Systems Programmer, Heal Thy PC
Part 1: Virus Removal

Session 10255, Tuesday, March 13, 2012

James Willette, Sunrise e-Services

Victor Freyer, Lemon Bay Computer Service

Disclaimer

- I use “virus” to refer to the whole class of malware that may infect your PC.
- Purists would say that virii are programs that spread themselves.
- Most of today’s malware is installed by the end user, and by definition is not a virus.

Do-It-Yourself Virus Removal

- Why do it yourself?
  - Company has Draconian rules about PC use
  - Anger and disbelief
  - Pride
  - Second career?
  - The Geek Squad™ wants to charge what!?
- What do you need?
  - Clean boot environment
  - An eye for what's unusual
  - A toolkit full of free tools

So you think you have a virus?

- Signs of malware
  - Computer is slow
  - Click on a Google result and go to some unrelated page
  - Lots of “undeliverable message” alerts in your inbox
  - “Warning, you have 732 viruses!!!!!”
  - Unable to run Windows updates
  - Unable to update your anti-virus program
  - Unable to connect to the Internet
  - Excessive TCP connections popup warning
  - “Do you want to allow this program to run?”

So you think you have a virus?

- Simple five step process
  - Turn the machine off – no graceful shutdown
  - Boot to a clean environment
  - Back up the boot drive
  - Disable the virus program
  - Fix corrupted registry and configuration files

Boot to a Clean Envionment

- WinBuilder – freeware to build Windows boot disks http://reboot.pro/forum/22 (registration required)
  - XP, Vista, Windows 7, Windows 8, Driveimage XML
- EaseUS Todo Backup Free – non-commercial use http://www.todo-backup.com/products/features/free-backup-software-winpe.htm
- Microsoft Diagnostics and Recovery Toolset
  - Available to Microsoft TechNet subscribers
- Linux LiveCD – SystemRescueCD http://www.sysresccd.org/Download
  - Boots from CD, flash, or hard drive
- Windows Vista and 7 recovery disks

Backup Your Boot Drive (SystemRescueCD)

- Check hard drive SMART statistics
  ```
  smartctl -a  /dev/sda
  ```
- Back up the MBR
  ```
  dd if=/dev/sda of=mbr.bin bs=512 count=1
  ```
- Back up the contents of the boot partition
  - PartImage (NTFS and FAT)
  - NTFSclone (NTFS only)
    ```
    ntfsclone --save-image -o backup.image /dev/sda1
    ```
- Registry backup
  - Regback
  - Regkey

Stand-Alone Anti-virus Software

- AVG Rescue CD
  http://www.avg.com/us-en/avg-rescue-cd

- Kaspersky Rescue Disk
  http://rescuedisk.kaspersky-labs.com/rescuedisk/updatable/kav_rescue_10.iso

- Microsoft Standalone System Sweeper (beta)
  http://connect.microsoft.com/systemsweeper

- F-Secure Rescue CD
  http://www.f-secure.com/en/web/labs_global/removal/rescue-cd

Clean-up and Repair

- Clean-up tools
  - Malwarebytes Anti-Malware – non-commercial use
    http://www.malwarebytes.org
  - Hijack This (now open source)
    http://sourceforge.net/projects/hjt
  - Sysinternals Autoruns
    http://technet.microsoft.com/en-us/sysinternals/bb963902
  - Spybot Search and Destroy
  - Windows command   SFC /SCANNOW
- Prevention
  - AVG Anti-virus Free Edition (non-commercial use)
  - Microsoft Security Essentials (free up to 15 computers)
  - ZoneAlarm Firewall (non-commercial use)

Thank You!

- The best virus prevention
  - Healthy paranoia
- Contact us
  - Jim Willette – jim.willette@q.com
  - Victor Freyer – victor@lemonbaycomputerservice.com
- Practice Safe Computing!