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
Hacked

The Pro

we are sorry to destroy your sites, but your government's policies and the interference in our internal 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.

PR048 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

Syrian Electronic Army Was Here via @Official_SEA16 #SEA

Tweets

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

Syrian Electronic Army Was Here via @Official_SEA16 #SEA
SilverHawk
Dates Mobile Tooling Packaged

- **SilverHawk**

<table>
<thead>
<tr>
<th>Date</th>
<th># of samples packaged</th>
</tr>
</thead>
<tbody>
<tr>
<td>01-2016</td>
<td></td>
</tr>
<tr>
<td>07-2016</td>
<td></td>
</tr>
<tr>
<td>01-2017</td>
<td></td>
</tr>
<tr>
<td>07-2017</td>
<td></td>
</tr>
<tr>
<td>01-2018</td>
<td></td>
</tr>
<tr>
<td>07-2018</td>
<td></td>
</tr>
</tbody>
</table>
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

```xml
<HmzaPacket>
  <Command></Command>
  <XMLData></XMLData>
  <MSG></MSG>
  <Success></Success>
</HmzaPacket></HAMZA_DELIMITER_STOP>
```

```xml
<HmzaPacket>
  <XMLData>&lt;SysInfo&gt;
    &lt;APK&gt;4.3.&lt;/APK&gt;
    &lt;Android&gt;4.3.&lt;/Android&gt;
    &lt;DeviceName&gt;Unknown AOSP on AVD Emulator&lt;/DeviceName&gt;
    &lt;IMEI&gt;&lt;/IMEI&gt;
    &lt;App&gt;&lt;/App&gt;
    &lt;SimInfo&gt;&lt;/SimInfo&gt;
    &lt;Root&gt;Rooted &lt;/Root&gt;
    &lt;SimId&gt;SIM1&lt;/SimId&gt;
    &lt;State&gt;&lt;/State&gt;
    &lt;Channel&gt;&lt;/Channel&gt;
    &lt;/SysInfo&gt;&lt;/XMLData&gt;
</HmzaPacket>
```
## SilverHawk
### Capabilities and Evolution

<table>
<thead>
<tr>
<th>COMMAND</th>
<th>TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>None</td>
<td>Sends an empty packet to the server and calls TryConnect() which updates all information on the server</td>
</tr>
<tr>
<td>17</td>
<td>XML</td>
<td>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.</td>
</tr>
</tbody>
</table>
| 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  
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 |
| 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      | Both | 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
Attack Vectors
<table>
<thead>
<tr>
<th>[ICO]</th>
<th>Name</th>
<th>Last modified</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[PARENTDIR]</td>
<td>Parent Directory</td>
<td></td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>[DIR]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>04/</td>
<td>2017-09-25 22:52</td>
<td>1.4M</td>
<td>-</td>
</tr>
<tr>
<td>[DIR]</td>
<td>05/</td>
<td>2017-04-09 20:25</td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>[DIR]</td>
<td>06/</td>
<td>2017-05-31 09:16</td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>[DIR]</td>
<td>07/</td>
<td>2017-06-01 11:27</td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>[DIR]</td>
<td>08/</td>
<td>2017-01-02 14:34</td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>[DIR]</td>
<td>09/</td>
<td>2017-08-01 16:31</td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>[DIR]</td>
<td>10/</td>
<td>2017-01-02 18:49</td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>[DIR]</td>
<td></td>
<td>2017-10-01 10:50</td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>[DIR]</td>
<td>ChatSecureLite.apk</td>
<td>2017-09-25 22:52</td>
<td>1.4M</td>
<td>-</td>
</tr>
<tr>
<td>[DIR]</td>
<td>ChatSecurePro.apk</td>
<td>2017-10-16 15:38</td>
<td>1.5M</td>
<td>-</td>
</tr>
<tr>
<td>[DIR]</td>
<td>WiFi Auto 3G.apk</td>
<td>2017-08-19 17:12</td>
<td>1.5M</td>
<td>-</td>
</tr>
<tr>
<td>[DIR]</td>
<td>WordActivation.apk</td>
<td>2017-10-16 15:27</td>
<td>1.4M</td>
<td>-</td>
</tr>
<tr>
<td>[DIR]</td>
<td>kaser-pro.aman.bgl.apk</td>
<td>2016-12-29 22:45</td>
<td>1.5M</td>
<td>-</td>
</tr>
<tr>
<td>[DIR]</td>
<td>skype.exe</td>
<td>2015-11-02 00:47</td>
<td>45M</td>
<td>-</td>
</tr>
<tr>
<td>[DIR]</td>
<td>telegramupdate_2017.apk</td>
<td>2017-10-16 15:41</td>
<td>1.5M</td>
<td>-</td>
</tr>
<tr>
<td>[DIR]</td>
<td>whatsapp_2017.apk</td>
<td>2017-10-26 11:54</td>
<td>1.5M</td>
<td>-</td>
</tr>
<tr>
<td>[DIR]</td>
<td>whatsappupdate_2017.apk</td>
<td>2017-10-16 15:45</td>
<td>1.5M</td>
<td>-</td>
</tr>
<tr>
<td>[DIR]</td>
<td>windows5000.key</td>
<td>2017-09-13 20:46</td>
<td>203K</td>
<td>-</td>
</tr>
<tr>
<td>Name</td>
<td>Last modified</td>
<td>Size</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>--------------</td>
<td>-------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>Parent Directory</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Facebook.apk</td>
<td>2016-01-29 19:56</td>
<td>102K</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firefox.apk</td>
<td>2016-01-29 16:25</td>
<td>35M</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Line.apk</td>
<td>2016-01-29 19:58</td>
<td>102K</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Messenger.apk</td>
<td>2016-01-29 19:58</td>
<td>102K</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Messenger1.apk</td>
<td>2016-01-29 16:29</td>
<td>26M</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Skype.apk</td>
<td>2016-01-29 19:59</td>
<td>102K</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SnapChat.apk</td>
<td>2016-01-29 19:59</td>
<td>102K</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Telegram.apk</td>
<td>2016-01-29 20:00</td>
<td>102K</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Twitter.apk</td>
<td>2016-01-29 20:01</td>
<td>102K</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UCMobile1.apk</td>
<td>2016-01-26 15:09</td>
<td>17M</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Viber.apk</td>
<td>2016-01-29 20:01</td>
<td>102K</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WhatsApp1.apk</td>
<td>2016-01-26 12:43</td>
<td>26M</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WhatsAppPlus.apk</td>
<td>2016-01-29 20:12</td>
<td>102K</td>
<td></td>
<td></td>
</tr>
<tr>
<td>baidu1.apk</td>
<td>2016-01-27 21:19</td>
<td>6.5M</td>
<td></td>
<td></td>
</tr>
<tr>
<td>chrome1.apk</td>
<td>2016-01-26 16:55</td>
<td>39M</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dolphin1.apk</td>
<td>2016-01-27 21:21</td>
<td>7.8M</td>
<td></td>
<td></td>
</tr>
<tr>
<td>facebook1.apk</td>
<td>2016-01-26 12:43</td>
<td>33M</td>
<td></td>
<td></td>
</tr>
<tr>
<td>imo.apk</td>
<td>2016-01-29 19:57</td>
<td>102K</td>
<td></td>
<td></td>
</tr>
<tr>
<td>imo1.apk</td>
<td>2016-01-27 14:09</td>
<td>5.0M</td>
<td></td>
<td></td>
</tr>
<tr>
<td>line1.apk</td>
<td>2016-01-27 14:03</td>
<td>33M</td>
<td></td>
<td></td>
</tr>
<tr>
<td>opera1.apk</td>
<td>2016-01-27 21:24</td>
<td>17M</td>
<td></td>
<td></td>
</tr>
<tr>
<td>skype1.apk</td>
<td>2016-01-27 14:04</td>
<td>36M</td>
<td></td>
<td></td>
</tr>
<tr>
<td>snapchat1.apk</td>
<td>2016-01-26 12:43</td>
<td>33M</td>
<td></td>
<td></td>
</tr>
<tr>
<td>telegram1.apk</td>
<td>2016-01-26 12:43</td>
<td>12M</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Baidu.apk</td>
<td>2016-01-29 20:13</td>
<td>102K</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chrome.apk</td>
<td>2016-01-29 20:14</td>
<td>102K</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dolphin.apk</td>
<td>2016-01-29 20:14</td>
<td>102K</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firefox.apk</td>
<td>2016-01-29 20:15</td>
<td>102K</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Opera.apk</td>
<td>2016-01-29 20:16</td>
<td>102K</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UCMobile.apk</td>
<td>2016-01-29 20:17</td>
<td>102K</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
• 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
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
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
Breaking: Two Explosions in the White House and Barack Obama is injured
Connected Personas

Metadata and Logging Statements

Related Dates
- Last Modified: 12/14/2016 11:06 PM
- Created: 11/23/2016 3:23 AM
- Last Printed:

Related People
- Author: IEUser
- Last Modified By: Khattap

Related Documents
- Open File Location
- Show All Properties

```java

go to label_40;

else {
    v3.writeBytes("cd " + PacketProvider.MyDir + "; " + arg9 + "; " + 
"\n";
v3.flush();
go to 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:
    v4.writeBytes("cd " + PacketProvider.MyDir + "; " + arg9 + "; " + "\n";
v4.flush();
go to label_129;
```
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/

Kaspersky Labs

FireEye

EFF

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

Email: threatintel@lookout.com

Michael Flossman
@terminalrift

Kristin Del Rosso
@kristindelrosso
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.