Wolf in Sheep's Clothing - Undressed

Virus Bulletin 2018

CSIS

REST ASSURED

www.csis.dk

Wolf in Sheep's Clothing - Undressed

Who's who	Aleksejs Kuprins Benoit Ancel

Wolf in Sheep's Clothing - Undressed

What to expect

1.00 Introduction
2.00 Win32.Agent
3.00 Android.Agent
4.00 IOS.Agent
5.00 Multi-platform-malware
6.00 [SPOILERS REDACTED]
7.00 Victims intelligence
8.00 Toolset

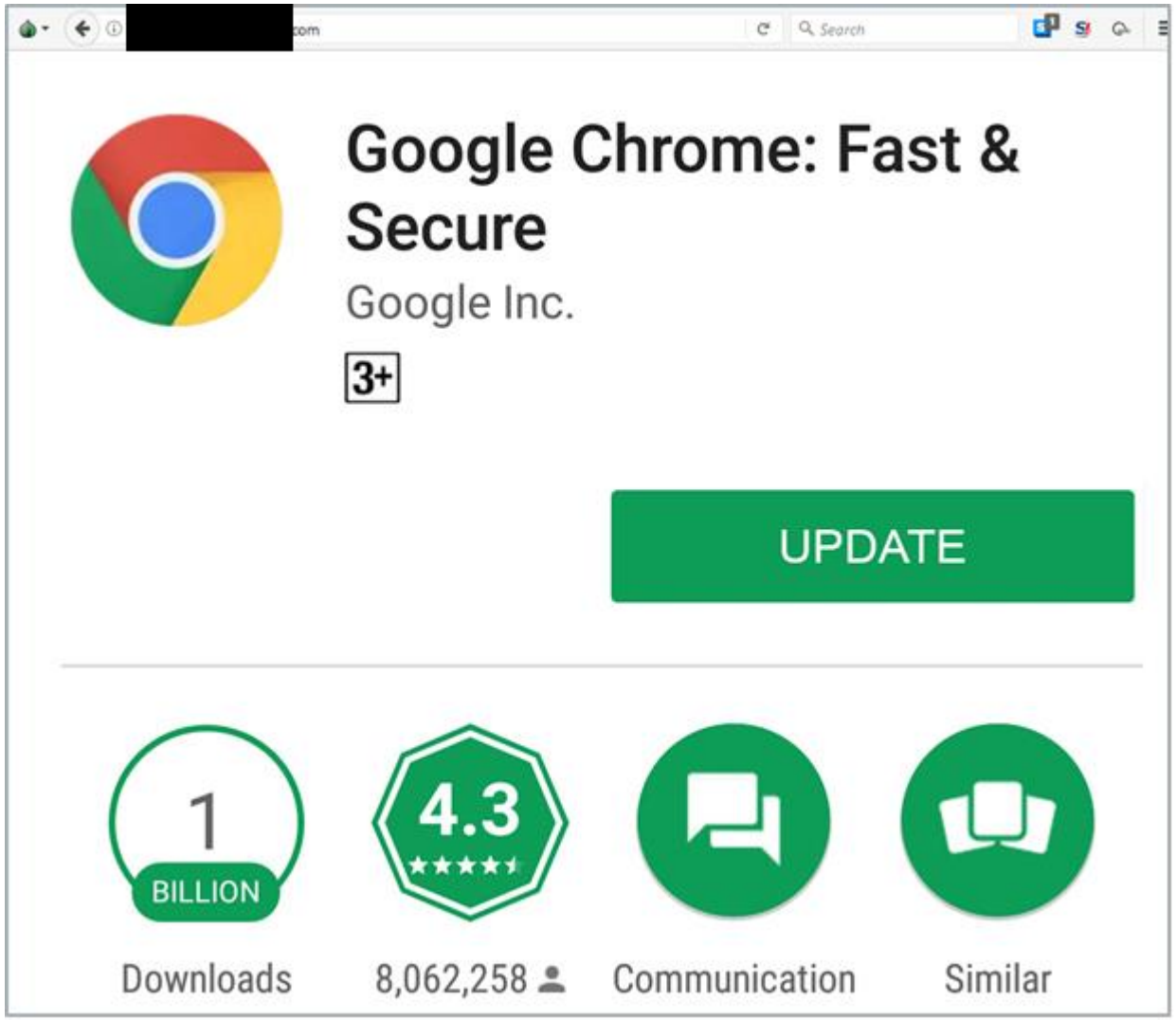
Wolf in Sheep's Clothing - Undressed

1.00
Introduction

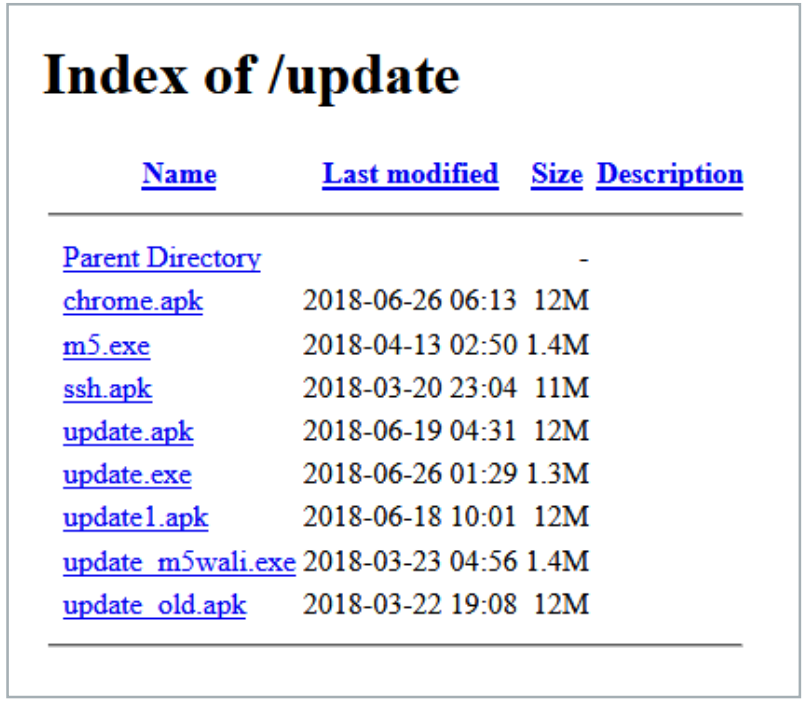
Origin of the research

Investigation around [redacted]
(VPS used for phishing, banking…)

- **1226** domains resolved
- 1 really interesting



- Fake Google Play page acting as dropzone.
- Payloads are selected depending on the User-Agent of the victim:
  - if(/iPhone|iPad|iPod/i.test(navigator.userAgent))
    - i.diawi.com/i3cuz6 (IPA)
  - else if (/Android/i.test(navigator.userAgent))
    - update.apk
  - else:
    - Update.exe



Index of /update

Name	Last modified	Size	Description
Parent Directory		-	
chrome.apk	2018-06-26 06:13	12M	
m5.exe	2018-04-13 02:50	1.4M	
ssh.apk	2018-03-20 23:04	11M	
update.apk	2018-06-19 04:31	12M	
update.exe	2018-06-26 01:29	1.3M	
update1.apk	2018-06-18 10:01	12M	
update_m5wali.exe	2018-03-23 04:56	1.4M	
update_old.apk	2018-03-22 19:08	12M	

Wolf in Sheep's Clothing - Undressed

2.00

Win32.Agent

Win32.Agent

- Update.exe is a RAT for Windows (probably a debug build)
  - The malware is composed of 2 stages:
    - 1- Loader
    - 2- RAT
  - Already on **VT** with good detections

Signature Verification

⚠ A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider.

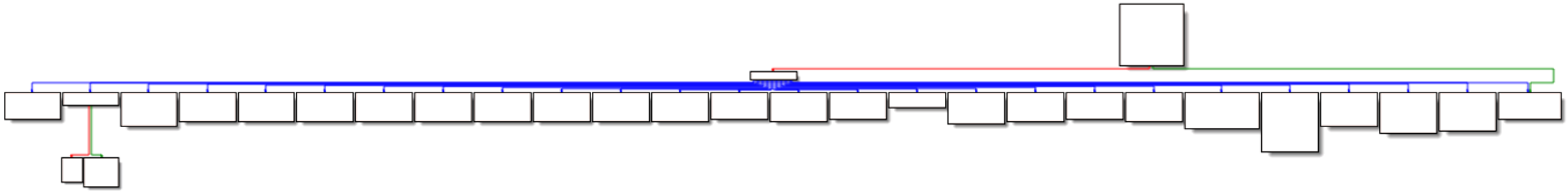
File Version Information

Copyright	Copyright 2017 Google Inc. All rights reserved.
Product	Google Chrome
Description	Google Chrome
Original Name	test.exe
Internal Name	Google Chrome
File Version	67.0.3396.87
Date Signed	1:55 PM 8/3/2018

Win32.Agent.W1_RAT

~ 20 features available, nothing advanced or fancy:

Fingerprint victim	Read file	Rename file	List processes	exec	Screencast
Search files	ls	Delete file	Kill process	Get keylogger logs	Mic
Upload file	Copy file	Create dir	Enum services	Credentials stealers	
Get file size	Move file	Edit timestamp file	Stop service	Autokill	



Wolf in Sheep's Clothing - Undressed

3.00

Android.Agent

Android.Agent

- Not packed (probably debug build)
- Looks like basic android RAT

```
package com.googleservices.utils;

public interface FtpAccess {
    public static final String FTP_FOLDER_PATH = "https://[redacted]/android_panel/ftp_file_uploads/";
    public static final String FTP_PASS = "cluj9090";
    public static final String FTP_USER = "ftpuser";
    public static final String HOST = "[redacted]";
}


package com.googleservices.utils;

public interface API {
    public static final String APP_INFO = "http://[redacted]/android_panel/index.php/api/spy/appInfo";
    public static final String BASEURL = "http://[redacted]/android_panel/index.php/api/";
    public static final String BROWSER_HISTORY = "http://[redacted]/android_panel/index.php/api/spy/browserHistoryInfo";
    public static final String Battery_Level = "http://[redacted]/android_panel/index.php/api/spy/deviceBatteryLevel";
    public static final String CALL_LOG = "http://[redacted]/android_panel/index.php/api/spy/callLog";
    public static final String CONTACT_INFO = "http://[redacted]/android_panel/index.php/api/spy/contactInfo";
    public static final String DEVICE_INFO = "http://[redacted]/android_panel/index.php/api/spy/deviceInfo";
    public static final String DEVICE_STATUS = "http://[redacted]/android_panel/index.php/api/spy/deviceStatus";
    public static final String DEVICE_TOKEN = "http://[redacted]/android_panel/index.php/api/spy/deviceToken";
    public static final String GPS_INFO = "http://[redacted]/android_panel/index.php/api/spy/gpsInfo";
    public static final String OCRMEDIAUPLOAD = "http://[redacted]/android_panel/index.php/api/media/ocrMediaUpload";
    public static final String OCRTRACKAPPS = "http://[redacted]/android_panel/index.php/api/spy/ocrTrackApps";
    public static final String SMS_INFO = "http://[redacted]/android_panel/index.php/api/spy/smsInfo";
    public static final String UPLOADMEDIA = "http://[redacted]/android_panel/index.php/api/media/mediaUpload";
    public static final String WIFI_INFO = "http://[redacted]/android_panel/index.php/api/spy/wifiInfo";
    public static final String deviceNotification = "http://[redacted]/android_panel/index.php/api/spy/deviceNotification";
    public static final String mobileIpInfo = "http://[redacted]/android_panel/index.php/api/spy/mobileIpInfo";
}
```

Android.Agent

- Patchwork of old codes:
  - https://github.com/koush/Screenshot (9yo)
  - https://github.com/murali129/ScreenOCR (1yo)
  - https://github.com/jakubkinst/DEECo-Offload (3yo)

Wolf in Sheep's Clothing - Undressed

4.00

IOS.Agent

IOS.Agent

- Copy paste from:
  - https://github.com/andrealufino/ALSystemUtilities (no longer maintained, 3yo)
  - https://github.com/gali8/Tesseract-OCR-iOS
  - https://github.com/davidmurray/ios-reversed-headers

- Broken application
  - Alpha ?

Wolf in Sheep's Clothing - Undressed

5.00

Multi-platform malware

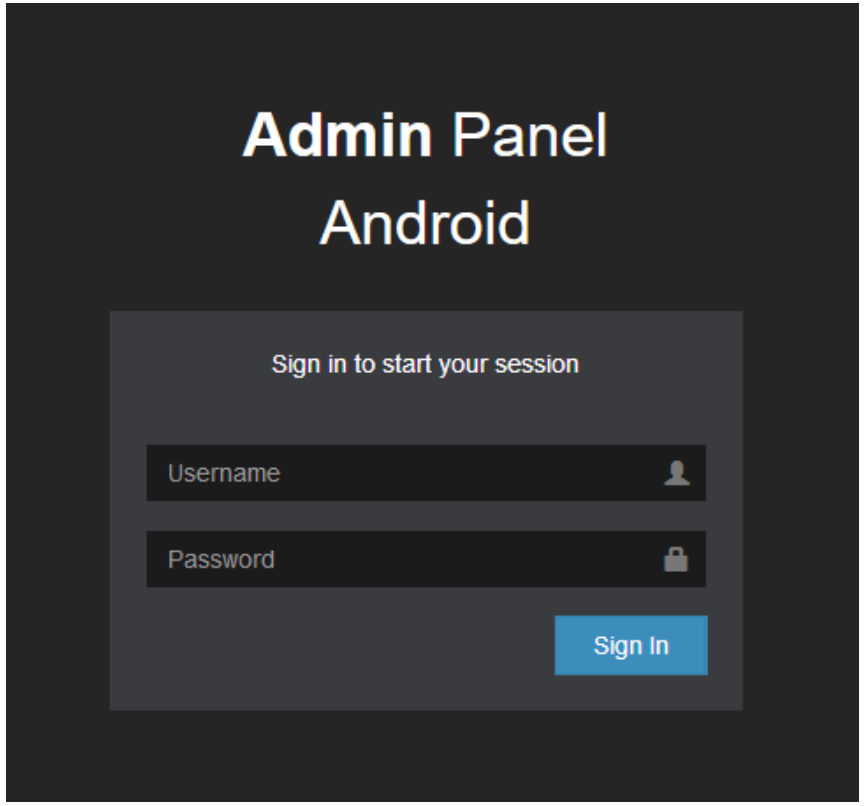
Multi-platform malware

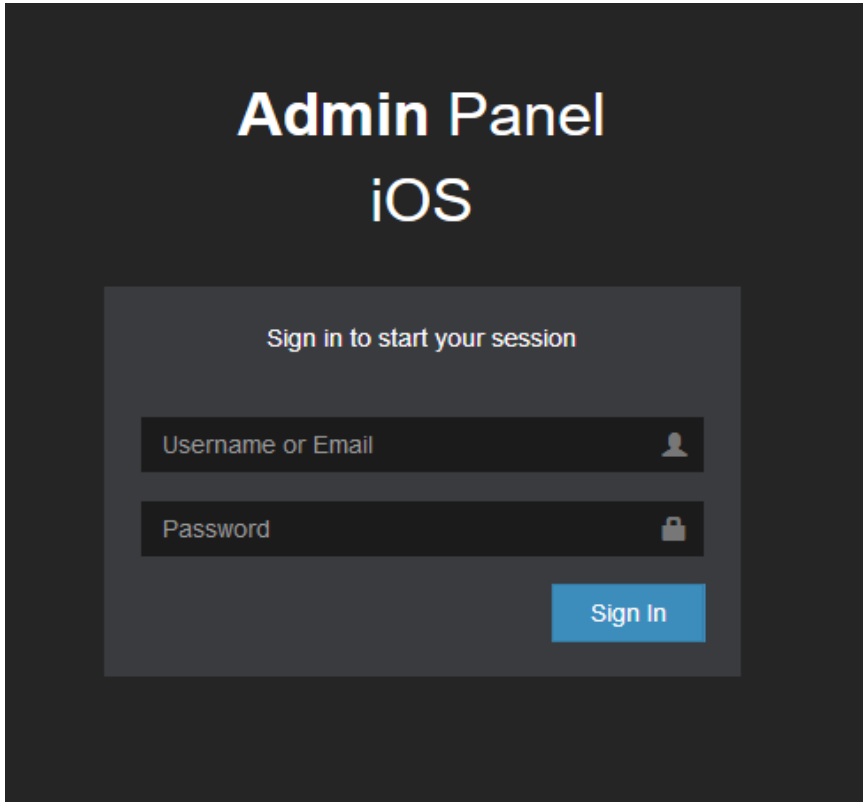
- It looks like somebody tried to have a multi-platform tool
- Lame code (copy paste, bugs, scam app (ios))
- Lame infrastructure

- It looks like an audacious cybercrime actor is trying something.

Aaahh… Panels!

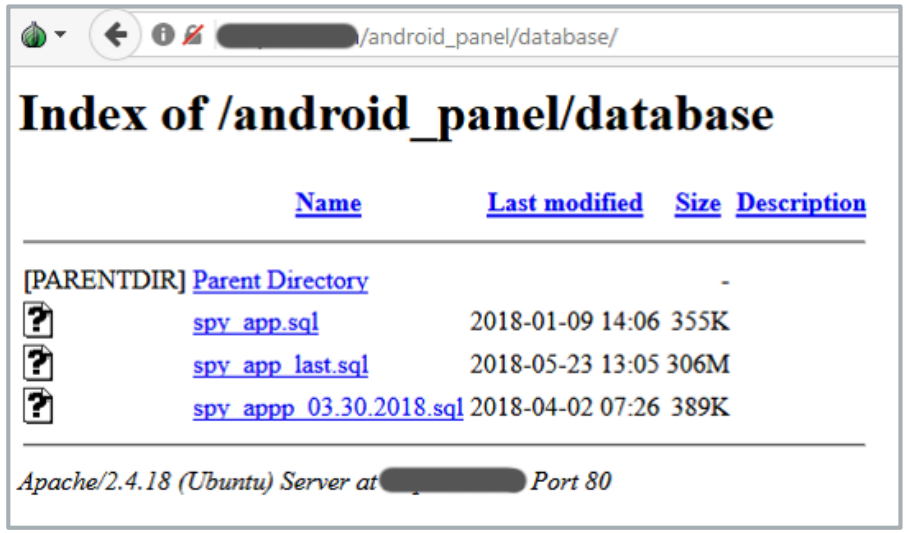
Unknown panels located on the same domain,
used as **C&C** for mobile malware

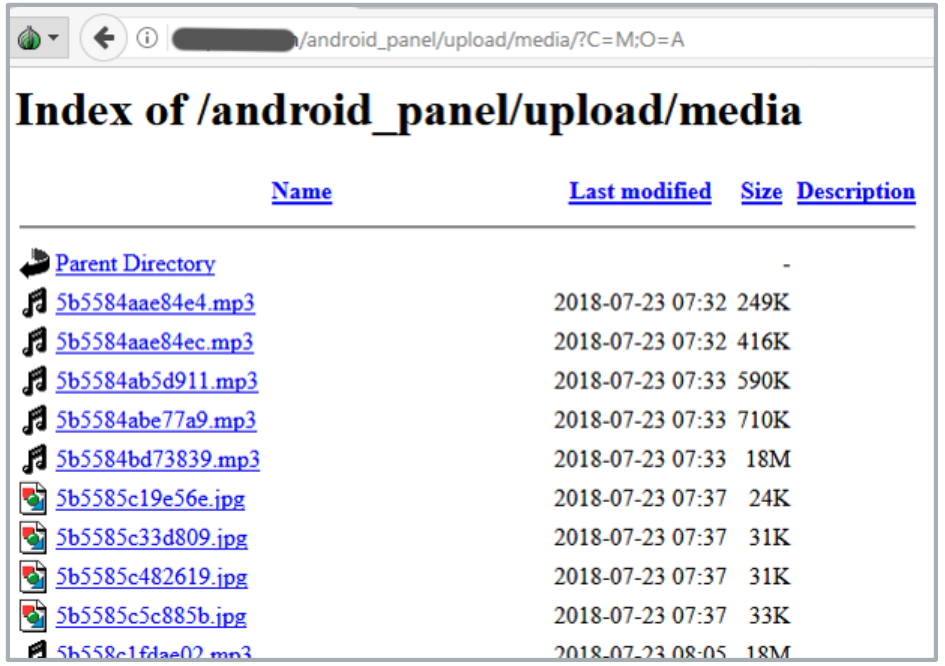




Aaahh… Panels!

Panels entirely open with full backup of databases and all stolen data.



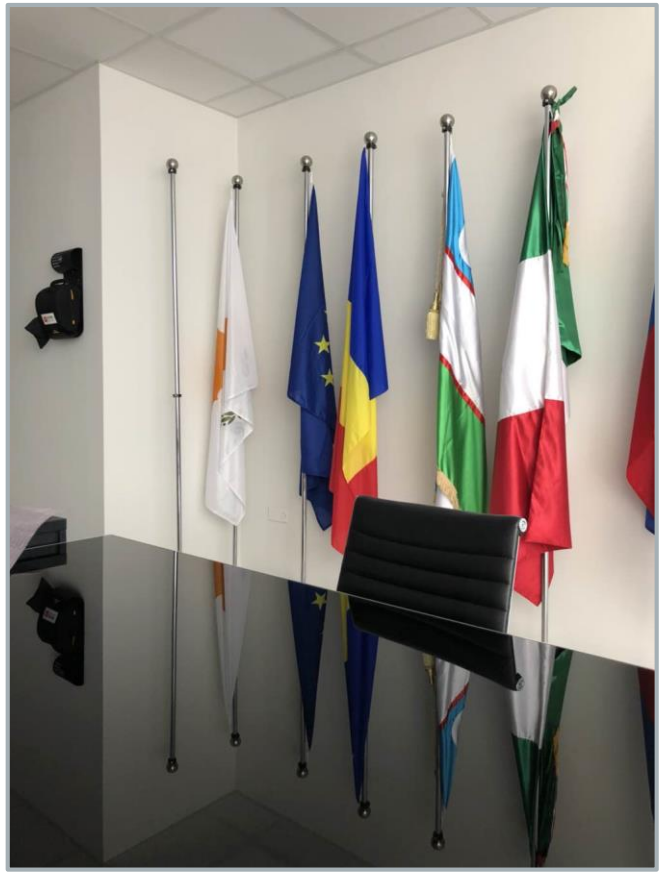


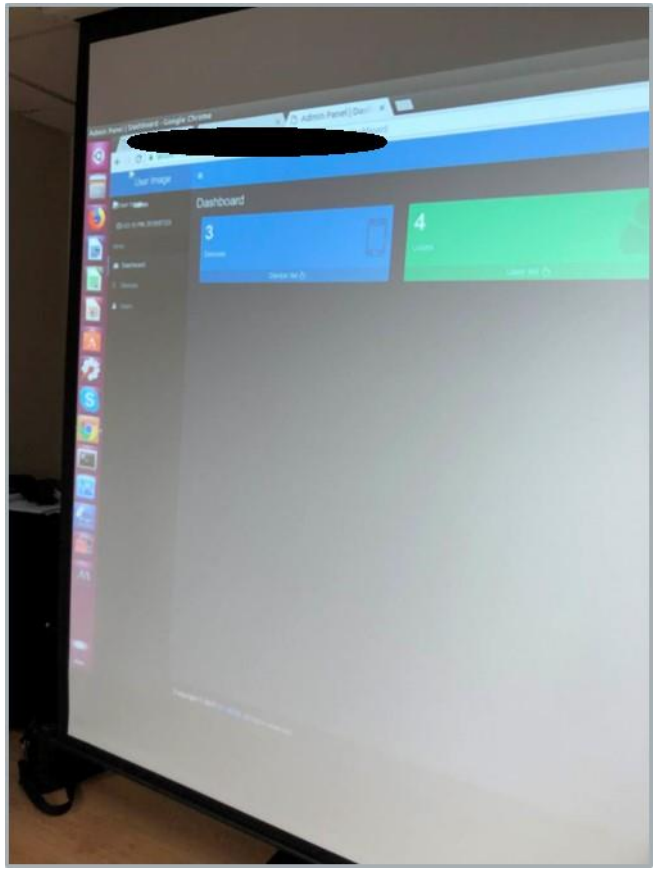
Data!

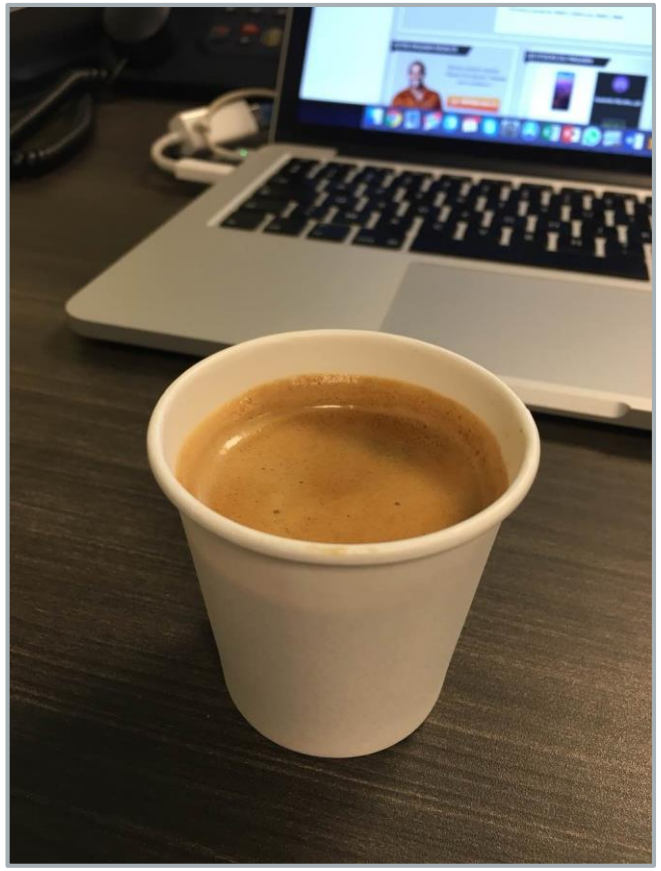
- It’s **~20 Gb** of data available
  - Pictures
  - Audio records
  - Documents
  - Smartphone configuration
  - Everything stolen is available in the databases

Data!

After a quick analysis it’s clear, this actor is interesting.







Wolf in Sheep's Clothing - Undressed

6.00

Kumar Manish, WOLF and the pack

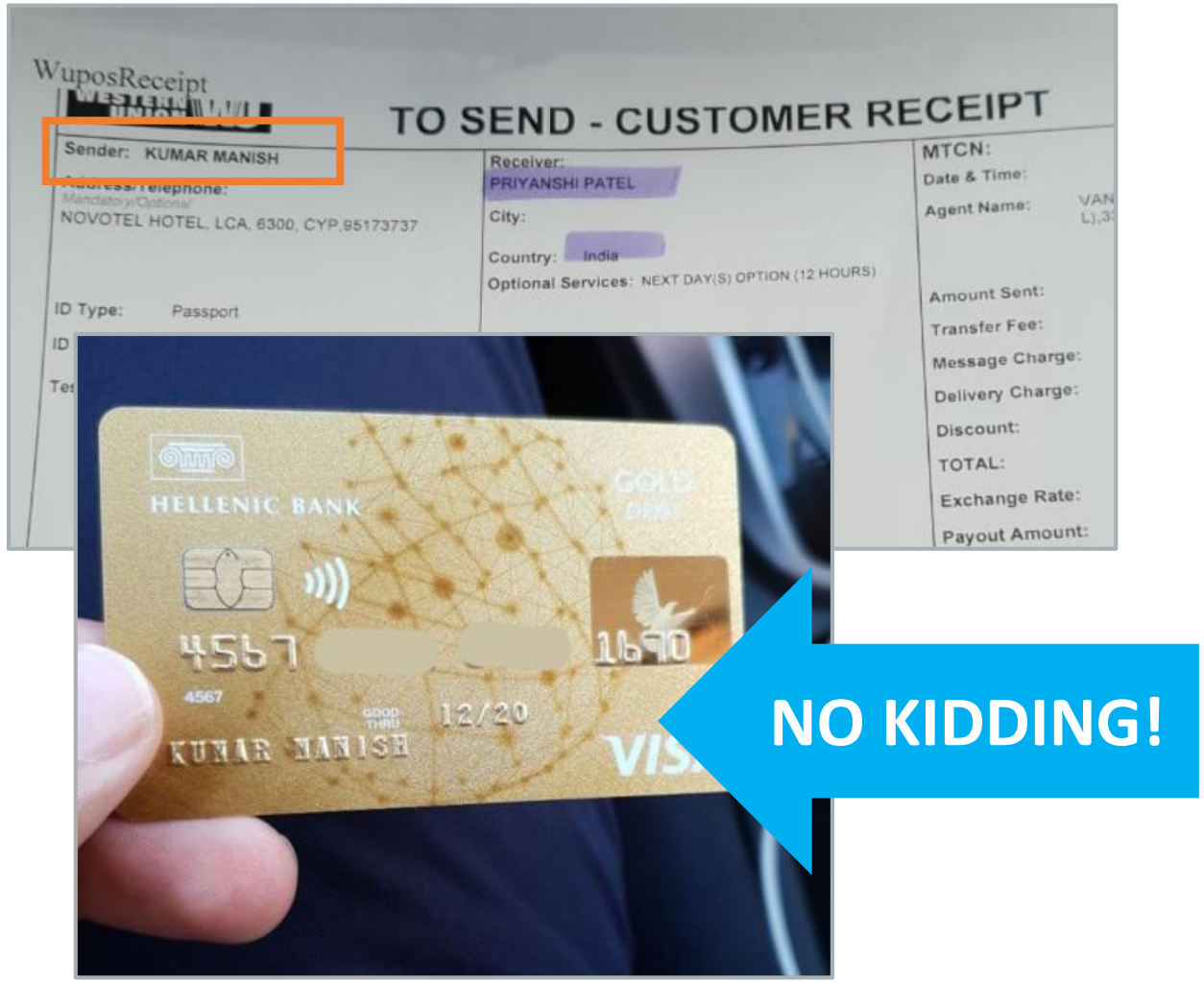
Kumar Manish

CEO of Wolf Research

- All the data point to a man: Kumar Manish from Wolf Research.
  - Fun fact: opendir « website_logo » on the malware C&C with Wolf Research Logo and Kumar Manish Picture

Kumar Manish

CEO of Wolf Research



Wolf Research

- Who is Wolf Research ?

WOLF RESEARCH

Wolf Research develops advanced big data systems, cyber security & AI, and data extraction solutions for the government and homeland security sectors.

HQ in Germany, offices in :**Cyprus**, **Bulgaria**, **Romania**, **India** and (possibly) **US**

Wolf Research

Known stories:

- Motherboard: The Forgotten Prisoner of a Spyware Deal Gone Wrong (Scam attempt against Mauritania Government)
- Forbes: Meet The 'Cowboys Of Creepware' -- Selling Government-Grade Surveillance To Spy On Your Spouse (spouseware business)
- Bloomberg: The Post-Snowden Cyber Arms Hustle
- Hacking Team emails leak

The company's co-founder Manish Kumar is a "criminal of the worst kind," according to ***David Vincenzetti, the CEO of Hacking Team***

- Approximate transcription:
  - “My developers are based in **Romania** at the moment. I am doing all my **development** in Romania. In Puna, in **India** I have develo… Sorry, the TESTING team. Testing. Testers. They are testers, MKAY? So, in India, I don’t do any developments, only **testing**. And these are **my own cousins**, you know, like my **family**, guys and… Because I need trusted people, I cannot give them the payload and they make a mistake, copy, you know and **integrity** is very important. I need to maintain the team. So, its very important, so…”

Wolf Research – leader of the pack

Sub contractors:

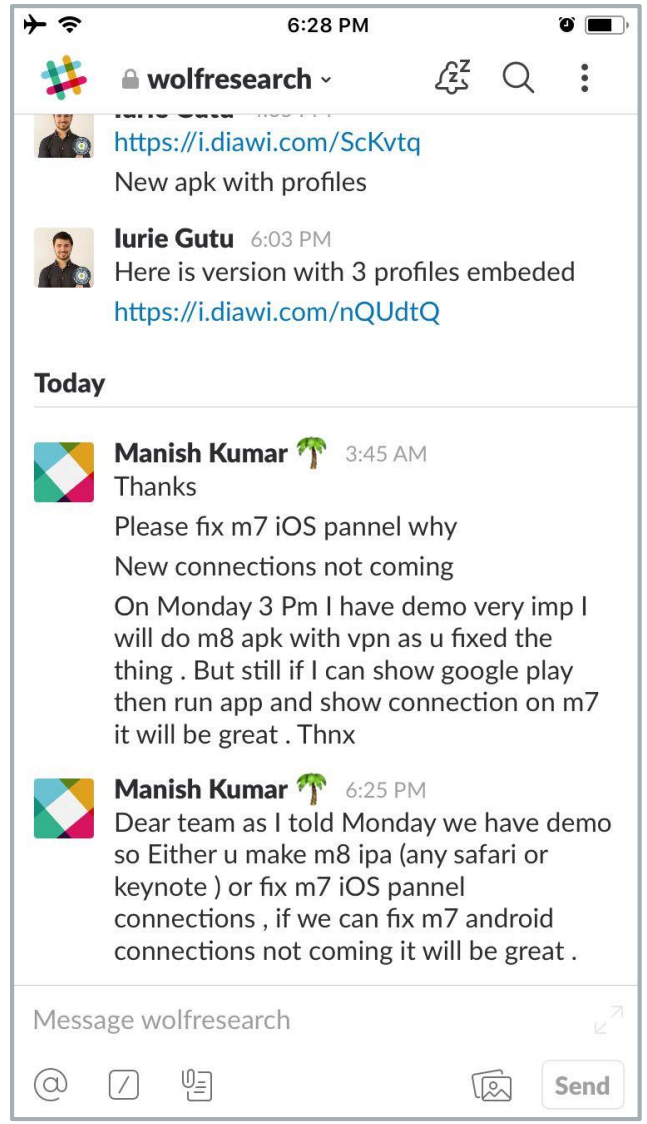
Development based in Romania (Decode.ro)

Testers in India (Puna) (Squarebits)

Dev - Decode.ro

This name appears everywhere: **Iurie Gutu**

- One of developers of IOS/Android malware (with Valentin Brad)
- The apk/ipa malware is invoiced to a Romanian Company: **Decode.ro**



Dev - Decode.ro

Panel and IOS developments

```
commit 1c594f94b3842d9b0787f22310d6a7a151cd804e
Author: Iura <iurie.gutu@decode.ro>
Date:   Tue Jun 19 10:17:04 2018 +0000

    device status

commit f357b4c7df79dffa5bdca898f3febc877caae24b
Author: Iura <iurie.gutu@decode.ro>
Date:   Wed Jun 6 09:11:23 2018 +0000

    screen recording and ocr separatly work

commit f2f4ad46051b01fc85ab810c99702bcec2e4a615
Author: Iura <iurie.gutu@decode.ro>
Date:   Mon Apr 2 07:41:43 2018 +0000

    wording change

commit 6548b54aab544e226abf8a8c4622026098ed7b8f
Author: Iura <iurie.gutu@decode.ro>
Date:   Mon Apr 2 07:23:52 2018 +0000

    css fixes

commit 2eb756ec0c5ef74daa56a3794ed1af4b60df3194
Author: Iura <iurie.gutu@decode.ro>
Date:   Fri Mar 30 14:48:54 2018 +0000

    pic
```

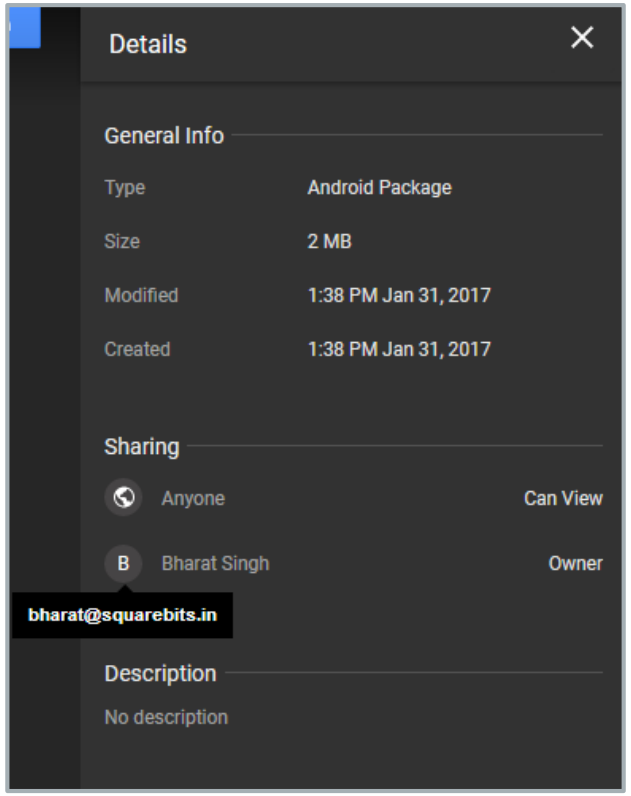
```
<key>ExpirationDate</key>
<date>2019-05-23T10:16:38Z</date>
<key>Name</key>
<string>only manish kb</string>
<key>ProvisionedDevices</key>
<array>
    <string>67dba1c31fa3aa1b543a507a5a2aad5952a79423</string>
    <string>1e89f341d923330e27738e685a8403bc7efa3b85</string>
    <string>fbd7ccb0e975b7d251d8d93b767522275d1f4b11</string>
    <string>dc7a49d7e2bd3d503089d5a814a5f8d1935fac75</string>
    <string>0dce5681b5043b7baab3e9f8d34de17a15664566</string>
    <string>63bb22c57d7dc7a611c804eb50009b343afd45af</string>
    <string>bda6d384eb80802e58e82577190c186ae1b8cdcc</string>
    <string>4ba881fbe6d66164f45681ef4e73503d1bac31a7</string>
    <string>4b0c1ab0b600e94c68fb797e2061b93384f92125</string>
    <string>2a6f096e07fa95b77069e617c001391734748fda</string>
    <string>1c3692f3e2f885e0ca1cdcaf03ec925016be1174</string>
    <string>70fb3010f149760a1937de21b50421b4bd01aa69</string>
    <string>0eb592db96ef328615012f72c9d561466ef73e98</string>
    <string>b274efbee88514ae9a1d96b387a2be16ab6be95c</string>
    <string>40418d7d6847d28a688d9a0fb15a6fd44769c097</string>
</array>
<key>TeamIdentifier</key>
<array>
    <string>PWD7G2H3KX</string>
</array>
<key>TeamName</key>
<string>Decode Software SRL</string>
<key>TimeToLive</key>
<integer>346</integer>
<key>UUID</key>
<string>fefde57c-a2fb-4811-9ad8-f71237323006</string>
<key>Version</key>
<integer>1</integer>
```

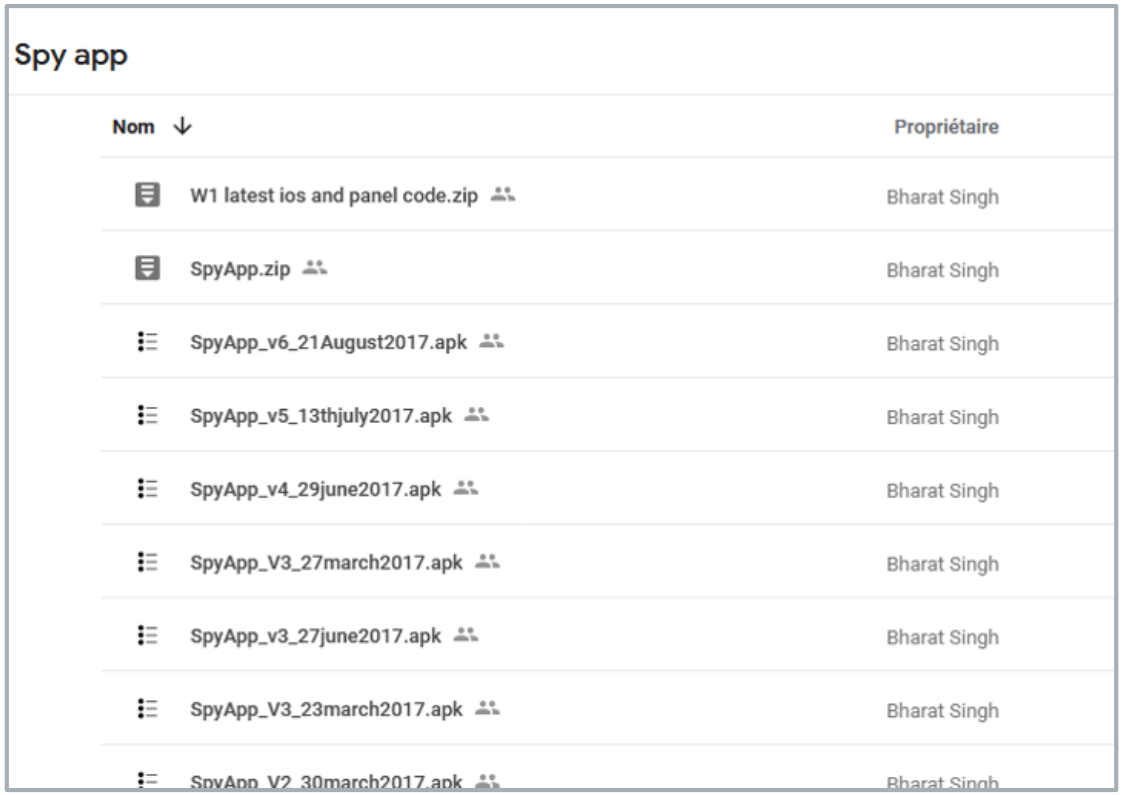
Squarebits

Mobile App Development Company based in India

Squarebits

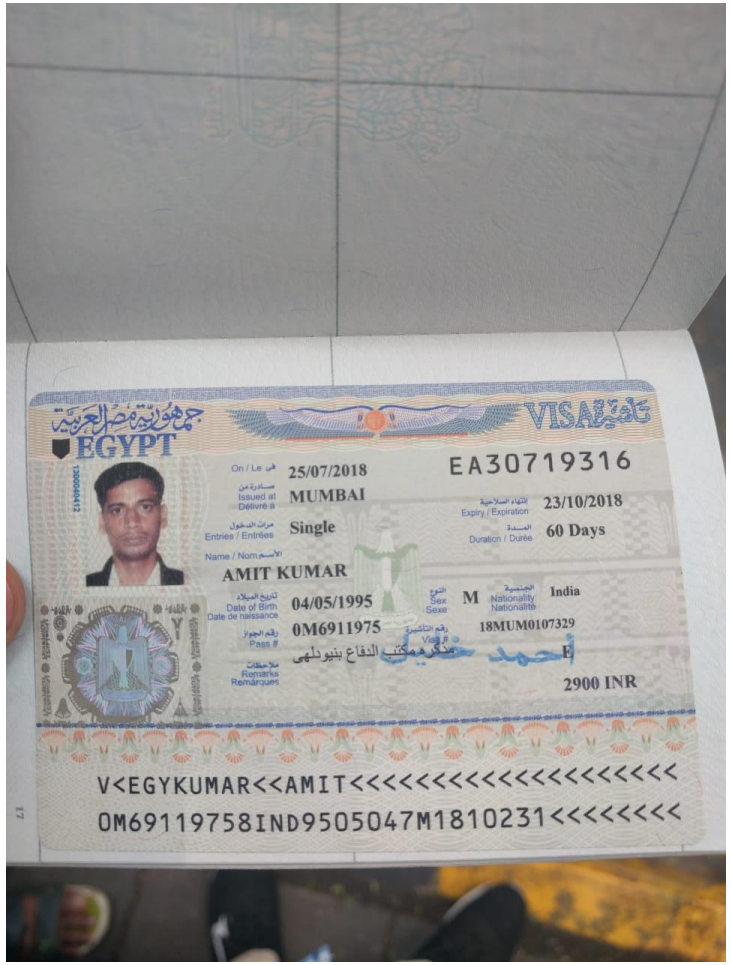
Google drive link found in the database:





Squarebits

THE KUMAR FAMILY



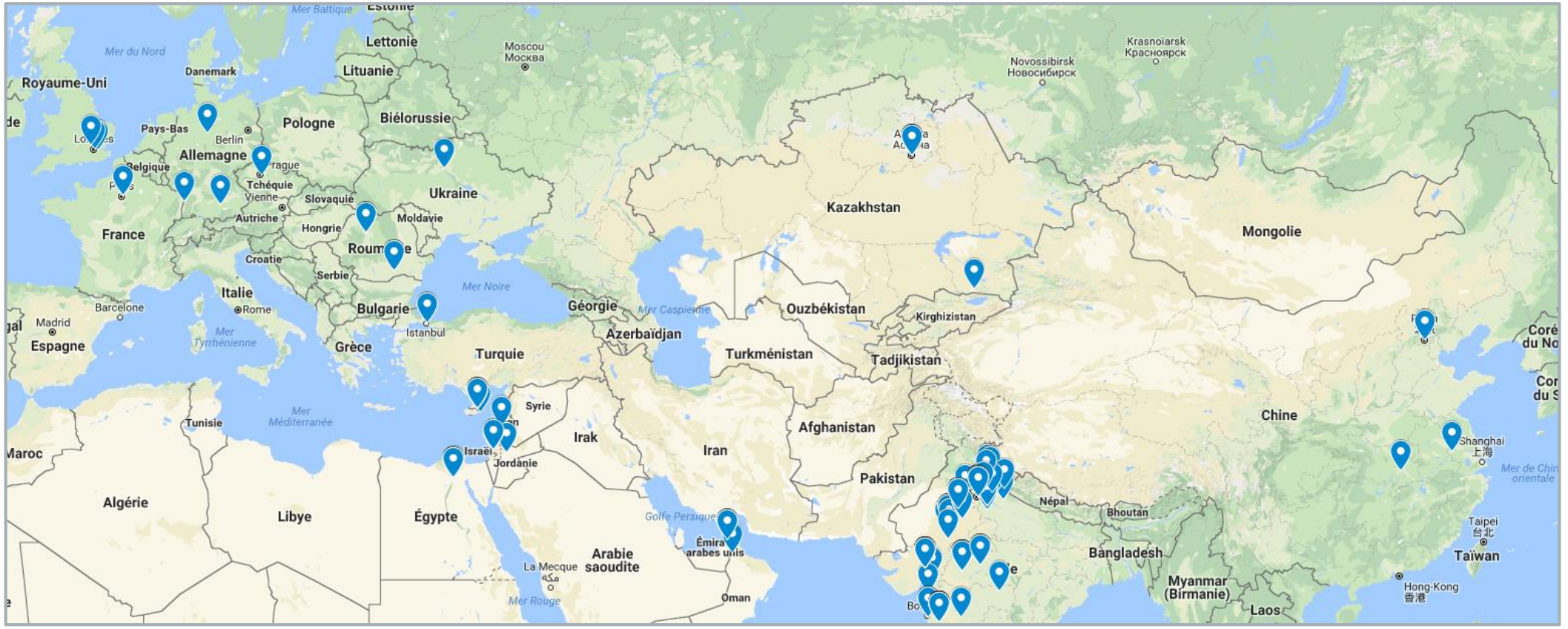
Wolf in Sheep's Clothing - Undressed

7.00
Victims intelligence

Victims intelligence

A true globetrotter

Public IPs based geolocation for the smartphone



Victims intelligence

- Looks like demo smartphone for sellers
- Different actors testing or presenting Wolf Research products

- Key quotes:
  - “You find your targets, you exploit them and after that you can use this kind of system to complete your investigation and have all the information you need”
  - “- We stay in touch ? – Yes, if you need another meeting “
  - “This is a test for a customer”

- “This is a test for our customer, how are you ? Good? […] It’s not too long this morning?”

Nexa

- Many calls/SMS from +336 numbers (France, mobile phone) in the database
- **French audio records**
- 90.102.1.97 used by the smartphone (registrant **rlh@nexatech.fr**)
- SMS in the database:

  « DHL EXPRESS from NEXA TECHNOLOGI is scheduled for delivery TODAY by End of Day. Track at … »
- A strange apk called « **Nexa Tracker** »
- Personal phone number used by a **Nexa VIP**

- Key quote:
  - “Allo, oui bien sur, ça va ? […] Je me parle tout seul”
  - “Hi, how are you ? I’m just talking to myself”

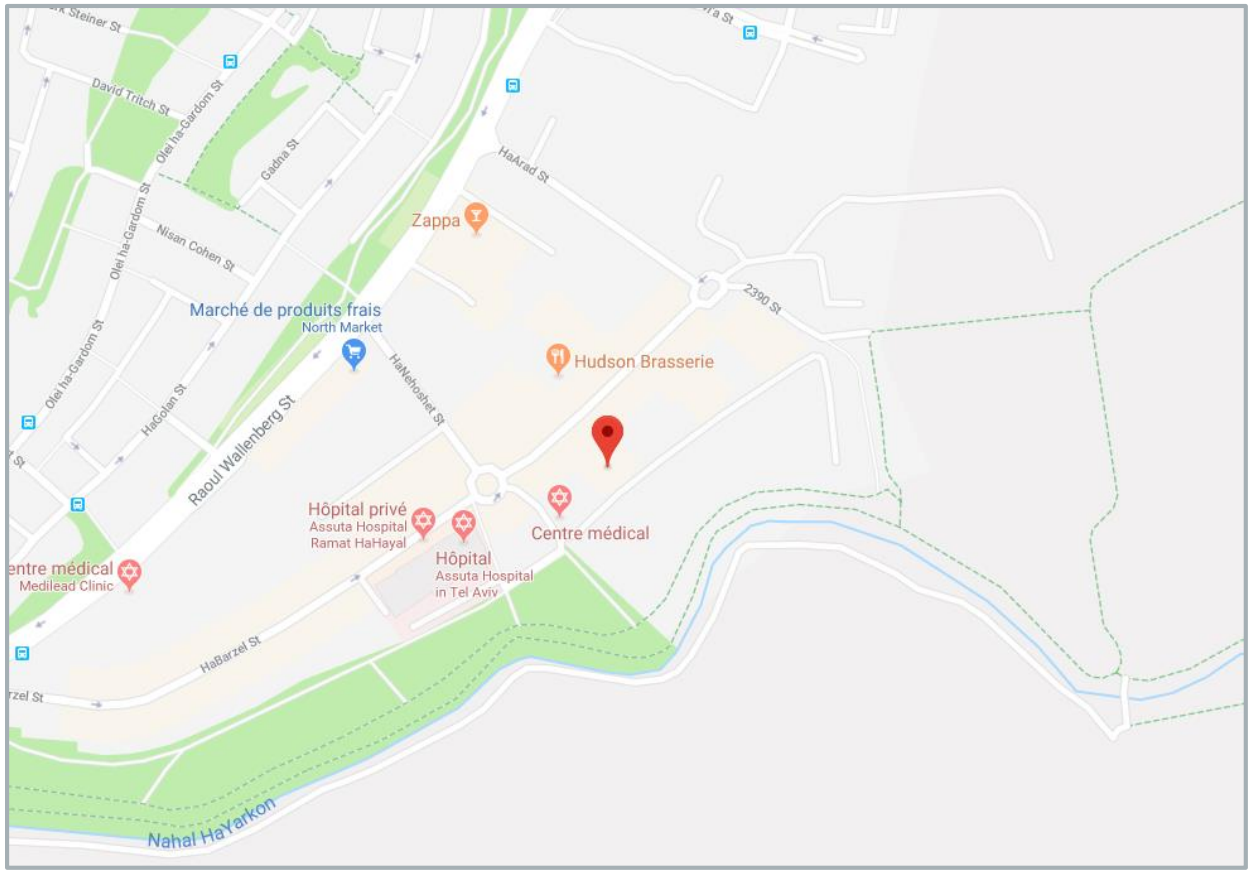
WiSpear

WIFI INTERCEPTION AND SECURITY SOLUTIONS

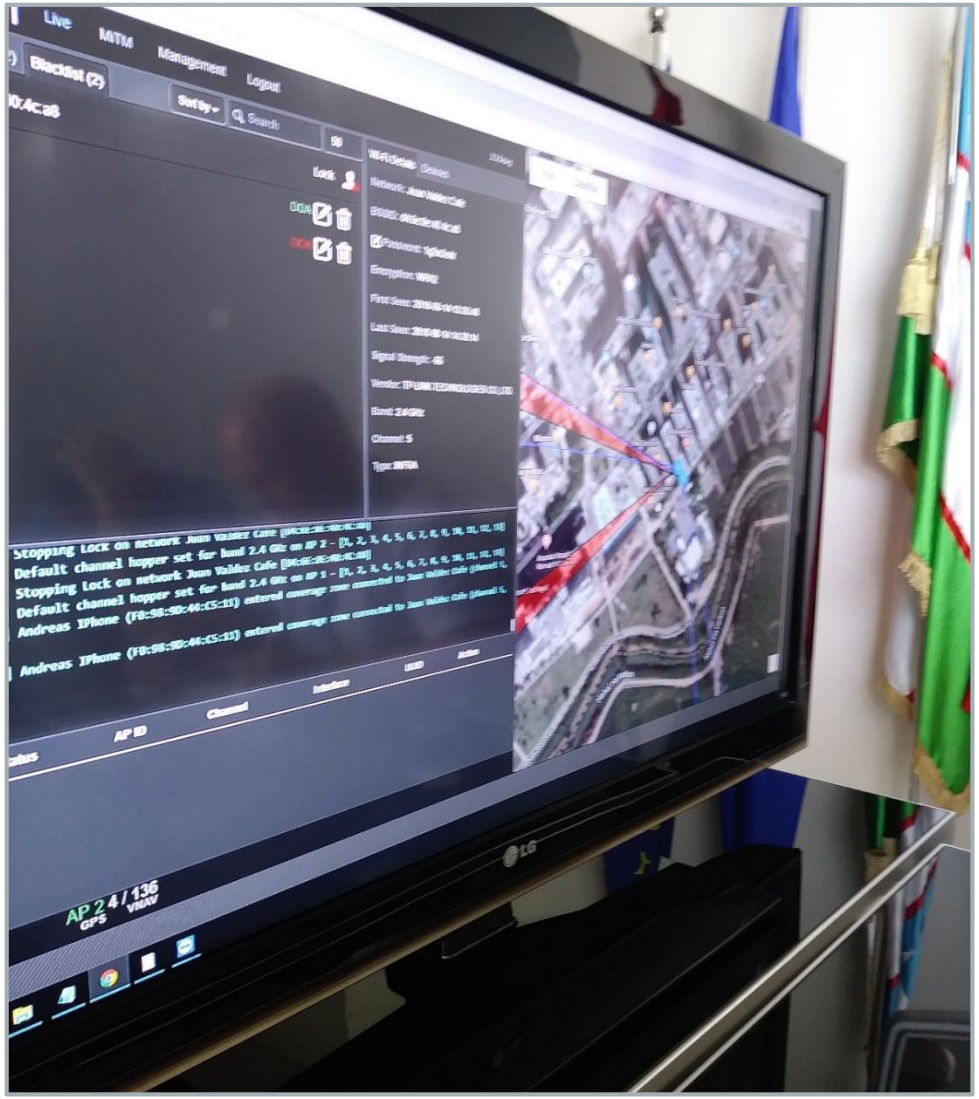
- Interesting connection:
  - Can be an attack vector
  - (Very) Big company in WIFI interception
- Interesting data
  - You don’t see WiSpear tools every days ☺
- Proof:
  - Smartphone named “Wispear”
  - Geolocation
  - Pictures

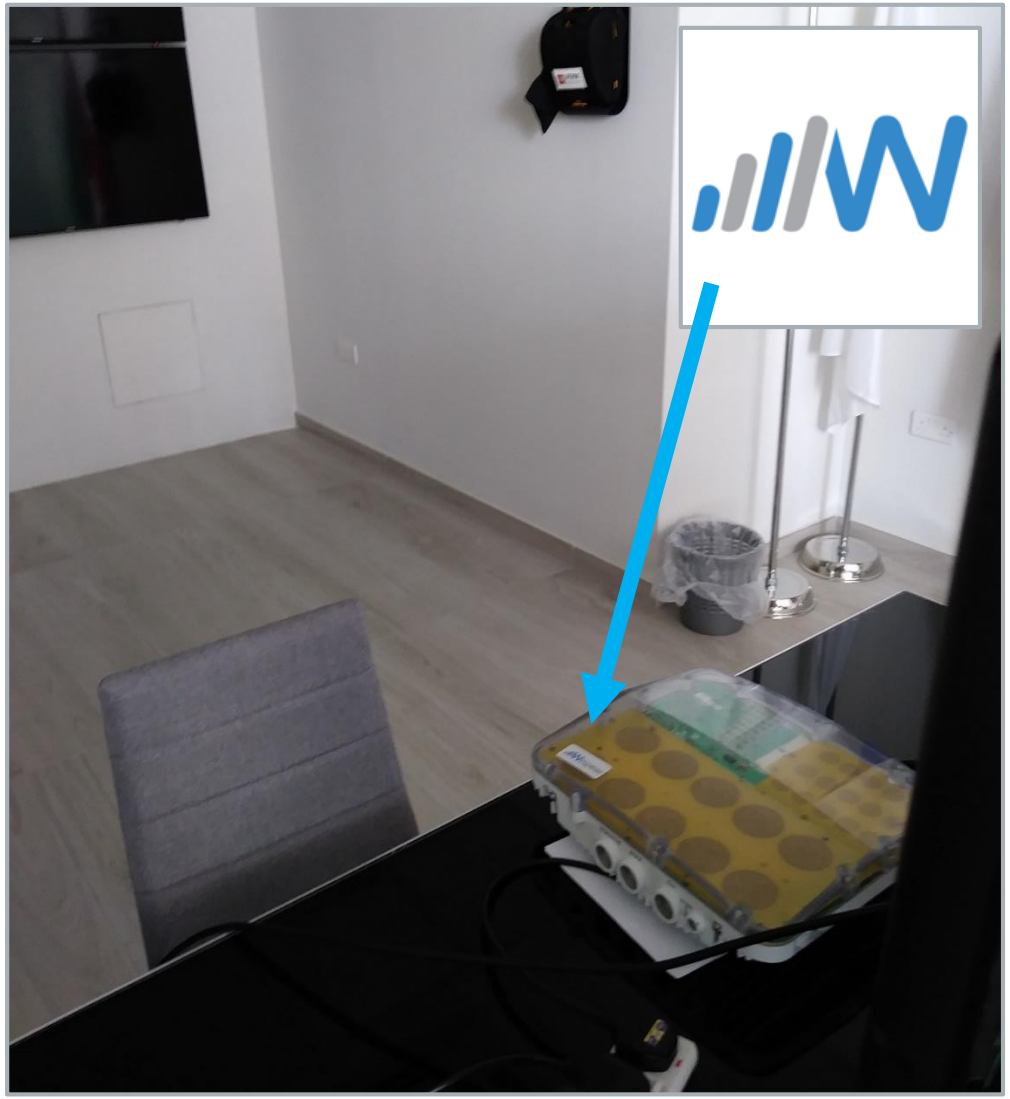
WiSpear


2018-06-27 09:36:05 | Running Time
2018-06-27 09:36:08 | Running Time:
2018-06-27 09:36:11 | Running Time:
2018-06-27 09:36:15 | Running Time:
2018-06-27 09:36:17 | Running Time:
2018-06-27 09:36:23 | Stopping MITM
2018-06-27 09:36:23 | Default channel
AP 1 1 / 48
GPS VNAV


Steiner St
David Tritch St
Olei ha-Gardom St
Gadna St
HaArad St
Zappa
Nisan Cohen St
2390 St
Marché de produits frais
North Market
Hudson Brasserie
HaGolan St
HaNehoshet St
Raoul Wallenberg St
Hôpital privé
Assuta Hospital
Ramat HaHayal
Centre médical
Hôpital
Assuta Hospital
in Tel Aviv
Medilead Clinic
HaBarzel St
Nahal HaYarkon

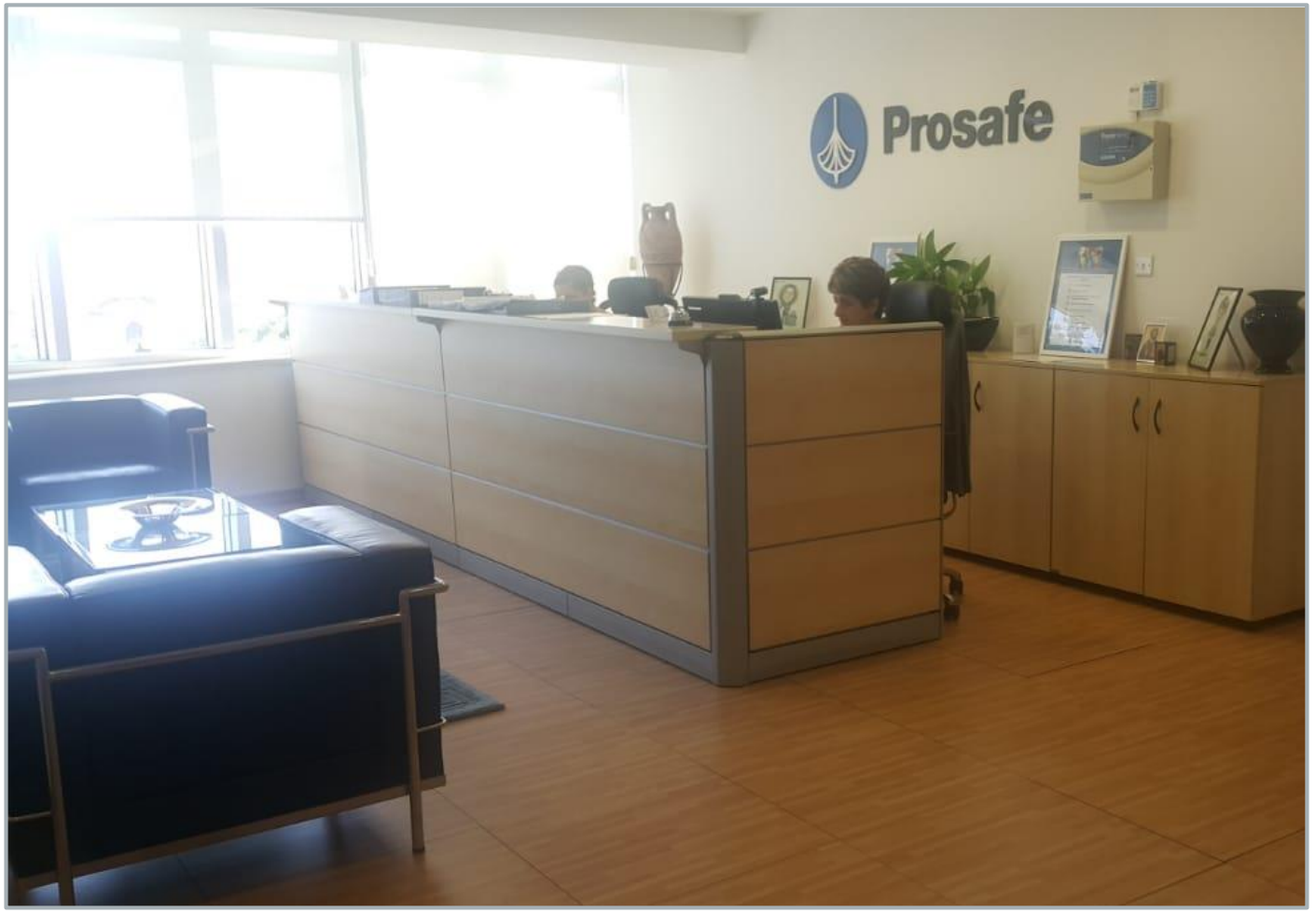
WiSpear


Live
MITM
Management
Logout
Blacklist (2)
Stopping Lock on network Juan Valdez Cafe
Default channel hopper set for band 2.4 GHz on AP 2 - [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13]
Stopping Lock on network Juan Valdez Cafe
Default channel hopper set for band 2.4 GHz on AP 1 - [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13]
Andreas IPhone (F0:98:9D:44:C5:11) entered coverage zone connected to Juan Valdez Cafe (Channel 5,
Andreas IPhone (F0:98:9D:44:C5:11) entered coverage zone connected to Juan Valdez Cafe (Channel 5,
Status
AP ID
Channel
Interface
UUID
Action
AP 2 4 / 136
GPS
WAV



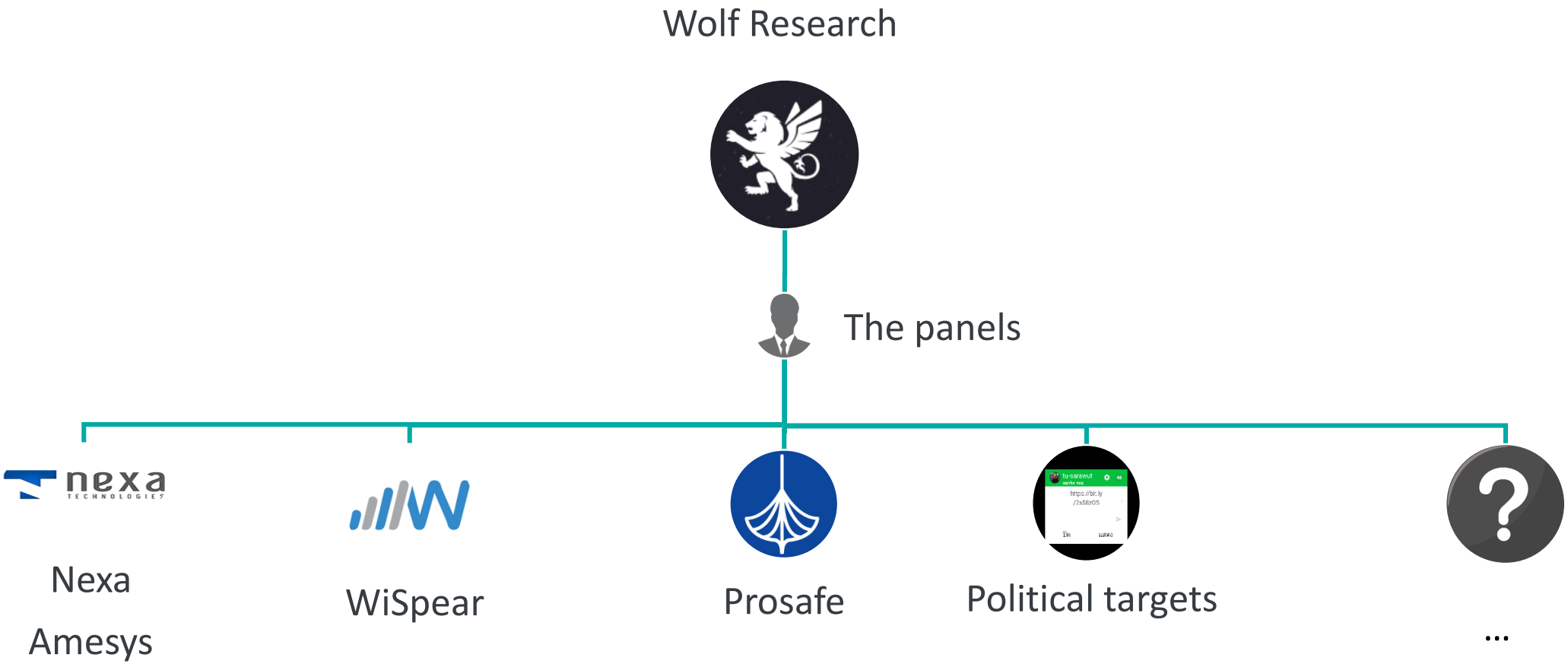
Prosafe

“Prosafe is a leading owner and operator of semi-submersible accommodation, safety and support vessels.”



A lot of pictures of the Prosafe HQ in Cyprus

Partnership

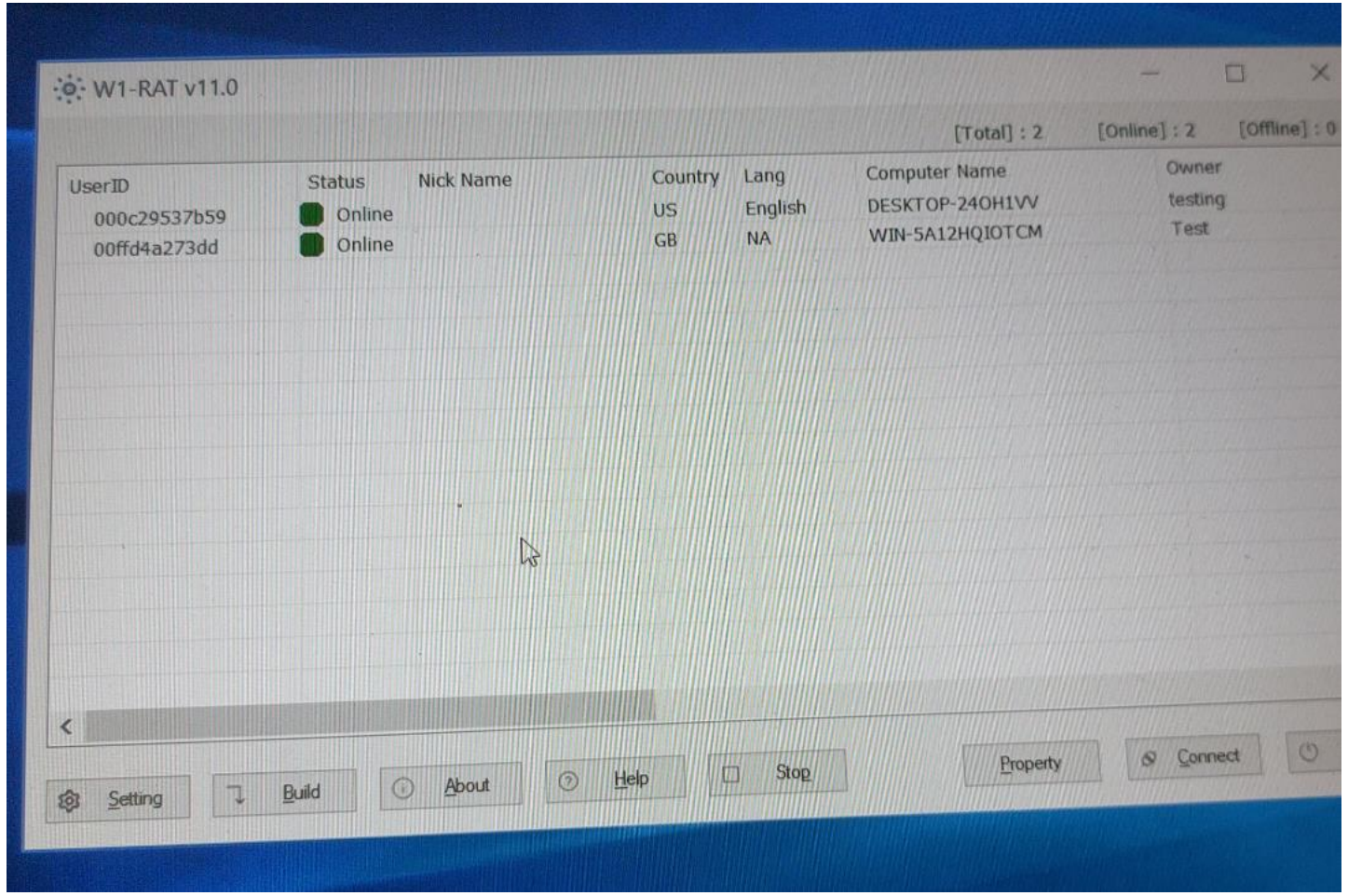


Wolf in Sheep's Clothing - Undressed

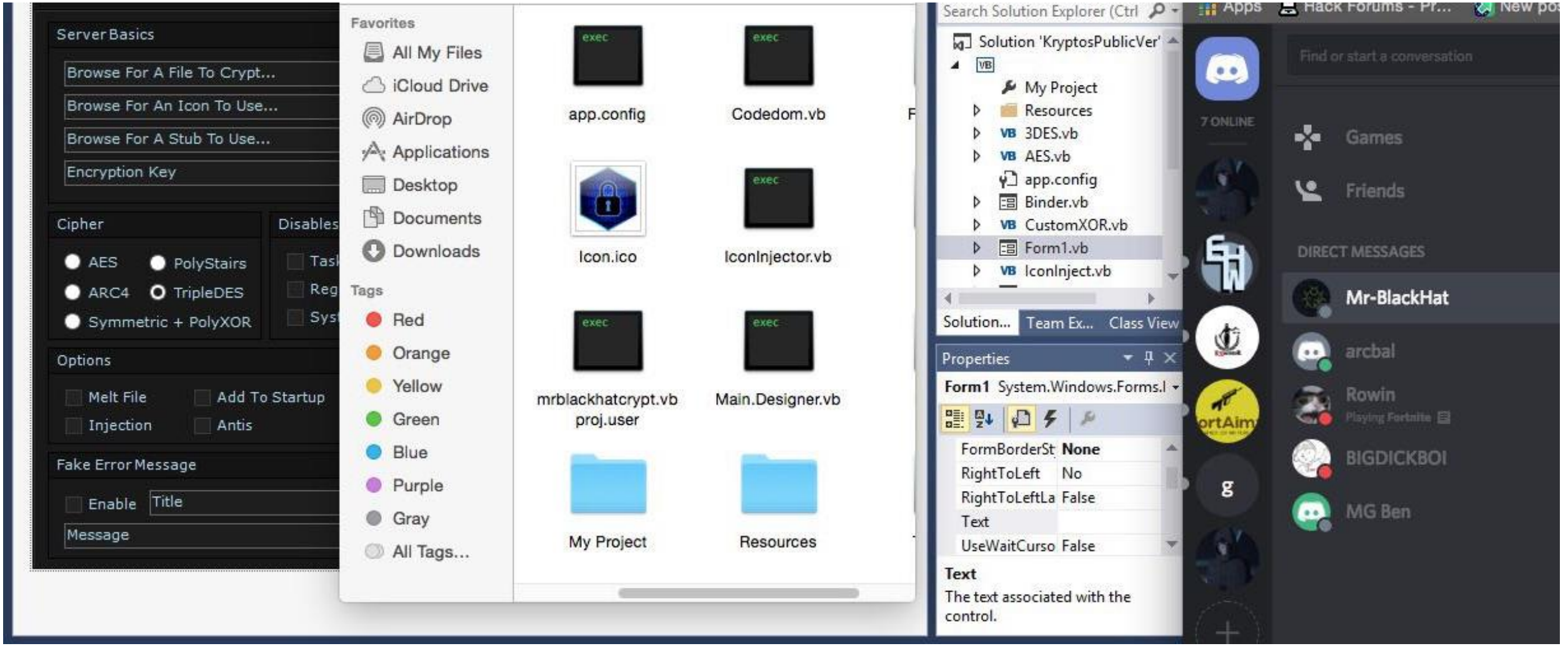
8.00
Toolset

The testing phone

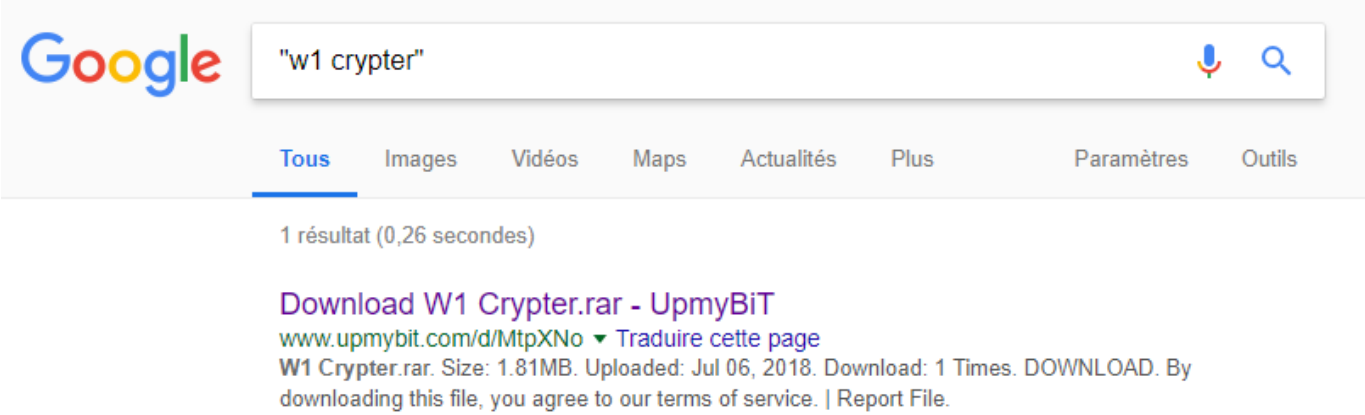
Test smartphones contain a lot of useful internal data:

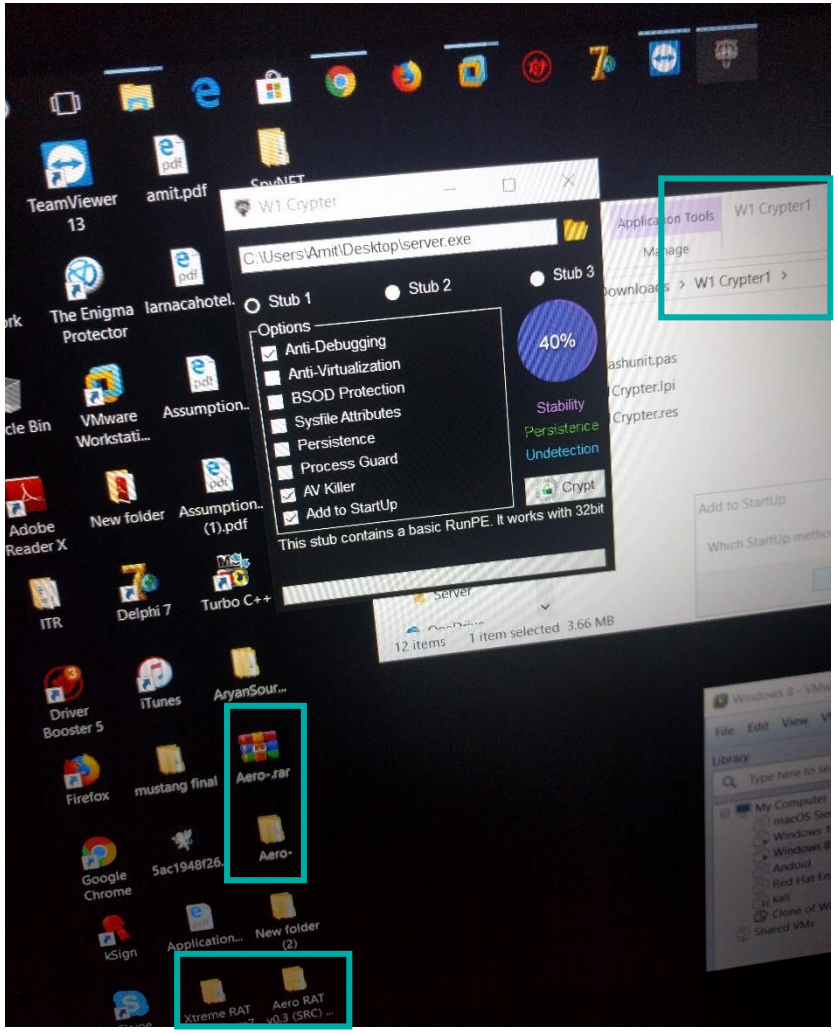


The testing phone



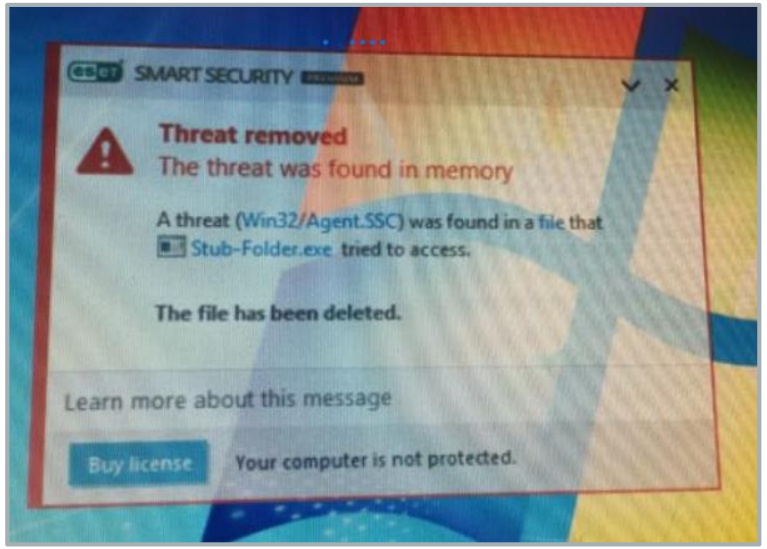
The W1 Crypter



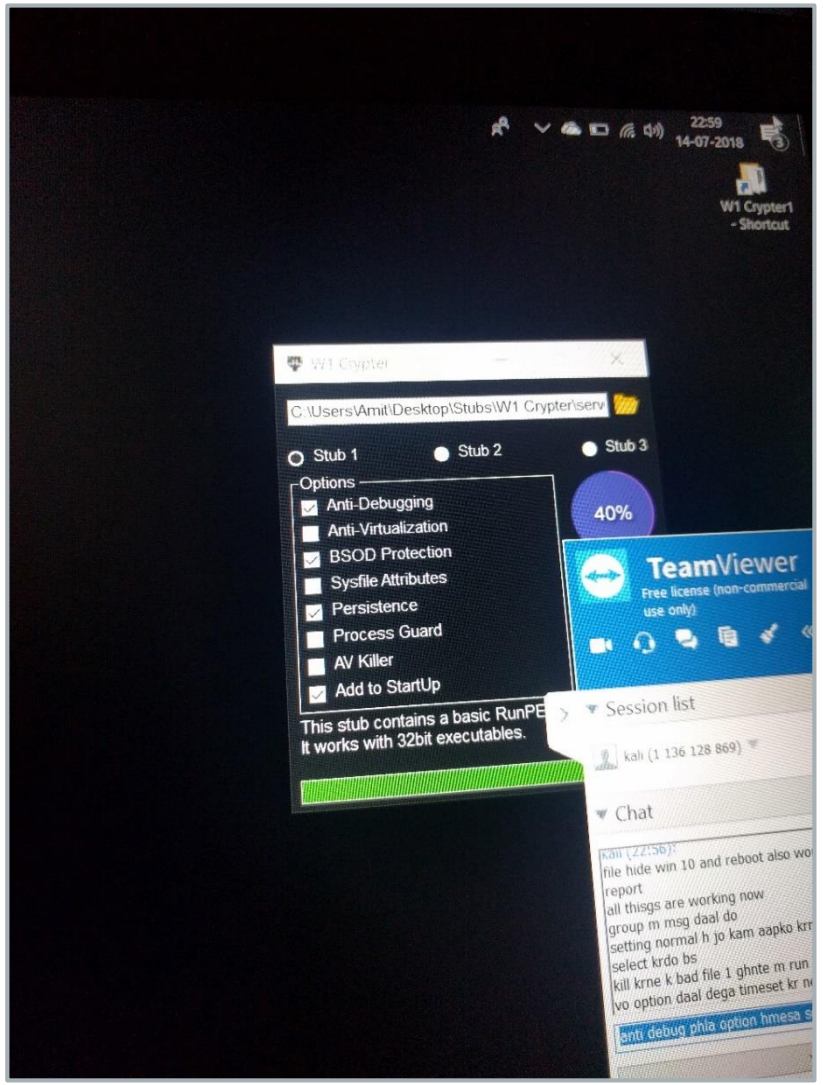


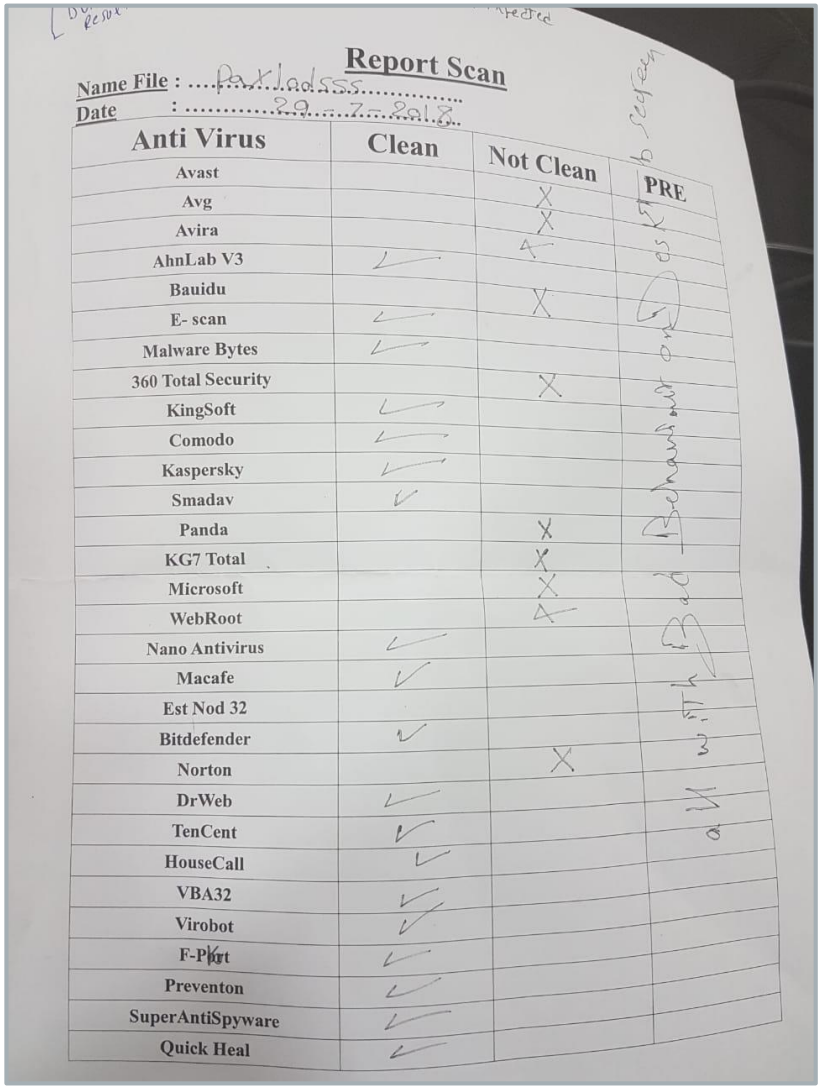
The W1 Crypter

```
begin
  FillChar(SI, SizeOf(TStartupInfoW), #0);
  FillChar(PI, SizeOf(TProcessInformation), #0);
  SI.cb := SizeOf(TStartupInfoW);
  //This is the trick, right here!
  //CreateProcessW doesn't get detected by most AVs
  //Because Wide versions of this trick aren't common.
  if CreateProcessW(PWideChar(WideString(FilePath)), PWideChar(WideString(Parameters)),
  nil, nil, FALSE, CREATE_SUSPENDED, nil, nil, SI, PI) then
  begin
    CT := Get4ByteAlignedContext(CTBase);
```



The W1 Crypter





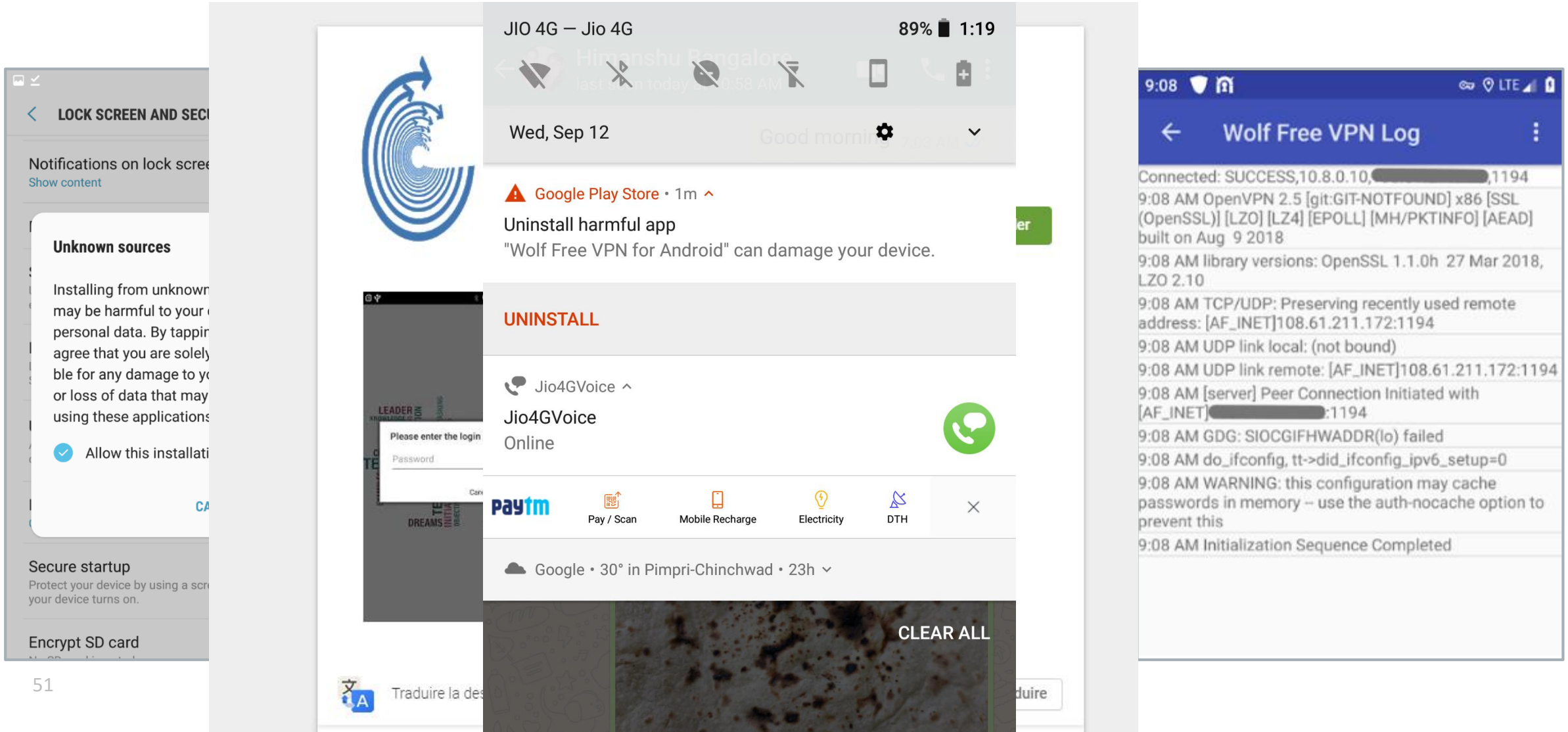
Report Scan

Name File : ....Paklodsss.....

Date : .....29-7-2018.....

Anti Virus	Clean	Not Clean	PRE
Avast		X	
Avg		X	
Avira		X	
AhnLab V3	✓		
Bauidu		X	
E- scan	✓		
Malware Bytes	✓		
360 Total Security		X	
KingSoft	✓		
Comodo	✓		
Kaspersky	✓		
Smadav	✓		
Panda		X	
KG7 Total		X	
Microsoft		X	
WebRoot		X	
Nano Antivirus	✓		
Macafe	✓		
Est Nod 32			
Bitdefender	✓		
Norton		X	
DrWeb	✓		
TenCent	✓		
HouseCall	✓		
VBA32	✓		
Virobot	✓		
F-Prot	✓		
Preventon	✓		
SuperAntiSpyware	✓		
Quick Heal	✓		

Attack vectors (?)

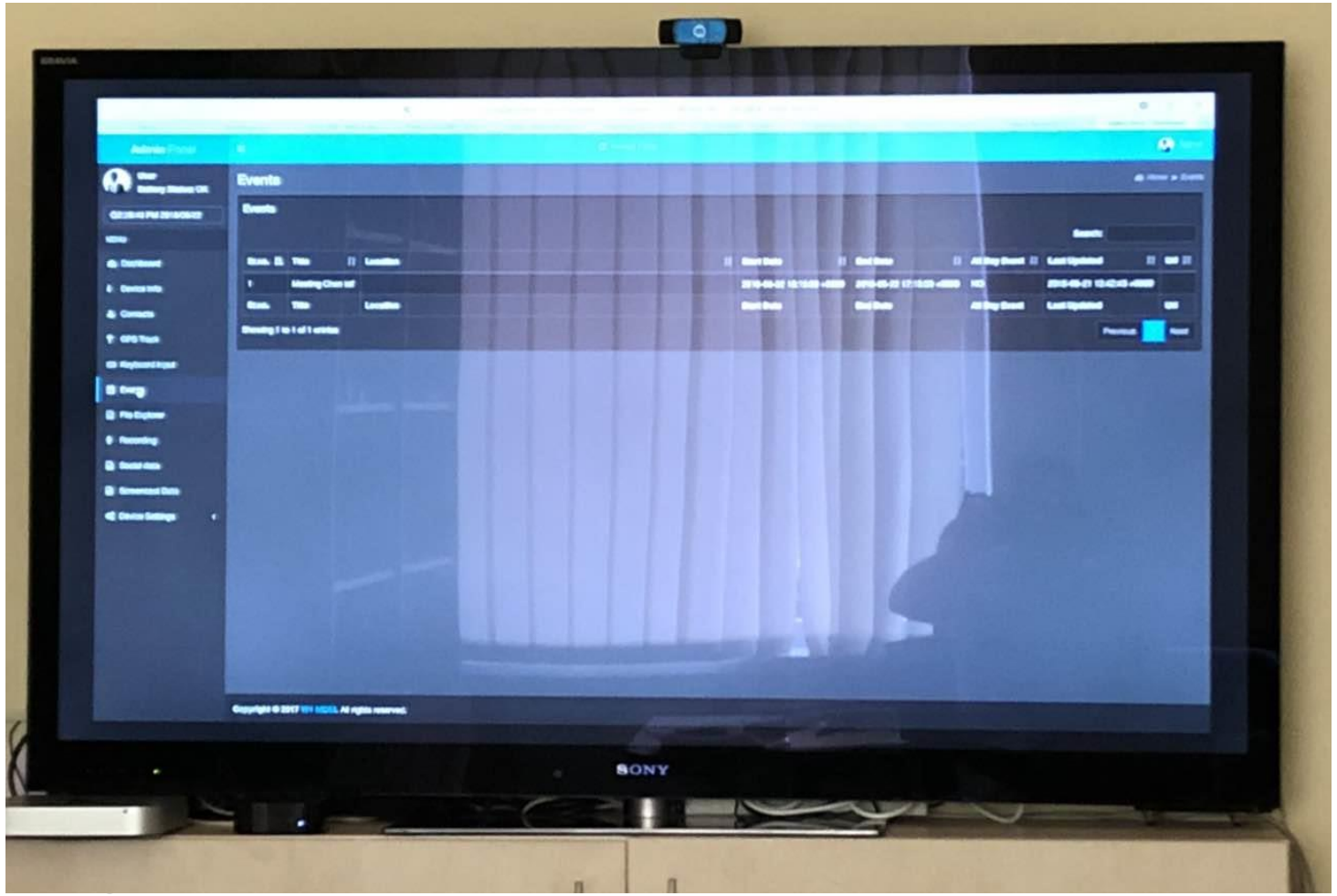


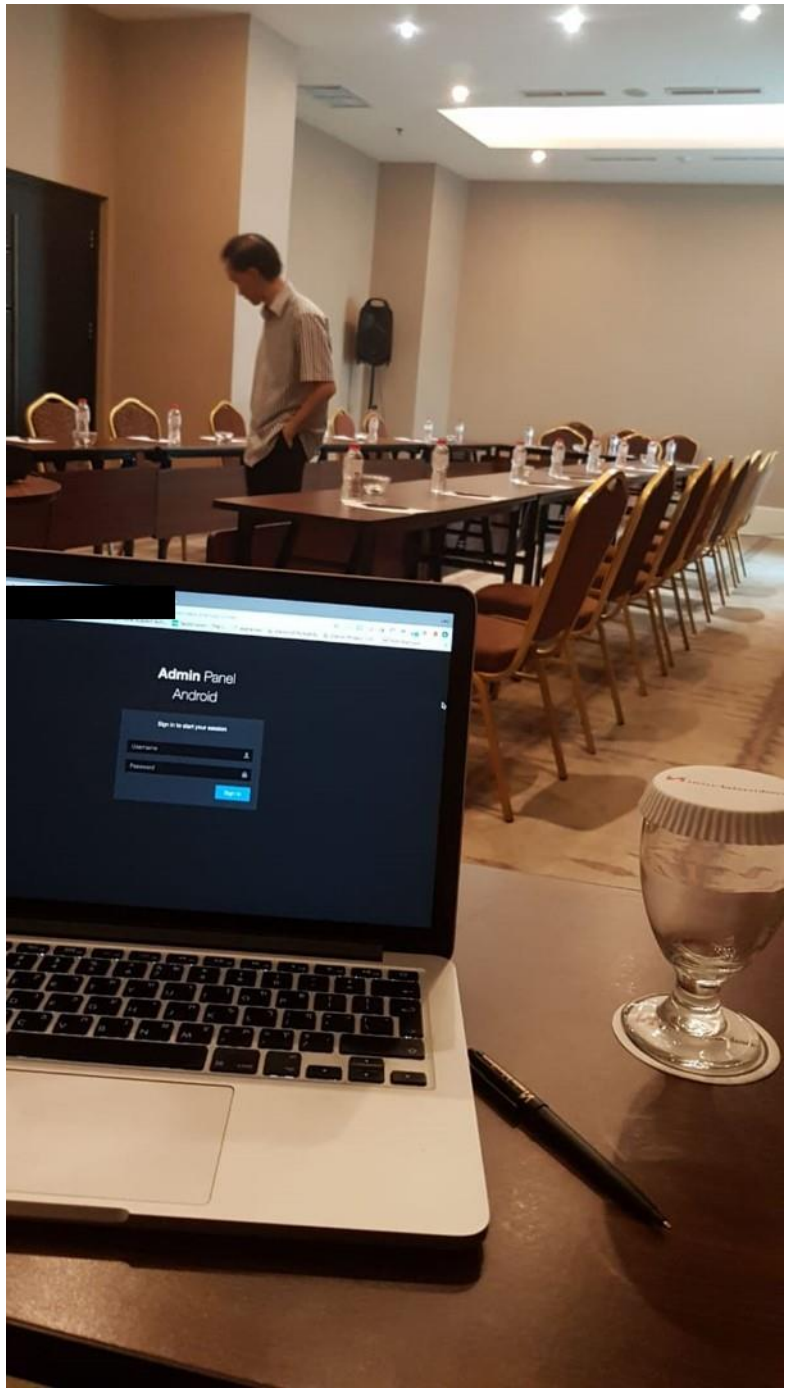
- Key quotes:
  - “- The target would get suspicious. What do you need to control?“
    “- I need to turn on this functionality”
    “- No-no-no, we are not rooting or jailbreaking. If you don’t root or jailbreak you cannot go any deeper, you cannot turn on or off…”
    “- Мы не джэйлбрэйкаем это дело.” (1st RU speaker: “We aren’t jailbreaking this.”)
    “- Поэтому мы не можем [сообщения вывезти].” (2nd RU speaker: “That’s why we cannot extract the messages.”)
    “- We can do only if we use 0 days.”

- Key quote:
  - “- Actually, we are using Google. Everyone does Google, [no one test the apps]”
    “- This is why we like this solution”
    “- Even Anti-Virus wouldn’t get it if it’s from the Google App Play store – it will bypass”
    “- All these years we always wanted to go into the market of phone penetration, but it always was based on Trojan horses and we didn’t want to be in this boat until we found this solution, so we integrated it, because this is something....”

MISC

- Audio records





- Key quotes:
  “- We prefer not to work with opposition guy.”
  “- We are not sure about this. Same as Bangladesh.”
  “- Because when they will loose the election, they will publish the blog, they will publish something in the news, we will be discovered somehow, we afraid of this stuff. So we never work with opposition, never. We always work with the leader.”

- Key quotes:
  - - “Although there are some **Israeli companies** that sold anything [everything?] [0days ?] But as far as I know, they don’t have the budget to spend on it”
    - “They have it my friend they have it”
    - Only for you”
    - [laughs]

- Key quotes:
  - “[???] start to **South America**, start in about **30 million**. I’m here since 8am.”
    - Really?
    - Since 8, I’m in the meetings here.
    - Really? How many meetings you are attending? Three-four?
    - It’s the second. Just the first one was like yesterday [???] TalkTalk. Until March 20 it’s talking.

- Approximate transcription:
  - “I’ve been to **Egypt** and we’ve done the same product. Also **Linux, Mac, Windows**. Same way, with **exploits**.”
  - “It was good?”
  - “We had it in **2015**. Now we are still going for service from time to time, **every year** we have to go…”

Conclusion

- Only the tip of the iceberg
- This kind of behavior can do great damage to international operations
  - Wolf Research: Bad legit company or good scammers?
  - Who is currently regulating the spyware business?

REST ASSURED

Thank you

For more information, please contact
pkr@csis.dk

www.csis.dk