**恶意代码分析与防治技术实验报告**

**Lab1**

1. **实验环境**

Windows7，VMWARE，Windows11

1. **实验工具**

STRINGS, IDAPro,PEVIEW，EXEInfo，YARA

1. **实验内容**

Lab 1-1

1. Upload the files to http://www.VirusTotal.com/ and view the reports. Does either file match any

existing antivirus signature?

Lab01-01.exe：

Lab01-01.dll：

可以看出，这两个文件都已被一些安全软件识别为病毒，匹配到了已有的反病毒软件特征。

2. When were these files compiled?

查看 Virus Total 给出的报告，可以查到 PE 头的相关信息，其中包含文件的编译时间。

从而知道，Lab01-01.exe 的编译时间为 2010-12-19 16:16:19；Lab01-01.dll 的编译时间为

2010-12-19 16:16:38。

3. Are there any indications that either of these files is packed or obfuscated? If so, what are these

indicators?

使用查壳工具 PEid 扫描文件，结果如下，可见没有加壳和混淆。

Lab01-01.exe： Lab01-01.dll：

4. Do any imports hint at what this malware does? If so, which imports are they?

查看 Virus Total 给出的报告，可以知道文件中包含了哪些导入函数。

Lab01-01.exe：

其中值得关注的是 FindFirstFileA、FindNextFileA 和 CopyFileA，这三个函数配合使用，可以搜

索文件系统里的所有文件并复制。

Lab01-01.dll：

其中 CreateMutexA 函数用于创建一个互斥对象，可以和 OpenMutexA 一起操作一个互斥对

象；CreateProcess 函数创建并启动一个新进程，如果恶意软件创建一个新的进程，新的流程

需要分析；Sleep 函数可以使计算机程序进入休眠。由此可以猜想，这个 DLL 会创建一个互

斥变量以保证一个资源同时只能被一个进程使用，如果这个互斥变量被锁，则其他的进程就

执行 Sleep 函数等待。

而 WS2\_32.dll 提供联网功能，该恶意软件很可能要执行网络相关的任务。

5. Are there any other files or host-based indicators that you could look for on infected systems?

使用 IDA 分析文件 Lab01-01.exe，观察 Strings 窗口，如下：

出现了 kerne132.dll，这里企图用 1(one)混淆了 l，说明这台主机已经被感染了。

此外，在下一行还会发现这个.exe 在运行时会导入 Lab01-01.dll，在上一题中已经分析了这

个.dll 文件可能出现的恶意行为。

6. What network-based indicators could be used to find this malware on infected machines?

使用 IDA 分析文件 Lab01-01.dll，观察 Strings 窗口，如下：

可以发现这里有一个 ip 地址，而在第四题分析导入函数时已经知道 WS2\_32.dll 提供联网功

能，该恶意软件很可能要执行网络相关的任务，因此可以推测是要与这里提到的网址联网通

信。

7. What would you guess is the purpose of these files?

通过以上分析可以推测，.dll 文件可能是一个后门，.exe 文件是用来安装与运行.dll 文件的。

Lab 1-2

1. Upload the Lab01-02.exe file to http://www.VirusTotal.com/ and view the reports. Does it match

any existing antivirus signature?

Lab01-02.exe：

可以看出，这个文件都已被一些安全软件识别为病毒，匹配到了已有的反病毒软件特征。

2. Are there any indications that this file is packed or obfuscated? If so, what are these indicators? If

the file is packed, unpack it if possible. 使用查壳工具 PEid 扫描文件，结果如下，说明该文件已经被加壳了。

使用 Kali 的 upx -d 命令脱壳，脱壳成功！

3. Do any imports hint at this program’s functionality? If so, which imports are they and what do

they tell you?

将脱壳后的 Lab01-02.exe 文件上传到 Virus Total 网站上，得到与脱壳前不同的导入函数，如

下：

推测该程序将有开启或创建服务、联网等行为。

4. What host- or network-based indicators could be used to identify this malware on infected

machines?

使用 IDA 分析文件 Lab01-02.exe，观察 Strings 窗口，如下：

有一些可疑字符串和可疑网址。

Lab 1-3

1. Upload the Lab01-03.exe file to http://www.VirusTotal.com/ and view the reports. Does it match

any existing antivirus signature?

Lab01-03.exe：

可以看出，这个文件都已被一些安全软件识别为病毒，匹配到了已有的反病毒软件特征。

2. Are there any indications that this file is packed or obfuscated? If so, what are these indicators? If

the file is packed, unpack it if possible. 使用查壳工具 PEid 扫描文件，结果如下，说明该文件已经被加壳了。

使用脱壳工具 LinxerUnpacker 进行壳特征脱壳，脱壳成功！

3. Do any imports hint at this program’s functionality? If so, which imports are they and what do

they tell you?

将脱壳后的 Lab01-03.exe 文件上传到 Virus Total 网站上，得到与脱壳前不同的导入函数，如

下：

该程序可能将有组件对象模型 COM、联网等相关操作。

4. What host- or network-based indicators could be used to identify this malware on infected

machines?

使用 IDA 分析文件 Lab01-03.exe，观察 Strings 窗口，如下：可以看到一些可疑字符串。

Lab 1-4

1. Upload the Lab01-04.exe file to http://www.VirusTotal.com/ and view the reports. Does it match

any existing antivirus signature?

Lab01-04.exe：

可以看出，这个文件都已被一些安全软件识别为病毒，匹配到了已有的反病毒软件特征。

2. Are there any indications that this file is packed or obfuscated? If so, what are these indicators? If

the file is packed, unpack it if possible. 使用查壳工具 PEid 扫描文件，结果如下，说明该文件没有被加壳或混淆。

3. When were these files compiled?

查看 Virus Total 给出的报告，可以查到 PE 头的相关信息，其中包含文件的编译时间。

因此这个文件的编译时间为 2019-08-30 22:26:59。（但我认为这是个不可信的时间）

4. Do any imports hint at this program’s functionality? If so, which imports are they and what do

they tell you?

该程序可能将有操作权限、创建可执行文件并运行、联网等行为。

5. What host- or network-based indicators could be used to identify this malware on infected

machines?

使用 IDA 分析文件 Lab01-04.exe，观察 Strings 窗口，如下：可以看到一些可疑字符串。其中

字符串”\\system32\\wupdmgr.exe”表示这个程序会在这个位置创建或者修改文件。

6. This file has one resource in the resource section. Use Resource Hacker to examine that resource, and then use it to extract the resource. What can you learn from the resource?

1. **实验心得**

**本次实验，我熟悉了对恶意代码分析工具有了更深入的理解。同时得到了充分的锻炼，并开始对本门课程的实验开始得心应手，做实验的速度越来越快了。**