Advanced Notification of Cyber Threats against GhostCtrl Malware

aeCERT Computer Emergency Response Team
فريق الاستجابة لطوارئ الحاسب الآلي

Security Advisory AE-Advisory 17- 40 **Criticality** Critical

Advisory Released On 27 July 2017

Impact

An Android backdoor that silently steals information and control many functionalities of an infected device.

Solution

Adhere the advices written under the solution section.

Affected Platforms

- Android Operating System (OS)

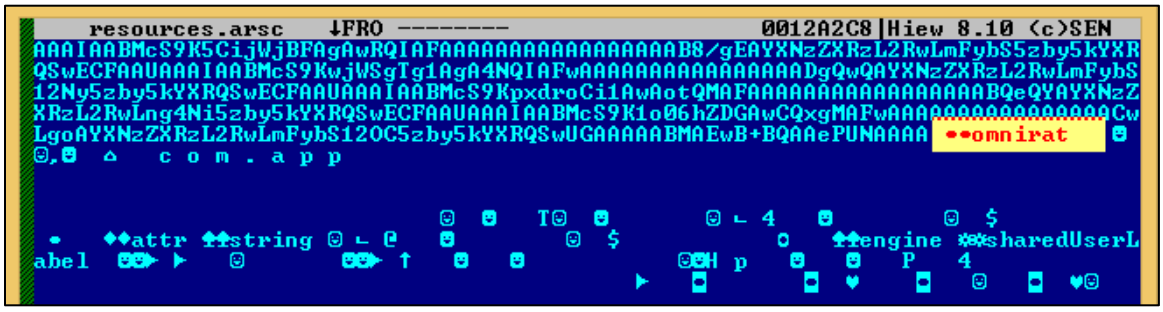
Summary

As the leading trusted secure cyber coordination center in the region, aeCERT has researched and found about a new malware currently named as “GhostCtrl”. GhostCtrl is an Android backdoor malware that can silently steal information from the device, and can also take control of various device functionalities.

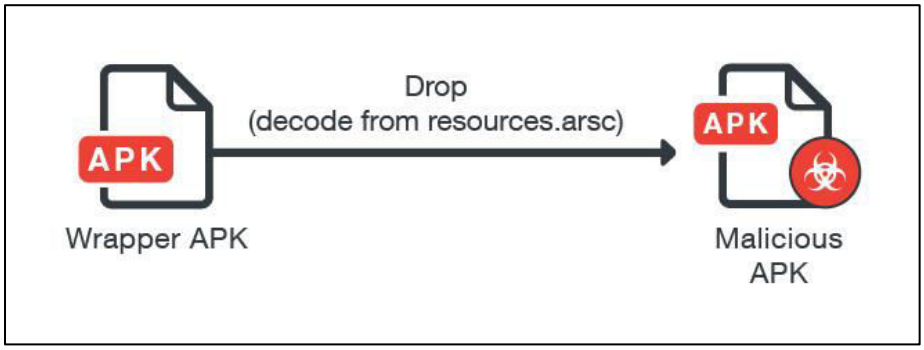
Threat Details

GhostCtrl malware is an Android backdoor that can silently steal information and take over an infected device. It is detected as "ANDROIDOS_GHOSTCTRL.OPS / ANDROIDOS_GHOSTCTRL.OPSA". GhostCtrl is a variant of OmniRAT but is specific to Android OS.

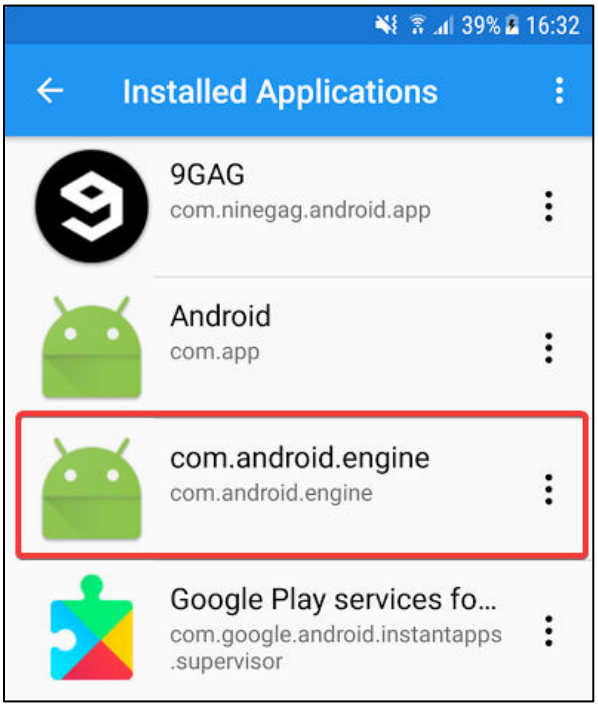
Furthermore, to infect an Android device the malware disguises itself as a legitimate or a popular app such as Pokemon GO, WhatsApp, and even MMS apps. However, this malware cannot be installed through the Store, to install the malware users must download it from an external source, and the device settings must allow installations from unknown sources.



Once the user taps on the malicious APK, GhostCtrl will initiate a persistent behavior to persuade users into installing it, even if the installation request is canceled, a new installation prompt will immediately pop-up. After installation, GhostCtrl will launch a service using a Wrapper APK to allow the Malicious APK to run in the background.



The APK of the malicious app which functions as a backdoor is named “com.android.engine”, the name is similar to Android system apps, for the purpose of deceiving users into believing that it is a legitimate system app.



There are three different versions of GhostCtrl, the first version steals information and silently controls some functionalities of the device, the second version controls additional functionalities of the infected device, and the third version enhances the first and second iteration in all aspects. Accordingly, it is expected that the malware evolves even further in upcoming iterations.

GhostCtrl issue commands to control an infected device from a C&C Server. The commands are encrypted, however the malicious APK decrypts them once they are received. Additionally, the backdoor connects to a domain rather than directly connecting to the C&C IP address.

These are some domains which led to the same C&C IP address:

- php[.]no-ip[.]biz
- ayalove[.]no-ip[.]biz
- hef–klife[.]ddns[.]net
- f–klife[.]ddns[.]net

The commands that are issued by GhostCtrl can take control of the following:

- Stealing device data, such as contacts, phone numbers, SMS records, SIM serial number, browser bookmarks, and location.
- Stealing information, such as Android OS version, Wi-Fi, battery, Bluetooth, audio states, UiMode, Sensor, data from camera, browser, searches, service processes, activity information, and wallpaper.
- Monitor the phone sensors' data in real time.
- Control the Wi-Fi state.
- Control the vibrate function, including the pattern and when it will vibrate.
- Control the system infrared transmitter.
- List the file information in the current directory and upload it to the C&C server.
- Delete a file in the indicated directory.
- Rename a file in the indicated directory.

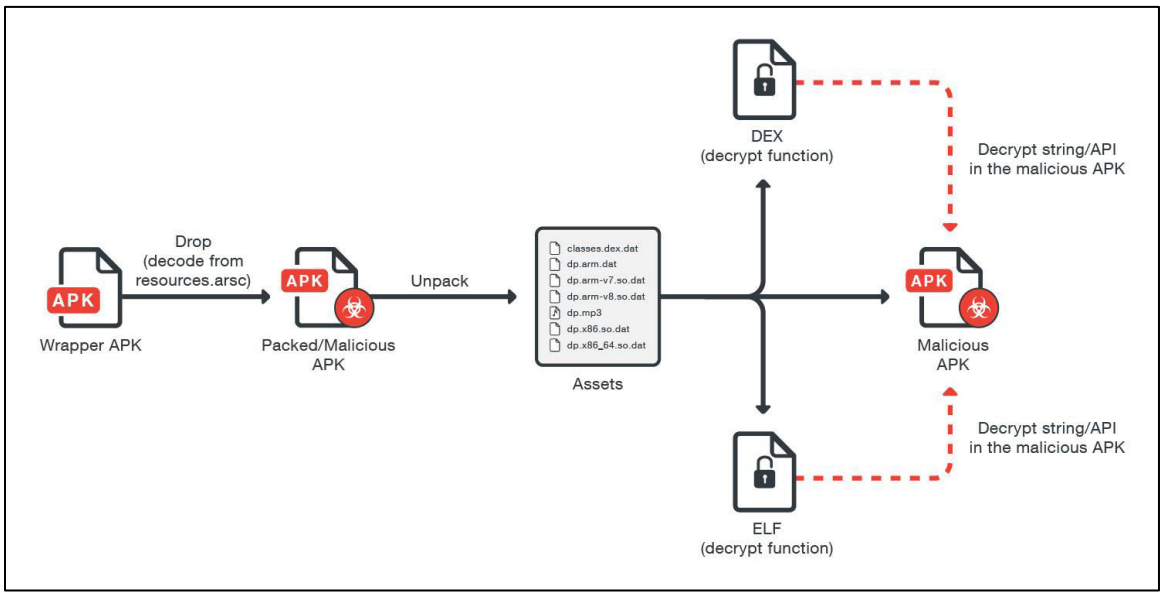
- Upload a desired file to the C&C server.
- Run a shell command specified by the attacker and upload the output result.
- Create an indicated directory.
- Download file.
- Download pictures and sets them as a wallpaper.
- Delete browser history.
- Delete SMS.
- Set phone's UiMode, like night mode/car mode.
- Use the text to speech feature (translate text to voice/audio).
- Send SMS/MMS to a number specified by the attacker; the content can also be customized.
- Call a phone number indicated by the attacker.
- Open activity view-related apps; the Uniform Resource Identifier (URI) can also be specified by the attacker (open browser, map, dial view, etc.).
- Clearing/resetting the password of an account specified by the attacker.
- Play different sound effects by command.
- Specify the content in the Clipboard.
- Customize the notification and shortcut link, including the style and content.
- Control the Bluetooth to search and connect to another device.
- Ability terminate an ongoing phone call.

Commands that were added in the second version of GhostCtrl:

- Capability to function as a ransomware to lock the device and reset its password.
- Roots the device and hijacks the camera of an infected device.
- Creates a scheduled task of taking pictures and recording videos, then silently uploads them to the C&C server as mp4 files.

Enhancements added in the third version of GhostCtrl:

- Incorporated techniques to hide its malicious routes



Solution

It is recommended to apply the following steps to prevent the malware from injecting:

1) Keep the device updated
2) Install a multilayered mobile security solution
3) Maintain updated antivirus software
4) Prevent installation from unknown sources in Android Settings
5) Regularly backup the device data
6) Follow @TheUAETRA on Instagram and Twitter for the latest updates

References

Trend Micro

Contact Us

aeCERT
P.O. Box 116688
Dubai, United Arab Emirates

Tel (+971) 4 230 0003
Fax (+971) 4 230 0100
Email info[at]aeCERT.ae

For secure communications with aeCERT with regards to sensitive or vulnerability information please send your correspondences to aeCERT[at]aeCERT.ae