Whatsapp, Signal & Telegram Attack Vectors

@rodsoto
www.rodsoto.net

$whoami

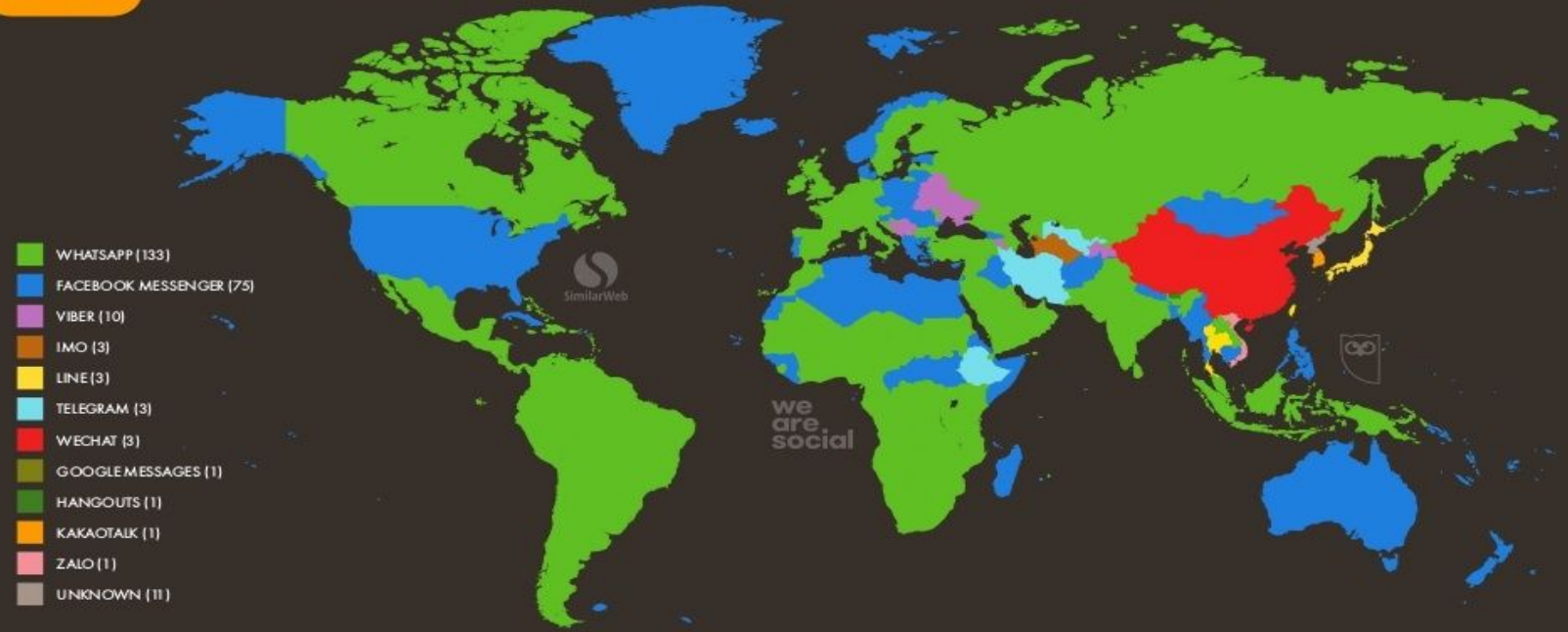
Over 15 years of experience in information technology and security. He has spoken at ISSA, ISC2, OWASP, DEFCON, RSA Conference,Hackmiami, DerbyCon, Splunk .CONF, Black Hat,BSides, Underground Economy and also been featured in Rolling Stone Magazine, Pentest Magazine, Univision, BBC, Forbes, VICE, Fox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



83

SOURCE: BASED ON SIMILARWEB'S ALGORITHM INTEGRATING CURRENT INSTALLS FROM THE GOOGLE PLAY STORE WITH ACTIVE APP USERS (DECEMBER 2018).
NOTE: FIGURES IN PARENTHESES IN THE LEGEND REPRESENT THE NUMBER OF COUNTRIES / TERRITORIES IN WHICH EACH PLATFORM IS THE TOP-RANKED MESSENGER APP.

Hootsuite™ we are social

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

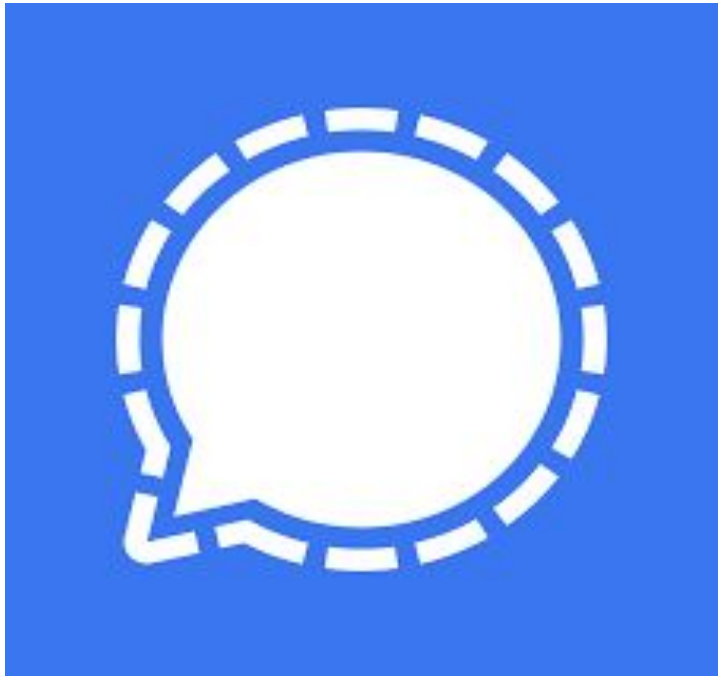
Telegram

- 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.[101][102] 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.

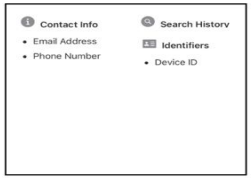
Security comparisons

	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

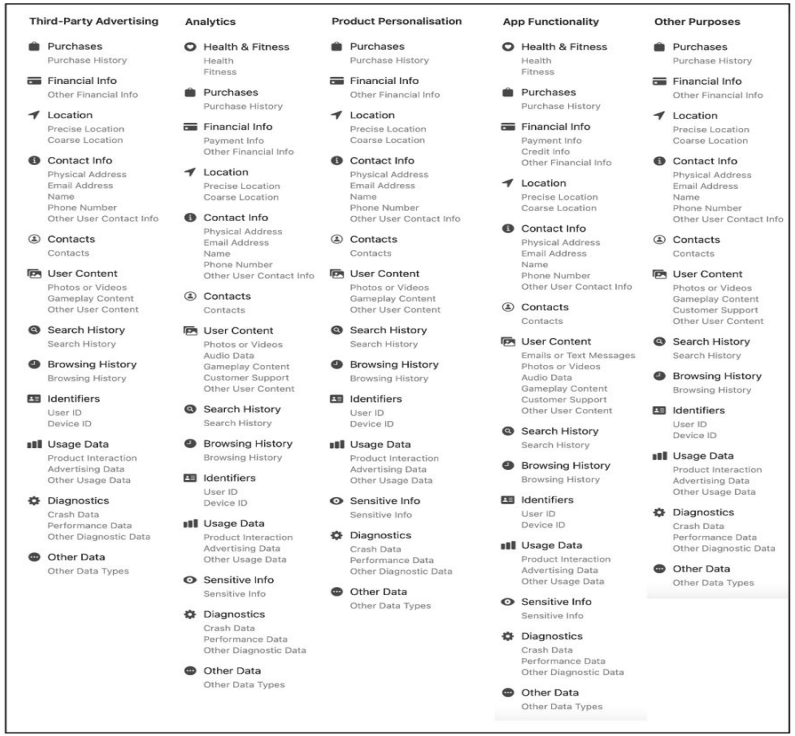
Signal
'Data Linked To You'

iMessage
'Data Linked To You'



WhatsApp
'Data Linked To You'

Facebook Messenger
'Data Linked To You'

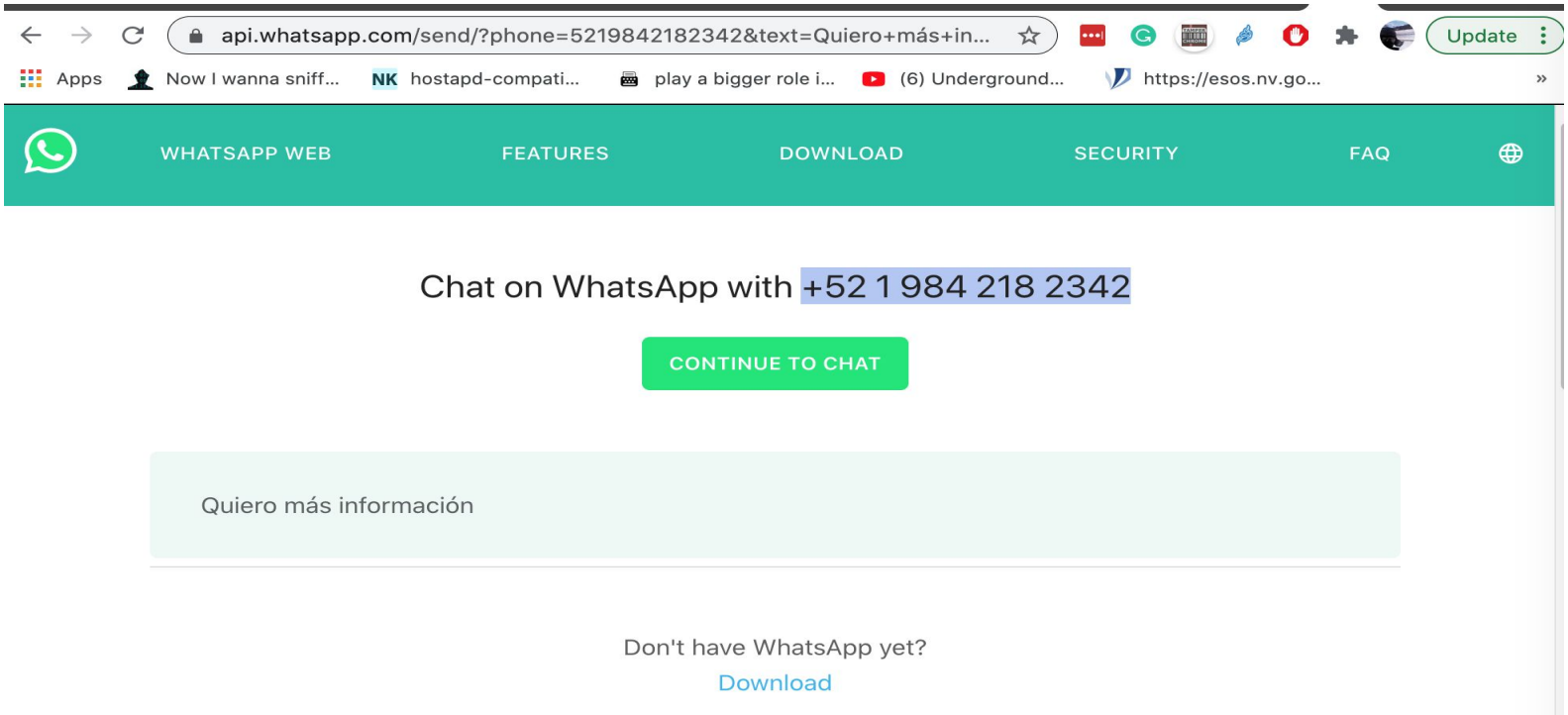


Vulnerabilities & Exploitation

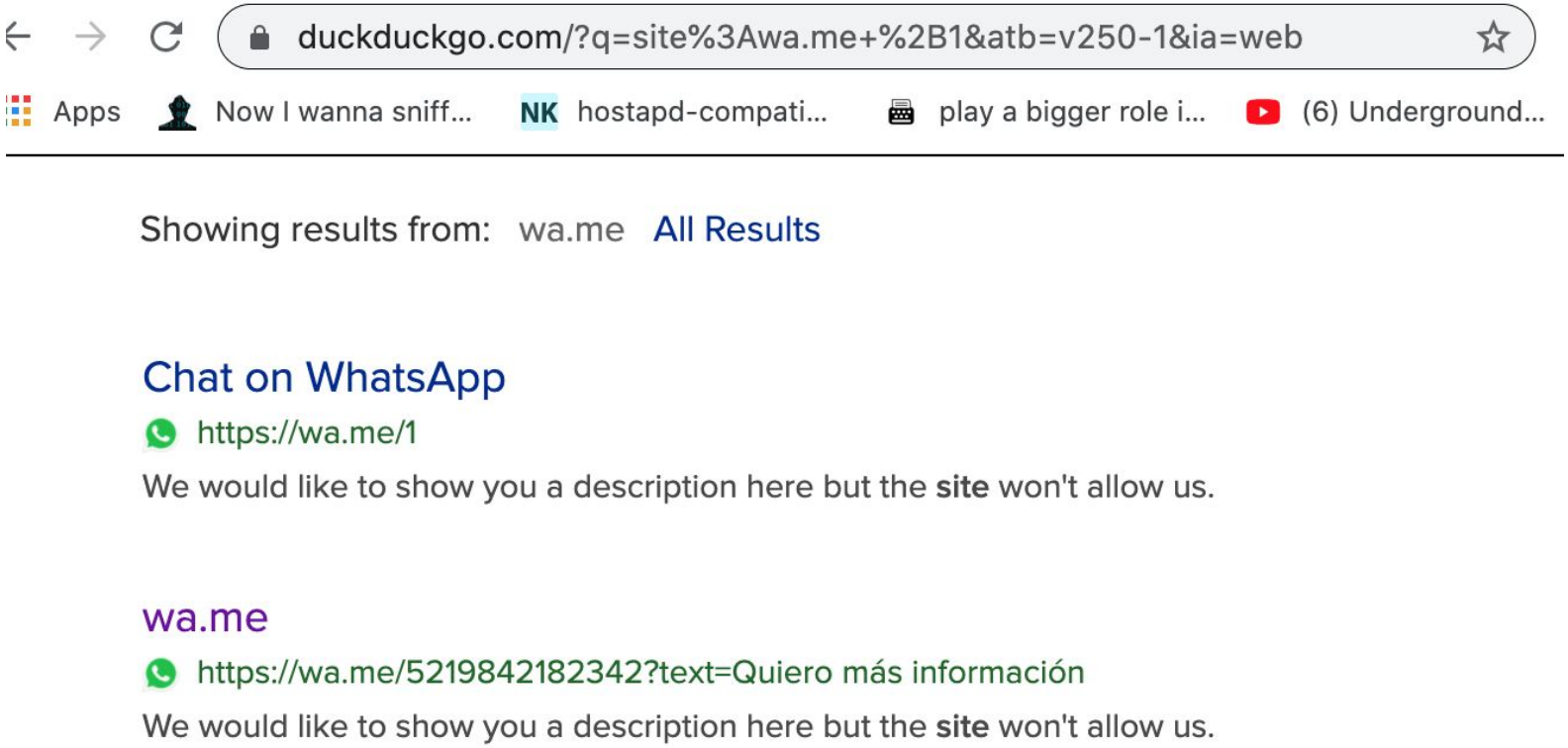
Whatsapp	Signal	Telegram
Link Previews	CVE-2020-5753 -- DNS Leakage	Telegram Scraper - Demo
Invalid Characters	CVE-2019-9970 -- Invalid Character -- IDN homograph attack	Telegrab -- steals telegram channel
QR Hijack -- Demo	CVE-2019-19954 -- Signal Desktop Privesc	Shadow Sessions via Malicious Apps (Does 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

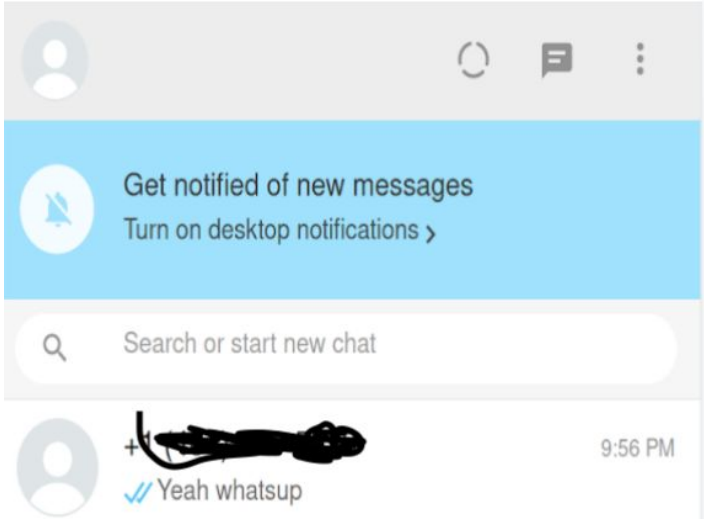
Here are web search engines indexing whatsapp conversations...

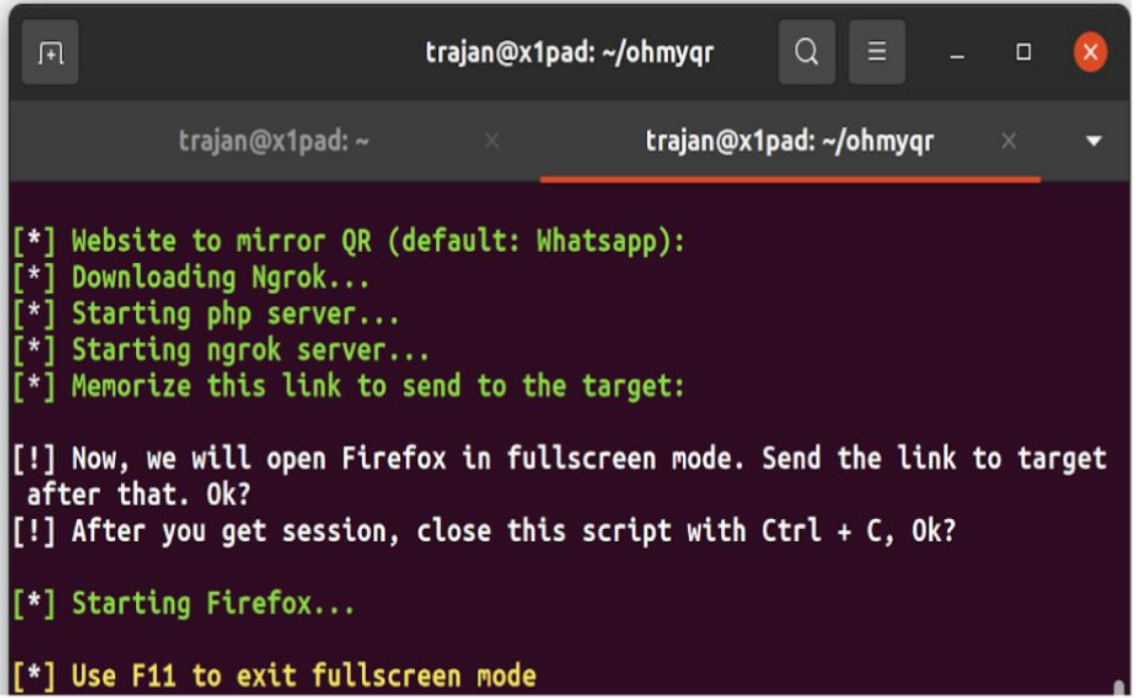


Search engines indexing whatsapp conversations

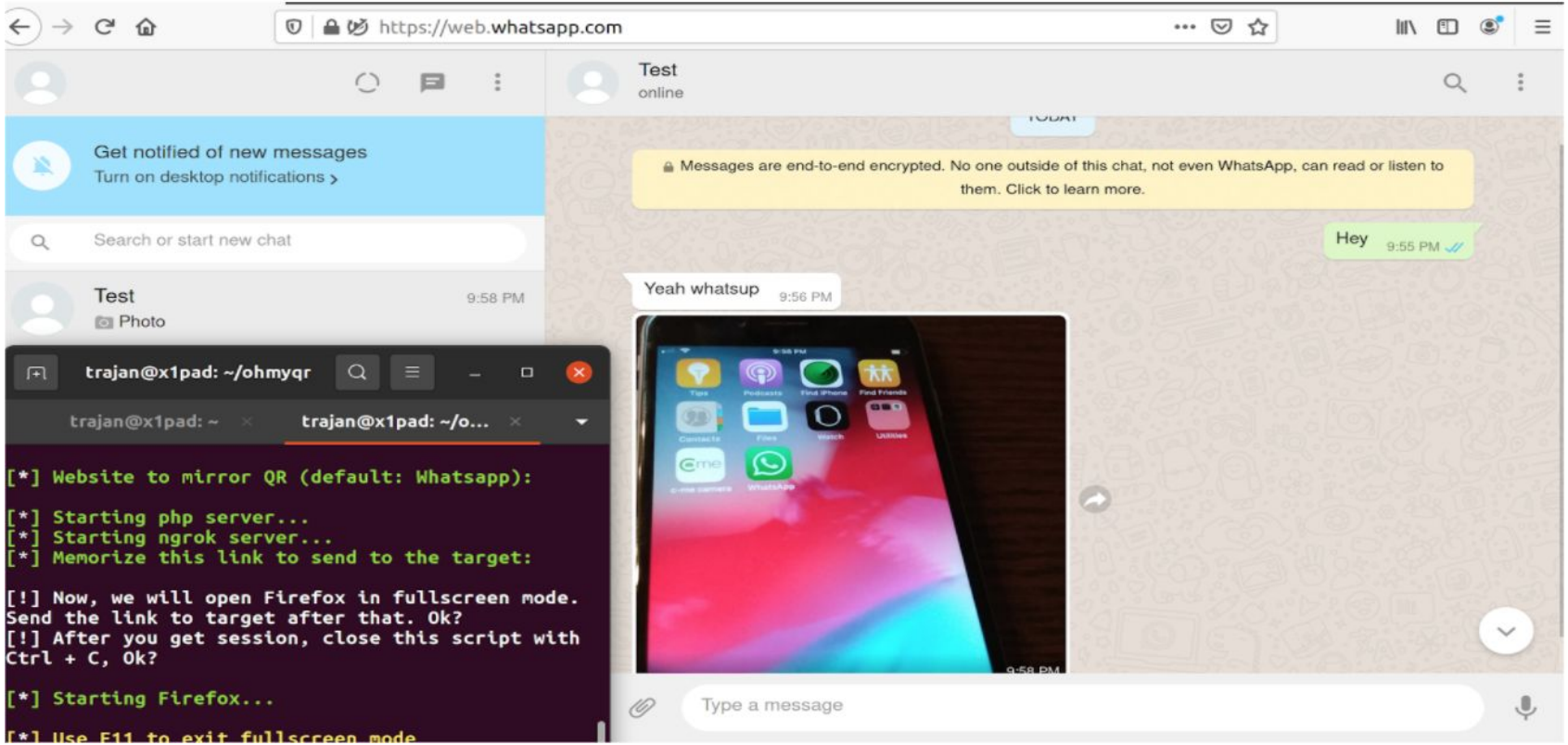


QR Hijack https://github.com/cryptedwolf/ohmyqr

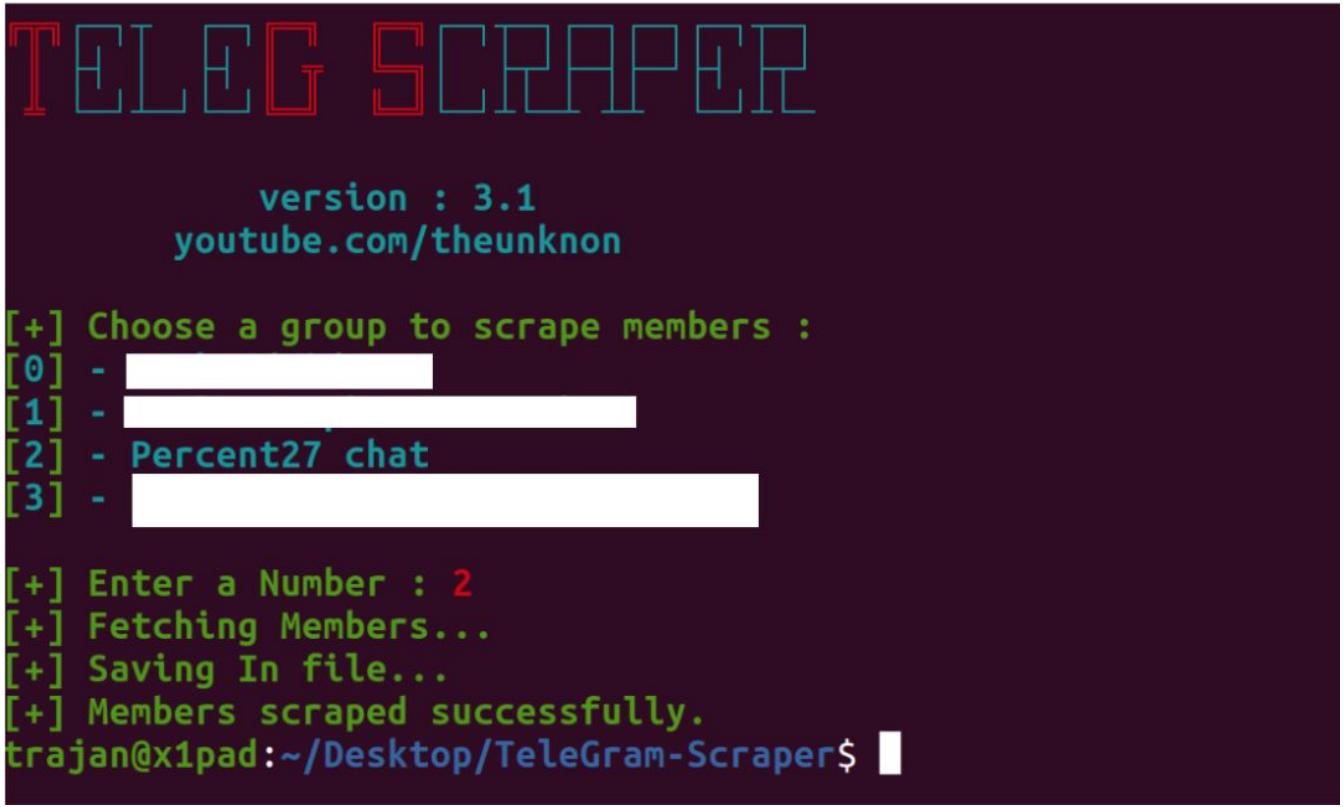




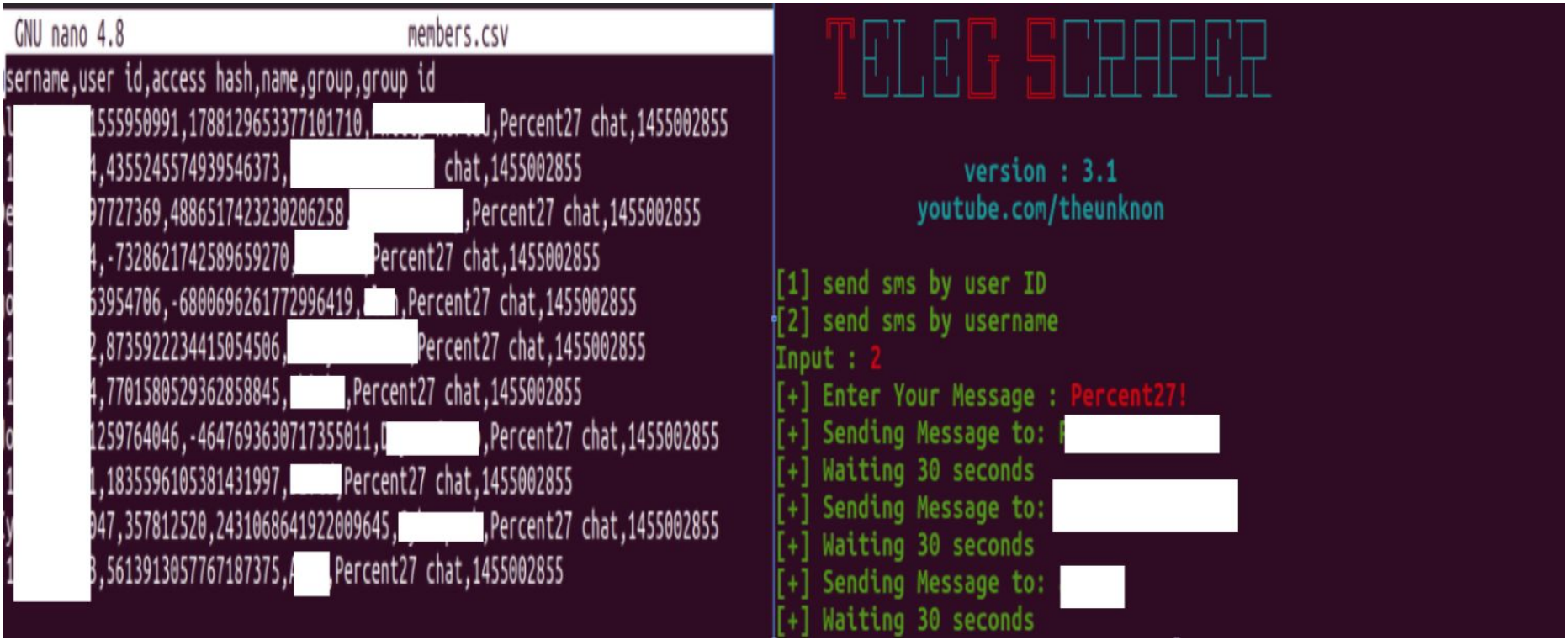
Ohmyqr https://github.com/cryptedwolf/ohmyqr



Telegram scraper demo



Telegram scraper



Wait there is more...

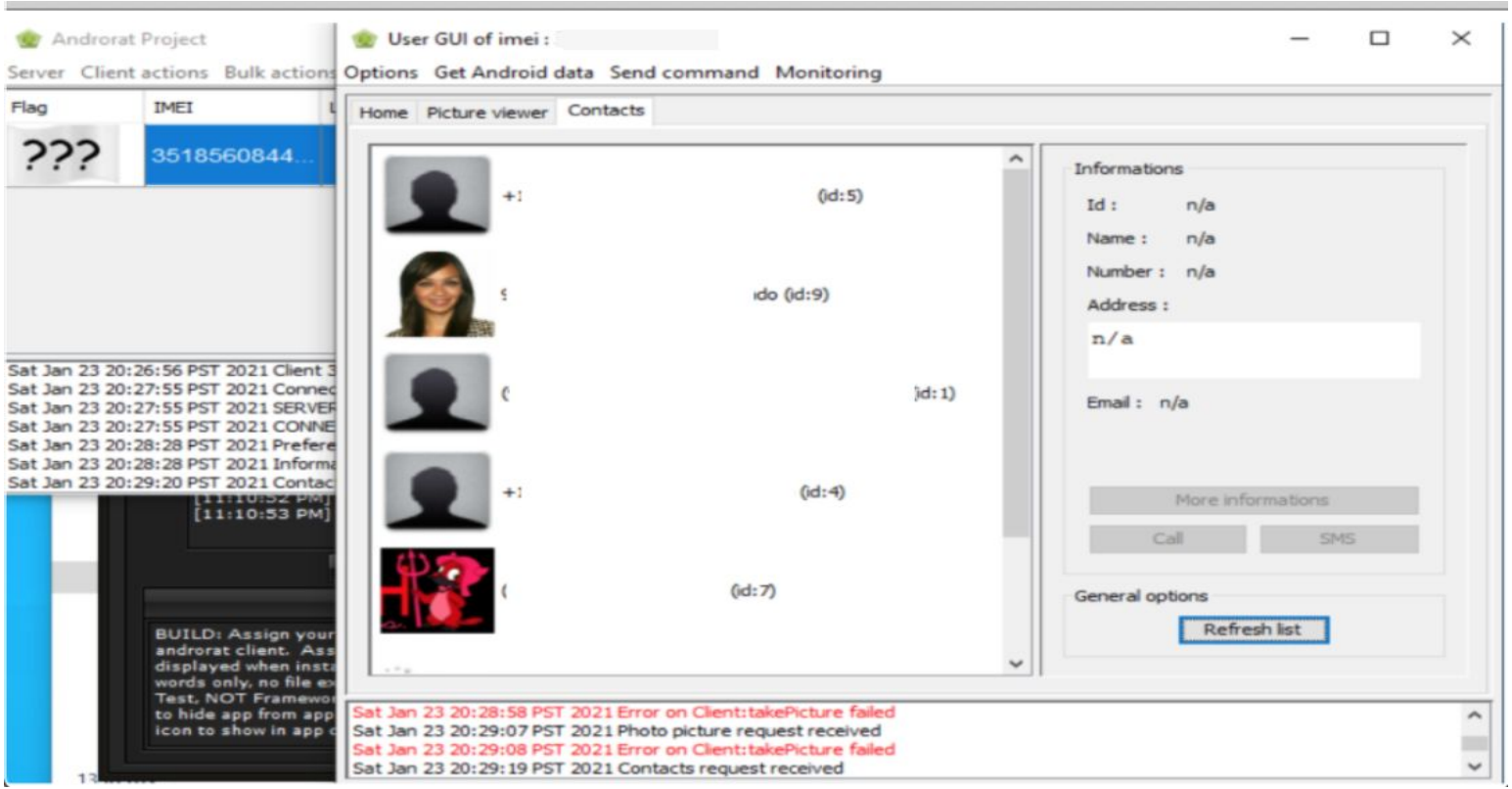
So why instead of attacking the app why not take over the whole phone…

Here are a couple of tools that i researched:

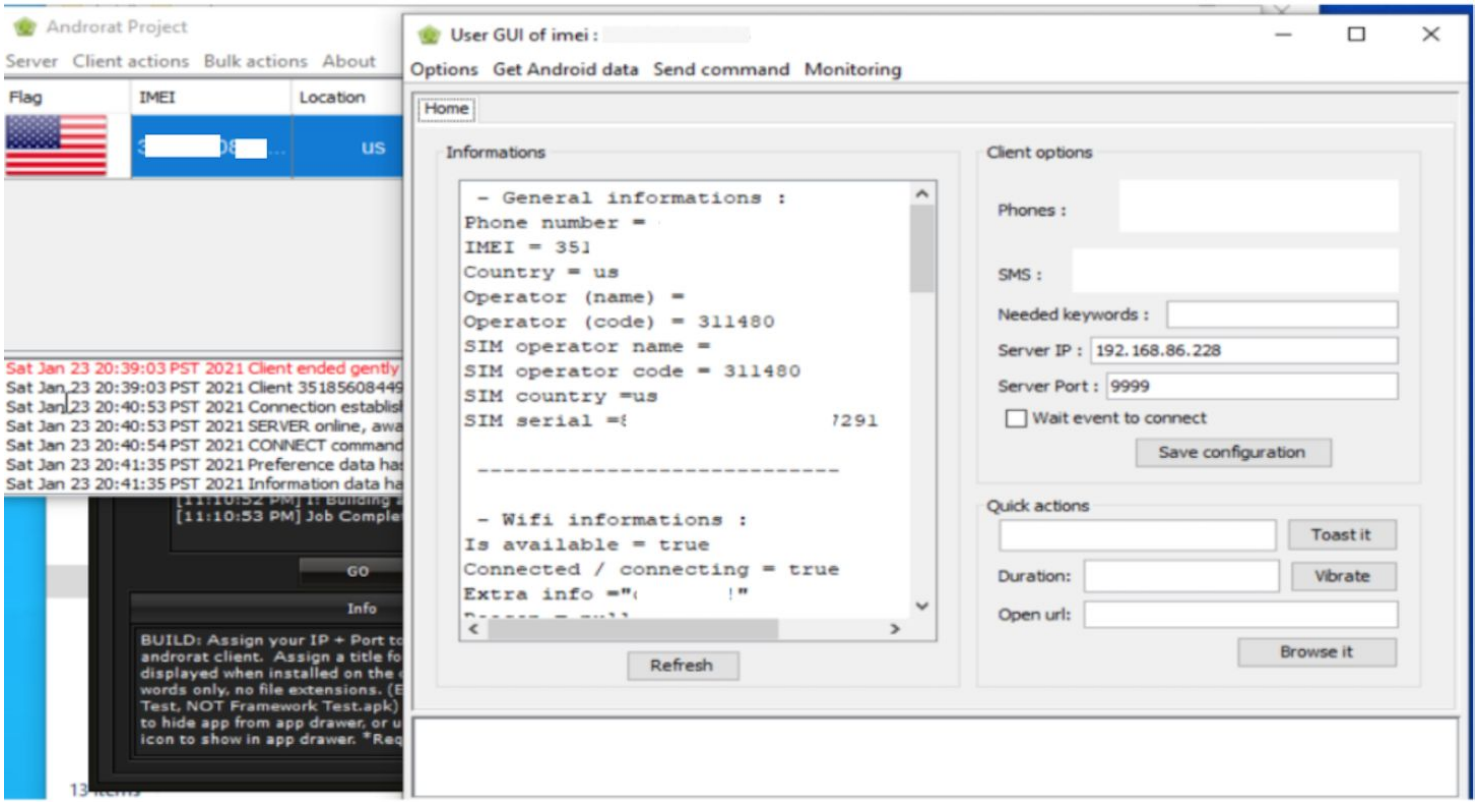
AndroRat: Popular Android Trojan

Mspy: Commercial surveillance tool for mobiles.

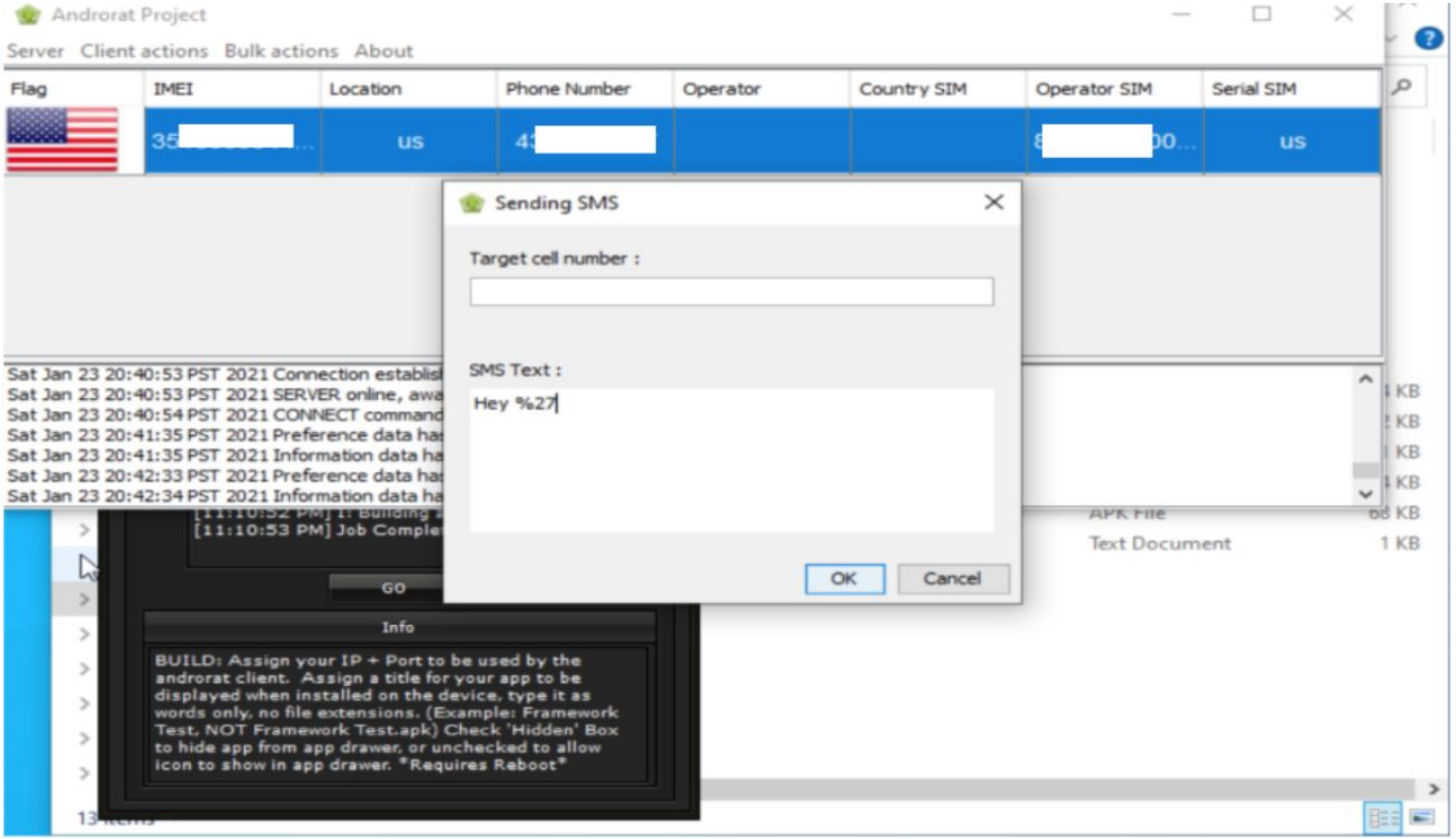
AndroRAT still works on Android 9



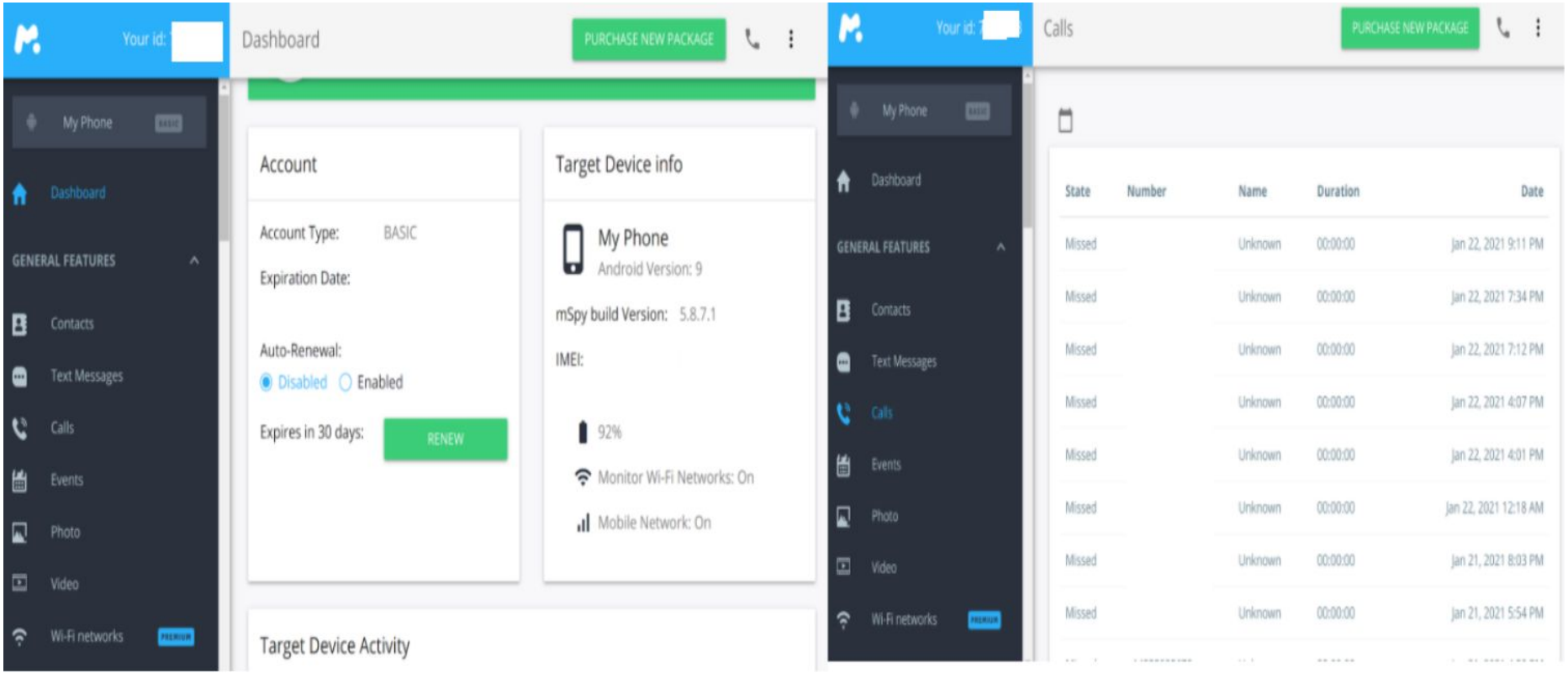
AndroRAT


Androrat Project
Server Client actions Bulk actions About
Flag
IMEI
Location
US
Sat Jan 23 20:39:03 PST 2021 Client ended gently
Sat Jan 23 20:39:03 PST 2021 Client 35185608449
Sat Jan 23 20:40:53 PST 2021 Connection establish
Sat Jan 23 20:40:53 PST 2021 SERVER online, awa
Sat Jan 23 20:40:54 PST 2021 CONNECT command
Sat Jan 23 20:41:35 PST 2021 Preference data ha
Sat Jan 23 20:41:35 PST 2021 Information data ha
[11:10:53 PM] Job Comple
GO
Info
BUILD: Assign your IP + Port to
androrat client. Assign a title fo
displayed when installed on the
words only, no file extensions. (E
Test, NOT Framework Test.apk)
to hide app from app drawer, or u
icon to show in app drawer. *Req
User GUI of imei :
Options Get Android data Send command Monitoring
Home
Informations
- General informations :
Phone number =
IMEI = 351
Country = us
Operator (name) =
Operator (code) = 311480
SIM operator name =
SIM operator code = 311480
SIM country =us
SIM serial =(7291
- Wifi informations :
Is available = true
Connected / connecting = true
Extra info ="(!"
Refresh
Client options
Phones :
SMS :
Needed keywords :
Server IP : 192.168.86.228
Server Port : 9999
Wait event to connect
Save configuration
Quick actions
Toast it
Duration:
Vibrate
Open url:
Browse it

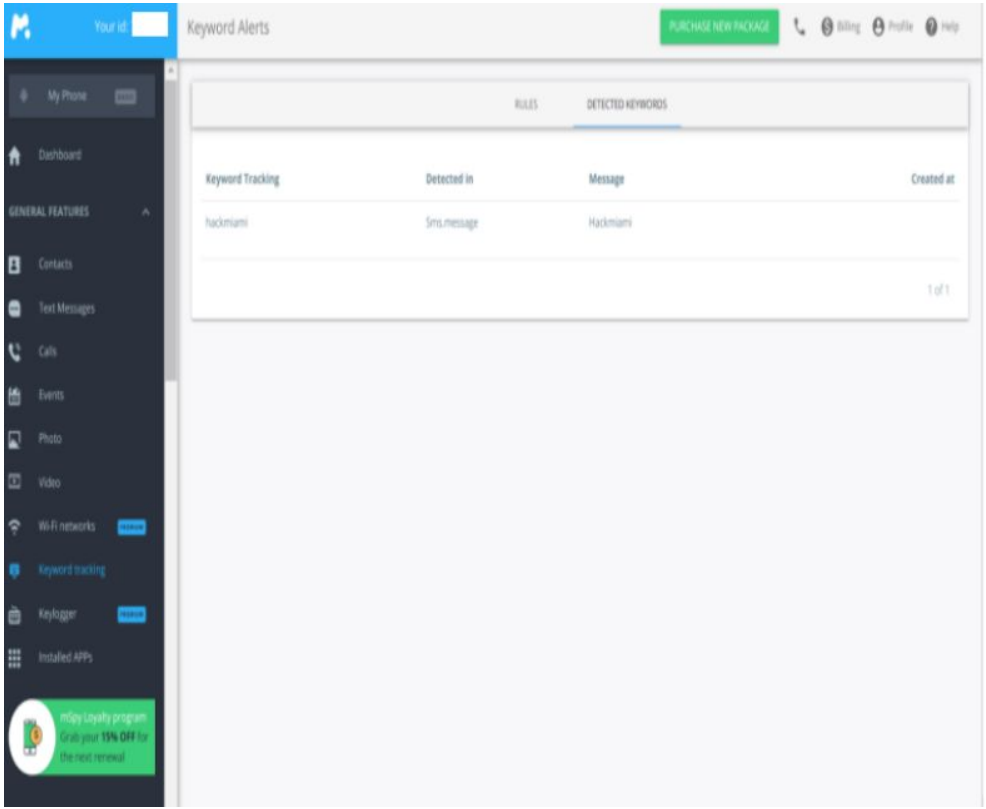
AndroRAT

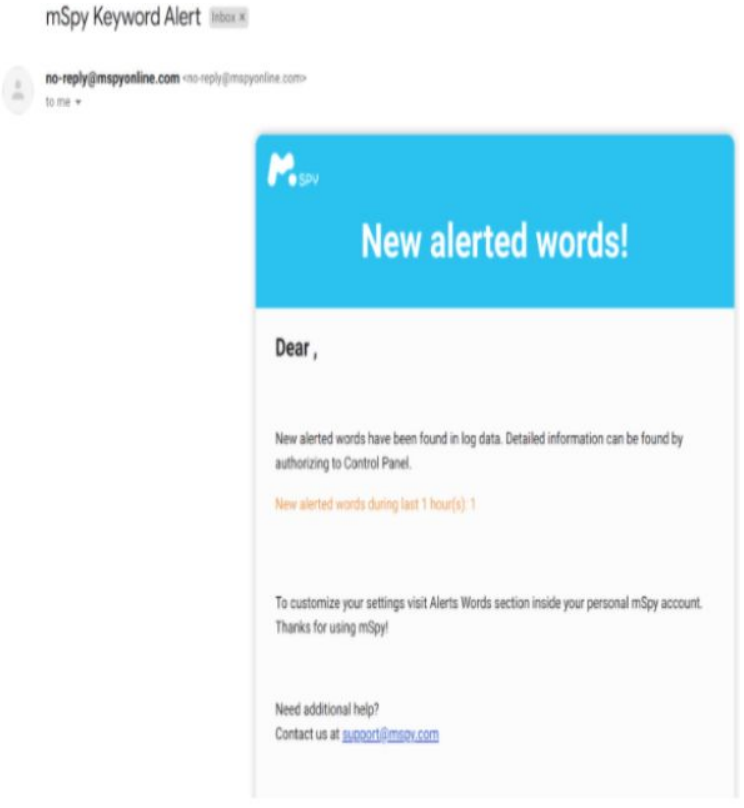

Androrat Project
Server
Client actions
Bulk actions
About
Flag
IMEI
Location
Phone Number
Operator
Country SIM
Operator SIM
Serial SIM
us
us
Sending SMS
Target cell number :
SMS Text :
Hey %27
OK
Cancel
Sat Jan 23 20:40:53 PST 2021 Connection establis
Sat Jan 23 20:40:53 PST 2021 SERVER online, awa
Sat Jan 23 20:40:54 PST 2021 CONNECT command
Sat Jan 23 20:41:35 PST 2021 Preference data ha
Sat Jan 23 20:41:35 PST 2021 Information data ha
Sat Jan 23 20:42:33 PST 2021 Preference data ha
Sat Jan 23 20:42:34 PST 2021 Information data ha
[11:10:53 PM] Job Comple
GO
Info
BUILD: Assign your IP + Port to be used by the androrat client. Assign a title for your app to be displayed when installed on the device, type it as words only, no file extensions. (Example: Framework Test, NOT Framework Test.apk) Check 'Hidden' Box to hide app from app drawer, or unchecked to allow icon to show in app drawer. *Requires Reboot*
Text Document
1 KB

MSPY

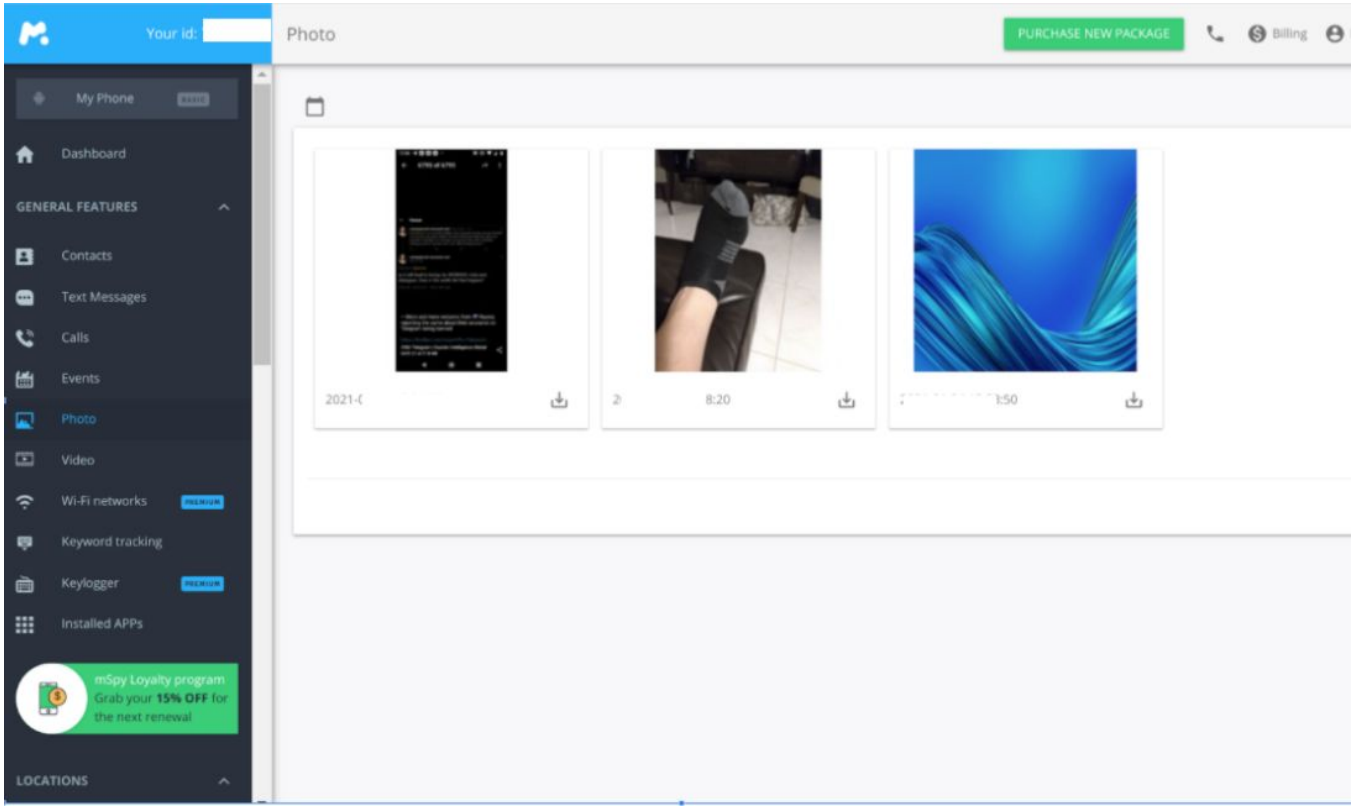

Your id:
Dashboard
PURCHASE NEW PACKAGE
My Phone
Dashboard
GENERAL FEATURES
Contacts
Text Messages
Calls
Events
Photo
Video
Wi-Fi networks
Account
Account Type: BASIC
Expiration Date:
Auto-Renewal:
Disabled
Enabled
Expires in 30 days:
RENEW
Target Device info
My Phone
Android Version: 9
mSpy build Version: 5.8.7.1
IMEI:
92%
Monitor Wi-Fi Networks: On
Mobile Network: On
Target Device Activity
Your id:
Calls
PURCHASE NEW PACKAGE
My Phone
Dashboard
GENERAL FEATURES
Contacts
Text Messages
Calls
Events
Photo
Video
Wi-Fi networks
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

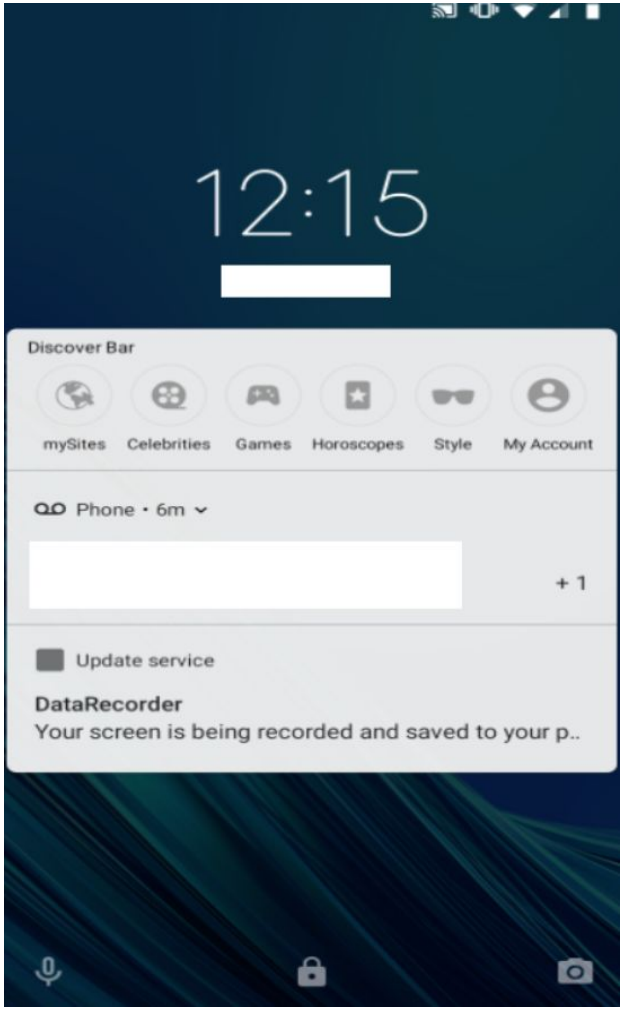

Your id
Keyword Alerts
PURCHASE NEW PACKAGE
Billing
Profile
Help
My Phone
Dashboard
GENERAL FEATURES
Contacts
Text Messages
Calls
Events
Photo
Video
Wi-Fi networks
Keyword tracking
Keylogger
Installed APPs
mSpy Loyalty program
Grab your 15% OFF for the next renewal
RULES
DETECTED KEYWORDS
Keyword Tracking
Detected in
Message
Created at
hackmiami
Sms,message
Hackmiami
1 of 1


mSpy Keyword Alert
Inbox ×
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

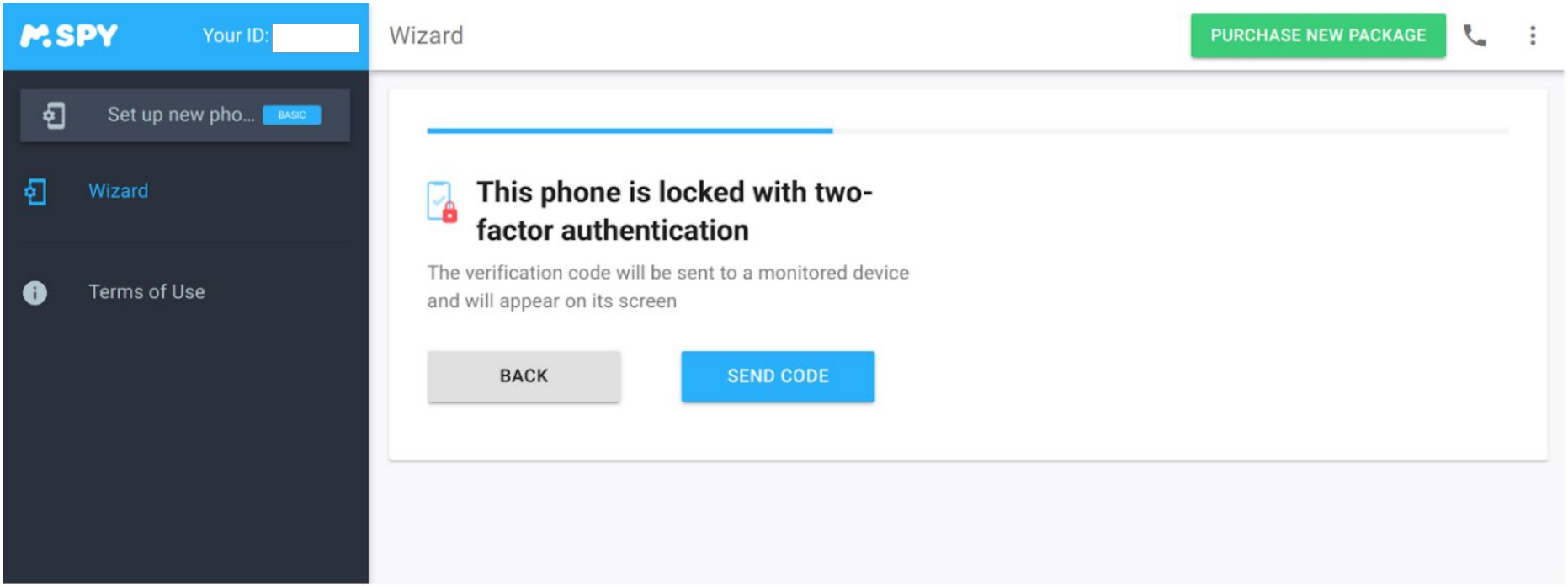
MSPY


Your id:
Photo
PURCHASE NEW PACKAGE
Billing
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
LOCATIONS
8:20

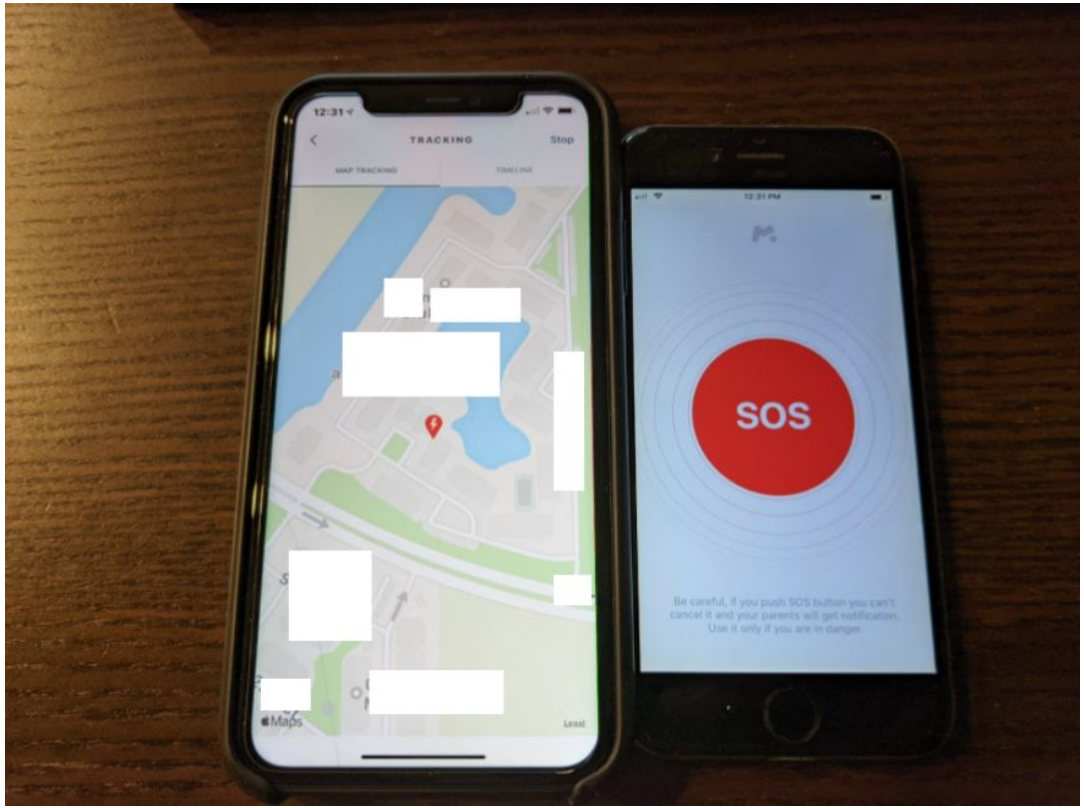
MSPY


12:15
Discover Bar
mySites
Celebrities
Games
Horoscopes
Style
My Account
Phone • 6m
+ 1
Update service
DataRecorder
Your screen is being recorded and saved to your p..

MSPY apple


M.SPY
Your ID:
Wizard
PURCHASE NEW PACKAGE
Set up new pho...
BASIC
Wizard
Terms of Use
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

MSPY Apple


12:31
TRACKING
Stop
MAP TRACKING
TIMELINE
Maps
Legal
SOS
Be careful, if you push SOS button you can't cancel it and your parents will get notification. Use it only if you are in danger.

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

@rodsoto