The Evolution of Malware

Matthew Best – matthew-best@utulsa.edu

University of Tulsa
Tulsa, Oklahoma 74104

April 3, 2012
Overview

- History of Malware
- Evolution of Motivations
- Evolution of Methods
60’s and 70’s
And so it begins... 

- Creeper created in 1971
  - Spread across ARPANET
  - First “worm”
  - Reaper created to kill it
- Wabbit fork bomb created in 1974
- ANIMAL
  - Game attempted to guess the user’s animal
  - Spread through system and to detachable media
  - First Trojan
80’s
Stuff gets real.

- Elk Cloner in 1981, first ”real” virus
- 1983 saw many papers
  - ”computer virus” coined by Frederick Cohen
- Many academic viruses
- First ”wild viruses”
  - Morris Worm - 1988
  - Ghostball Multipartite Virus - 1989
90’s
Mighty Morphin Polymorphs!!!

- Polymorphism appears with Chameleon in 1990
- First panic with Michelangelo
- BBS and shareware distribution
- Happy99 worms uses fireworks!
- Kak worm exploits bug in Outlook Express
Present
Because it’s too hard to say ”00’s”

- All your e-mail is ours!
- Worms everywhere
  - ILOVEYOU
  - SQL slammer
  - CodeRed
  - Blaster
  - Conficker
- Stuxnet
- Anti-AV
- Morto spreads via Remote Desktop
"For educational purposes."

**Assessment**
- Infection Rate: Low
- Danger/Damage: None

**Summary**
- Computers are now a field
- "What can we do with them?"
- Model after natural world
  - Genetic Algorithms
  - Self Replication (Viruses)
"Can I do it?"

Assessment

- Infection Rate: Medium-Low
- Danger/Damage: Low-None

Summary

- Similar to academia
- Hobby Programmers
- Enabled by early, unprotected internet
Anklebiters

Assessment

- Infection Rate: Medium-Low
- Danger/Damage: Medium-Low

Summary

- First malicious actors
- Cause misery/grief
Activists/Terrorists

Assessment
- Infection Rate: High-Medium
- Danger/Damage: High-Medium

Summary
- Focus on disruption and destruction
- DDoS and Disruptive Viruses
- Usually launch attacks through web hacking
- Ex: Anonymous
Criminals

Assessment
- Infection Rate: High
- Danger/Damage: High

Summary
- Monetary Goals
- Focus on stealth and information
- Keyloggers, Web Injection Viruses
- Botnets for sale
Nation States

Assessment
- Infection Rate: ?? (Targeted)
- Danger/Damage: High

Summary
- Lengthy/expensive development
- Stealth techniques
- Targeted attack vector
  - Damages/Infests only desired machines
  - Ignores others
- Stuxnet?
Assessment

- Difficulty: Low
- Effectiveness: High-Medium
Drive by Downloads

Assessment

- Difficulty: Medium-Low
- Effectiveness: High

Click to run an ActiveX control on this webpage
Assessment

- Difficulty: Medium
- Effectiveness: High

Security Warning:

Do you want to install and run "crack.zip"

By clicking Yes you are agreeing to the terms and conditions and installing xxx toolbar" signed on 2004/04/13 11:34 PM and distributed by:

Integrated Search Technologies

Publisher authenticity verified by Thawte Code Signing CA

Caution: Integrated Search Technologies asserts that this content is safe. You should only install/view this content if you trust Integrated Search Technologies to make that assertion.

- Always trust content from Integrated Search Technologies

[Yes No More Info]
Exploit Infection

Assessment

- Difficulty: High
- Effectiveness: High (until patched)

- Vulnerability and exploit development
- Expensive
- Robust - Gets into inaccessible networks
- Alternative channels (remote desktop)
File/Process Hiding

- Adds stealth to malware
- Increases difficulty of removal
- Rootkits
  - More difficult
  - Low-level
  - Difficult to remove
- OS dependent
Polymorphism

- Expands on packing techniques
- AV avoidance
- Signatures are ineffective
- Ex: Kraken
Command and Control

- Foundation of a Botnet
- Communicate with creators
- Enables advanced, dynamic behaviour
- Ex: Sality
Persistence

- MBR early on (easier)
- Bios and user-land made harder/unneeded
- Targets grow harder
- User-land persistence easier to thwart
**History of Malware**

**Evolution of Motivations**

**Evolution of Methods**

**Sources**

- [Timeline of computer viruses and worms](http://en.wikipedia.org/wiki/Timeline_of_computer_viruses_and_worms)
- [Evolutionary computation](http://en.wikipedia.org/wiki/Evolutionary_computation)
- [Duqu malware targeted sophisticated and likely nation-state sponsored](http://www.lgscout.com/blog/duqu_malware_targeted_sophisticated_and_likely_nation_state_sponsored)
- [Methods of infection](http://www.malwarehelp.org/methods-of-infection.html)