北非狐（APT-C-44）攻击活动揭露 - 360 核心安全技术博客

blogs.360.cn/post/APT-C-44.html

10月23, 2020

北非狐（APT-C-44）攻击活动揭露

主要发现

近期，360烽火实验室联合360高级威胁研究院发现一起针对阿拉伯语地区的长达三年的多次网络攻击活动。该攻击活动自2017年10月开始至今，攻击平台主要为Windows和Android。通过分析，我们发现此次攻击活动来自阿尔及利亚，主要利用钓鱼网站和第三方文件托管网站进行载荷投递，并且使用社交媒体进行传播，受害者主要分布在阿拉伯语地区，其中包含疑似具有军事背景的相关人员。根据此次攻击活动的伪装对象和攻击目标，我们认为该组织目的是为了获取情报先机。根据该组织所属国家的地理位置以及其他特点，我们将其命名为北非狐（APT-C-44）。

载荷投递

北非狐组织载荷投递方式主要为钓鱼网站和第三方文件托管网站，并且在不同的时间段使用了不同的载荷投递方式，我们将该组织的在载荷投递方式分为三个阶段。

第一阶段时间为2017年11月-2018年10月，使用钓鱼网站进行载荷投递。

第二阶段时间为2019年5月-2019年10月，使用第三方文件托管网站进行载荷投递。

第三阶段时间为2019年10月至今，使用钓鱼网站和第三方文件托管网站进行载荷投递。

攻击行动	活跃时间	载荷投递方式	载荷投递网站
第一次	2017.11-2018.10	钓鱼网站	http://egchaat[.]com
第二次	2019.5-2019.10	第三方文件托管网站	https://top4top[.]io/downloadf-12180r3ix1-apk.html
第三次	2019.10-至今	钓鱼网站 第三方文件托管网站	http://www.moltqana[.]com https://top4top[.]io/downloadf-12180r3ix1-apk.html

图1 载荷投递方式

钓鱼网站

EgChat是一款在阿拉伯地区比较流行聊天室程序，可以运行在Windows和Android平台上。EgChat官网（egchat[.]com）宣称可以提供安全，可靠且易于使用的网络会议室，并且具有出色的语音质量，快速的视频流以及对聊天室的完全控制。在其官网可以下载window版本或者通过GooglePlay下载Android版本。

2017年底，北非狐组织制作了一个仿冒EgChat官网的钓鱼网站（egchaat[.]com）进行载荷投递，钓鱼网站同样提供了Window平台和Android平台应用下载链接，但实际下载的应用为该组织进行攻击的RAT工具。钓鱼网站界面与官方网站只有极少的差异，即钓鱼网站将EgChat写成了EgChaat，如下图。

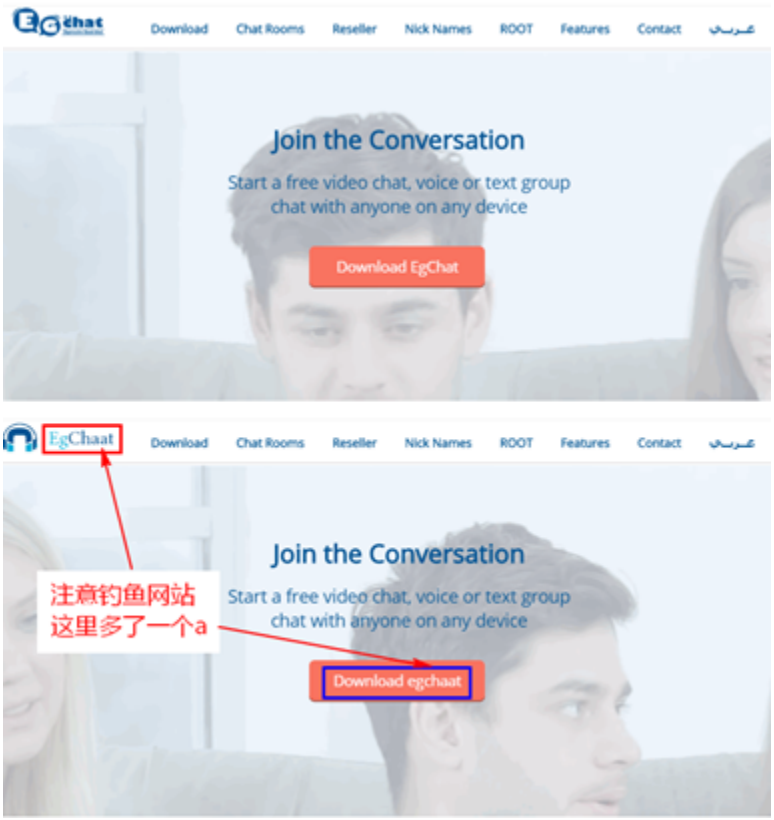

图2 EgChat官网（上）和钓鱼网站（下）

2018年6月，EgChat开发者停止了对EgChat的更新，转而开发了一款新的聊天室程序Mltqana用以替代EgChat，其官网地址（www.mltqana[.]com）也发生了变化。 2019年10月，北非狐组织再次制作了一个钓鱼网站（www.moltqana[.]com）进行载荷投递，该钓鱼网站仿造了Mltqana官网（见图2）。值得注意的是钓鱼网站页面不支持英语，只支持阿拉伯语，从侧面也说明了其针对目标群体分布在阿拉伯地区。

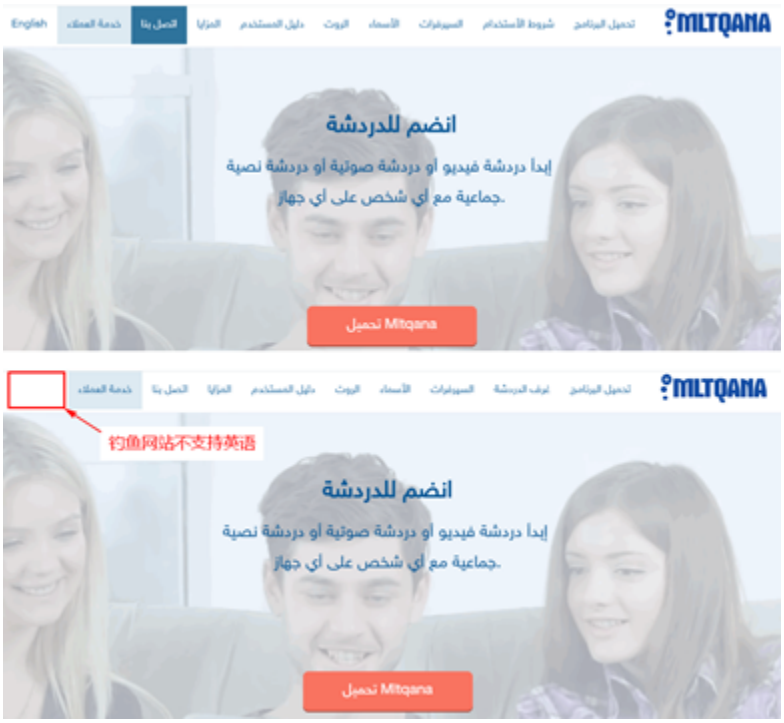

图3 Mltqana官网（上）和钓鱼网站（下）

第三方文件托管网站

除了使用了钓鱼网站进行载荷投递，该组织还使用第三方文件托管网站进行载荷投递，在文件托管网站页面的相关信息中可以发现恶意应用已经有16次的下载量了，如下图所示。

图4 恶意软件在文件托管网站详细信息

传播方式

北非狐组织主要传播方式是社交媒体，传播流程如下图。

图5 传播流程

2018年2月北非狐组织创建了一个Facebook账号用以传播恶意程序，该账号仿冒EgChat官方Facebook账号，后文中使用Fake EgChat表示仿冒账号。Fake EgChat主页与EgChat官方主页几乎一致（如下图所示），可见Facebook公司针对注册企业账号没有审核机制，正因如此，Facebook也成了APT组织传播恶意程序的常用渠道，此前我们揭露的黄金鼠组织同样使用了Facebook进行传播恶意程序。

图6 Fake EgChat Facebook主页

图7 EgChat官方Facebook主页

在Fake EgChat账号Facebook页面上可以发现所有的帖子均在传播钓鱼链接和恶意应用下载地址。其中的帖子最早可以追溯到2018年2月，并且至今仍然在更新相关钓鱼帖，如下图所示。

图8 FakeEgChat发布的相关帖子

样本分析

Android样本分析

通过钓鱼网站和第三方文件托管网站获取的Android样本安装运行后会隐藏图标，并且诱导受害者安装相应的原版聊天应用，然后在后台运行窃取隐私信息。通过关联发现，Android端攻击样本主要为Droidjack、SpyNote和SonicSpy三个家族的RAT工具。

Droidjack

Droidjack是一款针对安卓手机商业RAT工具，有自己的官方网站。该RAT工具主要功能如下：

- 可以生成一个APK，绑定在被控手机的任何APP上
- 可在电脑端控制手机，包括浏览、传输、删除文件等
- 可进行SMS短信收发和查看功能
- 可以控制手机的电话功能
- 联系人管理
- 麦克风监听
- GPS定位
- APP管理

Droidjack控制端界面如下图所示：

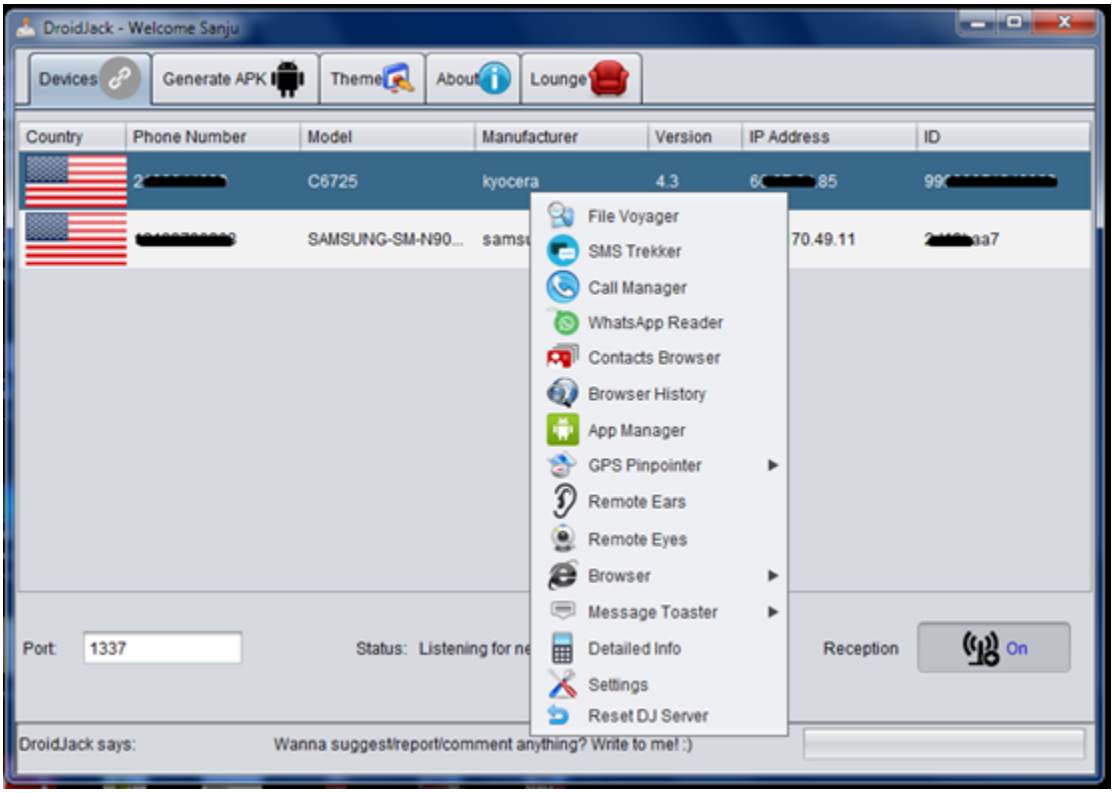

图9 Droidjack控制端界面

Droidjack包结构如下图所示：

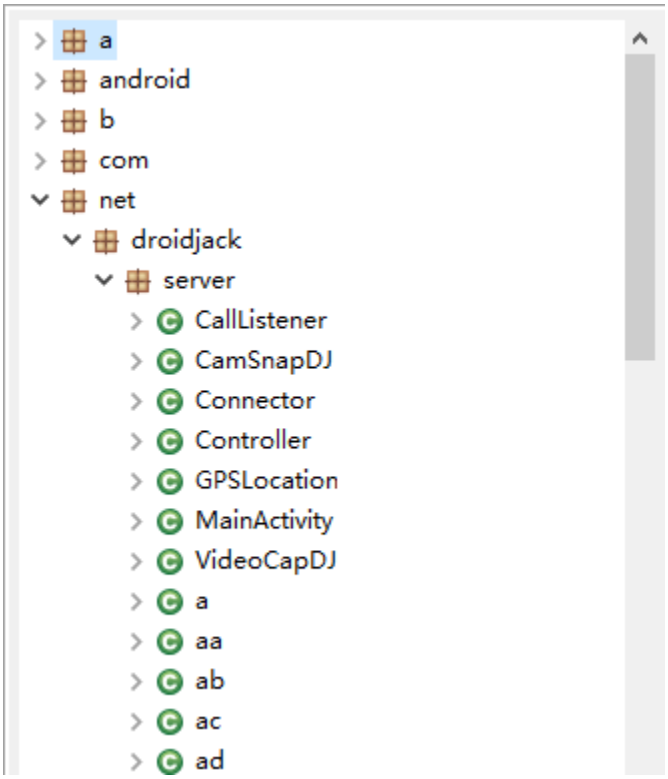

图10 Droidjack包结构

SpyNote

SpyNote类似Droidjack，也是一款针对安卓手机商业RAT工具，但是SpyNote的功能更加强大，其主要功能如下：

- 可以生成一个APK，绑定在被控手机的任何APP上
- 可在电脑端控制手机，包括浏览、传输、删除文件等
- 可进行SMS短信收发和查看功能
- 可以控制手机的电话功能
- 联系人管理
- 麦克风监听
- GPS定位
- APP管理
- 文件管理
- 查看手机系统信息
- 命令行控制

SpyNote控制端界面如下图所示：

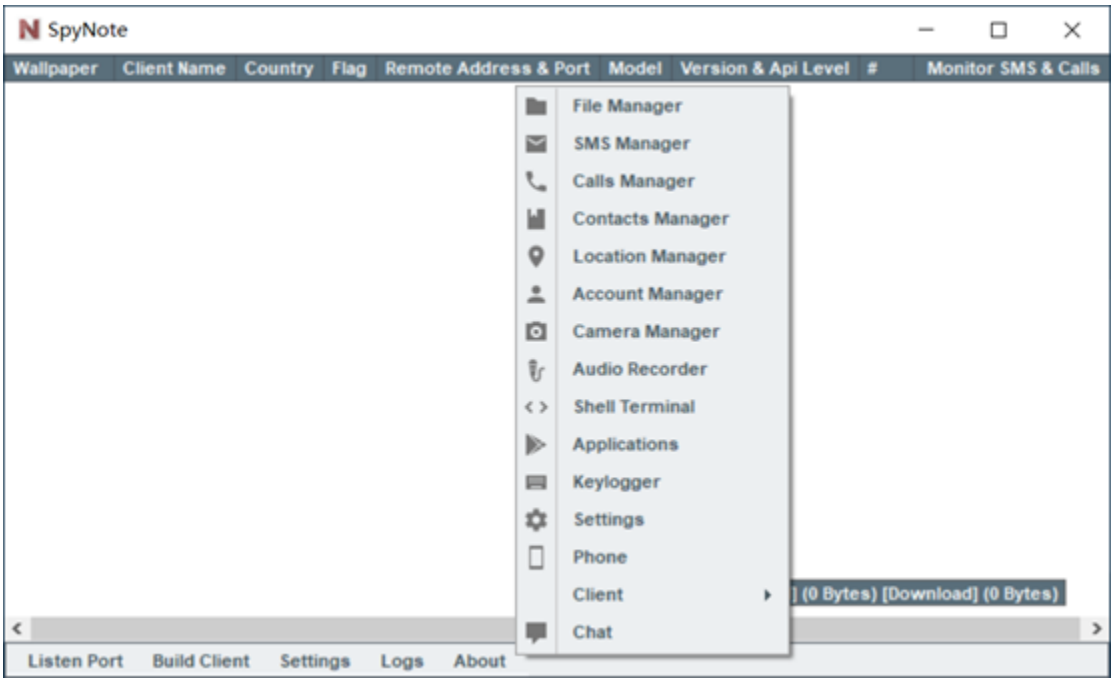

图11 SpyNote控制端界面

SpyNote包结构如下图所示：

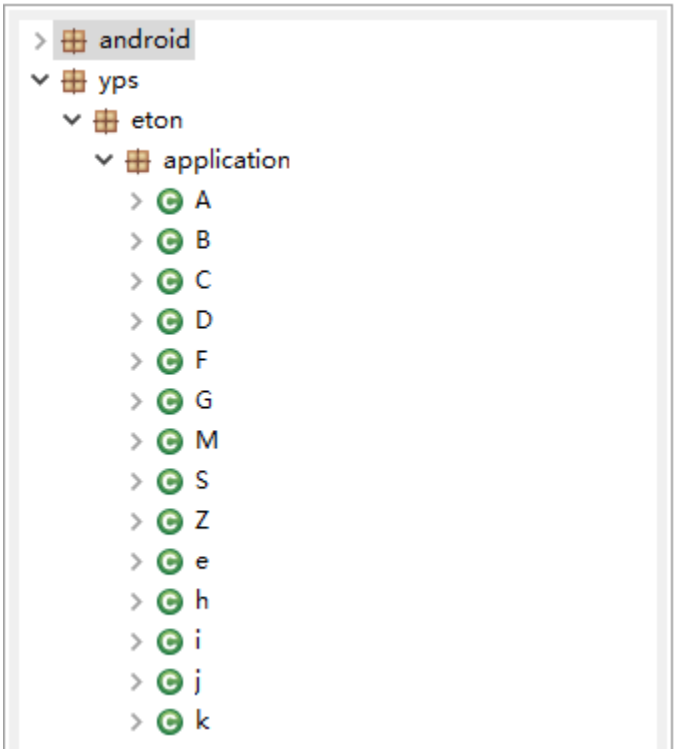

图12 SpyNote包结构

SonicSpy

SonicSpy是商业RAT工具SpyNote的一个变体，最早出现在2017年2月，整个SonicSpy系列产品支持73种不同的远程指令，其主要功能如下

- 以静默方式录制音频
- 使用相机拍照
- 拨打电话
- 向攻击者指定的号码发送短信
- 获取通话记录
- 获取联系人
- 获取Wi-Fi信息
- 获取位置信息

- 获取通知栏消息
- 获取短信
- 操作剪切板
- 执行远程命令

SonicSpy包结构如下图所示：

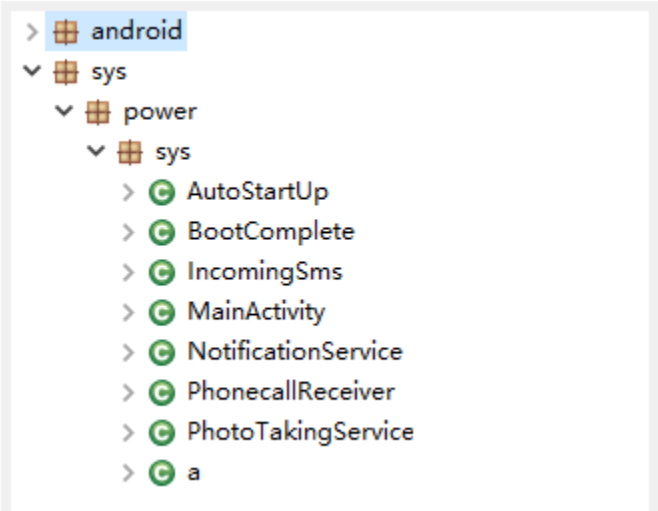

图13 SonicSpy包结构

PC样本分析

钓鱼网站对应的PC端样本，通过对原版聊天应用打包并在其中附加houdini RAT脚本文件，在样本安装的同时运行恶意脚本，窃取各种隐私数据。通过关联发现，该组织PC端主要使用了Houdini RAT、XtremeRAT、Hallaj Pro RAT、RevengeRAT四个家族的RAT工。

通过对样本的最早可能利用时间分析，我们发现攻击者最早17年初利用的是Hallaj Pro RAT，随后开始加入XtremeRAT，在18年初开始利用Revenge-RAT，Houdini RAT属于脚本RAT，无法发现编译时间，我们猜测在2017年底伪装网站上线时候已经开始利用。

可能的最早测试、编译或利用时间	RAT
2017-01-25	Hallaj Pro RAT
2017-10-22	XtremeRAT
2018-01-03	Revenge-RAT

houdini RAT

Houdini RAT由个人编写，国外安全厂商认为作者来自阿尔及利亚，并且通过共享代码库发现该RAT与njworm和njRAT / LV的作者njq8有联系，曾被用于针对国际能源行业的针对性攻击，已被APT-C-37组织使用过，其主要功能如下：

- 执行指定命令
- 更改恶意软件配置。例如，动态DNS名称
- 从系统中删除恶意软件并清除所有快捷方式.lnk
- 上传文件
- 将网站上托管的文件复制到受害者
- 下载文件
- 枚举磁盘信息
- 枚举所有文件和目录
- 枚举进程
- cmd命令
- 删除指定文件或目录
- 关闭指定进程
- 休眠

代码片段如下图所示：

```
"'<[ recoder : houdini (c) skype : houdini-fx ]>

'=-=-=-=-= config =-=-=-=-=-=-=-=-=-=-=-=-=-=-=

host = \"voly.ddns.net\"
port = 82
installdir = \"%appdata%\"
lnkfile = true
lnkfolder = true

'=-=-=-=-= public var =-=-=-=-=-=-=-=-=-=-=-=-=

dim shellobj
set shellobj = wscript.createobject(\"wscript.shell\")
dim filesystemobj
set filesystemobj = createobject(\"scripting.filesystemobject\")
dim httpobj
set httpobj = createobject(\"msxml2.xmlhttp\")


'=-=-=-=-= privat var =-=-=-=-=-=-=-=-=-=-=-=-=
```

图14 Houdini RAT代码片段

XtremeRAT

XtremeRAT从2010年开始被开发，是一款专业的商业间谍软件，功能丰富，目前XtremeRAT已经开源 https://github[.]com/mwsrc/XtremeRAT ，因为可以任意修改、编译而被广泛使用。其主要功能如下：

- 文件管理
- 进程管理
- CMD命令
- 键盘记录
- 服务管理
- 注册表管理

代码片段如下图所示：

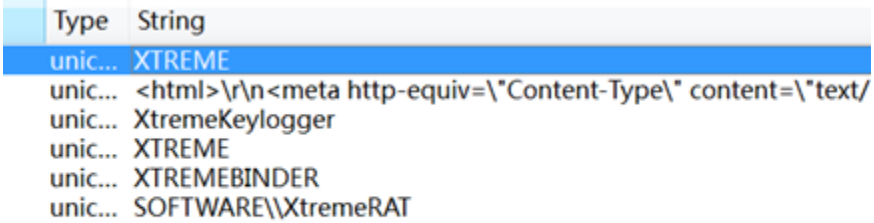

图15 XtremeRAT代码片段

Hallaj Pro RAT

Hallaj Pro RAT fixed最近刚被国外厂商报告用于中东地区威胁攻击，Hallaj是著名的NJRat Trojan的修改版，NJRat Trojan也是中东的地区经常被使用的RAT，已被拍拍熊（APT-C-37）、黄金鼠（APT-C-27）等APT组织使用。其主要功能如下：

- 键盘记录
- CMD命令
- 上传文件

代码片段如下图所示：

```
00000012    unic... SGFjS2Vk
0000002E    unic... Hallaj PRO Rat [Fixed]
00000016    unic... server.exe
0000000A    unic... TEMP
00000042    unic... 23e6d18d0fa7e25eb8844687c5ca5f5c
0000001C    unic... voly.ddns.net
00000006    unic... 81
00000012    unic... boolLove
0000000C    unic... False
00000038    unic... Software\\Microsoft\\Windows\\
00000014    unic... Software\\
00000006    unic... ll
00000006    unic... vn
```

图16 Hallaj Pro RAT代码片段

Revenge RAT

Revenge RAT的第一个版本由阿拉伯语恶意软件程序员Napoleon于2016年6月28日发布，在地下黑客论坛免费分享。RevengeRAT已经被多个APT组织广泛利用。而且其源代码曾经被泄漏过。其主要功能如下：

- 心跳包
- 获得当前窗口标题
- 设置注册表
- 执行内存恶意代码

代码片段如下图所示：

```
strings:… 00000012    un… *-]NK[-*
strings:… 00000018    un… Revenge-RAT
strings:… 0000001E    un… voly.ddns.net,
strings:… 00000004    un… ,
strings:… 00000008    un… 88,
strings:… 00000012    un… R3V1c3Q=
strings:… 00000032    un… RV_MUTEX-BUPRawrSNddXxdY
strings:… 00000018    un… lUATVve.txt
strings:… 00000024    un… google\\Client.exe
strings:… 0000000A    un… True
strings:… 0000000C    un… Start
strings:… 0000000E    un… google
strings:… 00000018    un… SystemDrive
strings:… 00000028    un… \\ProgramData\\google
```

图17 Revenge RAT代码片段

样本编译时间分析

下图显示的是样本的编译时间，其中有一些RAT是公开模块生成，编译时间统一。可以看出攻击从2017年末开始，其中包含有大量测试样本，样本编译数量较多，攻击处于准备阶段，到2018年始终保持样本的迭代，之后样本功能稳定。

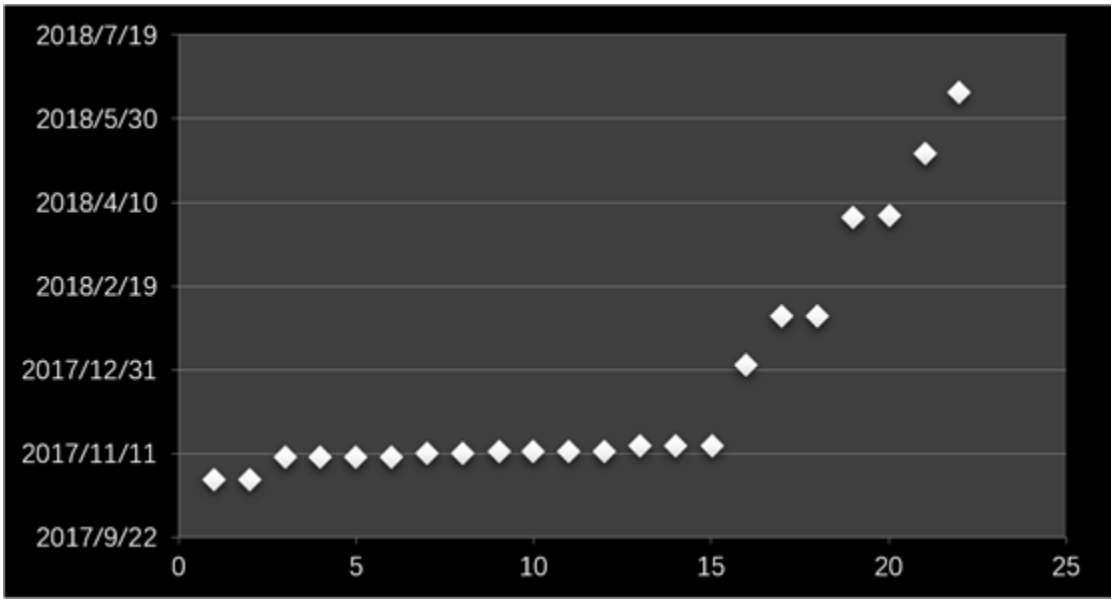

图18 样本编译时间

受害者分析

2018年1月8号一个Facebook用户分享了钓鱼网站创建的聊天室地址（该聊天室地址已失效）。对该用户相关信息进一步分析，我们猜测其为此次攻击的受害者，并且该分享帖中的评论用户可能也是相关受害者。该受害者位于阿尔及利亚，根据该用户点赞的相关账号，我们认为其可能是阿尔及利亚国民军伤残退役人员。

图19 受害者分享的聊天室地址

图20 受害者点赞的账号

在该组织发布的钓鱼帖子中，我们发现了另一个受害者，该受害者声称已经安装了该组织提供的软件，但是最终给出了未安装应用的提示，而实际上这是间谍软件隐藏图标的常规手法。通过分析该受害者相关信息，可以确定其位于约旦。


Egchat إيجي شآت
2018年7月19日
برنامج دردشة صوتية جديد ,من خلاله يمكنك التعرف على اصدقاء جدد تم بناء البرنامج ليحافظ على حرية وخصوصية المستخدم حيث تم اضافة العديد من المزايا لكل من المستخدم والمشرف
من ميزات البرنامج انه ..
اولا الدخول السهل لغرف الدردشة التي تحتوي على كاميرا ومايك وتمتاز الغرفه باشكال جميلة ومميزة والوان عديدة تسهيلا لدردشه وبسمايلات رائعة
ثانيا يمكنك الحصول على ملف شخصي #مجانا ولفترة محدودة يوضع فيه معلومات صفحتك الشخصية مثل الاسم والعمر والجنسية وتاريخ الميلاد والمهنة ..
ثالثا .. يحتوي البرنامج على لوحة تحكم سهلة الاستخدام وتحتوي على العديد من الخيارات التي تعطي لمالك الغرفه و الروت حريه كامله لتحكم بالغرفه
موقعنا ليس الوحيد لكنه تجربتنا الاولى نتمنى ان ينال اعجابكم ، زوروونا!
www.egchaat.com
查看翻译
دردشة ايجي شات الصوتية egchat
egchat الصوتية
3
4条评论
赞
评论
分享
最相关评论
写评论...
按 Enter 键发布。
بشار برهو
我的爱不是在安卓上工作, 而是在上传Google Play, 但通过研究或在Downwood的链接, 这个应用程序还没有找到
赞 · 回复 · 查看原文 (阿拉伯语) · 2年
作者
Egchat إيجي شآت
http://egchaat.com/EgChat.apk这是下载Android的链接
赞 · 回复 · 查看原文 (阿拉伯语) · 2年
بشار برهو
下载并跳过源设置, 但最终给出了未安装的应用
赞 · 回复 · 查看原文 (阿拉伯语) · 2年
作者
Egchat إيجي شآت
我的兄弟, 节目有另一个名字叫我们会面, 上帝保佑, 我们会改整版, 让名字出来
赞 · 回复 · 查看原文 (阿拉伯语) · 2年

图21 钓鱼帖子下面的求助信息

在该组织Facebook首页可以看到有数百位用户关注该账号，结合前面提到的第三方托管网站的下载次数，此次攻击活动中的受害者可能多达数百。

图22 仿冒EgChat官方Facebook首页

归属分析

2013年国外安全厂商批露信息显示，Houdini远控开发者来自阿尔及利亚。而此次攻击中同样使用了Houdini远控，并且攻击活动中所使用的两个钓鱼网站注册信息显示归属于阿尔及利亚，并且其中一个钓鱼网站的注册邮箱后缀归属法国。阿尔及利亚官方语言为现代标准阿拉伯语，国内通用阿尔及利亚阿拉伯语，而法语则因殖民历史原因成为国家行政、贸易和教育领域的专用语言。因此，我们推测此次攻击者位于阿尔及利亚。

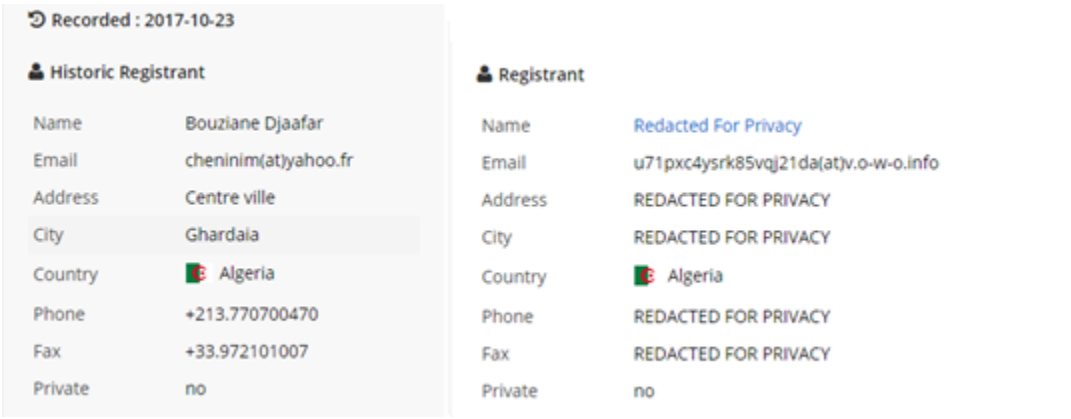

图23 钓鱼网站信息

进一步通过360威胁情报中心（https://ti.360.cn/）域名解析该组织的CC(voly.ddns.net)，发现近期解析的IP均在 41.105.0.0 - 41.105.255.255范围内，而该IP段归属阿尔及利亚。基于以上原因，我们将此次攻击活动归属于阿尔及利亚。

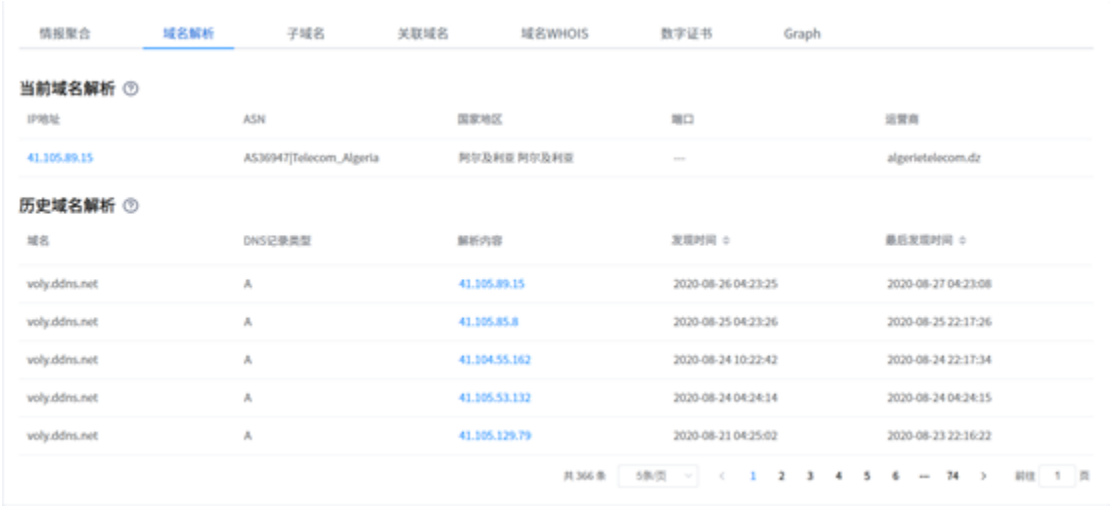

图24 360威胁情报域名解析

图25 域名解析的IP归属阿尔及利亚IP段

总结

阿拉伯剧变给阿拉伯国家政治发展带来了新的挑战，这包括政治版图的碎片化、政治安全的跨国化、恐怖主义的国际化和危机传播的网络化等问题。阿尔及利亚作为非洲北部的一个阿拉伯国家，无疑也面临这这些挑战。近年来，该国深受恐怖动乱之害，对恐怖活动保持高压打击态势。此次北非狐组织（APT-C-44）网络攻击活动中使用的伪装对象具有较强的针对性，目标人群对聊天应用安全性要求比较高，结合以及阿尔及利亚国内的政治状态，我们推测此次攻击活动主要为了通过网络攻击活动占领情报先机，防止恐怖主义冒头，从而维护国家政治稳定。

随着智能手机行业的高速发展，各种技术的迭代更新，手机功能变得更强大，智能手机逐渐成了人们工作生活中必不可少的工具。因此将会有越来越多的攻击组织会把移动端作为攻击的必备目标。在这种形式下，国内相关企业需要做好各个平台的安全防护以及相关的安全培训。

IOC

样本**md5**

Android

80bbdc982ed7d5728c9005f1713db4c7

8a8b2e08c4087735ca214640f52a7215

f4a2b85463cea2d05ca672069acfa364

1f6375a4a6cac6a12172c87eff7cafce

a228ba347cc2ca2b97f0c1e6e5e07558

fec9ff0cd85e820ac779ea25e3fefb24

PC

6ecd6914eb992734dfbca11cd41afb07

d6ba589af24ff96e9c1f356398243156

ca0697a4cb47108dc2322b09de1868e0

be6e448595e3a98ddd11c3cfb49e51e6

bd4d1f6a435639fc6f01af26237e0a31

e846dc1ab2fdeae0f02faf9f92626a9e

f68578468ff8fd930079871643277b9e

dc32f1e2c8e46a283522f680689df577

9da77984d89f70705f9fa9c7dd904f5a

a6bea852441fd3a2658d4882f1823492

98bc19c0196a9e12a334adf5c505a78d

9e1ef7349b74d0be83d7374909937c47

32e3e9106c57f1089c136fe78dfe5e38

57ac433c6ae67fa45699b8b08fb04142

ec9ccaf9a8e0421748c3460f76289a48

10335258e279c1ec346e9bedae2776dd

d7f7a907cd1dc1d34695759d4669409b

7958aab62e49c69ef8f64765a377788c

de7cfef57b848a8d7f0a1d4828d6f1ed

72425aac85ead205e3d26392fb414e1d

04b37c5776e2a2424d47472fc3e9aaf5

fe8b2df29417a27881f4727c35aae61e

291d4bdbab778d045aedd11788762e82

81b910bed85a80781aafadde79832405

c238894641abfeb9411f7e9ffb1999f4

6f7b51344e8956325859a2ec37ac2d25

ce0f944b84b823e1267175d6b4f5cdbd

f67674f89e1c9727ea6aeffd71949748

1455f631b08b4c7a4ae1c5c8c319d64f

508c7f8c30c558c3c5bdbdb3f6a8b1c9

78fc9320dc84109cd50d17379fada888

C&C

https://voly.ddns[.]net

http://egchaat[.]com（已失效）

http://www.moltqana[.]com

PDB

C:\Documents and Settings\Administrateur\Bureau\1830.pdb

C:\Documents and Settings\Administrateur\Bureau\5552.pdb

C:\Documents and Settings\Administrateur\Bureau\rexx.pdb

C:\Documents and Settings\Administrateur\Bureau\rexx.pdb

C:\Documents and Settings\Administrateur\Bureau\s.pdb

C:\Documents and Settings\Administrateur\Bureau\yo2.pdb

C:\Documents and Settings\Administrateur\Bureau\yo2.pdb

C:\Documents and Settings\Administrateur\Bureau\z.pdb

c:\Users\Administrator\Desktop\syystme - Copy\syystme\obj\Debug\syystme.pdb

c:\Users\Administrator\Desktop\syystme\syystme\obj\Debug\syystme.pdb

c:\Users\devil\Desktop\ART\ART\obj\Debug\ART.pdb

C:\Users\deviL\Desktop\test\test\obj\Debug\test.pdb

C:\Users\devil\Desktop\WindowsApplication1\WindowsApplication1\obj\Debug\system.pdb

参考

https://ti.360.cn/

https://www.facebook.com/eegchaat

https://www.facebook.com/pg/voiceegchat

https://www.facebook.com/100011589727981k

https://www.facebook.com/bashar.basha11

https://web.archive.org/web/20180605042224/http://egchat.com/egchat/

https://web.archive.org/web/20180805173429/http://egchaat.com/

https://top4top.io/downloadf-12180r3ix1-apk.html

本文链接：https://blogs.360.cn/post/APT-C-44.html

-- EOF --

Comments