Detect new Android malware fake system update to track and steal user information

The malware can disguise itself as a system update and is designed to automatically activate whenever new information is entered into a device.

International cybersecurity researchers recently discovered a new Android malware with deep espionage capabilities. After successfully penetrating the target Android system, the malicious code will immediately hide and silently steal many types of important data on the system.

More dangerously, the malware can disguise itself as a system update and is designed to automatically trigger whenever new information is entered into a device.

However, this spyware can only be installed as a 'System Update' app available on third-party Android app stores because it has never appeared on the Google Play Store. This feature greatly reduces the spread of the malware, as most experienced users will avoid installing it in the first place on their systems.

Greedy malware

This Remote Access Trojan (RAT) has the ability to steal data quite 'fearsome'. It can collect and extract a wide range of information from an infected Android device to its command and control server (C2 server), which includes many types of important personal data.

Researchers Zimperium - who first discovered the malicious code - observed the entire process of "data stealing, messages, photos and Android phone hijacking" that the trojan performed.

'Once the target device is in control, the hacker can order malicious code to record audio and phone calls, take pictures, review browser history, access WhatsApp messages and more' , Zimperium experts said.

The malware's ability to steal data on a large scale includes:

1. Stealing SMS messages;
2. Stealing SMS database files (if root is available);
3. Check the default browser's bookmarks and search query;
4. Check bookmarks and search history on Google Chrome, Mozilla Firefox and Samsung Internet Browser;
5. Search for files with a specific extension (including .pdf, .doc, .docx and .xls, .xlsx);
6. Check clipboard data;
7. Check the content of announcements;
8. Recording;
9. Voice call recording;
10. Take pictures (via front or rear camera);

11. Access the list of installed applications;
12. Stealing photos and videos;
13. GPS location monitoring;
14. Stealing SMS messages;
15. Stealing phone contacts;
16. Stealing call logs;
17. Filter device information (eg installed applications, device name, memory statistics).

After infecting on an Android device, the malware sends some pieces of information to its Firebase C2 server, including statistics about memory, type of internet connection, and presence of applications. apps like WhatsApp, Facebook .

The malicious code will collect data directly if it has root access or will use Accessibility Services after tricking the victim to enable the feature on the compromised device.

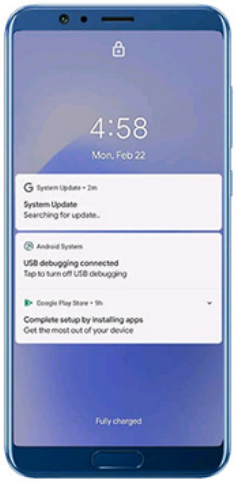
It will also scan the external storage for any cached or stored data, then collect and distribute it to C2 servers when the user connects to the Wi-Fi network.

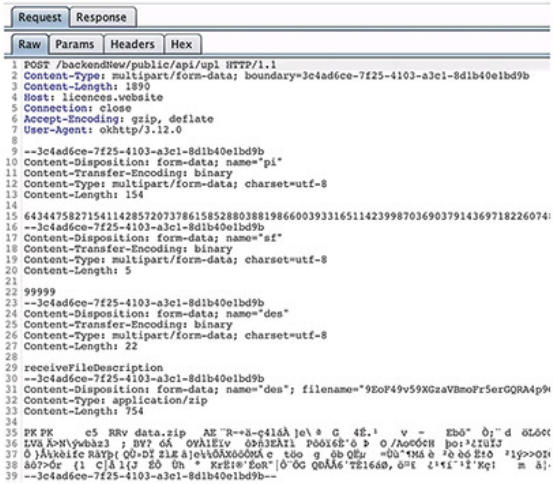
The ability to hide

Unlike other malware designed to steal data, this malware will only be activated using the Android contentObserver and Broadcast receiver when certain conditions are met, such as add a new contact, a new text message, or a new app being installed.

'Commands received through the Firebase messaging service will initiate actions like recording from the microphone and filtering data like SMS messages,' Zimperium said. 'Firebase communication is only used to issue commands and a dedicated C&C server is used to collect stolen data using POST requests'.

The malware will also display a "Searching for update ." fake system update message when it receives new commands from the drivers to disguise its malicious activity.





Additionally, this spyware also conceals its presence on infected Android devices by hiding the icon from the drawer / menu.

To avoid detection, it will only steal the thumb of the video and images it finds, thereby reducing the victim's bandwidth consumption to avoid attracting their attention to background filtering.

Unlike other malware that collects data in bulk, this malware will ensure that it only filters the most recent data, collects location data created and photos taken in the previous few minutes of the crash. multiply.

For now, all activities of this new malware are still closely monitored.