myntex

Weaponized Malware and Its Impact on Mobile Security

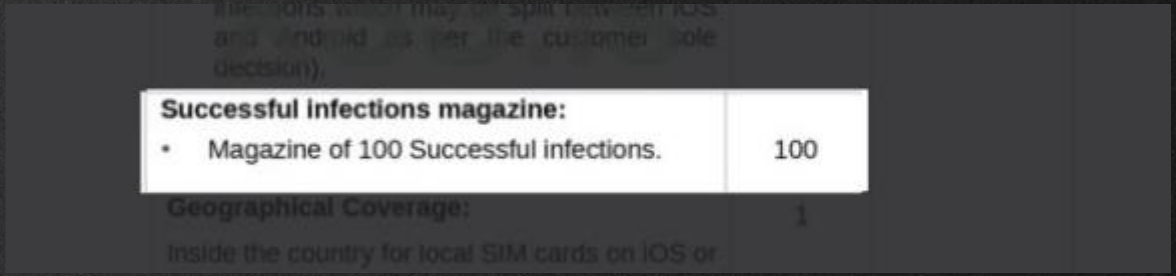
Understanding the Threats

CyberAlberta 2025

Classification: Protected A

Weaponized Malware 101

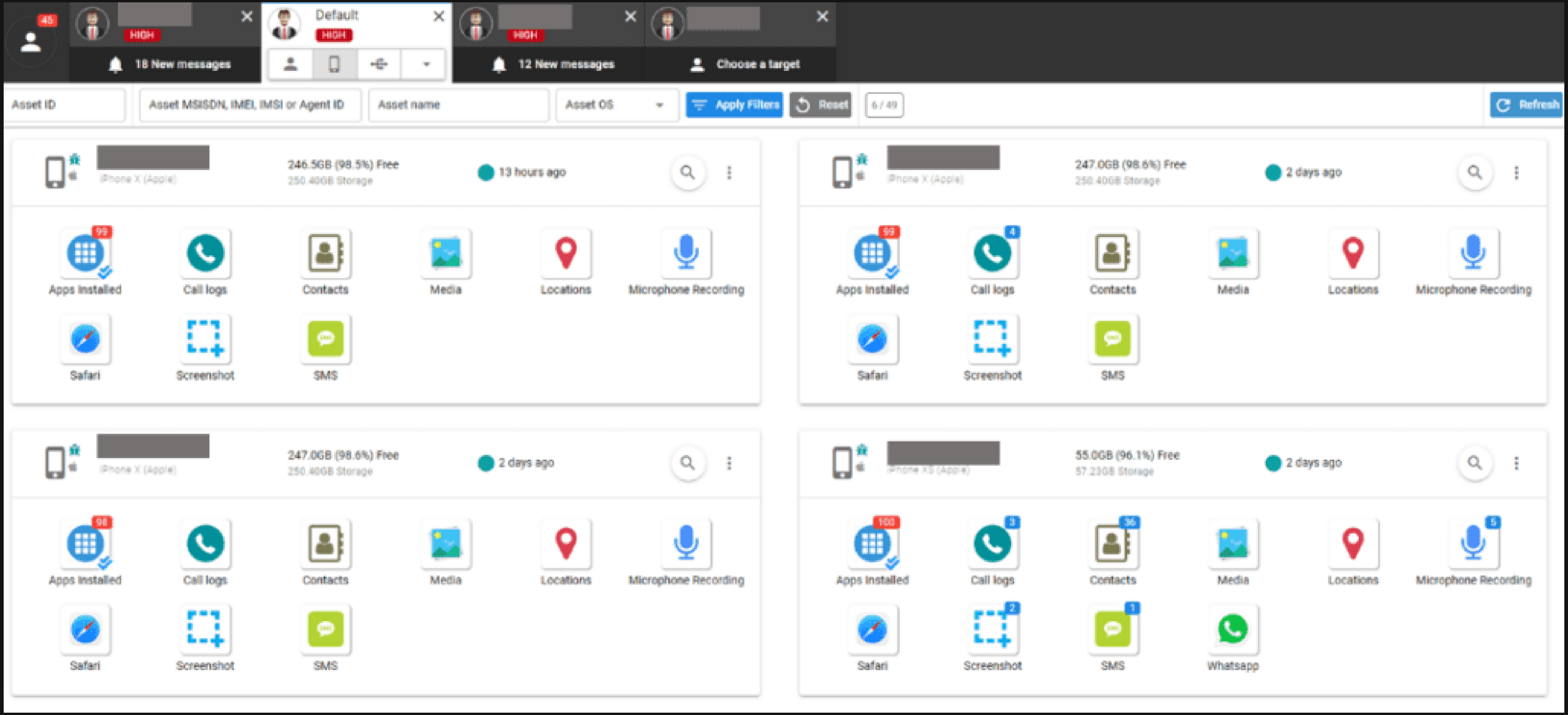
- Industrialization of digital exploits
- Commercially available and employed by government agencies and private entities
- Allows for unauthorized data collection from all spectrum of devices



infections which may be split between iOS and Android as per the customer sole decision).	
Successful infections magazine: • Magazine of 100 Successful infections.	100
Geographical Coverage: Inside the country for local SIM cards on iOS or	1

```
27448_
00274494        Py_SetProgramName(aname);
00274498        Py_Initialize();
002744a4        int64_t x0_1 = PyImport_AddModule("__main__");
002744a8        if (x0_1 != 0)
002744a8        {
002744ac            int64_t x19_1 = x0_1;
002744b4            if (PyEval_ThreadsInitialized() == 0)
```

```
t64_t)shared_fds.0));
t64_t)shared_fds.1));
g_FromUnsignedLongLong(0x12344
```



[redacted]
iPhone X (Apple)
246.5GB (98.5%) Free
250.40GB Storage
13 hours ago

[redacted]
iPhone X (Apple)
247.0GB (98.6%) Free
250.40GB Storage
2 days ago

[redacted]
iPhone X (Apple)
247.0GB (98.6%) Free
250.40GB Storage
2 days ago

[redacted]
iPhone XS (Apple)
55.0GB (96.1%) Free
57.23GB Storage
2 days ago

User interface of management software for Intellexa Predator spyware.

Terminology

- Zero-Click
- One-Click
- Tactical Infection
- Strategic ISP Infection
- MITM
- Command and Control (C2) Server
- Spear Phishing

Key Players

The ‘Predator Files’ investigation shows what we have long feared: that highly invasive surveillance products are being traded on a near industrial scale and are free to operate in the shadows without oversight or any genuine accountability. It proves, yet again, that European countries and institutions have failed to effectively regulate the sale and transfer of these products.

-Agnès Callamard, Amnesty International’s Secretary General

Intellexa Alliance

- Best known for Predator Spyware with zero-click delivery
- Group of companies specializing in advanced spyware, mass surveillance platforms, and tactical infection systems
- Frequent rebranding and changes in corporate structure, making its operations hard to trace.
- Ability to attack 2G/3G/4G/5G

NSO Group

- Developer of Pegasus spyware
- Involved in high-profile legal battles with companies like Apple and WhatsApp
- Real-time surveillance capabilities

RCS

a Cy4gate company

RCS Lab

- Italian surveillance company active for over 30 years
- Best known for Hermit: One-click spyware
- Found embedded in carrier branded applications
- Collaborates with local telecommunications providers

PARAGON

Paragon Solutions

- Less known in the industry
- Zero-click WhatsApp exploit used a malicious PDF

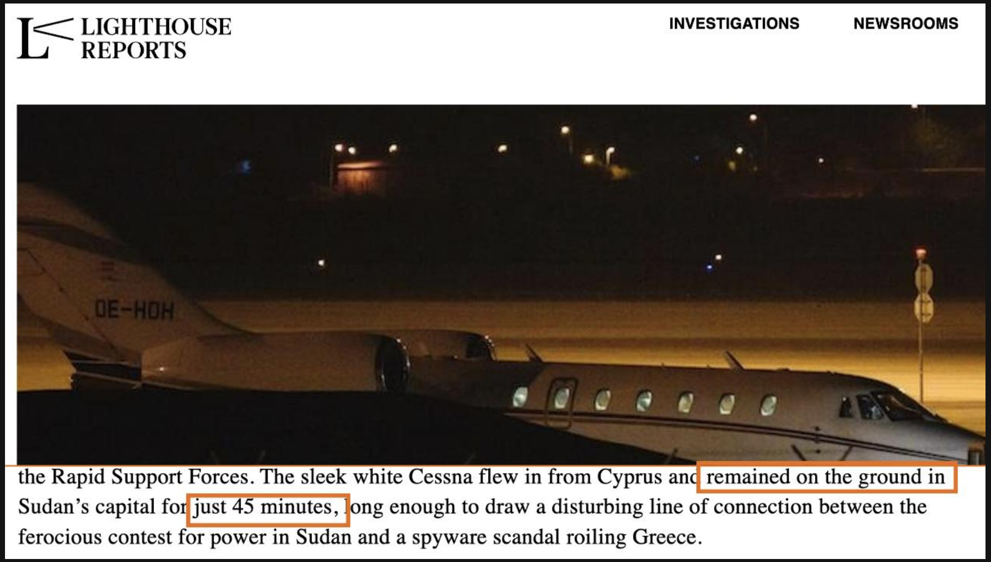
BLACK CUBE

Creative Intelligence

Black Cube

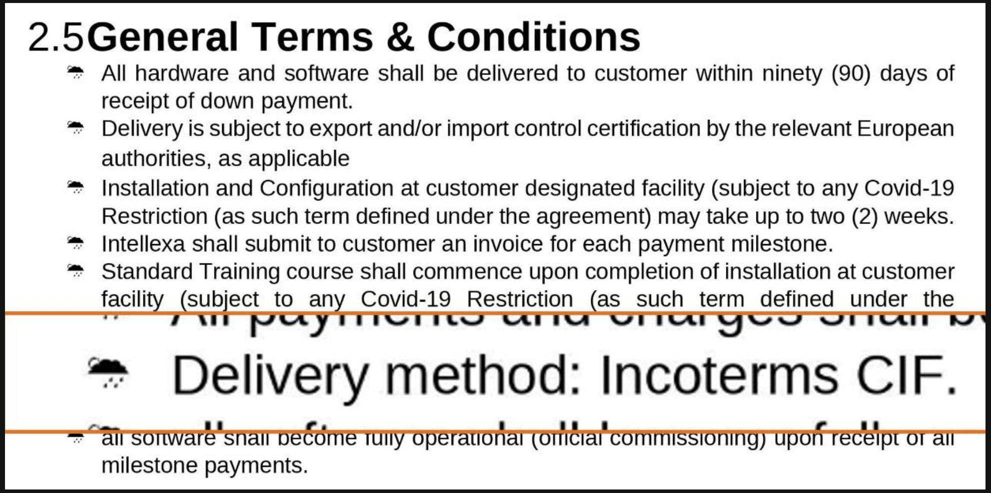
- Bluetooth Zero-Click Tactical Infection known as Arklys
- Assisted Harvey Weinstein to discredit his accusers
- Known to help companies with Corporate Espionage

The New Frontier



the Rapid Support Forces. The sleek white Cessna flew in from Cyprus and remained on the ground in Sudan's capital for just 45 minutes, long enough to draw a disturbing line of connection between the ferocious contest for power in Sudan and a spyware scandal roiling Greece.

Intellexa's private Cessna, used for delivering malware to clients.



2.5 **General Terms & Conditions**

- All hardware and software shall be delivered to customer within ninety (90) days of receipt of down payment.
- Delivery is subject to export and/or import control certification by the relevant European authorities, as applicable
- Installation and Configuration at customer designated facility (subject to any Covid-19 Restriction (as such term defined under the agreement) may take up to two (2) weeks.
- Intellexa shall submit to customer an invoice for each payment milestone.
- Standard Training course shall commence upon completion of installation at customer facility (subject to any Covid-19 Restriction (as such term defined under the
- All payments and charges shall be
- Delivery method: Incoterms CIF.
- all software shall become fully operational (official commissioning) upon receipt of all milestone payments.

A leaked document details Cost Insurance and Freight (CIF) delivery.

How To Buy Your Malware

1. Sign the contract
2. They fly to you in a private plane carrying your new surveillance technology
3. Visit them on the tarmac
4. Collect your equipment
5. Fly into the sunset

Operational Attack Flow

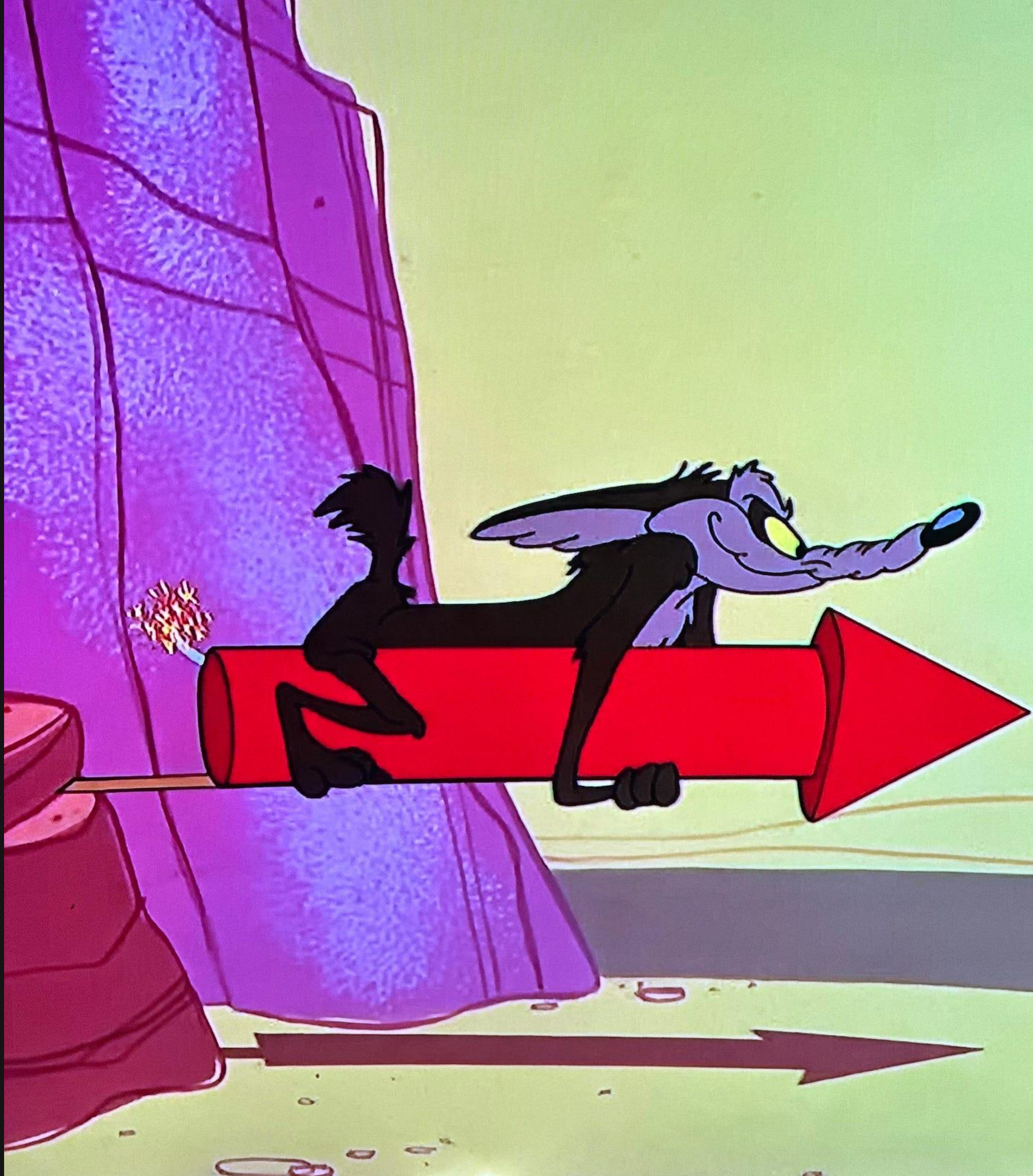
1. Target Identification

- Phone Number
- Physical Proximity
- Casting a big net/scattershot

myntex

2. Exploit Delivery

- Multiple attack techniques
- Leverage multiple CVEs
- Vulnerable iMessage, WhatsApp or FaceTime

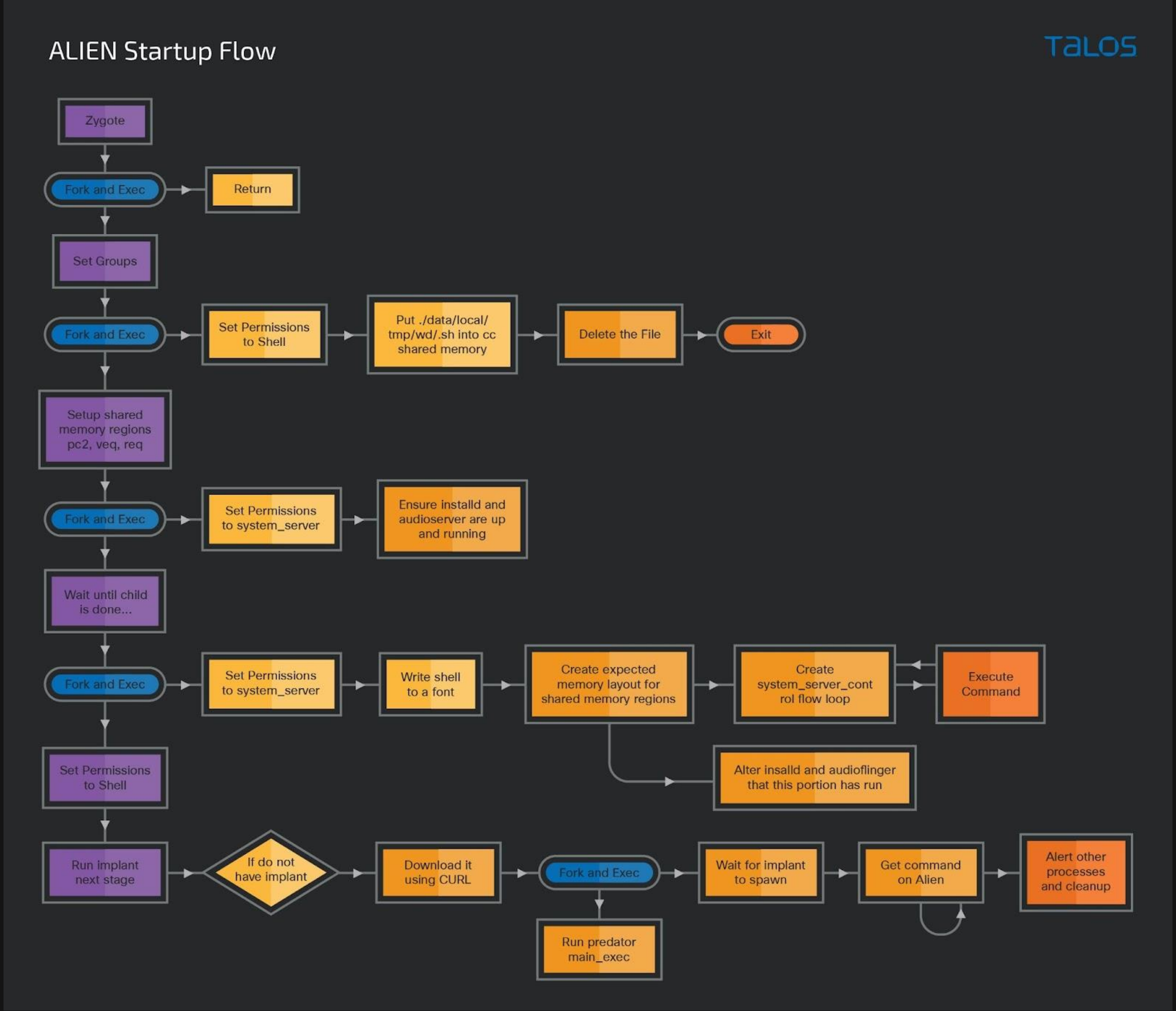


3. Initial Exploitation

- Existing infection
- System log monitoring
- Developer mode
- Process monitoring
- Rooted or Jailbroken
- Proxy
- Root Certificates

ALIEN ~~vs~~ PREDATOR

@Jimllpaintit

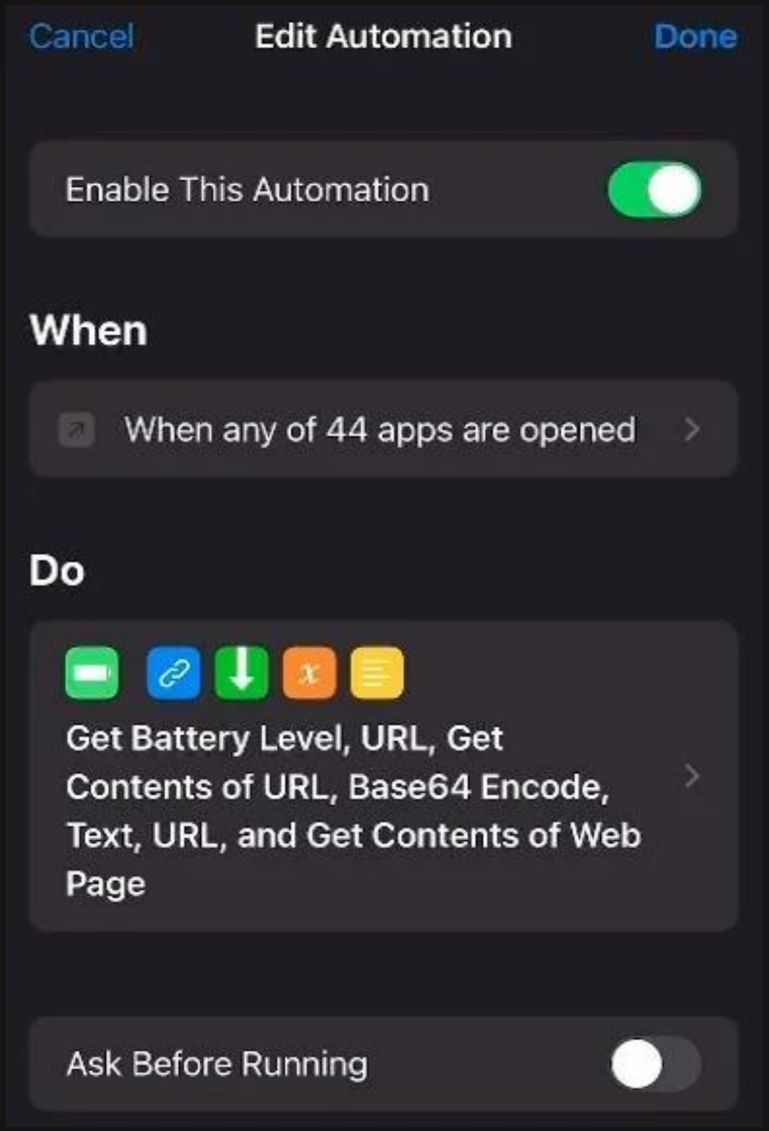

ALIEN Startup Flow
Talos
Zygote
Fork and Exec
Return
Set Groups
Fork and Exec
Set Permissions to Shell
Put ./data/local/ tmp/wd/.sh into cc shared memory
Delete the File
Exit
Setup shared memory regions pc2, veq, req
Fork and Exec
Set Permissions to system_server
Ensure installd and audioserver are up and running
Wait until child is done...
Fork and Exec
Set Permissions to system_server
Write shell to a font
Create expected memory layout for shared memory regions
Create system_server_cont rol flow loop
Execute Command
Alter insalld and audioflinger that this portion has run
Set Permissions to Shell
Run implant next stage
If do not have implant
Download it using CURL
Fork and Exec
Run predator main_exec
Wait for implant to spawn
Get command on Alien
Alert other processes and cleanup

A flowchart detailing the various checks and actions of ALIEN's startup flow.

myntex

4. Persistence

- Automatic re-infection for both Android and iOS
- Optional add-on feature
- Module based



Enable This Automation

When

When any of 44 apps are opened

Do

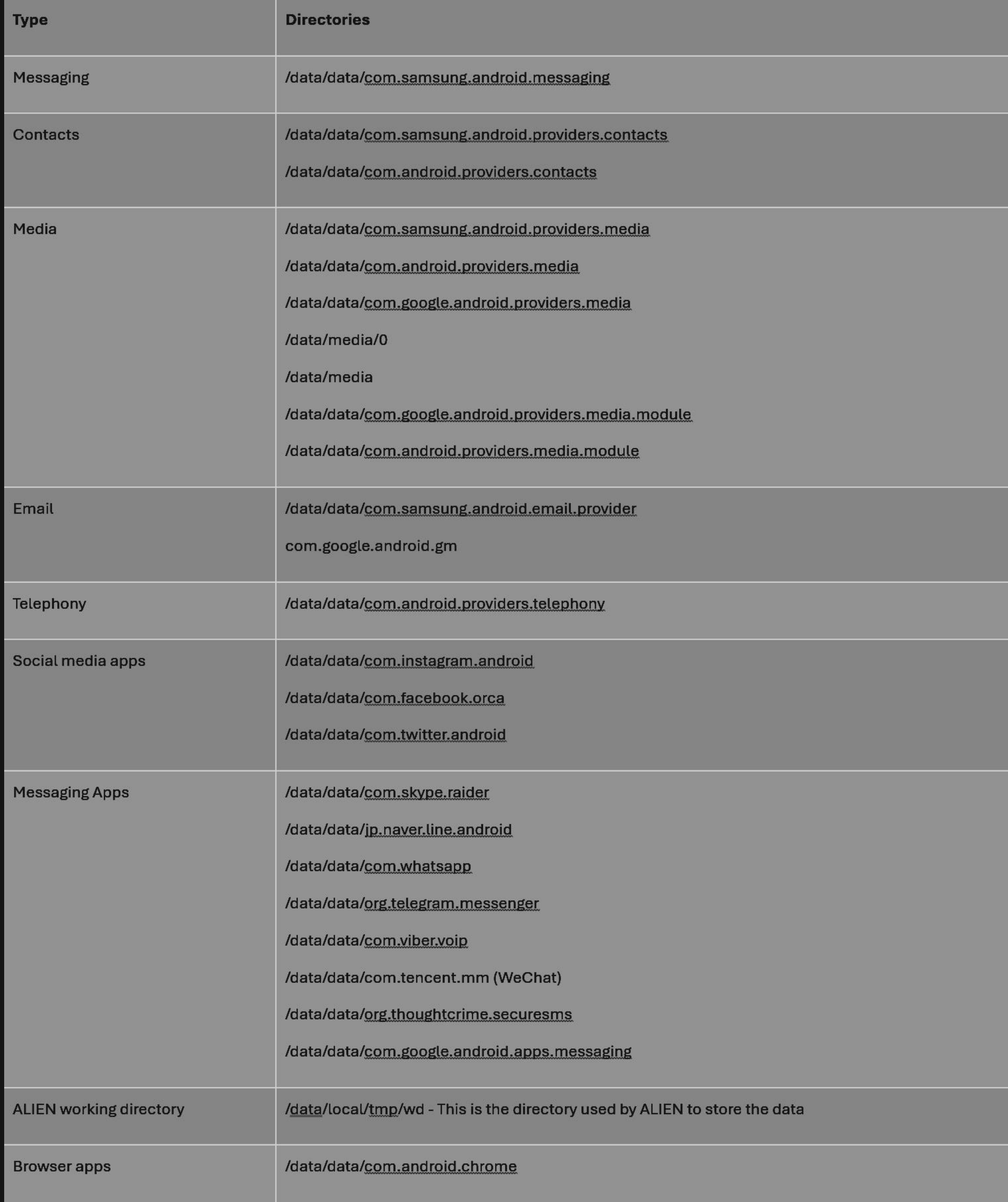
Get Battery Level, URL, Get Contents of URL, Base64 Encode, Text, URL, and Get Contents of Web Page

Ask Before Running

Sample of an automation script installed by Predator.

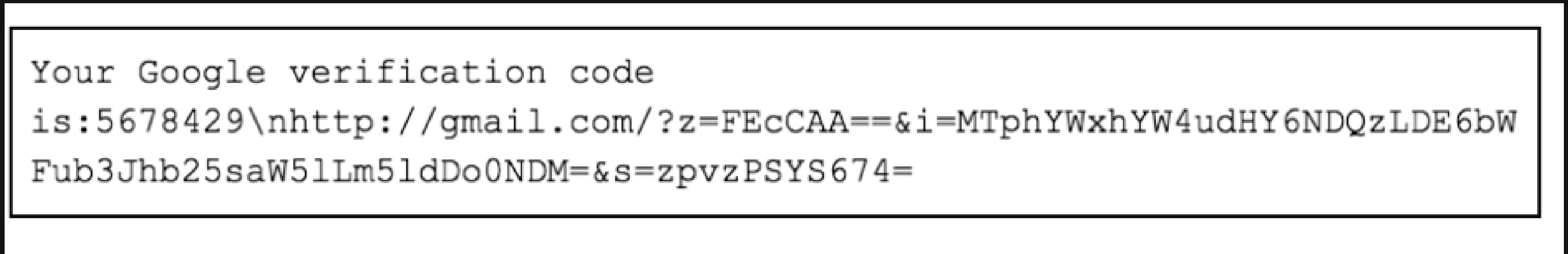
5. Data Collection & Exfiltration

- Ability to target specific packages based on the device manufacturer
- Stolen data uses a temporary directory to help with evidence cleanup after exfiltration



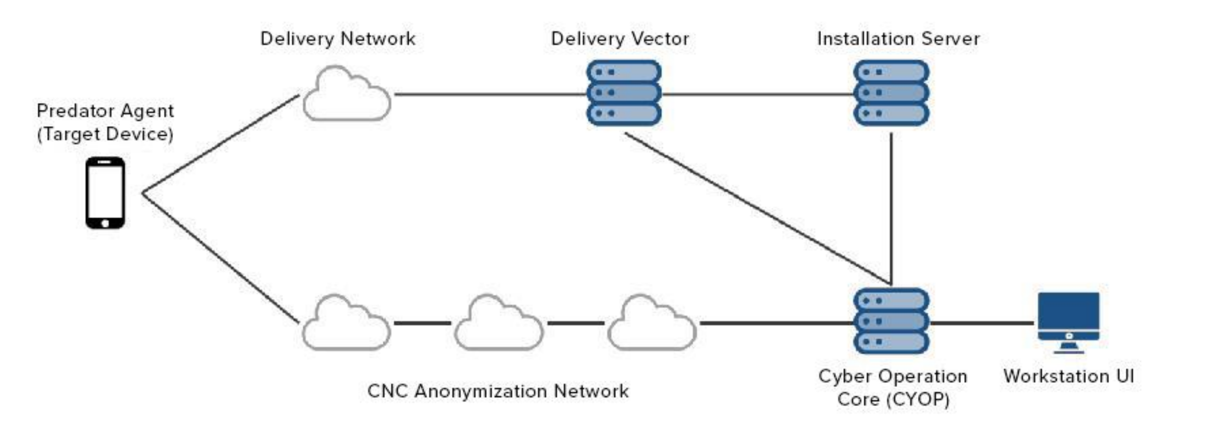
Type	Directories
Messaging	/data/data/com.samsung.android.messaging
Contacts	/data/data/com.samsung.android.providers.contacts /data/data/com.android.providers.contacts
Media	/data/data/com.samsung.android.providers.media /data/data/com.android.providers.media /data/data/com.google.android.providers.media /data/media/0 /data/media /data/data/com.google.android.providers.media.module /data/data/com.android.providers.media.module
Email	/data/data/com.samsung.android.email.provider com.google.android.gm
Telephony	/data/data/com.android.providers.telephony
Social media apps	/data/data/com.instagram.android /data/data/com.facebook.orca /data/data/com.twitter.android
Messaging Apps	/data/data/com.skype.raider /data/data/jp.naver.line.android /data/data/com.whatsapp /data/data/org.telegram.messenger /data/data/com.viber.voip /data/data/com.tencent.mm (WeChat) /data/data/org.thoughtcrime.securesms /data/data/com.google.android.apps.messaging
ALIEN working directory	/data/local/tmp/wd - This is the directory used by ALIEN to store the data
Browser apps	/data/data/com.android.chrome

List of directories that ALIEN targets for operation and data collection.



```
Your Google verification code
is:5678429\nhttp://gmail.com/?z=FEcCAA==&i=MTphYWxhYW4udHY6NDQzLDE6bW
Fub3Jhb25saW5lLm5ldDo0NDM=&s=zpvzPSYS674=
```

Sample of SMS that allows Pegasus to receive commands.



Predator high-level server architecture

6. Staying Undetected

- Scheduled Exfiltration
- Real Time Espionage

myntex

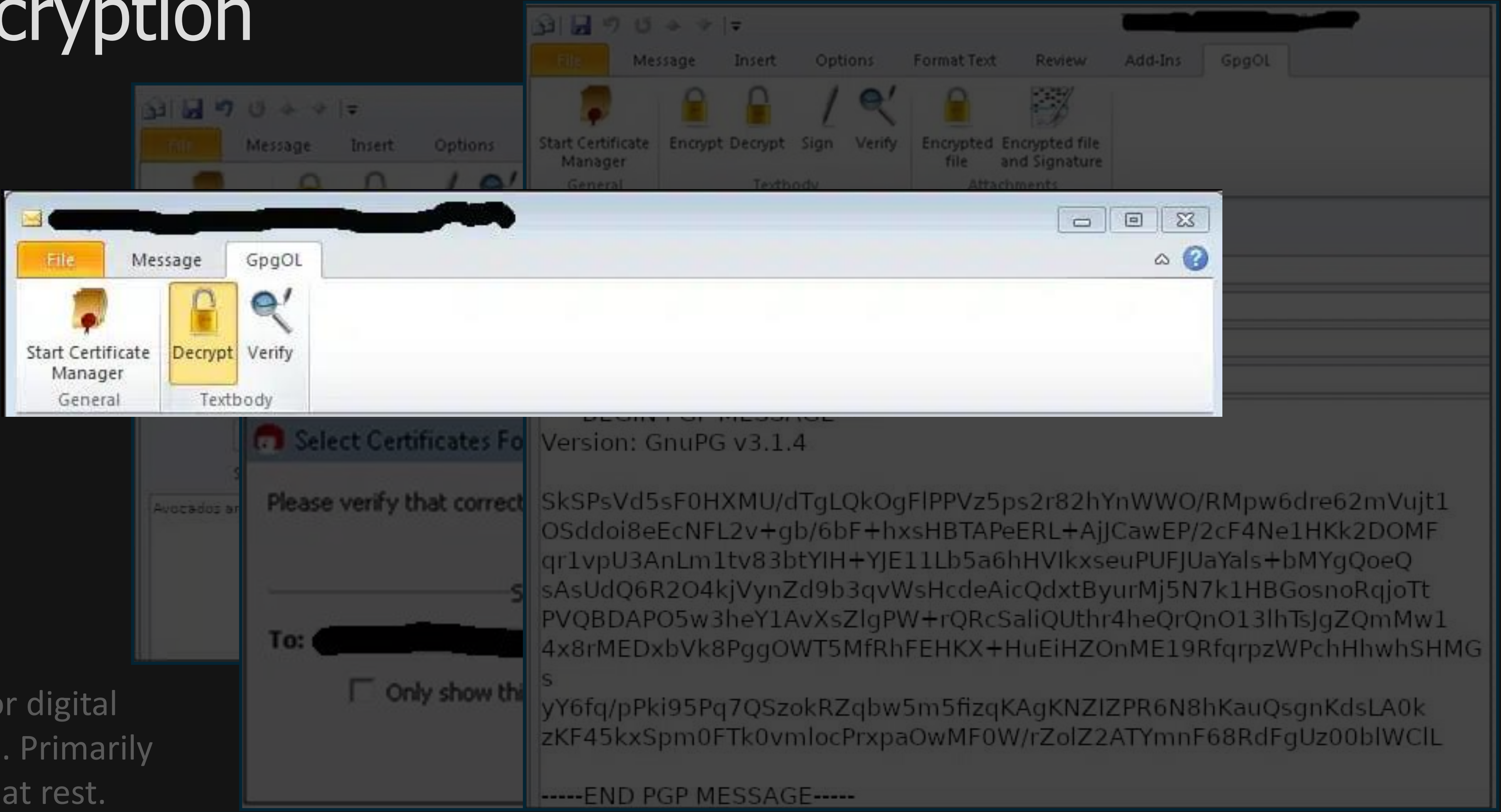
Classification: Protected A

7. Without a Trace

- Removes all evidence of infection
- Advanced self destruct mechanisms
- Remote capabilities to allow for further targeting

Encryption Works, Until it Doesn’t

PGP Encryption



[redacted]

[redacted]

Select Certificates Fo

Please verify that correct

To: [redacted]

□ Only show thi

Avocados ar

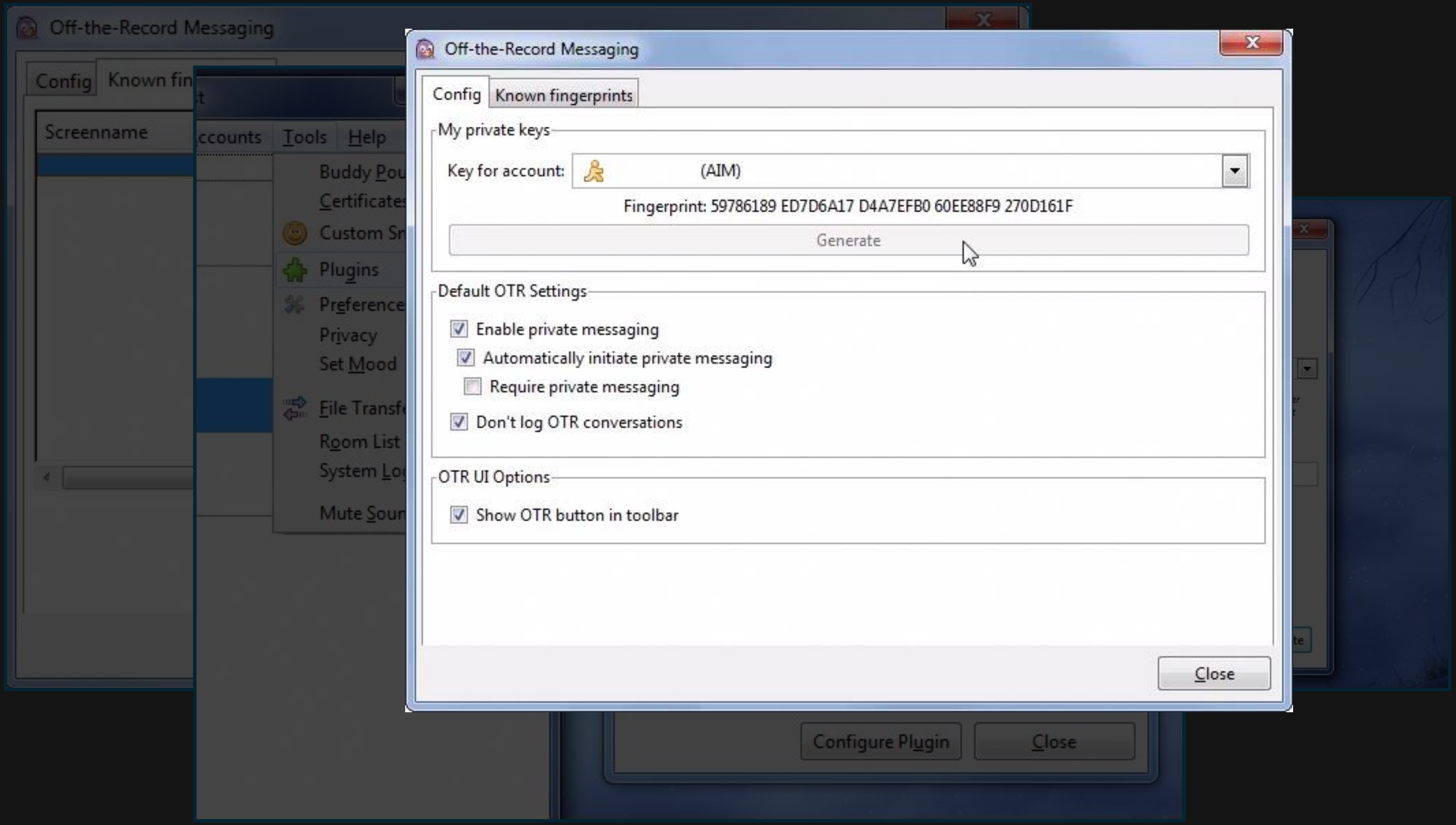
```
BEGIN PGP MESSAGE
Version: GnuPG v3.1.4

SkSPsVd5sF0HXMU/dTgLQkOgFlPPVz5ps2r82hYnWWO/RMpw6dre62mVujt1
OSddoi8eEcNFL2v+gb/6bF+hxsHBTAPeERL+AjJCawEP/2cF4Ne1HKk2DOMF
qr1vpU3AnLm1tv83btYlH+YJE11Lb5a6hHVIkxseuPUFJUaYals+bMYgQoeQ
sAsUdQ6R2O4kjVynZd9b3qvWsHcdeAicQdxtByurMj5N7k1HBGosnoRqjoTt
PVQBDAPO5w3heY1AvXsZlgPW+rQRcSaliQUthr4heQrQnO13lhTsJgZQmMw1
4x8rMEDxbVk8PggOWT5MfRhFEHKX+HuEiHZOnME19RfqrpzWPchHhwhSHMG
s
yY6fq/pPki95Pq7QSzokRZqbw5m5fizqKAgKNZIZPR6N8hKauQsgnKdsLA0k
zKF45kxSpm0FTk0vmlocPrxpaOwMF0W/rZolZ2ATYmnF68RdFgUz00blWClL

-----END PGP MESSAGE-----
```

Set the standard for digital encryption in 1991. Primarily for email and data at rest. Complex setup and use.

Pidgin Messenger, OTR



Off-the-Record Messaging

Config | Known fingerprints

My private keys

Key for account: (AIM)

Fingerprint: 59786189 ED7D6A17 D4A7EFB0 60EE88F9 270D161F

Generate

Default OTR Settings

☑ Enable private messaging

☑ Automatically initiate private messaging

□ Require private messaging

☑ Don't log OTR conversations

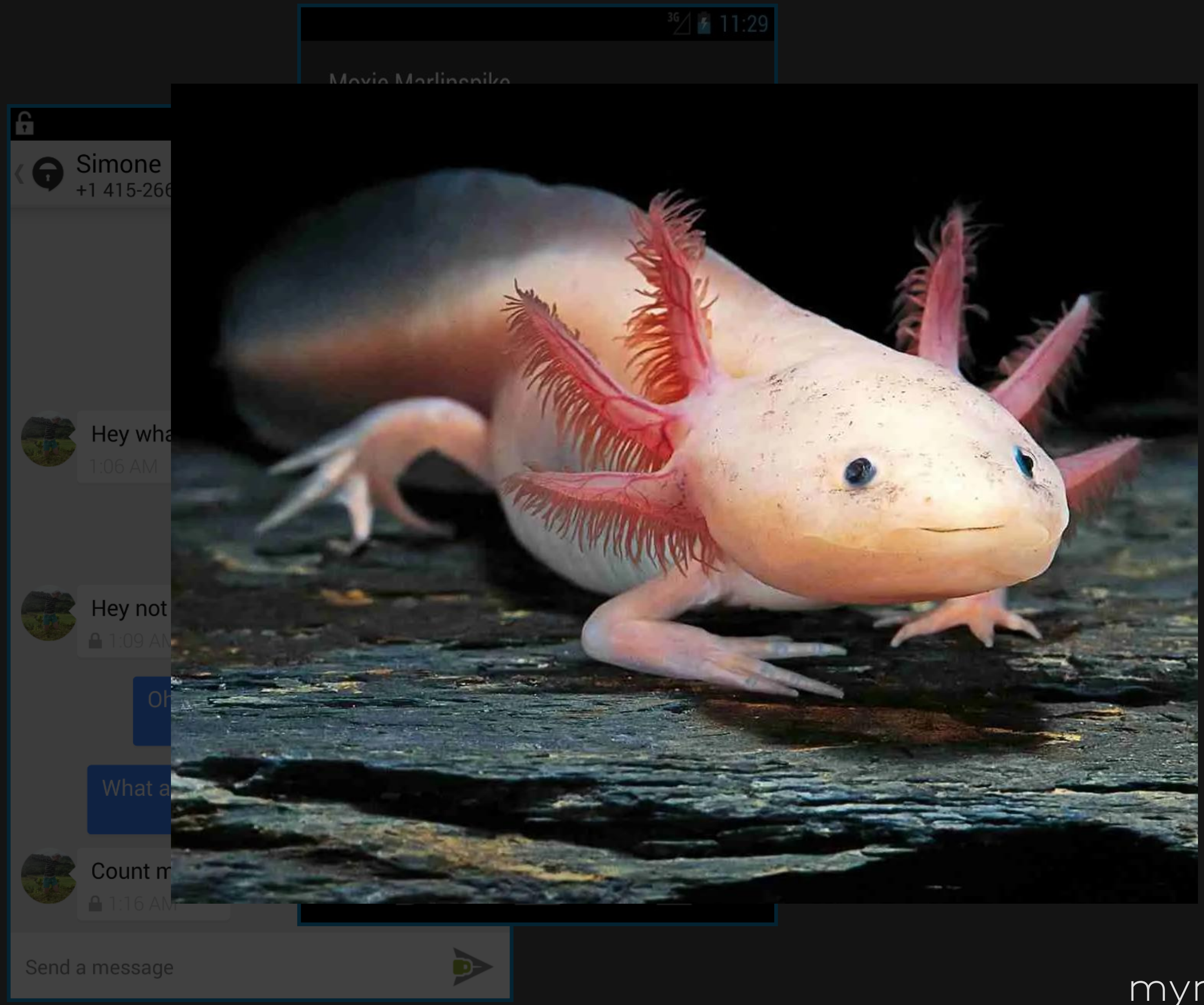
OTR UI Options

☑ Show OTR button in toolbar

Close

Improvement over OpenPGP. Allows real-time chat. Lead to MITM attack protection. Inspired Signal Protocol.

TextSecure, Axolotl Ratchet, Signal Protocol



11:29

Moxie Marlinspike

Simone
+1 415-266

Hey wha
1:06 AM

Hey not
1:09 AM

Oh

What a

Count m
1:16 AM

Send a message

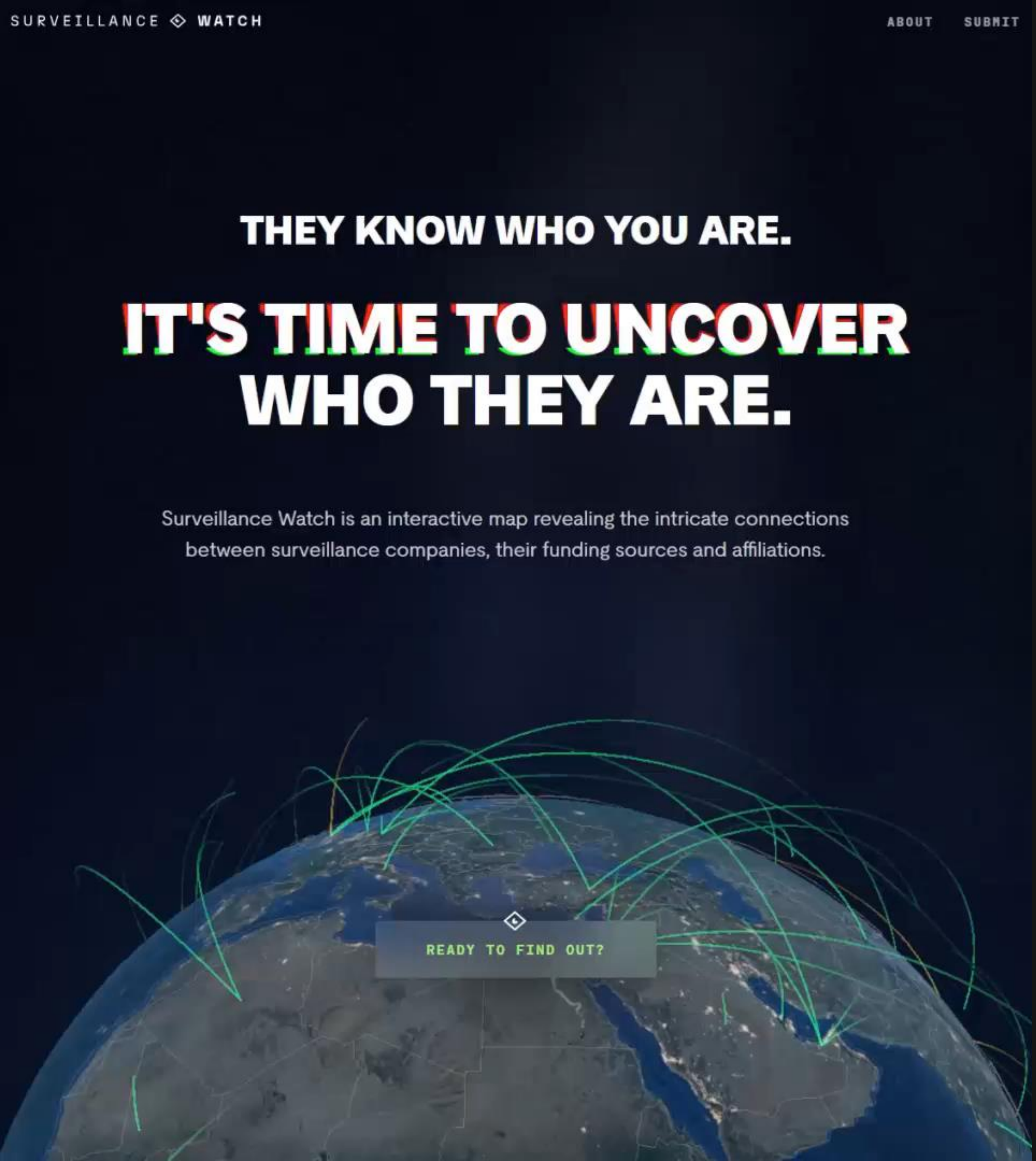
Backbone of modern secure messaging since 2010. Allows for refreshing of public keys, encrypted group chat, instant messaging.

Unencrypted Data at Rest

- Affects majority of apps that rely on OS for protection
- Makes user a sitting duck in face of weaponized malware
- Some developers use storage encryption, but not necessarily well…

Protecting Yourself

myntex



THEY KNOW WHO YOU ARE.

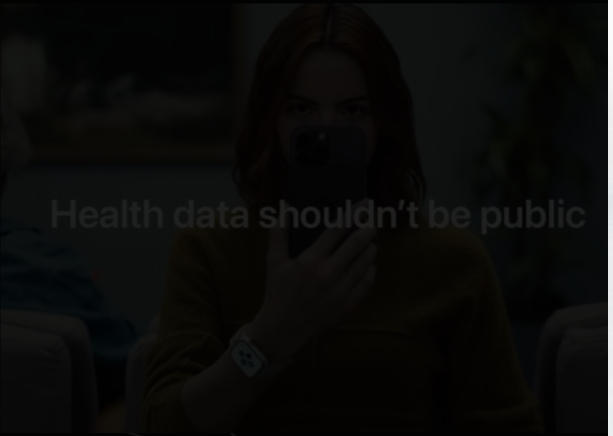
IT'S TIME TO UNCOVER WHO THEY ARE.

Surveillance Watch is an interactive map revealing the intricate connections between surveillance companies, their funding sources and affiliations.

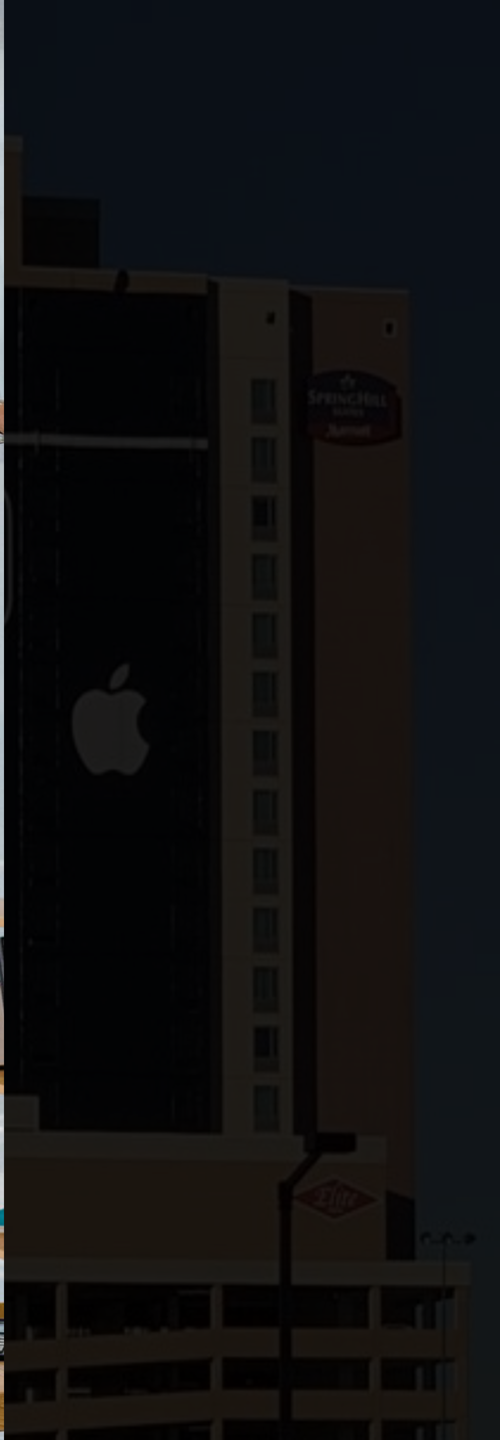
Turning The Tables

https://www.surveillancewatch.io/

Privacy Washi
goes to…



Health data shouldn't be public



Classification: Protected A

What about alternative mobile operating systems?

CALYXOS

GrapheneOS

iodé

PARANOID ANDROID

LINEAGE

Weaponized Malware Protection

- Don’t put sensitive information on a digital device.
- If you must, use a dedicated secure device ONLY for that purpose.
- Factory reset it regularly.

Thank you.

in Geoff Green

myntex