



“海莲花” 团伙近期利用Office漏洞发起高频攻击

Threatbook 

2018-05-23 共148445人围观，发现 4 个不明物体

安全报告

概要

“海莲花”，又名APT32和OceanLotus，是越南背景的黑客组织。该组织至少自2012年开始活跃，长期针对中国能源相关企业、海事机构、海域建设部门、科研院所和航运企业等进行网络攻击。除中国外，“海莲花”的标还包含全球的政府、军事机构和大型企业，以及本国的媒体、人权和公民社会等相关的组织和个人。

微步在线长期监控着“海莲花”的活动动向，曾发布多份关于该团伙的分析报告《“海莲花”团伙的最新动向析》、《“海莲花”团伙专用后门Denis最新变种分析》和《微步在线发现“海莲花”团伙最新macOS后门》。微步在线监测发现，2018年4月份以来，该团伙攻击活动异常频繁，并开始利用高危Office漏洞来投递其常用特木马Denis，具体内容包含：

据微步在线威胁情报云监测发现，本月APT32 的攻击活动异常频繁，中国能源和金融相关企业，以及越南周边的柬埔寨等国的相关目标遭到攻击，其中国内是重灾区。

2018年4月以来，APT32开始大量利用CVE-2017-11882和CVE-2017-8570等Office漏洞投递其特种木马Denis，攻击过程中利用了“白利用”技术。

APT32在2018年4月5日前后集中注册了几十个域名，并开始使用后缀为info、club和xyz的顶级域名，且其中部分已被用于真实的攻击。

鉴于此次攻击行动相比之前，目标更广、频次更高，建议国内相关行业（金融、能源和政府）及重点单位及时排查。

微步在线通过对相关样本、IP和域名的溯源分析，共提取59条相关IOC，可用于威胁情报检测。微步在线的威胁检测响应平台（TDP）、威胁情报订阅、API等均已支持此次攻击事件和团伙的检测。

详情

微步在线长期跟踪全球100余黑客组织。近期，微步在线监测到APT32的活动加剧，持续针对中国能源和金融相关企业，以及越南周边的柬埔寨等国的相关目标发起攻击。微步在线的狩猎系统捕获了一批APT32的最新攻击样本，分析发现这些样本利用了CVE-2017-11882和CVE-2017-8570漏洞投递其专有的特种木马Denis，相关样本如下：

SHA256	漏洞	C2	文件名
--------	----	----	-----

SHA256	漏洞	C2	文件名
e5c766ad580b5bc5f74acc8d2f5dd028c11495d2ce503de7c7a294f94583849d	CVE-2017-11882	straliaenollma.xyz andreagahuvrauvin.com byronorenstein.com	Document_GPI Invitation-UNSOOC China.doc
0d1577802d4560b9ba184a2d13570ba28ed0318eee520f2f7a6c5ef238671dd9	CVE-2017-11882	stopherau.com orinneamoure.com ochefort.com	
3a3bc31afcf2ec82ff9ac0016ce47e10833227665ab056117520bdf097525c63	CVE-2017-8570	tsworthoa.com earlase.com aximilian.com	
abfcba26e50a88c2ce507212b15d2ee24c28fc8b28edeaee27f70faaf6fae700	CVE-2017-8570	orinneamoure.com ochefort.com icmannaws.com	Monthly Report 03.2018.doc

Denis是APT32最常用的特种木马，是一个全功能的后门，包含多种对抗技术，其特征是使用DNS隧道技术与C2通信。Denis此前主要通过双扩展，虚假Word、Excel、WPS和PDF图标，虚假更新（Adobe、FireFox、Google），以及字体相关工具诱导受害者点击可执行文件进行传播。之前的一些诱饵文件的文件名和图标如下

文件名	图标
adobe-font-pack.exe	 adobe-font-pack.exe Windows Font Folder Microsoft Corporation
Chi tiet danh sach nhan vien sai quy dinh can xu phat.exe	 Chi tiet danh sach nhan vien sai quy dinh can xu ... Microsoft Word
FirefoxUpdate.exe	 FirefoxUpdate.exe Firefox Mozilla
GoogleUpdateSetup.exe	 GoogleUpdateSetup.exe Google Update Setup Google Inc.
TimeTable 27 November - 03 December 2017v4.exe	 TimeTable 27 November - 03 December 2017v4.exe WPS Writer
02 Meeting Report for Mar-2018 Cambodia.xls.exe	 02 Meeting Report for Mar-2018 Cambodia.xls.e... Microsoft Excel
请尽快补充完善《财务部之报告》.exe	 请尽快补充完善《财务部之报告》.exe Microsoft Word
Thu moi tham du Hoi thao-Final-FRONT-PAGE.exe	 Thu moi tham du Hoi thao-Final-FRONT-PAGE.... Foxit Reader 5.0, Best Re...

样本分析

以最新捕获的诱饵文档“Document_GPIInvitation-UNSOOC China.doc”为例进行分析，该文档包含CVE-2017-11882漏洞利用，触发漏洞利用之后会交付APT32的特种木马Denis。

1、该样本的基本信息如下：

文件类型	rtf
文件大小	3139367 字节
文件名	Document_GPI Invitation-UNSOOC China.doc
SHA256	e5c766ad580b5bc5f74acc8d2f5dd028c11495d2503de7c7a294f94583849d
SHA1	e2d949cf06842b5f7ae6b2dffaa49771a93a00d9
MD5	02ae075da4fb2a6d38ce06f8f40e397e

2、该样本在微步云沙箱的分析结果如下图：

⚠ 经检测该文件为恶意

文件名称: e5c766ad580b5bc5f74acc8d2f5dd028c11495d2ce503de7c7a294f94583849d.rtf

SHA256: e5c766ad580b5bc5f74acc8d2f5dd028c11495d2ce503de7c7a294f94583849d

运行环境: win7_sp1_enx86_office2010

提交时间: 2018-05-15 11:55:33

样本标签: Exploit CVE-2017-11882

UN?

39.2分

重新分析

收藏

报告

样本

PCAP

多引擎检出率

6 / 25

反病毒软件	检测结果
腾讯 (Tencent)	Office.Exploit.Generic.Eos
微软 (MSE)	Exploit:O97M/CVE-2017-11882
GDATA	Exploit.RTF-ObfsStrm.Gen
IKARUS	Exploit.RTF-ObfsStrm
360 (Qihoo 360)	virus.exp.21711882.d
安天 (Antiy)	Trojan[Exploit]/RTF.Obsecure.Gen

进程详情

共分析了3个进程

WINWORD.EXE (PID:3204)

"C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" C:\Users\vbccsb\AppData\Local\Temp\e5c766ad580b5bc5f74acc8d2f5dd028c11495d2ce503de7c7a294f94583849d.rtf

EQNEDT32.EXE (PID:4048)

"C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding

MicrosoftWindowsDiskDiagnosticResolver.exe (PID:268)

"C:\Program Files\Microsoft-Windows-DiskDiagnosticResolver_2021325962\MicrosoftWindowsDiskDiagnosticResolver.exe"

https://s.threatbook.cn/report/file/e5c766ad580b5bc5f74acc8d2f5dd028c11495d2ce503de7c7a294f94583849d/?env=win7_sp1_enx86_office2010

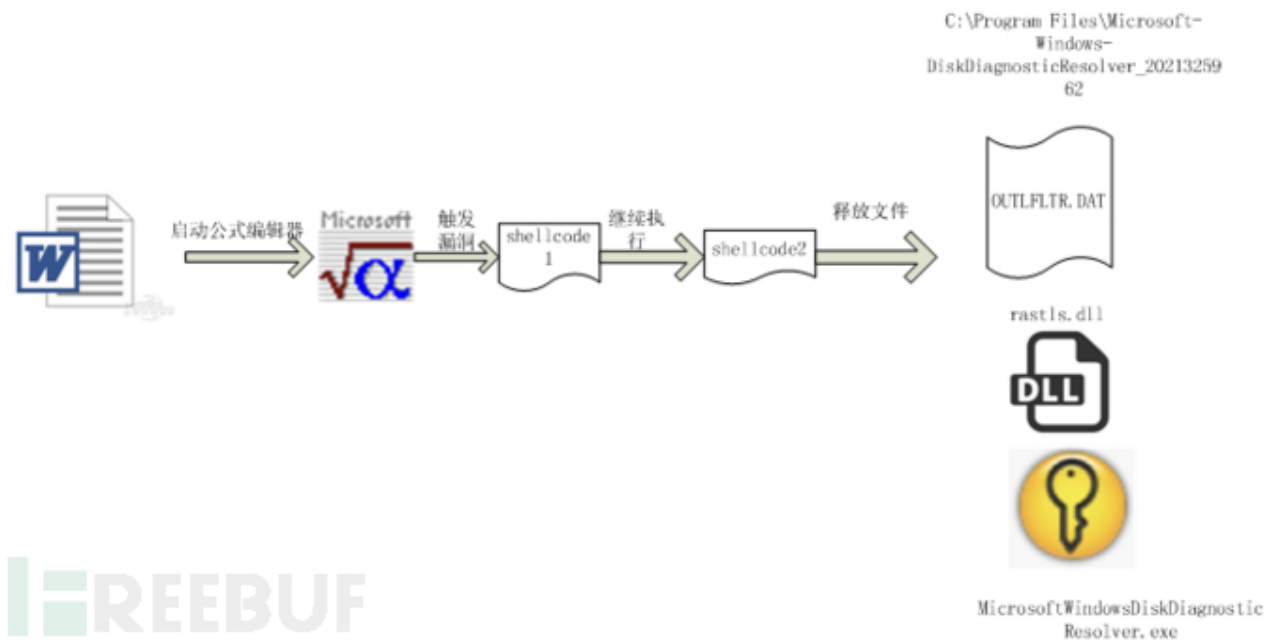
3、 该文档包含CVE-2017-11882漏洞利用，打开后会显示一模糊图片来迷惑受害者，如下图：

https://www.freebuf.com/articles/paper/172222.html

4/17



4、该诱饵文档触发CVE-2017-11882漏洞后的整体执行流程如下图，该漏洞的相关分析见附录的“漏洞分析”。



打开文档触发漏洞之后会执行shellcode1，shellcode1会继续执行shellcode2，shellcode2最终会在C:\Program Files\目录下创建一个隐藏文件夹Mic

目录释放三个文件：MicrosoftWindowsDiskDiagnosticResolver.exe、rastls.dll和OUTLFLTR.DAT，然后启动MicrosoftWindowsDiskDiagnosticResolver.exe。

MicrosoftWindowsDiskDiagnosticResolver.exe是一个包含Symantec签名的白文件，启动后会加载同目录下的恶意rastls.dll，这是典型的“白利用”技术。rastls.dll最终会交付APT32的特种木马Denis，相关“白利用”技术和Denis木马的详细分析见微步在线发布的报告《“海莲花”团伙专用后门Denis最新变种分析》。

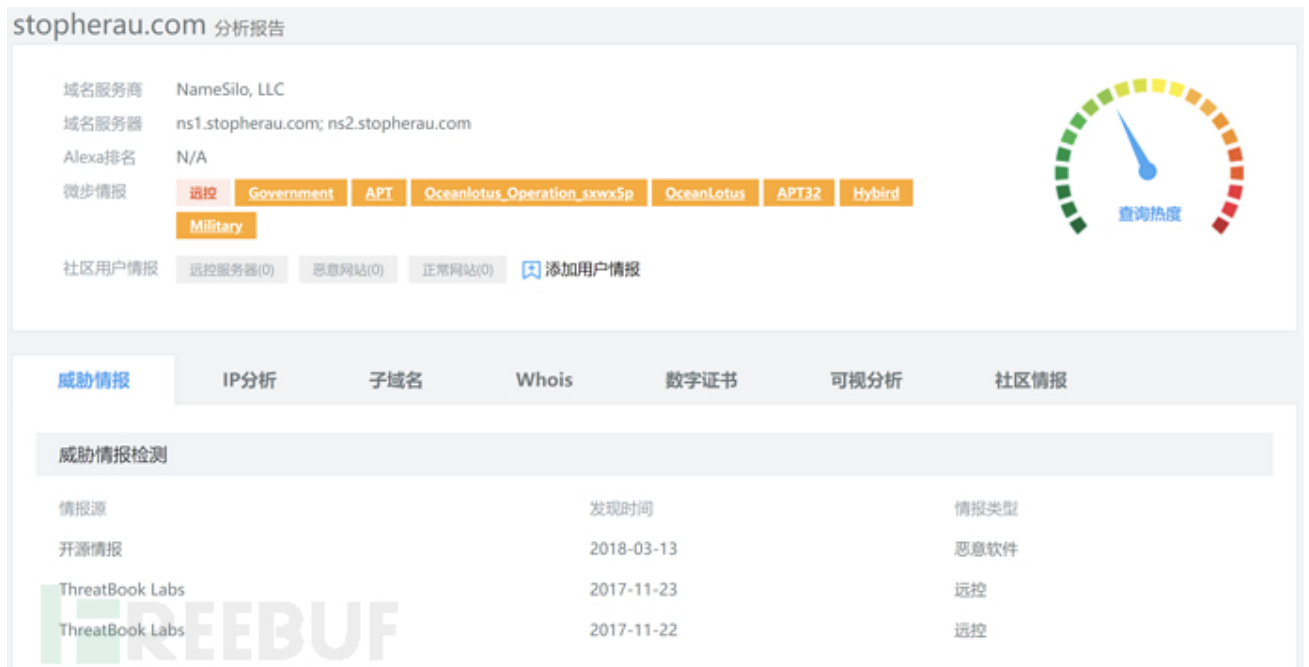
关联分析

微步在线监测发现，近期APT32的攻击活动加剧，中国能源和金融相关企业，以及越南周边的柬埔寨等国的相关目标遭到定向攻击，其中国内是重灾区。

使用x.threatbook.cn对straliaenollma.xyz、andreagahuvrauvin.com和byronorenstein.com进行关联发现发现三者的注册信息都使用了隐私保护，于近期注册且注册时间相同。在一个木马中使用多个注册时间相近（同为同一天，且域名服务商多相同）的域名作为C2一直是APT32的习惯。

C2域名	域名有效期	注册邮箱
straliaenollma.xyz	2018/04/06-2019/04/06	隐私保护
andreagahuvrauvin.com	2018/04/06-2019/04/06	隐私保护
byronorenstein.com	2018/04/06-2019/04/06	隐私保护

此外，使用x.threatbook.cn分析另一CVE2017-11882漏洞利用样本的C2 stopherau.com，发现其早已被微步在线识别：





根据微步在线威胁情报云数据，APT32近期（2018/04/04-2018/04/06）注册了几十个域名用作C2，且开始注册TLD为club、xyz和info等的域名，详细IOC见附录。其中部分在注册之后不到两周就被用于攻击，这也说明APT32近期攻击活动极为活跃。

漏洞分析

CVE-2017-11882是存在于Office公式编辑器中的一个内存破坏漏洞，漏洞相关分析如下：

- 1) 公式编辑器是一个独立的可执行程序，由Office启动。这里通过在注册表中设置镜像劫持，然后将调试器置为ollydbg来分析该程序，具体的路径如下：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Image File Execution Options\

 (默认)	REG_SZ	(数值未设置)
 debugger	REG_SZ	c:\Olllydbg\OlllyDBG.exe

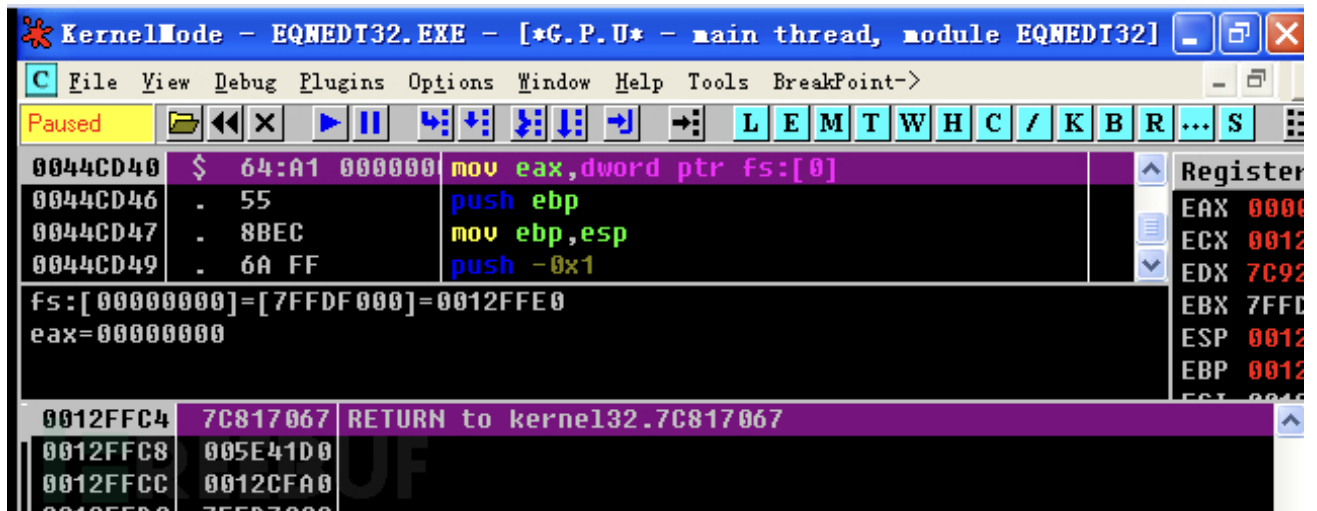
- 2) 首先启动公式编辑器，然后使用ollydbg附加其上，并在地址0x00411655上下一个软件断点0x00411655。这个地址是导致漏洞触发的位置（参考相关分析报告），然后关闭公式编辑器和ollydbg。如图：

```

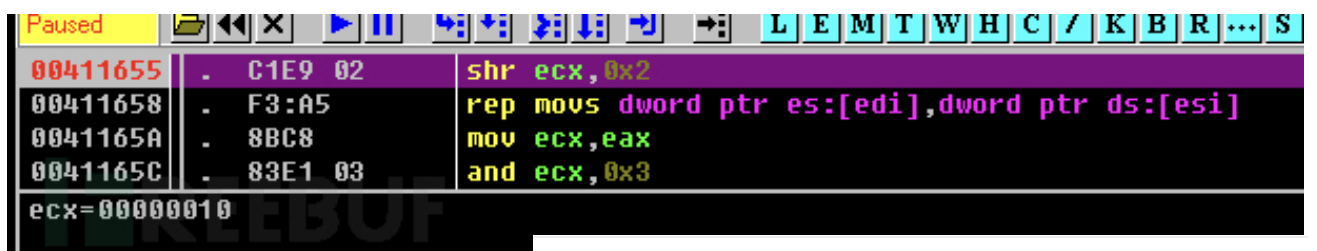
:00411653      mov     esi, edx
:00411655      shr     ecx, 2
:00411658      rep movsd
:0041165A      mov     ecx, eax
:0041165C      and     ecx, 3
:0041165F      rep movsb

```

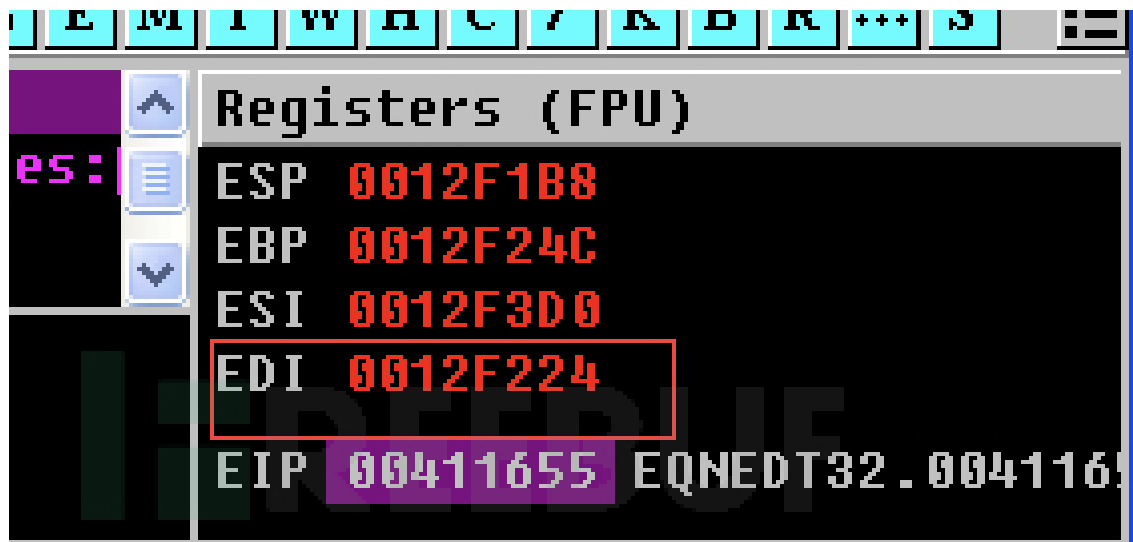
- 3) 打开漏洞利用样本，当漏洞成功触发后会启动公式编辑器，然后导致ollydb附加其上。如下图：



然后F9让公式编辑器运行起来，接着会触发新的断点，如下图：



栈溢出过程是在第二次，所以再次F9，再次断



此时EDI指向的地址位于栈上，如下图：

0012F224	77EFDDB1	RETURN to gdi32.77EFDDB1 from gdi32.77EF7D
0012F228	B4010A55	
0012F22C	0012F244	UNICODE "?"
0012F230	77EFDDB8	RETURN to gdi32.77EFDDB8 from ntdll.RtlLea
0012F234	77EFDDBD	RETURN to gdi32.77EFDDBD from gdi32.77EFD
0012F238	77EFDDBA	RETURN to gdi32.77EFDDBA from gdi32.77EFD
0012F23C	0012F660	
0012F240	0012FAB8	
0012F244	00000021	
0012F248	0000FFFF	
0012F24C	0012F290	
0012F250	004115D8	RETURN to EQNEDT32.004115D8 from EQNEDT32.
0012F254	0012F3D0	RETURN to 0012F3D0
0012F258	00000000	

在没有拷贝数据前，12F250处的值是4115D8，拷贝完成后如下：

0012F224	71EB44B8	
0012F228	5678BA12	
0012F22C	D0311234	
0012F230	098B088B	
0012F234	8366098B	
0012F238	E1FF3CC1	
0012F23C	90909090	
0012F240	90909090	
0012F244	90909090	
0012F248	90909090	
0012F24C	90909090	
0012F250	00402114	EQNEDT32.00402114
0012F254	0012F3D0	RETURN to 0012F3D0
0012F258	00000000	
0012F25C	0012F26C	UNICODE ``
0012F260	0012F660	
0012F264	0012F688	
0012F268	0012FAB8	

对比后会发现0012F250处的返回地址被覆盖为00402114，该地址位于公式编辑器中相关代码如下图，这里只有一个返回指令：

00402114	L. C3	retn
----------	-------	------

4) 在00402114处下软件断点。00402114处执行完后，会将0012f3D0作为返回地址弹出来，该处的代码如下：

0012F3D0	B8 44EB7112	mov eax,0x1271EB44
0012F3D5	BA 78563412	mov edx,0x12345678
0012F3DA	31D0	xor eax,edx
0012F3DC	8B08	mov ecx,dword ptr ds:[eax]
0012F3DE	8B09	mov ecx,dword ptr ds:[ecx]
0012F3E0	8B09	mov ecx,dword ptr ds:[ecx]
0012F3E2	66:83C1 3C	add cx,0x3C
0012F3E6	FFE1	jmp ecx

a) 该段代码执行完后会先获取kernel32的基地址，然后获取所需要的API，所要获取的 API 如下表：

kernel32. <u>GetModuleHandleW</u>	kernel32. <u>LoadLibraryW</u>	kernel32. <u>GetProcAddress</u>
kernel32. <u>CreateFileW</u>	kernel32. <u>SetFilePointer</u>	kernel32. <u>ReadFile</u>
kernel32. <u>WriteFile</u>	kernel32. <u>CloseHandle</u>	kernel32. <u>ExpandEnvironmentStringsW</u>
kernel32. <u>VirtualAlloc</u>	kernel32. <u>VirtualFree</u>	kernel32. <u>CreateThread</u>
kernel32. <u>WaitForSingleObject</u>	kernel32. <u>CopyFileW</u>	kernel32. <u>OpenProcess</u>
kernel32. <u>GetCurrentProcess</u>	kernel32. <u>GetCurrentProcessId</u>	kernel32. <u>CreateToolhelp32Snapshot</u>
kernel32. <u>Process32FirstW</u>	kernel32. <u>Process32NextW</u>	kernel32. <u>GetFileSize</u>
kernel32. <u>CreateFileMappingW</u>	kernel32. <u>MapViewOfFile</u>	kernel32. <u>GetLogicalDriveStringsW</u>
kernel32. <u>QueryDosDeviceW</u>	kernel32. <u>GetTempPathW</u>	kernel32. <u>OutputDebugStringW</u>
kernel32. <u>Sleep</u>		

b) 然后调用kernel32.GetProcAddress获取ntdll中的相关函数：

ntdll.ZwQuerySystemInformation

ntdll.ZwDuplicateObject

ntdll.ZwQueryObject

c) 接着获取ole32.dll中的ole32.CoInitialize, ole32.CoCreateInstance。

d) 接着获取oleaut32.VariantInit, oleaut32.GetActiveObject。

e) 接着获取psapi.GetMappedFileNameW。

5) 查找winword进程，然后遍历系统所有打开的句柄，找到winword打开的样本句柄，然后将这个文件映到公式编辑器的进程空间，从文件的尾部读取第二段shellcode。具体步骤如下：

a) 调用CreateToolhelp32Snapshot, Process32FirstW, Process32NextW, CloseHandle找到winword进程ID。

b) 调用ZwQuerySystemInformation遍历系统的所有打开的句柄。此时SystemInformationClass= SystemExtendedHandleInformation, 通过ZwQueryObject查询对象的类型，找到属于winword打开的文件。然后调用CreateFileMappingW和MapViewOfFile函数将打开的文件映射到公式编辑器的内存空间。然后判断文件尾部是否是以“yyyy”结束，如是则表示是样本本身。接着通过VirtualAlloc重新分配内存将样本尾部的数据拷贝进去，然后跳到该片内存中执行。

6) 文件尾部的shellcode使用了混淆，加密和PE重构等技术。垃圾指令的部分代码如下：

```

seg000:03189858          pushf
seg000:03189859          push     ecx
seg000:0318985A          shl     ecx, 3
seg000:0318985D          push     ebx
seg000:0318985E          inc     bh
seg000:03189860          or      ecx, ecx
seg000:03189862          shl     cx, 6
seg000:03189866          push     eax
seg000:03189867          aaa
seg000:03189868          push     edx
seg000:03189869          cwd
seg000:0318986B          cwd
seg000:0318986D          mov     eax, 2A02h
seg000:03189872          mov     ecx, 0DE43h
seg000:03189877          mul     ecx
seg000:03189879          neg     al
seg000:0318987B          bswap   ebx
seg000:0318987D          mov     ax, 6Ch ; 'l'
seg000:03189881          mov     cx, 50h ; 'P'
seg000:03189885          mul     cx
seg000:03189888          stc
seg000:03189889          sahf
seg000:0318988A          push     ecx
seg000:0318988B          cbw
seg000:0318988D          bswap   edx
seg000:0318988F          inc     edx
seg000:03189890          or      dh, dl
seg000:03189892          cdq
seg000:03189893          mov     edx, [esp+1Ch+var_18]
seg000:03189897          das
seg000:03189898          mov     bx, cx
seg000:0318989B          mov     ebx, [esp+1Ch+var_10]
seg000:0318989F          mov     ecx, [esp+1Ch+var_C]
seg000:031898A3          aas
seg000:031898A4          mov     eax, [esp+1Ch+var_8]
seg000:031898A8          push     eax
seg000:031898A9          popf

```

该段shellcode执行后会在内存中构建一个DLL文件，然后修复导入表和重定位表。接着调用这个DLL的DllMain函数完成初始化。然后调用这个DLL的导出函数DllEntry，在这个函数里后从DLL的资源节读取数据然后解压，并c:\Program Files\目录下创建一个隐藏文件夹Microsoft-Windows-DiskDiagnosticResolver_2021325962，后向这个目录下释放三个文件：MicrosoftWindowsDiskDiagnosticResolver.exe、rastls.dll和OUTFLTR.DAT，之后启动 MicrosoftWindowsDiskDiagnosticResolver.exe。

附录

C2

alphbbeauchemin.com
 andreagahuvrauvin.com
 angelinachilds.com
 audreybourgeois.com
 beaudrysang.xyz
 cesterlaunela.club

ckbeaudrysanger.xyz

correaplace.club

dieordaunt.com

erokeeobsto.club

esboonemba.com

etramartel.club

ettrobstustralia.club

ganmont.com

illagedrivestralia.xyz

jacobstott.club

karelbecker.com

kermacrescen.com

lauradesnoyers.com

loribrianarlisle.com

manongrover.com

minelauzier.club

nabmarseau.com

nelauzisterla.club

nettpropstoton.club

noycemarseau.com

obststottj.club

ollmarover.com

philippguizar.club

radeordaunt.com

reaplapguizar.club

relbecreybourge.com

robstustral.club

shawnabuddicom.com

sophiahoule.com

stienollmache.xyz

sulapreaplace.club

susannecliche.com

ustrali.club

jackbeaudry.club

andreagbridge.com

eetoramichel.info

byronorenstein.com

christienoll.xyz

christienollmache.xyz

straliaenollma.xyz

wnabudditig.com

sorensanger.xyz

stopherau.com

orinneamoure.com

ochefort.com

tsworthoa.com

earlase.com

aximilian.com

icmannaws.com

Hash

e5c766ad580b5bc5f74acc8d2f5dd028c11495d2ce503de7c7a294f94583849d

0d1577802d4560b9ba184a2d13570ba28ed0318eee520f2f7a6c5ef238671dd9

3a3bc31afcf2ec82ff9ac0016ce47e1083322766

abfcba26e50a88c2ce507212b15d2ee24c28fc8b28edeaae27f70faaf6fae700



单条 IOC的溯源信息可登录 x.threatbook.cn 查看。

TAG: 高级可持续攻击、APT32、海莲花、漏洞、Denis、CVE-2017-11882、CVE-2017-8570

TLP: 白

***本文作者:** Threatbook, 转载请注明来自 FreeBuf.COM。

上一篇: [SURFSRC | 一个针对“比特币”挖矿木马样本的分析](#)

下一篇: [数字货币钱包安全白皮书](#)

已有 4 条评论