CENTRAL RESERVE POLICE FORCE

CYBER BYTE

- **Telegram App Flaw Exploited to Spread Malware Hidden in Videos.**
- **Fake CrowdStrike repair manual pushes new infostealer malware.**
- **Evolution of jRAT JAVA Malware.**

CYBER BYTE
AUGUST-2024
EDITION

- **Cyber frauds updates**

- **Do's and Don'ts for IoT**

1.CYBER GEEKS NEWS

A) Telegram App Flaw Exploited to Spread Malware Hidden in Videos.

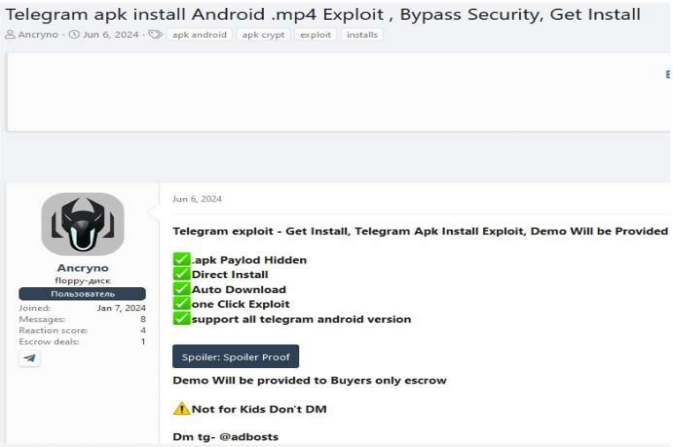
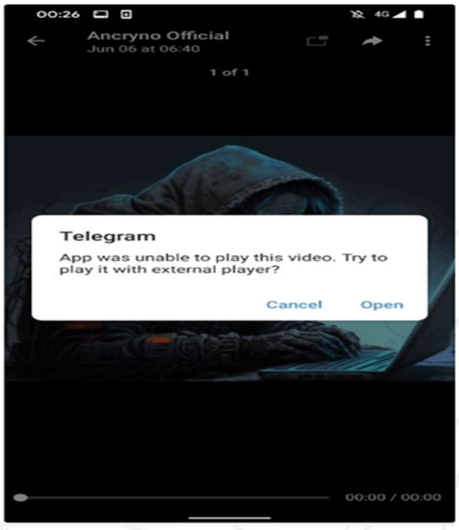


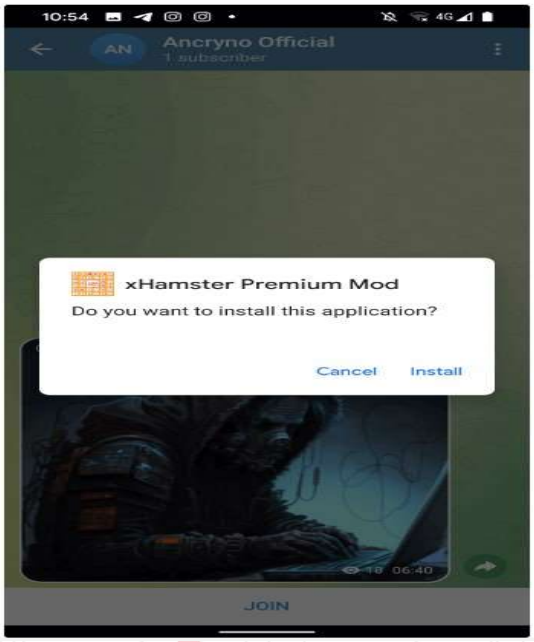
Figure 2. Post on an underground forum

A zero-day security flaw in Telegram's mobile app for Android, called Evil Video, made it possible for attackers to malicious files disguised as harmless-looking videos. The exploit appeared for sale at an unknown price in an underground market; the issue was addressed by **Telegram in version 10.14.5.**

"Attackers could share malicious Android payloads via Telegram channels, groups, and chat, and make them appear as multimedia files. It's believed that the payload is concocted using Telegram's application programming interface (API), which allows for programmatic uploads of multimedia files to chats and channels. In doing so, it enables an attacker to camouflage a malicious APK file as a 30-second video.



Users who click on the video are displayed an actual warning message stating that the video cannot be played and urging them to try playing it using an external player. If they proceed with this step, they are subsequently asked to allow the installation of an APK file through Telegram. The app in question is named **'xHamster Premium Mod".**



"By default, media files received via Telegram are set to download automatically. "This means that users with the option enabled will automatically download the malicious payload once they open the conversation where it was shared. While this option can be disabled manually, the payload can still be downloaded by tapping the download button accompanying the supposed video. It's worth noting that the attack does not work on Telegram clients for the web or the dedicated Windows app. It's currently not clear who is behind the exploit and how widely it was used in real-world attacks. The same actor, however, advertised in January 2024 a fully undetectable **Android crypter (aka cryptor)** that can reportedly bypass Google Play Protect.

Hamster Kombat's Viral Success Spawns Malicious Copycat#

The development comes as cyber criminals are capitalizing on the Telegram-based cryptocurrency game 'Hamster Kombat' for monetary gain. ESET has discovered fake app stores promoting the app, GitHub repositories hosting Lumma Stealer for Windows disguised as automation tools for the game, and an unofficial Telegram channel used to distribute an Android trojan called Ratel.

Ratel, offered via a Telegram channel named **"hamster_easy,"** is designed to impersonate the game **("Hamster.apk")** and prompts users to grant it notification access and set itself as the default SMS

application. It subsequently initiates contact with a remote server to get a phone number as response. In the next step, **the malware sends a Russian language SMS message to that phone number**, likely belonging to the malware operators, to receive additional instructions over SMS.

"The threat actors then become capable of controlling the compromised device via SMS: The operator message can contain a text to be sent to a specified number, or even instruct the device to call the number. "The malware is also able to check the victim's current banking account balance for **Sberbank Russia by sending a message with the text баланс (translation: balance**) to the number 900." Ratel abuses its notification access permissions to hide notifications from no less than 200 apps based on a hard-coded list embedded within it. It's suspected that this is being done in an attempt to subscribe the victims to various premium services and prevent them from being alerted. The Slovakian cybersecurity firm said it also spotted fake application storefronts claiming to offer Hamster Kombat for download, but actually directs users to unwanted ads, and GitHub repositories offering Hamster Kombat automation tools that deploy **Lumma Stealer** instead.

"The success of Hamster Kombat has also brought out cybercriminals, who have already started to deploy malware targeting the players of the game. "Hamster Kombat's popularity makes it ripe for abuse, which means that it is highly likely that the game will attract more malicious actors in the future."

BadPack Android Malware Slips Through the Cracks#

Beyond Telegram, malicious APK files targeting Android devices have also taken the form of BadPack, which refer to specially crafted package files in which the header information used in the ZIP archive format has been altered in an attempt to obstruct static analysis.

Suggestion

- **Update Telegram:** Ensure you're using the latest version of the app.
- **Scan for Malware:** Use antivirus software to check your device.
- **Be Cautious:** Avoid clicking on or downloading suspicious videos.
- **Enable 2FA**: Add two-factor authentication to your Telegram account.
- **Report Issues:** Notify Telegram support if you encounter suspicious activity.

B) Fake CrowdStrike repair manual pushes new infostealer malware.

CrowdStrike has warned that a fake recovery manual to repair Windows devices is installing a new information-stealing malware called Daolpu. The buggy CrowdStrike Falcon update caused global IT outages, threat actors have quickly begun to capitalize on the news to deliver malware through fake fixes. A new campaign conducted through phishing emails pretends to be instructions on using a new Recovery Tool that fixes Windows devices impacted by the recent CrowdStrike Falcon crashes. Once active on the system, the stealer harvests account credentials, browser history, and authentication cookies stored in Chrome, Edge, Firefox, and the Cốc Cốc web browsers.

Spreading Daolpu

Daolpu stealer is believed to be spread via phishing emails that carry a document attachment disguised as a Microsoft recovery manual, named **'New_Recovery_Tool_to_help_with_CrowdStrike_issue_impacting_Windows. docm**.'

This document is a copy of a Microsoft support bulletin that provides instructions on using a new Microsoft Recovery Tool that automates deleting the problematic CrowdStrike driver from Windows devices.

However, this document contains macros that, when enabled, download a base64-encoded DDL file from an external resource and drops it to '% TMP%mscorsvc.dll. 'Next, the macros use Windows certutil to decode the base64-encoded DLL, which is executed to launch the Daolpu stealer on the compromised device. Daolpu terminates all running Chrome processes and then attempts to collect login data and cookies saved on Chrome, Edge, Firefox, and other Chromium browsers.

Analysis by Bleeping Computer shows that it also targets Cốc Cốcm, a web browser primarily used in Vietnam, possibly indicating the malware's origin.

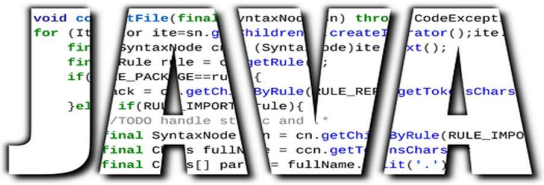
The stolen data is temporarily saved to '%TMP%\result.txt,' and then wiped after it's sent back to the attackers at their C2 server using the URL **'http[:]//172.104.160[.]126:5000/Uploadss'.**

CrowdStrike's advisory about the new malware includes a YARA rule to detect artifacts of the attack and lists the associated indicators of compromise. CrowdStrike urges its customers to only follow advice found on the company's website or other trusted sources after confirming the authenticity of their communications.
Unfortunately, Daolpu is just the latest example of a large-scale effort by cybercriminals to take advantage of the chaotic situation caused by CrowdStrike's Falcon update, causing approximately 8.5 million Windows systems to crash and requiring manual restoration effort. The malicious activity taking advantage of the CrowdStrike Falcon outages includes data wipers spread by the pro-Iranian hacktivist group 'Handala' and HijackLoader dropping Remcos RAT disguised as a CrowdStrike hotfix. In general, there has been a notable increase in phishing attempts impersonating CrowdStrike representatives to distribute malware and a massive effort to register new domains to conduct these malicious campaigns.

Suggestion

- Verify document authenticity.
- Update antivirus software.
- Educate users on phishing threats.
- Use advanced security measures.
- Conduct regular system scans.
- Backup important data.
- Monitor for unusual activity.
- Report suspicious emails.
- Up-to-date system patches.

C) Evolution of jRAT JAVA Malware.



JRat malware, also known as Java Remote Access Tool, is a type of remote access Trojan (RAT) that targets Windows and macOS systems. It is written in Java and uses the Java Runtime Environment (JRE) to execute its malicious code. JRat is a type of malware (malicious software) that is specifically designed to target and attack Java-based applications and systems.

Here are some key features and facts about JRat malware:

1. **Remote access:** JRat allows attackers to remotely access and control infected systems.
2. **Keylogging:** It can log keystrokes, capturing sensitive information like passwords and credit card numbers.
3. **Screen capture:** JRat can take screenshots of the infected system's screen.
4. **File management:** It can upload, download, and delete files on the infected system.
5. **Command execution:** JRat can execute commands and run programs on the infected system.
6. **Persistence:** It can maintain persistence on the infected system, even after rebooting.
7. **Communication:** JRat communicates with its command and control (C2) server using HTTP or HTTPS protocols.
8. **Obfuscation:** It uses obfuscation techniques to evade detection by security software.
9. **Distribution:** JRat is often spread through phishing emails, infected software downloads, or exploited vulnerabilities.

Suggestion

- Keep software up-to-date.
- Use strong antivirus software.
- Avoid suspicious downloads and emails.
- Use strong passwords and enable two-factor authentication.
- Regularly scan systems for malware.

2.CYBER FRAUDS

1. Pune Police constable duped of ₹7 lakh in Stock Market Investment Fraud.

Investment frauds in the guise of lucrative stock market returns are on the rise, with cybercriminals swindling citizens out of crores of rupees. It has now come to light that a police constable from the Pune City Police Department fell victim to such a scam, losing seven lakh rupees. The police constable lodged a complaint at the Shivajinagar Police Station regarding the incident. The constable came across an advertisement on social media promising triple returns on investments in the stock market. Intrigued, he contacted the phone number provided in the advertisement. Cybercriminals on the other end lured him with promises of high returns on stock market investments. The scammers directed him to download a specific app and subsequently instructed him to make investments through it. Over the past eight

months, the constable transferred a total of seven lakh forty-five thousand rupees to the bank accounts specified by the fraudsters. The app deceptively showed substantial returns on his investments, but when he attempted to withdraw the purported profits, he was unable to access the funds. Realizing that the mobile numbers used by the scammers were now inactive, the constable understood he had been duped and filed a complaint with the police. Senior Police Inspector is currently investigating the case.

ii) Bhopal Police arrested 4 for duping people for allegedly duping people on the pretext of making credit cards.

Four men were arrested by the Bhopal Police for allegedly duping people on the pretext of making credit cards of ICICI Bank and offering easy bank loans. In the operation, the Cyber Crime unit of the Bhopal Police also seized at least 10 mobile phones, nine SIM cards, and bank passbooks of several banks. According to the police, the accused lured people by posing as bank employees and offering free credit cards and easy loans. Once a person accepts their offer, they used to send fake website links to a private bank and ask them to provide their personal information. The police received a complaint from a person who said that he was duped by the accused by sending fake links under the guise of making an ICICI Bank credit card. The accused also withdrew more than Rs 60,000 from his bank account, the person said in his complaint.

3.TIP OF THE MONTH

Do's and Don'ts for IoT (Internet of Things).

Do's.

Change Default Passwords: Immediately replace default passwords with strong, unique passwords for each device.
Regularly Update Firmware: Keep your IoT devices updated with the latest firmware and security patches.
Use Strong Encryption: Ensure that data transmitted by IoT devices is encrypted.
Secure Your Network: Use a strong, unique password for your Wi-Fi network and enable WPA3 encryption.
Segment Networks: Create a separate network for your IoT devices to limit potential breaches.
Disable Unnecessary Features: Turn off features and services you do not use to reduce potential vulnerabilities.
Monitor Device Activity: Regularly check activity logs for any unusual behavior on your IoT devices.
Review Privacy Settings: Adjust the privacy settings on IoT devices to limit data collection and sharing.
Enable Two-Factor Authentication: Use two-factor authentication (2FA) whenever possible for added security.
Educate Yourself: Stay informed about the latest IoT security practices and threats.

Don'ts.

Ignore Updates: Don't neglect firmware and software updates for your IoT devices.
Use Default Credentials: Avoid using default usernames and passwords for any IoT device.
Connect Unnecessary Devices: Don't connect devices that you don't need to your network.
Overlook Privacy Settings: Don't ignore the privacy settings; ensure they are configured to protect your data.
Neglect Network Security: Don't use an unsecured Wi-Fi network for your IoT devices.
Share Passwords: Avoid sharing passwords for your IoT devices and networks.
Forget to Monitor: Don't forget to regularly monitor the activity of your IoT devices.
Ignore Security Warnings: Don't ignore security alerts or warnings related to your IoT devices.
Use Weak Passwords: Avoid using weak or easily guessable passwords for any device.
Connect to Public Wi-Fi: Don't connect your IoT devices to public Wi-Fi networks without proper security measures.


केन्द्रीय रिजर्व पुलिस बल
वीरता पदक अलंकरण समारोह-2024