Nation-state Mobile Malware Targets Syrians with COVID-19 Lures

blog.lookout.com/nation-state-mobile-malware-targets-syrians-with-covid-19-lures

Lookout researchers have uncovered a long-running surveillance campaign tied to Syrian nation-state actors, which recently started using the novel coronavirus as its newest lure to entice its targets to download malware.

This campaign appears to have been active since the start of January 2018, and targets Arabic-speaking users, likely in Syria and the surrounding region. None of these apps were available on the official Google Play Store, suggesting they were likely distributed through actor-operated watering holes or third-party app stores. Lookout previously reported on another surveillanceware campaign using COVID-19 related lures targeting Libya.

Applications from this surveillance campaign impersonate a variety of applications, with titles such as "Covid19", "Telegram Covid_19", "Android Telegram", and "Threema Arabic" (an end-to-end encrypted messaging application), as well as a phone signal booster and OfficeSuite application. Package names also allude to Syrian targeting, with names such as "com.syria.tel", "syria.tel.ctu", and "com.syriatel.ctu".

Syrian connections

Lookout researchers found 71 malicious Android applications connected to the same command-and-control (C2) server. The IP address of the C2 server is located in a block of addresses held by Tarassul Internet Service Provider, an ISP owned by – and sharing network infrastructure with – the Syrian Telecommunications Establishment (STE) (Freedom House, 2018). STE has a history of hosting infrastructure for the Syrian Electronic Army (SEA), a Syrian state-sponsored hacking group. Notably, the C2 servers of SilverHawk, an Android malware family previously reported on by Lookout researchers, were located on IP addresses belonging to STE.

Not all applications in this campaign were completely scrubbed of sensitive information when they were created. A large portion of the malicious applications are SpyNote samples, which store C2 information, along with user inputted names, version numbers, and other information, in res/values/strings.xml. In the strings.xml files of these applications, 22 APKs reference "Allosh", a name previously used in connection with a known Syrian Electronic Army persona.

Previous strings appearing in other malware associated with the Syrian Electronic Army contain this name, such as "c:\users\allosh hacker\documents\visual studio 2012\Projects\allosh\allosh\obj\Debug\Windows.pdb" mentioned in reporting by Citizen Lab on the SEA malicious repackaging of the Psiphon 3 circumvention tool, and "c:\Users\Allosh Hacker\Desktop\Application\obj\Debug\Clean Application.pdb" from pdb paths discovered in binaries associated with SilverHawk infrastructure.

```
<string name="app_name">
  Security Checker</string>
<string name="gp">
  11010</string>
<string name="h">
  [redacted]</string>
<string name="n">
  Allosh</string>
<string name="p">
  215</string>
<string name="ps">
  null</string>
<string name="s">
  Security</string>
<string name="search_menu_title">
  Search</string>
<string name="status_bar_notification_info_overflow">
  999+</string>
<string name="v">
  2.15.26</string>
```

Name	Number of Samples Referenced In
Allosh	22
Hamody	19
Hamodi	3
Ali	1
ali	2

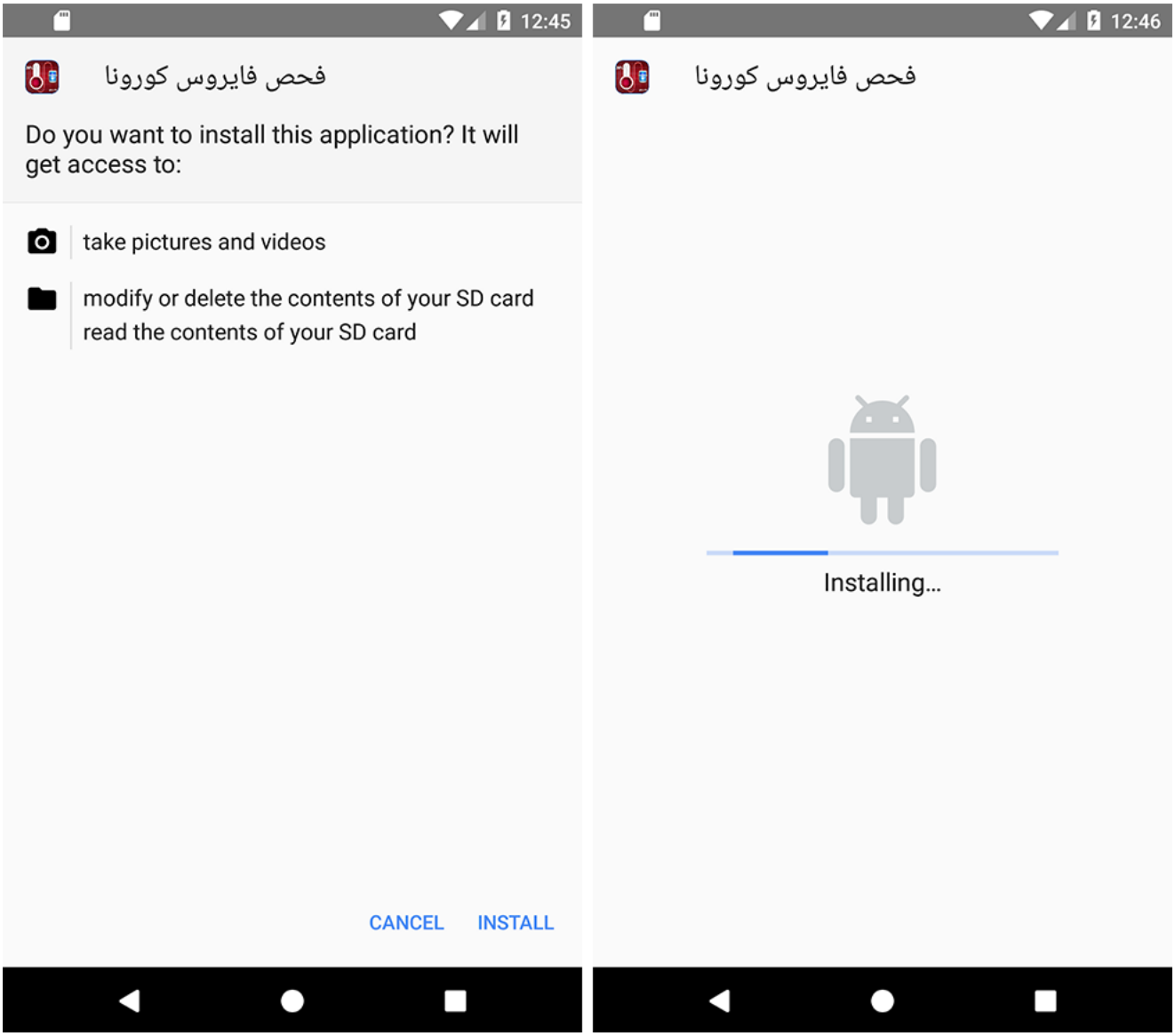
Screenshot of a strings.xml file, and all unique personas discovered in this campaign.

The Syrian Electronic Army has been active recently, with one of their Twitter accounts claiming responsibility this month for DDoS attacks against Belgian media, as well as defacing PayPal and eBay websites as recently as April 7, 2020.

Two of the most recent claims by @Official_SEA7, one of the Syrian Electronic Army's multiple Twitter accounts which has been active since 2013.

Syrian authorities are known to heavily censor their country's internet, with Syria ranking 174th on Reporters Without Borders 2019 World Press Freedom Index. In addition, according to the 2018 Freedom of the Net Report published by Freedom House, an NGO which conducts research and advocacy on democracy, political freedom, and human rights, "In areas controlled by the government, the Syrian Telecommunications Establishment (STE) serves as both an ISP and the telecommunications regulator, providing the government with

tight control over the internet Infrastructure. Furthermore, private fixed-line and mobile ISPs are required to sign a memorandum of understanding to connect to the international internet via gateways controlled by the Syrian Information Organization (SIO)" (Freedom on the Net 2018).



After installation, the original Covid19 application hides its icon and only displays the newly installed Degree Measure application.

The newly installed application (com.finger.body.temperature.ap) is a benign prank - a fake digital thermometer that serves as a decoy. Meanwhile the malware continues to operate in the background.

The user holds down on the screen on the fingerprint and is informed that their body temperature is 35°C.

Some AndoServer samples are purely surveillanceware that do not even pretend to be anything else, while others, like this sample here, contain legitimate applications inside the malware, with the benign APK hidden in the res/raw folder.

AndoServer samples receive commands, and are capable of:

- Taking a screenshot
- Getting battery levels and if the device is plugged in
- Reporting location (latitude and longitude)
- Getting a list of installed applications
- Launching an application specified by the malicious actor
- Checking the number of cameras on a device

- Choosing a specific camera to access

- Creating a specific pop-up message (toast)
- Recording audio
- Creating a file on external storage
- Exfiltrating call logs
- Listing files contained in a specified directory
- Calling a phone number
- Exfiltrating SMS messages
- Sending SMS to a phone number
- Exfiltrating the contact list
- Playing a ringtone and then sleeping

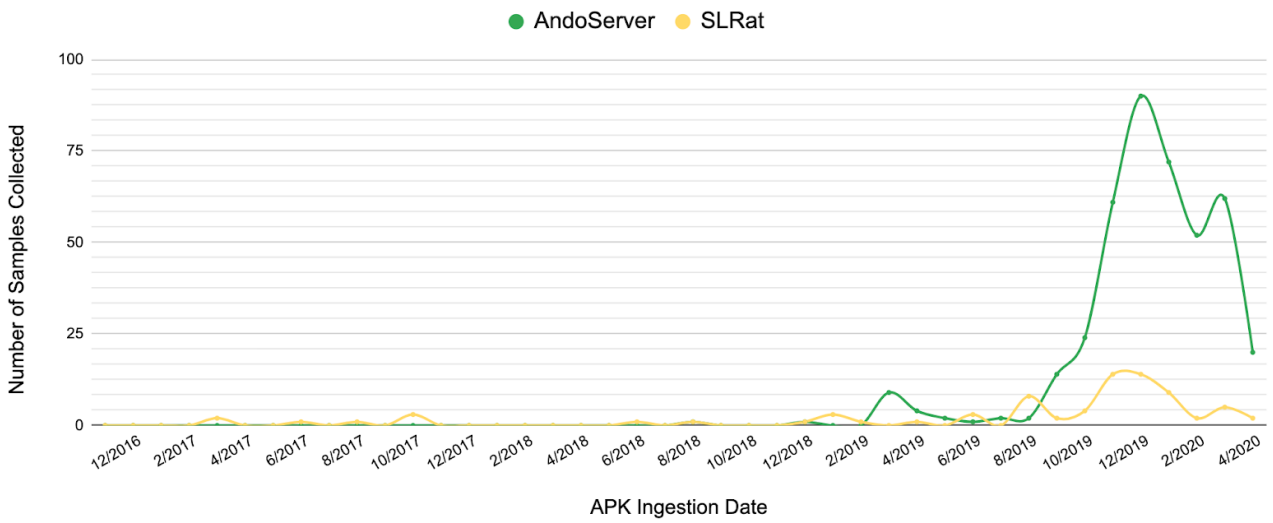
AndoServer malware has its C2 domain or IP address hard coded into the source code. Each sample also has its own unique identifier string at the start of its communication with C2 servers, that appears to be for the actor to monitor which application in their arsenal is responsible for the compromise, as they can see the unique application installed by the specific victim. While not always the case, some unique identifiers are similar to the name of the C2 domain, while other times they refer to the title of the application, highlighting another level of customization of this malware.

Prevalence of commercial surveillanceware

Of the malicious applications in this campaign, 64 of 71 are SpyNote samples, a well known commercial surveillanceware family. The remainder belong to the SandroRat, AndoServer, and SLRat families, of which the latter two have not yet been publicly reported on.

SLRat appears to have gained popularity since its developer first publicized it in May 2016, advertising it as “the Best and Free android remote admin tool”, while AndoServer has not yet been seen for sale or mentioned on public forums. Based on samples ingested to date however, Lookout researchers believe it is also a customizable Android malware that may be for sale, or only known about and used by a smaller group of operators.

Given Syria’s history of censorship and past mobile and desktop surveillance campaigns, it should come as no surprise that another campaign is active. SilverHawk actors initially entered the mobile malware space using the commercial Android surveillanceware AndroRat, before customizing it and then developing their own mobile tooling. It is in line with known TTPs that a new commercial or public spy tool might have been adopted and used by this actor as part of new surveillance efforts, and there are likely more to be discovered.



Lookout has been ingesting samples from the AndoServer and SJRat families since 2016, and has seen a spike in activity towards the end of 2019.

IOCs (SHA1 hashes of the malicious apps):

1aefc2ebaf1a78f23473ce6275b0b514bbcdfb08
213b7f8c3f26a87b116927143289886742b979a1
321682c8395216b6f71ac1f4a1188040bbddfeb4
8cae26c899440f890a8faca2e63ba42c0195cd3b
ccb143b25cedf043a8be46a1f3c3f8a0a3e4c2b2
61ecf4d82246a22dc2d390eca1e20abd6b961083
1e30cc843a32db0296502795781f8064adbceee6
a07370617fa695b047359ac345375d05a7135da0
915e3470e5ab85cb1fe565484b15004a19e88da6
3bfa1b4d98c02c43e7b3af9e536dbcd79e0b9197
d14bb8de94e6f6a733b0962c6d0847376286874f
3c5fd8b163b32cde47dd50c4b61ab087c0cad8d4
4dcc2d9ef4921b3eb4e4dc72dd3716520d558102
07c1edf35c60ea6f2ff02df6e0bfa24abb3029c1
50c607a138e33c8cbdcf2f617f61095b7efa06da
b1a9bc32ece469d7e2d43e894e68cb3bec17ac82
34cb80d4e5d19fcaf724b73aacfebbb19c79337e
c21919c6064c739533878da39d0feaf83e99f586
a62250430da13436b80a62f6a1fee67ed0050e37
246a17230dbe8a5c533231fa1da80d977985b111
358653280acdfd84b6ca326c9b06d12878af69c8
4ec39acfc6f3f9715d0d0e2b0a2f7121d617b605
9f09a4868f61d174ad075e5acaa8d849294dbf69

8952bdf2e3d777d01011e6f8619fca8835e8c434
b9dffff37efbfb8e577ee242c8807db967704a0d
5f6019eae4a16abd11d981b2da5d4ef05115a5c4
0b7cf990bb0dc62dd44d9fa6410ca591dfe47a5d
08162ad39a6237e4eebacf764a5ca6158816a86e
f2fb9826da43f92ff69686f999f205502a33342c
c2e5287433a0e3c7d059494e65b87c3c36f74a47
c7405d85a78a62003494f398084cff8f1794e2ab
16c9ef6ed5af0855a3e6b963ff9c2d65d70de11e
bae5c56d3cd888ec19c42bf5d782de327d012a37
34cc91ad64f52420b6e1531c097ac1602af1f089
00455a4652faf751753b5ebfbb0656bee530f4ef
b263eec151b11d0a6ebcfcf37b3b98458d2d530c
18cc448d71437e7a72558f6680ff10fb234fc64f
6a68f8d962adae7d767b6dfeb2d5b90be412b1f1
0fdc50226a7eb9aee6e6422907425d4531290374
aa43f78a2667909546c3cd993a2940b076634379
5b2e709dfc95e9fc4e4343b92c76cc2193acd49a
e6962b122e14e59c7c88a25d405d6c653b31590e
9c83fdecc8429bc278d03116ca9e2cff5013987e
536539843108459881030 51e7acf4ed336150b99
18451fc0e8fbe878f242e7ee1834091c455f8fc1
0f7bf07352b4d1852f651dda350fd446b3477740
615863ce030f3de3e377352637d6ecc55dfd185a
b46b241620a4d5682e9083ce726827fdbf4a96e5
ab259f11163ea51767a6b17855bc0e79a8ae96e4
447165f88f951f8d26bc721f3047533a54f59ce0
29e04da270da0a6bedfcaee3f6fe8251d6cdef31
6cebf3c27fb348272b72041451b232f78190f83d
e99ebc998ab63026b9b40fff55037c1b69a80369
ddf2b474a0ed1b47278d00872a84d2a2405cc33c
01963c9c70102961cb8b424f623e9be32d7b255b
8d664c9753f7bf65a8cce69dca5486971d1f06ca
2d01b7691ce5647e60c566eda33166bf2e9bcc53
44d8bc4406227aeec9711b74f771c05ddfd3d173
0c04da70ba0771734f99eba05a5676713675d0e8
37e11e1a45f166b16170e8d649c3b75ee93e90a8
dbfbfe43f04c58bcf5daa71df61dcc354bbf2d27
dc3778ffb7399e009a287983f0113e15fd8b227e
1a0a65e6b4a2c42e5dc3d7db2179c04952a03948

69f475024e006b51f7ec6a1990bad460fe9805f0
a32900a79d459da90e49ee8acf23dcfd03bfcb4b
5c8bf130f8e5c7756674a6d376dd7f25fbded4e4

Lookout researchers have uncovered a long-running surveillance campaign tied to Syrian nation-state actors, which recently started using the novel coronavirus as its newest lure to entice its targets to download malware.

This campaign appears to have been active since the start of January 2018, and targets Arabic-speaking users, likely in Syria and the surrounding region. None of these apps were available on the official Google Play Store, suggesting they were likely distributed through actor-operated watering holes or third-party app stores. Lookout previously reported on another surveillanceware campaign using COVID-19 related lures targeting Libya.

Applications from this surveillance campaign impersonate a variety of applications, with titles such as "Covid19", "Telegram Covid_19", "Android Telegram", and "Threema Arabic" (an end-to-end encrypted messaging application), as well as a phone signal booster and OfficeSuite application. Package names also allude to Syrian targeting, with names such as "com.syria.tel", "syria.tel.ctu", and "com.syriatel.ctu".

Syrian connections

Lookout researchers found 71 malicious Android applications connected to the same command-and-control (C2) server. The IP address of the C2 server is located in a block of addresses held by Tarassul Internet Service Provider, an ISP owned by – and sharing network infrastructure with – the Syrian Telecommunications Establishment (STE) (Freedom House, 2018). STE has a history of hosting infrastructure for the Syrian Electronic Army (SEA), a Syrian state-sponsored hacking group. Notably, the C2 servers of SilverHawk, an Android malware family previously reported on by Lookout researchers, were located on IP addresses belonging to STE.

Not all applications in this campaign were completely scrubbed of sensitive information when they were created. A large portion of the malicious applications are SpyNote samples, which store C2 information, along with user inputted names, version numbers, and other information, in res/values/strings.xml. In the strings.xml files of these applications, 22 APKs reference “Allosh”, a name previously used in connection with a known Syrian Electronic Army persona.

Previous strings appearing in other malware associated with the Syrian Electronic Army contain this name, such as “c:\users\allosh hacker\documents\visual studio 2012\Projects\allosh\allosh\obj\Debug\Windows.pdb” mentioned in reporting by Citizen Lab on the SEA malicious repackaging of the Psiphon 3 circumvention tool, and “c:\Users\Allosh Hacker\Desktop\Application\obj\Debug\Clean Application.pdb” from pdb paths discovered in binaries associated with SilverHawk infrastructure.

```
<string name="app_name">
  Security Checker</string>
<string name="gp">
  11010</string>
<string name="h">
  [redacted]</string>
<string name="n">
  Allosh</string>
<string name="p">
  215</string>
<string name="ps">
  null</string>
<string name="s">
  Security</string>
<string name="search_menu_title">
  Search</string>
<string name="status_bar_notification_info_overflow">
  999+</string>
<string name="v">
  2.15.26</string>
```

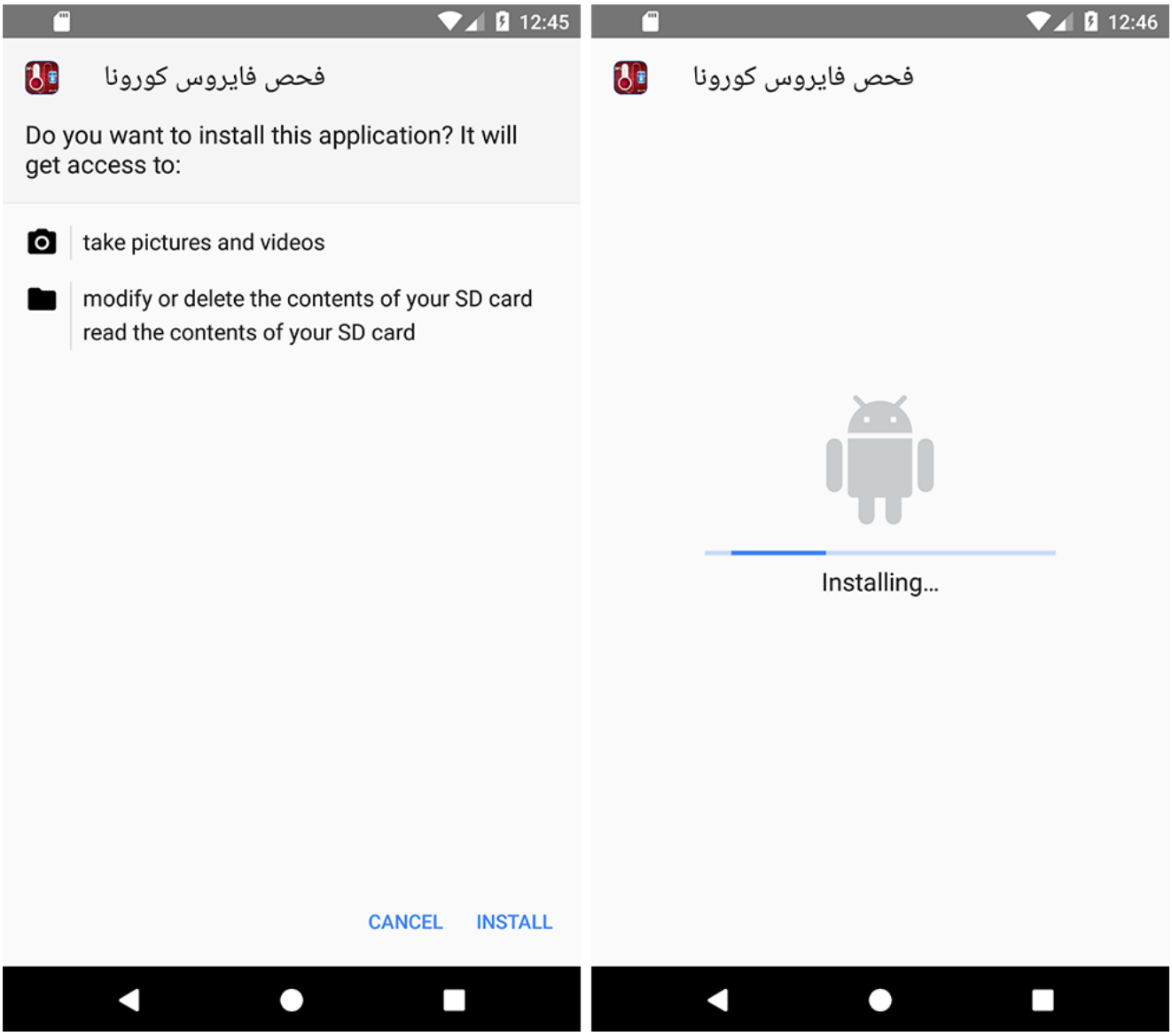
Name	Number of Samples Referenced In
Allosh	22
Hamody	19
Hamodi	3
Ali	1
ali	2

Screenshot of a strings.xml file, and all unique personas discovered in this campaign.

The Syrian Electronic Army has been active recently, with one of their Twitter accounts claiming responsibility this month for DDoS attacks against Belgian media, as well as defacing PayPal and eBay websites as recently as April 7, 2020.

Two of the most recent claims by @Official_SEA7, one of the Syrian Electronic Army's multiple Twitter accounts which has been active since 2013.

Syrian authorities are known to heavily censor their country's internet, with Syria ranking 174th on Reporters Without Borders 2019 World Press Freedom Index. In addition, according to the 2018 Freedom of the Net Report published by Freedom House, an NGO which conducts research and advocacy on democracy, political freedom, and human rights, "In areas controlled by the government, the Syrian Telecommunications Establishment (STE) serves as both an ISP and the telecommunications regulator, providing the government with tight control over the internet Infrastructure. Furthermore, private fixed-line and mobile ISPs are required to sign a memorandum of understanding to connect to the international internet via gateways controlled by the Syrian Information Organization (SIO)" (Freedom on the Net 2018).



After installation, the original Covid19 application hides its icon and only displays the newly installed Degree Measure application.

The newly installed application (com.finger.body.temperature.ap) is a benign prank - a fake digital thermometer that serves as a decoy. Meanwhile the malware continues to operate in the background.

The user holds down on the screen on the fingerprint and is informed that their body temperature is 35°C.

Some AndoServer samples are purely surveillanceware that do not even pretend to be anything else, while others, like this sample here, contain legitimate applications inside the malware, with the benign APK hidden in the res/raw folder.

AndoServer samples receive commands, and are capable of:

- Taking a screenshot
- Getting battery levels and if the device is plugged in
- Reporting location (latitude and longitude)
- Getting a list of installed applications
- Launching an application specified by the malicious actor
- Checking the number of cameras on a device

- Choosing a specific camera to access
- Creating a specific pop-up message (toast)
- Recording audio
- Creating a file on external storage
- Exfiltrating call logs
- Listing files contained in a specified directory
- Calling a phone number
- Exfiltrating SMS messages
- Sending SMS to a phone number
- Exfiltrating the contact list
- Playing a ringtone and then sleeping

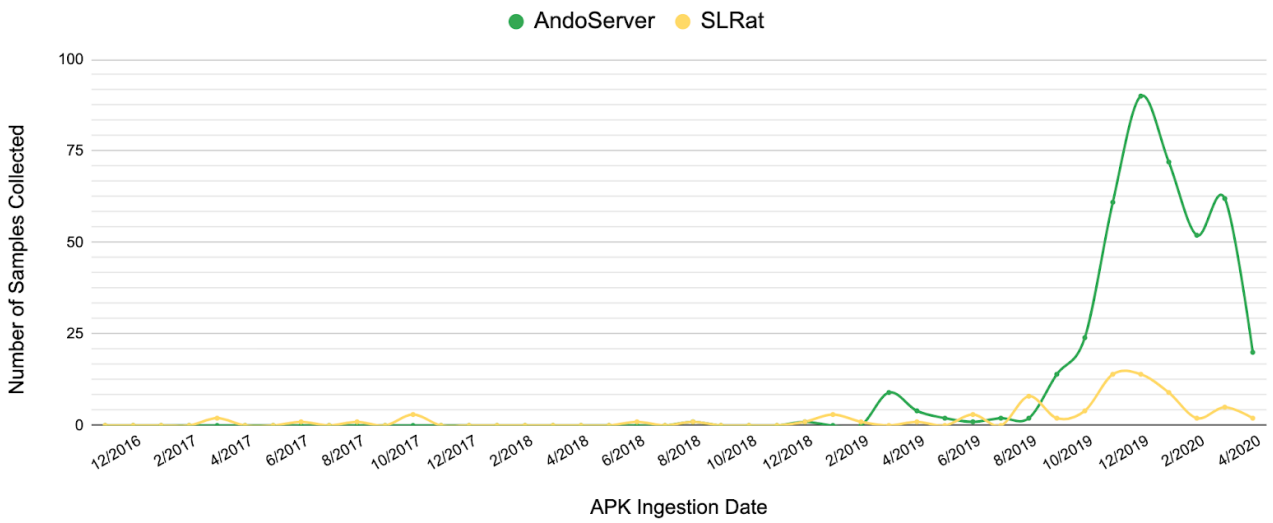
AndoServer malware has its C2 domain or IP address hard coded into the source code. Each sample also has its own unique identifier string at the start of its communication with C2 servers, that appears to be for the actor to monitor which application in their arsenal is responsible for the compromise, as they can see the unique application installed by the specific victim. While not always the case, some unique identifiers are similar to the name of the C2 domain, while other times they refer to the title of the application, highlighting another level of customization of this malware.

Prevalence of commercial surveillanceware

Of the malicious applications in this campaign, 64 of 71 are SpyNote samples, a well known commercial surveillanceware family. The remainder belong to the SandroRat, AndoServer, and SLRat families, of which the latter two have not yet been publicly reported on.

SLRat appears to have gained popularity since its developer first publicized it in May 2016, advertising it as “the Best and Free android remote admin tool”, while AndoServer has not yet been seen for sale or mentioned on public forums. Based on samples ingested to date however, Lookout researchers believe it is also a customizable Android malware that may be for sale, or only known about and used by a smaller group of operators.

Given Syria’s history of censorship and past mobile and desktop surveillance campaigns, it should come as no surprise that another campaign is active. SilverHawk actors initially entered the mobile malware space using the commercial Android surveillanceware AndroRat, before customizing it and then developing their own mobile tooling. It is in line with known TTPs that a new commercial or public spy tool might have been adopted and used by this actor as part of new surveillance efforts, and there are likely more to be discovered.



Lookout has been ingesting samples from the AndoServer and SJRat families since 2016, and has seen a spike in activity towards the end of 2019.

IOCs (SHA1 hashes of the malicious apps):

1aefc2ebaf1a78f23473ce6275b0b514bbcdfb08
213b7f8c3f26a87b116927143289886742b979a1
321682c8395216b6f71ac1f4a1188040bbddfeb4
8cae26c899440f890a8faca2e63ba42c0195cd3b
ccb143b25cedf043a8be46a1f3c3f8a0a3e4c2b2
61ecf4d82246a22dc2d390eca1e20abd6b961083
1e30cc843a32db0296502795781f8064adbceee6
a07370617fa695b047359ac345375d05a7135da0
915e3470e5ab85cb1fe565484b15004a19e88da6
3bfa1b4d98c02c43e7b3af9e536dbcd79e0b9197
d14bb8de94e6f6a733b0962c6d0847376286874f
3c5fd8b163b32cde47dd50c4b61ab087c0cad8d4
4dcc2d9ef4921b3eb4e4dc72dd3716520d558102
07c1edf35c60ea6f2ff02df6e0bfa24abb3029c1
50c607a138e33c8cbdcf2f617f61095b7efa06da
b1a9bc32ece469d7e2d43e894e68cb3bec17ac82
34cb80d4e5d19fcaf724b73aacfebbb19c79337e
c21919c6064c739533878da39d0feaf83e99f586
a62250430da13436b80a62f6a1fee67ed0050e37
246a17230dbe8a5c533231fa1da80d977985b111
358653280acdfd84b6ca326c9b06d12878af69c8
4ec39acfc6f3f9715d0d0e2b0a2f7121d617b605
9f09a4868f61d174ad075e5acaa8d849294dbf69

8952bdf2e3d777d01011e6f8619fca8835e8c434
b9dffff37efbfb8e577ee242c8807db967704a0d
5f6019eae4a16abd11d981b2da5d4ef05115a5c4
0b7cf990bb0dc62dd44d9fa6410ca591dfe47a5d
08162ad39a6237e4eebacf764a5ca6158816a86e
f2fb9826da43f92ff69686f999f205502a33342c
c2e5287433a0e3c7d059494e65b87c3c36f74a47
c7405d85a78a62003494f398084cff8f1794e2ab
16c9ef6ed5af0855a3e6b963ff9c2d65d70de11e
bae5c56d3cd888ec19c42bf5d782de327d012a37
34cc91ad64f52420b6e1531c097ac1602af1f089
00455a4652faf751753b5ebfbb0656bee530f4ef
b263eec151b11d0a6ebcfcf37b3b98458d2d530c
18cc448d71437e7a72558f6680ff10fb234fc64f
6a68f8d962adae7d767b6dfeb2d5b90be412b1f1
0fdc50226a7eb9aee6e6422907425d4531290374
aa43f78a2667909546c3cd993a2940b076634379
5b2e709dfc95e9fc4e4343b92c76cc2193acd49a
e6962b122e14e59c7c88a25d405d6c653b31590e
9c83fdecc8429bc278d03116ca9e2cff5013987e
536539843108459881030 51e7acf4ed336150b99
18451fc0e8fbe878f242e7ee1834091c455f8fc1
0f7bf07352b4d1852f651dda350fd446b3477740
615863ce030f3de3e377352637d6ecc55dfd185a
b46b241620a4d5682e9083ce726827fdbf4a96e5
ab259f11163ea51767a6b17855bc0e79a8ae96e4
447165f88f951f8d26bc721f3047533a54f59ce0
29e04da270da0a6bedfcaee3f6fe8251d6cdef31
6cebf3c27fb348272b72041451b232f78190f83d
e99ebc998ab63026b9b40fff55037c1b69a80369
ddf2b474a0ed1b47278d00872a84d2a2405cc33c
01963c9c70102961cb8b424f623e9be32d7b255b
8d664c9753f7bf65a8cce69dca5486971d1f06ca
2d01b7691ce5647e60c566eda33166bf2e9bcc53
44d8bc4406227aeec9711b74f771c05ddfd3d173
0c04da70ba0771734f99eba05a5676713675d0e8
37e11e1a45f166b16170e8d649c3b75ee93e90a8
dbfbfe43f04c58bcf5daa71df61dcc354bbf2d27
dc3778ffb7399e009a287983f0113e15fd8b227e
1a0a65e6b4a2c42e5dc3d7db2179c04952a03948

69f475024e006b51f7ec6a1990bad460fe9805f0
a32900a79d459da90e49ee8acf23dcfd03bfcb4b
5c8bf130f8e5c7756674a6d376dd7f25fbded4e4

April 15, 2020

Download Case Study
{{consumer="/components/cta/consumer"}}

TAGS:

|

Threat Intelligence