CENTRAL RESERVE POLICE FORCE

CYBER BYTE

- Rafel Rat, Android Malware from Espionage to Ransomware Operations.
- New Attack Technique 'Sleepy Pickle' Targets Machine Learning Models.
- New Credit Card Skimmer Targets WordPress, Magento, and OpenCart Sites.

- **Cyber frauds updates**

CYBER BYTE
JULY-2024
EDITION

1.CYBER GEEKS NEWS

A) Rafel Rat, Android Malware from Espionage to Ransomware Operations.

Android, Google's most popular mobile operating system, powers billions of smartphones and tablets globally. Known for its open-source nature and flexibility, Android offers users a wide array of features, customization options, and access to a vast ecosystem of applications through the Google Play Store and other sources.

However, widespread adoption and open environment comes with the risk of malicious activities. Android malware, a malicious software designed to target Android devices, poses a significant threat to users' privacy, security, and data integrity. These malicious programs come in various forms, including viruses, Trojans, ransomware, spyware, and adware, and they can infiltrate devices through multiple vectors, such as app downloads, malicious websites, phishing attacks, and even system vulnerabilities.

The evolving landscape of Android malware presents challenges for users, developers, and security experts. As attackers employ increasingly sophisticated techniques to evade detection and compromise devices, understanding the nature of Android malware, its distribution methods and effective prevention and mitigation strategies become paramount.

Rafel RAT is an open-source malware tool that operates stealthily on Android devices. It provides malicious actors with a powerful toolkit for remote administration and control, enabling a range of malicious activities from data theft to device manipulation.

Nodal agencies identified APT-C-35 / DoNot Team utilizing Rafel RAT. Rafel's features and capabilities, such as remote access, surveillance, data exfiltration, and persistence mechanisms, make it a potent tool for conducting covert operations and infiltrating high-value targets.

Suggestion

- Keep your Devices Updated.
- Use a trustworthy/Reputed Security Software.
- Review and manage app permissions carefully.
- Beware of Phishing and Social Engineering.
- Regularly back up important data stored on Android devices to secure cloud storage or external devices.
- Use Strong Authentication.
- Use device encryption to protect sensitive data stored on the device.
- Regularly scan your device for malware using a trustworthy/reputed mobile security app.

B) New Attack Technique 'Sleepy Pickle' Targets Machine Learning Models.

The security risks posed by the Pickle format have once again come to the fore with the discovery of a new "hybrid machine learning (ML) model exploitation technique" dubbed Sleepy Pickle.

The attack method, per Trail of Bits, weaponizes the ubiquitous format used to package and distribute machine learning (ML) models to corrupt the model itself, posing a severe supply chain risk to an organization's downstream customers.

"Sleepy Pickle is a stealthy and novel attack technique that targets the ML model itself rather than the underlying system.

While pickle is a widely used serialization format by ML libraries like PyTorch, it can be used to carry out arbitrary code execution attacks simply by loading a pickle file (i.e., during deserialization).

Sleepy Pickle works by inserting a payload into a pickle file using open-source tools like Fickling, and then delivering it to a target host by using one of the four techniques such as an adversary-in-the-middle (AitM) attack, phishing, supply chain compromise, or the exploitation of a system weakness.

Suggestion

- Conduct regular security checks of the system.
- Regularly monitor access logs.
- Use HTTPS for endpoints.
- Develop and update incident response plans.
- Provide ongoing security training.
- Regularly Update the Software patches.

C) New Credit Card Skimmer Targets WordPress, Magento, and OpenCart Sites.

Multiple content management system (CMS) platforms like WordPress, Magento, and OpenCart have been targeted by a new credit card web skimmer called Caesar Cipher Skimmer.

A web skimmer refers to malware that is injected into e-commerce sites with the goal of stealing financial and payment information. The latest campaign entails making malicious modifications to the checkout PHP page associated with the WooCommerce plugin for WordPress ("form-checkout.php") to steal credit card details.

The injections have been changed to look less suspicious than a long-obfuscated script noting the malware's attempt to masquerade as Google Analytics and Google Tag Manager. Specifically, it employs the same substitution mechanism employed in Caesar cipher to encode the malicious piece of code into a garbled string and conceal the external domain that's used to host the payload. It's presumed that all the websites have been previously compromised through other means to stage a PHP script that goes by the names "style.css" and "css.php" in an apparent effort to mimic an HTML style sheet and evade detection.

These scripts, in turn, are designed to load another obfuscated JavaScript code that creates a WebSocket and connects to another server to fetch the actual skimmer. The script sends the URL of the current web pages, which allows the attackers to send customized responses for each infected site. Some versions of the second layer script even check if it is loaded by a logged-in WordPress user and modify the response for them.

The form-checkout.php file in WooCommerce is not the only method used to deploy the skimmer, the attackers have also been spotted misusing the legitimate WPCode plugin to inject it into the website database. On websites that use Magento, the JavaScript injections are performed on database tables such as core_config_data. It's currently not known how this is accomplished on OpenCart sites. Due to its prevalent use as a foundation for websites, WordPress and the larger plugin ecosystem, have become a lucrative target for malicious actors, allowing them easy access to a vast attack surface.

It's imperative that site owners keep their CMS software and plugins up-to-date, enforce password hygiene, and periodically audit them for the presence of suspicious administrator accounts.

Suggestion

- Update Softwares Regularly.
- Use Security Plugins.
- Use strong, unique passwords and enable two-factor authentication (2FA) for admin accounts.
- Regularly review server and application logs for any suspicious activities.
- Restrict administrative access to only those who need it and from known IP addresses.
- Ensure your site uses HTTPS to encrypt data transmitted between the user and your website.
- Regularly scan your website for malware and vulnerabilities.

2.CYBER FRAUDS

A). A bank manager lost Rs 5.10 lakh in an online cyber fraud while she was trying to sell few of her household items.

A bank manager lost Rs 5.10 lakh in an online cyber fraud while she was trying to sell few of her household items in Nagpur. The 31-year-old victim uploaded details of a refrigerator and sofa which she wanted to sell. As soon as she filled up the details, she got a call from a person who said he wanted to buy the items.

The accused asked her to send Rs 60 as an initial verification transaction. After she did so, he withdrew Rs 1.01 lakh from her account. In the name of refunding this amount, she again paid Rs 9,000 and the accused withdrew Rs 5.10 lakh in all. According to the police, a case was lodged under Indian Penal Code and Information Technology Act provisions and efforts are on to nab the culprit.

B) Senior Citizen Loses Rs 3 Lakh in Sophisticated Voice Cloning Scam.

A 63-year-old man fell victim to a sophisticated cyber scam, losing Rs 3 lakh. The fraudster, pretending to be his son's friend, duped him by mimicking son's friend voice over a phone call. The elderly man, whose children reside abroad, was deceived when he received a call via WhatsApp from an unknown number. The caller, imitating son's friend voice, whom the victim knew since childhood, pleaded for urgent financial help. Trusting the caller's familiar voice, the victim transferred Rs 2 lakh to the provided account and convinced two friends to contribute Rs 50,000 each. However, suspicion arose when the caller demanded more money, and subsequent attempts to video call the fraudster were unsuccessful. Realizing the deception, the victim discovered that the real son's friend had made no such calls. The police have since registered the case and are conducting further investigations.

3.TIP OF THE MONTH

Broadband Security.

Broadband Internet connection is "Always On" & default configurations are extremely vulnerable.

Do's for Broadband Internet

1. **Change the Default SSID (Service Set Identifier):** it can be misused by the attacker to break into the network / computer.

2. **Enable Wireless Security:** Modem routers support wireless security. User can select any one protocol and a protection key. The same wireless security protocol and protection key has to be enabled in computer.

3. **Assign Static IP Addresses to Devices:** Most of the home users are allotted dynamic IP addresses, as DHCP technology is easy to setup. Turn off DHCP option in router or access point and use fixed IP address range.

4. Regularly update the firmware (driver code).

5. Always download broadband drivers from the legitimate websites recommended by the manufacturer.

6. Change Default Administrator Passwords and User names.

7. **Enable MAC Address Filtering:** Every device has a unique MAC address. Broadband access points can be combined with the MAC address of the equipment for limited access to the devices.

8. **Turn on (Compatible) WPA / WEP Encryption:** All Wi-Fi enabled modems/ router support some form of encryption technology, which has to be enabled.

9. Use effective end point security solution (with anti-virus, anti-spyware, desktop firewall etc.) to protect computer/ laptop from broadband Internet security threats.

10. Enable Firewall on Modem Router as well as Computer.

Don't for Broadband Internet

1. Don't leave broadband connectivity open when it is not utilized.

2. Don't use USB broadband modem with insecure computer/laptop.

3. Don't use connection without a filter for each broadband Internet line.

4. Don't enable the option for remote access/administration (via Internet), as it is not required for a home user.

5. Do not Enable Auto-Connect to Open Wi-Fi Networks.

6. Never connect to unknown or un-trusted network in case of Wi-Fi.

केन्द्रीय रिज़र्व पुलिस बल
शैक्षणिक उत्कृष्टता अलंकरण समारोह
22 जून 2024

CWA RAISING DAY-2024

29th CWA RAISING DAY
सार्थक सहयोग सर्वदा
CENTRAL RESERVE POLICE FORCE