



# **Kaymera Mobile Security Suite. 2020 Penetration Tests Summary**



# Table of Contents

<b>Reference Context &amp; Objectives</b>	<b>4</b>
Executive Summary	4
<b>Cyber Threat Landscape Analysis</b>	<b>5</b>
Points of Attack identification	5
<b>Penetration Test from Internet on Kaymera infrastructure</b>	<b>6</b>
Scope	6
Point of Attack	6
Methodology	6
Tools	7
Intelligence Gathering	7
Service Discovery	13
Vulnerability Analysis & Exploitation	14
HTTP/HTTPS service attack	14
SIP service attack	15
TURN service attack	16
SSL service attack	19
<b>Penetration Test on mobile device</b>	<b>23</b>
Scope	23
Point of Attack	23
Methodology	24
Support Instruments	24
USB analysis	24
File transfer	24
Android Debug Bridge (ADB)	25
Rooting Procedure Analysis	28
Communication Analysis	29
NFC analysis	35
File transfer	35
WiFi analysis	36
Untrusted AP access	36
Fake AP	38
Man-in-the-Middle with SSL Splitting	38



Man-in-the-Middle with ARP Spoofing	39
Man-in-the-Middle with Malicious SSL Proxy	40
Panic Mode Analysis	41
<b>Penetration Test from Client's network on Kaymera infrastructure</b>	<b>46</b>
Scope	46
Point of Attack	46
Methodology	47
Tools	47
Service Discovery	47
Attacks detection Analysis and Management Controller Overview	51
<b>App Installation &amp; Execution Analysis</b>	<b>57</b>
Scope	57
Point of Attack	57
Methodology	57
Tools	57
Installed app analysis	57
Security measures bypass	60
App removal	60
App download from alternative sources	60
Whitelisted app installation from Google Store	64
Whitelisted app installation from alternative sources	64
Non-whitelisted app installation from Google Store	68
Non-whitelisted app installation from alternative sources	68
Google Play Store interception	69
Vulnerabilities	70



## Reference Context & Objectives

**Objective** of this initiative is to perform a security assessment of Kaymera Mobile Security Solution to verify the security baseline of supporting infrastructure and identify targeted security mitigations both on mobile devices and infrastructure.

The **aim** of this document is to describe activities performed during multiple penetration tests by different organizations, and design possible mitigations to implement to improve the security level of Kaymera Solution.

## Executive Summary

The assessment activity was using the following modes:

- Penetration Test from Internet on Kaymera infrastructure
- Penetration Test on mobile device
- Penetration Test from Tester's network on Kaymera infrastructure
- App Installation & Execution Analysis

Efforts were placed on the identification and exploitation of security weaknesses that could allow a remote attacker to gain unauthorized access to organizational data.

No faults were found with network devices or configuration, and host operating systems and services were found to be well patched and configured. There were no vulnerabilities found that could be rated as critical.

The activity was divided in different phases:

- **Cyber Threat Landscape:** Analysis of the solution, hardware and software specs, features, input/output communications. This activity led to identification of Point of Attacks for target solution.
- **Penetration Test from Client's network on Kaymera infrastructure:** Evaluation of security exposure on infrastructure from Intranet.
- **Penetration Test on mobile device:** Evaluation of security exposure on Kaymera device.
- **Penetration Test from Internet on Kaymera infrastructure:** Evaluation of security exposure on infrastructure from Internet.
- **App Installation & Execution Analysis:** Identification of methodology to bypass whitelist/blacklist measures to install malicious apps.
- **Remediation Plan:** Definition of a Remediation Plan to address possible mitigations identified during the analysis



## Cyber Threat Landscape Analysis

Cyber Threat Landscape analysis was performed on target solution through the following phases:

- **Functional and behavioral analysis:** includes identification and evaluation of hardware and software specs and device features through legit interactions.
- **Physical interaction analysis:** includes identification and evaluation of hardware components to directly or indirectly interact, such as USB ports, serial connectors, debug ports or touch-screen.
- **Communication flows analysis:** includes identification and evaluation of input/output communication flows. Specifically, it includes Wi-Fi, LTE, Bluetooth and NFC. LTE channel analysis was not considered because of legal issues related to the assets required to perform the activity.

Based on obtained information, it has been identified a list of possible Points of Attack which have been leveraged in the attempt to perform a valuable exploit on target solution.

### Points of Attack identification

Using the information obtained from previous analysis, the following Points of Attack have been identified:

- **Public Infrastructure:** this Point of Attack does not require any specific pre-requirement, because the infrastructure exposed on the Internet is public by definition.
- **Client's Infrastructure:** this Point of Attack requires the attacker to be inside Client's network.
- **Physical device:** this Point of Attack requires proximity to the mobile device or physical access for the attacker.

From this Points of Attack, a list of activities has been identified to perform an assessment aiming to the identification of the overall level of vulnerability of the target system. Specifically:

- Penetration Test from Internet on Kaymera infrastructure
- Penetration Test on mobile device
- Penetration Test from Client's network on Kaymera infrastructure
- App Installation & Execution Analysis

The following describes the results of specified activities performed in the security assessment.



# Penetration Test from Internet on Kaymera infrastructure

The Penetration Test activity from the Internet on Kaymera infrastructure aims to identify exposed services, software versions, unsecure configurations and possible vulnerabilities.

## Scope

The activity scope includes the hosts exposed on the Internet by TEST and PRODUCTION environments.

### TEST ENVIRONMENT:

- IP 151.XX.XXX.XX (st-Client's-msk-kontroller.Client's.com)
- IP 151.XX.XXX.XX (st-Client's-msk-fs.Client's.com)
- IP 151.XX.XXX.XX (st-Client's-msk-vpn.Client's.com)
- 151.XX.XXX.XX (st-Client's-msk-ts.Client's.com)

### PRODUCTION ENVIRONMENT:

- 151.XX.XXX.XX (Client's-msk-kontroller.Client's.com)
- 151.XX.XXX.XX (Client's-msk-fs.Client's.com)
- 151.XX.XXX.XX (Client's-msk-vpn.Client's.com)
- 151.XX.XXX.XX (Client's-msk-ts.Client's.com)

## Point of Attack

All the activities were performed from the Internet using a Kali machine with source IP "52.XX.XX.XXX".

## Methodology

The methodology used for Penetration Test from Internet on the infrastructure was structured in the following phases:

1. **Intelligence Gathering:** detect and collect publicly available data related to Client's asset and individuals.
2. **Service Discovery:** identify services exposed from targets in scope.
3. **Vulnerability Analysis & Exploitation:** identify security issues on targets through direct/indirect interaction; these vulnerabilities were leveraged to execute Proof-of-Concepts of public/ad-hoc exploits which guarantee the repeatability of performed tests.
4. **Post Exploitation:** retrieve information (e.g. password, configurations, details) on compromised systems to be used for future attacks, gain higher privileges (i.e. privilege escalation) or perform lateral movement to attack other systems from exploited ones.



## Tools

In the following a non-exhaustive list of the tools used to perform the activity:

- Shodan
- Censys
- Tenable Nessus
- Burp Suite Professional
- Nmap
- TLSSled
- Metasploit Framework
- SipVicious
- Nikto

## Intelligence Gathering

The only public information identified for targets in scope are related to the following hosts: 151.XX.XXX.XX (st-Client's-msk-kontroller.Client's.com), 151.XX.XXX.XX (Client's-msk-kontroller.Client's.com). On these hosts, a “nginx” server (TCP/XXX) with untrusted certificate (CA.Client's.com) was detected.



### Public Information on 151.XX.XXX.XX

[Toggle screen reader support](#)

Find and replace



Find

7 of 59

Context:

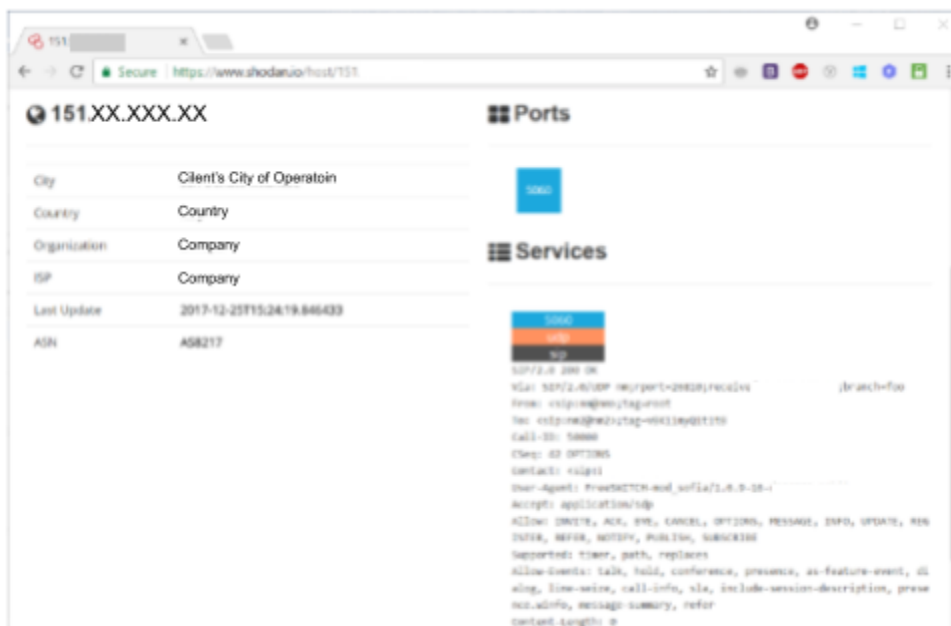
.Client's.com) an exposed SIP service (udp/XXX) wa



### Public Information on 151.XX.XXX.XX

On TEST host 151.XX.XXX.XX (st-Client's-msk-fs.Client's.com) an exposed SIP service (udp/XXX) was also detected. On the other hand, the PRODUCTION counterpart (151.XX.XXX.XX/Client's-msk-fs.Client's.com) does not seem to expose this service.



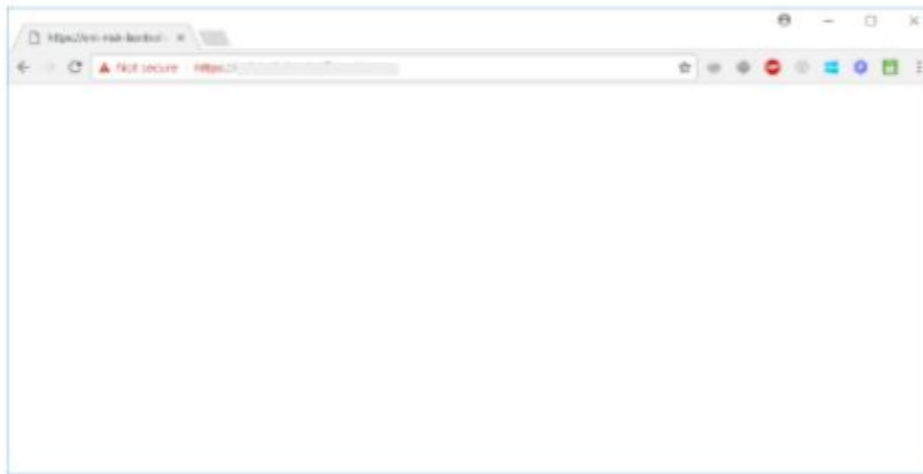


**Public Information on 151.XX.XXX.XX**

Both using DNS names or IPs, it is not possible to access or browse on web applications exposed from hosts st-Client's-msk-kontroller.Client's.com and Client's-msk-kontroller.Client's.com on port TCP/XXX. Even in this case, the certificate could not be trusted because it was released by an unknown CA (CA.Client's.com).

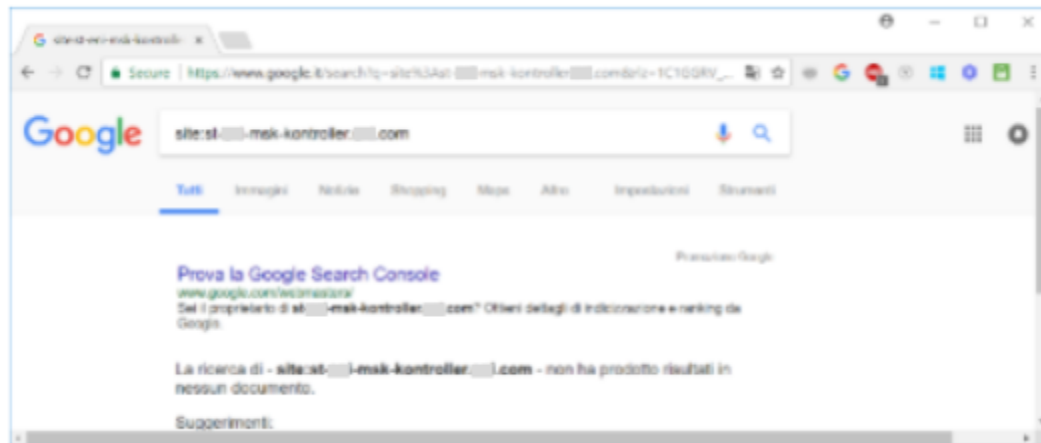


**Client's-msk-kontroller.Client's.com Web Application**

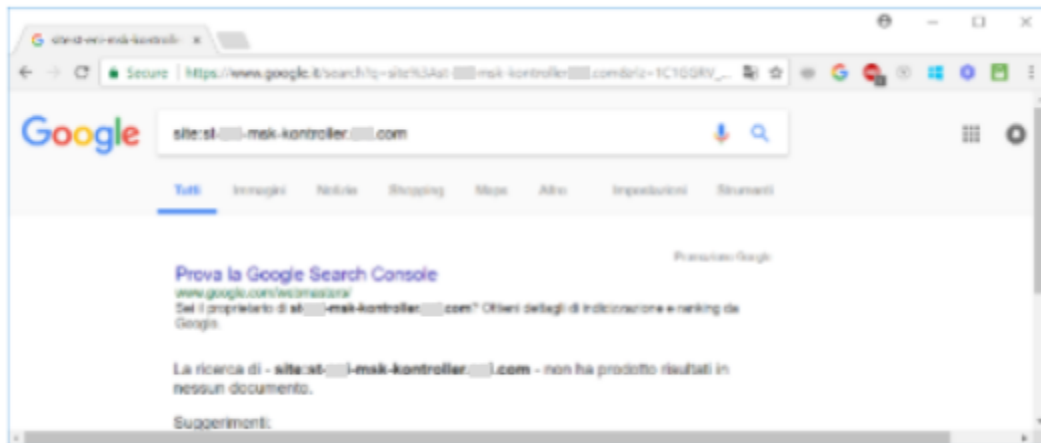


### st-Client's-msk-kontroller.Client's.com Web Application

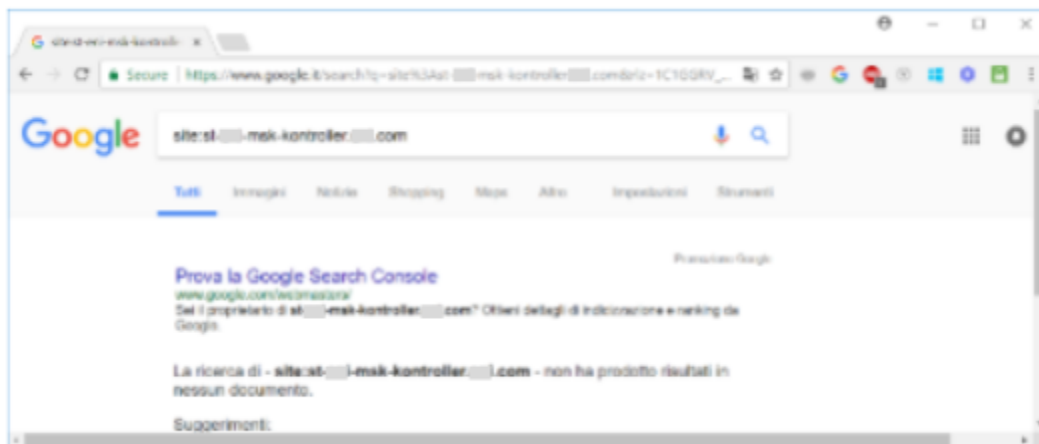
No pages indexed by Google were detected for TEST and PRODUCTION hostnames.



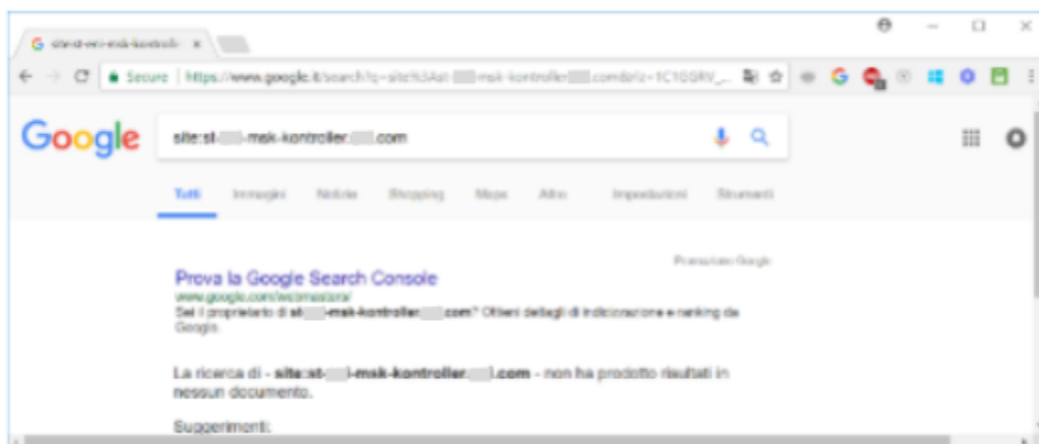
### st-Client's-msk-kontroller.Client's.com Google results



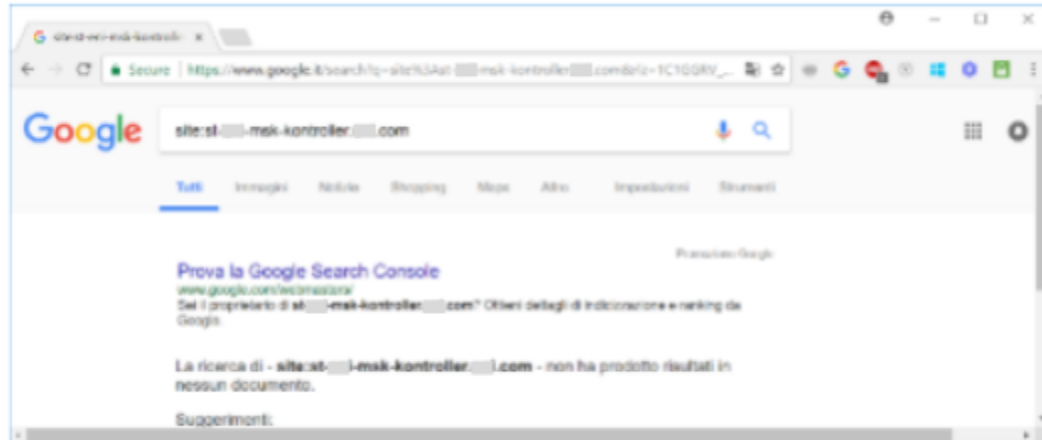
**st-Client's-msk-fs.Client's.com Google results**



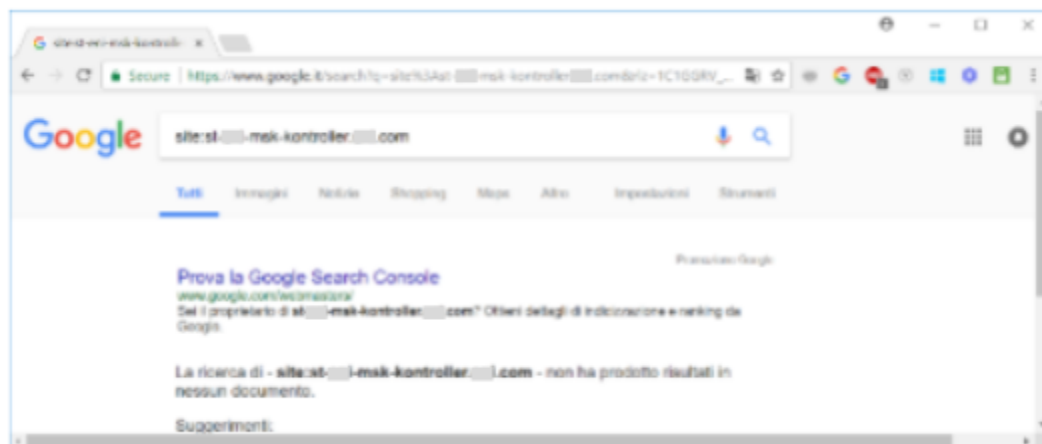
**st-Client's-msk-vpn.Client's.com Google results**



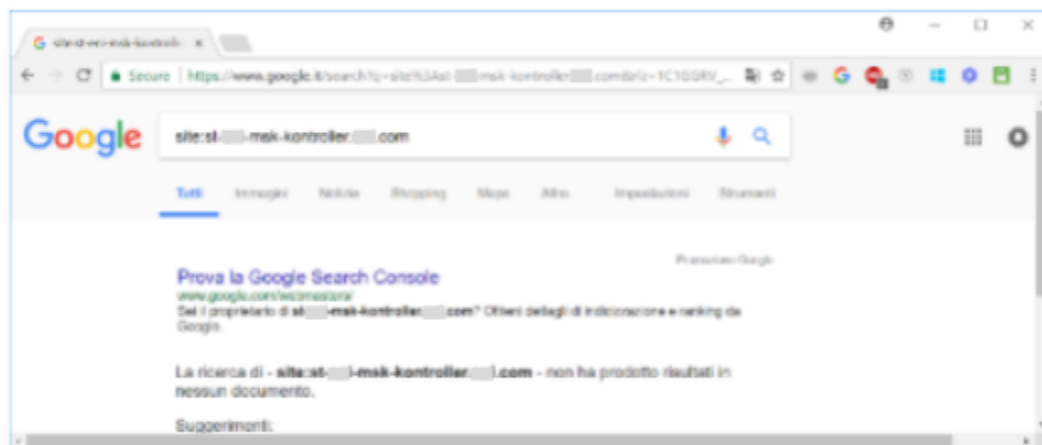
**st-Client's-msk-ts.Client's.com Google results**



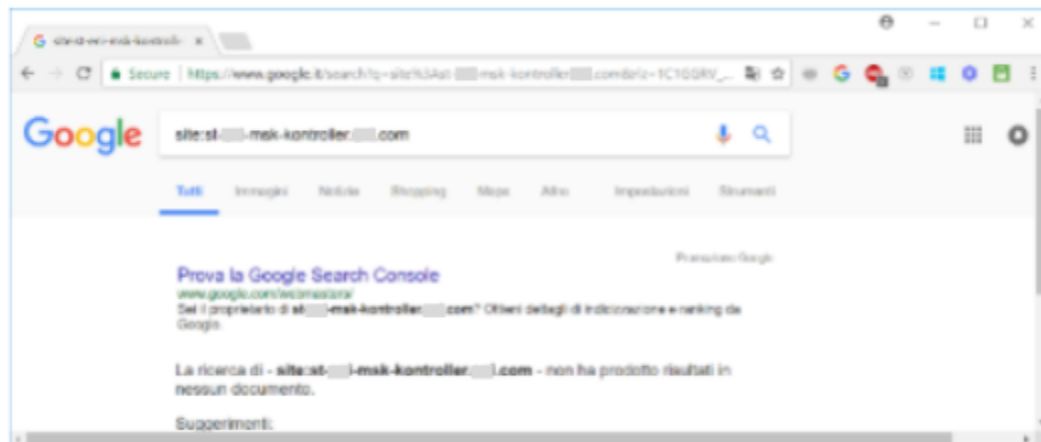
**Client's-msk-kontroller.Client's.com Google results**



**Client's-msk-fs.Client's.com Google results**



**Client's-msk-vpn.Client's.com Google results**



**Client's-msk-ts.Client's.com Google results**

## Service Discovery

Active port analysis on target hosts identified multiple exposed services:

IP/HOSTNAME	PORT	SERVICE
151.XX.XXX.XX/st-Client's-msk-kontroller.Client's.com	TCP/XX X	HTTPS
151.XX.XXX.XX/st-Client's-msk-fs.Client's.com	udp/XX X	SIP
151.XX.XXX.XX/st-Client's-msk-fs.Client's.com	TCP/XX XX	SSL (commonName=st-Client's-msk-fs.Client's.com)
151.XX.XXX.XX/st-Client's-msk-fs.Client's.com	TCP/XX XX	sip-proxy, FreeSWITCH mod_sofia 1.6.9-16-d574870~64bit
151.XX.XXX.XX/st-Client's-msk-fs.Client's.com	TCP/XX XX	SSL (commonName=st-Client's-msk-fs.Client's.com)
151.96.248.53/st-Client's-msk-vpn.Client's.com	TCP/XX XX	OpenVPN
151.XX.XXX.XX/st-Client's-msk-ts.Client's.com	TCP/XX XX	Coturn TURN server
151.XX.XXX.XX/Client's-msk-kontroller.Client's.com	TCP/XX X	HTTPS
151.XX.XXX.XX/Client's-msk-fs.Client's.com	udp/XX X	SIP
151.XX.XXX.XX/Client's-msk-fs.Client's.com	TCP/XX XX	SSL (commonName=Client's-msk-fs.Client's.com)
151.XX.XXX.XX/Client's-msk-fs.Client's.com	TCP/XX XX	sip-proxy, FreeSWITCH mod_sofia 1.6.9-16-d574870~64bit



151.XX.XXX.XX/Client's-msk-fs.Client's.com	TCP/XX XX	SSL (commonName=Client's-msk-fs.Client's.com)
151.XX.XXX.XX/Client's-msk-vpn.Client's.com	TCP/XX XX	OpenVPN
151.XX.XXX.XX/Client's-msk-ts.Client's.com	TCP/XX XX	Coturn TURN server

**Table 1: Exposed services from Internet**

## Vulnerability Analysis & Exploitation

Based on exposed services, different types of analysis were performed to identify possible issues, wrong configurations and vulnerabilities.

### HTTP/HTTPS service attack

Both on TEST (151.XX.XXX.XX/st-Client's-msk-kontroller.Client's.com) and PRODUCTION (151.XX.XXX.XX/Client's-msk-kontroller.Client's.com) environment was detected a "Nginx" web server on port TCP/XXX.

A brute force attack was executed to identify directories, known files and publicly available admin pages. No relevant results have been obtained by the activity.

```
Terminal - root@kali: ~
root@kali: ~
root@kali:~# nikto -host st-151.151.151.151.com -ssl -p 443
- Nikto v2.1.6
-----
+ Target IP: 151.151.151.151
+ Target Hostname: st-eni-msk-kontroller.eni.com
+ Target Port: 443
-----
+ SSL Info: Subject: /CN=st-eni-msk-kontroller.eni.com
Ciphers: ECDHE-RSA-AES256-GCM-SHA384
Issuer: /CN=CA.eni.com
+ Start Time: 2018-01-06 11:13:40 (GMT1)
-----
+ Server: nginx
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

**Web Server analysis on st-Client's-msk-kontroller.Client's.com**



```
Terminal - root@kali: ~
root@kali: ~
root@kali:~# nikto -host st-eni-msk-kontroller.eni.com -ssl -p 443
- Nikto v2.1.6
-----
+ Target IP: 151.100.100.100
+ Target Hostname: st-eni-msk-kontroller.eni.com
+ Target Port: 443
-----
+ SSL Info: Subject: /CN=st-eni-msk-kontroller.eni.com
           Ciphers: ECDHE-RSA-AES256-GCM-SHA384
           Issuer: /CN=CA.eni.com
+ Start Time: 2018-01-06 11:13:40 (GMT1)
-----
+ Server: nginx
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

**Web Server analysis on Client's-msk-kontroller.Client's.com**

## SIP service attack

Both on TEST (151.XX.XXX.XX/st-Client's-msk-fs.Client's.com) and PRODUCTION (151.XX.XXX.XX/Client's-msk-fs.Client's.com) environment a SIP server was detected with filtered port udp/XXX. Detected version on the TEST server is "FreeSWITCH mod\_sofia 1.6.9-16-d574870~64bit".

```
root@kali: ~/kaymera
File Edit View Search Terminal Help
root@kali:~/eni_kaymera# ssnmap 151.100.100.100
| SIP Device | User Agent | Fingerprint |
|-----|-----|-----|
| 151.100.100.100:5060 | FreeSWITCH-mod_sofia/1.6.9-16-d574870~64bit | disabled |
root@kali:~/eni_kaymera#
```

**FreeSwitch banner**

On both servers, a brute force attack was performed to identify existing SIP users. However no users were retrieved. In addition, on TEST server (151.XX.XXX.XX/st-Client's-msk-fs.Client's.com) the following active methods were detected: INVITE, ACK, BYE, CANCEL, OPTIONS, MESSAGE, INFO, UPDATE, REGISTER, REFER, NOTIFY, PUBLISH e SUBSCRIBE.



```
Terminal - root@kali: ~
File Edit View Terminal Tabs Help
PORT      STATE SERVICE
5060/udp  open  sip
| sip-brute:
|   Accounts: No valid accounts found
|   Statistics: Performed 2049 guesses in 602 seconds, average tps: 3.0
|_ sip-methods: INVITE, ACK, BYE, CANCEL, OPTIONS, MESSAGE, INFO, UPDATE, REGISTER, REFER, NOTIFY, PUBLISH, SUBSCRIBE
Nmap scan report for 151.XX.XXX.XX
Host is up.
PORT      STATE SERVICE
5060/udp  open|filtered sip
| sip-brute:
|   Accounts: No valid accounts found
|   Statistics: Performed 1415 guesses in 604 seconds, average tps: 2.1
Nmap done: 2 IP addresses (2 hosts up) scanned in 627.65 seconds
root@kali:~#
```

**SIP users brute force**

### TURN service attack

Both on TEST (151.XX.XXX.XX/st-Client's-msk-ts.Client's.com) and PRODUCTION (151.XX.XXX.XX/Client's-msk-ts.Client's.com) environment was detected by a TURN server web application. Detected version is "Coturn TURN server 4.X.X.X".

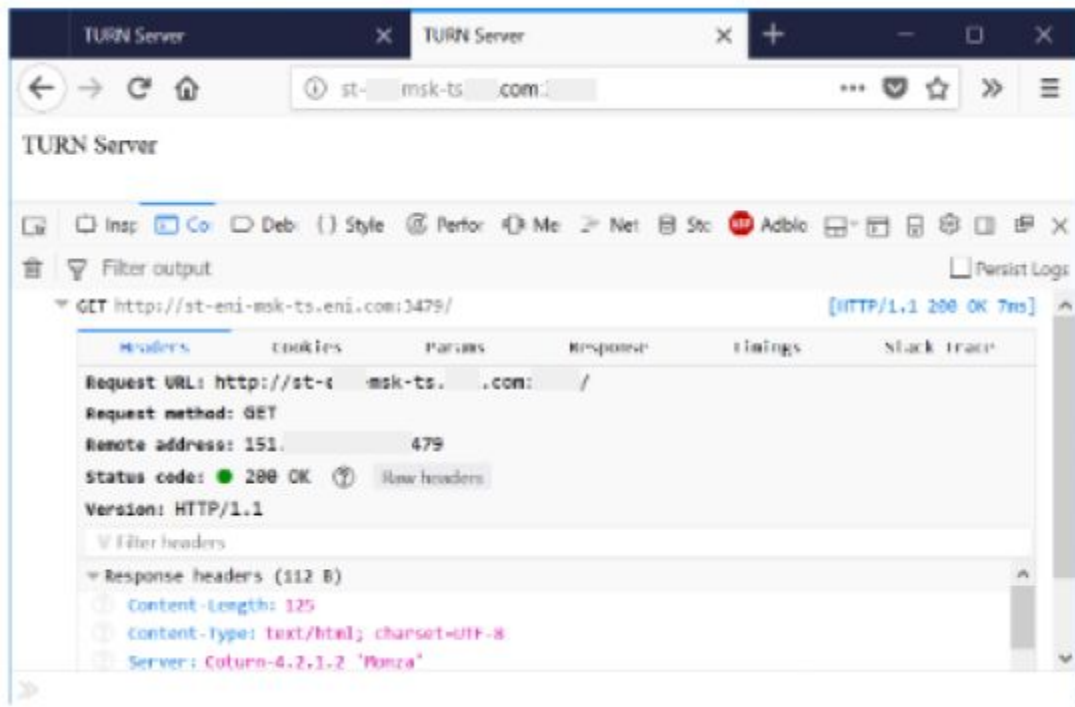


**TURN Server on host 151.XX.XXX.XX/st-Client's-msk-ts.Client's.com**

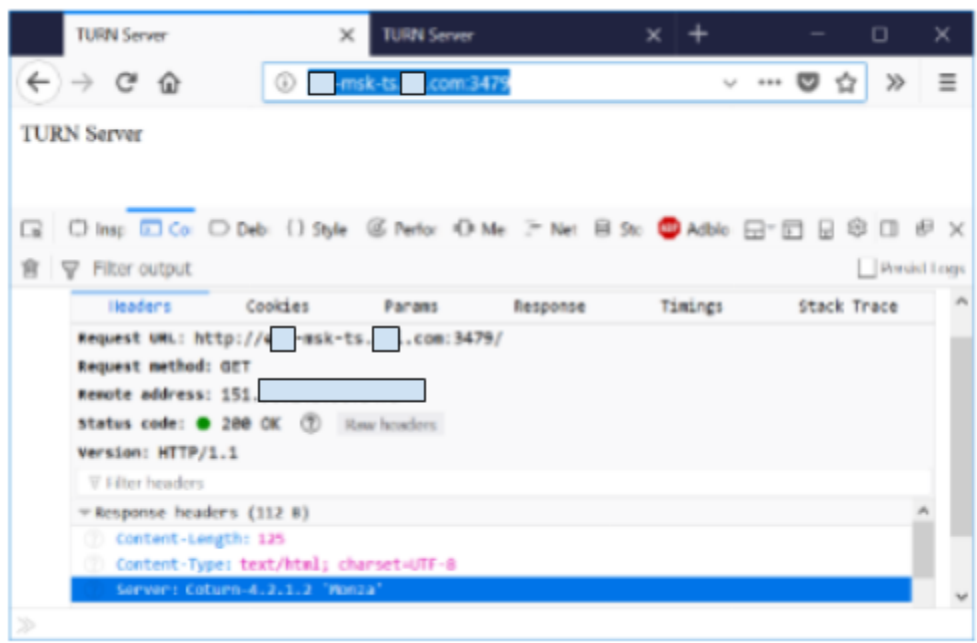


**TURN Server on host 151.XX.XXX.XX/Client's-msk-ts.Client's.com**





**Coturn 4.2.1.2 Banner**



**Coturn 4.2.1.2 Banner**



```
root@kali: ~/kaymera
File Edit View Search Terminal Tabs Help
root@kali: ~/kay.. x root@kali: ~/kay.. x root@kali: ~/kay.. x root@kali: ~/kay.. x
root@kali:~/kaymera# nikto -host st-client's-msk-ts-client's.com -p 3479
- Nikto v2.1.6
-----
+ Target IP: 151.101.1.1
+ Target Hostname: st-client's-msk-ts-client's.com
+ Target Port: 3479
+ Start Time: 2018-01-04 11:21:22 (GMT1)
-----
+ Server: Cofurn 4.2.1.2 'Manza'
+ IP address found in the 'server' header. The IP is '4.2.1.2'.
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 21 error(s) and 4 item(s) reported on remote host
+ End Time: 2018-01-04 11:29:12 (GMT1) (470 seconds)
-----
+ 1 host(s) tested
root@kali:~/kaymera#
```

**Info on 151.XX.XXX.XX/st-Client's-msk-ts.Client's.com**

```
root@kali: ~/kaymera
File Edit View Search Terminal Tabs Help
root@kali: ~/kay.. x root@kali: ~/kay.. x root@kali: ~/kay.. x root@kali: ~/kay.. x
root@kali:~/kaymera# nikto -host Client's-msk-ts.Client's.com -p 3479
- Nikto v2.1.6
-----
+ Target IP: 151.101.1.1
+ Target Hostname: Client's-msk-ts.Client's.com
+ Target Port: 3479
+ Start Time: 2018-01-04 11:20:33 (GMT1)
-----
+ Server: Cofurn 4.2.1.2 'Manza'
+ IP address found in the 'server' header. The IP is '4.2.1.2'.
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 21 error(s) and 4 item(s) reported on remote host
+ End Time: 2018-01-04 11:20:23 (GMT1) (470 seconds)
-----
+ 1 host(s) tested
root@kali:~/kaymera#
```

**Info on 151.XX.XXX.XX/Client's-msk-ts.Client's.com**



During the activities, although multiple test runs have been executed, some significant delay was detected in replies from the server which could have partially invalidated this test.

## SSL service attack

It was executed a drill-down analysis of SSL services exposed from the following servers: 151.XX.XXX.XX/st-Client's-msk-kontroller.Client's.com (TCP/XXX), 151.XX.XXX.XX/st-Client's-msk-fs.Client's.com (TCP/XXXX, TCP/XXXX), 151.XX.XXX.XX/Client's-msk-kontroller.Client's.com (TCP/XXX), 151.XX.XXX.XX/Client's-msk-fs.Client's.com (TCP/XXXX, TCP/XXXX).

On 151.XX.XXX.XX/st-Client's-msk-kontroller.Client's.com (TCP/XXX), 151.XX.XXX.XX/st-Client's-msk-fs.Client's.com (TCP/XXXX), 151.XX.XXX.XX/Client's-msk-kontroller.Client's.com (TCP/XXX) and 151.XX.XXX.XX/Client's-msk-fs.Client's.com (TCP/XXXX) hosts no unsecure cipher or deprecated hash mechanisms were detected.

```
root@kali:~# tlsxlied st-Client's-msk-kontroller.Client's.com 443
-----
TlSSlied - (1.3) based on sslls and openssl
  by Raul Siles (www.taddong.com)
-----
openssl version: OpenSSL 1.1.0f - 25 May 2017
-----
Date: 20180106-111411
-----
[*] Analyzing SSL/TLS on st-Client's-msk-kontroller.Client's.com:443 ...
  [-] Output directory: TlSSlied 1.3 st-Client's-msk-kontroller.Client's.com 443 20180106-111411 ...
[*] Checking if the target service speaks SSL/TLS ...
  [-] The target service st-Client's-msk-kontroller.Client's.com:443 seems to speak SSL/TLS ...
  [-] Using SSL/TLS protocol version:
      (empty means I'm using the default openssl protocol version(s))
[*] Running sslls on st-Client's-msk-kontroller.Client's.com:443 ...
  [-] Testing for SSLv2 ...
  [-] Testing for the NULL cipher ...
  [-] Testing for weak ciphers (based on key length - 40 or 56 bits) ...
```

**SSL analysis on st-Client's-msk-kontroller.Client's.com (port XXX)**



```
Terminal-root@kali: ~
File Edit View Terminal Tabs Help
root@kali:~$ tlsxsslied st-███-msk-fs.███.com 5072
-----
TLSSlied - (1.3) based on sslscan and openssl
by Raul Siles (www.taddong.com)
-----
openssl version: OpenSSL 1.1.0f 25 May 2017
-----
Date: 20180106 111449
-----
[*] Analyzing SSL/TLS on st-███-msk-fs.███.com:5072 ...
[-] Output directory: TLSSlied 1.3 st-███-msk-fs.███.com 5072 20180106 111449 ...
[*] Checking if the target service speaks SSL/TLS...
[-] The target service st-███-msk-fs.███.com:5072 seems to speak SSL/TLS...
[-] Using SSL/TLS protocol version:
    (empty means I'm using the default openssl protocol version(s))
[*] Running sslscan on st-███-msk-fs.███.com:5072 ...
[-] Testing for SSLv2 ...
[-] Testing for the NULL cipher ...
[-] Testing for weak ciphers (based on key length - 40 or 56 bits) ...
```

SSL analysis on st-Client's-msk-fs.Client's.com (port XXXX)

```
Terminal-root@kali: ~
File Edit View Terminal Tabs Help
root@kali:~$ tlsxsslied ███-msk-kontroller.███.com 443
-----
TLSSlied - (1.3) based on sslscan and openssl
by Raul Siles (www.taddong.com)
-----
openssl version: OpenSSL 1.1.0f 25 May 2017
-----
Date: 20180106 111422
-----
[*] Analyzing SSL/TLS on ███-msk-kontroller.███.com:443 ...
[-] Output directory: TLSSlied 1.3 ███-msk-kontroller.███.com 443 20180106 111422 ...
[*] Checking if the target service speaks SSL/TLS...
[-] The target service ███-msk-kontroller.███.com:443 seems to speak SSL/TLS...
[-] Using SSL/TLS protocol version:
    (empty means I'm using the default openssl protocol version(s))
[*] Running sslscan on ███-msk-kontroller.███.com:443 ...
[-] Testing for SSLv2 ...
[-] Testing for the NULL cipher ...
[-] Testing for weak ciphers (based on key length - 40 or 56 bits) ...
```

SSL analysis on Client's-msk-kontroller.Client's.com (port XXX)



```
Terminal - root@kali: -
root@kali:~# tlsxled [redacted]-msk-fs.[redacted].com 5072
-----
TISSled - (1.3) based on sslscan and openssl
by Raul Siles (www.toddong.com)
-----
openssl version: OpenSSL 1.1.0f  25 May 2017
-----
Date: 20180106 111459
-----
[*] Analyzing SSL/TLS on [redacted]-msk-fs.[redacted].com:5072 ...
  [-] Output directory: TISSled 1.3 out msk fs.oni.com 5072 20180106 111459 ...
[*] Checking if the target service speaks SSL/TLS...
  [-] The target service [redacted]-msk-fs.[redacted].com:5072 seems to speak SSL/TLS...
  [-] Using SSL/TLS protocol version:
      (empty means I'm using the default openssl protocol version(s))
[*] Running sslscan on [redacted]-msk-fs.[redacted].com:5072 ...
  [-] Testing for SSLv2 ...
  [-] Testing for the NULL cipher ...
  [-] Testing for weak ciphers (based on key length - 40 or 56 bits) ...
```

SSL analysis on st-Client's-msk-fs.Client's.com (port XXXX)

```
Terminal - root@kali: -
root@kali:~# tlsxled st-[redacted]-msk-fs.[redacted].com 5081
-----
TISSled - (1.3) based on sslscan and openssl
by Raul Siles (www.toddong.com)
-----
openssl version: OpenSSL 1.1.0f  25 May 2017
-----
Date: 20180106 111509
-----
[*] Analyzing SSL/TLS on st-[redacted]-msk-fs.[redacted].com:5081 ...
  [-] Output directory: TISSled 1.3 st oni msk fs.oni.com 5081 20180106 111509 ...
[*] Checking if the target service speaks SSL/TLS...
  [-] The target service st-[redacted]-msk-fs.[redacted].com:5081 seems to speak SSL/TLS...
  [-] Using SSL/TLS protocol version:
      (empty means I'm using the default openssl protocol version(s))
[*] Running sslscan on st-[redacted]-msk-fs.[redacted].com:5081 ...
  [-] Testing for SSLv2 ...
  [-] Testing for the NULL cipher ...
  [-] Testing for weak ciphers (based on key length - 40 or 56 bits) ...
```

SSL analysis on st-Client's-msk-fs.Client's.com (port XXXX)



```

[*] Testing for TLS v1.1 and v1.2 (CVE-2011-3389 vuln, aka BEAST) ...
[ ] Testing for SSLv3 and TLSv1 support ...
Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-GCM-SHA384 Curve P-256 DHE 256
Accepted TLSv1.2 256 bits TCDHE-RSA-AES256-SHA Curve P-256 DHF 256
Accepted TLSv1.2 256 bits AES256-GCM-SHA384 Curve P-256 DHE 256
Accepted TLSv1.2 256 bits AES256-SHA256 Curve P-256 DHE 256
Accepted TLSv1.2 256 bits AES256-SHA Curve P-256 DHE 256
Accepted TLSv1.2 256 bits CAMELLIA256-SHA Curve P-256 DHE 256
Accepted TLSv1.2 128 bits TCDHE-RSA-AES128-GCM-SHA256 Curve P-256 DHF 256
Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-SHA256 Curve P-256 DHE 256
Accepted TLSv1.2 128 bits TCDHE-RSA-AES128-SHA Curve P-256 DHF 256
Accepted TLSv1.2 128 bits AES128-GCM-SHA256 Curve P-256 DHE 256
Accepted TLSv1.2 128 bits AES128-SHA256 Curve P-256 DHE 256
Accepted TLSv1.2 128 bits AES128-SHA Curve P-256 DHE 256
Accepted TLSv1.2 128 bits SEED-SHA Curve P-256 DHE 256
Accepted TLSv1.2 128 bits CAMELLIA128-SHA Curve P-256 DHE 256
Accepted TLSv1.2 128 bits ECDHE-RSA-RC4-SHA Curve P-256 DHE 256
Accepted TLSv1.2 128 bits AES128-RC4-SHA Curve P-256 DHE 256
Accepted TLSv1.2 128 bits RC4-SHA Curve P-256 DHE 256
Accepted TLSv1.2 112 bits ECDHE-RSA-DES-CBC3-SHA Curve P-256 DHE 256
Accepted TLSv1.2 112 bits AES128-DES-CBC3-SHA Curve P-256 DHE 256

```

Unsecure hash mechanisms supported by st-Client's-msk-fs.Client's.com (port XXXX)

```

root@kali:~# tiSSlId -msk-fs.com 5001
-----
TISSlId - (1.3) based on sslscan and openssl
by Rael Siles (www.taddong.com)
-----
openssl version: OpenSSL 1.1.0f 25 May 2017
-----
Host: 20180106-111517
-----
[*] Analyzing SSL/TLS on msk-fs.com:5001 ...
[.] Output directory: TISSlId 1.3 msk-fs.com 5001 20180106-111517 ...
[*] Checking if the target service speaks SSL/TLS...
[.] The target service msk-fs.com:5001 seems to speak SSL/TLS...
[.] Using SSL/TLS protocol version:
(empty means I'm using the default openssl protocol version(s))
[*] Running sslscan on msk-fs.com:5001 ...
[.] Testing for SSLv2 ...
[.] Testing for the NULL cipher ...
[.] Testing for weak ciphers (based on key length - 40 or 56 bits) ...

```

SSL analysis on Client's-msk-fs.Client's.com (port XXXX)



```
Terminal - root@kali: ~
File Edit View Terminal Tabs Help
root@ka... x root@ka... x root@ka... x root@ka... x root@ka... x root@ka... x root@ka... x root@ka... x
[*] Testing for TLS v1.1 and v1.2 (CVE-2011-3389 vuln. aka BEAST) ...
[-] Testing for SSLv3 and TLSv1 support ...
Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-SHA384 Curve P-256 DHE 256
Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-SHA Curve P-256 DHE 256
Accepted TLSv1.2 256 bits AECDH-AES256-SHA Curve P-256 DHE 256
Accepted TLSv1.2 256 bits AES256-GCM-SHA384 Curve P-256 DHE 256
Accepted TLSv1.2 256 bits AES256-SHA256 Curve P-256 DHE 256
Accepted TLSv1.2 256 bits AES256-SHA Curve P-256 DHE 256
Accepted TLSv1.2 256 bits CAMELLIA256-SHA Curve P-256 DHE 256
Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-GCM-SHA256 Curve P-256 DHE 256
Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-SHA256 Curve P-256 DHE 256
Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-SHA Curve P-256 DHE 256
Accepted TLSv1.2 128 bits AECDH-AES128-SHA Curve P-256 DHE 256
Accepted TLSv1.2 128 bits AES128-GCM-SHA256 Curve P-256 DHE 256
Accepted TLSv1.2 128 bits AES128-SHA256 Curve P-256 DHE 256
Accepted TLSv1.2 128 bits AES128-SHA Curve P-256 DHE 256
Accepted TLSv1.2 128 bits SEED-SHA Curve P-256 DHE 256
Accepted TLSv1.2 128 bits CAMELLIA128-SHA Curve P-256 DHE 256
Accepted TLSv1.2 128 bits ECDHE-RSA-RC4-SHA Curve P-256 DHE 256
Accepted TLSv1.2 128 bits AECDH-RC4-SHA Curve P-256 DHE 256
Accepted TLSv1.2 128 bits RC4-SHA Curve P-256 DHE 256
Accepted TLSv1.2 112 bits ECDHE-RSA-DES-CBC3-SHA Curve P-256 DHE 256
Accepted TLSv1.2 112 bits AECDH-DES-CBC3-SHA Curve P-256 DHE 256
```

**Unsecure hash mechanisms supported by Client's-msk-fs.Client's.com (port XXXX)**

## Penetration Test on mobile device

Penetration Test activity on mobile devices aims to identify exposed services, used software versions, wrong/unsecure configurations and possible vulnerabilities.

### Scope

The activity scope includes the following areas:

- USB
- NFC
- WiFi

### Point of Attack

All the activities were performed from 2 Kaymera devices with a supporting Kali Linux machine.



## Methodology

Used methodology was divided into different phases:

1. USB analysis
2. NFC analysis
3. Wi-Fi analysis

## Support Instruments

In the following a non-exhaustive list of the tools used to perform the activity:

- Tenable Nessus
- Burp Suite Professional
- Nmap
- TLSSled
- WiFi Pineapple
- Metasploit Framework
- SipVicious
- Bettercap
- Nikto
- Hcitol
- Ubertooth One
- ADB

## USB analysis

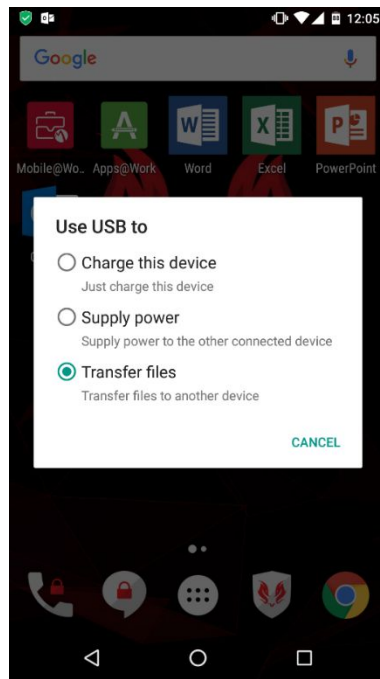
Physical ports analysis led to identification of a single USB type-C. This port can be used for:

- device charging
- power supply
- file transfer

### **File transfer**

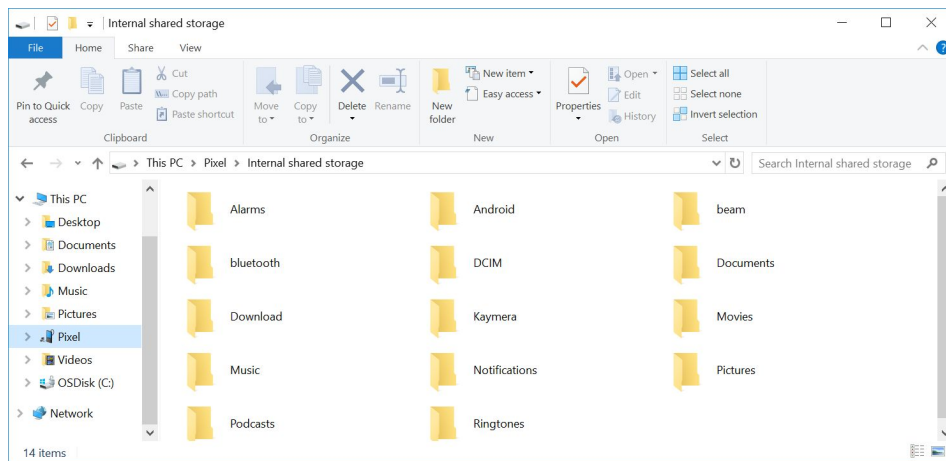
File transfer feature is not inhibited, so that an attacker with device physical access could obtain its data after lock-screen bypass.





### File transfer

File transfer feature allows mounting and browsing of device memory. In particular, it is possible to transfer screenshots, video or pictures.



### Device memory from external OS

#### 1.1.1 Android Debug Bridge (ADB)

Debug feature is enabled by default as honeypot. At first connection, the device requires the user to grant access to the connected computer.



```
z3n0wl@blade:~/Android
[z3n0wl@blade Android]$ adb devices
List of devices attached
* daemon not running; starting now at tcp:5037
* daemon started successfully
FA69V0302401    unauthorized

[z3n0wl@blade Android]$ adb devices
List of devices attached
FA69V0302401    device

[z3n0wl@blade Android]$
```

### ADB enabling

```
z3n0wl@blade:~/Android
[z3n0wl@blade Android]$ adb get-state
device
[z3n0wl@blade Android]$ adb get-devpath
usb:1-4
[z3n0wl@blade Android]$ adb get-serialno
FA69V0302401
[z3n0wl@blade Android]$
```

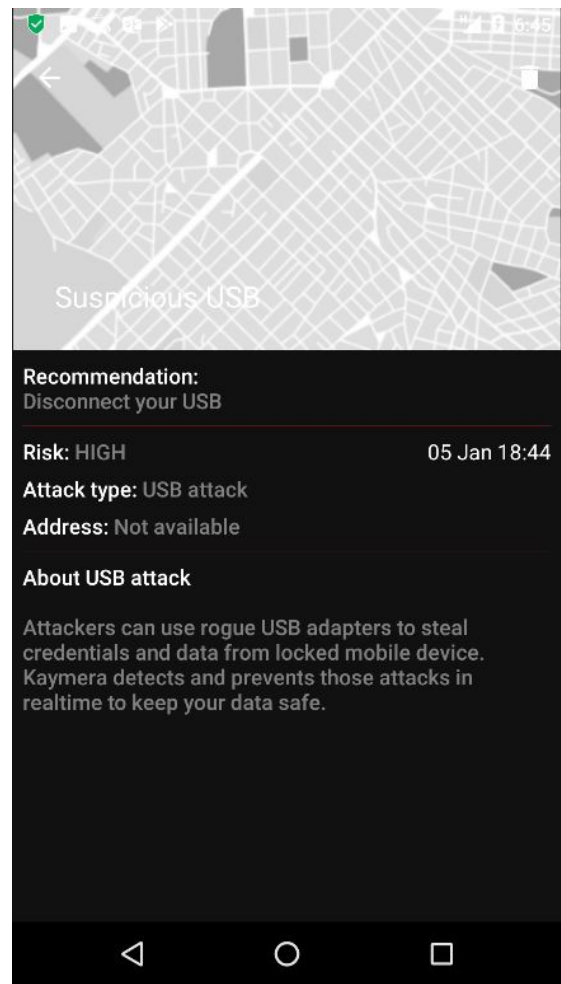
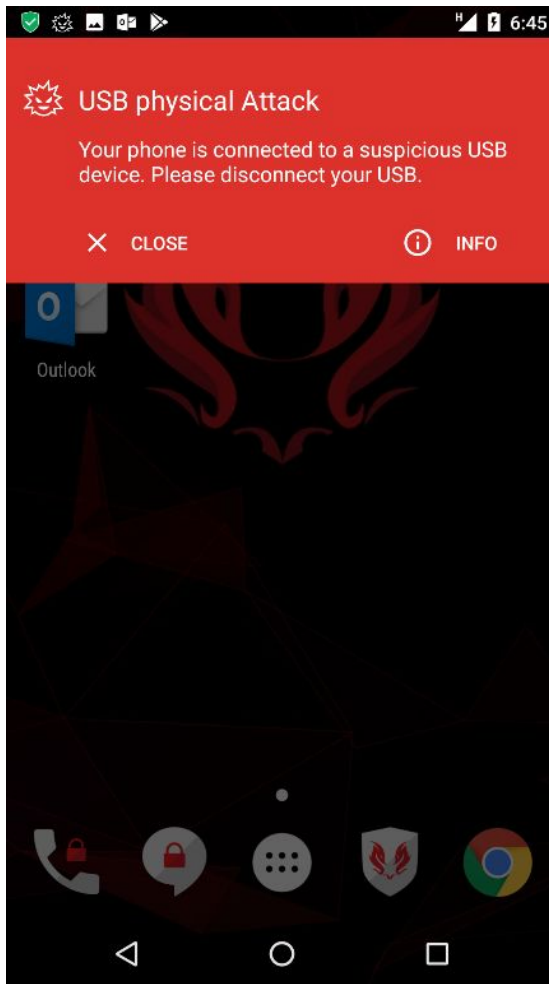
### ADB get-\* commands

Every attempt to use ADB with not “get-\*” commands are intercepted and blocked by the device.

```
z3n0wl@blade:~/Android
[z3n0wl@blade Android]$ adb shell
error: closed
[z3n0wl@blade Android]$ adb root
adb: unable to connect for root: closed
[z3n0wl@blade Android]$
```

### ADB other commands

The device shows a warning pop-up in case of detected unauthorized ADB command.



### ADB access detected & blocked

No root/unlock attempt was performed because of this security configuration.



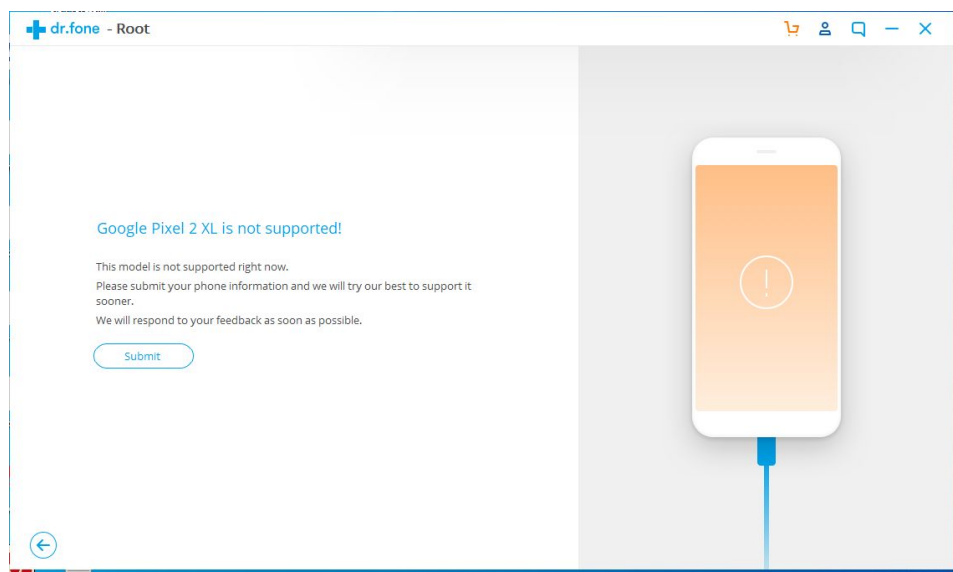
## Rooting Procedure Analysis

The rooting process of a device, in this case a customized android OS, is performed taking in consideration the following points:

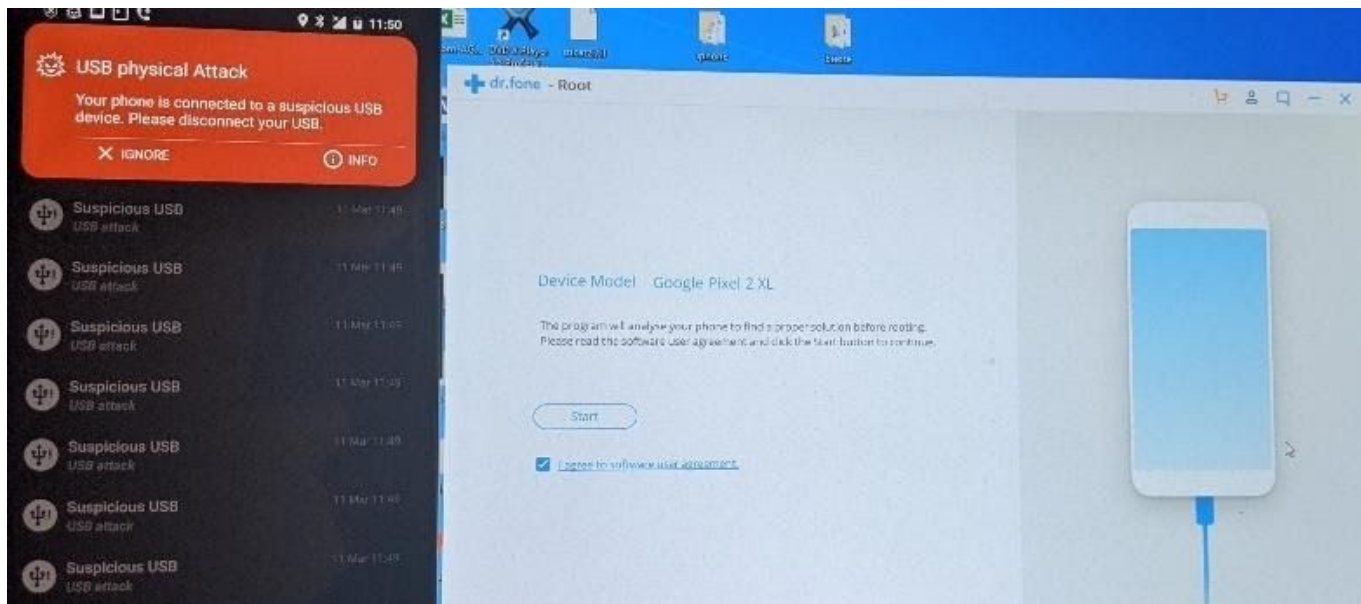
- I/O device's interfaces (WIFI, USB, Bluetooth)
- Camera input interpretation
- Unprotected services
- Android OS internals (vendor's configuration files, setuid scripts, android kernel version)
- Vulnerable installed binaries (toybox, busybox)

The first rooting attempt was performed using the USB data transfer feature. The android version installed in the analyzed device was not supported by the rooting software available in the market.

The following picture shows the result of the rooting attempt using the USB interface:



It is important to highlight that during the rooting attempt, the **Kaymera Centralized Security Center** was able to recognize the malicious use of the USB interface, and a warning message was shown as in the following picture.

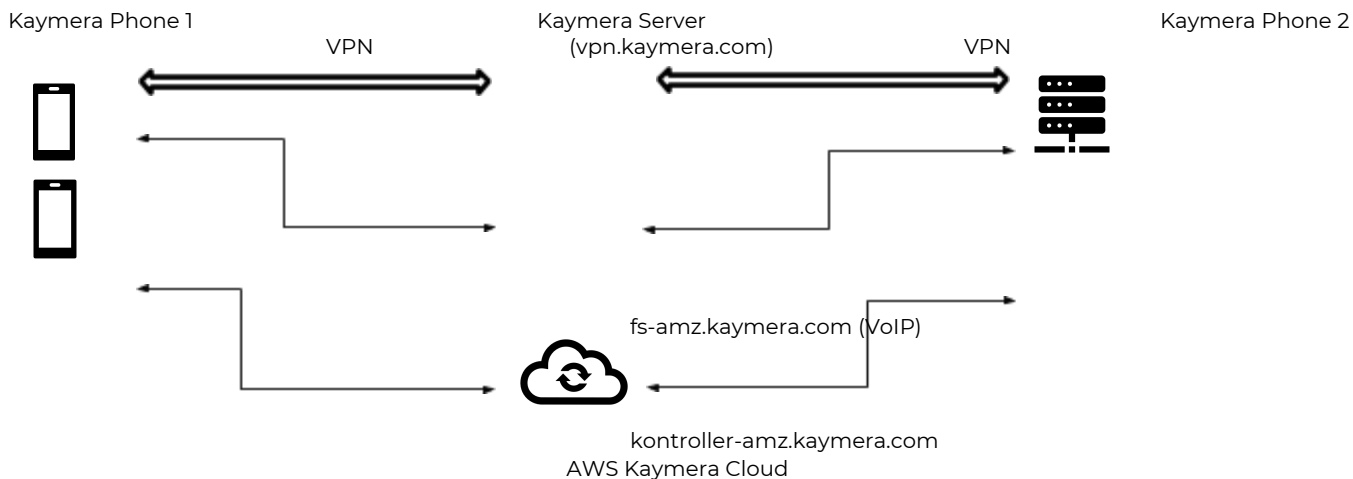


During the test, it was not possible to activate the android developer options which does not allow to perform further rootkitting attempts (recovery mode, or adb packet installation).

## Communication Analysis

The architectural solution provided by the vendor includes two calling methods (“Secure Call” and “Semi-Secure Call”) and a cryptographically protected messaging called “Encrypted Conversation”.

### Secure Call:





The secure call is established among two kaymera secure phones where applications are installed: **Kaymera Secure Communications App** (call & msg app) and **Kaymera Centralized Security Center** (Management, VPN, IDS, etc). During the test, the traffic generated performing a secure call was captured.

The phone devices (terminal) expose the VOIP service (sip/tls) on port XXXX/tcp. This allows to establish a VoIP connection directly with the phones.

#### # netstat -ntap

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp    91      0 0.0.0.0:XXXXX           0.0.0.0:*               UNKNOWN(138) -
tcp    91      0 0.0.0.0:XXXXX           0.0.0.0:*               UNKNOWN(138) -
tcp    91      0 0.0.0.0:XXXXX           0.0.0.0:*               UNKNOWN(138) -
tcp    91      0 0.0.0.0:XXXXX           0.0.0.0:*               UNKNOWN(138) -
tcp    92      0 0.0.0.0:XXXXX           0.0.0.0:*               UNKNOWN(138) -
tcp    91      0 0.0.0.0:XXXXX           0.0.0.0:*               UNKNOWN(138) -
tcp    0        0 127.0.0.XXXXXX         0.0.0.0:*               LISTEN      -
tcp    91      0 0.0.0.0:XXXXX           0.0.0.0:*               UNKNOWN(138) -
tcp    91      0 0.0.0.0:XXXXX           0.0.0.0:*               UNKNOWN(138) -
tcp    0        0 0.0.0.0:XXXXX          0.0.0.0:*               LISTEN      -
```

The phone terminal, in order to establish the secure call, opens several connections. The stream of such connections is shown below:

Server: `Kontroller-amz.kaymera.com`

IP: `34.XX.XX.XXX:XXX/tcp (TLS 1.2)`



```

.....5T...T.C...J..8.T....
.&.f...+.../.0...
...../5...[.....kontroller-amz.kaymera.com....
.....]...Y..Ls.Z.10n\...d.@T.....*p.M..X.....8...Nd...l...@...o...R...
0.....|...x.u..r0..n0..V.....60
.....*H..
..
..0.1.0...U...kaymera.com0..
190922123016Z.
290919123016Z0%1#0!..U...kontroller-amz.kaymera.com0.."0
.....*H..
.....0..
.....]! j.....A.F.[.....y...z.....\...q.XsTo.....P\k... a..u.$2 ..'h.n...$n..6..m..%.[++...^
".....i.....4.....Zna.@j}'<.....L'.....:.....Mf.....0y.....5..6..6..C.<.....2^4.....%.....}R.J!.</s.b.....
0..R..P...H...t..m...
Gf>/3...!p...X..|..{=4...T...W...M"&i.;;"A41.^..0.....|bj
..T...T.z.m.iv.R.r...dt...l<m...Cm..5n..Vo3.#...
n).j.<...Kf.c..D4+... M.+U.M...t..0...2.k..0..\C...f.0$.>e.....&5... .."N/...4+1...m..
-m..1B$].....G...0..U.....0..0..U...0..+.....+.....0%..U...0..kontroller-amz.kaymera.com0..U.....
0..U...um...)=0.. ..H...B.....0..U.#.0...V$1.w.....0
.....*H..
..
.....|B...d$#Q...../V$.k..8..e>\... (....KM
..V...X8...4.z.9..5HZk[-bY...y...Z...$......:..u..G.T.
q...oG...Q...e.Y.%..m..K...e...1#...W...:2..fe.....?;..t...}.D.....w..>m...U.#.....5..h.<.
1..>.
..X.Qr...M...I...A..j9.....0Cm.X...11...3^...&u/...1...Q...t?e.4q...|.....)*.....#3..5.....:2...[...5J..?.....
D...~*MTVm(.....1.Z1..6..1{.B...Z.#...L4...X...z...X..|.0.....5.....Q...1...r...|...v.../...c)dX'U...wNnH9..bS.A.rR.
3..?..U...%#m.d.1" *0D.?B...]... (0.Y..a.s.q...:d...&.....0h...G1...q...M...N.R^...0..
[D6...7..L.R.+K)...W.O...W..o]w]c... ..<...Q..T;[ ..5'.j..0..z..bW..91..17... ..N:'.U.....s..9..s.r...
6...ng6..ZK..P...e...e...E.d..6...D+?..60}>V..V_o...vp..{...km...H
@..@...@.....0.1.0...U...kaymera.com.....0..0.....K.$0
.....*H..
..
.....0.1.0...U...kaymera.com0..
70010100000Z.
300125132042Z0.1.0...U...3580350844760210.."0
.....*H..
.....0..
.....0.....'q.....G.y|.d.....y..^..b.....M6...X...b...q/...6...o.o.j[.g.....G!tuU"ABre...i...'.j..L6
]sn.>.9...WG.....T...)
..Y9..>9...T.....<...!q..7y.UT...o.M.....]..%..2..<...U=u...'.(..
.Y.....[!&..f.....%q8}]..b'.r.....*0(0..U.....0..U.%.....0

```

The connection is TLS protected. Therefore, it was not possible to read packets content.

Server: fs-amz.kaymera.com  
IP: 104.XXX.XX.XXX:XXXX/tcp (VoIP sip/tls)

```

.....1.....X.....) .. tm..E. ..G.o..8...K0...0...,$...
.....k.j.i.h.9.8.7.6.....2...*..&.....=5.../..+...#..... ..g.@?>.3.2.1.0.E.D.C.B.1..-).%.....<./A.....
..
.....p.....fs-amz.kaymera.com.....
.....
.....#...
0..0...0
.....*H..
..
..0.1.0...U...kaymera.com0..
140622081848Z.
240619081848Z0.1.0...U...fs-amz.kaymera.com0.."0
.....*H..
.....0..
.....<y..
P.y.0".....C.....k.....z&.....4..JE?89..W&].....&2..U.....d...<o..X...=..X..U.N.T~.I...2...kZ...u..d?|.....
1...4.Z...].ZnU.*.M...[.....:$.J...&.....).....p.....q{IR..|..M...I..b1b.k..I.r.....[.....n1..w.....^.....|Z..L...W.=o.8?
H2.....6.v$0c-e..}.6.%u..(.(J.#..Z..B...2H.<..
.VH(6..3.a%4...}8...f...b=L...k8..yUQ...W.QI GJ...DQ...V1././a.8s...hu...N...t...^.....}E.....=..8.2H...
%O.....{.....m..F."K.....|]q..Z@.....d...8.U..K.ov...7...7n...+K.....0
.....*H..
.....5.....0...J:..c<...?i...K..
...S.9.I'..V..N...ZXx..!j..KH..l..&...m..8.....)ac1Qu.M..E>5
.....!7.Q..5...L.j.i.i...|Z.t...>S.....}..c...rb...^6'..)=*(9.ox.e...f.6...V.....Dz6.....&.a.V.....XZu.
9...G..).6.T...0..0..... ..MQ..%0
.....*H..
.....0.1.0...U...kaymera.com0..
140622081823Z.
240619081823Z0.1.0...U...kaymera.com0.."0
.....*H..
.....0..
.....o.=.Z..x6.l..5K^|. w@y...dTt:..,k8...v..'1JG...t..wo.....BT\~.....)!...".>..s./7...!97.....H.....B.
6.<..H0_...6X..'A.5...L?..nTM..2.0%..).1.3.l..Z.tRqExu.R_m3Eh=q.Lf...g&d{.+.+.f.tq.g.h1.[4~ ..L..L.j...
*ck.....P0N0..U...V$1.w.....0..U.#.0...V$1.w.....0..U..0..0
.....*H..
.....1...H.....P..>...p ..G={...&.....<N...|...8...$...OS...V%..wE.....ld:c.*8.k..
9P..q.B7..e...g...mp...}.X.....>.j...=..n.....
:w:.....]9[w.E]|.....
..Q!..g...Bg..1.P.....t.4.F...8ao*.d..."".....C.<./B&.:%.....
.....M..I..A.....R0(g.....m.^..a...lz.h..
^.....V.....

```



Server: vpn.kaymera.com  
 IP: 35.XXX.XX.XXX:XXXX/udp (VPN)

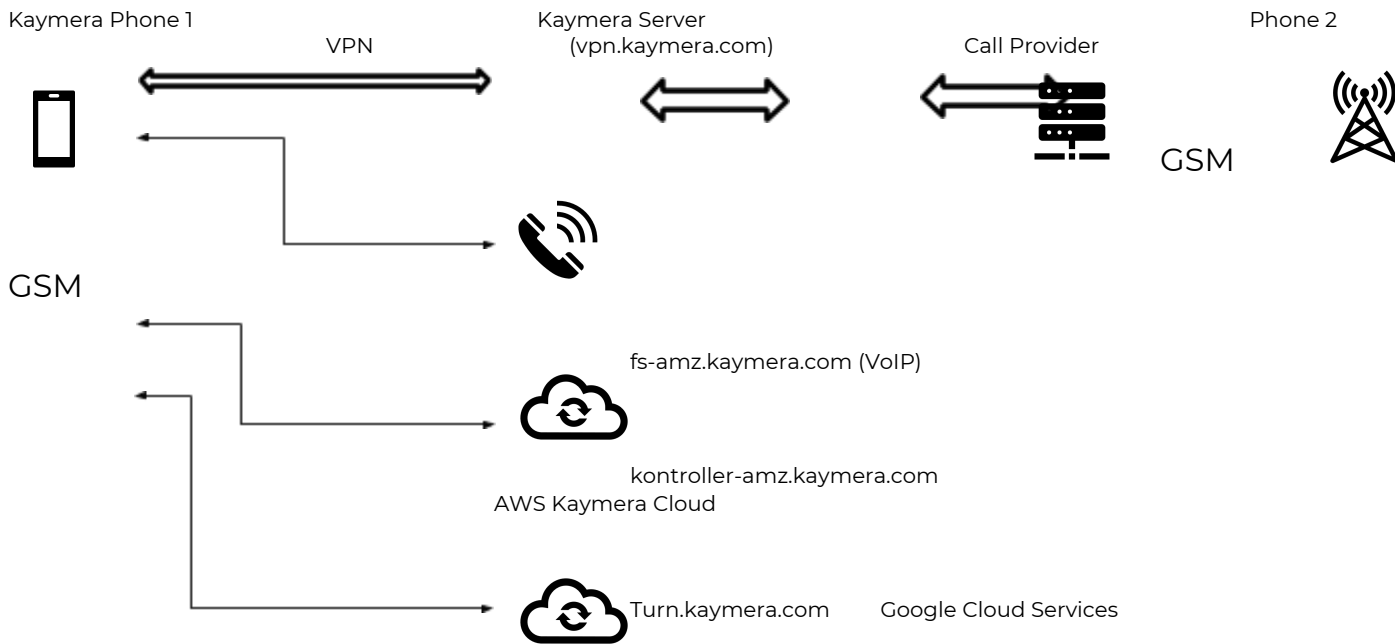
```

8X. \[b.....@.v.VH.....X.\[b.....(X.\[b.....v.VH... X.\[b.....U...Q.....F.....J.&].F.r.....\-F=.....$.
.....v.VH.....X.\[b.....1.....8ulV.....mBPJv...2..s.^].....1...h.e.
\0..X0..@.....L0
.....*..H..
.....
.....0.1.0...U...kaymera.com0..
19112599400Z.
291122090400Z0.1.0...U...vpn.kaymera.com0.."0
.....*..H..
.....
.....V_%.L.T.6...gD3.C>T.m....W....&...7...k...I..s.X2..V!..} C2.X...}.....".dh.!..L1..(=...B.J...J.7V}0
.....*.....$1..n../.0...&...m...t:zj..
.N(U)+".u.3g.C.".....C.G
ax...C..S:@.....>S.c.g...H.....\8.....y.#m.P.....().....eD{<"q...C.l.B.H
.C.e.(=.....:[:T.I..j...G...Q...s...#...U~%3...4".....|K..A..}z.B.{...P.....&k..F...{Q..
0.x0.."}x...j}*..@J..@.....-p~9...~.a..d-mO.. F[...V.8..5G..;(^...$.4..7C9..\.K...X3..~.`QD.v..j. H.=e'...*D.
{.jX..Yj}.....0..0..U.....0..0..U.%...0...+.....0...U...0...vpn.kaymera.com0...U.....
0..U...Yj}.....F2.x...U..v..`h..0..`..H...B.....0..U.#...0...V$1.w.....0
.....*..H..
.....
.....
.....g...d6.S..Y...&.X%..0..{:...UOGa..D...<<@..MzTE..nj.../.....^B5...%doR>.`.MIB..b.....V).U..p...ML../.W.g.....X.Q.
%......1Gk.<|...(#.m.....dd%.....6.S...q.....+RT.....+v2.....@.'...
6.[<
g.W.tu...S...+y//
%
%
.....v.VH.....0.....
.....MQ..%0
.....*..H..
.....0.1.0...U...kaymera.com0..
140622081823Z.
240619081823Z0.1.0...U...kaymera.com0.."0
.....*..H..
.....
.....
.....o..m..Z..x6..l..5K^..l..w@y...dTt:..k8...v..'1]G...t..wo.....BT\~.....).l..."}.....s./7...l.97...H.....B.
6.<..H0...6X..'A.5...L?.nTM..2.0%..).1.3.l..Z.tRqExu.R..m3EH=q.LF...g&d{...+...f.tq.g.h1.4~
*ck.....P0N0...U.....V$1.w.....0..U.#...0...V$1.w.....0..U...0...0
.....*..H..
.....
.....1...H...r..9>.._p...G={...&.....<.N...|...8...$.%...OS...V%..wE.....ld:c.*8.k..
9P..q.B7...e...g...mp..}.....X.....j:->'...n.....
.Wt.....}9[w.E]].....
..Q!..g...Bg..1.P...t.4.F...8ao*..d..."".....C...<./B&.:%.....
.....l.....%:j.x.m.o..$x.../..<i.UW...Y~[...kC...X]`..Hn...t..0...0...5
..)}...3..A...L.?.....k..||...L
.....

```

No other connections were detected during this test.

**Semi-Secure Call:**









Server: vpn.kaymera.com  
 IP: 35.XXX.XX.XXX:XXXX/udp (VPN)

```

8X.[b.....@.v.VH.....X.[b.....(X.[b.....v.VH.....X.[b.....U..Q.....F.....J.&].F.r.....\~F.....$.
.....@.v.VH.....X.[b.....1.....8uIV.....mBPJv...2..s.^].....l..h..e..
\0..X0..@.....L0
.
*H..
..
..0.1.0..U.....kaymera.com0..
1911250904002.
29112209040020.1.0..U.....vpn.kaymera.com0.. "0
.
*H..
.....0..
.....V..%..L.T.6...gD3.C>T.m...W.....&.....7..k...I..s.X2..V|..} C2.x...}.....".dh.l.l.L..(=...B.J...J.7V)0
.....*.....$!l..n../.0...&...m...t..zj..
.N(u)*.u.3g.C*.....C.G
ax..C..S..@.....>S.c.g.....H
.....\8.....y.#m.P .....{.....eD{<".q...C.l.B.H.
.C.e.(=...{...T.I.;...G..Q...s..#...U=%3...4"...[K..A..}z.B.{...P.....&k..F...{.Q.
0.x0.."}jx..j.*.@j..@.....-p~9.....a..d..mO.. F[...V.8..5G.;(^...$.4..7C9..\.K...X3~.`.QD.v..j. H="e"*D.
{.}X..Y.j}{.....0...0...U.....0..0...U..%..0...+.....0...U.....0...U.....vpn.kaymera.com0...U.....
0...U.....F2.x...U..v..h..0.. ..H...B.....0...U.#...0...V$1.w.....0
.
*H..
..
.....
.....g..d6.s..Y...&X%..0..{:...UOGa..D..<<..@..MzTE..nj.../.....^..B5...%doR>`.MIB..b....V).U..p...ML../.W.g....X.Q.
%.....1Gk..<(.#m.....dd.....6.S...q.....+RT.....+v2.....@'....
6.<[<
g.w.tu...S...+y/.
%
.v.VH.....0...0..... ..MQ..%0
.
*H..
.....0.1.0..U.....kaymera.com0..
1406220818232.
24061908182320.1.0..U.....kaymera.com0.. "0
.
*H..
.....0..
.....0..=Z..x6.l..5K^..l. w@y...dTt;..k8...v..'1G...t..wo.....BT~.....)l.."}.....s../..1.97.....j.H.....B.
6.<.H0.....6X.'A.5..L?..nTM..2.0%..}..1.3.l..Z..tRqExu.R..m3Eh=q.Lf....g&d{.+...f.tq.g.h1.l4~
*ck.....PmN0..U.....V$1.w.....0...U.#...0...V$1.w.....0...U.....0...0
.
*H..
.....1..H..r..9>...p ..G={...&...<N...|...8..$....0S...V%..wE....ld;c.*8.k..
9P..q.B7...e.....g..mp.).....X.....;=>'..n.....
w:.....}9[w.E]].....
..Ql...g...Bg..1.P.....t..4.F...8ao*.d..d.."}.....C...<./B&::%.....
.....l.....%;.x.m.o..$x../<.i.UW..Y~[...kC...X]"..Hn...t..0...0...5
.)...3..A.....L..?.....k..|].....L
.:
81 pacchetti clienti, 48 pacchetti server, 48 turni.

```

Server: turn.kaymera.com  
 IP: 104.XXX.XX.XXX (Traversal using Relay NAT)

```

....!.B9IyzqeYvID+U.....!.BCE2SqG4zg+kY.....Xl..B9IyzqeYvID+U.....xs9.....Ya...+....
.....
.....".Coturn-4.4.5.3 'Ardee West'..(.....!.BCE2SqG4zg+kY.....Unauthorized.....
1a65c74a60e7b7d5...kaymera.comu..".Coturn-4.4.5.3 'Ardee West'n.(...dP...L!..BfCmhM19bVcnH.....prod....kaymera.com....
1a65c74a60e7b7d5...2.8....P6..z.%/..g0...!.BfCmhM19bVcnH.....prod....kaymera.com....xs9..
.....X..".Coturn-4.4.5.3 'Ardee West'u.....g.....j'9.e.."}.....(..Y.....P!..BHFk2Z0et2D42.....f.I.....prod....kaymera.com....
1a65c74a60e7b7d5.....tR...Q..@!..BHFk2Z0et2D42..".Coturn-4.4.5.3 'Ardee West'X...V.;.....2..E...}..
(.....!.BmsFChuquUVV+M.....f.I.....p..|..BK5sxozRDkXle...ktEYTDLF3rgCvcyI:1seg...W.....
*.y].z.y).%.%.n.....L%..HRi..U&Jl...a1.8.(.PN.....!.Bn1Xok3m20tNV.....f.I.....p...|..B0E8Xem1HaTht...ktEYTDLF3rgCvcyI:
1seg...W.....
*.y].z.y).%.%.n.....]I].g..#:(.....!.BNDWjSLNumpC.....f.I.....p...|..BQEvbkRd9CK7...ktEYTDLF3rgCvcyI:
1seg...W.....
*.y].z.y).%.%.n.....ti..S.....45.....".(.....#......!.B+p91bkDyRHwd.....f.I.....p...|..BkNh/
gIUSX4Df...ktEYTDLF3rgCvcyI:1seg...W.....
*.y].z.y).%.%.n.....3-...? ..e..X
r.....(.....g...../KKPrpqoBNjL.....f.I.....p...|..BNBTsIeydK90i...ktEYTDLF3rgCvcyI:1seg...W.....
*.y].z.y).%.%.n.....;.....9..p.Ct+(.....!.BpwBnU2533LoP...Xl..BpwBnU2533LoP.....xs9.....Ya...+....
.....
.....".Coturn-4.4.5.3 'Ardee West'z.(...0.....!.BzZMoBv3u4sru...Xl..BzZMoBv3u4sru.....xs9.....Ya...+....
.....
.....".Coturn-4.4.5.3 'Ardee West'..(.....!.BpTLL7c1JU/zip.
.....prod....kaymera.com....1a65c74a60e7b7d5...l...g}.....c...d.....H!..BpTLL7c1JU/zip.
.....".Coturn-4.4.5.3 'Ardee West'.....L%I../7
.....t..l.v.(.....
12 pacchetti clienti, 7 pacchetti server, 11 turni.

```

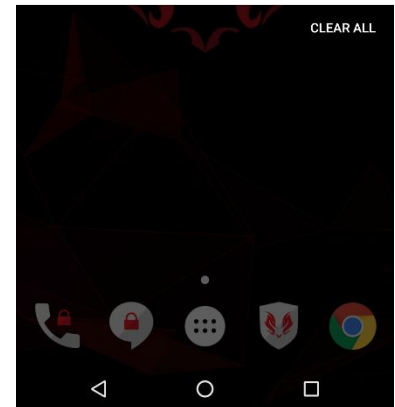
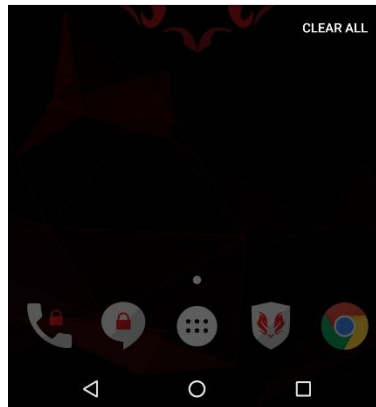
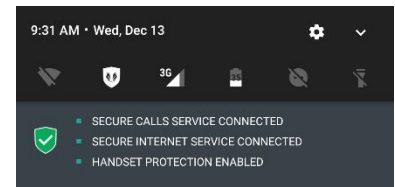
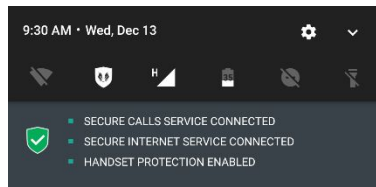
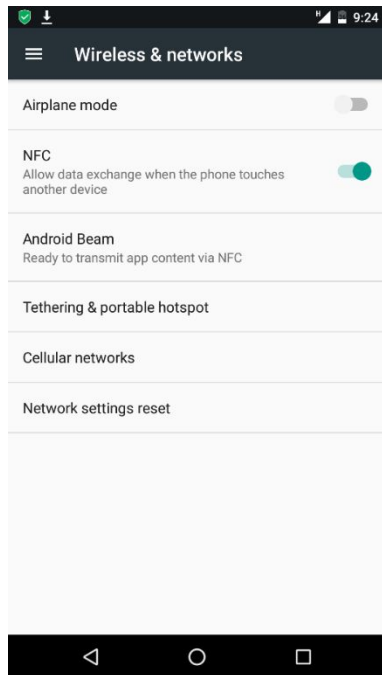


## NFC analysis

NFC analysis was executed to understand if the device offers protection from file transfer and offers specific protection countermeasures.

### 1.1.2 File transfer

File transfer feature is not inhibited, so that data can be moved even between non-Kaymera devices.



**File transfer through NFC**



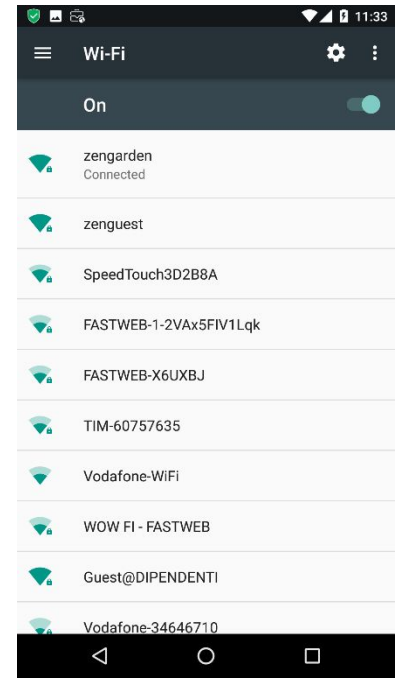
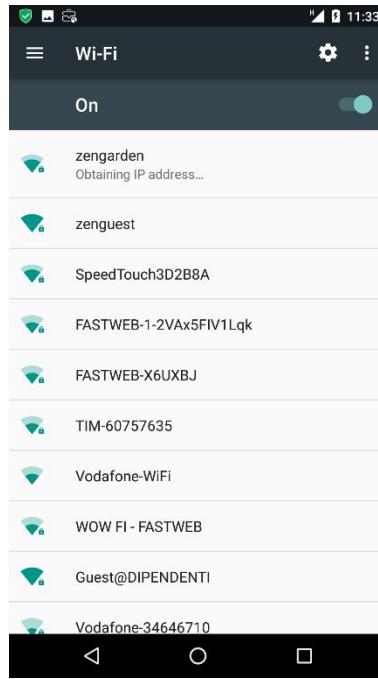
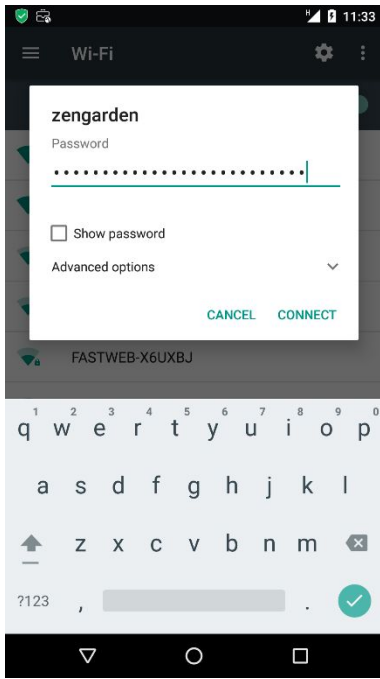
**Transferred image through NFC**

## WiFi analysis

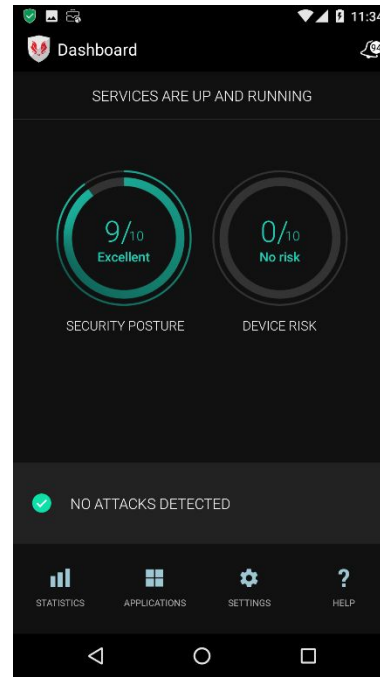
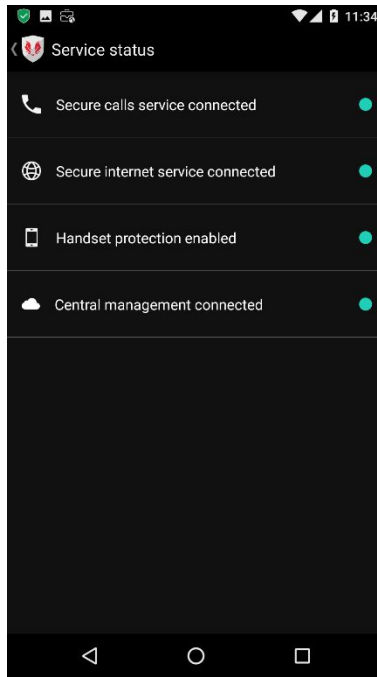
Wi-Fi analysis was made to understand if the device offers protection mechanisms against FakeAP (e.g. RogueAP, Evil Twin) and Man-in-the-Middle attacks. In addition, services exposed by mobile devices were analyzed.

### **Untrusted AP access**

From performed analysis, the device allows connection to a Wi-Fi network with untrusted SSID. Specifically, even connecting to an untrusted AP, the device manages to connect with Central Management and enable Secure Call, Secure Internet and Handset Protection services.



**Untrusted network access**



**Service enabling on untrusted network**

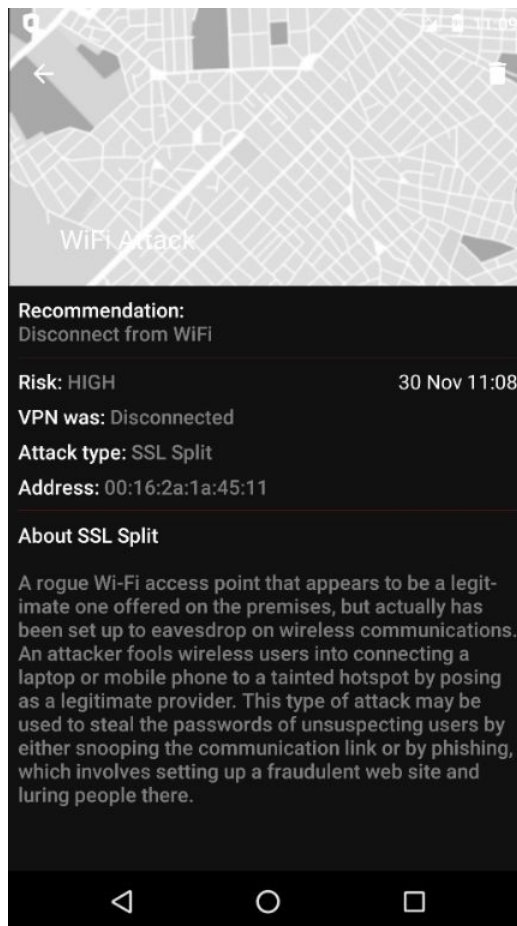


## Fake AP

The analysis resulted in the change of impersonating a network already saved on the device. Specifically, pre-configured Wi-Fi SSID (Client's-cert) was cloned on an external AP not owned by Client's and the device correctly connected to it even with a different authentication method – certificate for Client-cert and WPA for cloned AP. Using a Fake AP it is possible to intercept all clear text content transmitted and received from the device without being detected by its own security mechanisms.

## Man-in-the-Middle with SSL Splitting

The device is able to detect a MitM attempt only in case of usage of untrusted certificates, needed to perform SSL splitting attack and decode encrypted traffic towards/from legit websites. In case of detection, mobile device automatically disconnect from Wi-Fi networks.



**Detected SSL Split**



## Man-in-the-Middle with ARP Spoofing

It was evaluated as a chance to execute a Man-in-the-Middle attack through ARP Spoofing using a notebook connected to the same device network.

```
root@kali:~/Desktop/Bluetooth# bettercap -T 192.168.1.100 -G 192.168.1.100 --proxy-module replace_file.rb --file-extension apk --file replace_pirate_flag.jpg --no-sslstrip

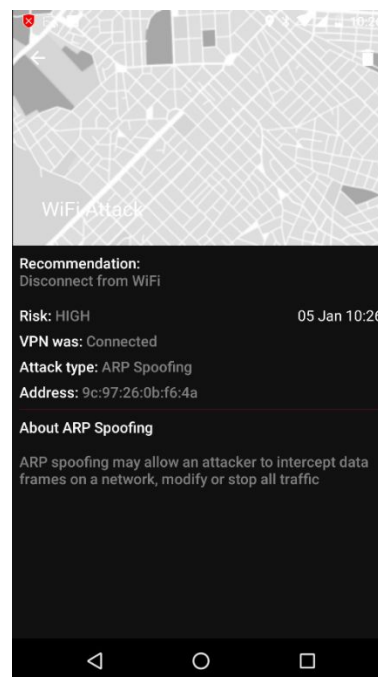
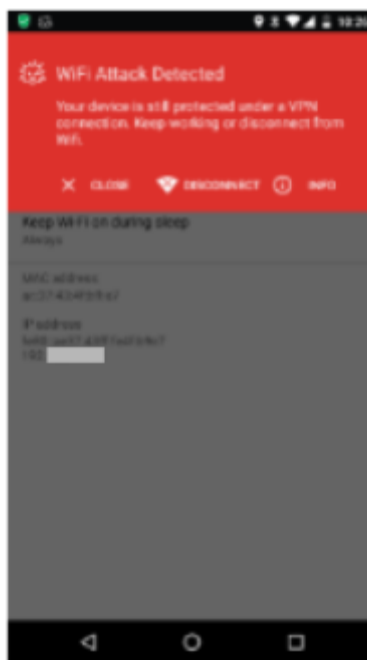
bettercap v1.6.2
http://bettercap.org/

[!] Found hostname android-978cc72bf334aef6 for address 192.168.1.100
[!] Starting [ spoofing: discovery: sniffer: tcp-proxy: udp-proxy: http-proxy: https-proxy: sslstrip: http-server: dns-server: ] ...

[!] [eth0] 192.168.1.100 : 00:0C:29:5C:84:4F / eth0 ( VMware )
[!] Found hostname dslddevice for address 192.168.1.100
[!] [GATEWAY] 192.168.1.1 : 9C:97:26:0B:F6:4A / dslddevice ( Technicolor )
[!] [HTTP] Proxy starting on 192.168.1.100:8080 ...
[!] [TARGET] 192.168.1.100 : AC:27:43:4F:89:E7 / android-978cc72bf334aef6 ( HTC )
```

MitM setup

In this case, the device detects the MitM attempt through ARP Spoofing.

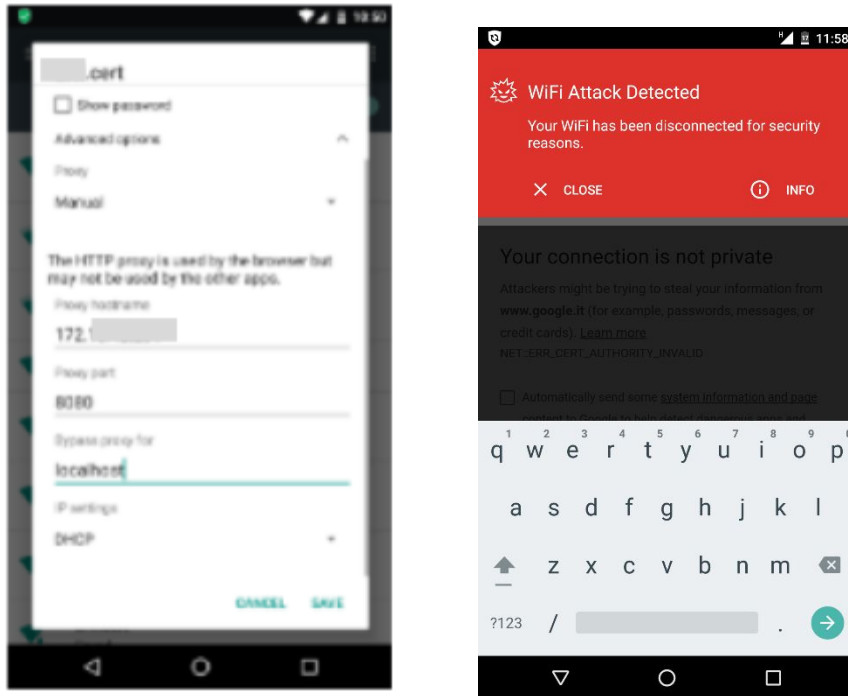


ARP Spoofing detection and block



## Man-in-the-Middle with Malicious SSL Proxy

Even installing a Proxy SSL certificate on the device, it is still able to detect a MitM attack, disconnecting it from the Wi-Fi network.



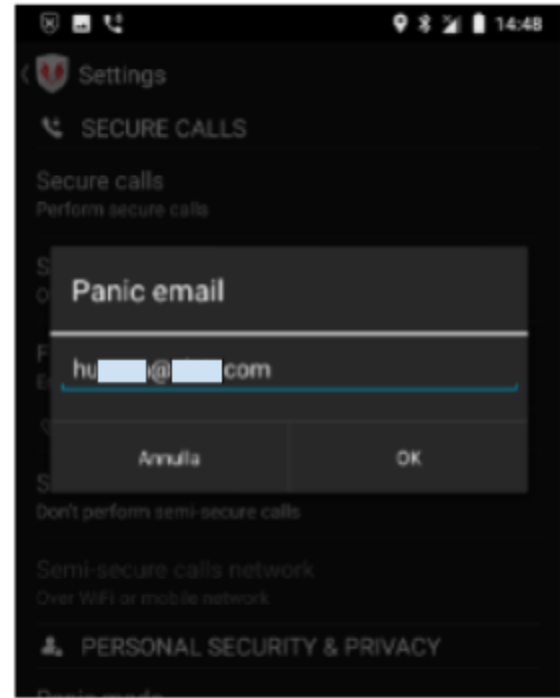
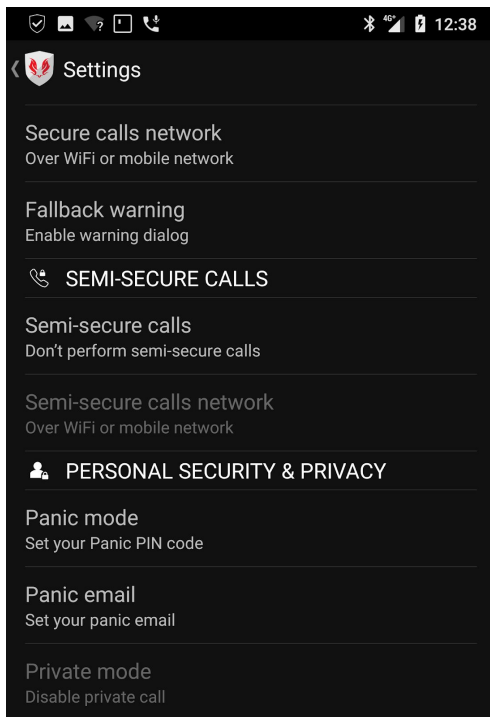
MitM Proxy settings





## Panic Mode Analysis

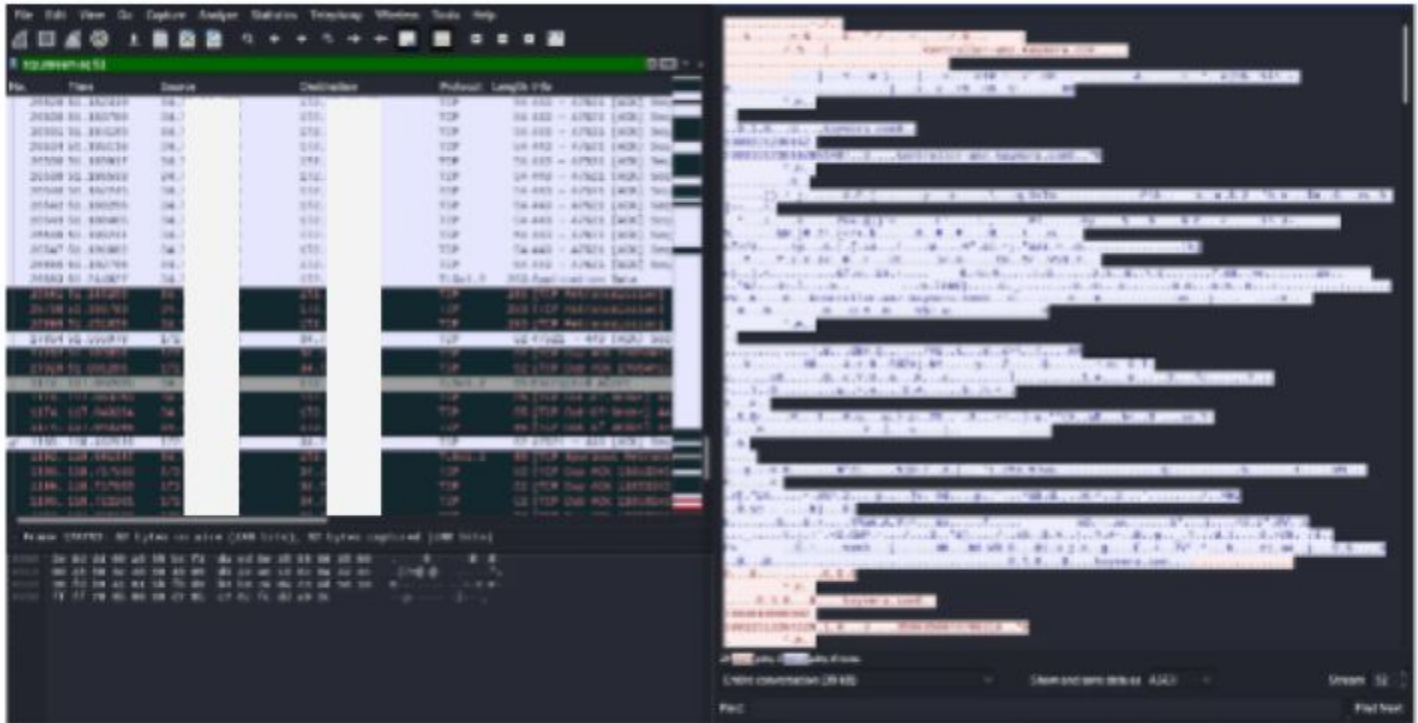
The Kaymera Secure Start Phone has a feature called “Panic Mode” which allows to modify the phone standard environment under attack. Using the Dashboard app (management app) it is possible to configure a Panic device PIN and an email address.



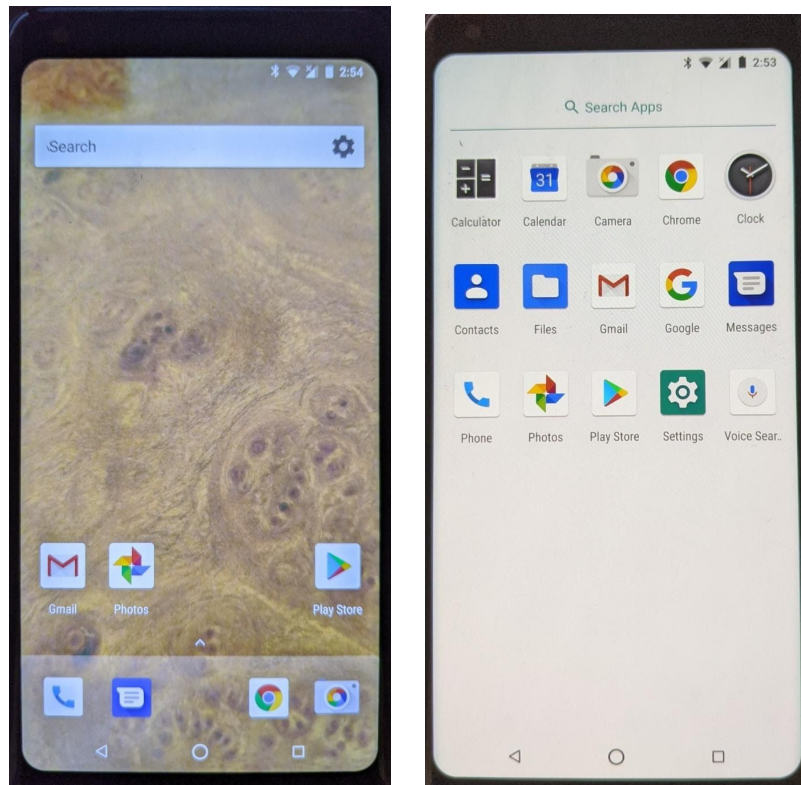
In case the final user is under attack, he/she will be able to unlock the phone with the PIN code specified in the Dashboard application. At this point, the device behaves as a standard android device in terms of android theme, launcher and installed applications. At the same time, the device starts to send its current GPS position, photos from both cameras and audio/video to the pre-configured email address.



The data is sent via HTTPS through the Kaymera Management Server. Follows an example of such traffic where the `xxxxx-xxx.kaymera.com` server was contacted.



Standard android launcher and applications:



Panic Mode Active Notification via Email address.

The first email contains the device's GPS location together with a picture from the rear and front device's camera.



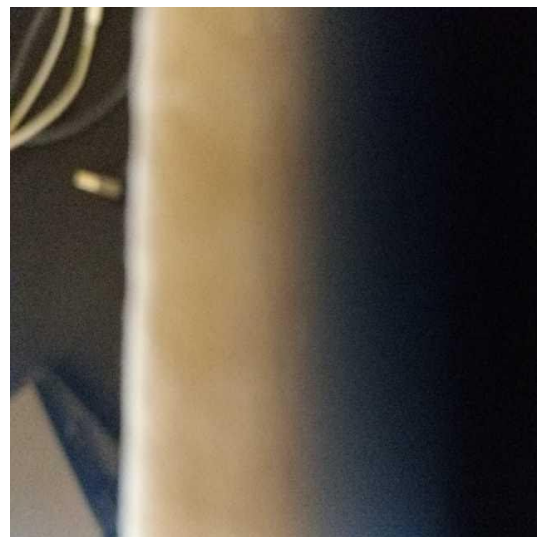
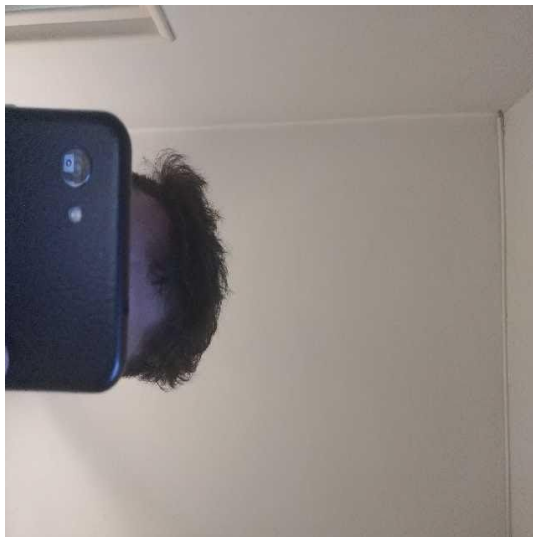
## PANIC ACTIVATED

Fri Mar 20 2020 13:53:39 UTC



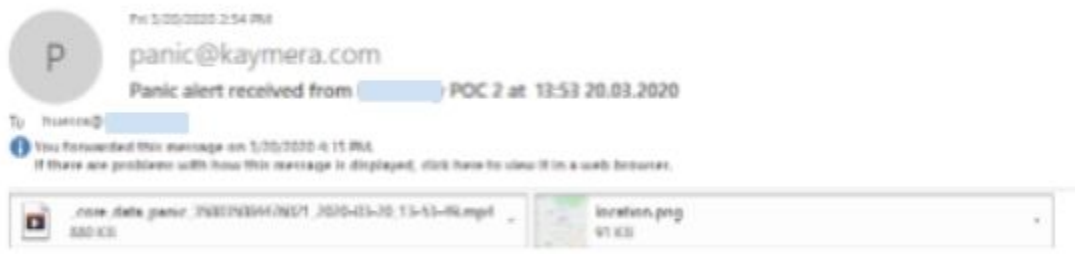
PICTURES FROM THE LOCATION ARE ATTACHED TO THIS EMAIL

Front and rear cameras:





The second received email contains a front camera video in MPEG-4 (.mp4) format and an upgrade of the device's GPS location.



### PANIC ACTIVATED

Fri Mar 20 2020 13:53:50 UTC

POC 2 [redacted]  
Mobile [redacted]  
IMEI [redacted] 1  
Location [redacted] 67-43 [redacted] 13:49

Update of the device's GPS Location:





During Panic Mode no unauthorized traffic or connection establishment was out of the Kaymera environment, such as towards third party servers (information trackers, etc).

## Penetration Test from Client's network on Kaymera infrastructure

The Penetration Test activity from the Internet on Kaymera infrastructure aims to identify exposed services, software versions, unsecure configurations and possible vulnerabilities.

### Scope

The activity scope includes the hosts exposed on the Internet by TEST and PRODUCTION environment.

#### TEST ENVIRONMENT:

- 10.XXX.XXX.XX
- 10.XXX.XXX.XX
- 10.XXX.XXX.XX
- 10.XXX.XXX.XX
- 10.XXX.XXX.XX
- 10.XXX.XXX.XX

#### PRODUCTION ENVIRONMENT:

- 10.XXX.XXX.XX
- 10.XXX.XXX.XX
- 10.XXX.XXX.XX
- 10.XXX.XXX.XX
- 10.XXX.XXX.XX
- 10.XXX.XXX.XX
- 10.XXX.XXX.XX
- 10.XXX.XXX.XX
- 10.XXX.XXX.XX

### Point of Attack

All the activities were performed from internal network through Virtual Desktop provided by Client's with IP address 10.XXX.XXX.XX/W10REVCU1101.ad00.Client's.intranet. This machine (OS: Windows 10), not allowing virtual machines execution or usage/installation of some required tools (e.g. Kali, Metasploit), limited the level of detail of the analysis described in the document.<sup>1</sup>

---

<sup>1</sup>The constraint was dictated by the temporal needs for the provision of the Kaymera solution by the Top management. .



To reach targets from this Point of Attack and execute the tests, it was required to authenticate through Juniper Firewall (with Client's domain credentials). Specifically, the following URLs were used: <https://auth-gdc-sb-a.Client's.com>, <https://auth-gdc-sb-b.Client's.com>, <https://auth-gdc-sb-c.Client's.com>, <https://auth-gdc-sb-d.Client's.com>.

## Methodology

The methodology used for Penetration Test from Internet on the infrastructure was structured in the following phases:

5. **Intelligence Gathering:** detect and collect publicly available data related to Client's asset and individuals.
6. **Service Discovery:** identify services exposed from targets in scope.
7. **Vulnerability Analysis & Exploitation:** identify security issues on targets through direct/indirect interaction; these vulnerabilities were leveraged to execute Proof-of-Concepts of public/ad-hoc exploits which guarantee the repeatability of performed tests.
8. **Post Exploitation:** retrieve information (e.g. password, configurations, details) on compromised systems to be used for future attacks, gain higher privileges (i.e. privilege escalation) or perform lateral movement to attack other systems from exploited ones.

## Tools

In the following a non-exhaustive list of the tools used to perform the activity:

- Tenable Nessus
- Burp Suite Professional
- Nmap
- Nikto

## Service Discovery

Active port analysis on target hosts identified multiple exposed services:

IP	PORT	SERVICE
10.XXX.XXX.XX	TCP/XX	ssh OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)
10.XXX.XXX.XX	UPD/XXX	rpcbind 2-4 (RPC #100000)
10.XXX.XXX.XX	UPD/XXX	ntp NTP v4 (secondary server)
10.XXX.XXX.XX	UPD/XXX	SNMPv1 server (public)
10.XXX.XXX.XX	TCP/XXXX	http Coturn TURN server http admin 4.2.1.2
10.XXX.XXX.XX	TCP/XXXX	tcpwrapped
10.XXX.XXX.XX	TCP/XXXXX	status 1 (RPC #100024)
10.XXX.XXX.XX	TCP/XX	ssh OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)
10.XXX.XXX.XX	UPD/XXX	rpcbind 2-4 (RPC #100000)



10.XXX.XXX.XX	UPD/XXX	ntp NTP v4 (secondary server)
10.XXX.XXX.XX	UPD/XXX	SNMPv1 server (public)
10.XXX.XXX.XX	TCP/XXXXX	postgresql PostgreSQL DB 9.4.9
10.XXX.XXX.XX	TCP/XXXX	tcpwrapped
10.XXX.XXX.XX	TCP/XXXXX	status 1 (RPC #100024)
10.XXX.XXX.XX	TCP/XX	ssh OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)
10.XXX.XXX.XX	UPD/XXX	rpcbind 2-4 (RPC #100000)
10.XXX.XXX.XX	UPD/XXX	ntp NTP v4 (secondary server)
10.XXX.XXX.XX	UPD/XXX	SNMPv1 server (public)
10.XXX.XXX.XX	TCP/XXXX	tcpwrapped
10.XXX.XXX.XX	TCP/XX	ssh OpenSSH 7.2 (protocol 2.0)
10.XXX.XXX.XX	TCP/XXXX	Openvpn OpenVPN
10.XXX.XXX.XX	TCP/XXXX	tcpwrapped
10.XXX.XXX.XX	TCP/XXXX	http nginx
10.XXX.XXX.XX	TCP/XX	ssh OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)
10.XXX.XXX.XX	UPD/XXX	rpcbind 2-4 (RPC #100000)
10.XXX.XXX.XX	UPD/XXX	ntp NTP v4 (secondary server)
10.XXX.XXX.XX	UPD/XXX	SNMPv1 server (public)
10.XXX.XXX.XX	udp/XXX	sip-proxy FreeSWITCH mod_sofia 1.6.9-16-d574870~64bit
10.XXX.XXX.XX	TCP/XXXX	ssl/ayiya
10.XXX.XXX.XX	TCP/XXXX	sip-proxy FreeSWITCH mod_sofia 1.6.9-16-d574870~64bit
10.XXX.XXX.XX	TCP/XXXX	ssl/sdl-ets
10.XXX.XXX.XX	TCP/XXXX	tcpwrapped
10.XXX.XXX.XX	TCP/XXXX	ftp-proxy
10.XXX.XXX.XX	TCP/59217	status 1 (RPC #100024)
10.XXX.XXX.XX	TCP/XX	OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
10.XXX.XXX.XX	TCP/XX	http nginx
10.XXX.XXX.XX	UPD/XXX	rpcbind 2-4 (RPC #100000)
10.XXX.XXX.XX	UPD/XXX	ntp NTP v4 (secondary server)
10.XXX.XXX.XX	UPD/XXX	SNMPv1 server (public)
10.XXX.XXX.XX	TCP/XXX	ssl/http nginx
10.XXX.XXX.XX	TCP/XXXX	ssl/http nginx
10.XXX.XXX.XX	TCP/XXXX	tcpwrapped
10.XXX.XXX.XX	TCP/XXXX	rtsp
10.XXX.XXX.XX	TCP/38345	status 1 (RPC #100024)
10.XXX.XXX.XX	TCP/XX	ssh OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)
10.XXX.XXX.XX	UPD/XXX	rpcbind 2-4 (RPC #100000)
10.XXX.XXX.XX	UPD/XXX	ntp NTP v4 (secondary server)
10.XXX.XXX.XX	UPD/XXX	SNMPv1 server (public)
10.XXX.XXX.XX	TCP/XXXX	tcpwrapped
10.XXX.XXX.XX	TCP/XXXX	mongodb MongoDB 2.5.1 or later
10.XXX.XXX.XX	TCP/XX	ssh OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)
10.XXX.XXX.XX	UPD/XXX	rpcbind 2-4 (RPC #100000)
10.XXX.XXX.XX	UPD/XXX	ntp NTP v4 (secondary server)





10.XXX.XXX.XX	UPD/XXX	SNMPv1 server (public)
10.XXX.XXX.XX	TCP/XXXXX	postgresql PostgreSQL DB 9.4.9
10.XXX.XXX.XX	TCP/XXXX	tcpwrapped
10.XXX.XXX.XX	TCP/XXXX	status 1 (RPC #100024)
10.XXX.XXX.XX	TCP/XX	ssh OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)
10.XXX.XXX.XX	TCP/XXXX	rpcbind 2-4 (RPC #100000)
10.XXX.XXX.XX	UPD/XXX	ntp NTP v4 (secondary server)
10.XXX.XXX.XX	UPD/XXX	SNMPv1 server (public)
10.XXX.XXX.XX	TCP/XXXX	http Coturn TURN server http admin 4.2.1.2
10.XXX.XXX.XX	TCP/XXXX	tcpwrapped
10.XXX.XXX.XX	TCP/XXXX	status 1 (RPC #100024)
10.XXX.XXX.XX	TCP/XX	Ssh OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)
10.XXX.XXX.XX	UPD/XXX	rpcbind 2-4 (RPC #100000)
10.XXX.XXX.XX	UPD/XXX	ntp NTP v4 (secondary server)
10.XXX.XXX.XX	UPD/XXX	SNMPv1 server (public)
10.XXX.XXX.XX	UDP/775	rpcbind
10.XXX.XXX.XX	TCP/XXXX	http Coturn TURN server http admin 4.2.1.2
10.XXX.XXX.XX	TCP/XXXX	tcpwrapped
10.XXX.XXX.XX	TCP/XXXX	status 1 (RPC #100024)
10.XXX.XXX.XX	TCP/XX	ssh OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)
10.XXX.XXX.XX	UPD/XXX	rpcbind 2-4 (RPC #100000)
10.XXX.XXX.XX	UPD/XXX	ntp NTP v4 (secondary server)
10.XXX.XXX.XX	UPD/XXX	SNMPv1 server (public)
10.XXX.XXX.XX	TCP/XXXXX	rpcbind
10.XXX.XXX.XX	TCP/XXXX	tcpwrapped
10.XXX.XXX.XX	TCP/XXXX	mongodb MongoDB 2.5.1 or later
10.XXX.XXX.XX	TCP/XX	ssh OpenSSH 7.2 (protocol 2.0)
10.XXX.XXX.XX	TCP/XXXXX	domain NLNet Labs Unbound
10.XXX.XXX.XX	UPD/XXX	ntp NTP v4 (secondary server)
10.XXX.XXX.XX	TCP/XXXX	openvpn OpenVPN
10.XXX.XXX.XX	TCP/XXXX	tcpwrapped
10.XXX.XXX.XX	TCP/XXXX	http nginx
10.XXX.XXX.XX	TCP/XX	ssh OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)
10.XXX.XXX.XX	UPD/XXX	rpcbind 2-4 (RPC #100000)
10.XXX.XXX.XX	UPD/XXX	ntp NTP v4 (secondary server)
10.XXX.XXX.XX	UPD/XXX	SNMP
10.XXX.XXX.XX	TCP/XXXX	tcoflashagent
10.XXX.XXX.XX	TCP/XXXX	ssl/ayiya
10.XXX.XXX.XX	TCP/XXXX	sip-proxy FreeSWITCH mod_sofia 1.6.9-16-d574870~64bit
10.XXX.XXX.XX	TCP/XXXX	ssl/sdl-ets
10.XXX.XXX.XX	TCP/XXXX	tcpwrapped
10.XXX.XXX.XX	TCP/XXXX	ftp-proxy (Cluecon)
10.XXX.XXX.XX	TCP/XXXX	status 1 (RPC #100024)
10.XXX.XXX.XX	TCP/XX	ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)



10.XXX.XXX.XX	TCP/XX	smtp Postfix smtpd
10.XXX.XXX.XX	TCP/XX	http nginx
10.XXX.XXX.XX	UPD/XXX	rpcbind 2-4 (RPC #100000)
10.XXX.XXX.XX	UPD/XXX	ntp NTP v4 (secondary server)
10.XXX.XXX.XX	UPD/XXX	snmp SNMPv1 server (public)
10.XXX.XXX.XX	TCP/XXX	ssl/http nginx
10.XXX.XXX.XX	TCP/XXXX	ssl/http nginx
10.XXX.XXX.XX	TCP/XXXX	tcpwrapped
10.XXX.XXX.XX	TCP/XXXX	rtsp
10.XXX.XXX.XX	TCP/XX	ssh OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)
10.XXX.XXX.XX	UPD/XXX	rpcbind 2-4 (RPC #100000)
10.XXX.XXX.XX	UPD/XXX	NTP v4 (secondary server)
10.XXX.XXX.XX	UPD/XXX	SNMPv1 server (public)
10.XXX.XXX.XX	TCP/XXXX	tcpwrapped
10.XXX.XXX.XX	TCP/XXXX	mongodb MongoDB 2.5.1 or later

**Table 5: Exposed services from Client's Intranet**

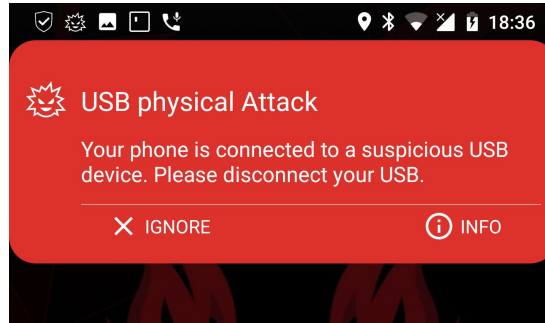


## Attacks detection Analysis and Management Controller Overview

The Kaymera Secure Smartphones were under attack during the Penetration Testing operation. The vendor's application Dashboard was able to detect some attacks such as the ones shown below:

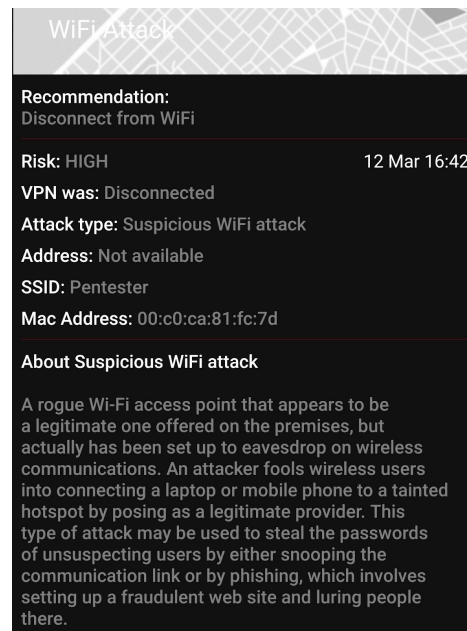
### USB attack – rooting procedure:

During the rooting procedure the Dashboard application was able to detect the malicious use of the USB interface.



### WIFI attack - Rogue AP:

During the Penetration Test activity, the Dashboard application was able to detect a Rogue AP to which the phone was connected. In this case the malicious AP was used for some attacks such as man-in-the-middle and to obtain an interactive shell in the device.

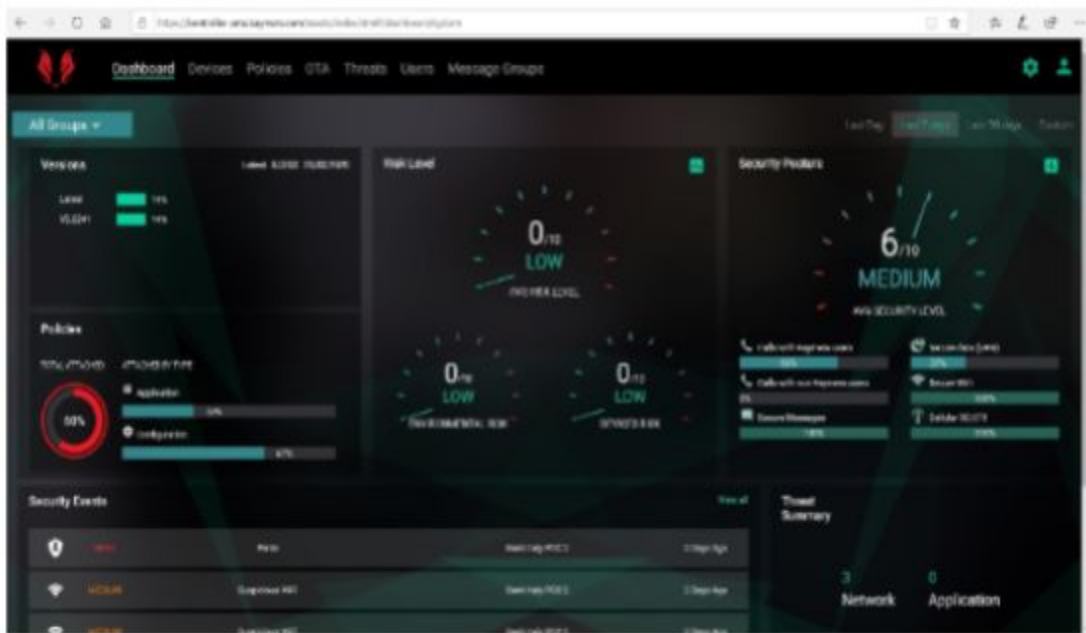




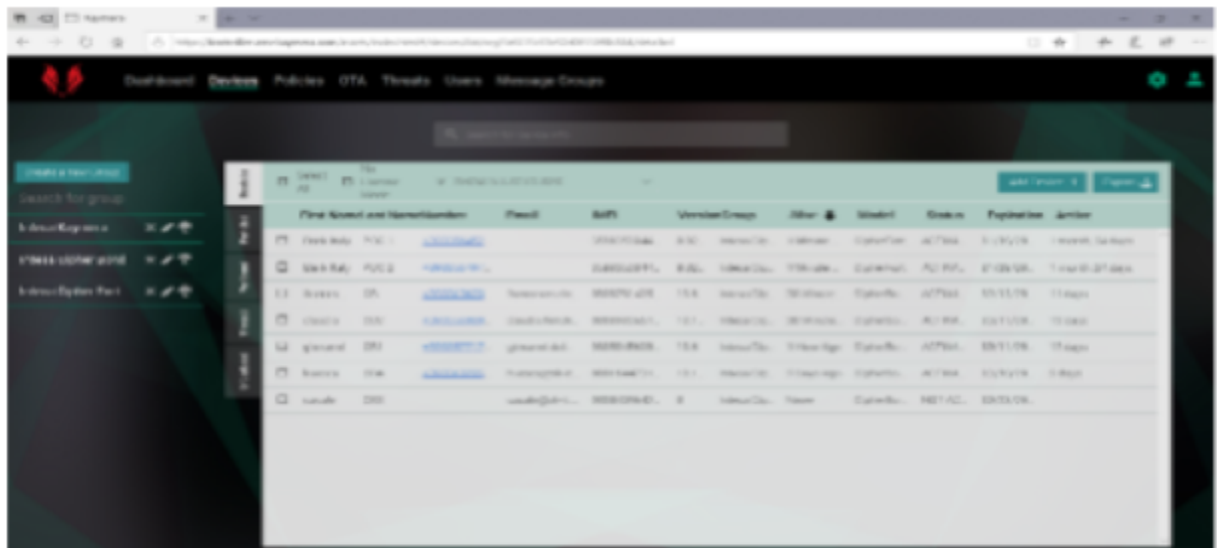
The Vendor provides an online administrative console “Kaymera Kontroller Console” from which an administrative client user is able to customize the Kaymera environment (Kaymera Secure Communications App , Kaymera Encrypted Smartphone, etc) in order to satisfy his organization requirement.

URL: <https://kontroller-amz.kaymera.com/assets/index.html#/dashboard/system>

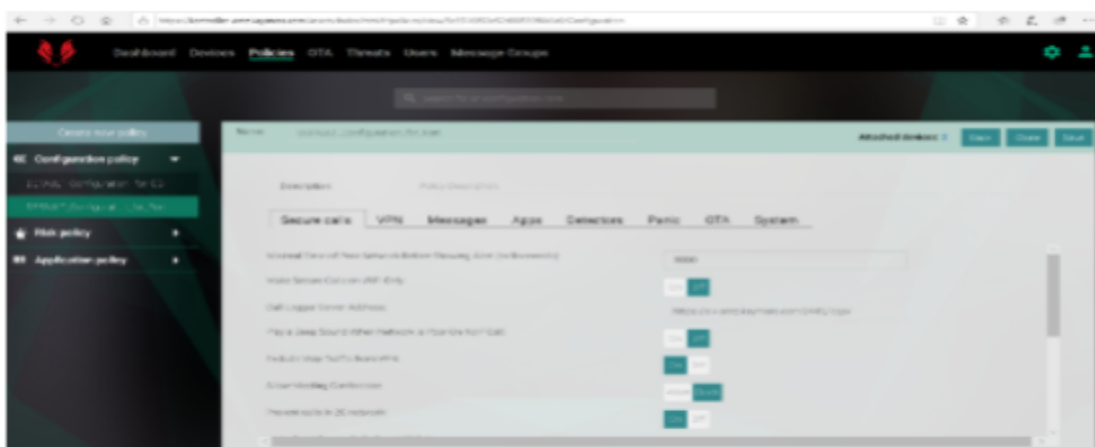
The administrative console uses a robust authentication method composed by the use of an X509 certificate in combination with a username and password authentication mechanism. It also implements a second authentication factor via OTP sent via SMS to the administrative client user. Following the kaymera controller console dashboard.



Registered devices with client’s phone private information “IMEI, email, phone number, etc”.



The Kaymera console allows to apply specific policies for each device or each group of devices:



Following the vendor's software-firmware updates for each devices "Over The Air":



The screenshot shows the 'Device Versions' section of the Kaymera Labs dashboard. It features a table with the following columns: Model, Version, Update Status, Shipping, and Date. The table lists 12 rows of device data.

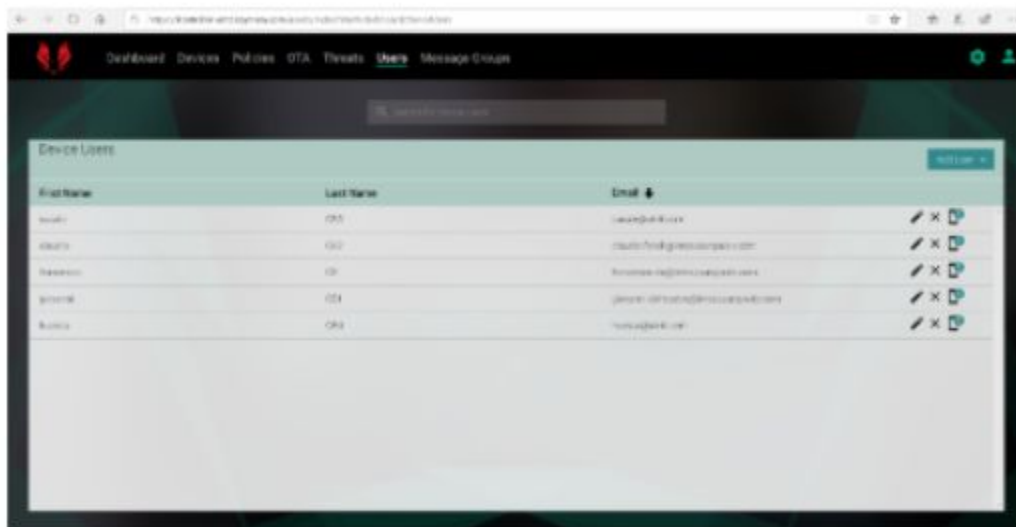
Model	Version	Update Status	Shipping	Date
Pixel 2 XL	8.0.0	0.0%	Pixel 2 XL (Pixel)	21.1
Pixel 2 XL	8	0.0%	Pixel 2 XL (Pixel)	20.1
Pixel 2 XL	8.0.1	0.0%	Pixel 2 XL (Pixel)	20.1
Pixel 2 XL	8.0.0	0.0%	Pixel 2 XL (Pixel)	20.1
Pixel 2 XL	8.0.0	0.0%	Pixel 2 XL (Pixel)	20.1
Pixel 2 XL	8.0.0	0.0%	Pixel 2 XL (Pixel)	20.1
Pixel 2 XL	8.0.0	0.0%	Pixel 2 XL (Pixel)	20.1
Pixel 2 XL	8.0.0	0.0%	Pixel 2 XL (Pixel)	20.1
Pixel 2 XL	8.0.0	0.0%	Pixel 2 XL (Pixel)	20.1
Pixel 2 XL	8.0.0	0.0%	Pixel 2 XL (Pixel)	20.1
Pixel 2 XL	8.0.0	0.0%	Pixel 2 XL (Pixel)	20.1
Pixel 2 XL	8.0.0	0.0%	Pixel 2 XL (Pixel)	20.1

### Security Events detected on the devices:

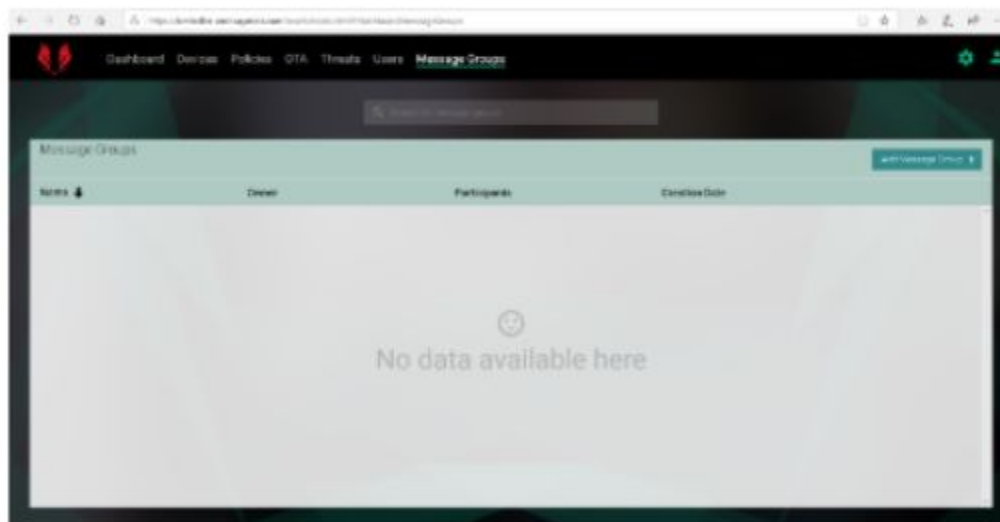
The screenshot shows the 'Security Events' section of the Kaymera Labs dashboard. It features a table with the following columns: Risk, Category, Type, User, and Date. The table lists 4 rows of security event data.

Risk	Category	Type	User	Date
High	Untrusted APK	Untrusted APK	Pixel 2 XL (Pixel)	21 Jan 2021
High	Untrusted APK	Untrusted APK	Pixel 2 XL (Pixel)	21 Jan 2021
High	Untrusted APK	Untrusted APK	Pixel 2 XL (Pixel)	21 Jan 2021
Low	Token	Token	Pixel 2 XL (Pixel)	21 Jan 2021

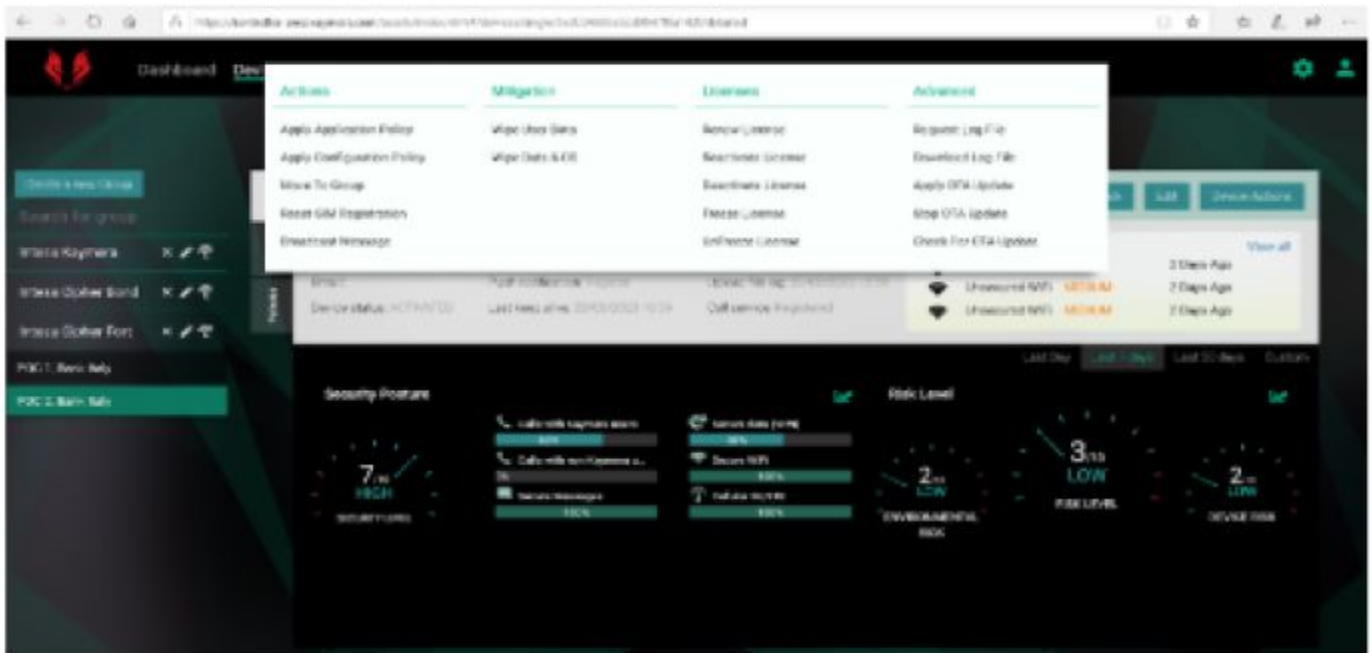
### Registered users for each device:



The Kaymera administrative console allows to send broadcast SMS using the “Message Group” feature:



Following some of the most important operations that an administrative user is able to perform remotely on the kaymera devices.



Some related information for a specific device:







# App Installation & Execution Analysis

App Installation & Execution Analysis aims to analyze app whitelist mechanisms, to evaluate the chance to bypass it and install custom apps to access software/hardware features and data on mobile devices.

## Scope

The activity scope includes the following areas:

- App removal
- App download
- App installation

## Point of Attack

All the activities have been performed through direct access to 2 Google Pixel (Kaymera) devices and using a supporting Kali Linux machine.

## Methodology

Used methodology was divided into different phases:

1. Installed app analysis
2. Security measures bypass

## Tools

In the following a non-exhaustive list of the tools used to perform the activity:

- WiFi Pineapple
- Bettercap
- Hcitol
- Ubertooth One
- ADB

## Installed app analysis

In the following, the list of apps installed on the device. This list includes apps that are surely included into whitelist, but does not include any possible allowed apps not yet installed at device delivery.

Vendor	Software	Versione	Tipologia
--------	----------	----------	-----------



Google	Android Keyboard (AOSP)	7.1	Software Keyboard
Google	Calculator	7.1	Calculator
Google	Calendar	7.1	Calendar
Google	Camera	2.0.002	Camera Management
Google	Chrome	62.0.3202.84	Browser
Google	Clock	4.5.0	Clock
Google	Contacts	1.4.22	Contact Management
Kaymera	Dashboard	296.5dcd244	Kaymera Console
Google	Email	7.1	Email Management
Microsoft	Excel	16.0.8730.2050	Document Elaboration
Google	Files	7.1	File Management
Google	Gallery	1.1.40030	Picture Management
Google	Gmail	7.11.5.177402951.release	Email Management
Google	Google	7.16.19.21.arm64	Google Profile Management
Google	Google Play services	11.9.51 (440-177350961)	Google Services
Google	Google Play services for Instant Apps	2.7-release-179555567	Google Services
Google	Google Play Store	8.5.39.W-all [0] [PR] 178322352	Google Store
Google	Launcher3	7.1	Launcher
Kaymera	Messages	296.5dcd244	Messages Management
MobileIron	MobileIron	9.5.1.11R	Device Management
Google	Music	7.1	Audio Management
9Folders Inc.	Nine	4.1.1b	Email Management
Microsoft	Outlook	2.2.74	Email Management
Kaymera	Phone	3.00.00	Call Management
Microsoft	PowerPoint	16.0.8730.2050	Document Elaboration



Google	Settings	7.1	Device Settings
Google	SIM Toolkit	7.1	SIM Management
Microsoft	Word	16.0.8827.2054	Document Elaboration
Client's	App@Work	n.a.	Client's Store
Microsoft	Skype for Business	6.17.0.7	Corporate Chat

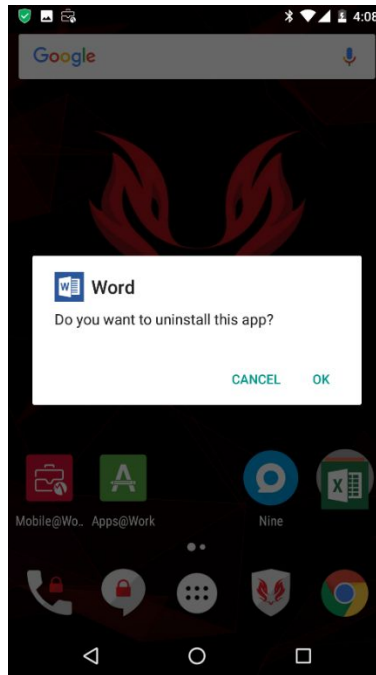
**Table 7: Device Kaymera Softwares**



## Security measures bypass

### App removal

It tested the possibility to uninstall pre-configured apps from the device. Test was performed on the "Microsoft Word" app. No protection mechanism against app removal was detected.



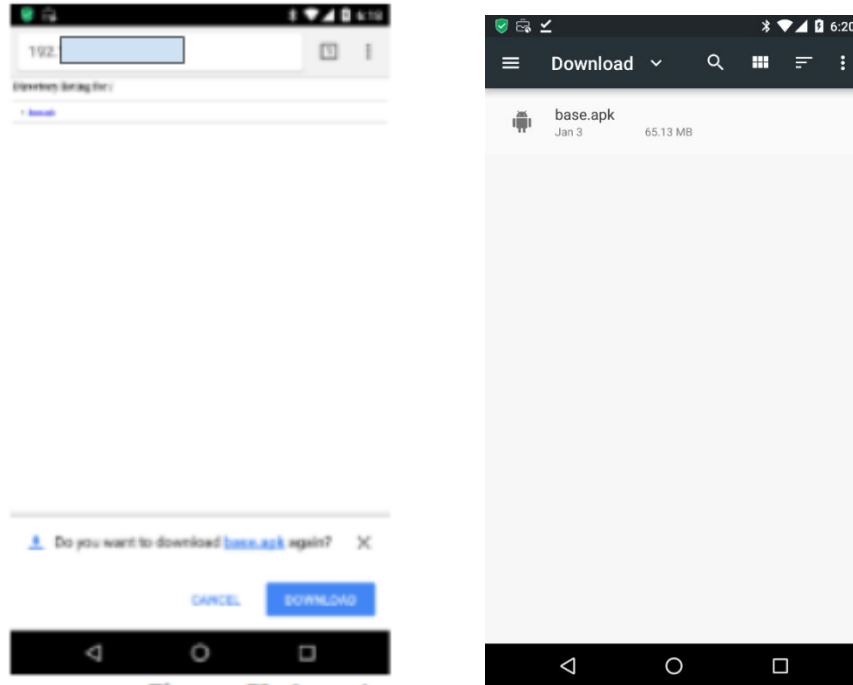
**Whitelisted app removal**

### App download from alternative sources

It tested the possibility to download an app from the browser instead of the official Google Store. Specifically, an app was deployed on a temporary web server on the same device network and it was executed as a download attempt from a mobile device. No protection mechanism was detected against app download from browser.

```
root@kali:~/Desktop/PythonFolder# python -m SimpleHTTPServer 3000
Serving HTTP on 0.0.0.0 port 3000 ...
192.168.1.100 - - [05/Jan/2018 19:34:01] "GET /base.apk HTTP/1.1" 200 -
```

**Web Server creation for browser download**

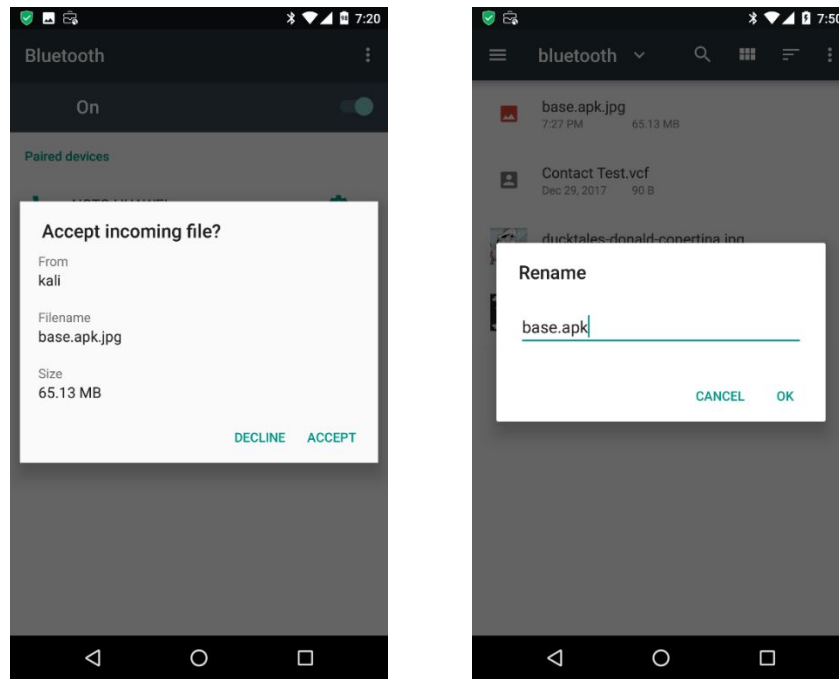


**App download on device**

It tested the possibility to receive an app through Bluetooth. Specifically, the app was sent from a Kali server on the same network of mobile devices using Bluetooth channel. No protection mechanism was detected against app download from Bluetooth, even if file renaming was needed to allow app sending.

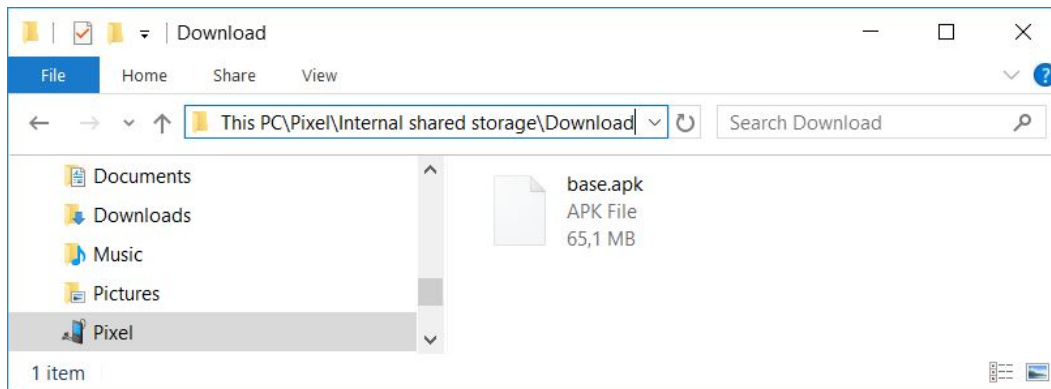
```
root@kali:~/Desktop/PythonFolder# bluetooth-sendto --device=AC:37:43:89:66:A6 ~/Desktop/PythonFolder/base.apk.jpg  
Gtk-Message: GtkDialog mapped without a transient parent. This is discouraged.
```

**App sending through Bluetooth**

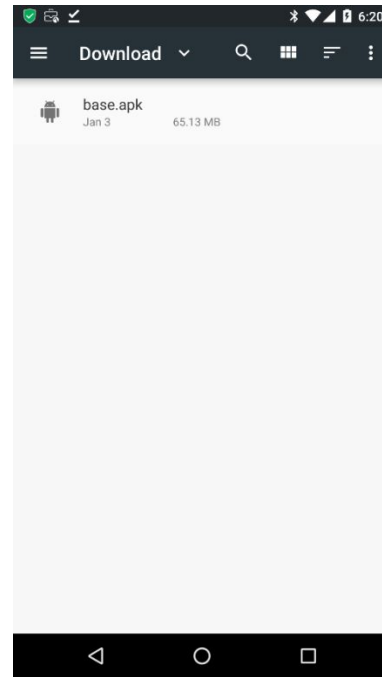
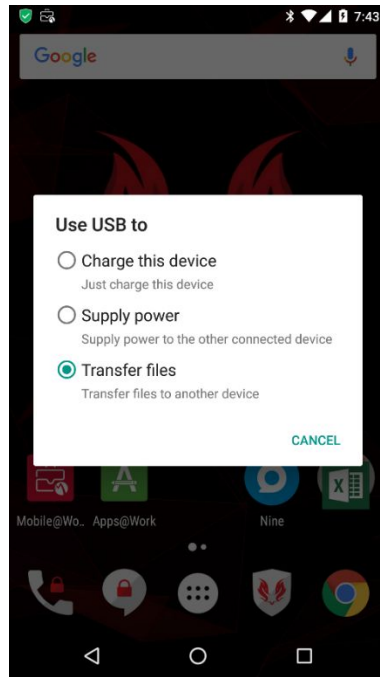


**App download on device through Bluetooth**

It tested the possibility to receive an app through USB transfer. Specifically, the app was transferred from a laptop directly connected to the device through USB. No protection mechanism was detected against app transfer through USB.

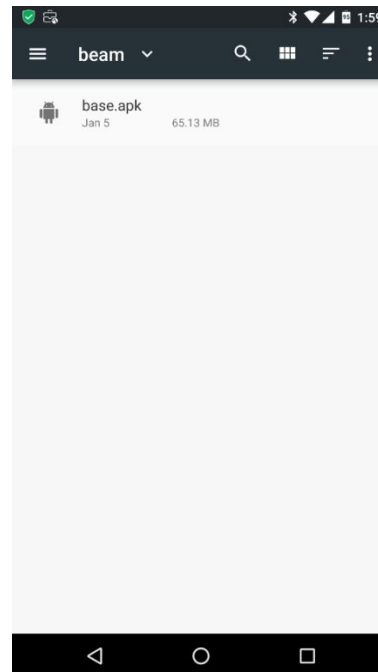
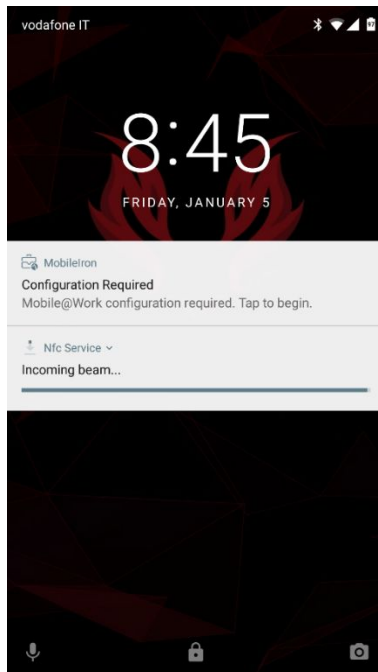


**Device memory**



**App download on device through USB**

The possibility to receive an app through NFC was tested. Specifically, the app was sent through NFC from a device next to the target device. No protection mechanism was detected against app transfer through NFC.



**App download on device through NFC**



## Whitelisted app installation from Google Store

It was tested the possibility to install a whitelisted app – previously removed – from the official Google Play Store. No issue was detected.



Whitelisted app installation from Google Store

## Whitelisted app installation from alternative sources

To verify the possibility to install a whitelisted app from File Explorer instead of the official Google Play Store, the apk of "Microsoft Word " (com.microsoft.office.word.apk) was downloaded and later transferred on Kaymera device. However the installation through File Explorer failed because the apk was not recognised as originated from a known source.





Package name or Google Play URL [Visit Play Store](#)

Package Name: com.microsoft.office.word [Play Store] 

File Size: 65.1 MB

QR Code:  [View](#)

MD5 File Hash: 09f81827ab1a2a3e5353606e526b9291

Last Fetched: 2017-06-14 05:08:54

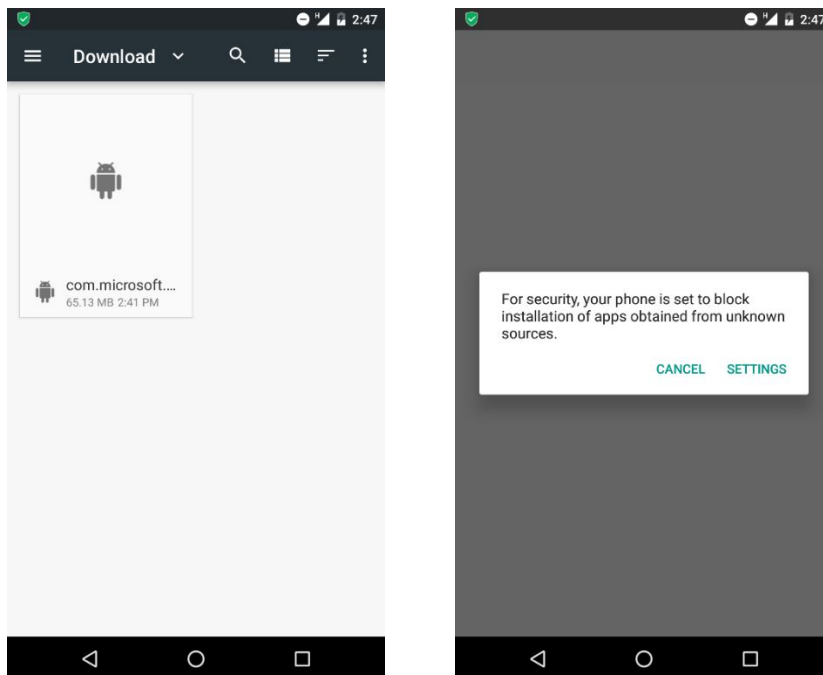
Version: 16.0.8201.1015 (2001406271)

[Generate Download Link](#)

[Click here to download com.microsoft.office.word now](#)

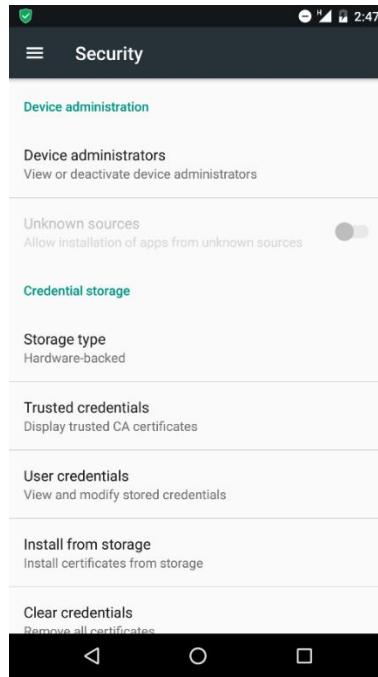
Request Update ▾

### MS Word apk download



### App installation attempt

To install the app it was tried to disable “Unknown sources” configuration from device GUI. This was not possible because the device inhibits the enabling of this feature from the settings menu.



### “Unknown Source” enabling attempt

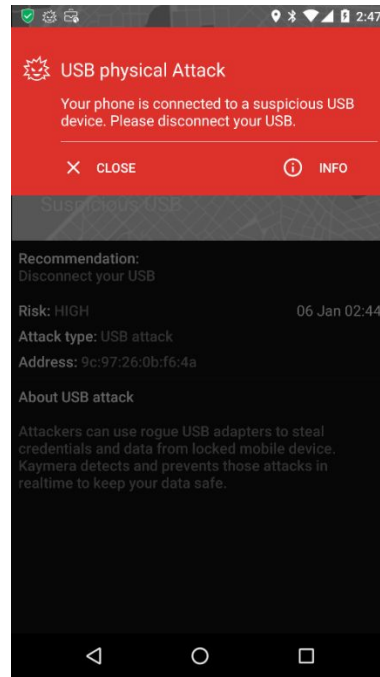
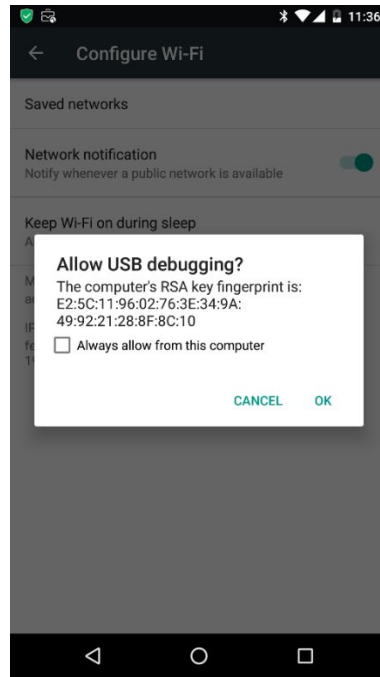
We also tried to enable “Unknown sources” setting through adb. This configuration allows app installation even if not directly downloaded from Google Play Store. However, ADB command was intercepted and blocked by the device.

```
C:\Users\PC-NotoAnonimo>adb devices
List of devices attached
FA69R0300969    unauthorized

C:\Users\PC-NotoAnonimo>adb devices
List of devices attached
FA69R0300969    device

C:\Users\PC-NotoAnonimo>adb shell settings put global install_non_market_apps 1
error: closed
```

### ADB feature enabling

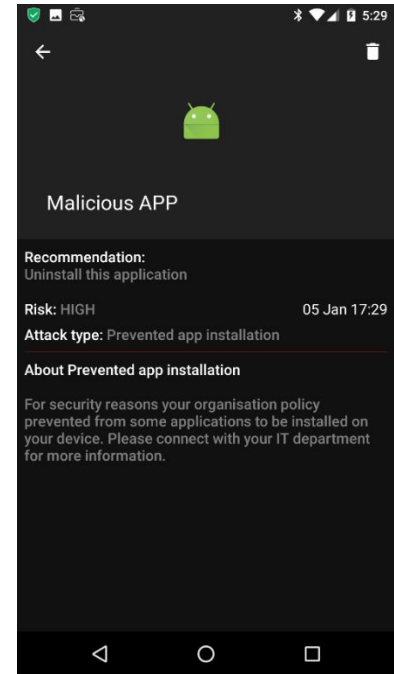
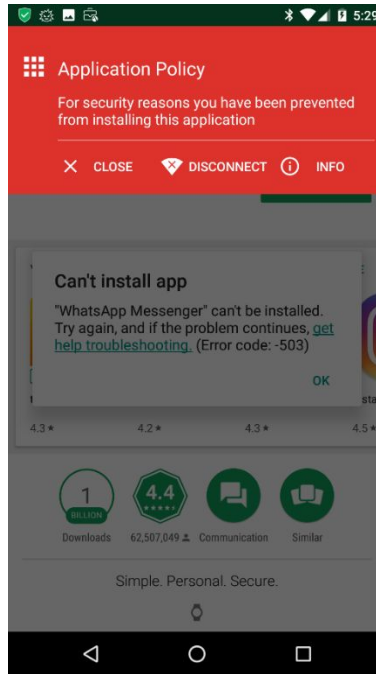
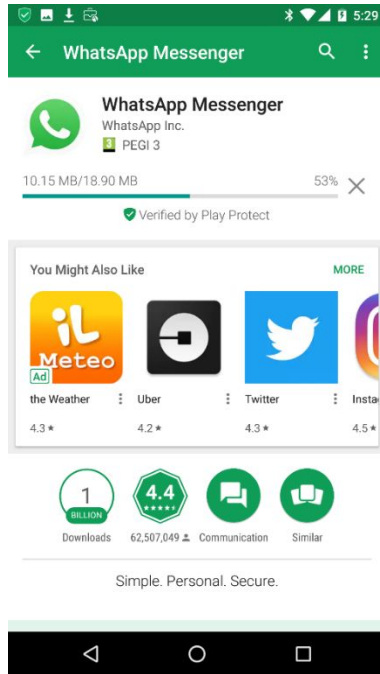


### ADB interception and block



## Non-whitelisted app installation from Google Store

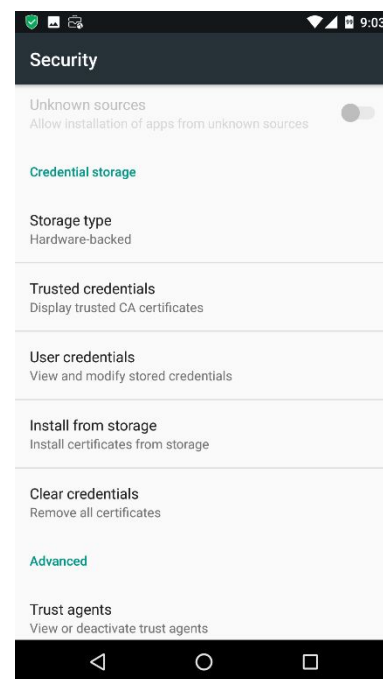
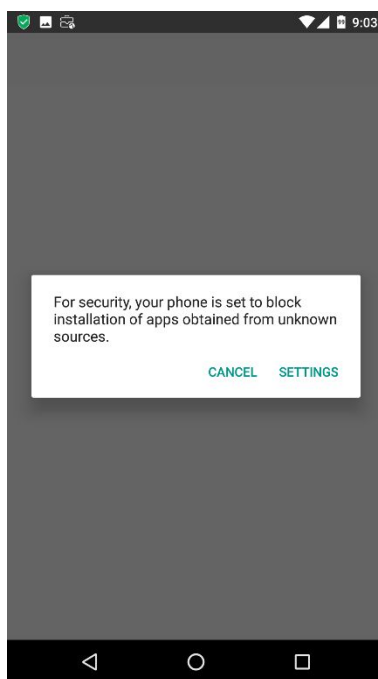
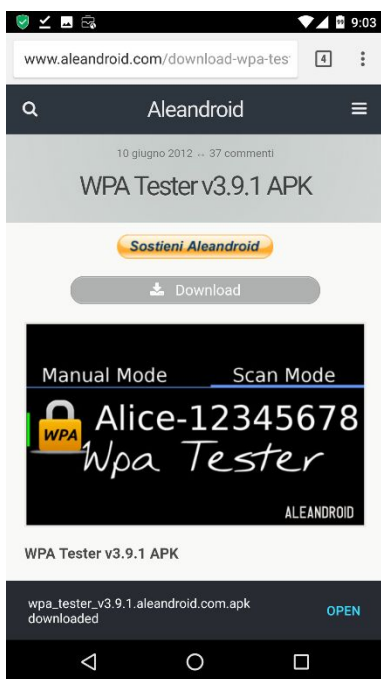
It was tested the possibility to install a not-whitelisted app from different sources. Even if the app is correctly downloaded (e.g. "WhatsApp" in our test), installation attempts are detected and blocked by mobile device.



Non-whitelisted app installation from Google Store

## Non-whitelisted app installation from alternative sources

Non-whitelisted app download from a repository different from Google Play Store is allowed, but, at installation submission, the device is able to detect the "Unknown source" nature of the file and blocks installation attempts.



**Non-whitelisted app installation from alternative sources**

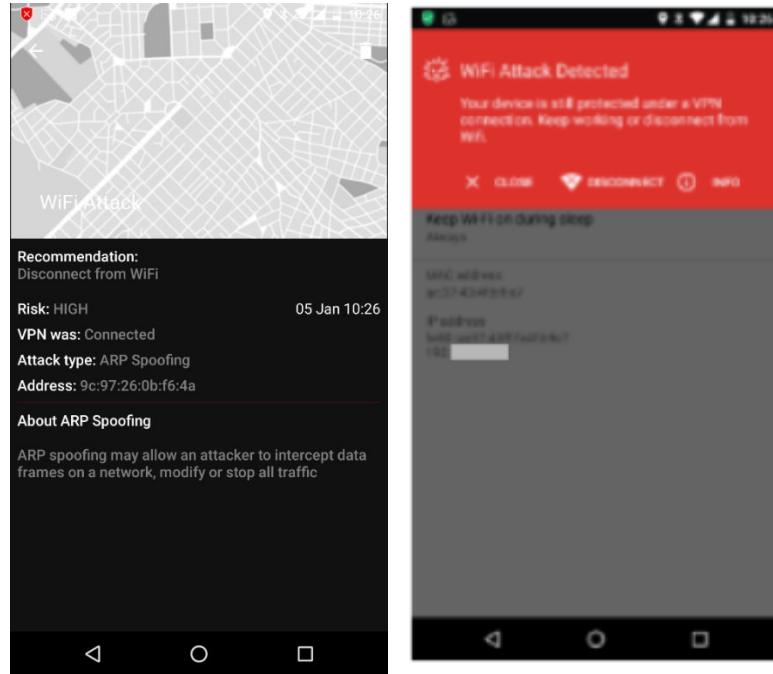
## Google Play Store interception

It was verified the chance to install an app through Man-in-the-Middle attack between device and official Google Play Store ufficiale, intercepting downloaded file and exchanging it with an alternative malicious file. Specifically, the attack was executed through ARP spoofing and requires device and attacker notebook to be in the same network.



**MitM with Google Play Store**

Malicious apk cannot be installed because MitM ARP spoofing is detected and blocked.



**ARP Spoofing detection and block**

## Vulnerabilities

Performed analysis didn't identify any change to bypass current whitelist/blacklist configurations.