Capturing and Detecting AndroidTester Remote Access Trojan with the Emergency VPN

civilsphereproject.org/blog/2021/9/21/capturing-and-detecting-androidtester-remote-access-trojan-with-the-emergency-vpn

Stratosphere IPS September 21, 2021

Mobile remote access trojans, or RATs, are malicious programs that allow attackers to fully control a mobile device. What does this mean in reality? The person controlling the malware will be able to access information on the phone, including SMS, pictures and messaging applications, and also be able to steal or implant files on the phone. RATs are precision tools used to track and gather information about a person.

In this blog post, we show how the Emergency VPN can help identify RAT infections on Android phones. The images and network traffic included in this blog post are part of the original research by Civilsphere researcher Kamila Babayeva on the Android Mischief Dataset [1].

Android Tester Remote Access Trojan

AndroidTester is a RAT for Android that has been around since approximately 2020, and it is believed to be a variation of another RAT known as SpyNote. Among its functionalities, the RAT can access files, SMS messages, calls, contacts, locations, accounts, applications, and allows access to the shell, microphone, camera, keylogs, settings, and other functionalities. This functionality is shown in Figure 1 and 2.

Once the phone is infected with the RAT, the attacker has complete access to the phone. As we can see in the screenshots below, the RAT can list all the files and all the installed applications, among other things.

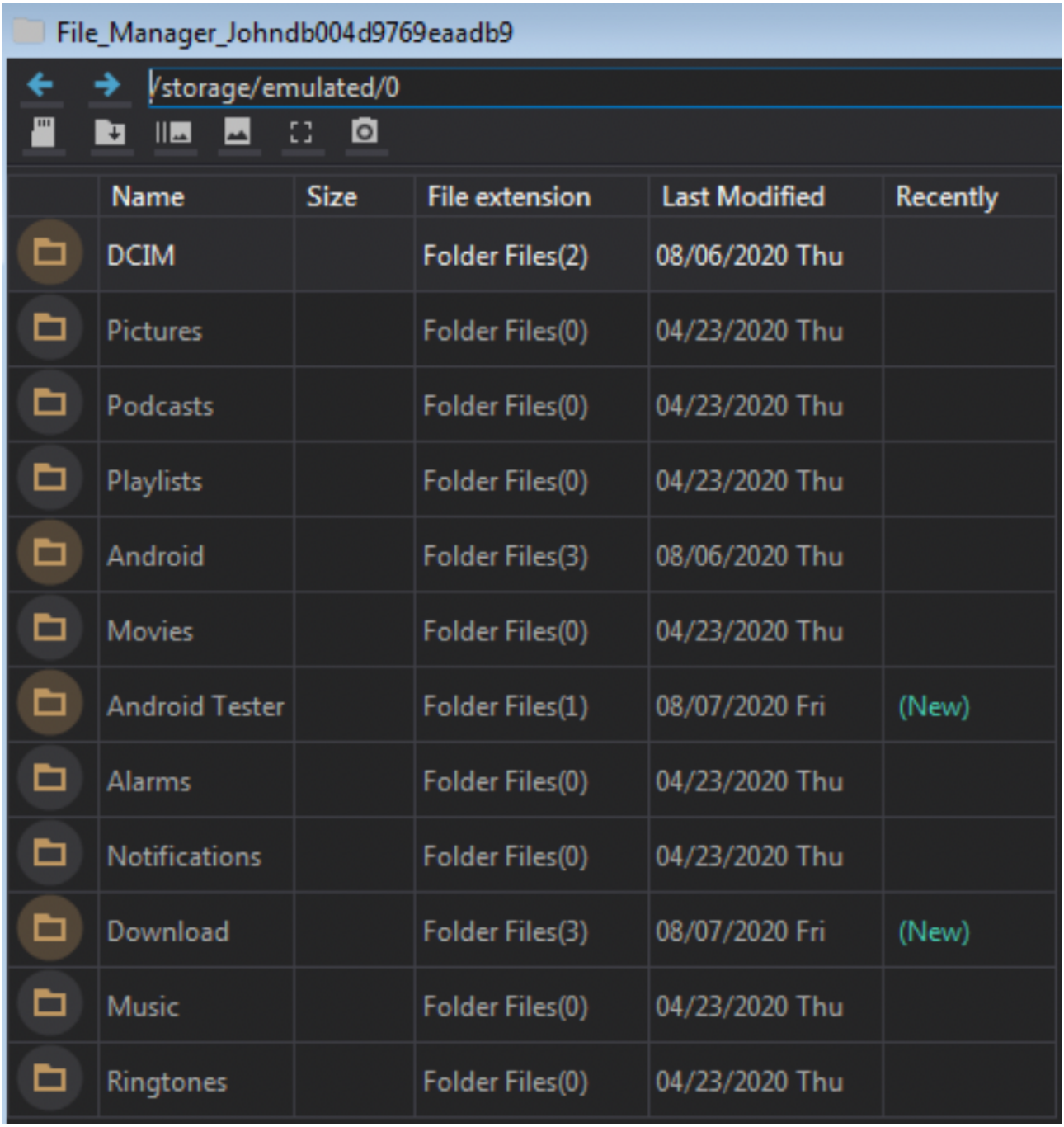
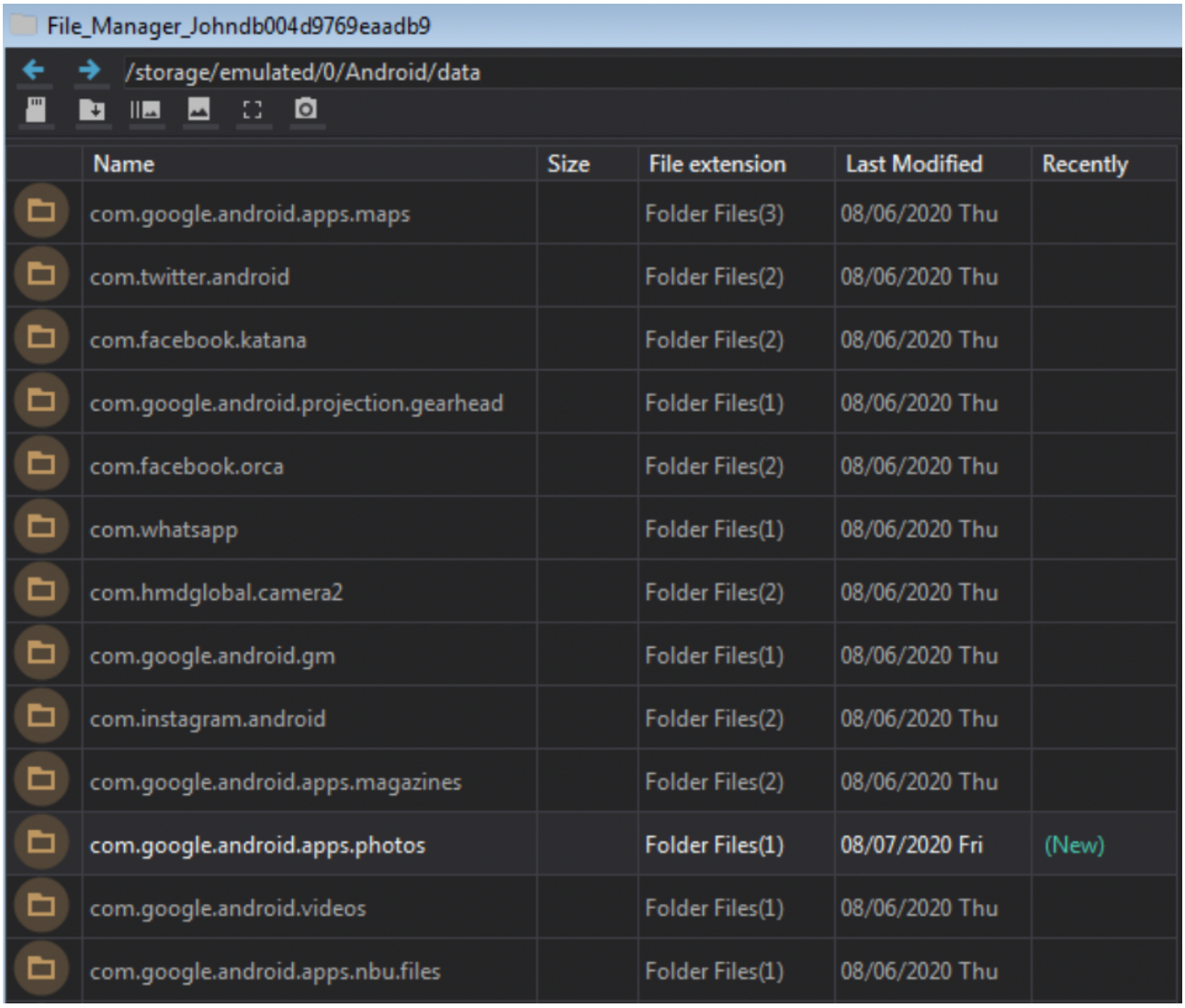


Figure 1 - AndroidTester can list the entire content of the phone SD card, including downloads, applications, movies, configurations, and pictures [4].



Name	Size	File extension	Last Modified	Recently
com.google.android.apps.maps		Folder Files(3)	08/06/2020 Thu	
com.twitter.android		Folder Files(2)	08/06/2020 Thu	
com.facebook.katana		Folder Files(2)	08/06/2020 Thu	
com.google.android.projection.gearhead		Folder Files(1)	08/06/2020 Thu	
com.facebook.orca		Folder Files(2)	08/06/2020 Thu	
com.whatsapp		Folder Files(1)	08/06/2020 Thu	
com.hmdglobal.camera2		Folder Files(2)	08/06/2020 Thu	
com.google.android.gm		Folder Files(1)	08/06/2020 Thu	
com.instagram.android		Folder Files(2)	08/06/2020 Thu	
com.google.android.apps.magazines		Folder Files(2)	08/06/2020 Thu	
com.google.android.apps.photos		Folder Files(1)	08/07/2020 Fri	(New)
com.google.android.videos		Folder Files(1)	08/06/2020 Thu	
com.google.android.apps.nbu.files		Folder Files(1)	08/06/2020 Thu	

Figure 2 - AndroidTester can list the applications installed on the device [5].

Capturing the Android Tester RAT with the Emergency VPN

The Emergency VPN is a service that provides a free security assessment of a phone's network traffic to determine if the device is infected, under attack, or compromised. The Emergency VPN works like any other VPN, with the addition that once you connect to the Emergency VPN, our team will capture the network traffic generated by the device in order to analyse it and find potential security threats. The high level workflow of the Emergency VPN is shown in Figure 3.

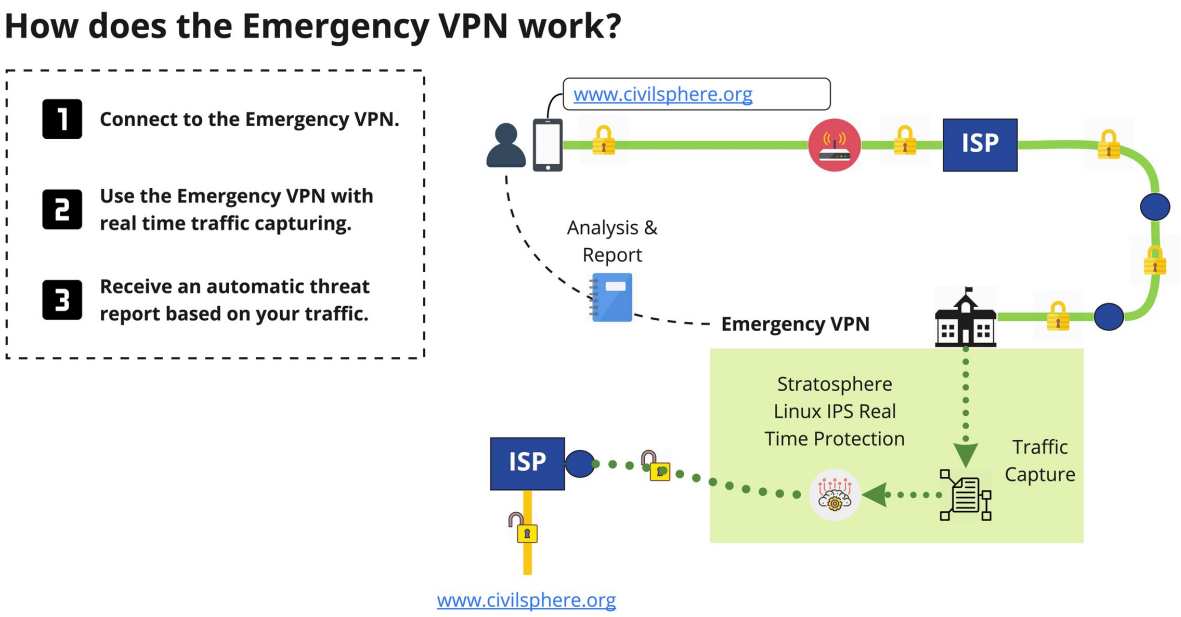


Figure 3 - The Emergency VPN allows users to safely browse the Internet while providing a security assessment of the network traffic to identify potential threats.

To capture the behavior of the AndroidTester RAT, we connected a Nokia Phone with Android 10 to our Emergency VPN and then infected the device with AndroidTester v.6.4.6. The Nokia Phone was remotely controlled like a real attacker would do, stealing information, adding and deleting contacts, and locating the device.

During all this time, the Emergency VPN was active and the network connections through the VPN were captured and then analysed by our analysts to identify if there were malicious connections identified or not.

Detecting the AndroidTester RAT with the Emergency VPN

The Emergency VPN captures and stores the network traffic in a PCAP file. This file contains all the network connections the device did using the VPN and it is the primary source for analysis that our researchers use to find malware infections.

In this session, the Emergency VPN was used for 1.2 hours resulting in 80MB of network traffic captured. With this data, we proceed to perform our analysis.

In this investigation, we focused on three things to detect the malware infection:

1. **Unusual data upload:** is the device uploading (a lot of) data to unusual services?
2. **Periodic connections:** are there network connections that appear not to be human?
3. **Data leaks: is there any personal information being leaked on the network?**

The first thing we usually look at are usual data uploads. Most users are data consumers, generally downloading more data than they send. This quick analysis highlighted one suspicious connection to a server not associated with any well-known service, where the device uploaded 43MB as it can be seen below:

Service	Origin	<->	Destination	Download	Upload	Total Transferred
Unknown	10.8.0.61	<->	147.32.83.234	780kB	43MB	44MB
Facebook	10.8.0.61	<->	157.240.30.27	19MB	128kB	19MB
Instagram	10.8.0.61	<->	157.240.30.63	1,680kB	566kB	2,247kB
Google Video	10.8.0.61	<->	195.113.214.206	2,030kB	44kB	2,075kB
Google	10.8.0.61	<->	216.58.201.110	1,623kB	84kB	1,708kB

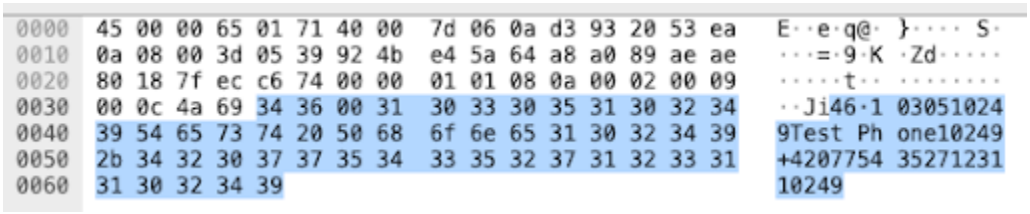
This connection is suspicious because the service is not known, the device uploads 43MB of data, but also, because compared to the other activities in the device this is an outlier. However suspicious, this alone is not enough to classify this connection as malicious and we investigate further.

Now that we have a connection that we consider suspicious, we analyse it to determine if this connection may have been generated by a human or a program. When humans browse the internet or use applications, we rarely do it in a periodic and automated fashion. Computers on the other hand, they do.

The Stratosphere Linux IPS is a network analysis tool that allows to quickly analyse if a connection is periodic. As shown below, the connection to this server is periodic, does not have an associated DNS name, and the data transfer occurs over a non-standard port (1337).

All of these individual findings show us that this connection appears more and more suspicious. We can examine the content of the connection and, if the traffic is not encrypted, we can see if there is anything else pointing out if this connection is malicious.

Upon examination, we find the attacker command and the device response sending the mobile phone number and name over the network:



With all the information gathered, our researchers will use existing Threat intelligence and their advanced knowledge on traffic analysis to try to associate the traffic with a specific malware family whenever possible to facilitate the risk assessment and remediation steps taken by users.

The Emergency VPN report for this device is available here. A technical in-depth analysis of AndroidTester network traffic is available in the Stratosphere Blog [6].

How to Avoid Getting Infected by RATs

These are our recommendations to stay safe:

- Install new apps only from the Google Play Store and trusted developers.
- The Google Play Protect is enabled by default, keep it enabled at all times.
- Click only on links sent by people you know and trust. When in doubt, do not click.
- Download and open attachments sent only by known and trusted contacts. When in doubt, do not download and do not open.
- Keep only the essential applications installed on the phone for maximum safety.
- Never leave your phone unattended or unlocked, even in trusted spaces.
- Never share your phone PIN or Pattern, even with loved ones.

Remember that you can use the service ShouldIClick to check links before clicking, and see its content without visiting the site directly on your phone. Get started using the Emergency VPN.

Should I Click?

Emergency VPN

References

[1] Execution, Analysis and Detection of Android RATs traffic, Civilsphere, https://www.civilsphereproject.org/research/execution-analysis-and-detection-of-android-rats-traffic. Accessed on 07/15/2021.

[2] A Study of Remote Access Trojans: This repository contains a curated list of papers, articles and other sources related to remote access trojans, GitHub, https://github.com/stratosphereips/a-study-of-remote-access-trojans. Accessed on 07/15/2021.

[3] ANDROID TESTER V6.4.6 (RAT) Cracked + Source, BlackHatRussia Web Archive, https://web.archive.org/web/20210705135241/https://www.blackhatrussia.com/1424-android-tester-v646-rat-cracked-source.html. Accessed on 07/15/2021.

[4] Screenshot from 2020-08-07 11-04-04.png, RAT01_AndroidTester, AndroidMischiefDataset_v2, https://mcfp.felk.cvut.cz/publicDatasets/Android-Mischief-Dataset/AndroidMischiefDataset_v2/RAT01_AndroidTester/RAT01_AndroidTester_screenshots/Screenshot%20from%202020-08-07%2011-04-04.png. Accessed on 07/15/2021.

[5] Screenshot from 2020-08-07 11-10-13.png, RAT01_AndroidTester, AndroidMischiefDataset_v2, https://mcfp.felk.cvut.cz/publicDatasets/Android-Mischief-Dataset/AndroidMischiefDataset_v2/RAT01_AndroidTester/RAT01_AndroidTester_screenshots/Screenshot%20from%202020-08-07%2011-10-13.png. Accessed on 07/15/2021.

[6] Dissecting a RAT. Android Tester Trojan Analysis and Decoding, Stratosphere IPS, https://www.stratosphereips.org/blog/2020/12/14/ngwqj0h060yv40w1afp51fg7wo9ijy-pzlhk. Accessed on 07/15/2021.