The Desert Falcons targeted attacks

SL securelist.com/blog/research/68817/the-desert-falcons-targeted-attacks/

Authors

- Expert Ghareeb Saad
- Mohamad Amin Hasbini

Download Full Report PDF

The Desert Falcons are a new group of Cyber Mercenaries operating in the Middle East and carrying out Cyber Espionage across that region. The group uses an arsenal of homemade malware tools and techniques to execute and conceal its campaigns on PC and Mobile OS.

> #FalconsAPT is the 1st known campaign to be fully developed by Arabic #hackers to target the Middle East #TheSAS2015
>
> Tweet

The first Desert Falcons operations were seen in 2011 and the group made its first infections in 2013. By the end of 2014 and beginning of 2015 the group was very active.

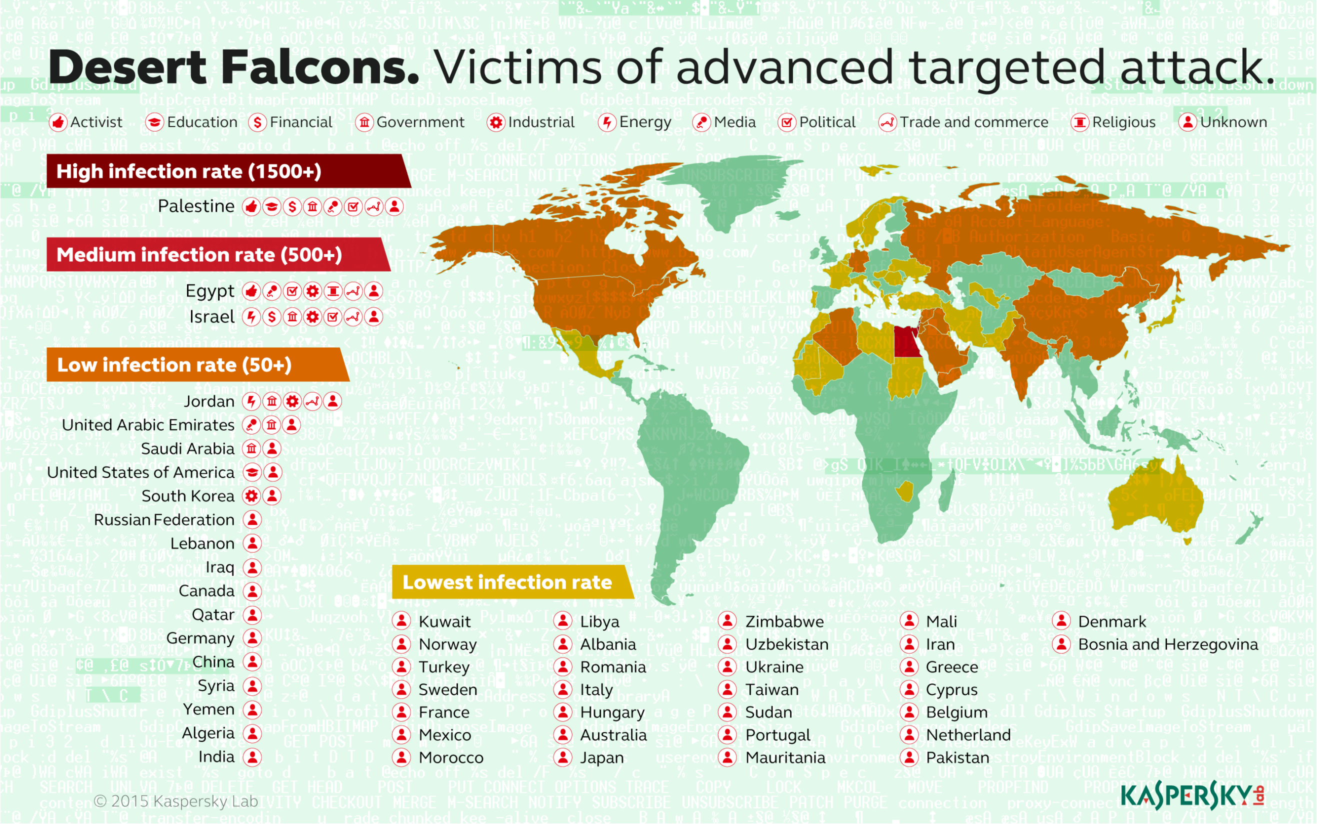
Full report

The full report can be found here.

FAQ

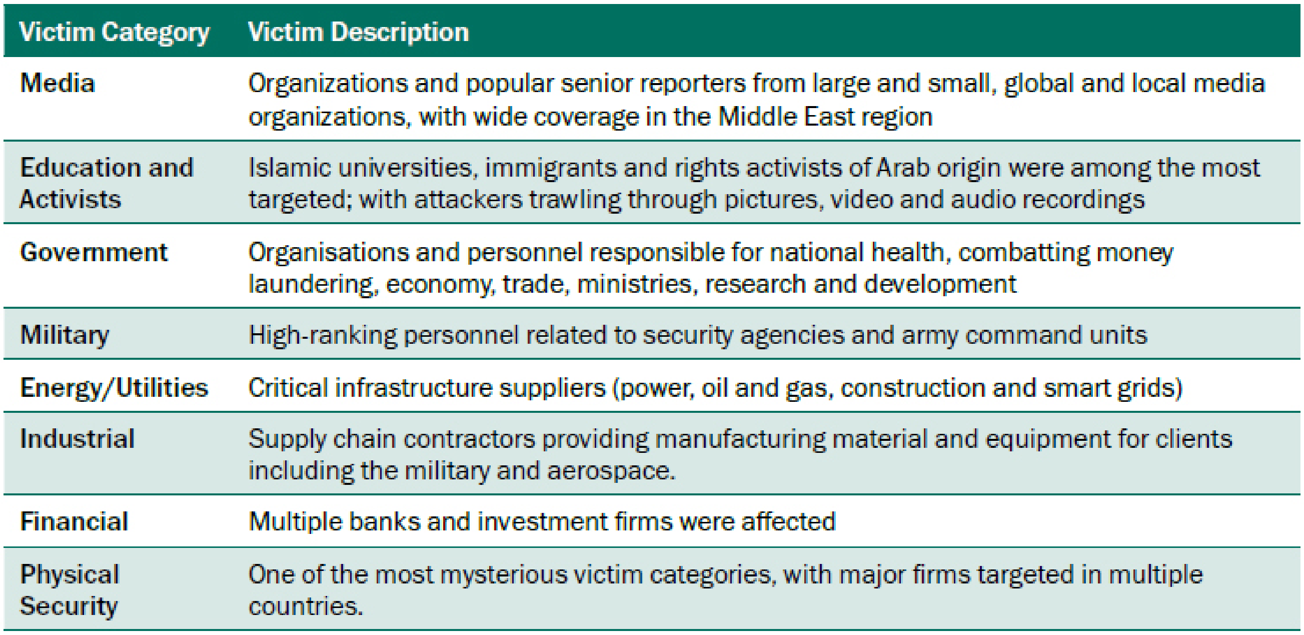
Where are the Victims Located?

There are more than 3,000 victims in 50+ countries. Most of them are found in Palestine, Egypt, Israel and Jordan, but others have been discovered in Saudi Arabia, the UAE, the US, South Korea, Morocco, Qatar and others.



Who are the Victims?

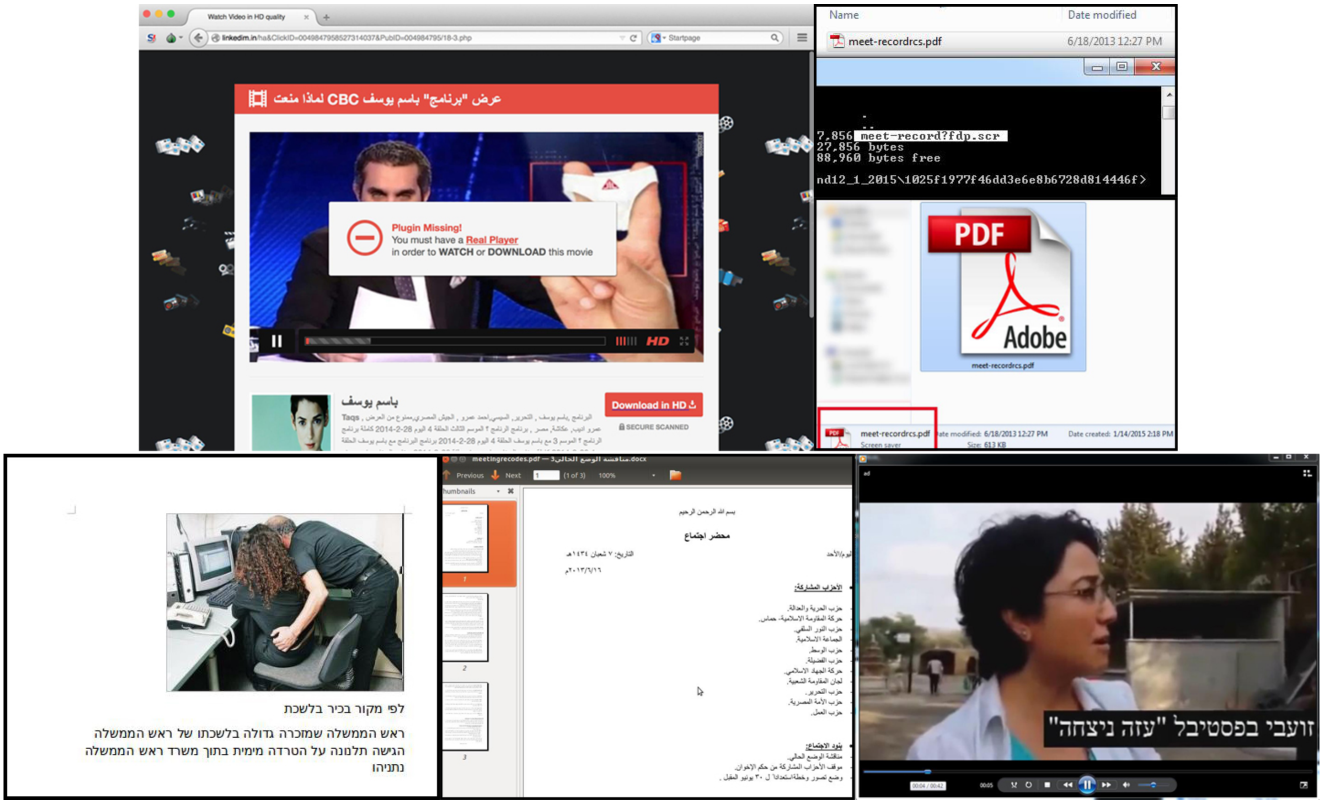
The attacks targeted several classes of victim, including Military and Government organizations, employees responsible for health organizations, combating money laundering, economic and financial institutions, leading media entities, research and educational institutions, energy and utilities providers, activists and political leaders, physical security companies and other targets that have access to important geopolitical information.



Victim Category	Victim Description
Media	Organizations and popular senior reporters from large and small, global and local media organizations, with wide coverage in the Middle East region
Education and Activists	Islamic universities, immigrants and rights activists of Arab origin were among the most targeted; with attackers trawling through pictures, video and audio recordings
Government	Organisations and personnel responsible for national health, combatting money laundering, economy, trade, ministries, research and development
Military	High-ranking personnel related to security agencies and army command units
Energy/Utilities	Critical infrastructure suppliers (power, oil and gas, construction and smart grids)
Industrial	Supply chain contractors providing manufacturing material and equipment for clients including the military and aerospace.
Financial	Multiple banks and investment firms were affected
Physical Security	One of the most mysterious victim categories, with major firms targeted in multiple countries.

How are the victims infected?

Malware writers use a variety of technical and social engineering methods to deliver their files and encourage victims to run them, creating an effective infection vector. Examples include a fake website that promises to publish censored political information and asks users to download a plugin to view a video (the plugin contains the malware). Another example involves the use of spear phishing emails or social network messages to deliver malicious files using an extension override (e.g. malicious files ending with **.fdp.scr** would appear **.rcs.pdf**).


Watch Video in HD quality
عرض "برنامج" باسم يوسف CBC لماذا منعت
Plugin Missing!
You must have a Real Player
in order to WATCH or DOWNLOAD this movie
HD
باسم يوسف
Download in HD
SECURE SCANNED
Name
Date modified
meet-recordrcs.pdf
6/18/2013 12:27 PM
PDF
Adobe
meet-recordrcs.pdf
Screen saver
Date modified: 6/18/2013 12:27 PM
Size: 613 KB
Date created: 1/14/2015 2:18 PM
meetingrecodes.pdf — مناقشة الوضع الحالي3.docx
Previous
Next
(1 of 3)
100%
Thumbnails

```
7,856 meet-record?fdp.scr
27,856 bytes
88,960 bytes free

nd12_1_2015\1025f1977f46dd3e6e8b6728d814446f>
```

לפי מקור בכיר בלשכת

ראש הממשלה שמזכרה גדולה בלשכתו של ראש הממשלה
הגישה תלונה על הטרדה מימית בתוך משרד ראש הממשלה
נתניהו

بسم الله الرحمن الرحيم

محضر اجتماع

اليوم/الأحد
التاريخ: ٧ شعبان ١٤٣٤هـ
٢٠١٣/٦/١٦م

- الأحزاب المشاركة:
  - حزب الحرية والعدالة.
  - حركة المقاومة الاسلامية- حماس.
  - حزب النور السلفي.
  - الجماعة الاسلامية.
  - حزب الوسط.
  - حزب الفضيلة.
  - حركة الجهاد الاسلامي.
  - لجان المقاومة الشعبية.
  - حزب التحرير.
  - حزب الأمة المصرية.
  - حزب العمل.
- بنود الاجتماع:
  - مناقشة الوضع الحالي.
  - موقف الأحزاب المشاركة من حكم الإخوان.
  - وضع تصور وخطة استعدادا ل ٣٠ يونيو المقبل .

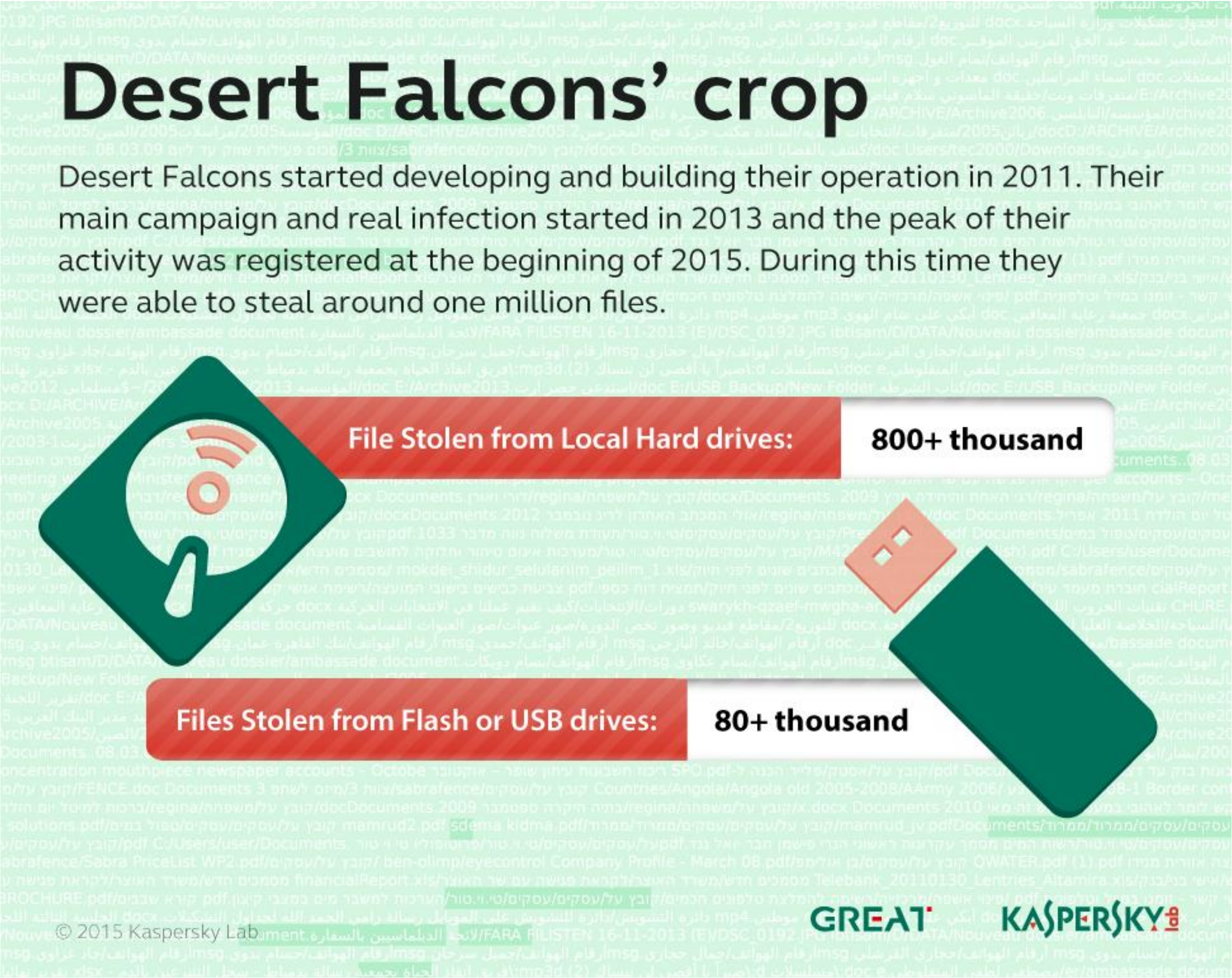
זועבי בפסטיבל "עזה ניצחה"

Sample of documents and videos used in spear phishing

What are the goals of the operations?

The attackers are looking for sensitive intelligence information that could help them in further operations or even extortion. The victims are targeted for the secrets in their possession or intelligence information relating to their positions in governments or important organizations.

More than 1 million files were stolen from victims. Stolen files include diplomatic communications from embassies, military plans and documents, financial documents, VIP and Media contact lists and files.



Desert Falcons’ crop

Desert Falcons started developing and building their operation in 2011. Their main campaign and real infection started in 2013 and the peak of their activity was registered at the beginning of 2015. During this time they were able to steal around one million files.

File Stolen from Local Hard drives: 800+ thousand

Files Stolen from Flash or USB drives: 80+ thousand

Who are the attackers and what do we know about them?

The Desert Falcons operators are native Arabic speakers. There are about 30 of them working in three teams. Some of their identities are already known. The attackers are running three campaigns to target different types of victim.

Where are the attackers based?

The attackers are based in Palestine, Egypt and Turkey.

Which malware do they use to infect their victims?

There are three main backdoors used to infect victim devices:

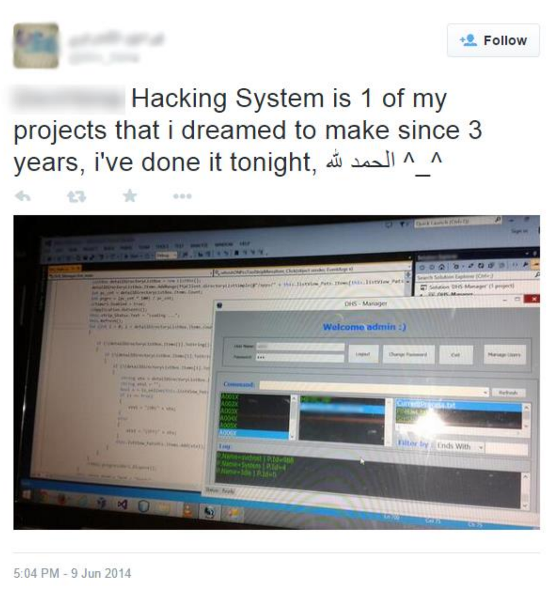
Computer backdoors

- The Main Falcons Trojan
- The DHS* Spyware Trojan

Computer Backdoors give the attackers full scope to use keyloggers and screenshotters, access files and even make audio recordings. DHS naming is used by the attackers to describe the nickname initials of one of the developers (D** H*** Spyware).

Mobile Backdoor

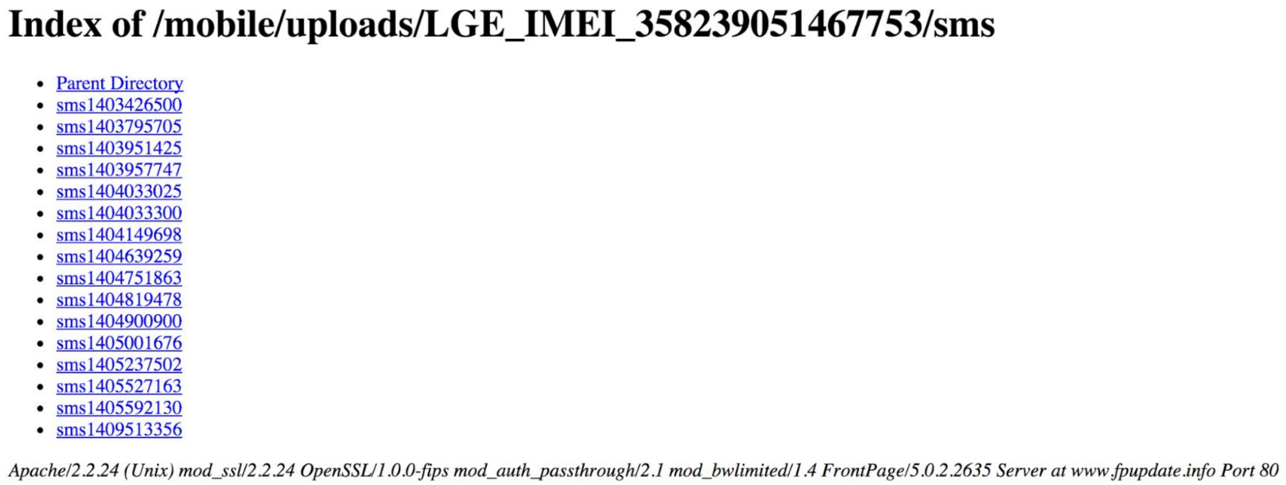
- A mobile backdoor targeting Android devices.
- Mobile Backdoors give attackers access to Call and SMS logs



[redacted]

[redacted] Hacking System is 1 of my projects that i dreamed to make since 3 years, i've done it tonight, الحمد لله ^_^

5:04 PM - 9 Jun 2014



Index of /mobile/uploads/LGE_IMEI_358239051467753/sms

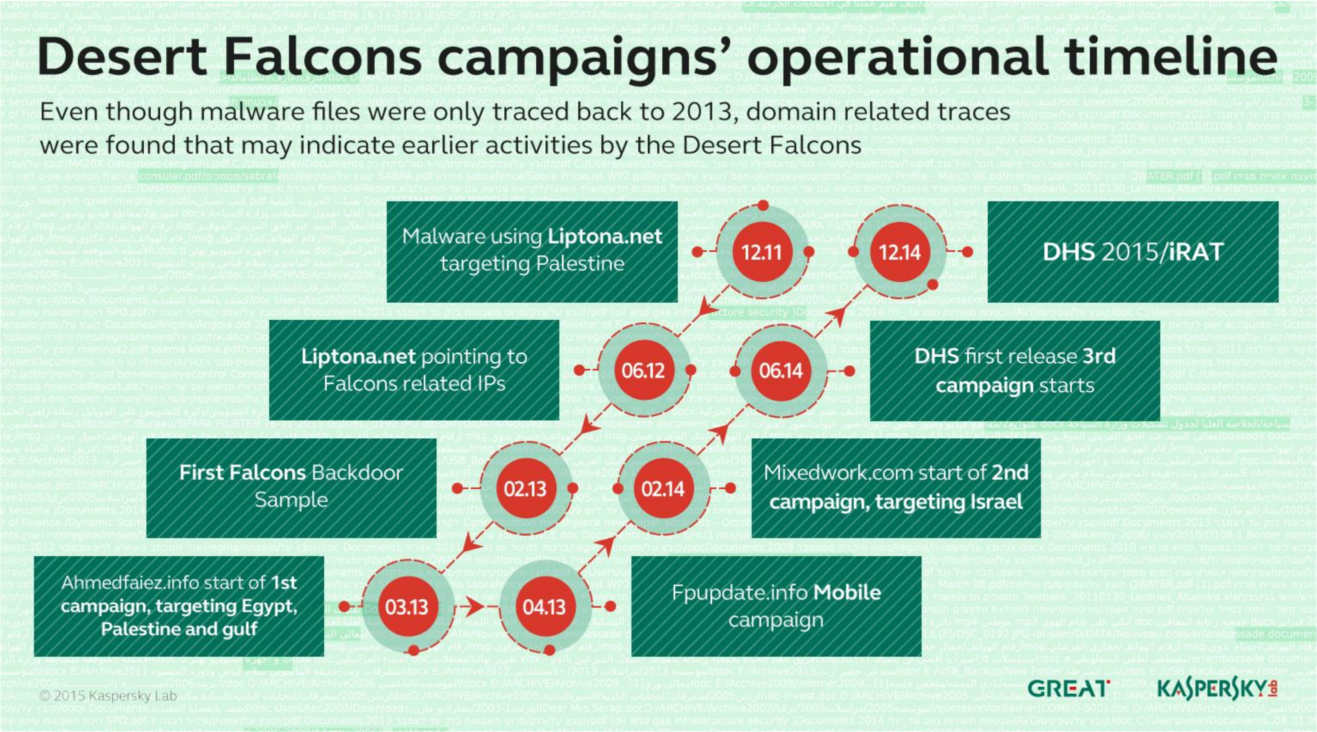
- Parent Directory
- sms1403426500
- sms1403795705
- sms1403951425
- sms1403957747
- sms1404033025
- sms1404033300
- sms1404149698
- sms1404639259
- sms1404751863
- sms1404819478
- sms1404900900
- sms1405001676
- sms1405237502
- sms1405527163
- sms1405592130
- sms1409513356

Apache/2.2.24 (Unix) mod_ssl/2.2.24 OpenSSL/1.0.0-fips mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 Server at www.fpupdate.info Port 80

How did you become aware of this threat? Who reported it?

We became aware of the threat during an incident investigation in the Middle East.

Is it still active?



Desert Falcons 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

Malware using Liptona.net targeting Palestine
12.11
12.14
DHS 2015/iRAT
Liptona.net pointing to Falcons related IPs
06.12
06.14
DHS first release 3rd campaign starts
First Falcons Backdoor Sample
02.13
02.14
Mixedwork.com start of 2nd campaign, targeting Israel
Ahmedfaiez.info start of 1st campaign, targeting Egypt, Palestine and gulf
03.13
04.13
Fpupdate.info Mobile campaign
© 2015 Kaspersky Lab
GREAT
KASPERSKY lab

The operation is very active and is currently in peak condition. We are continuously identifying new samples and victims for all related campaigns.

How is this different from any other Cyber espionage attacks?

Desert Falcons are the first known Cyber espionage attacks to be fully developed and operated by Arabic speakers to target the Middle East. It has affected a stunning range of victims, stealing more than 1 million special files.

Is this a nation-state sponsored attack?

The profiles of the targeted victims and the apparent political motives behind the attacks make it possible that Desert Falcons operations could be nation state sponsored. At present, though, this cannot be confirmed.

Why this name?

The falcon is a rare bird that has been highly prized for a centuries in desert countries in the Arab world. It is a symbol of hunting and sharp vision. The Desert Falcons are proficient cyberhunters with carefully chosen targets, all of whom are thoroughly investigated before the attack and closely watched after being infected.

How can users protect themselves?

Kaspersky Lab products detect and block all variants of the malware used in this campaign:

- 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

The Desert Falcons targeted attacks
