdrawal process. Falling prey to their elaborate scheme, victim transferred a total of Rs 1.36 crore in multiple transactions. Unfortunately, after successfully duping a significant sum from the doctor, the scammers vanished. Victim even tried to contact them through all available channels. With all communication channels severed and his attempts to retrieve his investments failing, victim finally approached the police to file a formal complaint.

3.TIP OF THE MONTH

Android Security:

Device Security:

Keep Software Updated: Regularly update your Android operating system and apps to patch security vulnerabilities.

Use Strong Lock Screen: Set up a secure lock screen method, such as PIN, password, or pattern, to protect against unauthorized access.
Enable Find My Device: Activate the "Find My Device" feature to locate, lock, or wipe your device remotely if needed.
Encrypt Your Device: Enable device encryption to protect your data in case your device falls into the wrong hands.
Biometric Authentication: If available, use fingerprint or facial recognition for an additional layer of security.

App Security:
Download Apps from Trusted Sources: Only install apps from reputable sources like the Google Play Store to avoid malware.
Review App Permissions: Check and understand the permissions requested by apps before installing them.
App Auto-Updates: Enable automatic app updates to ensure you have the latest security patches.
Use Security Apps: Install a reliable antivirus or security app to scan for and protect against malware.
App Permissions Audit: Periodically review and revoke unnecessary app permissions to enhance privacy.

Network and Connectivity:
Use Secure Wi-Fi: Avoid connecting to open or unsecured Wi-Fi networks; use a VPN for added security.
Bluetooth Security: Disable Bluetooth when not in use to prevent unauthorized access.
Google Account Security: Enable Two-Factor **Authentication:** Add an extra layer of security to your Google account with two-factor authentication.
Regularly Update Passwords: Change your Google account password regularly to enhance security.
Review Google Account Activity: Periodically check your account activity for any unauthorized access.

Data Protection:
Device Backup: Regularly back up your device to safeguard important data.
Secure Cloud Storage: If using cloud services, enable two-factor authentication and encrypt sensitive files.

Safe Browsing:
Use a Secure Browser: Choose a trusted browser and keep it updated for the latest security features.
Be Cautious with Links: Avoid clicking on suspicious links in emails or messages to prevent phishing.

General Security Practices:
Educate Yourself: Stay informed about the latest security threats and best practices.
Avoid Rooting Your Device: Rooting your device can expose it to security risks; avoid unless absolutely necessary.
Regularly Check for Malware: Use security apps to scan for malware regularly.
Disable Unknown Sources: Turn off the installation of apps from unknown sources in your device settings.

Privacy Controls:

Manage Location Settings: Limit app access to your location to enhance privacy.
Control Personal Data Sharing: Be cautious about the information you share on social media and other platforms.

Communication Security:
Use Encrypted Messaging Apps: Choose messaging apps that offer end-to-end encryption for secure communication.
Secure Email Accounts: Use strong passwords for email accounts and consider enabling two-factor authentication.

Physical Security:
Be Mindful in Public: Avoid displaying sensitive information in public spaces to prevent unauthorized access.
Use a Screen Protector: Protect your screen from prying eyes in crowded places.
Track Permissions Changes: Be vigilant for any unexpected changes in app permissions and investigate if needed.

Case Study

Case details: - Malware Analysis of PE filevarbaytsa.exe and ragihaca.exe

1. Summary of filevarbayrsa.exe

Malware Analysis of varbaytsa.exe (4 MB) (vdhrh madtvin.exe) CRIMSON RAT Family reveals that given malware is Keyloger and variant of Crimson RAT family. Given Malware is a RAT which is highly sophisticated malware developed in Microsoft.net with metadata name rebok vkolge.exe created on 2023-06-14 12:57:19 UTC. Malware is reading network information, files, directory listing, from the different partitions and external drives. The malware saves keystrokes and clipboard data in varbaytsa file. Malware utilizes execution using PowerShell scripts.

It also contains anti debug code, anti vm code and antivirus evasion code like higher sleep time to hide itself from security solutions. It is making communication to 5.189.132.99 (Contabo GMBH, Germany), 82.146.34.137 (Russia). Attacker has used Cobalt strike adversary simulation tool for sending payloads to compromise systems.

2. Summary of ragihaca.exe

Malware Analysis of ragihaca.exe reveals that given malware contains a fake WhatsApp icon to mislead users. Given Malware is a Trojan/Backdoor which is highly sophisticated malware developed in Microsoft .net with metadata name rebok vkolge.exe created on 2023-06-14 12:57:19 UTC. Malware is reading network information, files, directory listing, from the different partitions and external drives. It seems that after cnc communication malware downloads fake pdf, ppt files listed in the blawstom Ink file. Malware utilizes execution using PowerShell scripts.

Given malware contains anti debug code, anti vm code and antivirus evasion code like higher sleep time to hide itself from security solutions. It is making communication to 5.189.132.99 (Contabo GMBH, Germeny), 82.146.34.137 (Russia). Attacker has used Cobalt strike adversary simulation tool for sending payloads to compromised systems.

COMN. & IT DIRECTORATE, CRPF