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

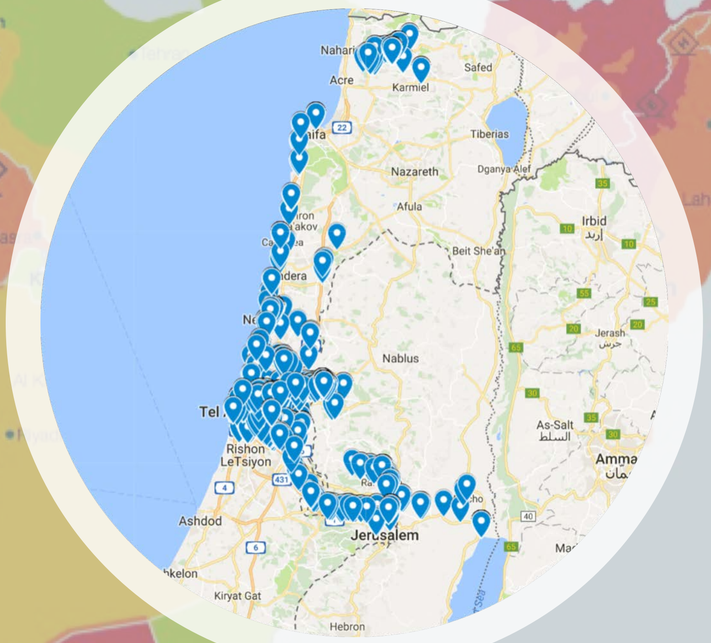
Agenda

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

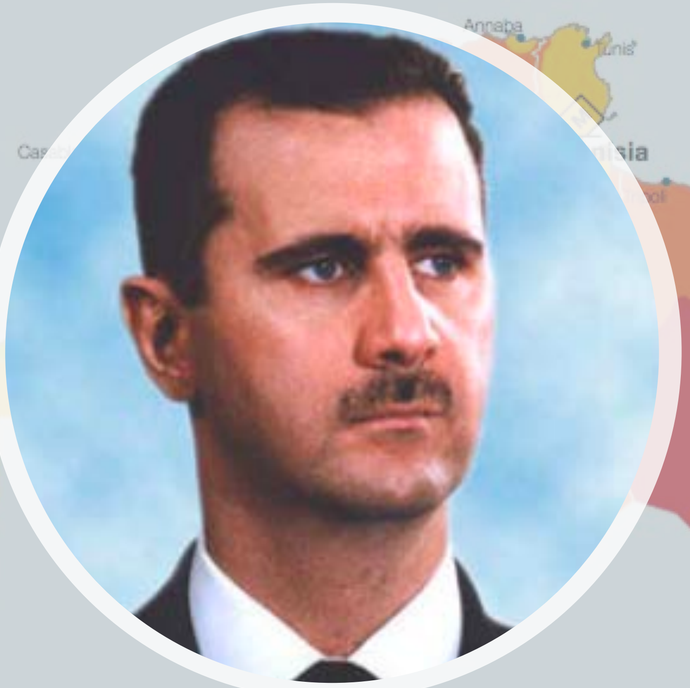
Upgrading Traditional Warfare

Security risk forecast

Political risk forecast



Upgrading Traditional Warfare



Enemies of the Internet 2014

Security risk forecast

Political risk forecast

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

PR0@Hotmail.NL


Skype
@Skype
Follow
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

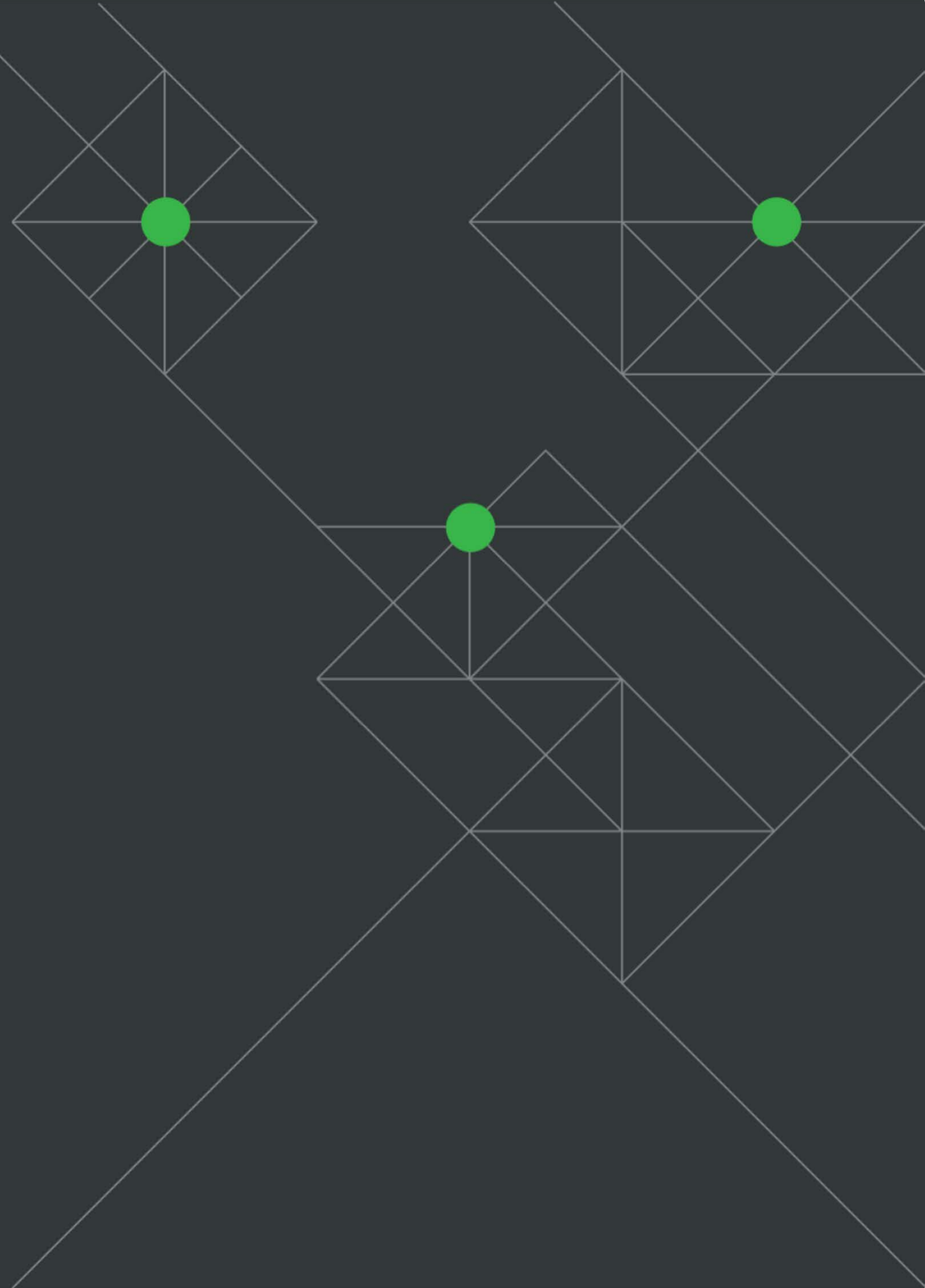

Microsoft News
@MSFTnews
Follow
Syrian Electronic Army Was Here via @Official_SEA16 #SEA pic.twitter.com/MDxQXK6CIJ
Reply Retweet Favorite Pocket More
14 RETWEETS
1 FAVORITE
2:31 PM - 11 Jan 14
Flag media


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

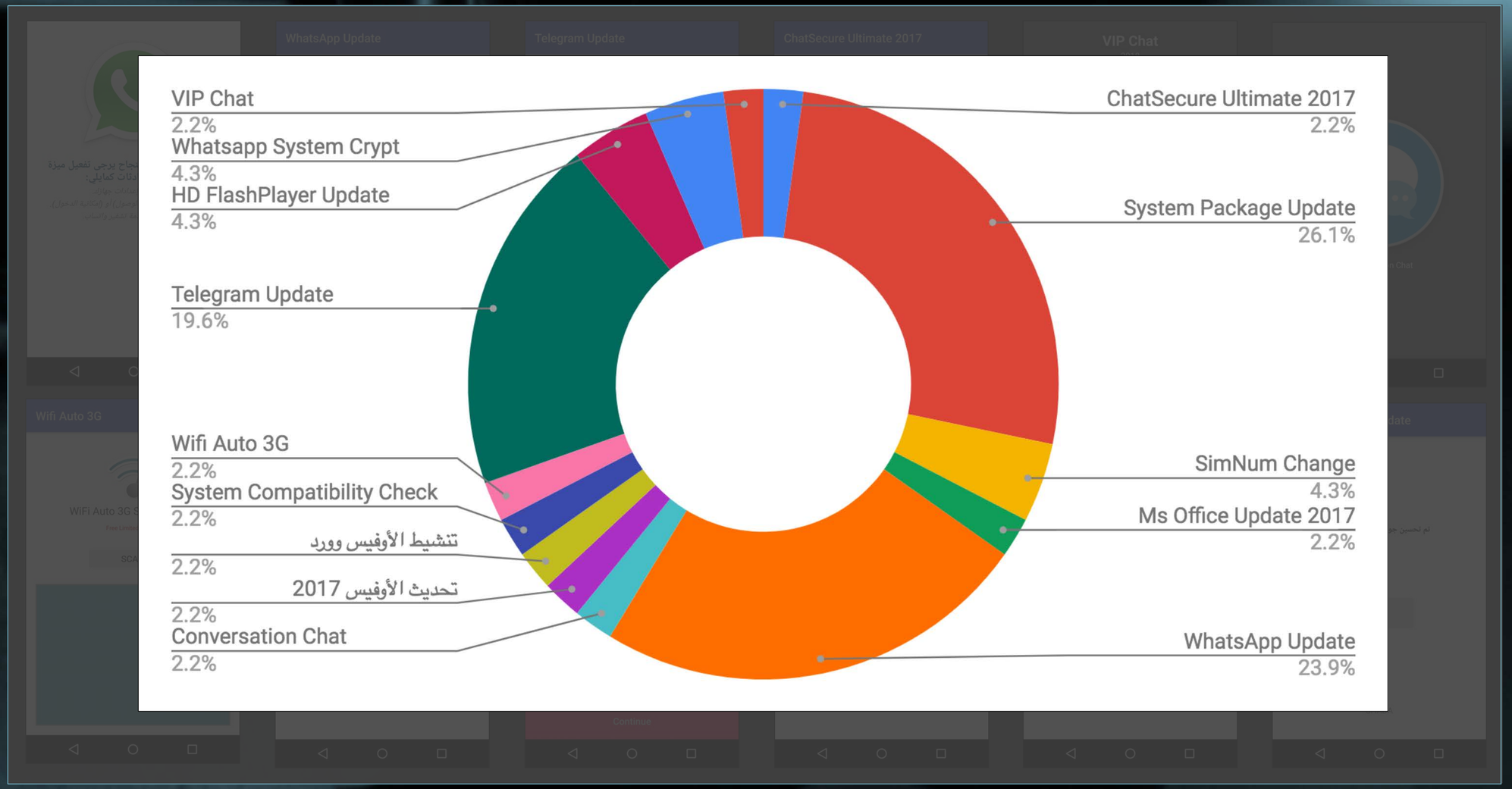

CNN
@CNN
Follow
Syrian Electronic Army Was Here... Stop lying... All your reports are fake! via @Official_SEA16 #SEA
Reply Retweet Favorite More
92 RETWEETS
25 FAVORITES
© Twitter

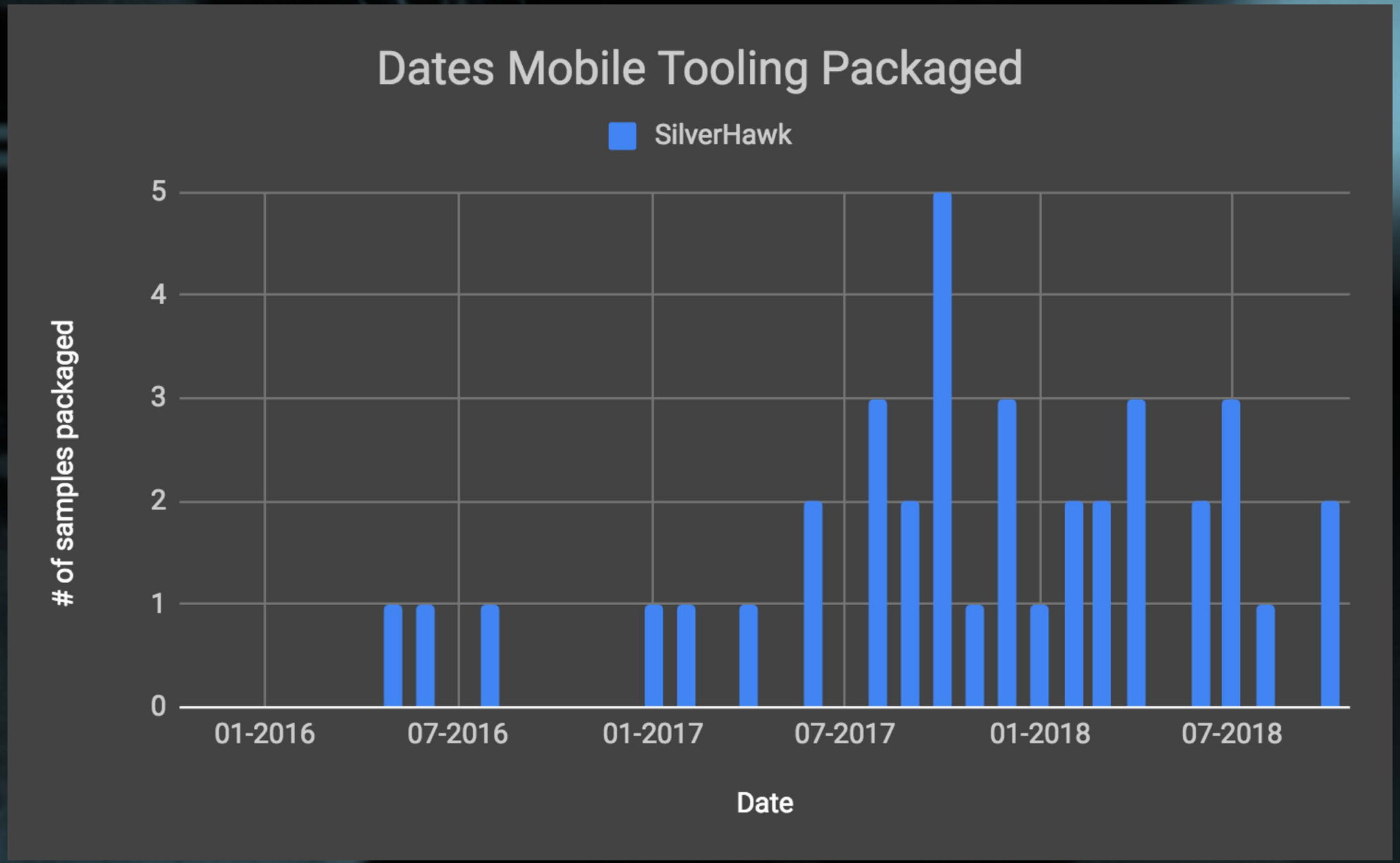

Tweets All / No replies
FC Barcelona @FCBarcelona · 2m
Special Hi to @RealMadrid! via @Official_SEA16 #SEA
Expand
Retweeted by FC Barcelona
FC Barcelona @FCBarcelona_cat · 7m
Dear FC Barcelona management, Don't let the Qatari money funds you, it's full of blood and kill via @Official_SEA16 #SEA #FCB
Expand
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
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

SilverHawk



SilverHawk


VIP Chat
2.2%
Whatsapp System Crypt
4.3%
HD FlashPlayer Update
4.3%
Telegram Update
19.6%
Wifi Auto 3G
2.2%
System Compatibility Check
2.2%
تنشيط الأوفيس وورد
2.2%
تحديث الأوفيس 2017
2.2%
Conversation Chat
2.2%
ChatSecure Ultimate 2017
2.2%
System Package Update
26.1%
SimNum Change
4.3%
Ms Office Update 2017
2.2%
WhatsApp Update
23.9%


Dates Mobile Tooling Packaged
SilverHawk
# of samples packaged
0
1
2
3
4
5
01-2016
07-2016
01-2017
07-2017
01-2018
07-2018
Date

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>

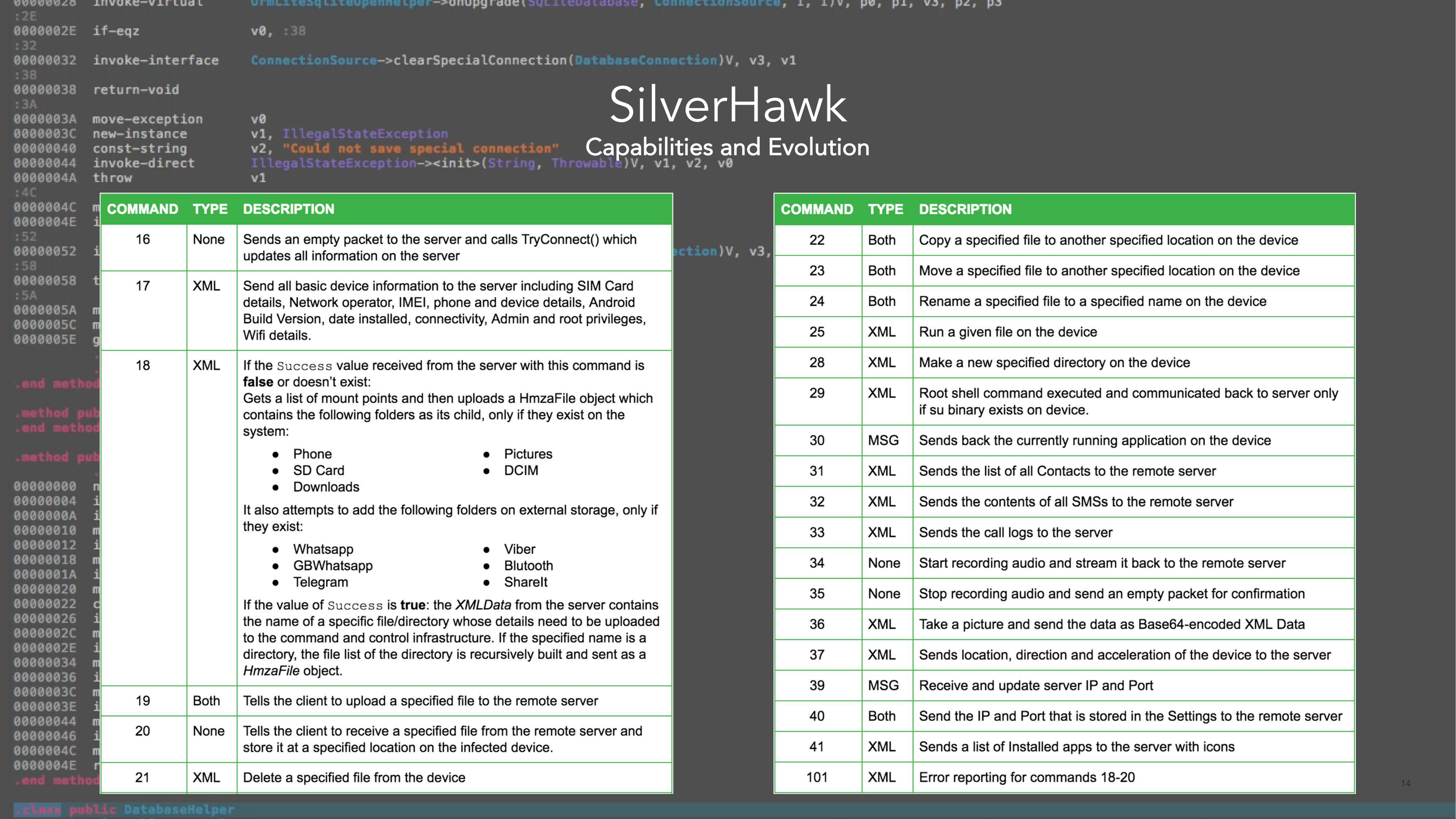
<XMLData></XMLData>

<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 @ : [redacted] GMT&lt;/DateOn&gt;
  &lt;DeviceName&gt;Unknown AOSP on ARM Emulator&lt;/DeviceName&gt;
  &lt;IMEI&gt;[redacted]&lt;/IMEI&gt;
  &lt;Loc&gt;us&lt;/Loc&gt;
  &lt;Oper&gt;[redacted]lt;/Oper&gt;
  &lt;SimSer&gt;[redacted]&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>
```



SilverHawk

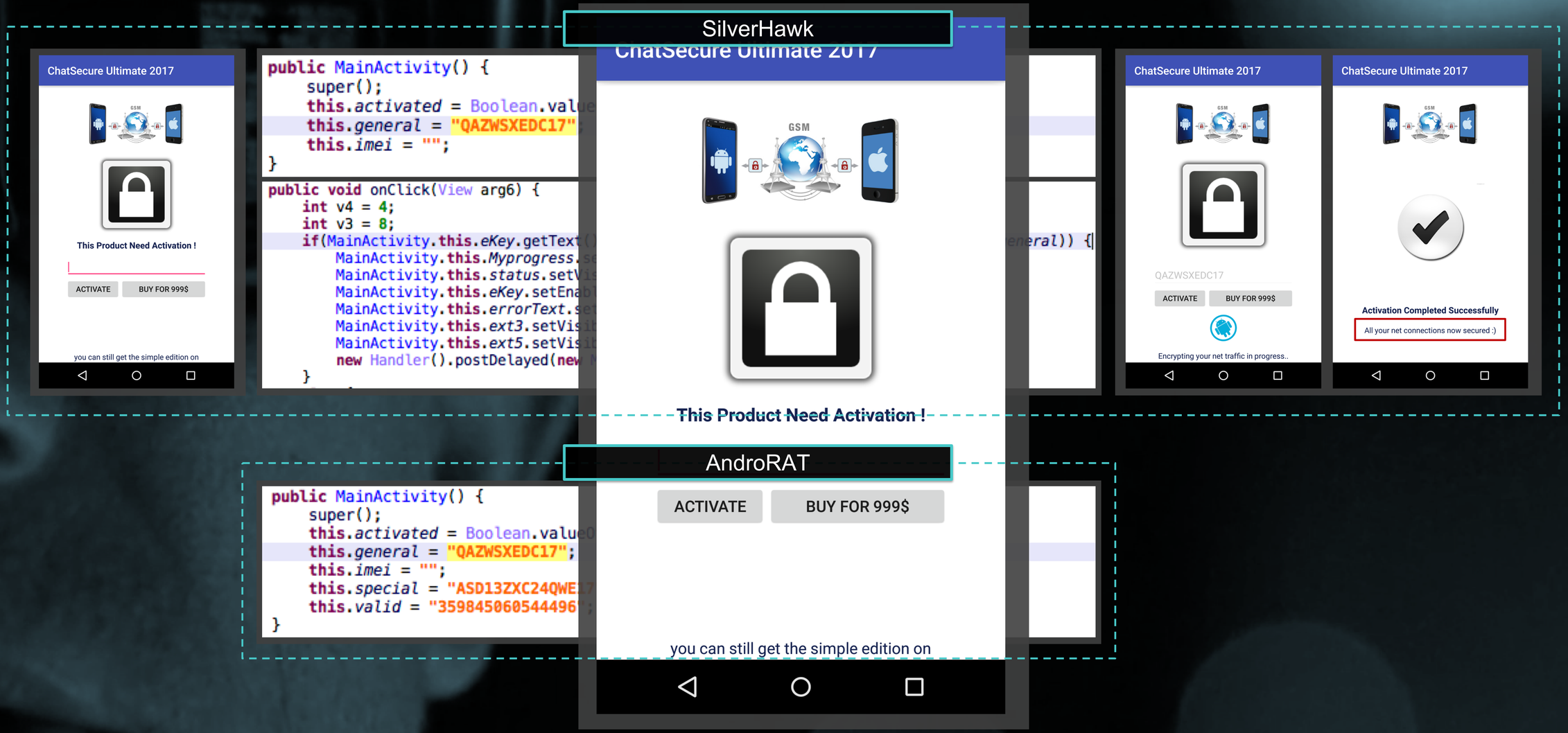
Capabilities and Evolution

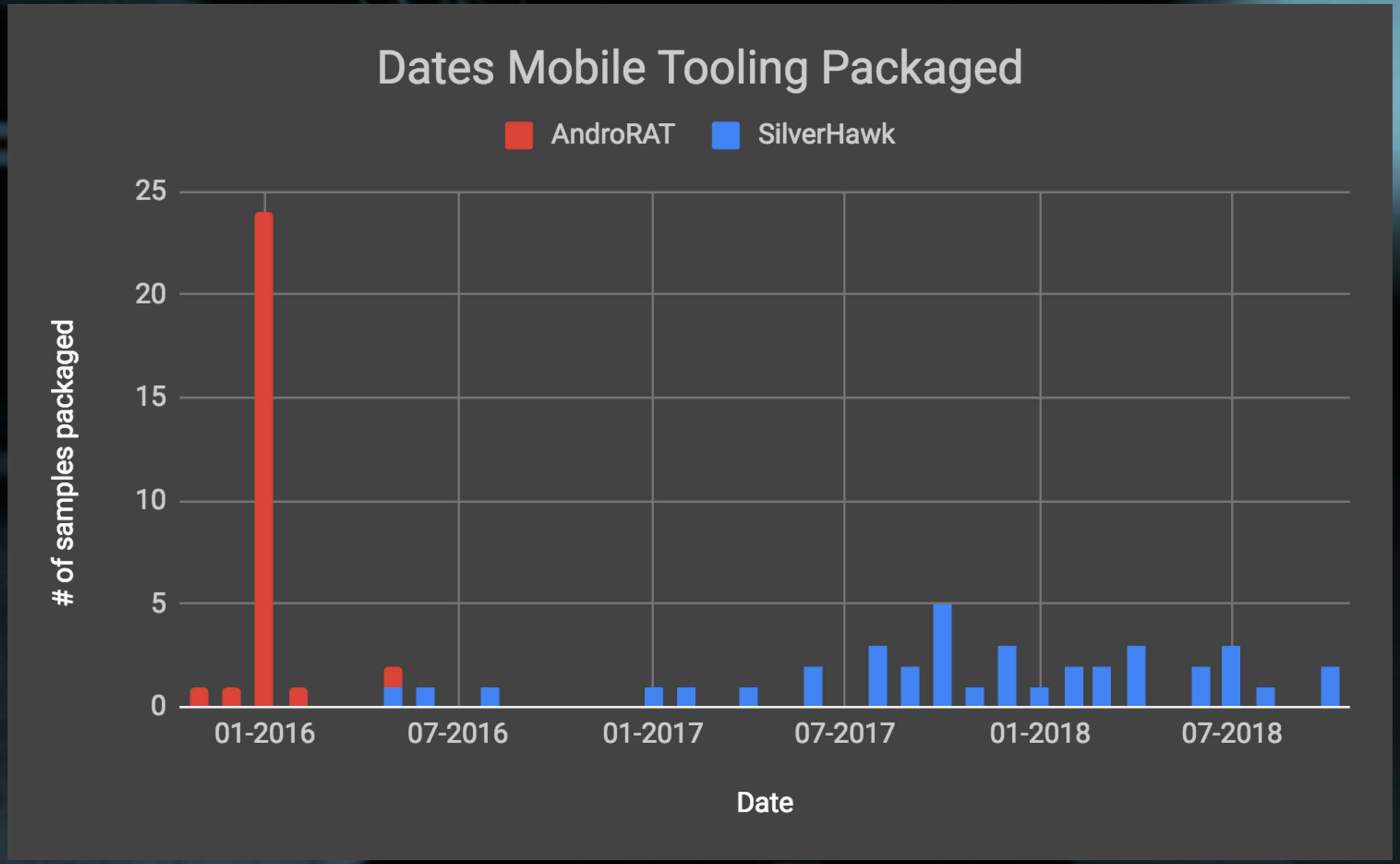
COMMAND	TYPE	DESCRIPTION
16	None	Sends an empty packet to the server and calls TryConnect() which updates all information on the server
17	XML	Send all basic device information to the server including SIM Card details, Network operator, IMEI, phone and device details, Android Build Version, date installed, connectivity, Admin and root privileges, Wifi details.
18	XML	If the `Success` value received from the server with this command is **false** or doesn't exist: Gets a list of mount points and then uploads a HmzaFile object which contains the following folders as its child, only if they exist on the system: • Phone • SD Card • Downloads • Pictures • DCIM It also attempts to add the following folders on external storage, only if they exist: • Whatsapp • GBWhatsapp • Telegram • Viber • Blutooth • ShareIt If the value of `Success` is **true**: the *XMLData* 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 *HmzaFile* object.
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

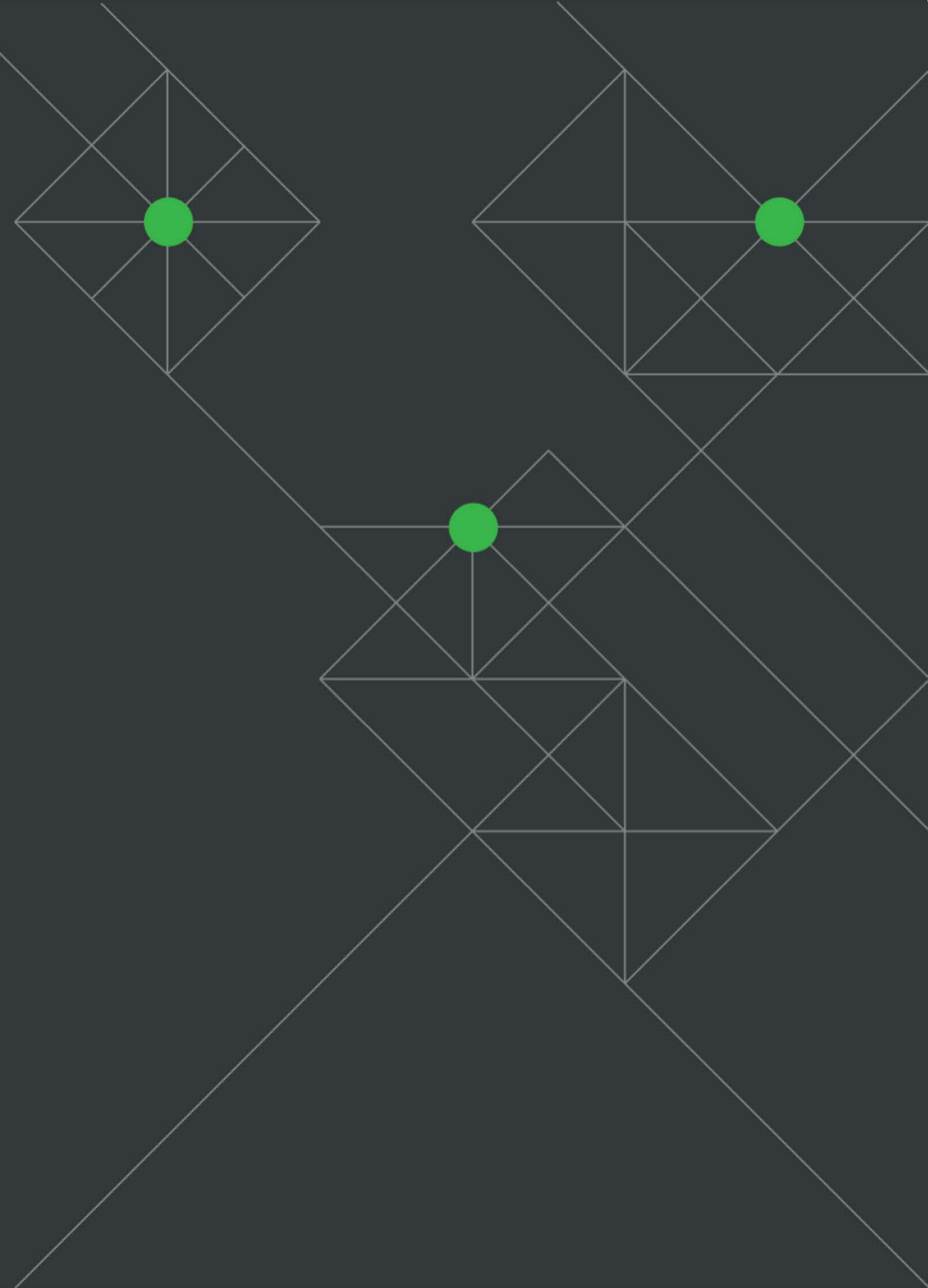
SilverHawk

The AndroRAT Connection




Dates Mobile Tooling Packaged
AndroRAT
SilverHawk
# of samples packaged
25
20
15
10
5
0
01-2016
07-2016
01-2017
07-2017
01-2018
07-2018
Date

Attack Vectors



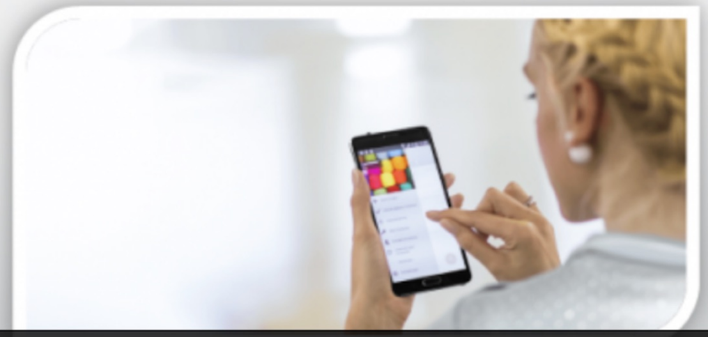
Search

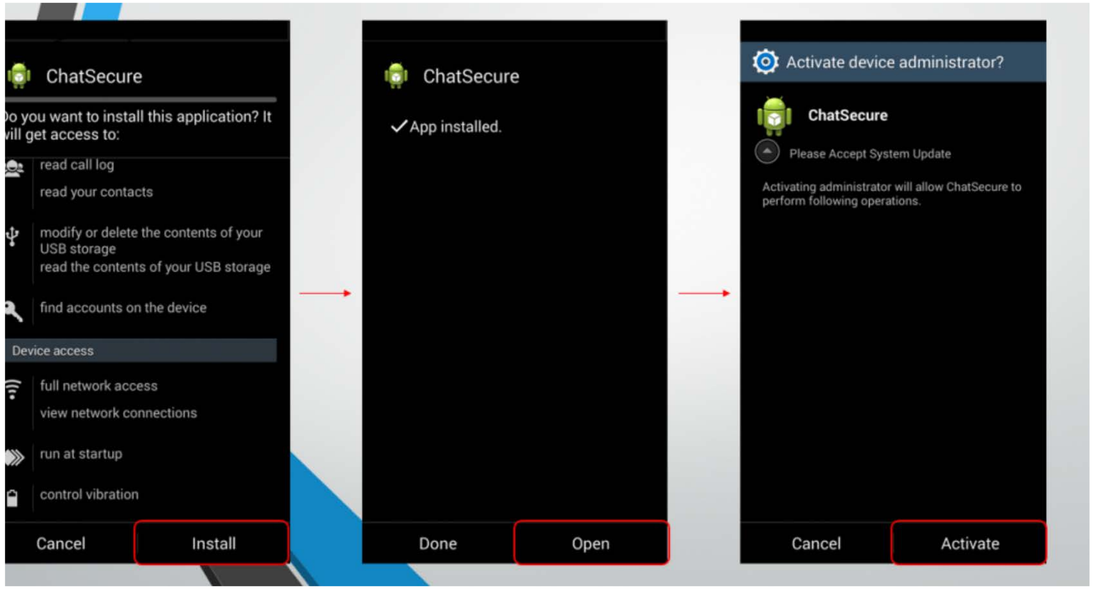
ChatSecure Lit

حول المنتج | تحميل البرنامج | سئلة و أجوبة

Chat Secure

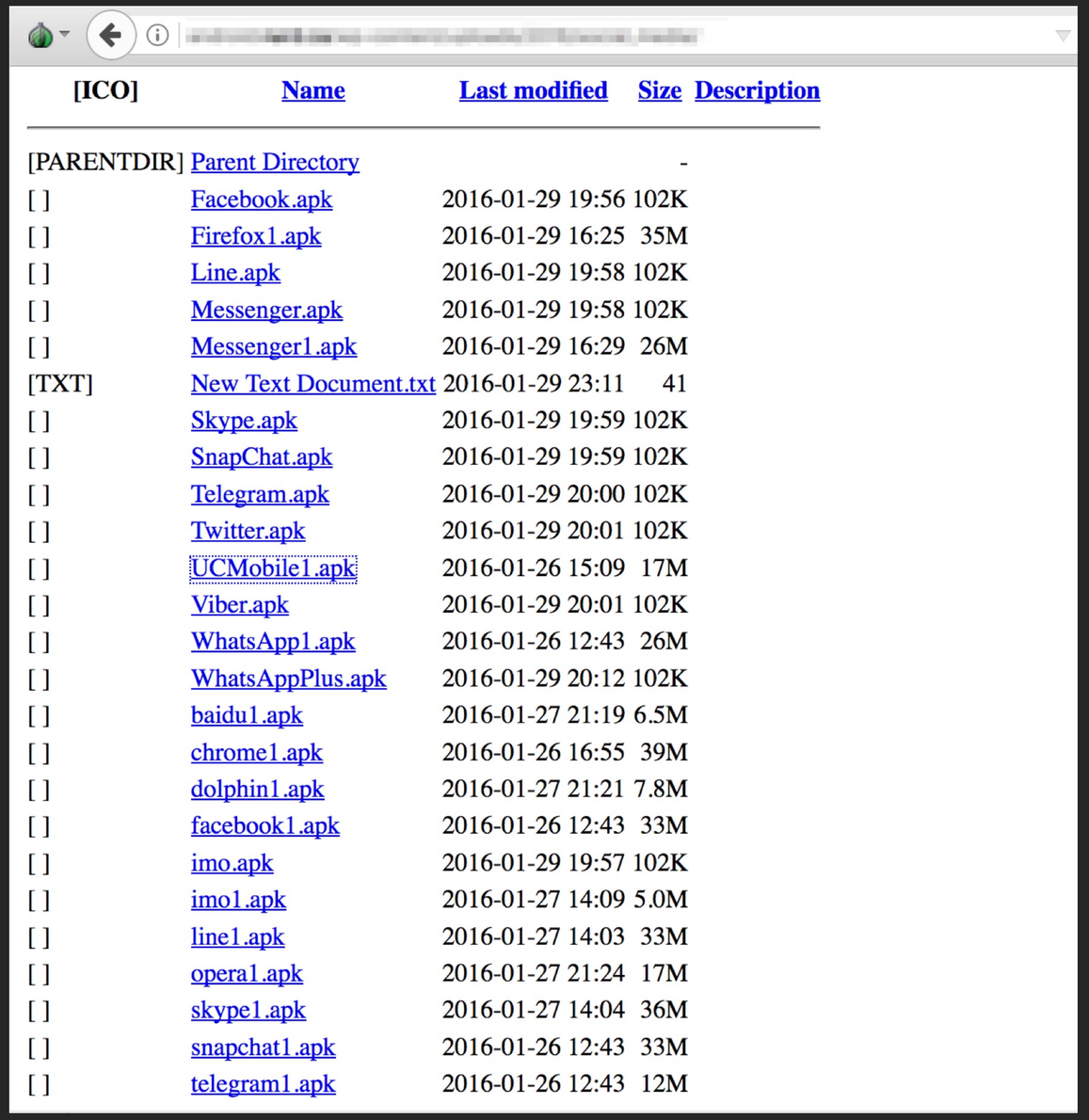
ي مفتوح المصدر لحماية كافة المراسلات على برامج الدردشة الخاصة بأجهزة الأندرويد



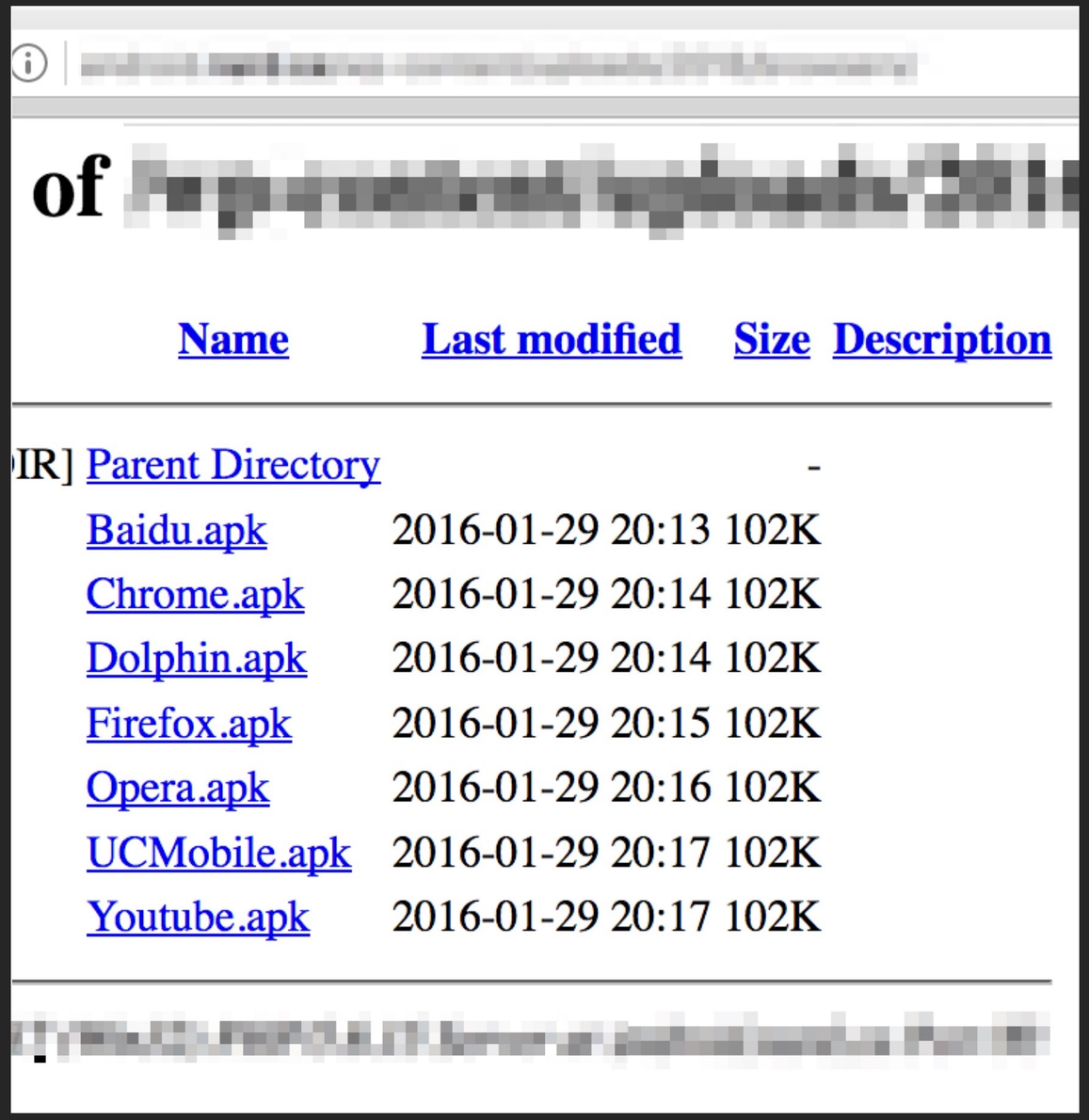


Index of [redacted]

[ICO]	Name	Last modified	Size	Description
[PARENTDIR]	Parent Directory		-	
[ ]	ح.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	



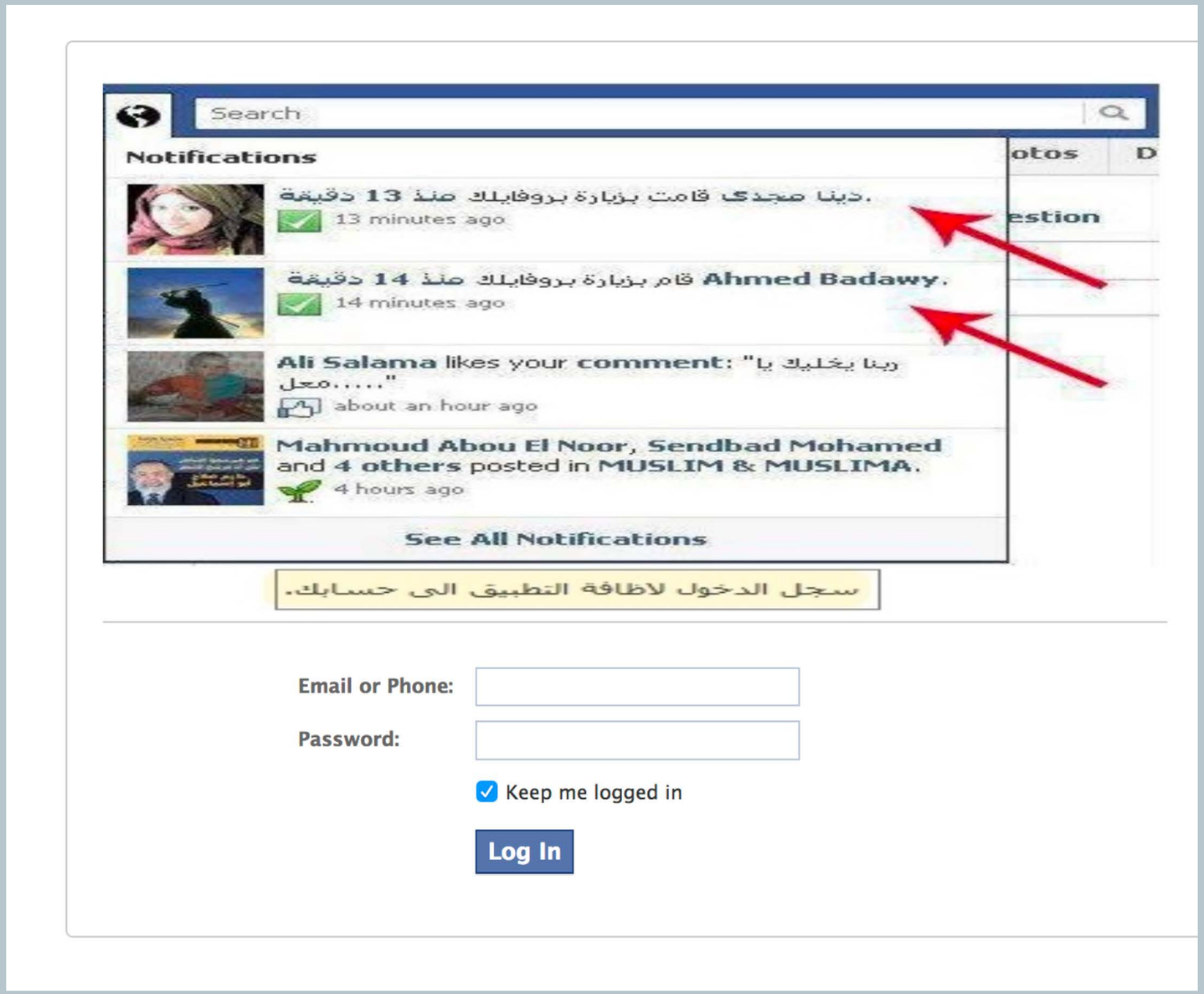
of [redacted]

	Name	Last modified	Size	Description
IR]	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	

[redacted]

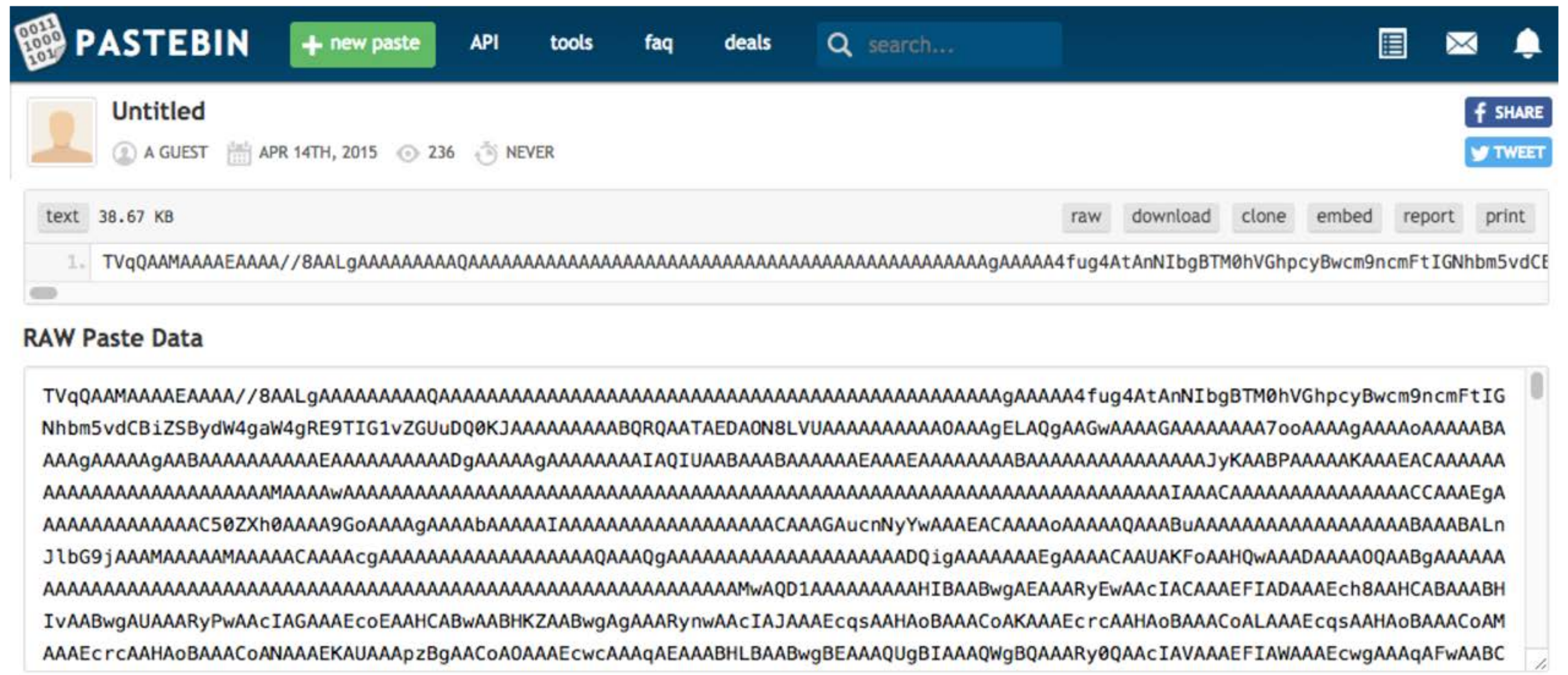

Chose a facebook Color

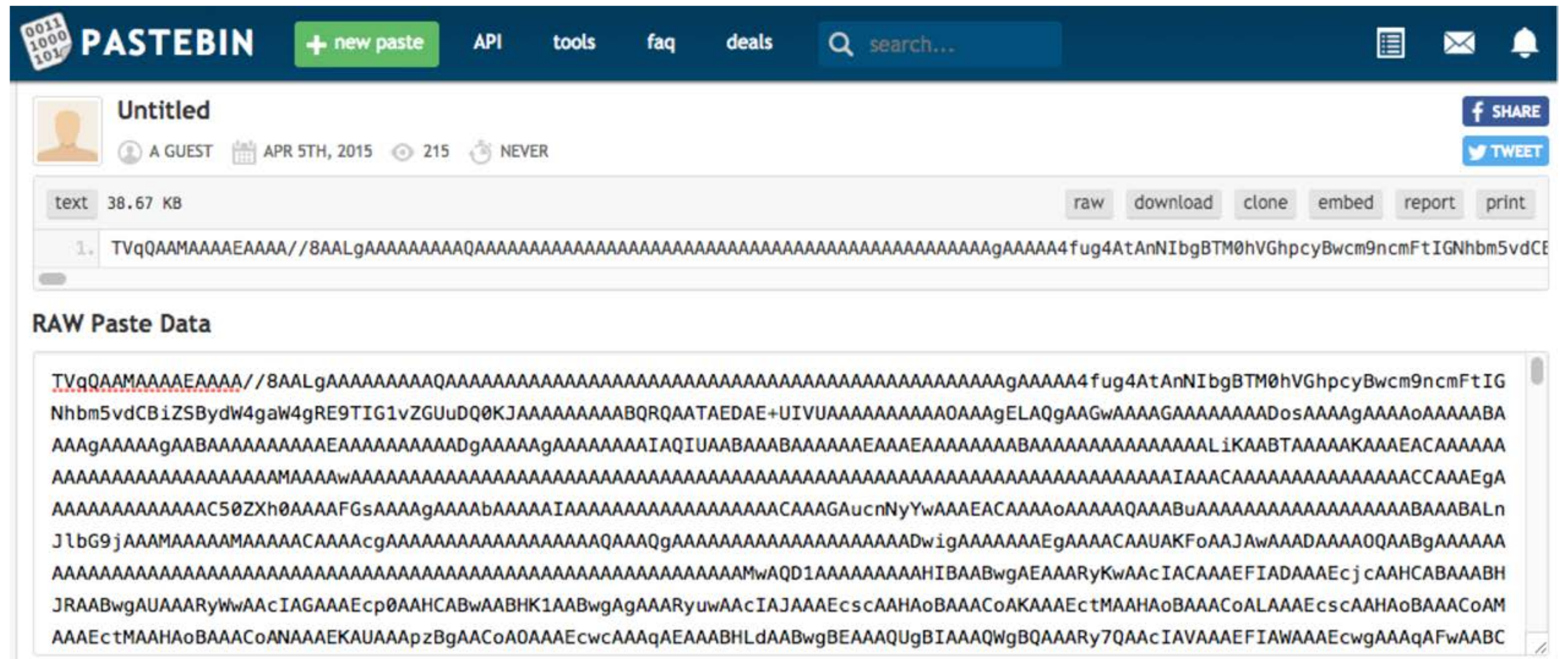

Like
Follow
Share
Create Post
Write a post...
Photo/Video
Tag Friends
Check in
Posts
التجمع الوطني الديمقراطي السوري
Syrian National Democratic Alliance
May 25, 2017
#أول وثيقة يعلن عنها العميد مناف طلاس
النظام الداخلي للجيش السوري الوطني ورئاسة هيئة الأركان العليا
#وثيقة_رقم_1
http://download1480.mediafire.com/
...../%D9%88%D8%AB%D9%8A%D9%8
#First document to be announced by Dean benefits
Rules of procedure of the Syrian National Army and the presidency
التجمع الوطني الديمقراطي السوري
Syrian National Democratic Alliance
Home
Posts
Photos
About
Community

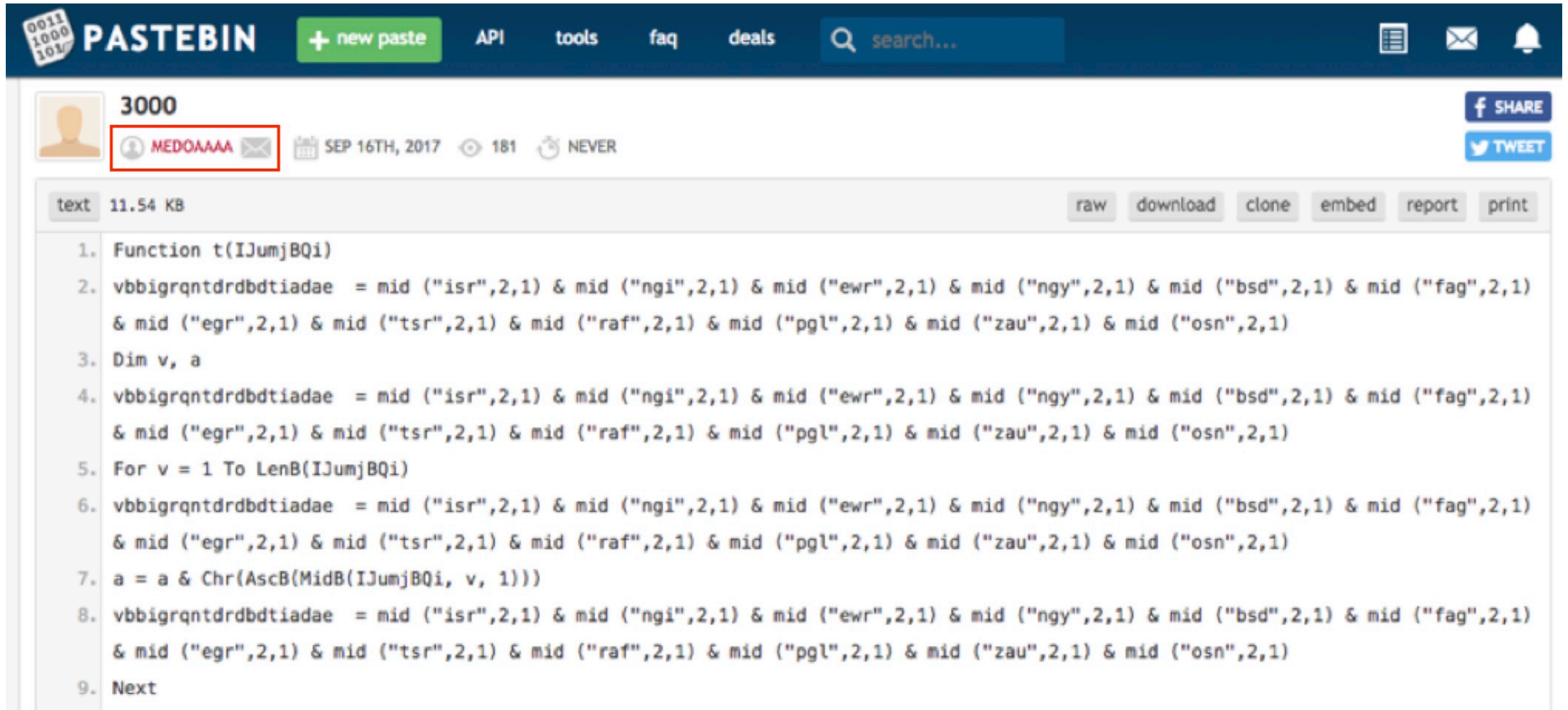

Search
Notifications
دينا محمد قامت بزيارة بروفايلك منذ 13 دقيقة.
13 minutes ago
Ahmed Badawy قام بزيارة بروفايلك منذ 14 دقيقة.
14 minutes ago
Ali Salama likes your comment: "ربنا يخليك يا معل....."
about an hour ago
Mahmoud Abou El Noor, Sendbad Mohamed and 4 others posted in MUSLIM & MUSLIMA.
4 hours ago
See All Notifications
سجل الدخول لاظافة التطبيق الى حسابك.
Email or Phone:
Password:
Keep me logged in
Log In

- 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

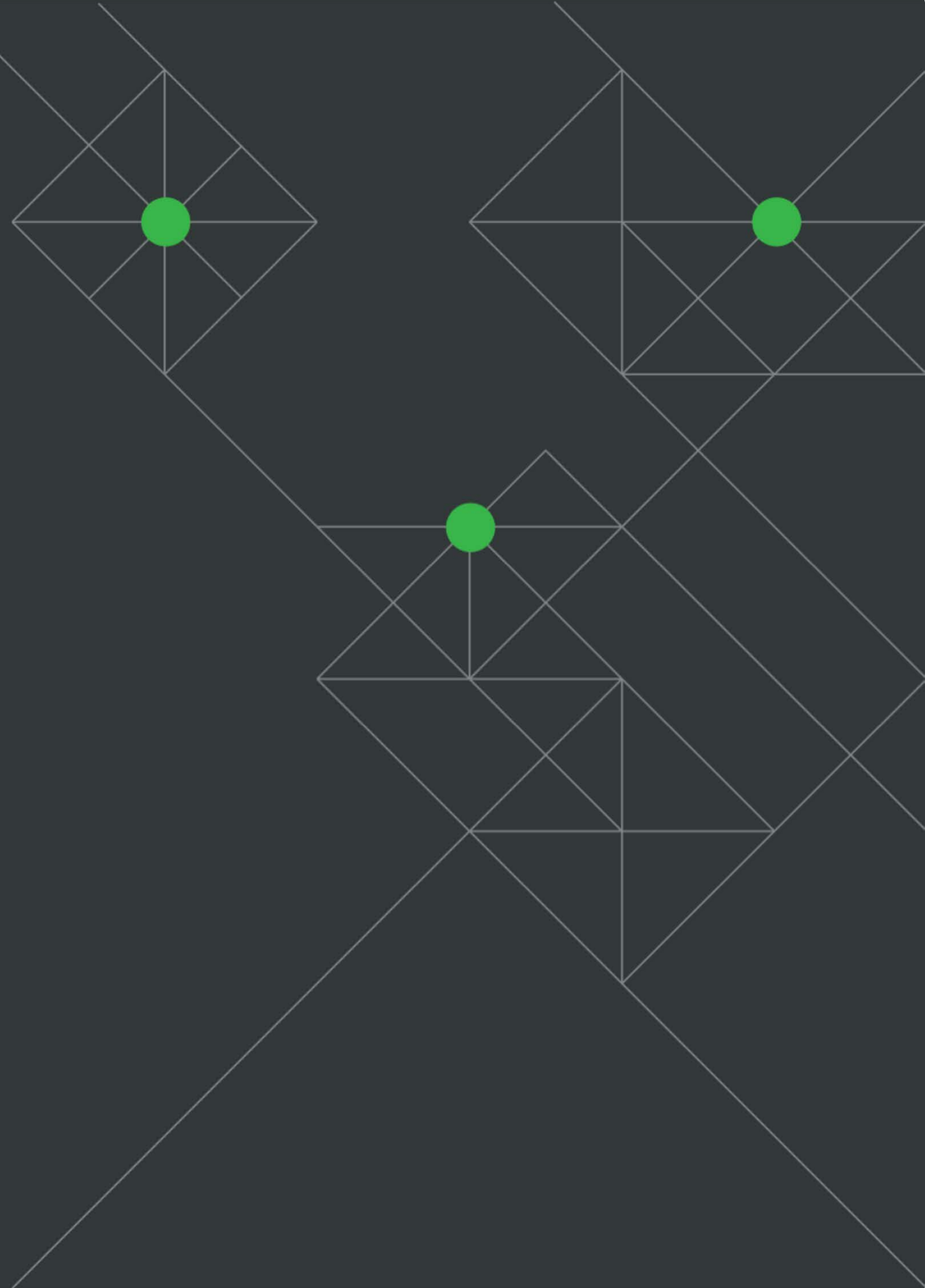
NjRAT
H-Worm Plus
Custom .NET Downloader
DarkComet


PASTEBIN
new paste
API
tools
faq
deals
Untitled
A GUEST
APR 14TH, 2015
236
NEVER
text 38.67 KB
raw
download
clone
embed
report
print
RAW Paste Data


PASTEBIN
new paste
API
tools
faq
deals
Untitled
A GUEST
APR 5TH, 2015
215
NEVER
text 38.67 KB
raw
download
clone
embed
report
print
RAW Paste Data


PASTEBIN
new paste
API
tools
faq
deals
search...
3000
MEDOAAAA
SEP 16TH, 2017
181
NEVER
SHARE
TWEET
text 11.54 KB
raw
download
clone
embed
report
print
Function t(IJumjBQi)
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)
Dim v, a
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)
For v = 1 To LenB(IJumjBQi)
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)
a = a & Chr(AscB(MidB(IJumjBQi, v, 1)))
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)
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

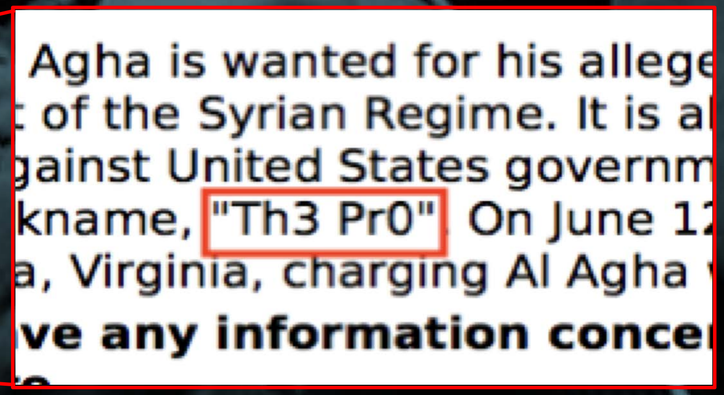
Ahmed Al Agha is wanted for his alleged involvement in the Syrian Electronic Army (SEA), a group of individuals who allegedly commit hacks in support of the Syrian Regime. It is alleged that, between September of 2011 and January of 2014, Al Agha committed dozens of cyber attacks against United States 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



AP The Associated Press
@AP

Following

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

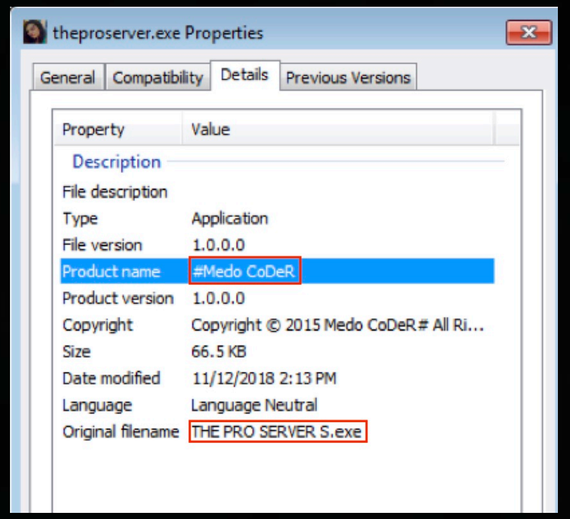
Reply Retweet Favorite More

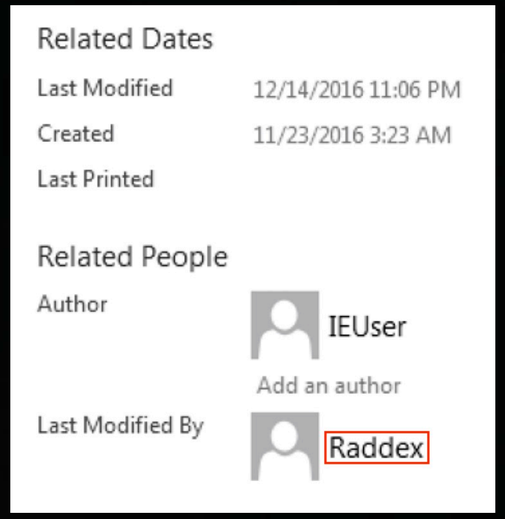
3,063 RETWEETS **144** FAVORITES

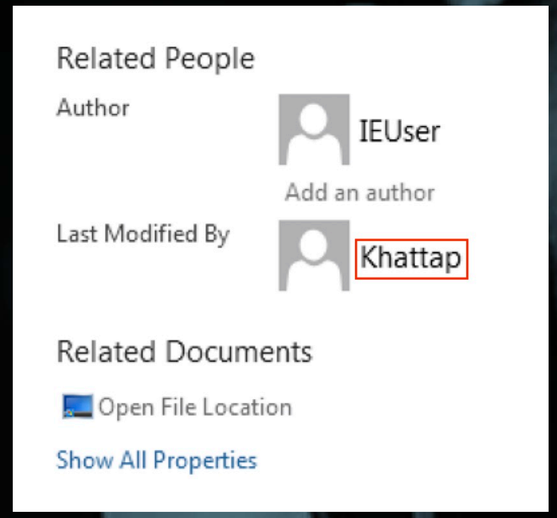
12:07 PM - 23 Apr 13

Connected Personas

Metadata and Logging Statements







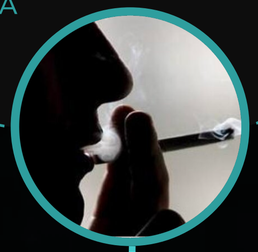

```
    PacketProvider.MyDir = v6.trim().startsWith("/") ? v6.trim() : PacketProvider.MyDir + "/" + v6.trim();
    goto label_40;
}
else {
    v3.writeBytes("cd " + PacketProvider.MyDir + "; " + arg9 + ";" + "\n");
    v3.flush();
    goto label_113;
label_40:
    File v6_1 = new File(PacketProvider.MyDir);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

    PacketProvider.MyDir = PacketProvider.getPWD();
}

bel_113:
```

Allosh Hacker

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

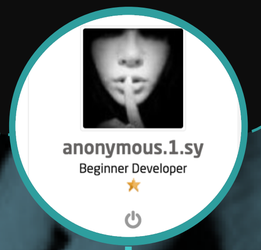


Ahmed Al Agha

- "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

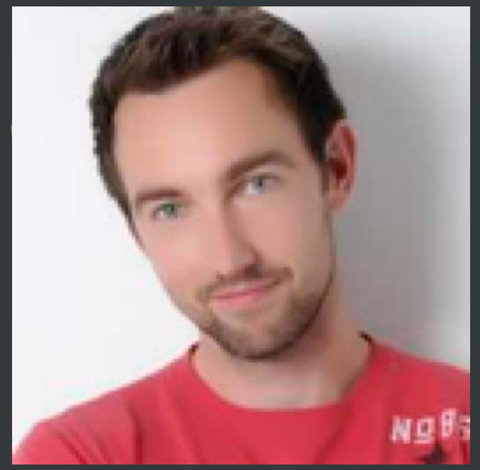
Citizen Lab

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

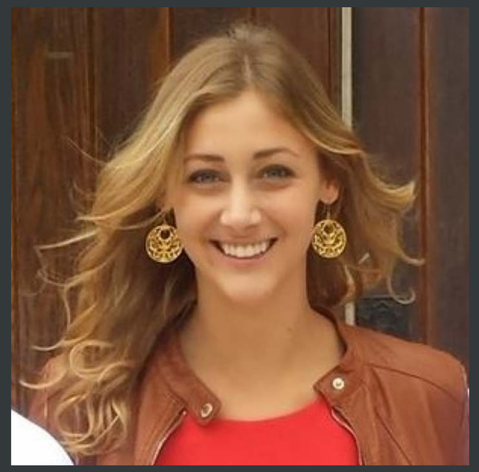
Key Takeaways

- 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.