分析 Regin 的 Hopscotch 和 Legspin 模块

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	An analysis of Regin's Hopscotch and Legspin		
原文作者	Costin Raiu, Igor Soumenkov	**原文发布日期**	2015 年 1 月 22 日
作者简介	Costin Raiu 是卡巴斯基实验室全球研究和分析团队的总监。也是一位自由思想家、软件开发员、建筑师、摄影师、编辑。 http://securelist.com/author/costin/		
原文发布单位	卡巴斯基实验室		
原文出处	http://securelist.com/blog/research/68438/an-analysis-of-regins-hopscotch-and-legspin/		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。		

分析 Regin 的 Hopscotch 和 Legspin 模块

Costin Raiu, Igor Soumenkov

2015 年 1 月 22 日

对于 Regin 这样的高级威胁来说，失误是非常罕见的。然而，当涉及到人类编写代码时，有些错误是难以避免的。分析 Regin 行动时，我们发现的最有趣的事情是一些模块的被遗忘的代号。

这些模块是：

- Hopscotch
- Legspin
- Willischeck
- U_STARBUCKS

我们决定更详细地分析其中两个模块：Hopscotch 和 Legspin.。

尽管 Regin 平台整体复杂性很高（有时甚至过度工程化），但这些工具却是很简单直接的，能够为 Regin 操作者提供互动控制台接口。有趣的是，这些工具在多年前就开发了，甚至在 Regin 平台本身创建之前。

Hopscotch 模块

MD5	6c34031d7a5fc2b091b623981a8ae61c
大小	36864 字节
类型	Win32 EXE
编译时间	2006.03.22 19:09:29 (GMT)

该模块还有另一个二进制模块，作为资源 103 存储。

MD5	42eaf2ab25c9ead201f25ecbdc96fb60
大小	18432 字节
类型	Win32 EXE
编译时间	2006.03.22 19:09:29 (GMT)

这个可执行模块被设计为用于横向运动的独立交互式工具。它不包含任何漏洞，而是利

用以前获得的凭证在使用标准 API 的远程机器上进行身份验证。

该模块从标准输入（操作者）接收目标机器的名称和可选的远程文件名。执行时，攻击者可以从多个选项进行选择，该工具提供人类可读的响应和建议。

下面是在虚拟机中运行的“Hopscotch”的示例：

```
验证机制(SU or NETUSE) [S]/N:
继续？ [n]:
远程计算机上已经存在同名文件 – 不删除…
```

该模块可以使用两个例程在目标机器上进行验证：或者连接到一个名为“IPC$”（称为“NET USE”）的标准共享，或作为拥有足够权限来执行进一步行动的本地用户（“SU”或“切换用户”）登陆。

然后，它从它的资源中提取有效载荷的可执行文件，将其写入目标机器上的位置。有效载荷的默认位置是：\\%target%\ADMIN$\SYSTEM32\SVCSTAT.EXE。一旦成功，它连接到远程计算机的服务管理器，并创建一个名为“服务控制管理器”的新服务，以启动该有效载荷。该服务立即启动，执行一秒后停止并删除。

该模块使用两个命名管道，用远程有效载荷 SVCSTAT.EXE 建立双向加密通信信道。一个管道从操作者向有效载荷提交输入，另一个则从有效载荷向标准输出写入数据。数据使用 RC4 算法加密，并且初始密钥交换使用非对称加密予以保护。

\\%target%\pipe\{66fbe87a-4372-1f51-101d-1aaf0043127a}

\\%target%\pipe\{44fdg23a-1522-6f9e-d05d-1aaf0176138a}

一旦完成，该工具就会删除远程文件，并关闭验证会话，从而有效地消除所有的操作痕迹。

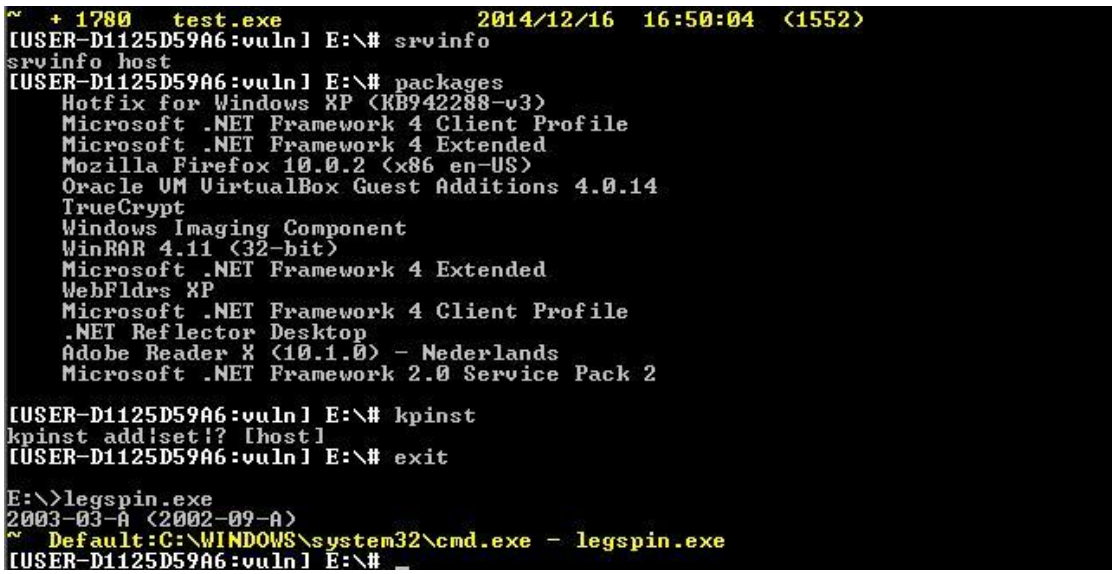
SVCSTAT.EXE 有效载荷模块在进程 dllhost.exe 中启动其副本，然后在目标机器上准备相应的命名管道，之后等待数据。一旦原始模块连接到管道，它就会设置管道通信的加密，并等待 shellcode 输入。

可执行文件被注入新的进程 dllhost.exe 或 svchost.exe，然后执行，其输入和输出句柄重定向到发起攻击的远程插件。这使得操作者能够控制注入的模块并与它进行交互。

Legspin 模块

MD5	29105f46e4d33f66fee346cfd099d1cc
大小	67584 字节
类型	Win32 EXE
编译时间	2003.03.17 08:33:50 (GMT)

该模块也是为计算机管理开发的独立命令行程序。当远程运行时，它就会成为一个强大的后门。值得注意的是，当本地运行时，该程序具有完全控制台支持功能。它甚至能够区分支持 Windows 控制台 API 和支持 TTY 兼容终端（接受颜色转义码）的控制台。



标准控制台窗口中的“Legspin”输出（高亮）

除了在 PE 标头中的编译时间戳，还有两个迹象显示其真实编译时间是 2003 年。该程序输出两个版本标签：

- 2002-09-A, referenced as "lib version"
- 2003-03-A

此外，该程序采用传统的 API 函数，如在 Windows 2000 中引入并在 Windows Vista 中废弃的“NetBIOS”。

一旦启动和初始化，它就为操作者提供一个交互式命令提示符，等待传入命令。可用的命令列表相当大，允许操作者执行许多管理操作。一些命令要求来自操作者的其他信息，并且命令需提供可用参数的文本描述。该程序实际上是一个管理 shell，旨在由攻击者/使用者

手动操作。

命令	描述
cd	改变当前的工作目录
dir ls dirl dirs	文件和目录的列表
tar	查找匹配给定的掩码和时间范围的文件，将其内容写入到 XOR 加密的文档中
tree	输出使用伪图的目录树 
trash	读取并输出 Windows“回收站”目录中的内容
get	检索目标机器上的任意文件，并进行 LZO 压缩
put	向目标机器上传任意文件，并进行 LZO 压缩
del	删除文件
ren mv copy cp	复制或移动文件到新的位置
gtm	获取文件的创建、访问、编写时间戳，并记住这些值
stm	将文件的创建、访问、编写时间戳设置为先前检索到的值
mtm	修改之前检索到的文件时间戳
scan strings	从给定的文件中查找并输出出所有可读字符串
more	输出任意文件的内容
access	检索和输出文件或目录的 DACL 项
audit	检索和输出文件或目录的 SACL 项
finfo	检索和输出给定文件的版本信息

cs	转储任意文件或几个系统文件的前 10,000 字节 advapi32.dll kernel32.dll msvcrt.dll ntdll.dll ntoskrnl.exe win32k.sys cmd.exe ping.exe ipconfig.exe tracert.exe netstat.exe net.exe user32.dll gdi32.dll shell32.dll
lnk	搜索 LNK 文件，解析并输出其内容。
info	输出一般系统信息： • CPU 类型 • 内存状态 • 计算机名称 • Windows 和 Internet Explorer 版本号 • Windows 安装路径 • 代码页
dl	输出有关磁盘的信息： • 类型 • 可用/已用空间 • 分区列表，其文件系统类型。
ps	列出所有正在运行的进程
logdump	未完成的，只显示参数说明。
reglist	转储本地或远程蜂巢的注册表信息
windows	枚举所有可用的台式机和所有打开的窗口
view	列出一个域中所有可见的服务器
domains	列出网络中的域控制器
shares	列出所有可见的网络共享
regs	输出注册表中的其他系统信息： • IE 版本 • Outlook Express 的版本 • 默认的登录用户名 • 系统安装日期 • BIOS 日期 • CPU 频率 • 系统根目录
ips	列出网络适配器信息：

	• DHCP/静态 IP 地址 • 默认网关地址
times	从本地或远程计算机获得当前时间
who	列出机器访问的当前用户和域名
net nbtstat tracert ipconfig netstat ping	运行相应的系统程序并输出结果
tel	连接到主机的一个给定 TCP 端口，发送由操作者提供的一个字符串，输出响应。
dns arps	使用 DNS 或 ARP 请求解析主机
users	列出所有用户帐户的信息
admins	列出具有管理权限的用户帐户的信息
groups	列出有关用户组的信息
trusts	列出有关域间信任用户帐户的信息
packages	输出安装的软件包的名称
sharepw	执行暴力登录攻击，试图获取远程共享的密码。
sharelist	连接到远程共享
srvinfo	检索指定服务器的当前配置信息
netuse	连接、断开或列出网络共享
netshare	在当前机器上创建或删除网络共享
nbstat	列出 NetBIOS LAN 适配器信息
run	创建一个进程，将其输出重定向到操作者
system	使用 WinExec API 运行任意命令
exit	退出程序
set	设置用于其他 shell 命令的各种内部变量
su	作为不同用户登录
kill	根据 PID 终止进程
kpinst	修改注册表值： [HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon] System 这个值通常应指向 "lsass.exe"。
svc drv	创建、修改或删除系统服务。
help ?	输出支持的命令列表

我们发现的 Legspin 模块没有内置的 C&C 机制。相反，它依赖于 Regin 平台将控制台输入/输出重定向到操作者，反之亦然。

结论

与 Regin 的大多数其他模块不同，Legspin 和 Hopscotch 似乎是更早开发的独立工具。特别是，Legspin 后门可以追溯到 2003 年，甚至 2002 年。值得指出的是，并非所有的 Regin 部署都包含 Legspin 模块；在大多数情况下，攻击者通过其他 Regin 平台功能管理受害者。

这意味着，在 Regin 平台之外，Legspin 可以作为一个带有输入/输出包装器的简单后门独立使用。

虽然我们对 Regin 的了解越来越多，但是仍然有很多未知内容。有一点已经很清楚：锁着时间的推移，我们所了解的 Regin 模块可能会被新的模块和技术所替代。