Stunex病毒的传播所利用的漏洞及对策

冯 旭

（重庆电子工程职业学院 重庆 401331）

[摘 要] Stuxnet是一个非常著名的病毒，其具有复杂的结构和多样的攻击方式。本文将介绍其传播和攻击使用到的4个漏洞，详细介绍Stuxnet如何利用这些病毒，并分别介绍针对某个漏洞的解决方案。

[关键词] 病毒；漏洞；Stuxnet

本文将讨论Stuxnet的感染策略。实际上不管是感染步骤或提升权限步骤，Stuxnet都需要利用Microsoft的漏洞。本章将分为四个部分，包括四个漏洞。前两个用于感染主机，后两个用于完成提权。图1显示了这些漏洞用于什么目标：

这个漏洞可以通过可移动设备来感染主机。在大多数情况下，Stuxnet都是工厂的本地网络，很少连接到Internet。

1、MS10-046漏洞

此漏洞位于Microsoft产品的·LNK文件中。Microsoft安全咨询CVE-2010-2568包含此漏洞利用细节的链接。Windows .LNK文件在通过Windows浏览器展示时，则将从CPL文件加载.LNK文件的图标。如CPL文件表示一个动态链接库，加载图标表示某些dll文件将被加载，这是该漏洞的关键。

感染了Stuxnet蠕虫的USB闪存驱动器，您可以找到六个文件：

1.快捷方式副本到.link；

2.快捷方式副本到.lnk的副本；

3.快捷方式副本副本的副本。

4.复制到.lnk的快捷方式副本的副本的副本；

5.～WTR4141.TMP；

6.～WTR4123.TMP。

前四个文件是.LNK文件，它们的功能相同，但是每个都定义了到～WTR4141.tmp文件的不同的路径。

2、MS10-046漏洞对策

如上所述，该漏洞会导致恶意代码在加载图标的过程被执行。关键是调用LoadLibraryW（）不检查加载的dll文件。此漏洞的一种对策是在函数LoadLibraryW（）之前或内部添加检查。但是，这是微软的代码，我们无能为力除了下载官方的补丁。

我发现的另一种方法是在函数调用开始之前检查.LNK文件。如提到了“文件位置信息”，则专门指出了应该从何处加载库。解决方案是检查该字段。首先，创建白名单以限制可以加载库的位置。然后比较“文件位置”中的信息白名单，如果位置在列表中，就执行其余操作；如果不在列表中，则停止并向屏幕发送警告。

3、MS10-061漏洞

攻击分为两个阶段：第一阶段是复制Stuxnet吸管和其他需要的档案到Windows \ System32 \ winsta.exe和Windows \ Sytem32 \ wbem \ mof \ sysnullevnt.mof；第二阶段是执行滴管。

第一阶段使用的漏洞是MS10-061。客户端可以向主机发送请求，要求主机打印文档。在要求中包含要打印文件的信息：所有者，页面，大小，提交时间和输出端口。

在攻击的第二阶段，需要sysnullevnt.mof文件。这样的文件是通常针对提供者，创建或注册WMI的事件。在某些情况下winsta.exe将被执行以感染主机。

4、MS10-061漏洞对策

如上所述，应对此漏洞的对策是Microsoft的补丁程序，用于检查OutputFile参数。与添加的补丁不同的方式是在打印过程中检查，在MULVAL中可以实现的可能方法是在客户端和主机之间添加过滤器。该过滤器将检查打印请求，并将客户端的权限和OutputFile参数与一个列表匹配。当在列表中找不到请求的组合的时候，阻止该请求。另一种方法是创建一个作业，当诸如将数据写入系统级文件之类的行为发生时向管理者发出警告并要求管理者根据情况做出决定。

5、MS10-073漏洞

感染主机是Stuxnet蠕虫应完成的第一步。但是在某些情况下该恶意软件将无法安装自身或执行某些特殊操作。然后下一步是完成权限升级。

如果出现MS10-073漏洞，则该恶意软件会在它没有权限自行安装的时候尝试时利用。易受攻击的系统是Microsoft Windows 2000和未修补的Windows XP。

6、MS10-073漏洞对策

Microsoft对该漏洞的补丁程序是添加检查以防止NLSFEProcType字段VK_F结构超出_aNLSVKProc表的边界。但是这个补丁仍在Microsoft的代码内部，无法在MULVAL中表达。但是，我们可以从网络更高层来考虑对策。

7、MS10-092漏洞

此漏洞与Windows操作系统中的Task Scheduler Service有关。Stuxnet可以利用此漏洞将权限提升到系统级别。

8、MS10-092漏洞对策

该漏洞的对策是替换原来的算法CRC32，使用已知的能够抵抗碰撞的哈希算法。

参考文献

[1]Falliere, N., Murchu, L.O., & Chien, E.（2011）.W32.stuxnet dossier.White paper, Symantec Corp., Security Response.

[2]Ou, X., Govindavajhala, S., & Appel, A.W.（2005, August）.MulVAL: A logic-based network security analyzer.In 14th USENIX Security Symposium（pp.1-16）.

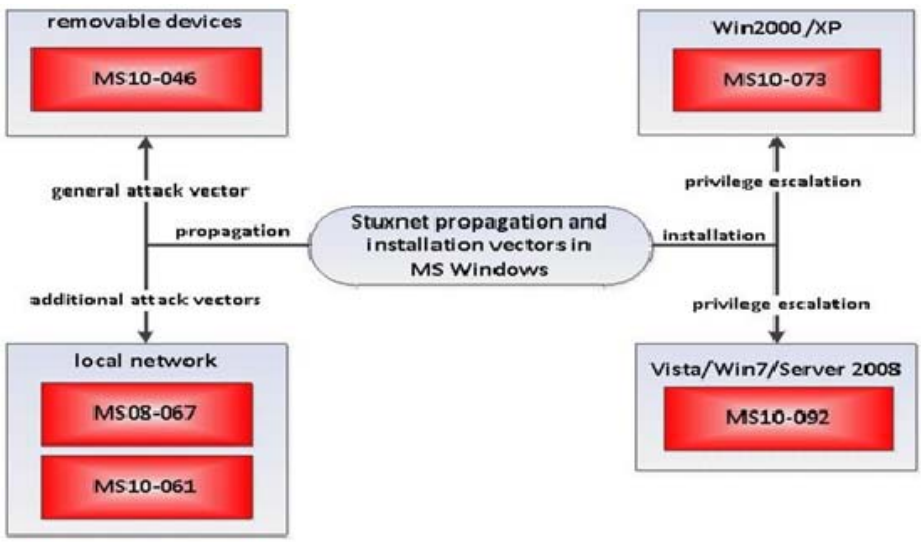

图 1