

# Whatsapp, Signal & Telegram Attack Vectors

@rodsoto  
[www.rodsoto.net](http://www.rodsoto.net)

# \$whoami



Over 15 years of experience in information technology and security. He has spoken at ISSA, ISC2, OWASP, DEFCON, RSA Conference, Hackmiami, DerbyCon, Splunk .CONF, Black Hat, BSides, Underground Economy and also been featured in Rolling Stone Magazine, Pentest Magazine, Univision, BBC, Forbes, VICE, Fox News and CNN.

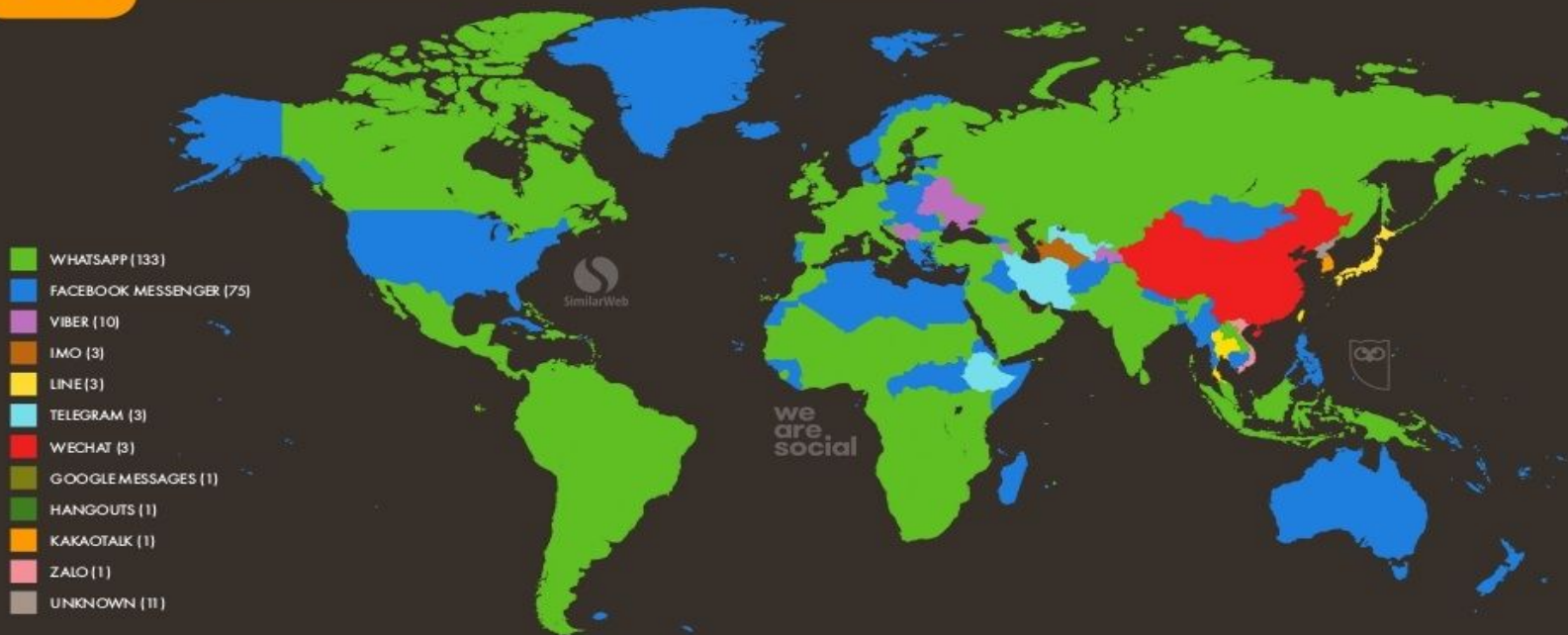
# These apps dwell in mobile phones...



JAN  
2019

## TOP SOCIAL MESSENGERS AROUND THE WORLD

THE MOST POPULAR MESSENGER APP BY COUNTRY / TERRITORY IN DECEMBER 2018



# Whatsapp, Telegram Signal

- Most popular messaging applications
- Provide multimedia messaging (Picture, Video, Voice, Text)
- All these applications process, transmit and receive sensitive information
- Depending on phone platform the reach of these applications can be of high risk (Permissions, Access, Take Control of Phone)
- The phone has become the ultimate crown jewel when targeting a person as pretty much their lives are recorded by it. As we will see these applications can be used as accessories to compromise devices and actual personas.

# WhatsApp



- Owned by Facebook
- Claims 2 Billion users around the world
- Available 180 countries in 60 languages
- Before recent privacy fiasco whatsapp was estimated to have 1 out of 5 US Adults
- Estimated use of around 5 Million businesses
- Biggest market is India with 340 Million users
- Proprietary
- Blocked in Cuba, Russia, Syria, Iran, North Korea

# Whatsapp Features

- End to end encryption
- Voice calls
- Video Calls
- File sharing
- Group chats
- Two step verification

# Telegram



- Founded by the same founders of Russian VK (Facebook clone)
- Headquarters in Dubai
- Claims 500 Million users (This places them ahead of twitter)
- Telegram is certainly the leader in very specific markets (i.e Iran)
- Open source



# Telegram Features

- Accounts linked to a phone number can be accessed from multiple devices
- Web interface
- Two step verification
- Secret chat end to end encryption
- Web messages encrypted via TLS/SSL, encryption key at server
- Browsable channels
- Browsable links and files
- People nearby
- Symmetric encryption via MProto 256-bit symmetric **AES** encryption
- Blocked in Russia, Iran, China, Pakistan,

# Signal



- Created by Moxie Marlinspike
- Approximate of 20 + Million users
- Available in over 40 countries
- The least popular of all three
- Blocked in Iran, Egypt, UAE, Qatar

# Signal features

- End to end video calling, messaging, and texting
- Group calls up to 8 people
- Automatic end to end encryption
- Message timers
- Mandatory connection to a phone number
- Encryption via signal protocol combines the [Double Ratchet Algorithm](#), prekeys, and an Extended Triple [Diffie–Hellman](#) (X3DH) handshake.<sup>[101][102]</sup> It uses [Curve25519](#), [AES-256](#), and [HMAC-SHA256](#) as primitives
- Relies on centralized server, this server uses registered users contacts for discovery and exchange of keys.

# Security comparisons

	Signal	Telegram	Whatsapp
Data Collection	Does not collect data only Phone Number	Name, Phone #, Contacts, userID, IP	Collects a F**KTON
Cost	Free No Ads	Free No Ads	Free
Open source?	Full	Partial	Proprietary
Encryption	Signal Protocol - Full encryption end to end	MProto - Not encrypted by default	Signal Protocol - Full encryption. Cloud backups are NOT encrypted
MFA	Yes	Yes	Yes
Disappearing messages	Yes	Yes	Supposed to have it soon

# Yeah about whatsapp.... NOT PRIVACY FRIENDLY

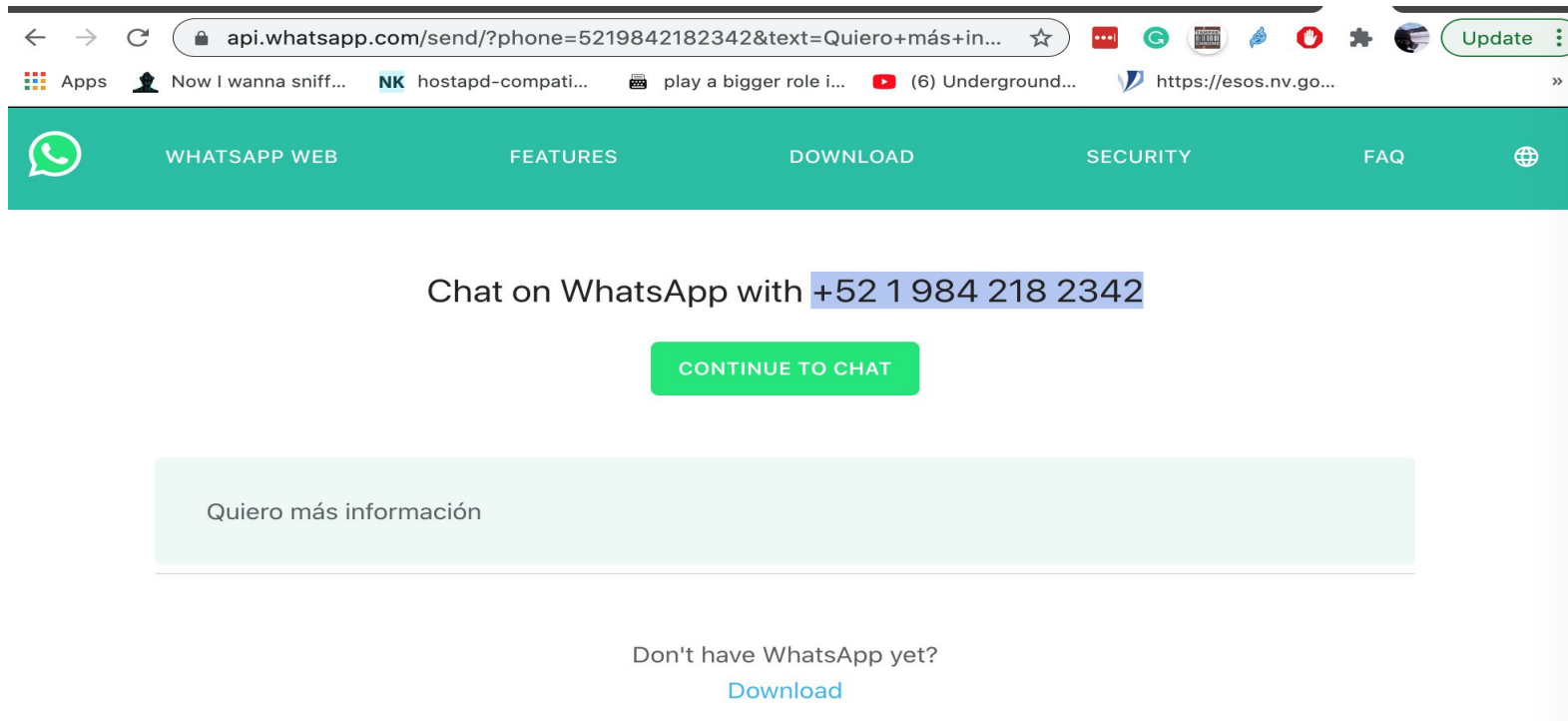
Signal 'Data Linked To You'	iMessage 'Data Linked To You'	WhatsApp 'Data Linked To You'	Facebook Messenger 'Data Linked To You'
<div></div>	<div><div><div>Contact Info<ul style="list-style-type: none"><li>Email Address</li><li>Phone Number</li></ul></div><div>Search History<ul style="list-style-type: none"><li>Identifiers<ul style="list-style-type: none"><li>Device ID</li></ul></li></ul></div></div></div>	<div><div><div>Analytics<ul style="list-style-type: none"><li>Purchases<ul style="list-style-type: none"><li>Purchase History</li></ul></li><li>Location<ul style="list-style-type: none"><li>Coarse Location</li></ul></li><li>Contact Info<ul style="list-style-type: none"><li>Phone Number</li></ul></li><li>User Content<ul style="list-style-type: none"><li>Other User Content</li></ul></li><li>Identifiers<ul style="list-style-type: none"><li>User ID</li><li>Device ID</li></ul></li><li>Usage Data<ul style="list-style-type: none"><li>Product Interaction</li><li>Advertising Data</li></ul></li><li>Diagnostics<ul style="list-style-type: none"><li>Crash Data</li><li>Performance Data</li><li>Other Diagnostic Data</li></ul></li></ul></div><div><div>App Functionality<ul style="list-style-type: none"><li>Purchases<ul style="list-style-type: none"><li>Purchase History</li></ul></li><li>Financial Info<ul style="list-style-type: none"><li>Payment Info</li></ul></li><li>Location<ul style="list-style-type: none"><li>Coarse Location</li></ul></li><li>Contact Info<ul style="list-style-type: none"><li>Email Address</li><li>Phone Number</li></ul></li><li>Contacts<ul style="list-style-type: none"><li>Contacts</li></ul></li><li>User Content<ul style="list-style-type: none"><li>Customer Support</li><li>Other User Content</li></ul></li><li>Identifiers<ul style="list-style-type: none"><li>User ID</li><li>Device ID</li></ul></li><li>Usage Data<ul style="list-style-type: none"><li>Product Interaction</li></ul></li><li>Diagnostics<ul style="list-style-type: none"><li>Crash Data</li><li>Performance Data</li><li>Other Diagnostic Data</li></ul></li></ul></div></div></div></div>	<div><div><div>Third-Party Advertising<ul style="list-style-type: none"><li>Purchases<ul style="list-style-type: none"><li>Purchase History</li></ul></li><li>Financial Info<ul style="list-style-type: none"><li>Other Financial Info</li></ul></li><li>Location<ul style="list-style-type: none"><li>Precise Location</li><li>Coarse Location</li></ul></li><li>Contact Info<ul style="list-style-type: none"><li>Physical Address</li><li>Email Address</li><li>Name</li><li>Phone Number</li><li>Other User Contact Info</li></ul></li><li>Contacts<ul style="list-style-type: none"><li>Contacts</li></ul></li><li>User Content<ul style="list-style-type: none"><li>Photos or Videos</li><li>Gameplay Content</li><li>Other User Content</li></ul></li><li>Search History<ul style="list-style-type: none"><li>Search History</li></ul></li><li>Browsing History<ul style="list-style-type: none"><li>Browsing History</li></ul></li><li>Identifiers<ul style="list-style-type: none"><li>User ID</li><li>Device ID</li></ul></li><li>Usage Data<ul style="list-style-type: none"><li>Product Interaction</li><li>Advertising Data</li><li>Other Usage Data</li></ul></li><li>Diagnostics<ul style="list-style-type: none"><li>Crash Data</li><li>Performance Data</li><li>Other Diagnostic Data</li></ul></li><li>Other Data<ul style="list-style-type: none"><li>Other Data Types</li></ul></li></ul></div><div><div>Analytics<ul style="list-style-type: none"><li>Health &amp; Fitness<ul style="list-style-type: none"><li>Health</li><li>Fitness</li></ul></li><li>Purchases<ul style="list-style-type: none"><li>Purchase History</li></ul></li><li>Financial Info<ul style="list-style-type: none"><li>Payment Info</li><li>Other Financial Info</li></ul></li><li>Location<ul style="list-style-type: none"><li>Precise Location</li><li>Coarse Location</li></ul></li><li>Contact Info<ul style="list-style-type: none"><li>Physical Address</li><li>Email Address</li><li>Name</li><li>Phone Number</li><li>Other User Contact Info</li></ul></li><li>Contacts<ul style="list-style-type: none"><li>Contacts</li></ul></li><li>User Content<ul style="list-style-type: none"><li>Photos or Videos</li><li>Gameplay Content</li><li>Other User Content</li></ul></li><li>Search History<ul style="list-style-type: none"><li>Search History</li></ul></li><li>Browsing History<ul style="list-style-type: none"><li>Browsing History</li></ul></li><li>Identifiers<ul style="list-style-type: none"><li>User ID</li><li>Device ID</li></ul></li><li>Usage Data<ul style="list-style-type: none"><li>Product Interaction</li><li>Advertising Data</li><li>Other Usage Data</li></ul></li><li>Diagnostics<ul style="list-style-type: none"><li>Crash Data</li><li>Performance Data</li><li>Other Diagnostic Data</li></ul></li><li>Other Data<ul style="list-style-type: none"><li>Other Data Types</li></ul></li></ul></div><div><div>Product Personalisation<ul style="list-style-type: none"><li>Purchases<ul style="list-style-type: none"><li>Purchase History</li></ul></li><li>Financial Info<ul style="list-style-type: none"><li>Other Financial Info</li></ul></li><li>Location<ul style="list-style-type: none"><li>Precise Location</li><li>Coarse Location</li></ul></li><li>Contact Info<ul style="list-style-type: none"><li>Physical Address</li><li>Email Address</li><li>Name</li><li>Phone Number</li><li>Other User Contact Info</li></ul></li><li>Contacts<ul style="list-style-type: none"><li>Contacts</li></ul></li><li>User Content<ul style="list-style-type: none"><li>Photos or Videos</li><li>Gameplay Content</li><li>Other User Content</li></ul></li><li>Search History<ul style="list-style-type: none"><li>Search History</li></ul></li><li>Browsing History<ul style="list-style-type: none"><li>Browsing History</li></ul></li><li>Identifiers<ul style="list-style-type: none"><li>User ID</li><li>Device ID</li></ul></li><li>Usage Data<ul style="list-style-type: none"><li>Product Interaction</li><li>Advertising Data</li><li>Other Usage Data</li></ul></li><li>Sensitive Info<ul style="list-style-type: none"><li>Sensitive Info</li></ul></li><li>Diagnostics<ul style="list-style-type: none"><li>Crash Data</li><li>Performance Data</li><li>Other Diagnostic Data</li></ul></li><li>Other Data<ul style="list-style-type: none"><li>Other Data Types</li></ul></li></ul></div><div><div>App Functionality<ul style="list-style-type: none"><li>Health &amp; Fitness<ul style="list-style-type: none"><li>Health</li><li>Fitness</li></ul></li><li>Purchases<ul style="list-style-type: none"><li>Purchase History</li></ul></li><li>Financial Info<ul style="list-style-type: none"><li>Payment Info</li><li>Credit Info</li><li>Other Financial Info</li></ul></li><li>Location<ul style="list-style-type: none"><li>Precise Location</li><li>Coarse Location</li></ul></li><li>Contact Info<ul style="list-style-type: none"><li>Physical Address</li><li>Email Address</li><li>Name</li><li>Phone Number</li><li>Other User Contact Info</li></ul></li><li>Contacts<ul style="list-style-type: none"><li>Contacts</li></ul></li><li>User Content<ul style="list-style-type: none"><li>Photos or Videos</li><li>Gameplay Content</li><li>Other User Content</li></ul></li><li>Search History<ul style="list-style-type: none"><li>Search History</li></ul></li><li>Browsing History<ul style="list-style-type: none"><li>Browsing History</li></ul></li><li>Identifiers<ul style="list-style-type: none"><li>User ID</li><li>Device ID</li></ul></li><li>Usage Data<ul style="list-style-type: none"><li>Product Interaction</li><li>Advertising Data</li><li>Other Usage Data</li></ul></li><li>Diagnostics<ul style="list-style-type: none"><li>Crash Data</li><li>Performance Data</li><li>Other Diagnostic Data</li></ul></li><li>Other Data<ul style="list-style-type: none"><li>Other Data Types</li></ul></li></ul></div><div><div>Other Purposes<ul style="list-style-type: none"><li>Purchases<ul style="list-style-type: none"><li>Purchase History</li></ul></li><li>Financial Info<ul style="list-style-type: none"><li>Other Financial Info</li></ul></li><li>Location<ul style="list-style-type: none"><li>Precise Location</li><li>Coarse Location</li></ul></li><li>Contact Info<ul style="list-style-type: none"><li>Physical Address</li><li>Email Address</li><li>Name</li><li>Phone Number</li><li>Other User Contact Info</li></ul></li><li>Contacts<ul style="list-style-type: none"><li>Contacts</li></ul></li><li>User Content<ul style="list-style-type: none"><li>Photos or Videos</li><li>Gameplay Content</li><li>Customer Support</li><li>Other User Content</li></ul></li><li>Search History<ul style="list-style-type: none"><li>Search History</li></ul></li><li>Browsing History<ul style="list-style-type: none"><li>Browsing History</li></ul></li><li>Identifiers<ul style="list-style-type: none"><li>User ID</li><li>Device ID</li></ul></li><li>Usage Data<ul style="list-style-type: none"><li>Product Interaction</li><li>Advertising Data</li><li>Other Usage Data</li></ul></li><li>Diagnostics<ul style="list-style-type: none"><li>Crash Data</li><li>Performance Data</li><li>Other Diagnostic Data</li></ul></li><li>Other Data<ul style="list-style-type: none"><li>Other Data Types</li></ul></li></ul></div></div></div></div></div></div></div>

# Vulnerabilities & Exploitation

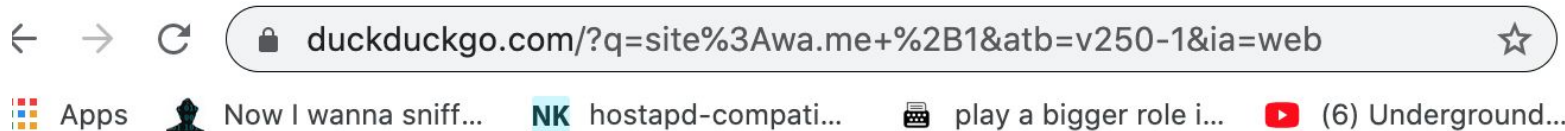
Whatsapp	Signal	Telegram
Link Previews	CVE-2020-5753 -- DNS Leakage	Telegram Scraper - Demo
Invalid Characters	CVE-2019-9970 -- Invalid Character -- IDN homograph attack	Telegrab -- steals telegram channel
QR Hijack -- Demo	CVE-2019-19954 -- Signal Desktop Privesc	Shadow Sessions via Malicious Apps (Does not notify of a second session)
Call Forwarding -- Uses call forwarding to get data from account	CVE-2018-16132 -- Forces device restart	Telegram Channel Stealer - Binary
OTP Sniffing -- Shoulder Surfing or Screen exposure		SIM SWAP
CVE-201911931 - Buffer over Flow (MP4)		CVE-2018-17780 - Telegram Desktop leaks user IP during calls
Voice Mail -- Use verification when victim is away access VM		RATAttack telegram based botnet
Web search engines indexing chats -- Demo		Katyusha Telegram based sql injection scanner
		DeepFake Bot - Took genuinen pictures of women and placed face on nude bodies

# Demo screenshots

Here are web search engines indexing whatsapp conversations...



# Search engines indexing whatsapp conversations



Showing results from: [wa.me](#) [All Results](#)

## Chat on WhatsApp

 <https://wa.me/1>

We would like to show you a description here but the **site** won't allow us.

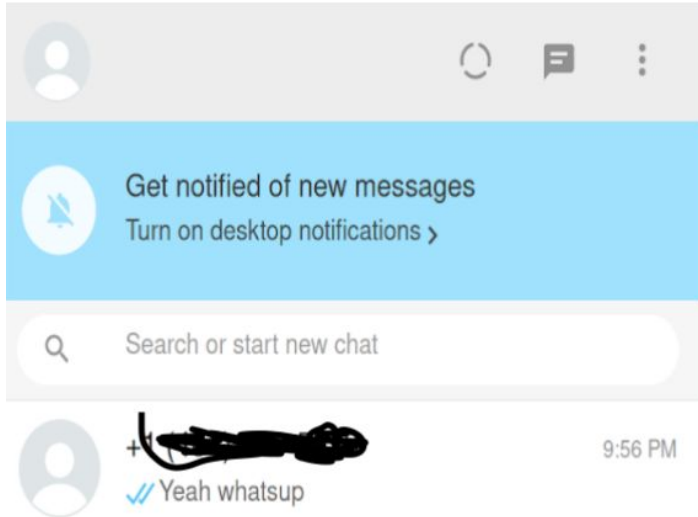
[wa.me](#)

 <https://wa.me/5219842182342?text=Quiero más información>

We would like to show you a description here but the **site** won't allow us.



# QR Hijack <https://github.com/cryptedwolf/ohmyqr>



```
trajan@x1pad: ~/ohmyqr

trajan@x1pad: ~
trajan@x1pad: ~/ohmyqr

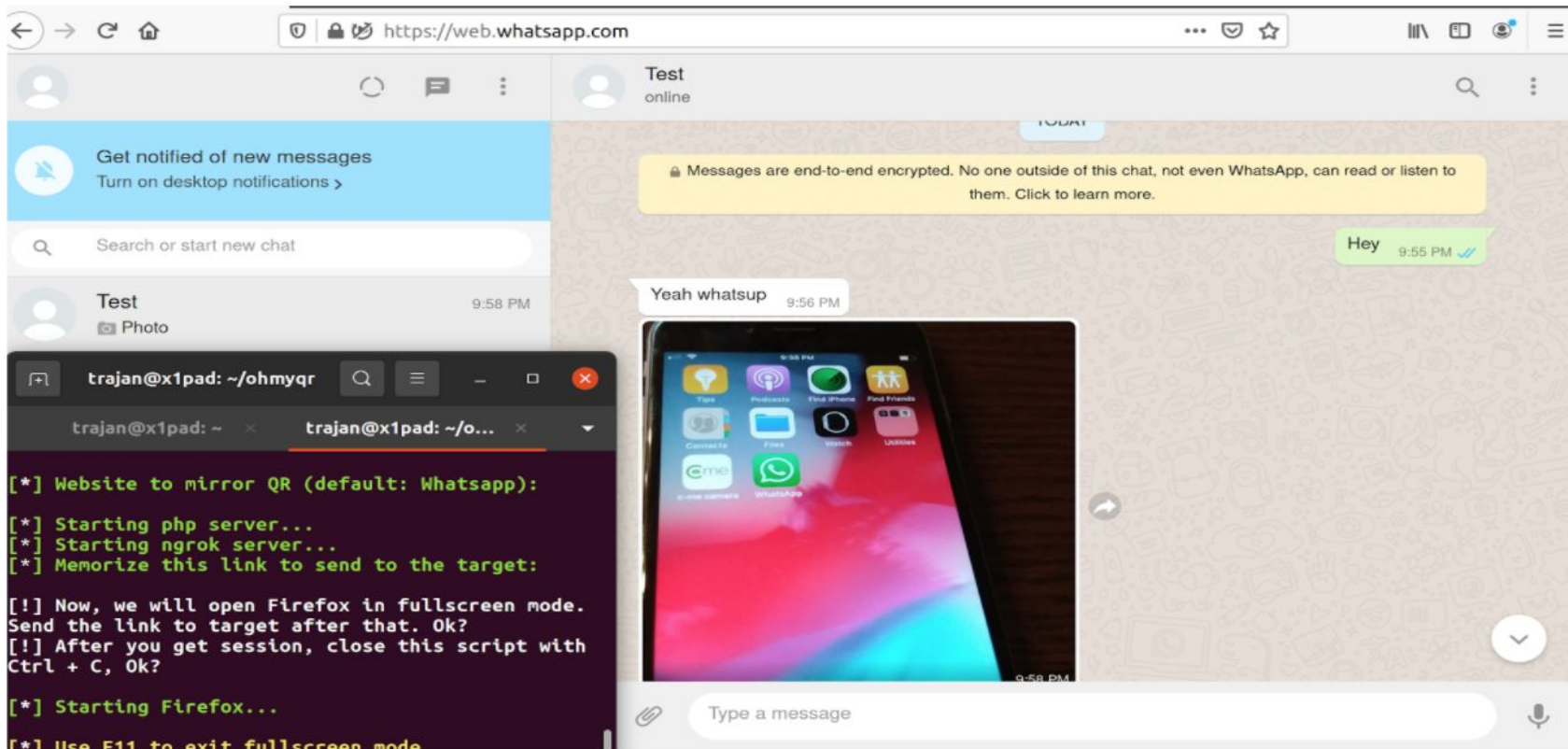
[*] Website to mirror QR (default: Whatsapp):
[*] Downloading Ngrok...
[*] Starting php server...
[*] Starting ngrok server...
[*] Memorize this link to send to the target:

[!] Now, we will open Firefox in fullscreen mode. Send the link to target
    after that. Ok?
[!] After you get session, close this script with Ctrl + C, Ok?

[*] Starting Firefox...

[*] Use F11 to exit fullscreen mode
```

# Ohmyqr <https://github.com/ryptedwolf/ohmyqr>



# Telegram scraper demo

TELEG SCRAPER

version : 3.1  
[youtube.com/theunknon](https://youtube.com/theunknon)

[+] Choose a group to scrape members :

[0] -

[1] -

[2] - Percent27 chat

[3] -

[+] Enter a Number : 2

[+] Fetching Members...

[+] Saving In file...

[+] Members scraped successfully.

trajan@x1pad:~/Desktop/TeleGram-Scraper\$

# Telegram scraper

```
GNU nano 4.8                                members.csv
username,user id,access hash,name,group,group id
1555950991,1788129653377101710,██████████,Percent27 chat,1455002855
14,4355245574939546373,██████████ chat,1455002855
e97727369,4886517423230206258,██████████,Percent27 chat,1455002855
14,-7328621742589659270,██████████,Percent27 chat,1455002855
c63954706,-6800696261772996419,██████████,Percent27 chat,1455002855
12,8735922234415054506,██████████,Percent27 chat,1455002855
14,7701580529362858845,██████████,Percent27 chat,1455002855
c1259764046,-4647693630717355011,██████████,Percent27 chat,1455002855
11,1835596105381431997,██████████,Percent27 chat,1455002855
y047,357812520,2431068641922009645,██████████,Percent27 chat,1455002855
118,5613913057767187375,██████████,Percent27 chat,1455002855
```

# TELEG SCRAPER

version : 3.1

[youtube.com/theunknon](https://youtube.com/theunknon)

[1] send sms by user ID

[2] send sms by username

Input : 2

[+] Enter Your Message : Percent27!

[+] Sending Message to: ██████████

[+] Waiting 30 seconds

[+] Sending Message to: ██████████

[+] Waiting 30 seconds

[+] Sending Message to: ██████████

[+] Waiting 30 seconds

# Wait there is more...

So why instead of attacking the app why not take over the whole phone...

Here are a couple of tools that i researched:

**AndroRat:** Popular Android Trojan

**Mspy:** Commercial surveillance tool for mobiles.

# AndroRAT still works on Android 9

The screenshot displays the AndroRAT application interface. The top bar shows the 'Andorant Project' logo and the title 'User GUI of imei: [redacted]'. Below the title bar, there are tabs for 'Options', 'Get Android data', 'Send command', and 'Monitoring'. The main content area is divided into two sections: a list of contacts on the left and a detailed view of a selected contact on the right.

The contact list on the left shows five entries, each with a profile picture, a name, and an ID. The first entry has a placeholder image and the name '???'. The second entry has a photo of a woman and the name 'ido (id:9)'. The third entry has a placeholder image and the name '(id:1)'. The fourth entry has a placeholder image and the name '(id:4)'. The fifth entry has a red devil icon and the name '(id:7)'. The right section shows the 'Informations' for the selected contact, including fields for 'Id', 'Name', 'Number', 'Address', and 'Email', all of which are currently set to 'n/a'. Below these fields are buttons for 'More informations', 'Call', and 'SMS'. At the bottom of the right section is a 'General options' section with a 'Refresh list' button.

On the left side of the interface, there is a log window showing system events. The log entries include:

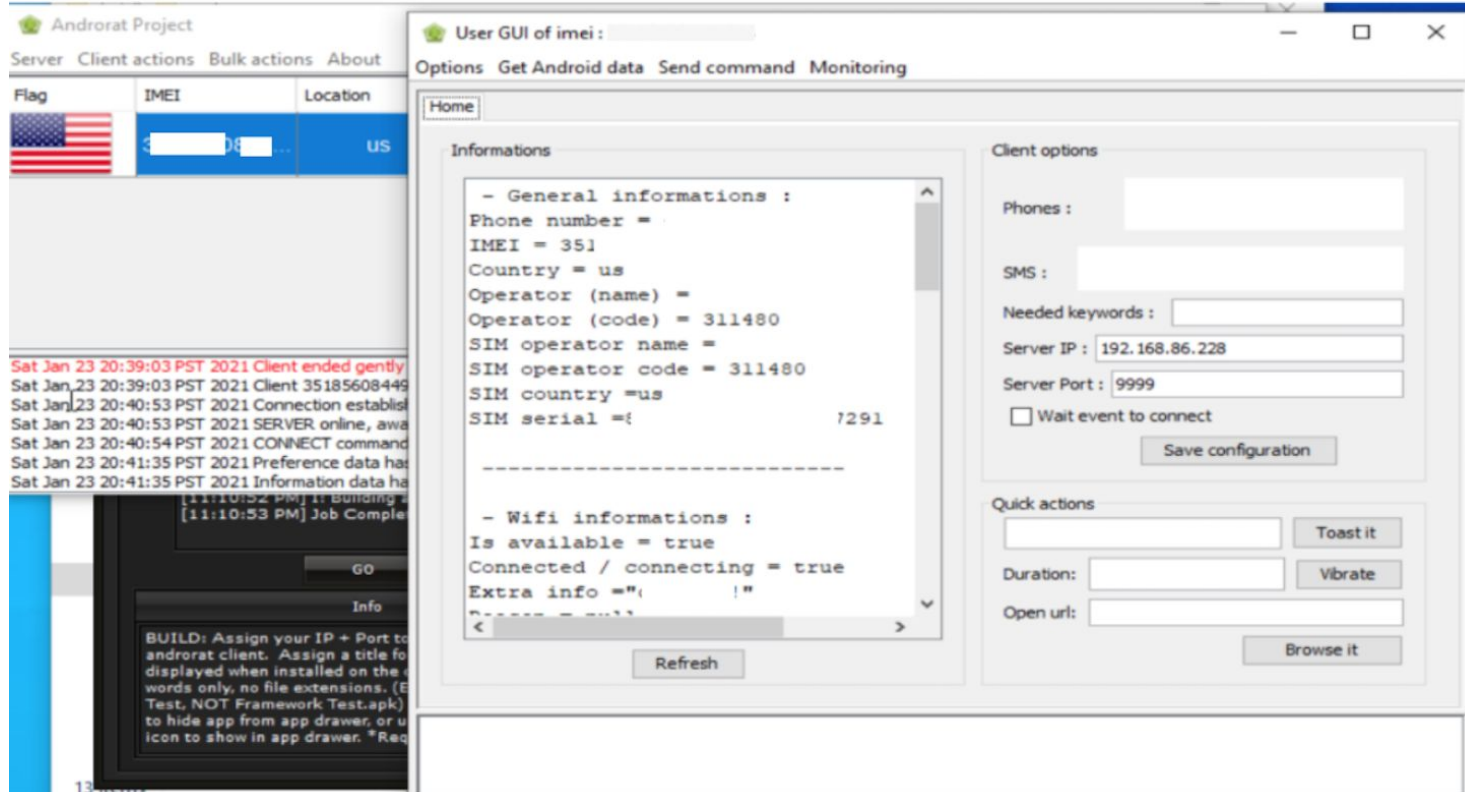
- Sat Jan 23 20:26:56 PST 2021 Client 3
- Sat Jan 23 20:27:55 PST 2021 Connec
- Sat Jan 23 20:27:55 PST 2021 SERVER
- Sat Jan 23 20:27:55 PST 2021 CONNE
- Sat Jan 23 20:28:28 PST 2021 Prefere
- Sat Jan 23 20:28:28 PST 2021 Informa
- Sat Jan 23 20:29:20 PST 2021 Contac

At the bottom of the log window, there is a blue box with the text: 'BUILD: Assign your androrat client. Ass displayed when insta words only, no file ex Test, NOT Framework to hide app from app icon to show in app o'.

At the bottom of the main interface, there is a log window showing system events. The log entries include:

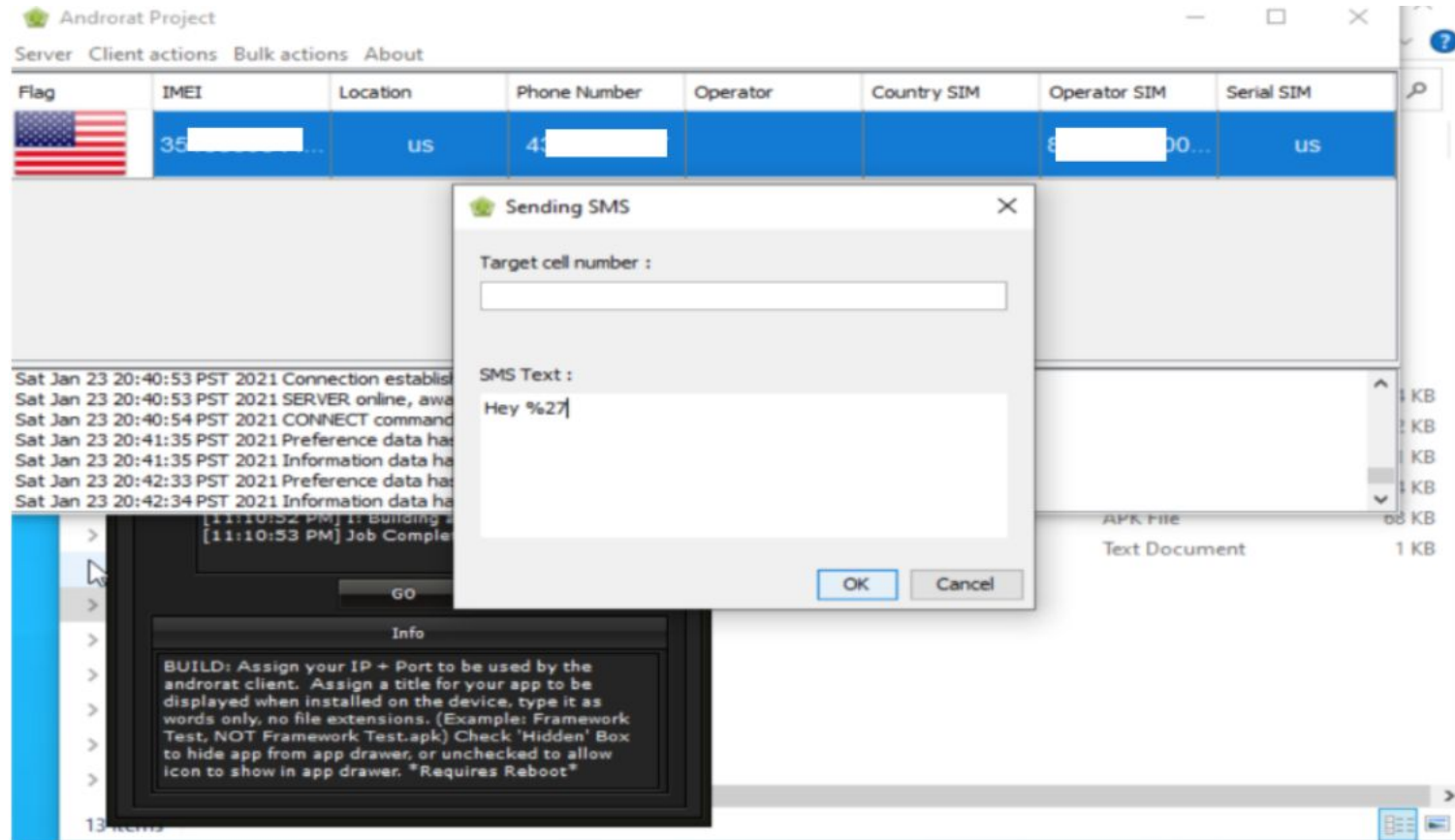
- Sat Jan 23 20:28:58 PST 2021 Error on Client:takePicture failed
- Sat Jan 23 20:29:07 PST 2021 Photo picture request received
- Sat Jan 23 20:29:08 PST 2021 Error on Client:takePicture failed
- Sat Jan 23 20:29:19 PST 2021 Contacts request received

# AndroRAT






# AndroRAT





# MSPY

 Your id:

My Phone

BASIC

Dashboard

GENERAL FEATURES

Contacts

Text Messages

Calls

Events

Photo

Video

Wi-Fi networks

Dashboard

PURCHASE NEW PACKAGE

Account

Account Type: BASIC

Expiration Date:

Auto-Renewal:  
☒ Disabled ☐ Enabled

Expires in 30 days: 

RENEW

Target Device info

My Phone

Android Version: 9

mSpy build Version: 5.8.7.1

IMEI:

92%

Monitor Wi-Fi Networks: On

Mobile Network: On

Target Device Activity

My Phone

BASIC

Dashboard

GENERAL FEATURES

Contacts

Text Messages

Calls

Events

Photo

Video


Wi-Fi networks

Calls

PURCHASE NEW PACKAGE

State	Number	Name	Duration	Date
Missed		Unknown	00:00:00	Jan 22, 2021 9:11 PM
Missed		Unknown	00:00:00	Jan 22, 2021 7:34 PM
Missed		Unknown	00:00:00	Jan 22, 2021 7:12 PM
Missed		Unknown	00:00:00	Jan 22, 2021 4:07 PM
Missed		Unknown	00:00:00	Jan 22, 2021 4:01 PM
Missed		Unknown	00:00:00	Jan 22, 2021 12:18 AM
Missed		Unknown	00:00:00	Jan 21, 2021 8:03 PM
Missed		Unknown	00:00:00	Jan 21, 2021 5:54 PM

# MSPY

 Your ID: [redacted]

My Phone

Dashboard

GENERAL FEATURES

Contacts

Text Messages

Calls

Events

Photo

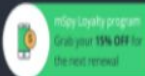
Video

Wi-Fi networks

Keyword tracking

Keylogger

Installed APPs

 mSpy Loyalty program  
Grab your 15% OFF for the next renewal

Keyword Alerts

PURCHASE NEW PACKAGE

Billing

Profile

Help

RULES


DETECTED KEYWORDS

Keyword Tracking	Detected in	Message	Created at
hackmiami	Sms.message	Hackmiami	

1 of 1

## mSpy Keyword Alert

no-reply@mspyonline.com <no-reply@mspyonline.com>  
to me

 mSpy

New alerted words!

Dear ,

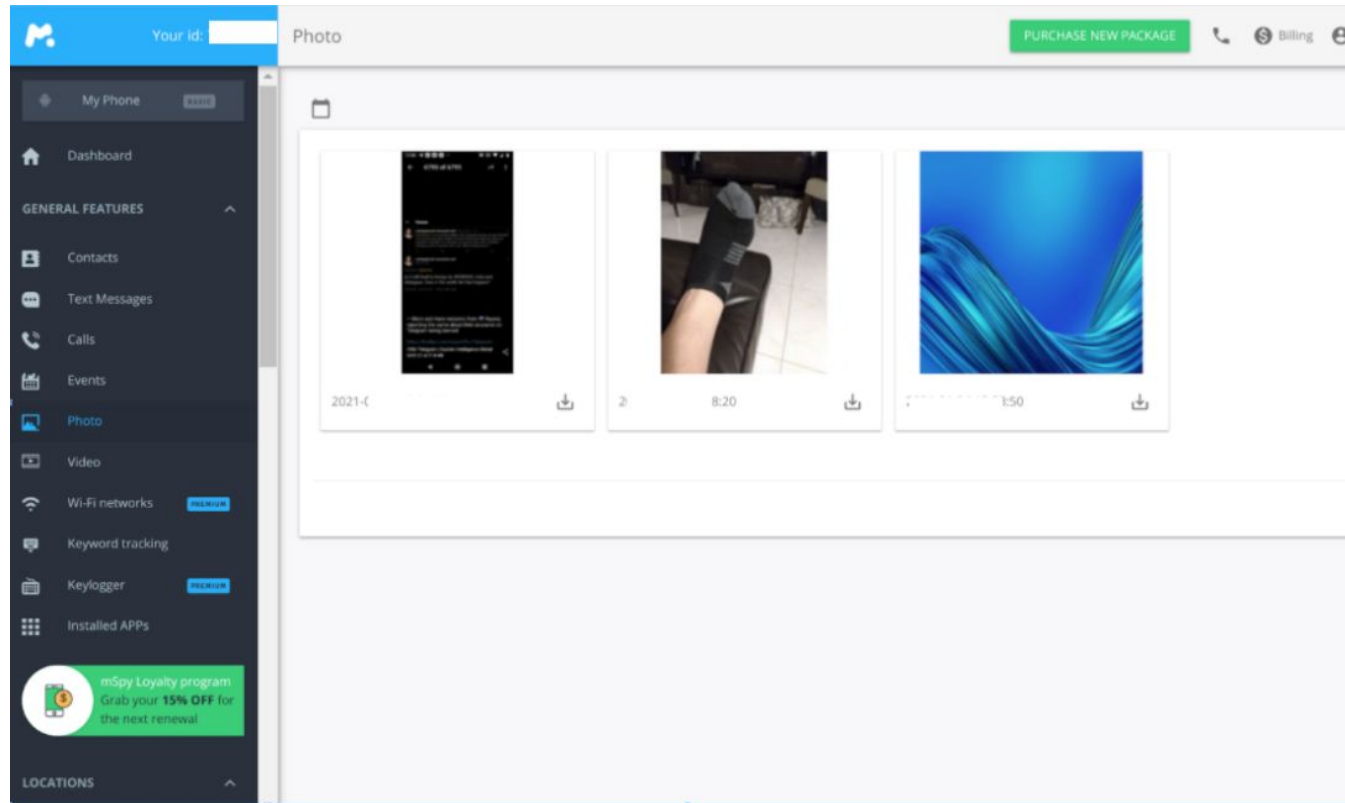
New alerted words have been found in log data. Detailed information can be found by authorizing to Control Panel.

New alerted words during last 1 hour(s): 1

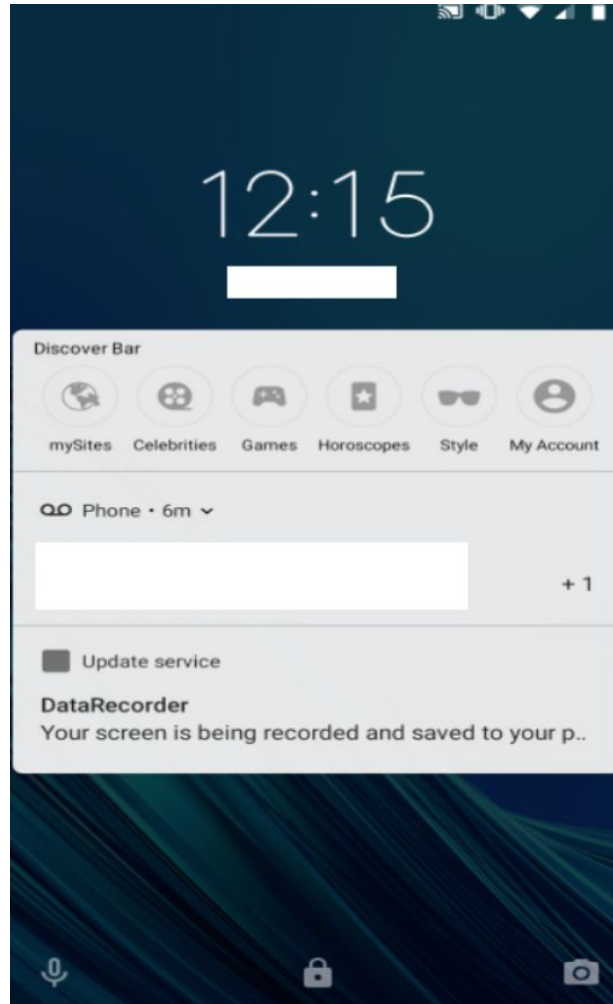
To customize your settings visit Alerts Words section inside your personal mSpy account. Thanks for using mSpy!

Need additional help?  
Contact us at [support@mspy.com](mailto:support@mspy.com)


# MSPY





# MSPY




# MSPY apple


Your ID:

Set up new pho... BASIC

Wizard

Terms of Use

Wizard



**This phone is locked with two-factor authentication**

The verification code will be sent to a monitored device and will appear on its screen

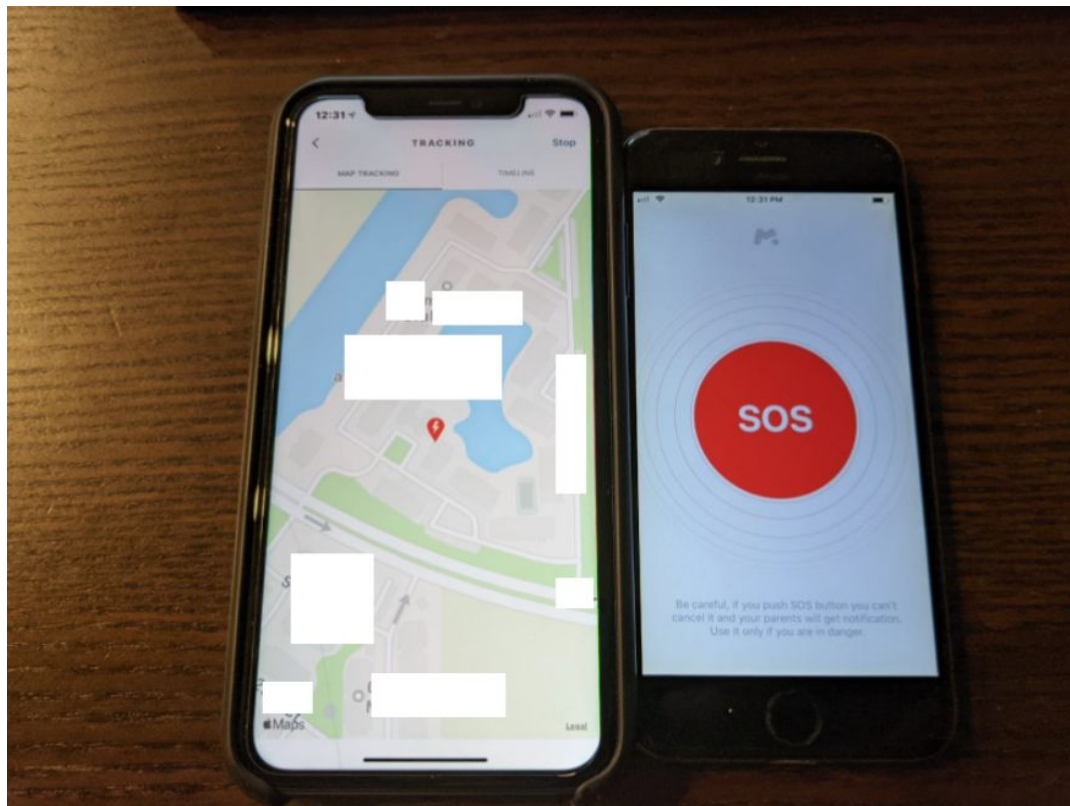
BACK

SEND CODE

PURCHASE NEW PACKAGE



# MSPY Apple



# Mitigation

- Do not root, jailbreak
- Whatsapp may be good for business but not for privacy (Remember don't mix both)
- Setup MFA at every sensitive application
- Iphone most secure device
- Signal is the most private messaging Application
- Lock up your phone, do not even show texts on your screen when locked
- Do not install apps from unknown sources
- Do not even open messages from unknown sources
- When in doubt factory reset, DISCARD device
- Telegram is cool for research use it with burner not for private
- Activate find my phone or equivalent, be ready to wipe it if lost or stolen
- Do not back up your whatsapp chats if you still use it
- Keep phone updated use security products for mobiles
- Google Fi is the most secure phone carrier (Almost impossible to SIM SWAP)
- Do not mix business with pleasure (Phone for private, phone for business)

# Thank you

[www.rodsoto.net](http://www.rodsoto.net)

@rodsoto