The Discovery of a Government Malware and an Unexpected Spy Scandal

Lorenzo Franceschi-Bicchierai
WHOAMI

- Senior staff writer at VICE Motherboard
- Been covering infosec for 6+ years
- Chatted with Guccifer 2.0
- I secretly dream about becoming a pizza reporter.
The Discovery of a Government Malware and an Unexpected Spy Scandal

Attribution Ain’t That Hard
The Discovery of a Government Malware and an Unexpected Spy Scandal

... 

Even Skids Can Slip Malware on The Google Play Store
The Discovery of a Government Malware and an Unexpected Spy Scandal

Pizza, Spaghetti, Spyware
GLOSSARY

- **Government malware**: malicious software that collects data from computers and cellphones for cops and spies. AKA “spyware,” “government trojan” (“Bundestrojaner,” “Trojan di Stato.”) Remote Access Trojans (RATs), implants.

- **Lawful intercept**: industry of companies that do contract work for cops and spies, making the RATs, and sometimes exploits (0days, Ndays). Example: Hacking Team, FinFisher, NSO Group, etc.

- **Sources and methods**: there are some thing I can say, and some things I cannot in order to protect my sources.
— Discovery of rare Android malware called Exodus

— One of first in-depth investigation into how local law enforcement in EU (ab)uses spyware.

— Case study for collaboration between security researchers and journalists.
TL;DR

- Behind the scenes of joint investigation between journalists and security researchers.

— Reverse engineering malware

— Reporting techniques (interviews, FOIA, etc)

— Each of these feeds into the other.
La polizia italiana ha un listino prezzi per la sorveglianza telefonica
THE BIRTH OF THE EXODUS INVESTIGATION

- Italian cops can legally compel ISPs to send phishing text messages to install spyware on target devices.

  - Bait: maintenance, service requests.

- End-to-end encryption everywhere brought us here.

  - Before E2E: get warrant, the ISP gives you data
  - After E2E: data is on the two ends only.
THE BIRTH OF THE EXODUS INVESTIGATION
THE BIRTH OF THE EXODUS INVESTIGATION
THE BIRTH OF THE EXODUS INVESTIGATION

-Sources start talking about a new company from Calabria, in the south of Italy, which is doing very well lately.
THE BIRTH OF THE EXODUS INVESTIGATION

-Sources start talking about a new company from Calabria, in the south of Italy, which is doing very well lately.
THE BIRTH OF THE EXODUS INVESTIGATION

-Sources start talking about a new company from Calabria, in the south of Italy, which is doing very well lately.
THE BIRTH OF THE EXODUS INVESTIGATION

-Sources start talking about a new company from Calabria, in the south of Italy, which is doing very well lately.

-Security Without Borders finds suspicious apps on Google Play Store.
THE BIRTH OF THE EXODUS INVESTIGATION
THE BIRTH OF THE EXODUS INVESTIGATION
THE BIRTH OF THE EXODUS INVESTIGATION
THE BIRTH OF THE EXODUS INVESTIGATION

Big questions:

- Are these malicious apps?
- Is this how Italian cops phish targets to get spyware on devices?
- Is it just crimeware?
- Who makes the apps?
- Who installed them?
THE BIRTH OF THE EXODUS INVESTIGATION

**The Big Question**: is there even a story here?

- Malware on Google Play is not a new thing.
- We didn’t have any info on victims — hard to find a narrative.
THE BIRTH OF THE EXODUS INVESTIGATION
THE MALWARE

- 25 malicious apps on Google Play Store from 2016 to 2019.

- Fewer than 1,000 victims, according to Google.
THE MALWARE

-25 malicious apps on Google Play Store from 2016 to 2019.

-Fewer than 1,000 victims, according to Google.

-Exodus was programmed to act in two stages:
  
  ● Stage 1: dropper that collects IMEI and Phone Number. “CheckValidTarget”
    
    *** In tests malware was upgraded immediately to Stage 2.
  
  ● Stage 2: Malware downloads and executes payload.
    ○ (Spoiler: it’s a RAT)
THE MALWARE
THE MALWARE

- Stage 2: Malware downloads and executes payload.
  - List of apps
  - Record surrounding audio
  - Browser history
  - Call logs
  - Record phone calls
  - Take pictures
  - Facebook contact list
  - Exfil SMS, Telegram, WhatsApp, Viber, WeChat
  - Extract GPS coordinates
  - Extract WiFi password
THE MALWARE

-Problems:

- Exodus opens remote reverse shell to C&C with *no* TLS
  - MiTM
  - Spying on the spies.
THE MALWARE

-Problems:
THE MALWARE

- Problems:

  ● Anyone on the same network can get shell on infected device
    ○ Tampering with device
    ○ Removing evidence
THE MALWARE

-Problems:

```
user@laptop:~$ nmap 192.168.1.99 -p6000-7000

Starting Nmap 7.40 (https://nmap.org) at 2019-02-28 17:12 CET
Nmap scan report for android-[REDACTED] (192.168.1.99)
Host is up (0.035s latency).
Not shown: 994 closed ports
PORT       STATE     SERVICE
6200/tcp   open     lm-x
6201/tcp   open     thermo-calc
6205/tcp   open     unknown
6209/tcp   open     qmtps
6211/tcp   open     unknown
6212/tcp   open     unknown
6842/tcp   open     netmo-http

Nmap done: 1 IP address (1 host up) scanned in 2.30 seconds
```
THE MALWARE
THE MALWARE

- Lookout discovers iOS version.

- Similar to Android but... requires user to accept enterprise certificate.

  ● More limited access:
    ○ Contacts
    ○ Audio Recordings
    ○ Photos
    ○ Videos
    ○ GPS
    ○ Device info
THE VICTIMS

- No data on victims.

- No data on how apps were installed on target device. (Phishing? Physical access? 0day?)
THE VICTIMS

- No data on victims.

- No data on how apps were installed on target device. (Phishing? Physical access?)

- Source reveals: operators infected random people as “guinea pigs”

— Court documents obtained later confirmed this.
THE VICTIMS

-Problems:

— Putting malware on Google Play may not be legal in Italy.

— Vulnerabilities in malware (risk of MiTM) put investigations at risk.
“Putting something on the Play Store thinking you’re going to infect an undetermined number of people, and do trawling is something absolutely illegal.” […]  

“Opening up security holes and leaving them available to anyone is crazy and senseless, even before being illegal.”  

— Police Agent
“Attribution is hard.” — everyone in the threat intelligence industry.
THE ATTRIBUTION

“In true Greek irony, the Cassandras of the modern age are hamstrung by their own Apollonian curse: as intelligence agencies they are blessed with the ability to see but not to publicly substantiate. The gift to attribute without being believed.”

THE ATTFIBUTION

— Maybe only NSA, FSB, state actors, should do it because “there’s no attribution without retribution.”

— Reality: It’s hard but not impossible.
— Maybe only NSA, FSB, state actors, should do it because “there’s no attribution without retribution.”

— Reality: It’s hard but not impossible.

— It’s OK for journalists to do it—responsibly.

— Must weigh public interest

— “Whodunit” is key in journalism
THE ATTRIBUTION

a("MUNDIZZA", "09081427-FE30-46B7-BFC6-50425D3F85CC", ".*", false);
this.b.info("UPLOADSERVICE Aggiunti i file mundizza. Dimensione coda upload {}",}
THE ATTRIBUTION

a("MUNDIZZA", "09081427-FE30-46B7-BFC6-50425D3F85CC", ".*", false);
this.b.info("UPLOADSERVICE Aggiunti i file mundizza. Dimensione coda upload {}",

THE ATTRIBUTION
THE ATTRIBUTION
THE ATTRIBUTION

ws.my-local-weather[.]com
THE ATTRIBUTION

- Apps C&C server with self-signed TLS cert.
- Search for TLS cert fingerprint on Censys.io returned other servers.
- Many servers shared the same favicon.
THE ATTRIBUTION
THE ATTRIBUTION

— Searching favicon on Shodan returned 40 servers

— All servers were linked to eSurv, company based in Catanzaro, Calabria (Italy)
THE ATTRIBUTION
THE ATTRIBUTION

TOTAL RESULTS

40

TOP COUNTRIES

<table>
<thead>
<tr>
<th>Country</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Italy</td>
<td>29</td>
</tr>
<tr>
<td>United States</td>
<td>6</td>
</tr>
<tr>
<td>France</td>
<td>4</td>
</tr>
<tr>
<td>Germany</td>
<td>1</td>
</tr>
</tbody>
</table>

HTTP | HTTPS | HTTP (8080)

<table>
<thead>
<tr>
<th>Service</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telecom Italia Mobile</td>
<td>6</td>
</tr>
<tr>
<td>Telecom Italia Business</td>
<td>4</td>
</tr>
<tr>
<td>Telecom Italia</td>
<td>4</td>
</tr>
<tr>
<td>OVH SAS</td>
<td>4</td>
</tr>
<tr>
<td>Amazon.com</td>
<td>4</td>
</tr>
</tbody>
</table>

HTTP/1.1 200 OK
Date: Thu, 14 Feb 2019 16:50:37 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips mod_fcgid/2.3.9 PHP/5.4.41
X-Powered-By: PHP/5.4.41
Set-Cookie: PHPSESSID=04agcsd8flu8jghs77pe67ol4; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=

HTTP/1.1 200 OK
Date: Thu, 14 Feb 2019 18:19:29 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips mod_fcgid/2.3.9 PHP/5.4.41
X-Powered-By: PHP/5.4.41
Set-Cookie: PHPSESSID=imme7obocer6djvltvcdhqr16; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=

HTTP/1.1 200 OK
Date: Thu, 14 Feb 2019 04:31:04 GMT
Server: Apache/2.2.22 (Ubuntu)
X-Powered-By: PHP/5.3.10-1ubuntu3.11
Set-Cookie: PHPSESSID=l1vo9o56nt4o2afdu6isr12416; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=

HTTP/1.1 200 OK
Date: Thu, 14 Feb 2019 16:50:37 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips mod_fcgid/2.3.9 PHP/5.4.41
X-Powered-By: PHP/5.4.41
Set-Cookie: PHPSESSID=04agcsd8flu8jghs77pe67ol4; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=

HTTP/1.1 200 OK
Date: Thu, 14 Feb 2019 18:19:29 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips mod_fcgid/2.3.9 PHP/5.4.41
X-Powered-By: PHP/5.4.41
Set-Cookie: PHPSESSID=imme7obocer6djvltvcdhqr16; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=

HTTP/1.1 200 OK
Date: Thu, 14 Feb 2019 04:31:04 GMT
Server: Apache/2.2.22 (Ubuntu)
X-Powered-By: PHP/5.3.10-1ubuntu3.11
Set-Cookie: PHPSESSID=l1vo9o56nt4o2afdu6isr12416; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=
— eSurv employee wrote in his LinkedIn:

[... ] developed “an ‘agent’ application to gather data from Android devices and send it to a C&C server.”
THE ATTRIBUTION

— eSurv employee wrote in his LinkedIn:

[...] developed “an ‘agent’ application to gather data from Android devices and send it to a C&C server.”

— Source tells us eSurv secretly develops malware called “Exodus”
THE ATTRIBUTION

— eSurv employee wrote in his LinkedIn:

[...] developed “an ‘agent’ application to gather data from Android devices and send it to a C&C server.”

— Source tells us eSurv secretly develops malware called “Exodus”

— Italian government document reveals eSurv had 300,000 EUR contract with “Polizia di Stato” to develop “passive and active interception system.”
THE ATTRIBUTION
THE ATTRIBUTION

- What we know at this point:
  — eSurv makes spyware called Exodus
  — eSurv has contract with the cops
  — 25 eSurv apps were on Play Store
  — Exodus infected less than 1,000 targets
  — We still have no idea who the targets are.
THE ATTRIBUTION

- Final questions:
  - Do we name the company?
  - How many details do we include? (Apps screenshots, IP addresses, etc)
  - Do we alert authorities?

-Significant risk of putting legitimate investigations into serious crimes in danger.
THE ATTRIBUTION

- We contact company

  — They deny making malware, then ghost us.
THE ATTRIBUTION

- We contact company
  — They deny making malware, then ghost us.

- We contact Polizia di Stato, prosecutors offices, asking for comment.
  — No answers
THE ATTRIBUTION

- We contact company
  — They deny making malware, then ghost us.

- We contact Polizia di Stato, prosecutors offices, asking for comment.
  — No answers

- We contact Italian government through intermediary.
  — No answers
THE ATTRIBUTION
- We did not expect this story to have a huge impact.

— Italy is full of malware makers
THE AFTERMATH

- We did not expect this story to have a huge impact.

— Italy is full of malware makers
We did not expect this story to have a huge impact.

— Italy is full of malware makers
THE AFTERMATH

-We **did not** expect this story to have a huge impact.

— Italy is full of malware makers
- We did not expect this story to have a huge impact.

— Italy is full of malware makers
THE AFTERMATH

-We **did not** expect this story to have a huge impact.

— Italy is full of malware makers
THE AFTERMATH

- We did not expect this story to have a huge impact.

— Italy is full of malware makers
THE AFTERMATH

-As it turns out ... Exodus became a huge story in Italy.

— eSurv spying on “guinea pigs” made everyone a potential victim.

— Story became: “this could have happened to you.”
THE AFTERMATH

-Local news reports that two prosecutor’s offices in Italy had opened inquiry into eSurv weeks before.
Local news reports that two prosecutor’s offices in Italy had opened inquiry into eSurv weeks before.

— Illegal wiretapping: eSurv monitored innocents with Exodus
- Local news reports that two prosecutor’s offices in Italy had opened inquiry into eSurv weeks before.

— Illegal wiretapping: eSurv monitored innocents with Exodus

— Employees listened to calls in eSurv’s office, called them “volunteers.”
THE AFTERMATH

- Local news reports that two prosecutor’s offices in Italy had opened inquiry into eSurv weeks before.

— Illegal wiretapping: eSurv monitored innocents with Exodus

— Employees listened to calls in eSurv’s office, called them “volunteers.”

— Servers in prosecutor’s offices were empty, no operating system.
THE AFTERMATH

-Italian law:

— Servers for wiretapping need to be on government premises
- Italian law:

— Servers for wiretapping need to be on government premises

- eSurv used AWS
- Italian law:
  — Servers for wiretapping need to be on government premises
    
  - eSurv used AWS

  — Prosecutors in one office are only authorized to access their investigations’ data
THE AFTERMATH

- Italian law:
  - Servers for wiretapping need to be on government premises
    - eSurv used AWS
  - Prosecutors in one office are only authorized to access their investigations’ data
    - Anyone using Exodus could read all investigations data
THE AFTERMATH

— eSurv’s CEO and CTO under house arrest, under criminal investigation for illegal wiretapping.

— Authorities estimate ~200 out of ~800 targets were unauthorized.

— Multiple prosecutor’s offices investigating use of Exodus by police and intelligence agencies.

— Italian Data Protection Authority questions use of Government Trojans and calls for safeguards
HOW DID WE GET HERE?

The history of Lawful Intercept industry is poorly documented

— 2010s have a lot of documented cases

  • Citizen Lab investigations
  • AV reports
  • Leaked documents

— 2000s, 1990s are not well documented.
How old is Lawful Intercept?

— Early days (1990s, 2000s) are not very well documented, but governments were already using malware because of end-to-end encryption.
HOW DID WE GET HERE?

— Anecdotes:

● Developer on LinkedIn says he’s been working on Windows malware for 20+ years.
● 2002: off the shelf $40 RAT to investigate terrorist operation in European country.
● Uptick of government employees coming to Black Hat looking for talent and tools in mid 2000s.
HOW DID WE GET HERE?

-Lawful Intercept history in US has some earlier data points.
HOW DID WE GET HERE?

-Lawful Intercept history in US has some earlier data points.

— 1998: FBI’s network surveillance system “Carnivore”

— 1999: FBI uses malware (keylogger) to steal PGP private key of mob boss.
HOW DID WE GET HERE?

-Lawful Intercept history in US has some earlier data points.

— 2001: FBI’s Magic Lantern malware

— 2003: FBI uses spyware against animal welfare group. (Operation Trail Mix)

— 2007: FBI uses “CIPAV” (Computer and Internet Protocol Address Verifier) malware to trace bomb threats to a 15-year-old
HOW DID WE GET HERE?

-Meanwhile in Europe...

— 2003: Hacking Team is born in Italy.

— 2004: Hacking Team’s first sale outside of Italy (Spain)

— 2011: WikiLeaks’ Spy Files reveal existence of Hacking Team’s spyware
HOW DID WE GET HERE?

-Meanwhile in Europe...

HOW DID WE GET HERE?

-Hacking Team and FinFisher conquer the world.

— Hacking Team: present in 41 countries before 2015 breach.

— FinFisher: present in 32 countries as of 2015.
HOW DID WE GET HERE?
HOW DID WE GET HERE?

- NSO Group (Israel) takes over.

— 60+ customers in 35 countries as of 2019
HOW DID WE GET HERE?
HOW DID WE GET HERE?

- NSO Group (Israel) takes over.

— 60+ customers in 35 countries as of 2019

— $251 million revenue in 2018
HOW DID WE GET HERE?

-The Lawful Intercept market today:

— Worth $12 billion (Moody’s and S&P estimate).

— **Multiple** companies can have presence in the **same** countries (UAE, Ethiopia, Mexico...).
- The Lawful Intercept market today:
  — Worth $12 billion (Moody’s and S&P estimate).
  — **Multiple** companies can have presence in the **same** countries (UAE, Ethiopia, Mexico...)

  - Agencies need different products depending on target (Mobile, Desktop)
  - Agency buys product for defensive purposes (track and detect malware).
HOW DID WE GET HERE?

-The Lawful Intercept market today:

— “Five Eyes” (US/UK/CA/NZ/AU) work almost exclusively with local companies.

— China: government is moving toward keeping all offensive capabilities within China.
HOW DID WE GET HERE?

-Italy is an interesting case study in Europe.

— Authorities love wiretapping ("interrcettazioni"), especially against organized crime.

— Every prosecutor’s office has a lot of freedom when buying solutions.
HOW DID WE GET HERE?

- Italy is an interesting case study in Europe.

— Authorities love wiretapping ("intercettazioni"), especially against organized crime.

— Every prosecutor’s office has a lot of freedom when buying solutions.

— Result: fragmented market with a lot of small companies.

  ● First: network level interception (Area, RCS Lab)
  ● Then: malware (HT, Raxir, Negg...)
HOW DID WE GET HERE?

- Recent data from Italy in 2017: (Ministry of Justice)
  - Phone wiretaps with providers’ help: 106,000
  - Wiretaps through “bugs”: 16,000 (“ambient” wiretaps)
  - Wiretaps through malware: 4,542 (“electronic wiretaps”)
  - 148 licensed companies.
HOW DID WE GET HERE?
Lawful Intercept industry is here to stay:

— End-to-end encryption makes old wiretapping obsolete

— Cops and spies need wiretapped data.

— Contractors (HT, FinFisher, NSO...) are offering those solutions right now.
CONCLUSION

-Future challenges:

— Vet spyware companies and products

— Figure out who gets access to surveillance data.
GRAZIE

— Security Without Borders
— Riccardo Coluccini
— Trail of Bits
QUESTIONS? COMMENTS? TIPS?

سائل؟ تعليقات؟ نصائح؟

البريد الإلكتروني: lorenzofb@vice.com

المتابعة على تويتر: @lorenzofb

الاتصال الأمان: lorenzofb.com/#contact