Windows 快捷方式漏洞利用实验

1、漏洞行为描述

Ink 漏洞中毒的典型症状为系统运行缓慢、打开程序很久没有反应。网速的反应迟缓，如果所装的杀毒软件开启了实时监控，会不时弹出非法访问的提示，系统的各个盘符 T 莫名其妙出现 autorun.inf 和各种无规律的 exe 可执行文件。

Ink 漏洞对传播者而言具有非常好的触发性，形象描述为“看一眼就中毒”，病毒传播者构造一个特殊的 Ink 文件和一个 Ink 调用的病毒文件。通过 U 盘、移动硬盘、数码存储卡复制传播这些文件，也可以将病毒文件打包在正常程序的压缩包中。病毒被复制或解压到目标位置，当用户使用资源管理器软件去访问这些文件夹时，不需要其它任何操作，病毒程序就会被立即执行。如果病毒保存在 USB 存储器上，对于多数启动了 U 盘自动运行功能的电脑，插入 U 盘的动作即可运行病毒。在局域网的共享文件夹中若存在这样的文件，正常电脑访问这些共享文件夹，就会立即中毒。也可以通过及时聊天工具，如 QQ、MSN、UC 等软件的聊天信息，或发送垃圾邮件的方式附带基于 Ink 漏洞的病毒文件进行传播。

2、漏洞的原理分析

2.1 Ink 文件格式

为了方便用户操作，Windows 操作系统中用户可以创建各类文件的快捷方式，快捷方式实质上只保存了打开该文件的路径，或称为链接(link)。其作用就是使用户在其它方便的地方打开该文件或程序双击程序的快捷方式，再由快捷方式启动相应的程序。快捷方式的扩展名为 Ink，Ink 文件多存在于桌面、开始菜单的各个程序组、任务栏的快速启动栏。Ink 文件结构如表 l。

表 1 为 Ink 文件整体结构，其中内容 2 至内容 8 在 Jnk 文件中是可选项，即不是必须存在的，但是如果存在，则必须按照图 l 的顺序组织。出现漏洞的控制面板程序的快捷方式没有内容 3 到内容 8，所以这里只介绍和 Ink 漏洞相关的文件头和 shell Item Id List 段。

(1)文件头:内容 1 为 tnk 文件的文件头,其偏移 Ox14 处的值是重要的 Flags，用来标识．Ink 文件中有哪些可选属性，也就是哪些节是可选的，Flags 的含义如表 2。

(2) SheIJ Item Id List 段：该段是可选结构，由文件头中偏移 Ox14 位置处的 bit 值来决定，bit 值为 l 时，表示该 Ink 文件包含该结构。如果存在该结构，偏移 Ox4c 的位置的一个 unsigned short int 是 Shell Item Id List 结构的大小标识，后面紧跟一个 SHITEMID 结构，该结构体定义如下:

```
typedef struct _SHITEMID
{
unsigned short int cb;
unsigned char abID[O];
} SHITEMID,*LPSHITEMID;
```

SHITEMID 结构的第一个成员 cb 标识的是 SHITEMID 数据的大小，因为 SHITEMID 结构的第二个成员 abID 是一个指针，存储具体数据，大小不固定，其指向的第 0 项里的数据是不能修改的(通常为电脑的 GUID)，否则 Ink 文件无法运行。图 l 是用 WinHex 打开的控制面板程序上的“显示”快捷方式。

图 1 是一个控制面板程序的快捷方式，从偏移 Ox14 处的值 Ox81，对照前面表 2 中每个 bit 位代表的含义可以看出该 Ink 文件没有表 l 所示的内容 3 至内容 8。

2.2 漏洞工作原理

Windows 操作系统为了在快捷方式显示对应的图标，会派发一个任务给 She1132.dll 去完成快捷方式图标的解析工作。对于一般文件的快捷方式，它会解析这个 Ink 文件的内容 8，即图标文件段，然后试图读取图标文件。但是对于没有图标文件段的控制面板程序（以 CPL 为后缀的文件），其快捷方式的偏移 Ox7A 位置有一个值，这个值是系统图标的 ID，系统默认有多个图标 ID，图 l 中的 9CFFFF 是其中的一个。She1132 可以通过这个 ID 获得图标，具体解析控制面板程序快捷方式图标的过程如图 2 所示。

Ink 漏洞的关键在于调用 LoadLibrary 函数，当偏移 Ox7A 处的值为 0 时，也就是 she1132 无法通过此处的数值获得预设的图标，那么 she1132 就会调用 LoadLibrary 函数来加载目标文件，即一个 cpl 文件(cpl 文件是一种特殊的 dll 文件)来获取图标信息。Ink 漏洞就是利用了这个解析机制的安全缺陷，攻击者恶意构造一个特殊的控制面板程序的 Ink 文件，使其 Ox7A 处的偏移为 O，需要加载的目标文件为攻击者构造的恶意 dll 文件，当 she1132 将这个恶意 dll 文件加载到内存中执行时，病毒获得执行。所以 Windows 在显示 Ink 文件并解析恶意构造的 Ink 文件时被触发恶意代码，造成“看一眼就中毒”的现象。

表 1　lnk 文件结构

次序	内容
1	文件头
2	Shell Item Id List 段
3	文件位置信息段
4	描述字符段
5	相对路径段
6	工作目录段
7	命令行段
8	图标文件段
9	附加信息段

表 2　lnk 文件结构

bit 位	该 bit 置 1 时代表的含义(置 0 表示相反的内容)
0	包含 shell item id list 节，修改文件过滤掉该节，不影响.lnk 执行目标，但影响其它功能
1	指向文件或文件夹，如果此位为 0 表示指向其它。
2	存在描述字符串
3	存在相对路径
4	存在工作路径
5	存在命令行参数
6	存在自定义图标，该位置一般用于病毒判断是否感染目标文件的标志

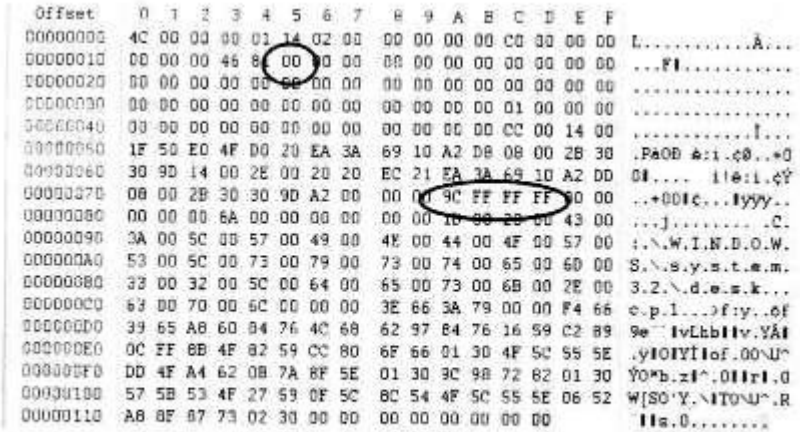

图 1　控制面板程序“显示”的 lnk 文件

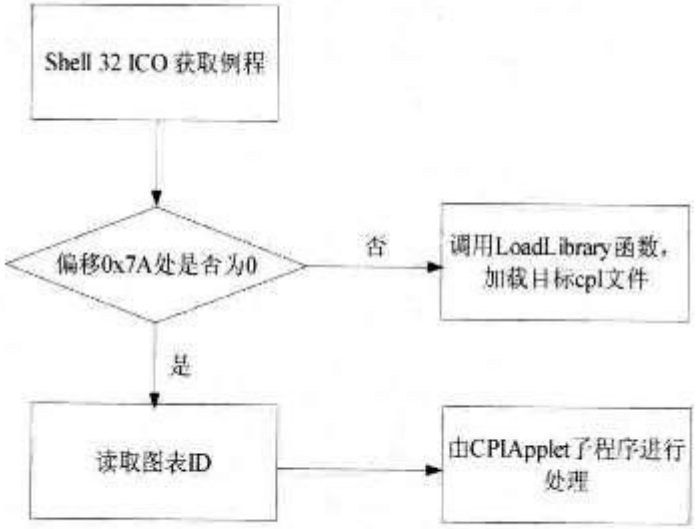

图 2　shell32 解析控制面板程序快捷方式图标的过程

2.3 防范手段

为了不受 Ink 漏洞的影响，用户应该及时打上微软发布的补丁，对于无法及时打上补丁的用户，可以采用下面的一些临时防范方法：①不要打开未知或不可信任来源的带有 Ink 扩展名的文件或浏览其属性；②下载 360safe、金山、瑞星、趋势科技、nod32 等病毒专杀工具；③关闭快捷方式图标显示，不过这会让桌面变的很简陋。

3、实验测试

为了对上述的漏洞原理进行验证，我们实现了一个恶意 Ink 文件来呈现 Ink 漏洞被利用的过程。实验环境为 Windows 7 操作系统，使用的分析工具包括 winhex、VS2008 和 ollydbg。

实验首先创建一个正常的“显示”Ink 文件，步骤如下：到“控制面板”下面，右键点“显示”，点“创建快捷方式”，把快捷方式创建在桌面上。然后在桌面用 WinHex 打开“显示.lnk”文件，如上面图 1 所示。

实验第二步对该 Ink 文件进行修改，把偏移 7A 处的 9CFF FF FF[来自 WwW.lw5u.cOm] 改成 00 00 00 00，把后面的文件名 C:\WINDOWSYsystem32\desk.cpl 改成 C:\box.dIl(UNICODE 格式)。保存文件，并把这个文件复制到任意目录下，当用户浏览该目录时，就会加载 C:\box.dll 文件，图 3 为修改后的 Ink 文件。

Ink 的目标文件存放在 Shell Item Id List 的 SHITEMID 结构里面，这个结构按照层来表示一个目标的，每一层就是前面讲述的一个 SfflTEMID 结构。图 3 显示 Ink 文件中，第一层是

00000040
14 00
00000050 F 50 E0 4F D0 20 EA 3A 69 10 A2 D8 08 00 28 30
00000060 30 9D

14 00 代表长度，后面的 16 字节是“我的电脑”的 GUID{20D04FE0-3AEA-1069-A2D8-08002830309D}。第二层是

00000060 14 00 2E 00 20 20 EC 21 EA 3A 69 10 A2 DD
00000070 08 00 28 30 30 9D

14 00 代表长度，后面的是 “控制面板” 的 GUID{ 21EC2020-3 AEA-1069-A2 DD-08002830309D}。第三层就是后面长度为 OxA2 的目标文件，图 3 中显示的 Shellltem Id List 所指向的文件就是：我的电脑->控制面板->C:\box.dll。

实验第三步是提供一个恶意的 dll，把一个写好的 box.dll 放入 C 盘，我们的例子调用此 dll 文件就会弹出一个对话框，浏览 Ink 文件所在的快捷方式，系统就会加栽这个 box．dJJ。

图 4 是测试用的一个简单的 dll 程序代码，该 dll 文件有一个入口函数 DIIMain，当 dll 文件被载入内存后就会先执行 DIIMain 函数，所以把触发木马或病毒的程序放在 DIIMain 适当的位置，当用户浏览快捷方式的目录时就会激活恶意代码。

实验结果如图 5，当仅仅浏览快捷方式所在的目录时就会弹出一个 hello 的对话框，这也证实了前面对于漏洞的分析。

我们将测试用的 Ink 文件上传到 VirusTotal 上检测其绕过反病毒软件的能力，VirusTotal 是一款免费提供对可疑文件进行分析 Web 服务，通过各种知名反病毒引擎，对所上传的文件进行检测，以判断文件是否被病毒，蠕虫，木马，以及各类恶意软件感染。

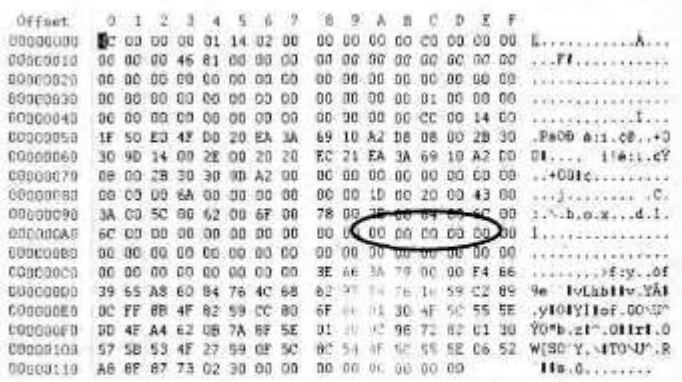

图 3　修改过的 lnk 文件

```
#include <stdio.h>
#include <windows.h>

BOOL APIENTRY DllMain(HANDLE hModule, DWORD ul_reason_for_call,
LPVOID lpReserved)
{
switch( ul_reason_for_call )
{
case DLL_PROCESS_ATTACH:
    MessageBox(NULL,"成功加载box.dll","Greetings",MB_OKCANCEL);
 break;}
case DLL_THREAD_ATTACH:
case DLL_THREAD_DETACH:
case DLL_PROCESS_DETACH:
break;
}
return TRUE;
}
```

图 4　测试用 box.dll 的代码

图 5　测试结果

4、总结

Windows Ink 漏洞不需要用户运行任何程序，仅仅浏览其所在目录就可触发，其影响范围比较广泛。随着微软发布了官方的补丁，加上众多安全软件对 Ink 病

毒的查杀，预计这个漏洞和利用此漏洞的病毒可能很快会消失。分析该漏洞的本质，其利用了 Ink 文件的解析过程和 dll 文件装载过程的安全检查不够的缺陷，dll 文件的安全装载并不是一个新问题，Ink 漏洞只不过是发现了该缺陷的一个新应用场合，所以加强主动性防御才是根本性解决方法。