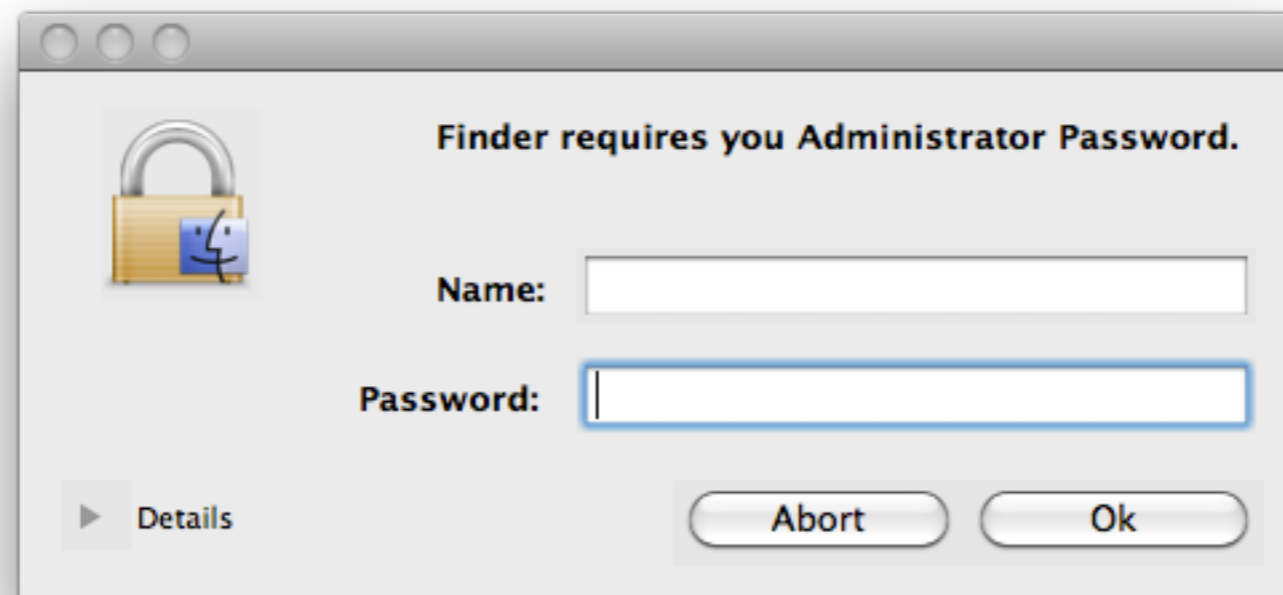


Malware

Rik Farrow © 2011
rikfarrow.com



Malware

- Malware is software that is hostile
 - It may just be annoying or intrusive
 - It can be destructive
 - It can steal information
 - It is often hard to get rid of

Malware Types

- Viruses, malware that spreads with help
- Worms, like viruses, but spreads itself
- Trojans, provide backdoors and other features
- Spyware, malware that collects information
- Adware, malware that displays advertising

Malware History

- Creeper, first network virus - 1971
- Elk cloner, spread via floppies on Macs only - 1982
- Jerusalem, deleted any program executed - 1987
- Michelangelo, deleted files on March 6 - 1992

Malware History

- Melissa, a worm that infected Word docs and used Outlook to spread - 1999
- I LOVE YOU, worm that spread via email - 2000
- Code Red, infected MS Web servers - 2001
- Sasser, infected Windows PCs, flooded networks - 2004

Malware History

- MyTob, turns infected Windows PCs into members of a botnet for spamming - 2005
- Storm botnet, robust botnet infecting Windows PCs, first large botnet - 2007
- Koobface, botnet malware that spreads via Facebook and other social networks - 2008

Malware History

- Conficker, both a worm like Sasser and a robust botnet, infected millions of PCs, including businesses, hospitals and military - 2009
- Stuxnet, spread via USB sticks, designed specifically to attack Iranian centrifuges - 2010

Spreading Malware

- Viruses:
 - Early viruses spread via infected floppy disks
 - Later viruses spread via email
 - Some viruses could infect Windows even if the email was not opened
 - Other viruses require some user action

SpearPhishing

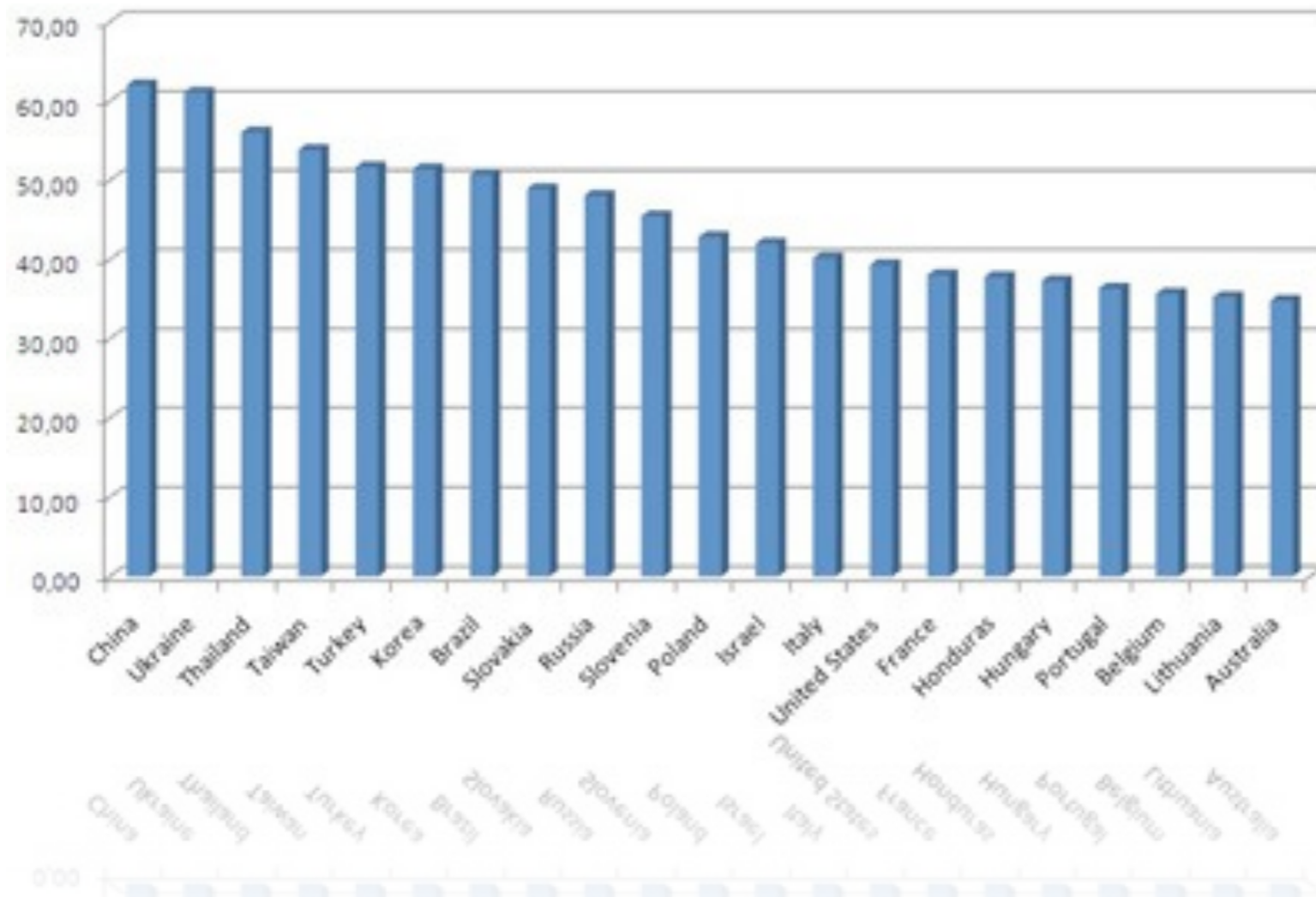
- Spearphishing is a directed attack that uses email
 - Email appears to come from trusted sender
 - Subject seems relevant
 - Content is malware or links to malware
 - Recent attack used Flash embedded in Word docs aimed at US government sites

Spreading Malware

- Worms spread themselves
- Can attack vulnerable systems from the network
- Can use email or social networks to spread
- Slammer, Sasser, and CodeRed as examples

Malware Spreading

- Malware often spreads via Web servers
- Attacker gains access to a Web server
- Adds links or scripts to existing web pages
- Visiting the web site starts the installation process



Estimate of Infected Systems

Avoiding Malware

- Computer systems are very complex
- Very good code contains one bug per thousand lines
- Most code is not that good
- Windows, and MacOSX contain tens of millions of lines of code, ~ 50,000 bugs

Anti-Malware and Anti-Virus

- Anti-virus software is 20% effective
 - Two 'new' viruses generated every minute
 - Encryption and packing used to confuse AV
 - Malware creators use services that pack/encrypt then check malware with AV
- You still **must** use AV in Windows!

Fake Anti-Virus Software

- Fake AV software is very popular today
 - Malware gets installed on a Windows PC
 - Malware displays a dialog warning of infection
 - Runs a fake scan
 - Installs more malware instead of removing any

Use Real AV

- There are many real AV companies:
 - McAfee, Symantec, F-Secure, Kaspersky, Panda, **Sophos**, Trend Micro, BitDefender, ClamAV, perhaps 33 others
 - These companies charge money for keeping malware signatures updated daily

Microsoft Security Essentials

- As MS Windows is the most common victim of malware, perhaps they should do something?
- MS Security Essentials works for “free”:
 - Works in the background
 - Looks for malware
 - Removes known malware

Microsoft Security Essentials

- Security Essentials works on licensed copies of Windows
- And, the deal is, MS gets a copy of everything that might be malware
 - This allows MS to collect potential malware for sampling
 - Give MS a near realtime view
 - Also an invasion of privacy, but it's "free"

Other Things You can Do

- Use accounts without Administrator privileges
- Administrator privilege is required to make changes to the system
- Do not enter your Administrator password while working with the Web or email
- Switch to an Administrator account only when needed

Do Not Use Windows XP

- Windows XP is both old and dangerous
 - Almost all exploits work on XP
 - IE 6 is terribly vulnerable
- Use Windows 7 and IE 9 (or more recent) for the best security you can get with Windows

Use Search Engines

- Google actively searches the Web for malicious Web sites
- Warns you before you can visit a known malicious Web site
 - Firefox includes SafeBrowsing too
- Use search engines to find banking Web sites
 - More reliable than typing long names

Be Cautious about What You Install

- Malware is often installed by unsuspecting users
 - Offers of free AV
 - Free codecs for viewing movies
 - Plugins for Web browsers
 - Only install plugins approved by your browser vendor

Mac OS X Is **Not** Immune

- There is very little evidence for Mac malware today
- I did find two recent backdoor trojans for Macs
- Mac OS X runs Web browsers (Safari, Firefox, and IE) that have been exploited
- You can install browser plugins that work on any computer, and these can be malicious

Use Your Firewall

- Mac OS X includes a built-in firewall
 - It's not very intrusive
 - System Preferences->Personal->Security Firewall Tab
 - Only protects against unknown services running on your Mac (like backdoors)
 - But not outward-connecting backdoors
 - Use Little Snitch for blocking these

Use a Firewall

- Most WiFi routers include a simple firewall
 - One that allows outgoing connections
 - And blocks incoming ones
 - Prevents some backdoors from working
- If you run a small business, get a real firewall and configure it conservatively

Malware

- Somewhere between 30% and 67% of all Windows PCs are infected today
 - Even within businesses
 - Even with AV and firewalls
- Do use AV and firewalls
- http://www.youtube.com/v/wKl5dgIcs74?fs=1&hl=en_US