Possibly Italy-Born Android RAT Reported in China, Find Bitdefender Researchers

hotforsecurity.bitdefender.com/blog/possibly-italy-born-android-rat-reported-in-china-find-bitdefender-researchers-16264.html

Industry News
5 min read

Liviu ARSENE
August 08, 2016

One product to protect all your devices, without slowing them down.
Free 90-day trial

Bitdefender researchers have found a new Android threat designed for spying, with the ability to take screenshots, listen to phone conversations, and upload them to Italy-based C&C servers. The Android RAT was mostly spotted in China and Japan. What makes it a “targeted threat” is that it **seems to have been developed by Italian speakers targeting specific Android devices, selecting their victims based on their devices” IMEI codes**. The analyzed samples date from December 2015 to June 2016.

Key Findings:

- Checks if it”s installed on specific devices, based on IMEI numbers;
- Contains code strings in Italian;
- Connects to Italian C&C servers;
- Targets rooted devices;
- Mostly spotted in China;

Context: The analyzed Android RAT requires a rooted device to exfiltrate data. Considering that 80 percent of China”s mobile users use rooted smartphones, this further supports that it might have been intended for spying on specific devices â€“ possibly on the Chinese market – using IMEI filtering capabilities.

However, even if the targeted device is not rooted, previous Bitdefender research has revealed that some malicious Android applications come fully loaded with exploit packs aimed at rooting Android devices, regardless of the operating system they"re running. Consequently, it"s not difficult to envision a scenario in which a device can be stealthily rooted and then remotely controlled with a RAT like the one analyzed here.

While during our previous research we found that a malicious app could pack four different exploit packs, other security researchers have also revealed that some malware can even pack up to 18 different Android rooting modules to gain full control over the device. Of course, in that particular instance the Trojan was only used to generate revenue by downloading and installing apps on victim"s devices, not to install surveillance tools.

Analyzing Samples

Bitdefender researchers found a series of samples containing this highly targeted Android RAT, dating from December 2015 to June 2016. While it"s been distributed under two package names – **“it.cyprus.client”** and **“it.assistenzaumts.update”** â€“ the basic functionality of the RAT is the same. Neither of the two packages has any interface once it lands on the device.

Although the samples were not found in Google Play, one ound in early February 2016 (**md5: 667452e44935325c2b20a3d7204efe3b**, package: **“it.assistenzaumts.update”)** stirred curiosity as it only connected to specific Command and Control servers only if it validated a series of IMEI codes.

Since the IMEI number usually can identify the exact model of an Android device, the devices the RAT specifically searched for were a **Samsung N9005 Galaxy Note 3 LTE**, a **Samsung SM-G355HN Galaxy 2 Core**, a **LG D820 Nexus 5** and a **G355H Galaxy Core II (SM-G355HN**). (Fig. 1)

If the IMEI scan resulted in a match, the RAT would connect to a specific IP address â€“ belonging to the attacker-controlled command and control center â€“ and start pulling various instructions.

Possibly Italy-Born Android RAT Reported in China, Find Bitdefender Researchers

Fig. 1 â€“Code from January sample that checks for specific IMEI codes.

Other RAT functionalities found in the sample point to traditional behavior, such as taking screenshots at various time intervals, copying the device"s phone settings and sending them to the command and control server, and moving screenshots to the device"s SD card and the uploading them to the attackers" server. (Fig. 2)

Possibly Italy-Born Android RAT Reported in China, Find Bitdefender Researchers

Fig. 2 – Code from January sample that copies screenshots onto SD card

In late June and early July, Bitdefender researchers found two more versions of the same RAT, but this time mostdevices that reported the samples seemed to originate in China. The original sample for February seems to indicate that the device the RAT was tested on was only used for testing, probably for ironing out bugs or checking the malware"s functionality.

However, these new reports seem to indicate that the **it.assistenzaumts.update** package was reported by **7 Android devices in China and one in Netherlands**, according to Bitdefender telemetry. (Fig. 3)

Possibly Italy-Born Android RAT Reported in China, Find Bitdefender Researchers

Fig. 3 â€“ Telemetry on “it.assistenzaumts.update” reports, between January â€“ July 2016

Another interesting aspect of the newly found **“it.assistenzaumts.update”** RAT samples (MD5: **83c90e931a1a9b249b2f9ce8bf5ecd0b** and MD5: **88e8e4ff540fb881d1300f9759026904**), seem to indicate that the newer versions don”t have the C&C server IP addresses hardcoded to the IMEI. (Fig. 4) In fact, they just send the victim”s IMEI code to a specific IP and port address. Naturally, the new C&C IP still originates in Italy.

Possibly Italy-Born Android RAT Reported in China, Find Bitdefender Researchers

Fig. 4 â€“ New version of “it.assistenzaumts.update” that doesn”t have C&C IP”s hardcoded based on IMEI codes

Interestingly enough, the **“it.cyprus.client”** package was not only reported in China, but also in Japan. (Fig. 5) The package seems to have the same abilities as the one analyzed above, except that it”s delivered under a different name.

Possibly Italy-Born Android RAT Reported in China, Find Bitdefender Researchers

Fig. 5 Telemetry on “it.cyprus.client” reports, December 2015 â€“ July 2016

Takeaway

It”s worth mentioning that the RAT”s full spying capabilities only work on rooted devices. While some of it”s basic capabilities, such as device identification, work on non-rooted devices, the malware appears to designed specifically for rooted Android smartphones.

China is well known for having its own surprisingly large Android marketplaces. Coupling this with the fact that the RAT specifically seeks out particular IMEI codes (devices), one can speculate that its developers are highly keen on infecting specific individuals there.

Since only advanced persistent threats (APT) normally exhibit this type of selectivity when infecting victims, this Android RAT could be part of a wider attack that we”ve yet to uncover.

As usual, make sure that you always use a mobile security solution on your devices, as to prevent malicious applications from installing, and make sure that you only download apps from official marketplaces.

Samples:

MD5	Package Name	Detection
3170ea805a0f216c21c554bb576e75fb	it.cyprus.client	Android.Trojan.AndroRAT.B
695a9f7bb0d7ecb810fe8a3dbe90a173	it.cyprus.client	Android.Trojan.AndroRAT.B
6e83b72fcb0abf9e65a48d405f739e93	it.cyprus.client	Android.Trojan.AndroRAT.B
667452e44935325c2b20a3d7204efe3b	it.assistenzaumts.update	Android.Trojan.AndroRAT.B

83c90e931a1a9b249b2f9ce8bf5ecd0b	it.assistenzaumts.update	Android.Trojan.AndroRAT.ZA
88e8e4ff540fb881d1300f9759026904	it.assistenzaumts.update	Android.Trojan.AndroRAT.ZA

Note: This article is based on technical information provided courtesy of Bitdefender Researchers Alin Barbatei and Marius Mihai Tivadar, Team Leader â€“ Malware Research.

TAGS

industry news

AUTHOR

ding energy. That's what's been helping him work his everything off