专家教你手工处理lpk.dll病毒

2011-10-21 15:52  中证网    [我要评论(0)](http://news.newhua.com/news/2011/1021/135049.shtml#comment)

字号：**T**|**T**

华军资讯10月21日消息 安全问题是个人用户不容忽视的问题之一，本文将为大家带来流行病毒“lpk.dll病毒”的手工查杀方法，希望给用户带来利用杀软和专杀对付病毒问题之外的思路，**详细如下文：**

lpk.dll病毒相信大家并不陌生，此类病毒已经流行有一段时间了，对应的专杀工具也可以从网上搜索下载到，这足以表明该病毒的广泛性及危险性。

**本文对该病毒进行了行为分析，并向您呈现了手动处理的全部过程。**

瑞星专家指出：并不是所有lpk.dll文件都是病毒。正常系统中本身就会存在lpk.dll文件，它是微软操作系统的语言包，位于C:\WINDOWS\system32和C:\WINDOWS\system32\dllcache目录下。

lpk.dll病毒的典型特征是感染存在可执行文件的目录，并隐藏自身，删除后又再生成，当同目录中的exe文件运行时，lpk.dll就会被Windows动态链接，从而激活病毒，进而导致不能彻底清除。

所以当发现磁盘很多文件夹中都存在lpk.dll文件时，那么基本可以肯定您的计算机已经中招了。lpk.dll病毒是个恶意后门病毒，计算机染毒后会在后台下载更多恶意程序，可造成用户机器被远程控制、资料被盗等状况。很多用户在发现电脑中招后会习惯性地重装系统，但重装系统并不能清除非系统盘目录下的lpk.dll文件，因此当运行其他盘符目录下的可执行文件时又会激活病毒，再次全盘感染，令人十分头疼。

**病毒现象**

1) 通过文件夹选项的设置显示出所有隐藏文件，包括操作系统文件，然后全盘搜索lpk.dll，这时会发现很多目录下都存在lpk.dll文件，大小一致，属性为隐藏。



图1：病毒现象：全盘搜索发现很多目录下存在有LPK.dll文件，且大小一致，属性为隐藏。

注意：全盘搜索lpk.dll时要注意勾选“搜索隐藏的文件和文件夹”，如下图所示：



图2：搜索时需勾选“搜索隐藏的文件和文件夹”选项

2) C:\Documents and Settings\Administrator\Local Settings\Temp目录下生成许多tmp格式的文件，大小一致，命名有一定规律。从文件后缀来看，这些文件似乎是临时文件，但其实是PE格式，并不是普通的tmp文件。

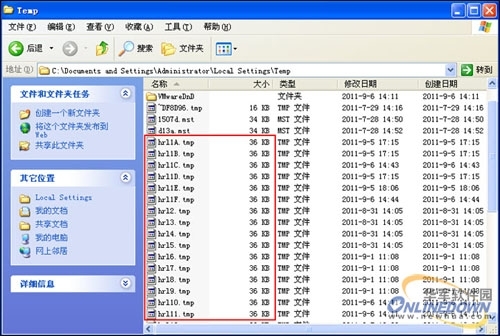


图3：病毒现象：众多有明明规范的tmp格式文件，且大小一致。

3) 使用XueTr查看系统进程，explorer.exe等很多进程下加载了lpk.dll。



图4：病毒现象：很多进程下都加载了lpk.dll。

**处理方法**

1) 把之前搜索到的lpk.dll文件全部删除(不包括C:\WINDOWS\system32和C:\WINDOWS\system32\dllcache目录)。删除C:\Documents and Settings\Administrator\Local Settings\Temp目录下大小为36KB的hrlXX.tmp文件。

2) 某些lpk.dll删除时会出现系统报错，如下图。

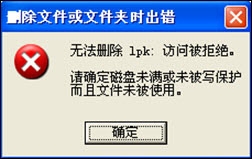


图5：删除某些lpk.dll文件时会报错，是因为该病毒文件已经被激活调用。

这是由于病毒文件已经被激活调用，普通方式无法直接删除。这时通过XueTr可以看到删除报错的lpk.dll正挂在系统正在运行的进程下，逐一找到正加载的lpk.dll，右键选中将其删除。



图6：对于这些已经被激活调用的lpk.dll，可使用工具将其从进程中删除。

3) 在用XueTr逐一检查系统进程的过程中，发现其中一个svchost.exe进程下加载了一个十分可疑的模块文件hra33.dll，且无数字签名。

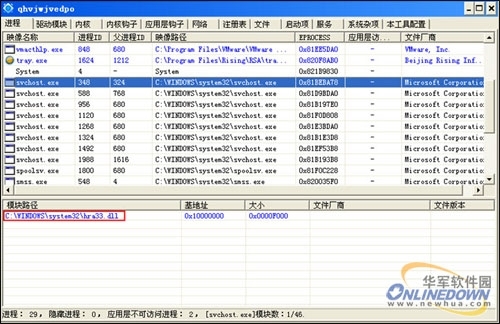


图7：某个svchost进程下加载了可疑dll模块。

右键选中查看模块文件属性，可以看到该文件大小也是43KB，与lpk.dll相同，创建日期也与lpk.dll一致。另外有没有觉得这个文件名很熟悉?再回想一下会发现该文件命名与temp目录下的hrlXX.tmp文件命名方式有异曲同工之处。综上所述，已经可以确定该文件与lpk.dll性质相同，直接用XueTr删之。



图8：仔细查看该模块详细信息，可确定其为病毒文件。

4) 上述删除操作完成后，再全盘搜索一次，会发现刚刚删除的lpk.dll病毒文件又出现了，真是“阴魂不散”。很明显系统中还存在残余病毒体不断释放lpk.dll文件，还需要进一步检查将其彻底清除。通过XueTr检查系统当前服务，发现一个很可疑的服务，对应的映像文件kkwgks.exe无数字签名。

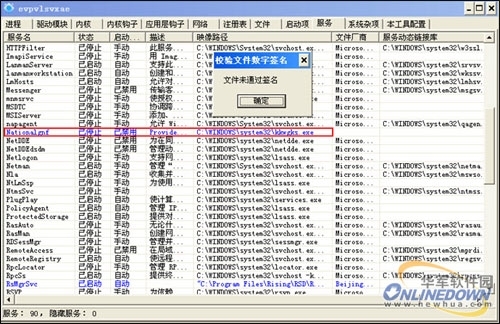


图9：再次检查系统服务，可发现这个服务对应的文件没有数字签名。

查看kkwgks.exe文件属性发现该文件创建时间与lpk.dll一致，且文件大小与Temp目录下的hrlXX.tmp文件相同，十分可疑，直接将其删除。



图10：具体查看该程序，可发现该文件为病毒。

5) 删除kkwgks.exe文件即结束了病毒服务，还需要执行上面步骤1-3的删除操作，把再次释放的lpk.dll等文件全部清除，然后重启电脑再全盘搜索检查一遍，原来的病毒文件都不复存在了。

**病毒行为分析**

经过了上面的手动处理过程后，可以逆向思维简单分析一下病毒行为如下。

1) 病毒运行后会把自己拷贝到系统system32目录下以随机数命名(就是上面的kkwgks.exe)，并创建一个名为Nationalgnf的服务。

2) 新的服务启动后，利用特殊手段让病毒映像替换svchost.exe，进程中看到的还是svchost.exe，似乎没有什么异样，但此时病毒已经将自己隐藏在svchost.exe里运行，病毒在这里完成的功能包括：

a. 完成病毒所有的后门任务;

b. 在系统system32目录下生成hraXX.dll(XX是生成的随机名);

c. 在系统临时文件目录下不断释放hrlXX.tmp文件(XX是生成的随机名)，这里的hrlXX.tmp文件其实是system32下kkwgks.exe文件的备份，非常危险，作用是恢复system32下被删除的exe病毒文件;

d. 在存在可执行文件的目录下生成假的lpk.dll，属性为隐藏，当同目录下的exe运行时会自动加载，激活病毒。

**总结**

经过上述分析处理的过程，相信大家对于lpk.dll病毒已经有了一定的了解。虽然这类病毒变种较多、感染性强、危险性高，但若是真遇上了也不必惊慌，网上可以搜索下载到它的专杀工具，多数杀毒软件也已将其入库，只要借助合适的工具，通过合理的途径，不难解决。