【sample 样本】分析报告

一、概述

作者：dyj
样本来源：教师机
时间： 2017-11-23

二、名词解释

OEP:程序入口点

三、相关文件

样本文件：sample.exe.v（UPX 壳）
样本释放文件 1：sampleSrv.exe.v（sample.exe 脱壳后）
样本释放文件 2：DesktopLayer.exe.v（主体）
样本注入浏览器 dll：noname.dll
样本在默认浏览器下创建的数据文件：dmlconf.dat

四、行为预览

样本名称:sample.exe

样本类型：未知

样本大小：55.0 KB(56320 字节)

传播方式:通过感染本地磁盘和和移动磁盘的 PE 格式文件和 html 格式文件进行传播。

样本具体行为：

1. 运行样本，样本在同级目录下释放子程序：samplesrv.exe

2. 样本创建进程启动子程序 samplesrv.exe

3. 子程序 samplesrv.exe 在机器上的七个备选路径下顺序选择一个存在的路径创建“Microsoft”文件夹，并释放 DesktopLayer.exe。同时通过注册表找到默认浏览器路径，并在该路径下检测是否存在其浏览器。

4. 母体程序 sample.exe 持续修改其他进程的内存，并在其他进程中创建线程，作用未知。

5. samplesrv.exe 创建进程启动它释放的子程序：DesktopLayer.exe

6. DesktopLayer.exe 通过 hook CreateProcessA 中的 zwWriteVirtualMemory 函数将样本 dll：noname.dll 注入到第三步拿到的浏览器中，修改默认浏览器的程序入口点到注入代码，使得浏览器只是一个占据地址空间的外壳，。

注入代码具体行为：

注入代码首先会创建互斥体：”KyUffThOkYwRRtgPP”，用来保证只有一个样本在运行。然后初始化网络环境，接着获取磁盘信息，版本信息，机器环境的数据，然后创建 6 个线程，由这 6 个线程完成核心工作。

线程 1：以 1 秒钟为间隔查看注册表项：

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit
```

检查释放样本样本 desktoplayer.exe 的路径是否存在。如果不存在就将该路径添加，目的是实现开机自启的功能

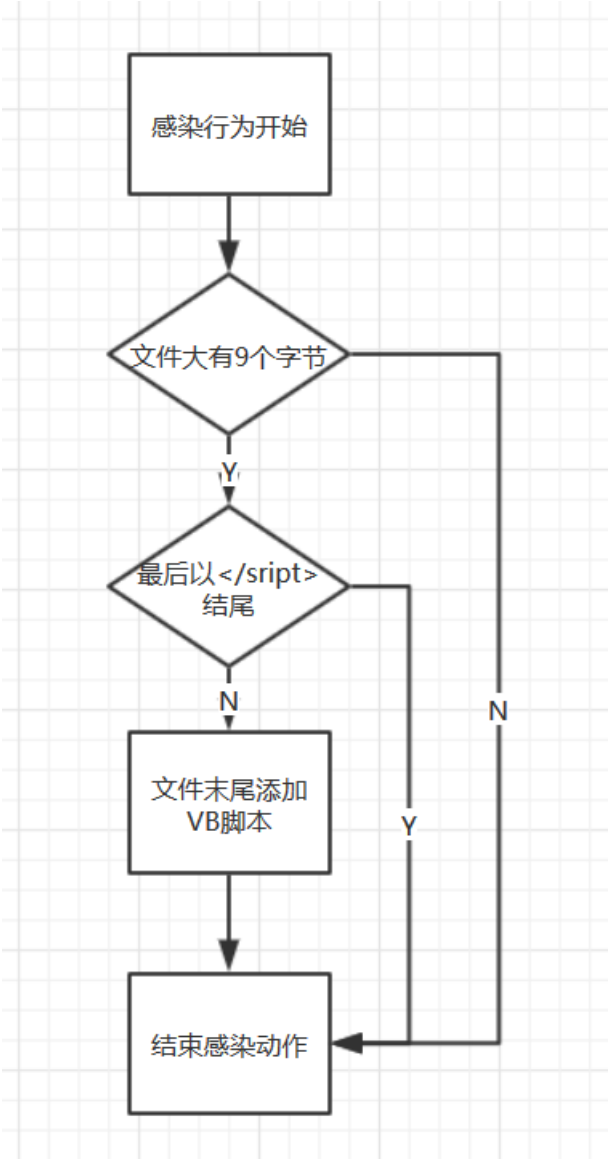
线程 2：与 google.com:80、bing.com:80、yahoo.com:80 测试是否连通，如果连通就保存两次连通的时间差。

线程 3：在默认浏览器的目录下创建文件 dmlconf.dat，以 1 分钟为间隔，项内写入 16 个字节的数据，前 8 个字节是系统时间，中间 4 个字节是线程 2 拿到并保存的连通时间差，最后 4 个字节作用未知，一直是 0。

线程 4：以 10 分钟为间隔，向 fget-career.com:443 发送之前拿到的有关本机的相关信息。

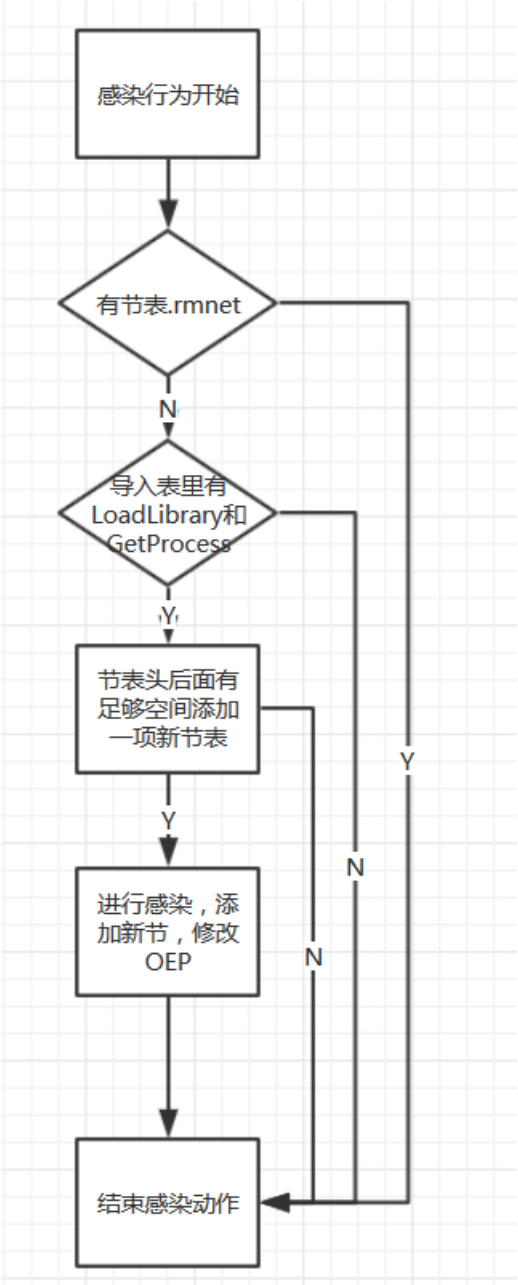
线程 5：实现感染本地磁盘和移动磁盘。

感染 html 文件方式 ：首先检测文件的最后是不是</SCRIPT>，如果是的话，说明已经被感染了，跳过感染步骤，如果没有，则在文件末尾添加 VB 脚本，脚本的功能是执行 PE 文件。



感染 PE 格式文件的方式：

首先查看导入表里有没有函数 LoadLibraryA 和 GetProcessAddress，有的话获取 Rva，没有就不感染。查看节表后面是否存在再添加一个节表的空间，有就添加一个新节名称为“.rmnet”，没有就不感染，重定位 LoadLibraryA 和 GetProcessAddress，之后进行使用，在末尾添加新节”.rmnet”，并更改程序 OEP 到新的节，



.

线程 6：遍历磁盘文件，以 10 秒钟为间隔，当判断是移动磁盘的时候，判断根目录下是否存在”autorun.inf”文件，且该文件小于等于 3 个字节，文件头标志不为”RmN”，满足条件进行感染。

五、清理方式

1. 通过注册表拿到默认浏览器路径，使用"KyUffThOkYwRRtgPP"特征创建互斥体，若已存在，则遍历进程，关闭"DesktopLayer "和有关默认浏览器的相关进程。

2. 在以下 7 个目录下检测是否存在”Microsoft”文件夹，如果找到，直接删除该文件夹以及文件夹中的内容。

1:"C:\Program Files\ ";
2:"C:\Program Files\Common Files\ ";
3:"C:\Documents and Settings\Administrator\ ";
4:"C:\Documents and Settings\Administrator\Application Data\ ";
5:"C:\WINDOWS\system32\ ";
6:"C:\WINDOWS\ ";
7:"C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\";0

3. 读取注册表项：

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit
```

如果有 desktoplayer.exe 的启动路径，删除。

4. 遍历全盘的 html，exe，dll 文件。

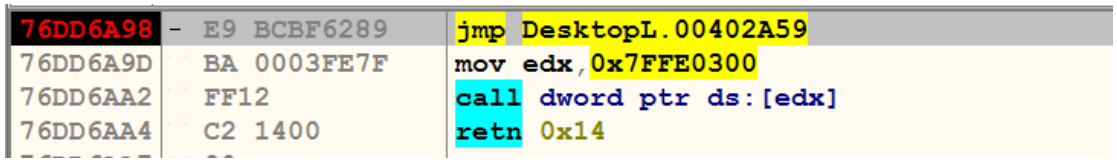
对于 HTML 文件，若文件最后 9 个字节是”</sript>”，则找到文件中的“<SCRIPT Language=VBScript>”，删除它和它之后的内容。

对于 PE 格式的文件，查看节表中若存在”.rmnet”节，则删除节表中的.rmnet 节信息，删除文件末尾的.rmnet 节中所有数据，修改节个数，修改文件 OEP。

对于移动磁盘，检查"autorun.inf"的文件头是否为：RmN，如果是的，修复其中的 exe 和 html。

六、正文

sample.exe 脱壳后的程序，samplesrv.exe 在 zwWriteVirtualMemory 下钩子，跳到主模块执行代码



当调用 CreateProcessA 的时候，来到 hook 的地址，跳转到主模块进行对默认浏览器的注入行为

注入行为：在 地址 00402054 第一次申请堆空间 20010000，然后马上释放掉这个堆空间。然后在进程句柄为 b8 的进程里开辟 20010000 这个地址的空间。

接着再次在本进程申请 20010000 空间，向里面写入注入的 pe 头，大小为 D00，接着把本进程 20010000 空间内的 pe 头数据写入默认本进程的 20010000 空间，再分两次把节表数据写入，这样就将一个映射好的 dll 写到内存，再一次性把 PE 文件写入浏览器的 20010000 空间。

ie 被修改入口点后执行 dll 中的代码。