



Under the SEA:

A Look at the Syrian Electronic Army's Mobile Tooling

BlackHat Europe 2018
London, England

Who are we?



Michael Flossman
Head of Threat Intelligence
[@Lookout](#)



Kristin Del Rosso
Security Intelligence Analyst
[@Lookout](#)

Discover, track, disrupt, and understand
the context around targeted
Surveillanceware

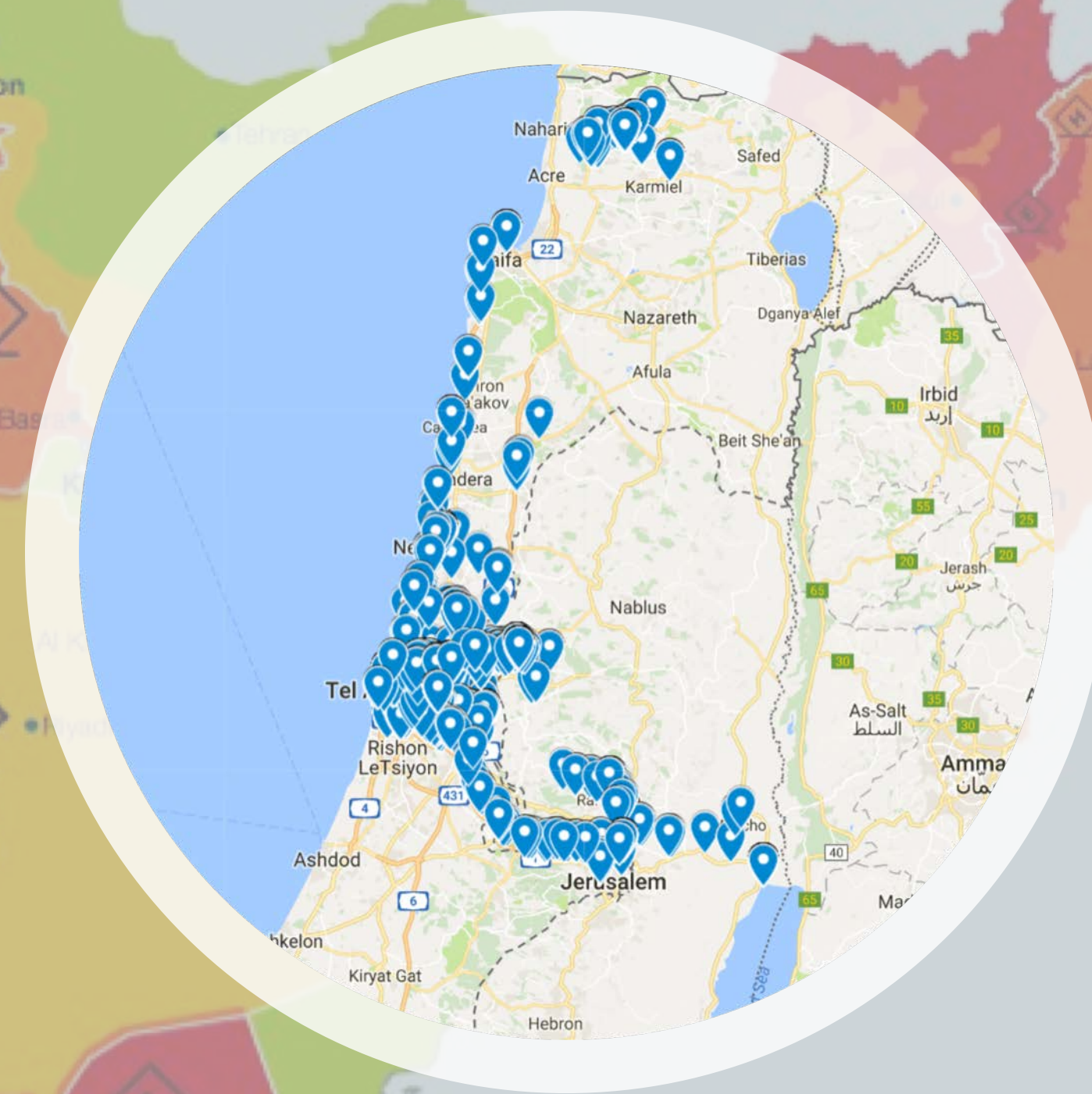
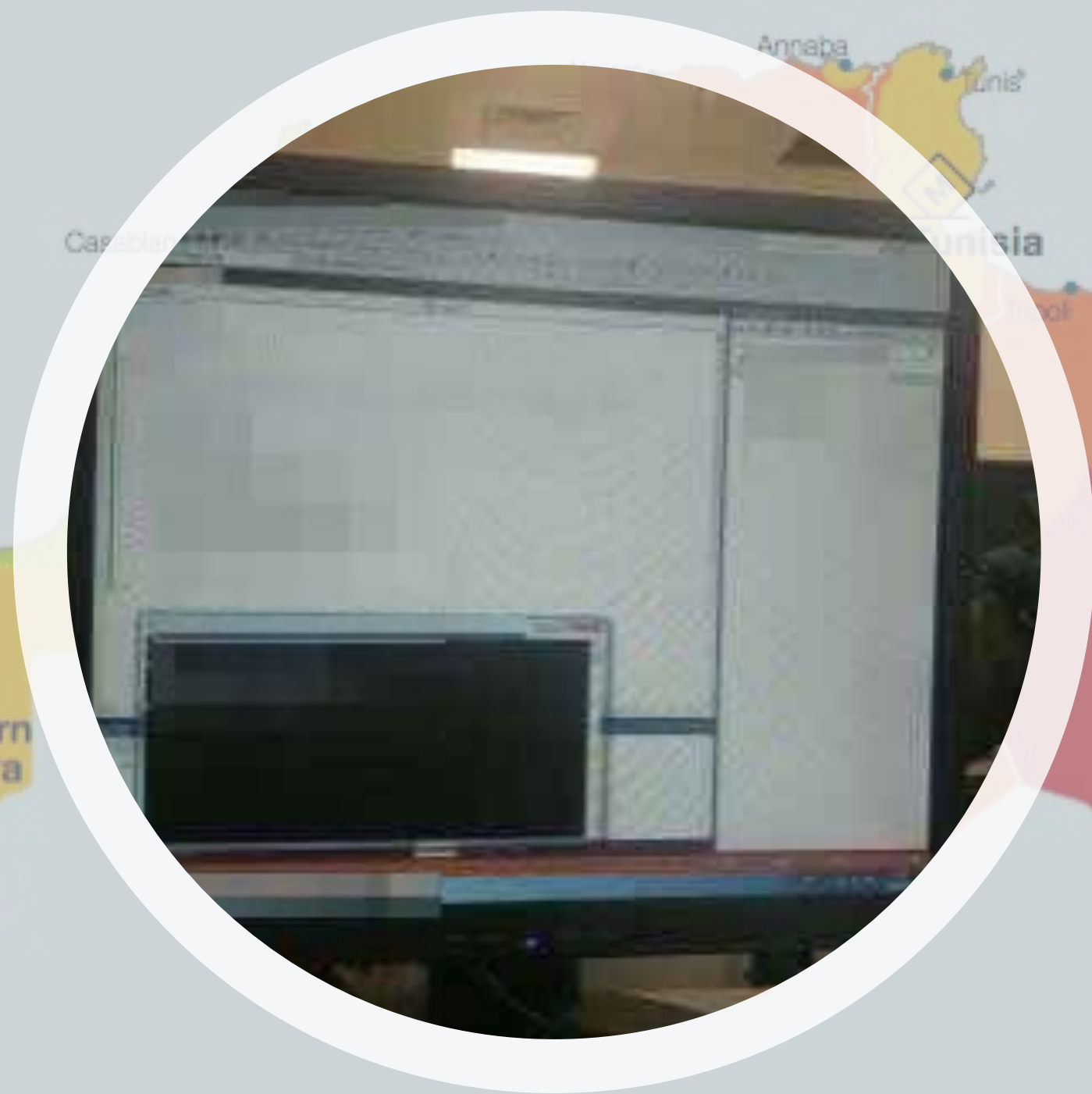
Pegasus, ViperRAT, DarkCaracal,
StealthMango, and many many more

Agenda

- Who is the SEA?
- SilverHawk
- Attack Vectors
- Personas & Attribution



Upgrading Traditional Warfare



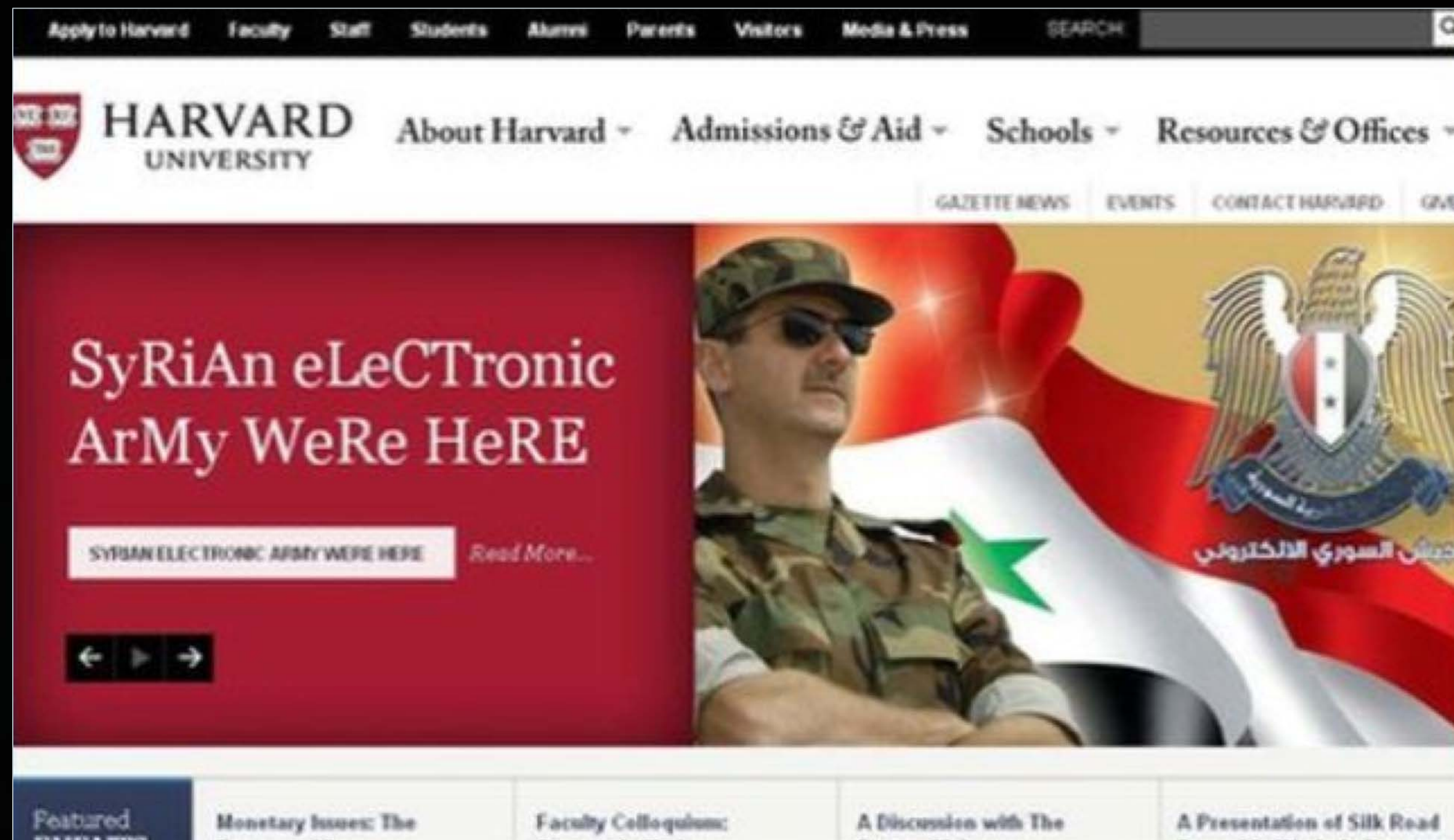
Upgrading Traditional Warfare



Enemies of the Internet 2014

Copyright © Control Risks 2017. All rights reserved. Reproduction in whole or in part prohibited without the prior consent of the Company.
The Risk Ratings are compiled from sources that Control Risks considers to be reliable or are expressions of opinion. Control Risks has made reasonable commercial efforts to ensure the accuracy of the information on which the Risk Ratings are based, however, the Risk Ratings are provided "as is" and include reasonable judgments in the circumstances prevailing at the time. The Risk Ratings provided should not be construed as definitive or binding advice. Boundaries and names shown on this map do not imply endorsement or acceptance by Control Risks.





Hacked

The Pro

we are sorry to destroy your sites , but your government's policies and the interfere in our Interior affairs forced us to hack your official sites so you will be able to listen to our voices live from Syria , we love our country and we love our President Bashar al Assad and we will not allow anyone to interfere in our Internal Affairs

PRO@Hotmail.NL



Don't use Microsoft emails(hotmail,outlook),They are monitoring your accounts and selling the data to the governments.More details soon #SEA

Reply Retweeted Favorite More

8,209 RETWEETS

2,026 FAVORITES



12:34 AM - 2 Jan 14



Syrian Electronic Army Was Here via @Official_SEA16 #SEA pic.twitter.com/MDxQXK6CLJ

Reply Retweet Favorite Pocket More



14 RETWEETS

1 FAVORITE



2:31 PM - 11 Jan 14

Flag media



BBC Weather @bbcweather

34m

Earthquake warning for Qatar: Hamad Bin Khalifah about to exit vehicle

Expand



BBC Weather @bbcweather

41m

Saudi weather station down due to head on-collision with camel

Expand



BBC Weather @bbcweather

55m

Chaotic weather forecast for Lebanon as the government decides to distance itself from the Milky Way

Expand



BBC Weather @bbcweather

1h

Tsunami alert for Haifa: Residents are advised to return to Poland.

Expand



BBC Weather @bbcweather

1h

Forecast for Tel Aviv on Saturday - 5000 degrees Kelvin with northern fog and eastern high pressure front

Expand



BBC Weather @bbcweather

1h

Long Live #Syria Al-Assad #SEA

Expand



CNN @CNN



Syrian Electronic Army Was Here... Stop lying... All your reports are fake! via @Official_SEA16 #SEA

Reply Retweet Favorite More

92

RETWEETS

25

FAVORITES



© Twitter

Tweets All / No replies



FC Barcelona @FCBarcelona · 2m

Special Hi to @RealMadrid! via @Official_SEA16 #SEA

Expand

Reply Retweet Favorite More



Retweeted by FC Barcelona

FC Barcelona @FCBarcelona_cat · 7m

Dear FC Barcelona management, Don't let the Qatari money funds you, it's full of blood and kill via @Official_SEA16 #SEA #FCB

Expand

Reply Retweet Favorite More



Retweeted by FC Barcelona

FC Barcelona @FCBarcelona_es · 7m

Dear FC Barcelona management, Don't let the Qatari money funds you, it's full of blood and kill via @Official_SEA16 #SEA #FCB

Expand

Reply Retweet Favorite More



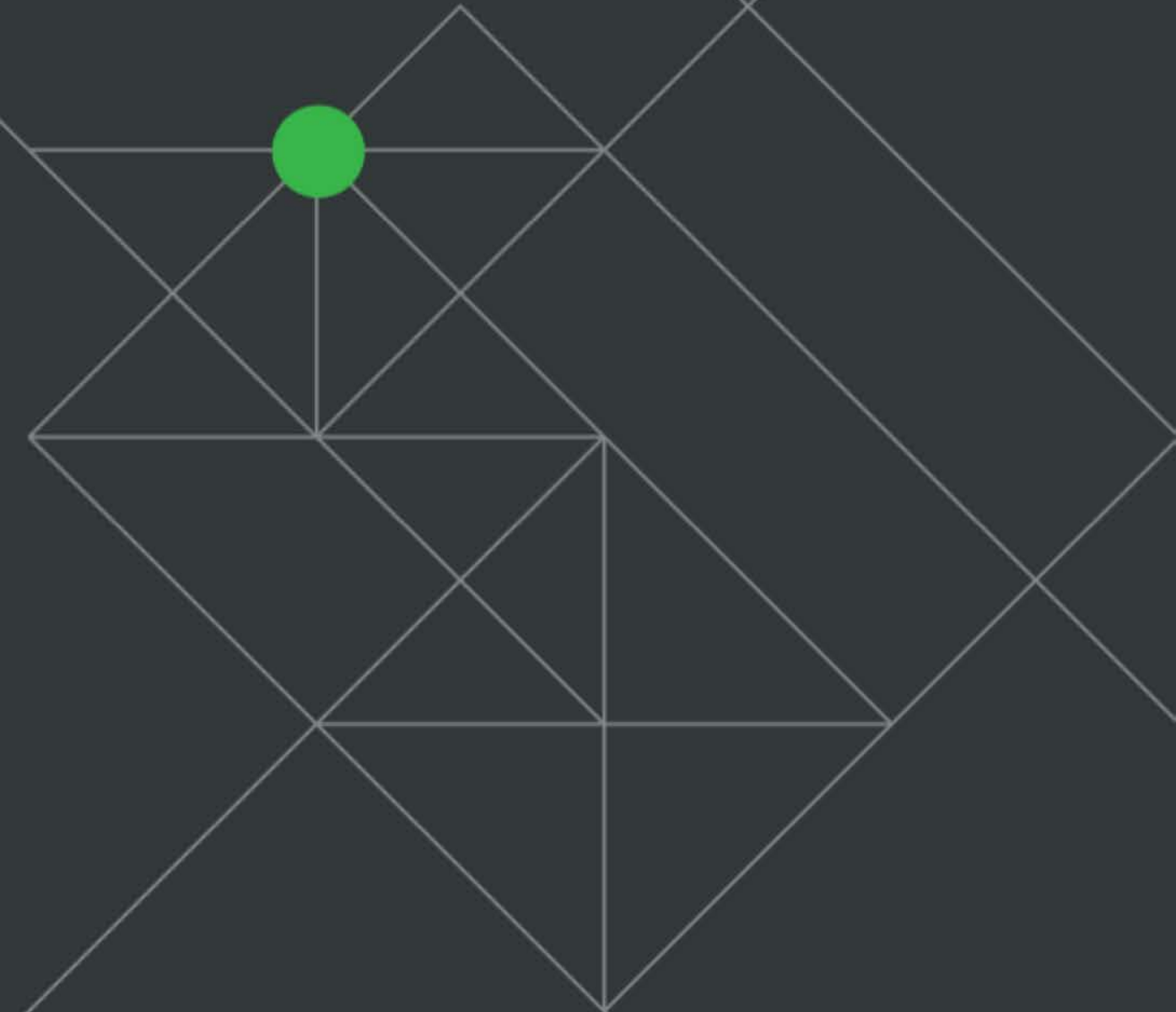
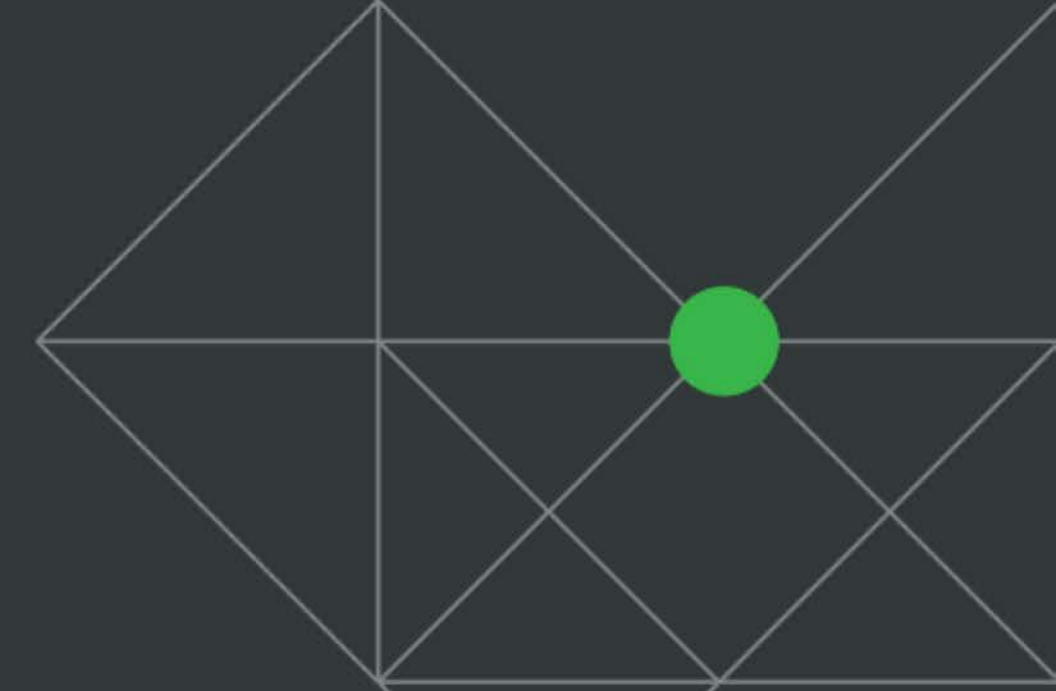
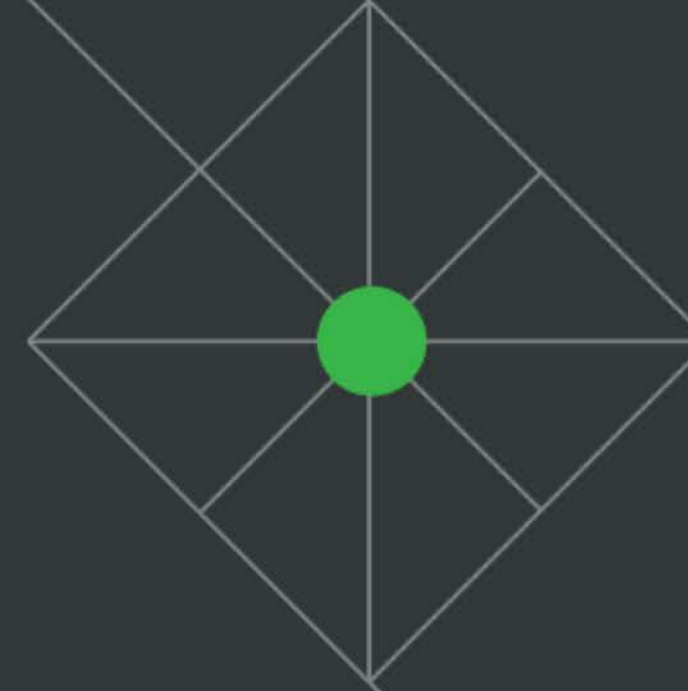
FC Barcelona @FCBarcelona · 7m

Dear FC Barcelona management, Don't let the Qatari money funds you, it's full of blood and kill via @Official_SEA16 #SEA #FCB

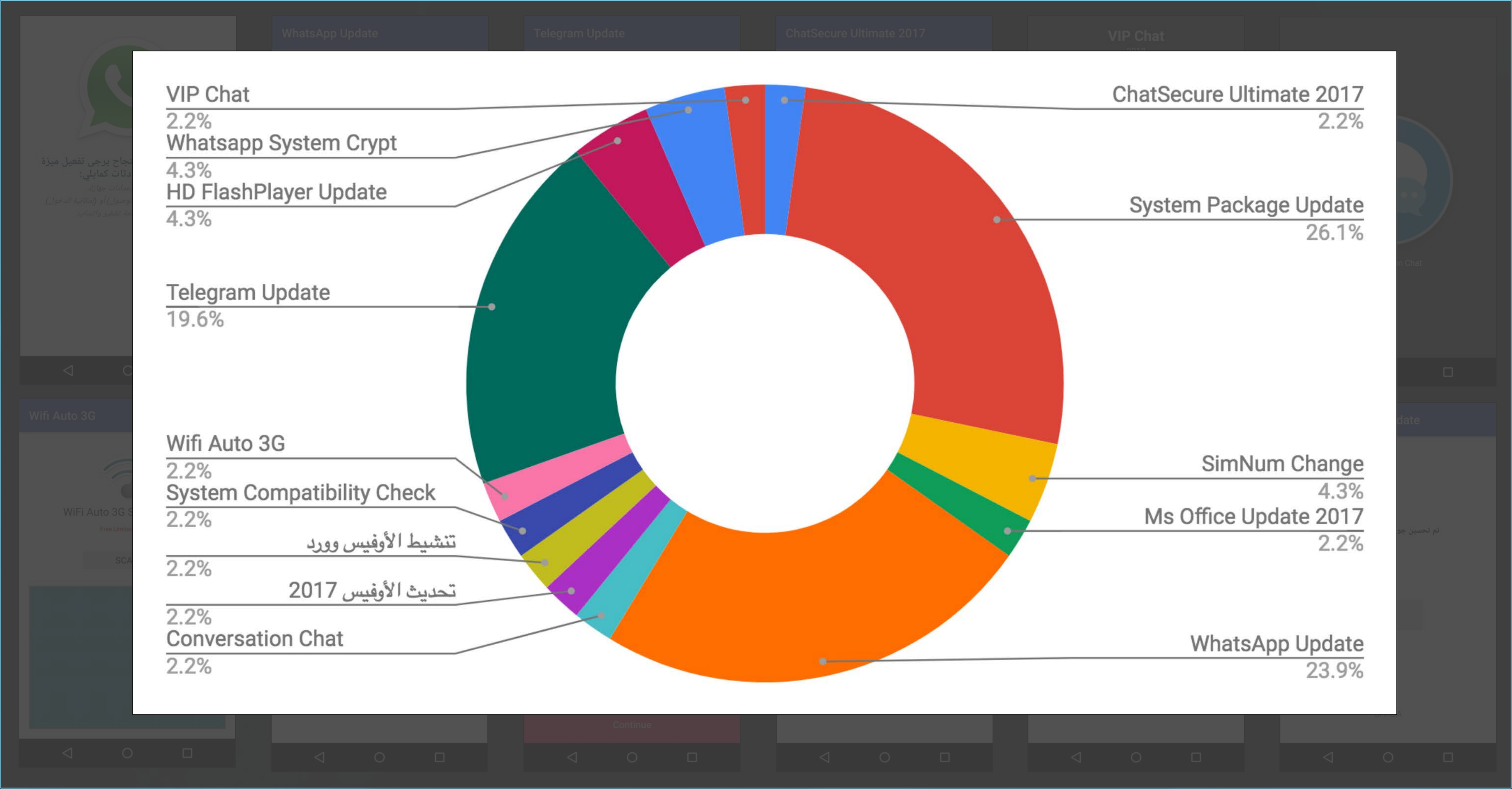
Expand

Reply Retweet Favorite More

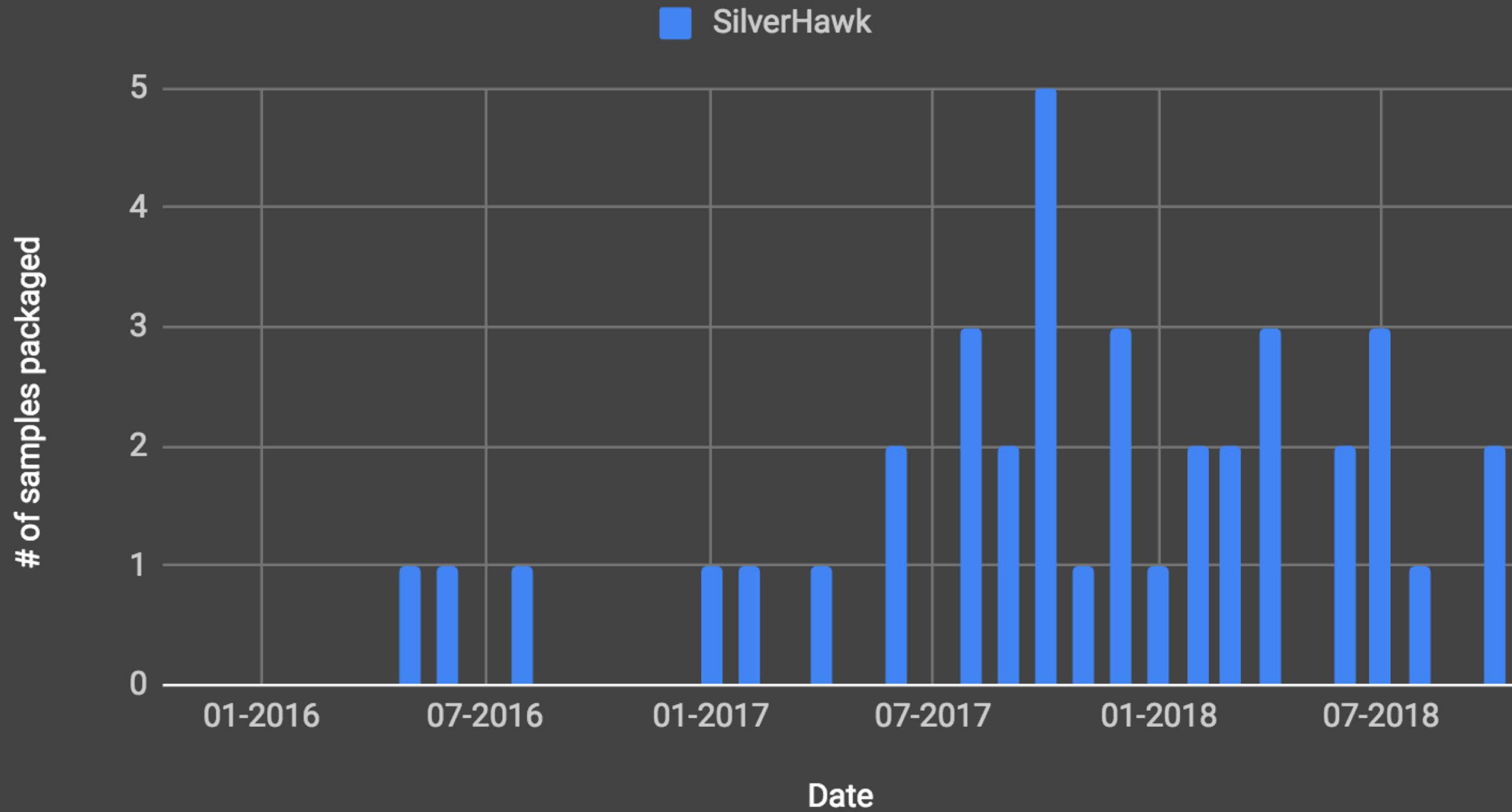
SilverHawk



SilverHawk



Dates Mobile Tooling Packaged



SilverHawk

Where on the phone did the malware touch you?

App Capabilities

- Record Audio
 - Stream environment audio over raw socket when instructed
- Take photos with device camera
- Survival counter - failed server connections and it stops
- Retrieve files from external storage
 - Top directory
 - Downloads , Pictures, DCIM directories
 - WhatsApp, Telegram, Viber, ShareIt content
 - Files sent over Bluetooth*
- File utility to copy, move, rename, and delete files
- Download attacker specified files
- Enumerate installed apps incl. date & time installed
- Attempt to execute attacker specified commands or binary as root
- Retrieve contacts and related data:
 - Call logs
 - Contacts
 - Text Messages
- Location, direction, and acceleration of the device
- Remotely updateable C2 IP and port
- Hide Icon
- Device information
 - Retrieve battery levels, WiFi and GPS status, storage and cellular carrier info

SilverHawk

Custom Communication Protocol

```
<HmzaPacket>
```

```
<Command></Command>
```

```
<XMLData></XMLData>
```

```
<MSG></MSG>
```

```
<Success></Success>
```

```
</HmzaPacket></HAMZA_DELIMITER_STOP>
```

```
<HmzaPacket>
  <XMLData>&lt;SysInfo&gt;
    &lt;APK&gt;Telgram_21_2_2017_SoundBuffer&lt;/APK&gt;
    &lt;Android&gt;4.3&lt;/Android&gt;
    &lt;WIFI&gt;3G&lt;/WIFI&gt;
    &lt;DBName&gt;&lt;/DBName&gt;
    &lt;DateOn&gt;Installed @ : GMT&lt;/DateOn&gt;
    &lt;DeviceName&gt;Unknown AOSP on ARM Emulator&lt;/DeviceName&gt;
    &lt;IMEI&gt;&lt;/IMEI&gt;
    &lt;Loc&gt;us&lt;/Loc&gt;
    &lt;Oper&gt;&lt;/Oper&gt;
    &lt;SimSer&gt;&lt;/SimSer&gt;
    &lt;Root&gt;Rooted &lt;/Root&gt;
    &lt;Sim&gt;T-Mobile&lt;/Sim&gt;
    &lt;Rate&gt;0&lt;/Rate&gt;
    &lt;Chanel&gt;0&lt;/Chanel&gt;
  &lt;/SysInfo&gt;</XMLData>
  <MSG></MSG>
  <Success>true</Success>
  <Command>17</Command>
</HmzaPacket></HAMZA_DELIMITER_STOP><HmzaPacket>
  <XMLData></XMLData>
  <MSG>com.systemappsy.update.telegram</MSG>
  <Success>true</Success>
  <Command>30</Command>
</HmzaPacket></HAMZA_DELIMITER_STOP><HmzaPacket>
  <XMLData></XMLData>
  <MSG>com.systemappsy.update.telegram</MSG>
  <Success>true</Success>
  <Command>30</Command>
</HmzaPacket></HAMZA_DELIMITER_STOP><HmzaPacket>
  <XMLData></XMLData>
  <MSG>com.systemappsy.update.telegram</MSG>
  <Success>true</Success>
  <Command>30</Command>
</HmzaPacket></HAMZA_DELIMITER_STOP>
```



```
0000002E if-eqz v0, :38
00000032 invoke-interface ConnectionSource->clearSpecialConnection(DatabaseConnection)V, v3, v1
00000038 return-void
0000003A move-exception v0
0000003C new-instance v1, IllegalStateException
00000040 const-string v2, "Could not save special connection"
00000044 invoke-direct IllegalArgumentException-><init>(String, Throwable)V, v1, v2, v0
0000004A throw v1
```

SilverHawk

Capabilities and Evolution

COMMAND	TYPE	DESCRIPTION
16	None	Sends an empty packet to the server and calls TryConnect() which updates all information on the server
17	XML	Send all basic device information to the server including SIM Card details, Network operator, IMEI, phone and device details, Android Build Version, date installed, connectivity, Admin and root privileges, Wifi details.
18	XML	<p>If the <code>Success</code> value received from the server with this command is false or doesn't exist: Gets a list of mount points and then uploads a <code>HmzaFile</code> object which contains the following folders as its child, only if they exist on the system:</p> <ul style="list-style-type: none">• Phone• SD Card• Downloads• Pictures• DCIM <p>It also attempts to add the following folders on external storage, only if they exist:</p> <ul style="list-style-type: none">• Whatsapp• GBWhatsapp• Telegram• Viber• Bluetooth• ShareIt <p>If the value of <code>Success</code> is true: the <code>XMLData</code> from the server contains the name of a specific file/directory whose details need to be uploaded to the command and control infrastructure. If the specified name is a directory, the file list of the directory is recursively built and sent as a <code>HmzaFile</code> object.</p>
19	Both	Tells the client to upload a specified file to the remote server
20	None	Tells the client to receive a specified file from the remote server and store it at a specified location on the infected device.
21	XML	Delete a specified file from the device

COMMAND	TYPE	DESCRIPTION
22	Both	Copy a specified file to another specified location on the device
23	Both	Move a specified file to another specified location on the device
24	Both	Rename a specified file to a specified name on the device
25	XML	Run a given file on the device
28	XML	Make a new specified directory on the device
29	XML	Root shell command executed and communicated back to server only if su binary exists on device.
30	MSG	Sends back the currently running application on the device
31	XML	Sends the list of all Contacts to the remote server
32	XML	Sends the contents of all SMSs to the remote server
33	XML	Sends the call logs to the server
34	None	Start recording audio and stream it back to the remote server
35	None	Stop recording audio and send an empty packet for confirmation
36	XML	Take a picture and send the data as Base64-encoded XML Data
37	XML	Sends location, direction and acceleration of the device to the server
39	MSG	Receive and update server IP and Port
40	Both	Send the IP and Port that is stored in the Settings to the remote server
41	XML	Sends a list of Installed apps to the server with icons
101	XML	Error reporting for commands 18-20

SilverHawk

The AndroRAT Connection

SilverHawk

ChatSecure Ultimate 2017

ChatSecure Ultimate 2017



This Product Need Activation !

ACTIVATE BUY FOR 999\$

you can still get the simple edition on

```
public MainActivity() {
    super();
    this.activated = Boolean.valueOf(false);
    this.general = "QAZWSXEDC17";
    this.imei = "";

    public void onClick(View arg6) {
        int v4 = 4;
        int v3 = 8;
        if(MainActivity.this.eKey.getText().equals("")) {
            MainActivity.this.Myprogress.setVisibility(View.VISIBLE);
            MainActivity.this.status.setText("Activating...");
            MainActivity.this.eKey.setEnabled(false);
            MainActivity.this.errorText.setVisibility(View.VISIBLE);
            MainActivity.this.ext3.setVisibility(View.VISIBLE);
            MainActivity.this.ext5.setVisibility(View.VISIBLE);
            new Handler().postDelayed(new Runnable() {
                @Override public void run() {
                    MainActivity.this.eKey.setEnabled(true);
                    MainActivity.this.errorText.setVisibility(View.GONE);
                    MainActivity.this.ext3.setVisibility(View.GONE);
                    MainActivity.this.ext5.setVisibility(View.GONE);
                    MainActivity.this.Myprogress.setVisibility(View.GONE);
                    MainActivity.this.status.setText("");
                }
            }, 5000);
        }
    }
}
```



This Product Need Activation!

AndroRAT

ACTIVATE

BUY FOR 999\$

you can still get the simple edition on

ChatSecure Ultimate 2017



QAZWSXEDC17

ACTIVATE BUY FOR 999\$



Encrypting your net traffic in progress..

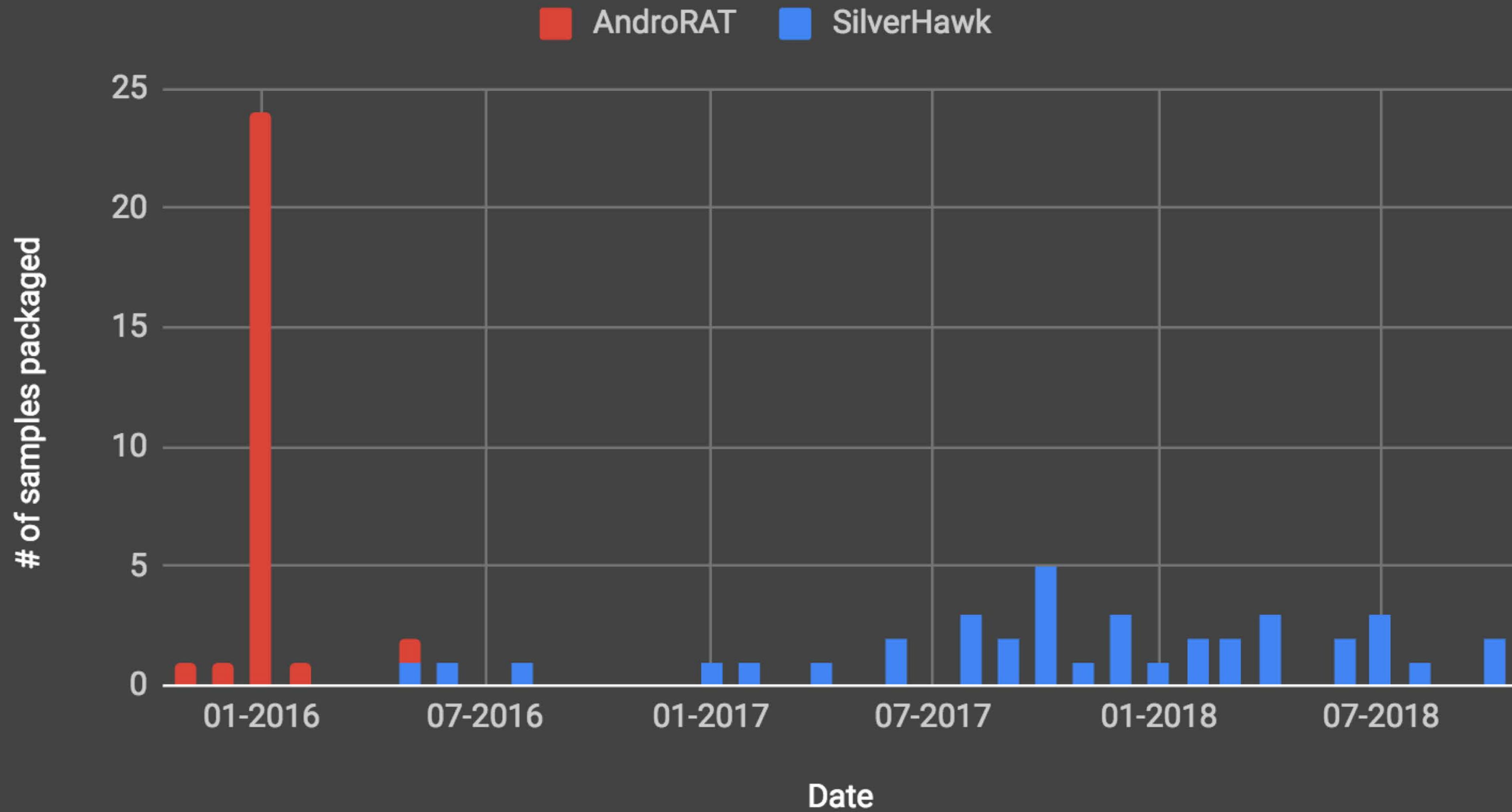
ChatSecure Ultimate 2017



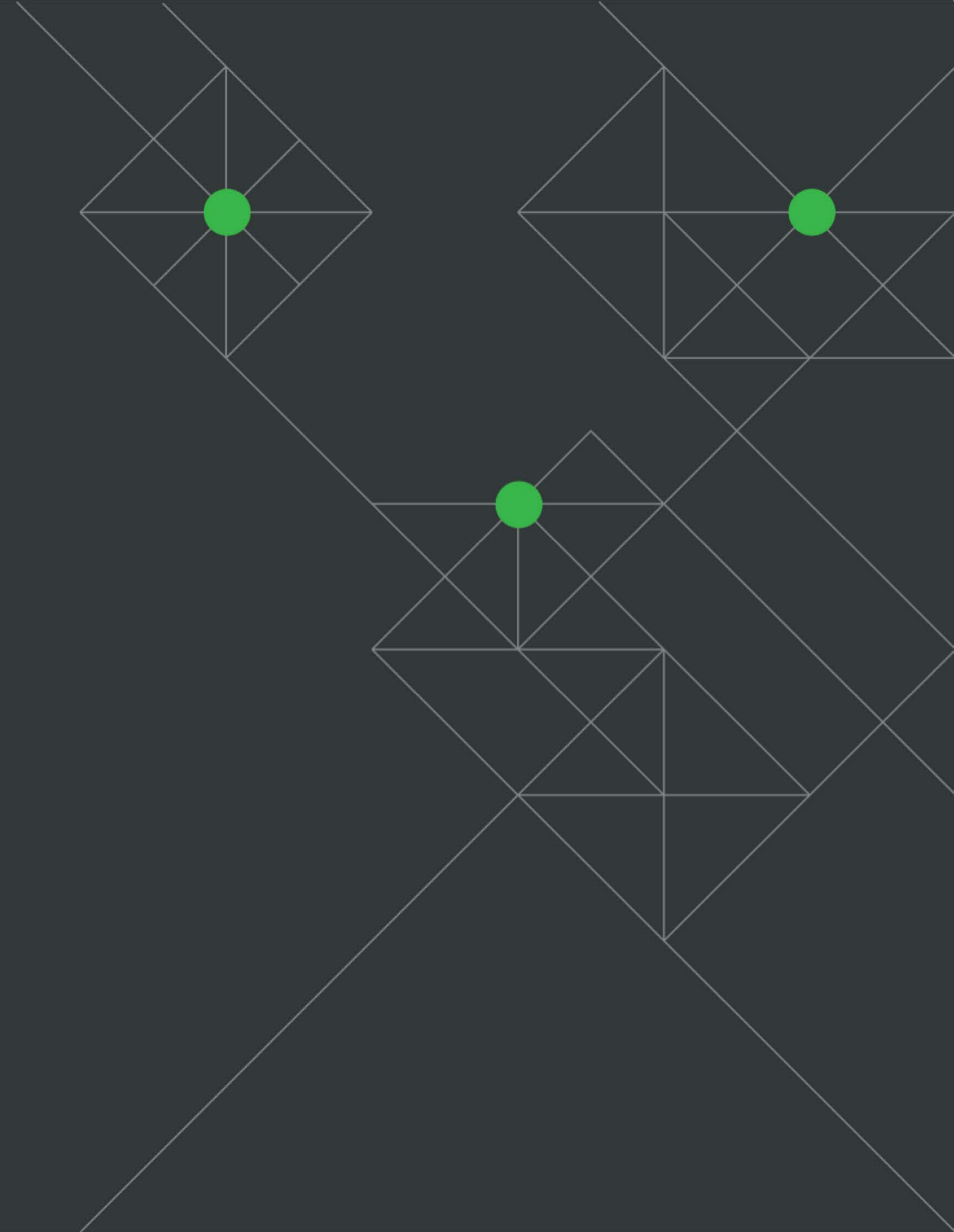
Activation Completed Successfully

All your net connections now secured :)

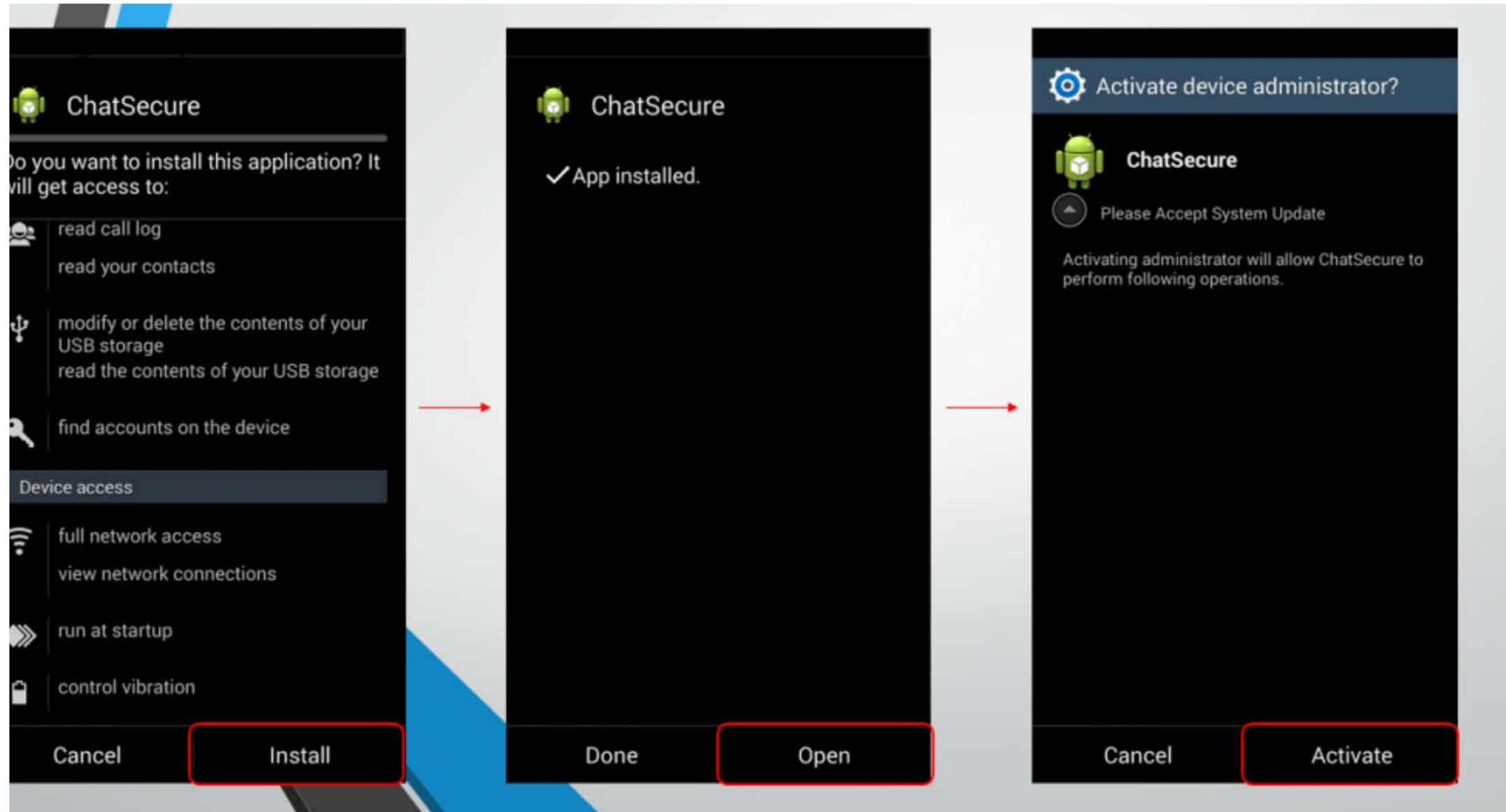
Dates Mobile Tooling Packaged



Attack Vectors







Index of

[ICO]	Name	Last modified	Size	Description
[PARENTDIR]	Parent Directory		-	
[]	>.تسريع نت مج	2017-09-25 22:52	1.4M	
[DIR]	04/	2017-04-09 20:25	-	
[DIR]	05/	2017-05-31 09:16	-	
[DIR]	06/	2017-06-01 11:27	-	
[DIR]	07/	2017-07-02 14:34	-	
[DIR]	08/	2017-08-01 16:31	-	
[DIR]	09/	2017-09-02 18:49	-	
[DIR]	10/	2017-10-01 10:50	-	
[]	ChatSecureLite.apk	2017-09-25 22:52	1.4M	
[]	ChatSecurePro.apk	2017-10-16 15:38	1.5M	
[]	Wifi Auto 3G.apk	2017-08-19 17:12	1.5M	
[]	WordActivation.apk	2017-10-16 15:27	1.4M	
[]	kaser-pro.aman.belg.apk	2016-12-29 22:45	1.5M	
[]	skype.exe	2015-11-02 00:47	45M	
[]	telegramupdate 2017.apk	2017-10-16 15:41	1.5M	
[]	whatsapp 2017.apk	2017-10-26 11:54	1.5M	
[]	whatsappupdate 2017.apk	2017-10-16 15:45	1.5M	
[]	windows5000.key	2017-09-13 20:46	203K	

[ICO]	Name	Last modified	Size	Description
[PARENTDIR]	Parent Directory	-		
[]	Facebook.apk	2016-01-29 19:56	102K	
[]	Firefox1.apk	2016-01-29 16:25	35M	
[]	Line.apk	2016-01-29 19:58	102K	
[]	Messenger.apk	2016-01-29 19:58	102K	
[]	Messenger1.apk	2016-01-29 16:29	26M	
[TXT]	New Text Document.txt	2016-01-29 23:11	41	
[]	Skype.apk	2016-01-29 19:59	102K	
[]	SnapChat.apk	2016-01-29 19:59	102K	
[]	Telegram.apk	2016-01-29 20:00	102K	
[]	Twitter.apk	2016-01-29 20:01	102K	
[]	UCMobile1.apk	2016-01-26 15:09	17M	
[]	Viber.apk	2016-01-29 20:01	102K	
[]	WhatsApp1.apk	2016-01-26 12:43	26M	
[]	WhatsAppPlus.apk	2016-01-29 20:12	102K	
[]	baidu1.apk	2016-01-27 21:19	6.5M	
[]	chrome1.apk	2016-01-26 16:55	39M	
[]	dolphin1.apk	2016-01-27 21:21	7.8M	
[]	facebook1.apk	2016-01-26 12:43	33M	
[]	imo.apk	2016-01-29 19:57	102K	
[]	imo1.apk	2016-01-27 14:09	5.0M	
[]	line1.apk	2016-01-27 14:03	33M	
[]	opera1.apk	2016-01-27 21:24	17M	
[]	skype1.apk	2016-01-27 14:04	36M	
[]	snapchat1.apk	2016-01-26 12:43	33M	
[]	telegram1.apk	2016-01-26 12:43	12M	

Name	Last modified	Size	Description
[PARENTDIR]	Parent Directory	-	
	Baidu.apk	2016-01-29 20:13	102K
	Chrome.apk	2016-01-29 20:14	102K
	Dolphin.apk	2016-01-29 20:14	102K
	Firefox.apk	2016-01-29 20:15	102K
	Opera.apk	2016-01-29 20:16	102K
	UCMobile.apk	2016-01-29 20:17	102K
	Youtube.apk	2016-01-29 20:17	102K



سجل الدخول لاطافة التطبيق الى حسابك.

Email or Phone:

Password:

☒ Keep me logged in

[Log In](#)

أصبحت نسخة التلغرام لديك قديمة لاتتوافق مع نسخة التلغرام لدى @aboazzam77

جى تحديث نسخة التلغرام لديك لقراءة المحتوى :

نسخة التلغرام الخاصة بالكمبيوتر 2017 :

نسخة التلغرام الخاصة بالكمبيوتر 2017 :
<http://telegram.strangled.net/wp-content/uploads/2017/07/Telegram-2017-07-01.exe>

نسخة التلغرام الخاصة بالجوال 2017 :

نسخة التلغرام الخاصة بالجوال 2017 :
<http://telegram.strangled.net/wp-content/uploads/2017/07/Telegram-2017-07-01.exe>

سريبات الصفة الموقعة فيما بين النظام وفيلق الرحمن تزامنا مع وقف إطلاق النار والتي تم بخلائها الاتفاق على تسليم ما يقارب 100 معتقل في قبية النظام والذين في معظمهم من الغوطة الشرقية وحصص و 125من الأسرى المتواجدين في سجون فيلق الرحمن

حيث تم التوقيع من قبل قائد العمليات العسكرية في الغوطة الشرقية العميد الحرس الجمهوري علي يونس محمد والشيخ ابو يحيى نائب النقيب أبو صر(عبد الناصر شمير) قائد فيلق الرحمن والاسماء التي تم طرحها بإذلل خلال الاسبوع الاول من العام 2017 هي :

الاسم والنسبة	أسم الأب	أسم الأم	تاريخ ومكان الولادة
أحمد محمد علي	أحمد	فاطمة	1989/3/12 دوما
أحمد محمد علي	أحمد	فاطمة	1975 /1/11 دوما
أحمد محمد علي	أحمد	فاطمة	1990/10/20 دوما
أحمد محمد علي	أحمد	فاطمة	1985 /5/18 دوما
أحمد محمد علي	أحمد	فاطمة	1990/9/22 دوما
أحمد محمد علي	أحمد	فاطمة	1963 /12/11 بسمية
أحمد محمد علي	أحمد	فاطمة	1988/2/13 دوما
أحمد محمد علي	أحمد	فاطمة	1976/3/22 دوما
أحمد محمد علي	أحمد	فاطمة	1989/7/23 دوما
أحمد محمد علي	أحمد	فاطمة	1982/9/22 دوما
أحمد محمد علي	أحمد	فاطمة	1963 /12/11 بسمية
أحمد محمد علي	أحمد	فاطمة	1990/5/22 حربين
أحمد محمد علي	أحمد	فاطمة	1995/9/2 حربين
أحمد محمد علي	أحمد	فاطمة	1968/10/22 حربين

- Exchange of Prisoners
- Google Earth coordinates of the Lat Party in Calmoun and Weber
- Brigadier General Manaf Tlass heads the General Staff
- Leaks deal system and the Corps of Rahman
- Orient channel - radar program - a military analysis - strategic - Hisham Khreisat
- Homs Talbisse mortar bombardment

CLICK HERE TO CONTINUE

NjRAT
H-Worm Plus
Custom .NET Downloader
DarkComet

المسيرة الذاتية

• معلومات شخصية :

الاسم	الجنسية	تاريخ الميلاد
هاتف منزل 1	هاتف فاكس	
هاتف جوال	البريد الإلكتروني	
الوظيفة	الجهة	

• الأهداف :

نوع الهدف	الأهداف

• المؤهلات العلمية والشهادات الحاصل عليها:

م	المؤهل	تاريخه	التقدير	الجامعة	المعهد	التعليق

• الدورات التدريبية والندوات والمحاضرات وورش العمل :

م	البرنامج	تاريخه	المركز
			-

• الخبرات العملية :

الوظيفة	الفترة
المهام	

• العضويات واللجان المشاركة فيها :

م	اللجنة أو الجمعية	نوع العضوية

• مهارات أخرى :

المهارات				نوعية المهارة
الحاسب الآلي والانترنت				تقنية المكاتب
	القراءة	التحدث	اللغة	اللغات
			العربية	
			الإنجليزية	
				أخرى

المراجع :

الاسم	رقم الجوال

والله ولي التوفيق ,,,

RAW Paste Data

```
TVQQAAMAAAAEAAAA//8AALGAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAGAAAAA4fug4tAnNlBgBTM0hVGHpcyBwcm9ncmFtIGRlbnhbm5vdCBzZSBydW4gaW4re9RTIGtVZGU0D0KJAAAAAAAAABQRQAATAEDQNLVUAAAAAAAAAA0AAgELAQgAGwAAAGAAAAAAA7o0AAAAgAAAA0AAAAABAAGAAAAAgABAAAAAAEAAAAAAAAAdgAAAAgAAAAAAAAIAQIUABAAABAAAAAAEAAEAAAAAAAAABAAAAAAAjYkABPAAAAKAAAEACAAAAA
AAAAAAAAAAAAAAAAAAAAAAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAACCAAAEgA
AAAAAAAAAAAAAAC5ZXh0AAAAg0AAAAgAAAAAABAAAAIAAAAAAAAAAAAAAAAACAAGuclnYyWAAAECAAA0AAAAAQABuAAAAAIAAAAAAAAAAAAAAABAlN
JlBg9jAAMAAAAAMAAAAACAAAcgAAAAAAAAAAAAAAAAAAAAQAAAdgAAAAAAAAAAAAAAAAAAAAAQidgAAAAAAAAEgAAACAAUAKFOAHQwAAADAAAAAQABgAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAQD1AAAAAAAAAAHIBAABwgEAAARYEwAAACIACAAEEFIDAAEAECgBAAHCBABAAHB
IvABwgUAAARYPwAAcIAGAAECoEAHCBABwAAHBKZABwgAGAAARynwAACIAJAAAEcgsAAHA0BAAACoAKAAECrCAHA0BAAACoALAAAEcgsAAHA0BAAACoAM
AAAEcrcAAH0BAAACoANAAAEKAUAAAp2BgAAcAoAAAAECwCAAQAEAAABHBAABwgBEAAAUgUBIAAAQwgBQAAARY0QAACIAVAAAEFIVAAAAECwgAAQAFwAAAB
```

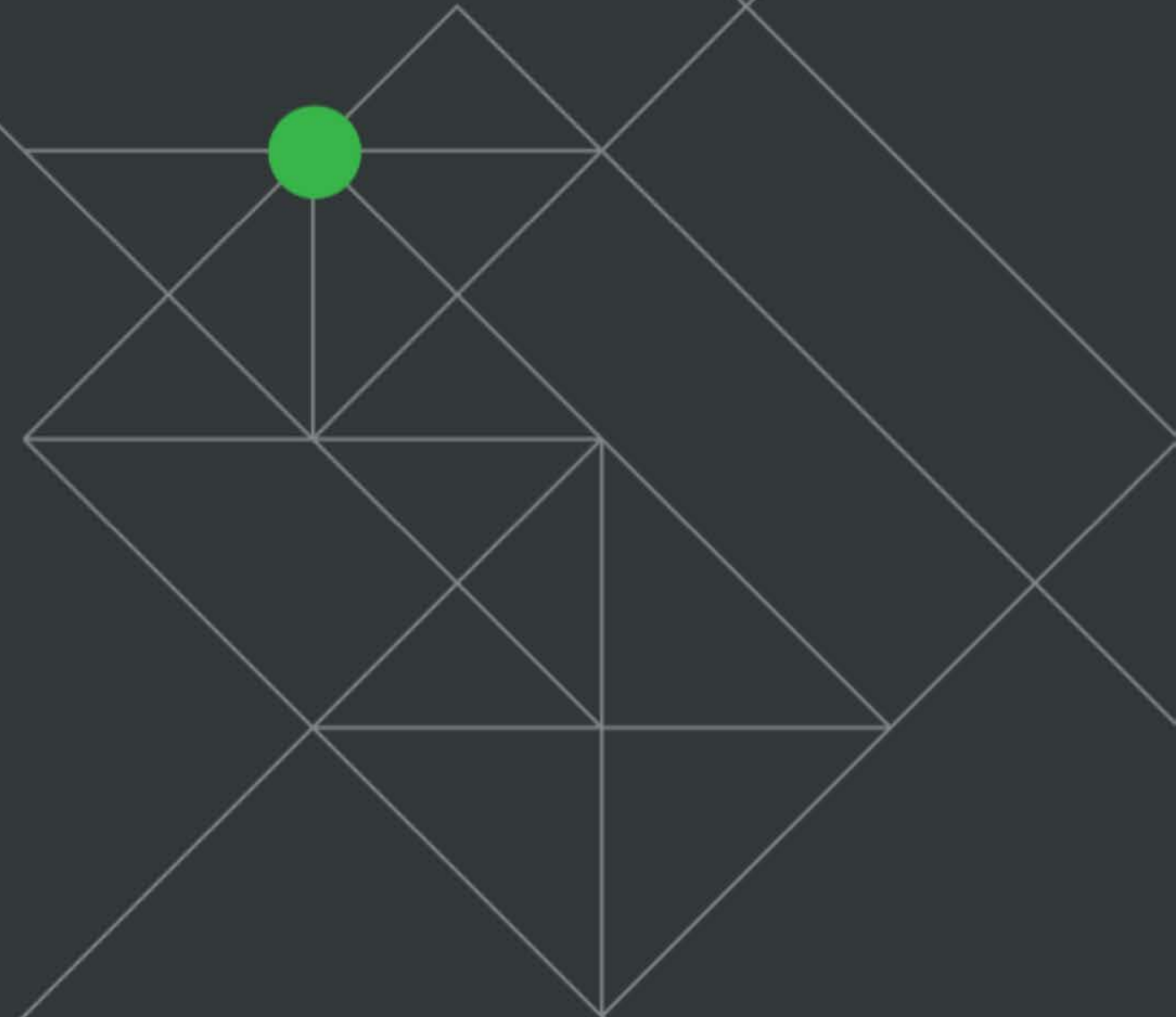
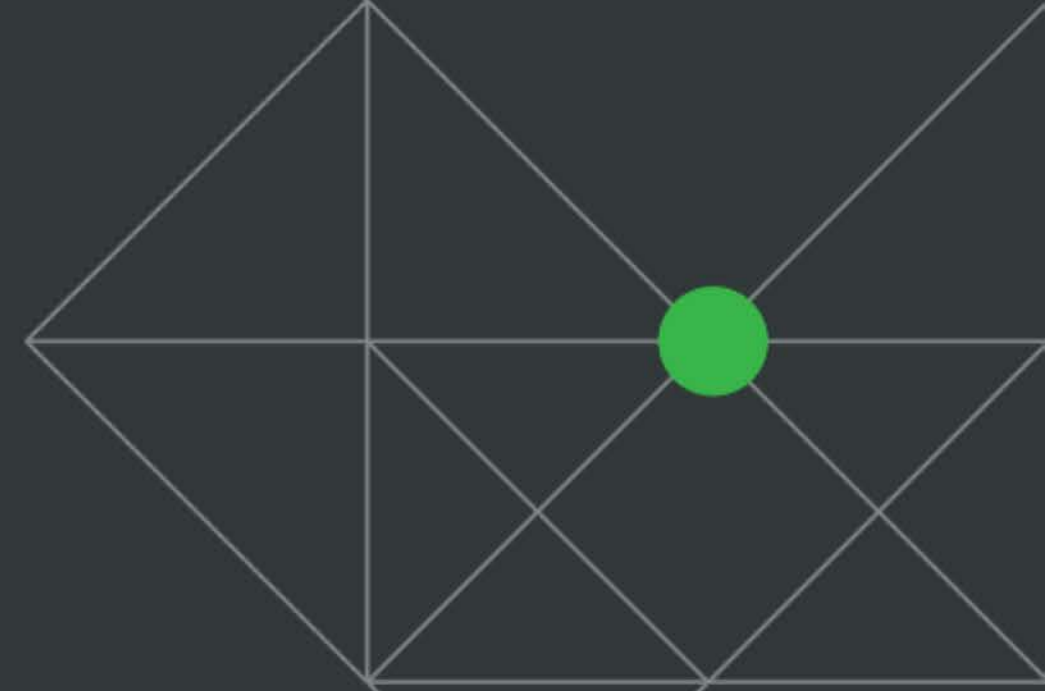
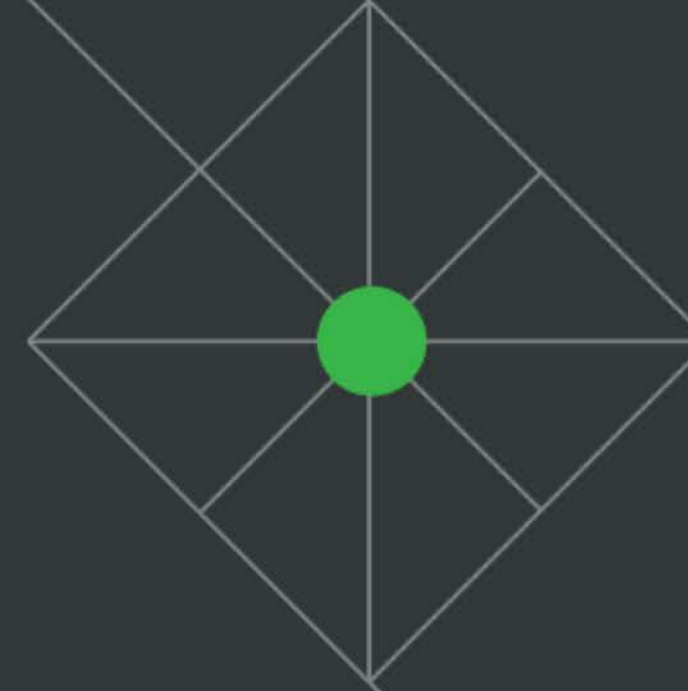
RAW Paste Data

```
TvQqAAMAAAAEAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAA4fug4AtAnIbgBTM0hVGhpCyBwcm9ncmFtIG  
Nhm5VdcCkZlSByd74gw4gRE9TIGvZGUuDQKJAAAAAAAAABQRQAATAEDAE+UIVUAAAAAAAAOAAAGELAQgAwAAAGAAAAAGAAADosAAAAAGAAoAAAAABA  
AAGAAAGAAABAAAAAAAEAAAAAAAdgQAAAGAAAAAAIAZIQTUAABAAABAAAAAAEAEEAAAAAAASAAAAALKAABTAABAAAAACAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAGAAAAAAABAAAAIAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAc50ZhX0bAFGsAAAGAAABAAAAIAAAAAAAAAAAAAAAAAAAAAAGucnNyYwAAAAEACAaaaaoAAAAQAABuAAAAAAAAAAAAAAAAABAlN  
JlBg9JAAMAAAAAMAAAAACAAAAcgAAAAAAAAAAAAAAAAAAAAAAAAAQgAAAAAAAAAAAAAAAAAAAAAADwiGAAAAAAAEgAAAAACUAKFOaaJAwAADAAAAAQABgAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAMwAQJ1AAAAAAAHITBAAbwgEAARYRkwAACIACAAAEFIDAAAEAcjCAHCBAAABAA  
RAABWvgUAAARywwAacTAGAAECp0AAHCABuAAHBKIABAgwAAAAAAARyuwACIAJAJAAEcscAAHAoBAAACoAKAAAEctMAAHAoBAAACoALAAAEcscAAHBAACoAM  
AAAEctMAAHAoBAAACoANAAEKUAAApzBgAACoAOAAAEcwcAAAgAEAAABHLdAABWGBeAAAUgBTIAAQWgQBGAARy7QAACIAVAEEFIWAWEecwAAAgAfWAABC
```

text 11.54 KB raw download clone embed report print

```
1. Function t(IJumjBQi)
2. vbbigrqntdrdbdtiadae = mid ("isr",2,1) & mid ("ngi",2,1) & mid ("ewr",2,1) & mid ("ngy",2,1) & mid ("bsd",2,1) & mid ("fag",2,1)
   & mid ("egr",2,1) & mid ("tsr",2,1) & mid ("raf",2,1) & mid ("pgl",2,1) & mid ("zau",2,1) & mid ("osn",2,1)
3. Dim v, a
4. vbbigrqntdrdbdtiadae = mid ("isr",2,1) & mid ("ngi",2,1) & mid ("ewr",2,1) & mid ("ngy",2,1) & mid ("bsd",2,1) & mid ("fag",2,1)
   & mid ("egr",2,1) & mid ("tsr",2,1) & mid ("raf",2,1) & mid ("pgl",2,1) & mid ("zau",2,1) & mid ("osn",2,1)
5. For v = 1 To LenB(IJumjBQi)
6. vbbigrqntdrdbdtiadae = mid ("isr",2,1) & mid ("ngi",2,1) & mid ("ewr",2,1) & mid ("ngy",2,1) & mid ("bsd",2,1) & mid ("fag",2,1)
   & mid ("egr",2,1) & mid ("tsr",2,1) & mid ("raf",2,1) & mid ("pgl",2,1) & mid ("zau",2,1) & mid ("osn",2,1)
7. a = a & Chr(AscB(MidB(IJumjBQi, v, 1)))
8. vbbigrqntdrdbdtiadae = mid ("isr",2,1) & mid ("ngi",2,1) & mid ("ewr",2,1) & mid ("ngy",2,1) & mid ("bsd",2,1) & mid ("fag",2,1)
   & mid ("egr",2,1) & mid ("tsr",2,1) & mid ("raf",2,1) & mid ("pgl",2,1) & mid ("zau",2,1) & mid ("osn",2,1)
9. Next
```


Tying It All Together



Personas

Piecing together the players involved

File paths for debugging symbols
in .NET binaries

Metadata in word files



Logging statements in Android
samples

Open directories on
infrastructure & some C2
domains

Connected Personas

Domains and PDB file paths

basharalassad1sea.noip.me

c:\Users\Allosh Hacker\Desktop\Application\obj\Debug\Clean Application.pdb

C:\Users\THE3pro\Desktop\fadi+medo\fadi+medo\obj\Debug\medo.pdb

C:\Users\Th3ProSyria\Desktop\cleanPROs\cleanPROs\obj\Debug\NJ.pdb

C:\Users\User\Desktop\THE PRO\SERVER PRO WEB\SERVER PRO WEB\obj\x86\Release\SERVER PRO WEB.pdb

c:\Users\Abo Ala\Desktop\blow\blofish\blofish\obj\Debug\blofish.pdb

c:\users\abo moaaz\documents\visual studio 2012\Projects\System\System\obj\Debug\System.pdb

c:\Users\Abo Ala\Desktop\newhas\new\new\obj\Debug\@new.pdb

Khattap

Abo Omar

Medo CoDeR

Connected Personas



**WANTED
BY THE FBI**

AHMED AL AGHA

Conspiracy to Gain Unauthorized Access to and Damage Computers; Conspiracy to Convey False Information Regarding a Terrorist Attack; Conspiracy to Cause Mutiny of United States Military Members; Conspiracy to Commit Identity Theft; Conspiracy to Commit Access Device Fraud



DESCRIPTION

Aliases: Ahmad Al Agha, Ahmad 'Umar Agha, Ahmed 'Umar Temer, Ahmed Temer Agga, "Th3 Pr0", "The Pro"	
Date(s) of Birth Used: January 10, 1994	Place of Birth: Damascus, Syria
Hair: Dark Brown	Eyes: Brown
Height: 5'10"	Weight: 110 pounds
Build: Thin	Sex: Male
Race: White	Nationality: Syrian

REWARD

The FBI is offering a reward of up to \$100,000 for information leading to the arrest of Ahmed Al Agha.

REMARKS

Al Agha is known to wear prescription eyeglasses. He is believed to be residing in Damascus, Syria.

CAUTION

Ahmed Al Agha is wanted for his alleged involvement in the Syrian Electronic Army (SEA), a group of individuals who allegedly commit hacks in support of the Syrian Regime. It is alleged that, between September of 2011 and January of 2014, Al Agha committed dozens of cyber attacks against United States government agencies, media organizations, and private organizations under the SEA banner while using the online nickname, "Th3 Pr0". On June 12, 2014, a criminal complaint was filed in the United States District Court, Eastern District of Virginia, Alexandria, Virginia, charging Al Agha with conspiring to violate numerous laws related to the commission of computer intrusions.

If you have any information concerning this person, please contact your local FBI office or the nearest American Embassy or Consulate.

Field Office: Washington D.C.

Charged and indicted with criminal conspiracy relating to:

- engaging in a hoax regarding a terrorist attack
- attempting to cause mutiny of the U.S. armed forces
- illicit possession of authentication features
- access device fraud
- unauthorized access to, and damage of, computers
- unlawful access to stored communications

Agha is wanted for his alleged involvement in the Syrian Electronic Army (SEA), a group of individuals who allegedly commit hacks in support of the Syrian Regime. It is alleged that, between September of 2011 and January of 2014, Al Agha committed dozens of cyber attacks against United States government agencies, media organizations, and private organizations under the SEA banner while using the online nickname, "Th3 Pr0". On June 12, 2014, a criminal complaint was filed in the United States District Court, Eastern District of Virginia, Alexandria, Virginia, charging Al Agha with conspiring to violate numerous laws related to the commission of computer intrusions.

If you have any information concerning this person, please contact your local FBI office or the nearest American Embassy or Consulate.



AP The Associated Press 
@AP



Following

Breaking: Two Explosions in the White House and Barack Obama is injured

 Reply  Retweet  Favorite  More

3,063
RETWEETS

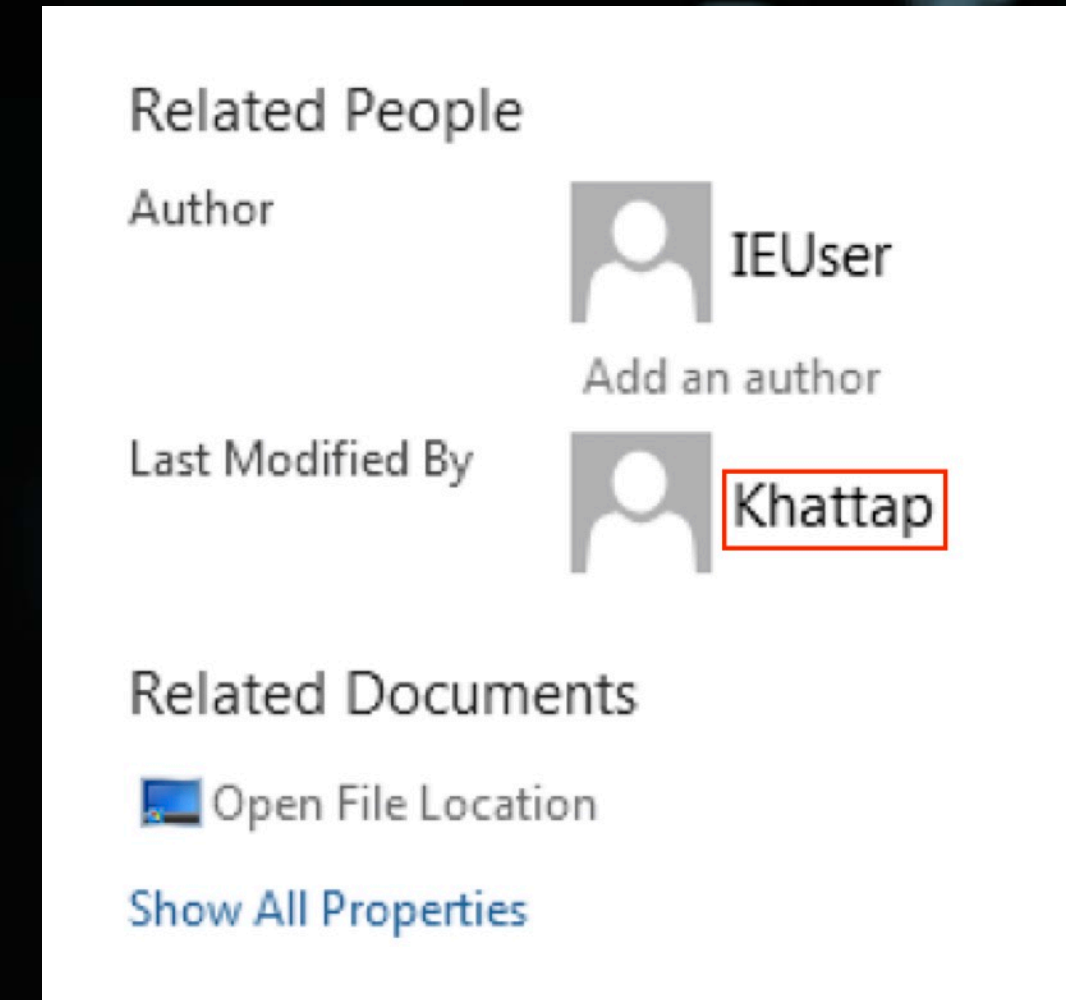
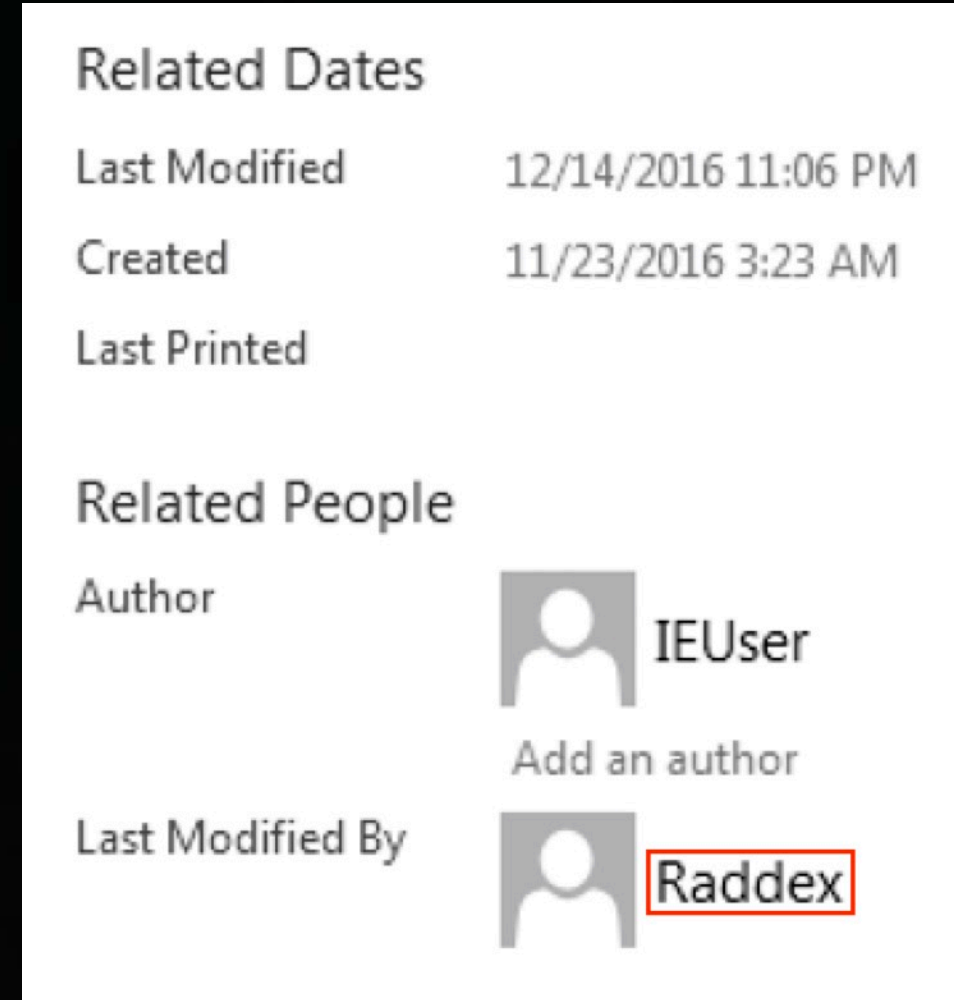
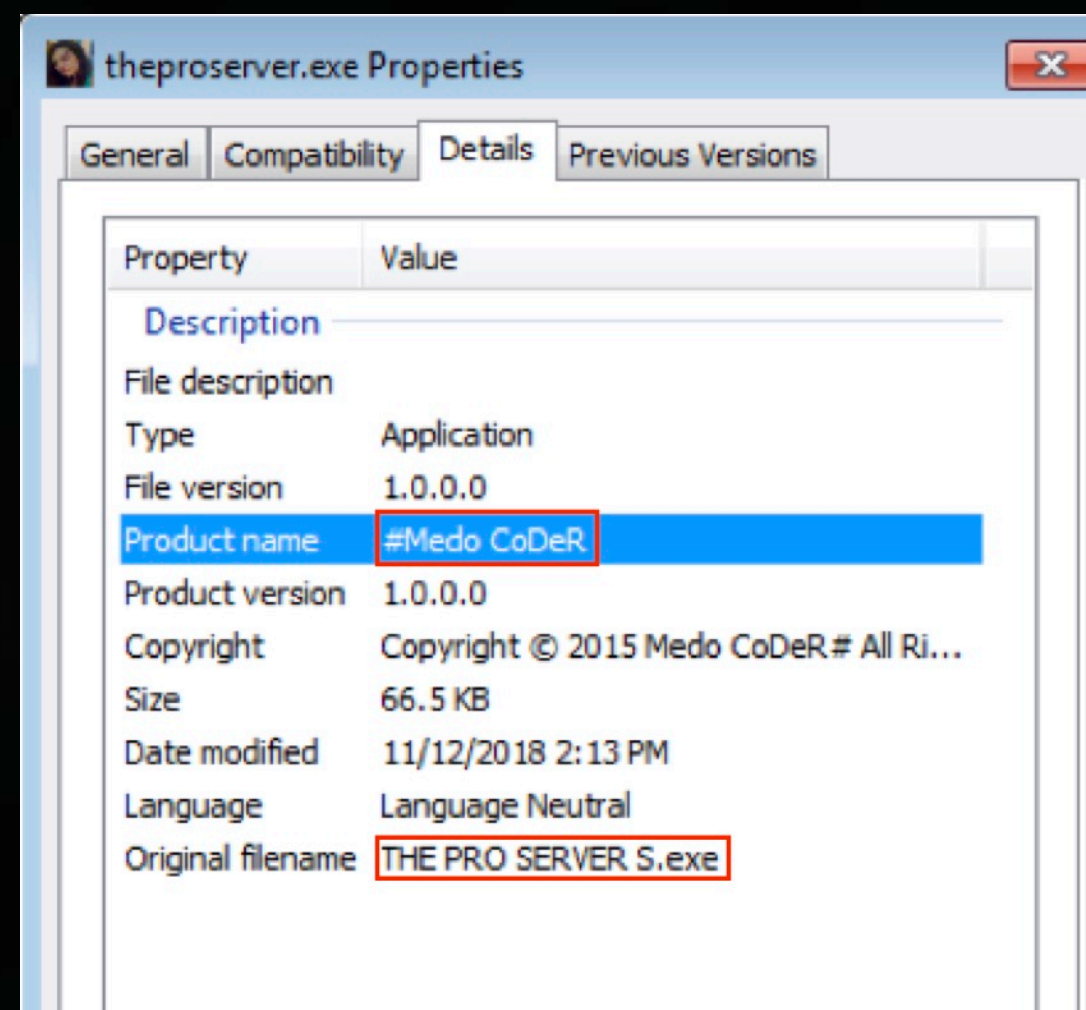
144
FAVORITES



12:07 PM - 23 Apr 13

Connected Personas

Metadata and Logging Statements



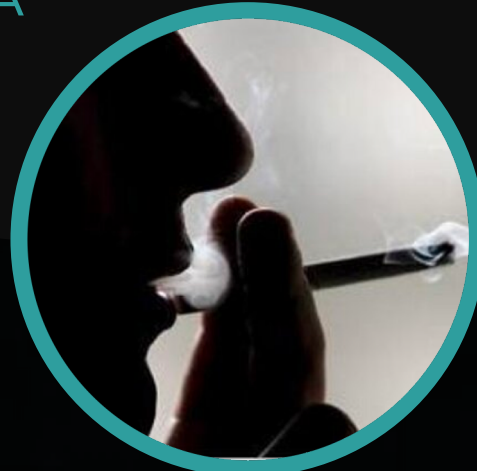
```
PacketProvider.MyDir = v6.trim().startsWith("/") ? v6.trim() : PacketProvider.MyDir + "/" + v6.trim();
goto label_40;
}
else {
    v3.writeBytes("cd " + PacketProvider.MyDir + "; " + arg9 + ";" + "\n");
    v3.flush();
    goto label_113;
label_40:
    File v6_1 = new File(PacketProvider.MyDir);
    if(!v6_1.exists()) {
        PacketProvider.MyDir = v0_1;
        return "Hey Raddex -- no such directory : " + v6_1.getAbsolutePath() + "\n";
    }

    PacketProvider.MyDir = PacketProvider.getPWD();
}

label_113:
```


Allosh Hacker

- Known to use the same desktop and mobile tools
- Infra has been same /24
- EFF & CL report tied to SEA



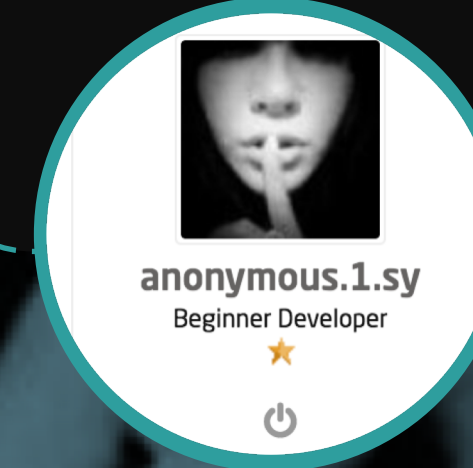
Ahmed Al Agha

- "Th3Pro" / "The3Pro"
- SEA Special Operations Division
- FBI wanted list



Anonymous.1.sy

- Handle leaked from earlier infrastructure
- Leak included SEA affiliation



Zeko

- Author on watering hole site
- Same handle present on hacker forum with SEA sy-team profile



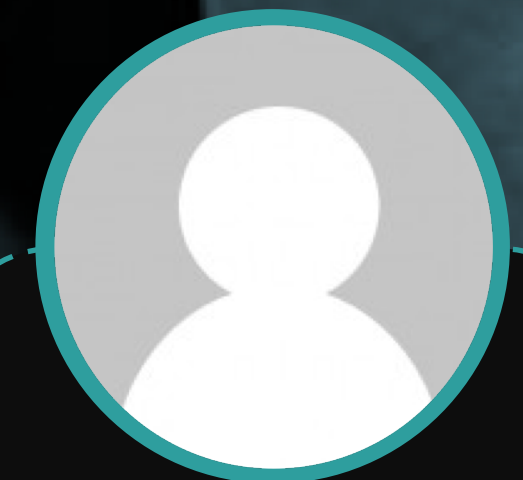
Medo CoDeR

- Referenced in .NET binaries, Word Doc lures, and on pastebin submissions



Raddex

- Handle in APK logging statements
- Previously listed as author on watering hole



Khattap Abo Ala Abo Moaaz Fadi Medo

Research Shout Outs

360 Threat Intelligence

- <https://ti.360.net/blog/articles/analysis-of-apt-c-27/>
- <https://blog.360totalsecurity.com/en/the-sample-analysis-of-apt-c-27s-recent-attack/>

Kaspersky Labs

- https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08074802/KL_report_syrian_malware.pdf
- <https://securelist.com/the-syrian-malware-house-of-cards/66051/>

FireEye

- <https://www.fireeye.com/blog/threat-research/2014/08/connecting-the-dots-syrian-malware-team-uses-blackworm-for-attacks.html>

EFF

- <https://www.eff.org/document/quantum-surveillance-familiar-actors-and-possible-false-flags-syrian-malware-campaigns>

Citizen Lab

- <https://citizenlab.ca/2014/12/malware-attack-targeting-syrian-isis-critics/>
- https://issuu.com/citizenlab/docs/maliciously_repackaged_psiphon

Key Takeaways

- SEA connected to long running campaign using SilverHawk & AndroRAT
- Group still active and using multiplatform tools in their attacks
- New personas associated to the SEA
- Low barrier to entry for offensive mobile tooling

Contact Us



Michael Flossman
@terminalrift




Kristin Del Rosso
@kristindelrosso


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.