【原创】一份通过IPC和lpkdll感染方式的病毒分析报告

zzzhhh / 2017-06-05 14:13:20 / 浏览数 4158 安全技术 漏洞分析 顶(0) 踩(0)

样本来自52pojie论坛，从事过两年渗透开始学病毒分析后看到IPC$真是再熟悉不过。

1．样本概况

1.1 样本信息

病毒名称：3601.exe
MD5值：96043b8dcc7a977b16a2892c4b38d87f
病毒行为： 自删除，感染压缩包（zip、rar）、释放lpk.dll文件

1.2 测试环境及工具

操作系统：win7 32位
操作工具：火绒剑、OD、IDA、MD5工具

1.3 分析目标

分析此病毒的恶意行为和生成相关文件。

2．具体行为分析

2.1 主要行为

病毒首先使用RegOpenKeyExW函数读取注册表中【HKEY_LOCAL_MACHINE\system\CurrentControlset\services\Ghijkl Nopqrstu Wxy】
这个键项；如果键项不存在，则创建病毒的系统服务，流程图大体如下：

有【Ghijkl Nopqrstu Wxy】这个键项的时候，病毒的行为流程图如下：

如果键项存在则进入一个创建服务的函数，做了以下4个步骤：
1、检查互斥体，防止多开；
2、释放、加载资源文件C:\windows\system32\hra33.dll；
3、开启四个线程（IPC$破解、收集主机操作系统与网络信息、CPU字符串和主频率描述）
其中线程A是用于IPC$密码破解，感染同局域网内其他主机。
线程B、线程C、线程D功能一致，连接的域名不一样。
感染模块基本流程

2.1.1 恶意程序对用户造成的危害(图)
在rar、zip、exe中释放一个lpk.dll的文件，运行exe后加载病毒程序图1 感染压缩包

图2 有exe的目录下释放lpk.dll

2.1.2 恶意程序在系统中生成的文件
(1)权限相关()
1.创建服务
图3 创建的服务名
2.生成文件图4 生成的病毒exe

图5 生成的病毒DLL

3.创建注册表
图6 注册表所增加的注册表键值
(2)服务/广播
连接域名
1 sbcq.f3322.org2 www.520123.xyz
3 （加密）www.520520520.org:9426

2.2 恶意代码分析

2.2.1 加固后的恶意代码树结构图

1.使用PEID检查出病毒程序采用upx壳压缩图7 PEID查壳为upx
2.连接域名使用base64加密图8 连接域名为base64加密

2.2.2 恶意程序的代码分析片段

病毒首先使用RegOpenKeyExW函数读取注册表中有没有【HKEY_LOCAL_MACHINE\system\CurrentControlset\services\ Ghijkl Nopqrstu Wxy】这个键项；图9 判断键项-OD反汇编代码注释
如果没有这个键项的时候则进入一个创建服务的函数，做了以下4个步骤：1、复制自身到C:\windows；2、将【C:\windows\随机文件名.exe】注册服务；3、创建注册表键
图10 IDA-复制自身到C:\windows
图11 OD反汇编-堆栈窗口-随机生成文件名
将生成的文件作为系统服务对象创建，系统服务名为【Ghijklmn Pqrstuvwx Abcdefg Ijklmnop Rst】，代码片段如下：图12 IDA伪C代码-创建系统服务
检查病毒是否已经在机器上运行过，创建注册表键项：【HKEY_LOCAL_MACHINE\system\CurrentControlset\services\Ghijkl Nopqrstu Wxy】图13
IDA伪C代码-创建注册表键项
病毒运行后会做删除自身的处理，首先获取当前进程路径、文件短路径、CMD.exe路径。用shellexecute()函数删除自身。然后设置进程的执行级别使自身有足够的时间从内
图14 IDA伪C代码-删除自身

如果键项存在则进入一个创建服务的函数，做了以下步骤：

1、检查互斥体，防止多开；

2、释放、加载资源文件C:\windows\system32\hra33.dll；

3、开启三个线程（IPC$破解、收集主机操作系统与网络信息、CPU字符串和主频率描述）

检查互斥体Ghijkl Nopqrstu
Wxy是否存在，如果已经存在时退出程序；183对应着宏定义ERROR_ALREADY_EXISTX。然后释放自定义资源，将自定义资源命名为hra33.dll。

图15 检查互斥体与释放自定义资源

释放自定义资源文件hra33.dll 到C:\windows\system32\hra33.dll,改写文件的PE头，让其成为PE文件。代码片段如下:

图16 释放自定义资源，改写PE头为MZ

创建了四个线程，分别命名为线程A、线程B、线程C、线程D。代码片段如下：

图17 创建四个线程

线程A通过IPC$共享用内置的弱口令字典破解感染同局域网内其他主机。将自身复制到其他主机的共享后，使用at(定制计划任务)的方式执行。

图18 IPC$破解

线程B、线程C、线程D功能大体一致，连接的域名不一样。获取操作系统版本号、
CPU字符串和主频描述、内存、网络流量信息创建套接字发送给控制端，然后等待接收控制端发过来的指令，执行相关的操作。

主要功能

1)连接域名

2)获取操作系统版本号、 CPU字符串和主频描述

3)实现功能-（下载文件、更新服务端、打开网页）

线程B 进入回调函数后,首先进入连接域名函数，创建网络套接字后所连接的域名为:sbcq.f3322.org，代码片段如下：

图19 IDA伪c代码-创建网络套接字连接sbcq.f3322.org

当连接域名成功，代码向下执行会调用搜集操作系统信息的函数，加载hra33.dll。

图20 OD反汇编代码-调用搜集操作系统信息函数

使用GetVersionExA()函数获取操作系统版本号、 CPU字符串和主频描述的代码片段如下：

图21 IDA伪C代码-获取操作系统版本号

图22 IDA伪C代码-获取CPU字符串和主频描述

利用Send（ ）函数发送消息通知控制端已经加载hra33.dll成功，代码片段如下：

图23 IDA伪C代码-加载hra33.dll后发送0XB0给控制端

根据控制端传送过来的命令执行相关的操作。定义了URLDownloadToFileA()、winexec()函数，会下载指定url的文件保存到本地中,初步推断是为了实现下载自定义文件的功

图24 定义UrlDownloadToFileA函数

当接收的参数大于6个字节时，接收到的值等于0x10，从接收到的URL地址处下载文件保存到本地的临时目录，文件名由GetTickCount()函数随机生成，代码片段如下：

图25 接收命令后下载文件

接收到的值等于0x12时候，创建互斥体【Ghijkl Nopqrstu
Wxy】，随机生成文件名。把控制端发送过来的url地址下载保持成本地文件，关闭病毒创建的名称为【Ghijkl Nopqrstu
Wxy】服务，删除注册表【HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ Ghijkl Nopqrstu Wxy
】键项，删除病毒进程的文件自身。将新的文件重新注册成为系统服务。初步判断这是一个更新自身服务端的功能。代码片段如下：

图26 下载新的病毒文件

图 27 删除原有的服务和注册表

接收到0x14的命令时调用ShellExecute函数将控制端发送过来的控制数据作为IE程序的指定启动参数，打开iexplore.exe进程。

图28 IDA伪C代码-自带IE打开网页

其他参数还接收了0x2、0x3、0x4、0x5,其中0x2/0x4/0x5未发现有实质的操作，接收到0x3的控制指令后，线程的作用是利用文件路径C:\WINDOWS\system32\Program
Files\Internet Explorer\iexplore.exe下的iexplore.exe程序向网址发送GET形式的Http数据请求包。代码片段如下：

图29 接收命令参数

图30 发送GET形式的Http数据请求包

线程C的功能与线程B大体一致，连接的域名为：

图31 连接域名www.520123.xyz

线程D的连接域名使用了加密函数。

图32 IDA伪C代码-线程D加密函数

在OD载入后动态执行时结果被解密出来。

图33 OD反汇编代码-连接域名www.520520520.org:9426

Hra33.dll功能是通过加载lpk.dll对其他exe和压缩包进行感染。代码片段如下：

图34 hra33.dll入口点函数

遍历文件目录，如果找到.exe的目录就把lpk.dll放到该目录下。代码片段如下：

图35 感染函数

感染zip/rar的方式主要还是利用winrar.rar的rar.exe（命令行工具），首先搜索压缩包内有没有lpk.dll这个文件，然后如果有.exe，就将压缩包重新解压添加lpk.dll文件再压

图36 感染压缩文件

3．解决方案

3.1 提取病毒的特征，利用杀毒软件查杀

Ghijkl Nopqrstu Wxy 对应hex 4768696A6B6C204E6F70717273747520577879

提取特征码的方式

1、利用哈希值作为病毒特征

2、选取病毒内部的特征字符串

3、选取病毒内部的特色代码

4、双重校验和

3.2 手工查杀步骤或是工具查杀步骤或是查杀思路等。

1、停止【Ghijkl Nopqrstu Wxy】名称的服务

2、删除【Ghijkl Nopqrstu Wxy】键项的注册表

3、删除【C:\windows\system32\hra33.dll】文件

4、清空除了C:\Windows\System32\lpk.dll外，所有zip、rar、exe下的lpk.dll文件

黑客交流通常用IDA就够了。。这是IDA的分析文件和OD注释文件，还有提取出来的hra33.dll

链接: http://pan.baidu.com/s/1bps2sn9 密码: gipa
压缩包解压密码为：52pojie

同时这也是我在52pojie拿到的第一篇精华帖。

点击收藏 | 0 关注 | 0
上一篇：两种钓鱼方法分析 下一篇：【原创】秒抢红包锁屏样本手动查杀操作
1. 2 条回复

 网络惘然 2017-06-05 18:44:15

这些楼主得分享，

0 回复Ta

 hades 2017-06-12 02:19:56

感谢咯

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板