CONFIDENTIAL

EMERGENCY VPN REPORT

Summary

In this session of the Emergency VPN we found the device is infected with a type of malware known as Remote Access Trojan (RAT). This type of malware is used to extract information from the device, including pictures, messages, documents, and more. The information on the device should be considered fully compromised. We recommend an immediate factory reset of the device and repeating this assessment to ensure the malicious behavior is no longer present.

Level	Description	Explanation
Critical	Malware Infection - Possible RAT (Server 147.32.83.234)	The device is infected with malware that is stealing information from the device. Given the behavior observed, our analysts believe this could be a Remote Access Trojan (RAT) infection. At this moment we are unable to identify the exact malware family, however, we suspect it's a variant of the SpyNote RAT. The information on the device should be considered fully compromised. We recommend an immediate factory reset of the mobile device and repeating this assessment to ensure the malicious behavior is no longer present.
Informative	Information Leaked Via Insecure HTTP Requests	The mobile device is communicating without encryption (plain HTTP) with several websites. These insecure connections leak information about the user increasing the security risk of the user. We recommend uninstalling all applications that are not strictly necessary. Use a VPN when using public and not trusted networks.
Informative	Advertisement Trackers	We identified that the mobile device communicates with 13 different advertisement tracker servers. Advertisement trackers collect huge amounts of user data to re-sell. We recommend minimizing the number of applications showing advertisements on the phone, as well as using a privacy blocker browser that will reduce the number of advertisements shown when browsing the web.

Packet Capture Information

```
File name:           RAT01_AndroidTester.pcap
Number of packets:   89k
File size:           80MB
Data size:           79MB
Capture duration:    5179.260040 seconds
First packet time:   2020-08-07 10:49:24.509987
Last packet time:    2020-08-07 12:15:43.770027
Average packet size: 884.05 bytes
SHA256:              af22b503852390d914d0581e6f4cc1ebeb03203c7005464438a4708c22c59045
```

Data Uploads Summary

Malicious applications usually steal data (photos, messages, files, voice recordings) from the device. The stolen data is uploaded to malicious servers. Recognizing which services the device is sending data to is important to identify possible malicious activity.

These are the top 5 IP addresses where the mobile device uploaded data. If you do not recognize any of these services, we recommend factory resetting the device to remove any suspicious activity.

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

Top DNS Requests Resolved

In this session the following domain names were resolved:

```
1  infinitedata-pa.googleapis.com.
```

Detailed Findings

Malware Infection - Possible RAT (Server 147.32.83.234)

RISK LEVEL: CRITICAL

The device is infected with malware that is stealing information from the device. Given the behavior observed, our analysts believe this could be a Remote Access Trojan (RAT) infection. At this moment we are unable to identify the exact malware family, however, we suspect it's a variant of the SpyNote RAT[1]. The information on the device should be considered fully compromised. We recommend an immediate factory reset of the mobile device and repeating this assessment to ensure the malicious behavior is no longer present.

The analysis shows that the attacker requested the following data, which then the device sent back encoded:

- content://sms/
    - content://sms/sent
    - content://sms/queued
    - content://sms/outbox
    - content://sms/inbox
- com.instagram.android
- config07-08-2020.log
- config07-08-2020.log
- cat /proc/version
- com.instagram.android
- /storage/emulated/
- /storage/emulated/0/Pictures
- /storage/emulated/0/Pictures/Screenshots
- /storage/emulated/0/Download
- /storage/emulated/0/DCIM
    - /storage/emulated/0/DCIM/Camera
        - VID_20200806_190033.mp4
        - IMG_20200806_190030.jpg
- /storage/emulated/0/Android
    - /storage/emulated/0/Android/data
        - /storage/emulated/0/Android/data/com.google.android.apps.photos
- GetExternalStorage

[1] An in-depth analysis of SpyNote remote access trojan, BullDogJob Blog, https://bulldogjob.pl/articles/1200-an-in-depth-analysis-of-spynote-remote-access-trojan. Accessed on 07/16/2021.

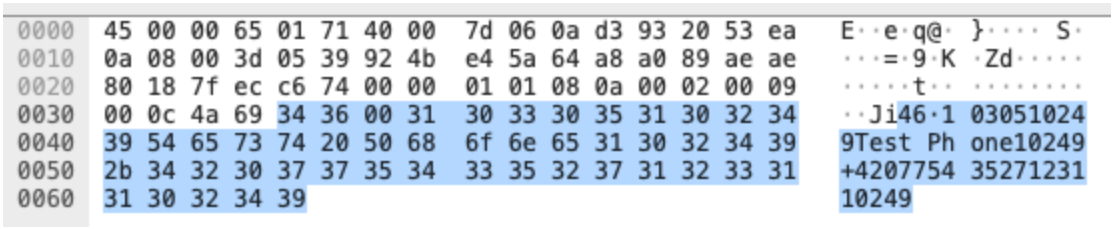
The first suspicious activity was an unusual data upload to a server not associated with any well-known service, as can be seen below:

Service	Origin	<->	Destination	Download	Upload	Total Transferred
Unknown	10.8.0.61	<->	147.32.83.234	780kB	43MB	44MB

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):

key	string	dns_resolution
147.32.83.234:1337:tcp	99+I+i.h*Y,h,h,h,h,h,i.	
172.217.23.234:443:udp	9	

Example of the attacker commands sent to the device:



```
0000  45 00 00 65 01 71 40 00  7d 06 0a d3 93 20 53 ea   E··e·q@· }···· S·
0010  0a 08 00 3d 05 39 92 4b  e4 5a 64 a8 a0 89 ae ae   ···=·9·K ·Zd·····
0020  80 18 7f ec c6 74 00 00  01 01 08 0a 00 02 00 09   ·····t·· ········
0030  00 0c 4a 69 34 36 00 31  30 33 30 35 31 30 32 34   ··Ji46·1 03051024
0040  39 54 65 73 74 20 50 68  6f 6e 65 31 30 32 34 39   9Test Ph one10249
0050  2b 34 32 30 37 37 35 34  33 35 32 37 31 32 33 31   +4207754 35271231
0060  31 30 32 34 39                                     10249
```

Information Leaked Via Insecure HTTP Requests

RISK LEVEL: INFORMATIVE

The mobile device is communicating without encryption (plain HTTP) with several websites. These insecure connections leak information about the user increasing the security risk of the user. We recommend uninstalling all applications that are not strictly necessary. Use a VPN when using public and not trusted networks.

Each connection sent from the mobile device that is not encrypted (uses HTTP instead of HTTPS), transfers information that potentially anyone with access to the device traffic can see without major effort. Who can access the traffic? This is illustrated by the Electronic Frontier Foundation at https://www.eff.org/pages/tor-and-https. People that share your WiFi, internet service providers, mobile cellular networks, and others. For maximum privacy, all connections from the phone should be encrypted.

The list of websites visited using HTTP are listed below:

- google.com

- msftconnecttest.com

Every HTTP connection has many pieces of data, among them the User-Agent. User-Agents identify the device and application so the content is properly shown on the mobile phone. We automatically analyze the User-Agents observed in the insecure connections listed above and extract information about the application and phone:

- Dalvik/2.1.0 (Linux; U; Android 10; Nokia 6.1 Build/QKQ1.190828.002)
    - Information extracted: Nokia 6.1 / Android 10 / Other

Advertisement Trackers

RISK LEVEL: INFORMATIVE

We identified that the mobile device communicates with 13 different advertisement tracker servers. Advertisement trackers collect huge amounts of user data to re-sell. We recommend minimizing the number of applications showing advertisements on the phone, as well as using a privacy blocker browser that will reduce the number of advertisements shown when browsing the web.

The following list shows the list of trackers servers the phone attempted to contact via DNS requests:

- `ads1.msn.com`
- `app-measurement.com`
- `connect.facebook.net`
- `doubleclick.net`
- `.facebook.com`
- `facebook.com`
- `g.doubleclick.net`
- `googleads.g.doubleclick.net`
- `.google.com`
- `graph.facebook.com`
- `graph.instagram.com`
- `static.xx.fbcdn.net`
- `t.co`