malware

Slides: Thanks to J. Espinosa

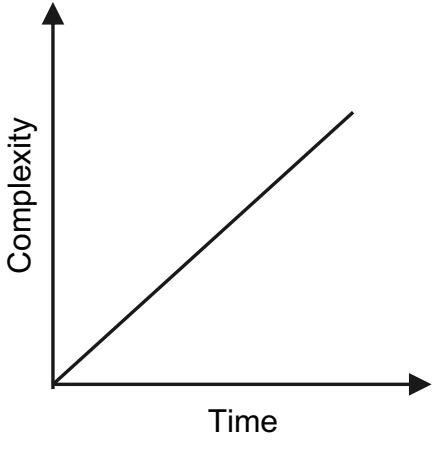
agenda

- malwhat?
- malware analysis
- threat intelligence
- security research

what is malware

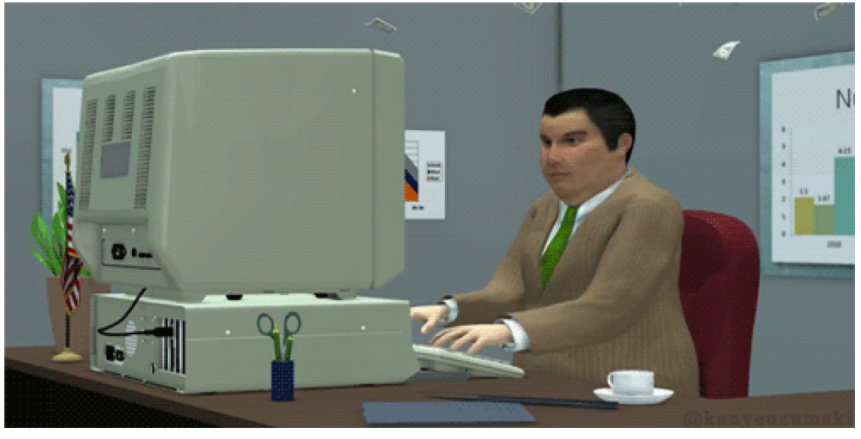
- Portmanteau of “**mal**icious soft**ware**”
- Software that performs actions that are not advantageous to the owner/operator of the infected systems

once upon a time



why does it exist?

- financial gain
  - click-fraud
  - banking/credit info
  - ransom demands
- espionage
  - trade secrets
- cyber weapons
  - activism
  - state-sponsored
  - world domination



actual malware author

http://hackertyper.com/

types of malware

- Traditionally, we learn to classify malware by its method of distribution
  - Virus/worm/Trojan horse
  - Good for containment and remediation, but not much else
- Focus on malware functionality and source

malware functionality

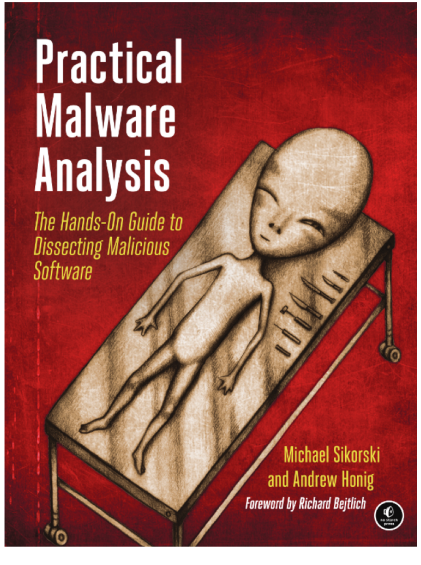
Functionality	Description
Droppers/Loaders	Download and execute additional malware
Spyware	Record user activity
Adware	Serve advertisements to victims
Ransomware	Deny access to a user’s computer resources until a ransom is paid
Backdoors	Provide persistent access to a system
Rootkits	Hide malicious activity via anti-forensics techniques

malware analysis

- Malware analysis is a collection of tools, tactics, and procedures that defensive security professionals use to determine the functionality of a malware sample
- Should be thought of as iterative, not linear

what you will need

- Google and MSDN
- Malware samples
- Analysis Tools
- Coffee
- Suggested reading:
  - **Practical Malware Analysis**
  - http://www.amazon.com/Practical-Malware-Analysis-Dissecting-Malicious/dp/1593272901



static malware analysis

- Purpose
  - Analyze the structure of the PE file
  - Headers, code segments, data segments, etc.
- Pros
  - You can learn a lot from PE headers and a disassembler
  - Low risk
- Cons
  - Packing/encryption can defeat static analysis
  - You miss a lot if you use static analysis alone
  - Time consuming

dynamic malware analysis

- Purpose
  - Analyze the behavior of a malware sample as it executes
  - Network communications, changes to the OS, etc.
- Pros
  - Regardless of any anti-reversing techniques used by a piece of malware, data and function arguments must be sane to use
  - Faster than static analysis if you know what you're looking for
- Cons
  - Riskier than static analysis
  - Harder to get a big picture understanding. You need static analysis.

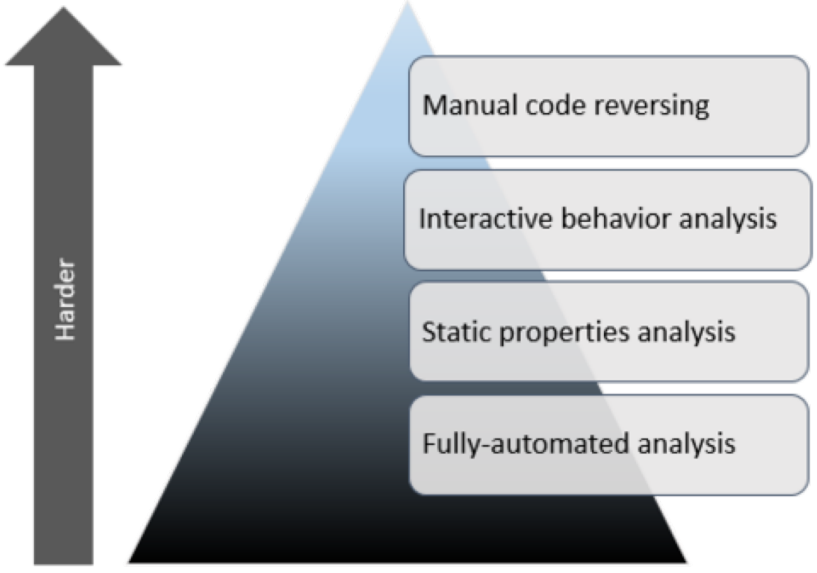
malware vs dynamic analysis

anti-reversing techniques

- anti-disassembler techniques
- anti-debugging techniques
- anti-virtualization techniques
- anti-forensic techniques
- antidisestablishmentarianism?
  http://en.wikipedia.org/wiki/Antidisestablishmentarianism

depth of analysis

- The amount of time you spend reversing malware depends on your goals
  - Creating simple network signatures == quick
  - Fully decompiled source code analysis == s l o w
- Time constraints also affect depth of analysis



http://blog.zeltser.com/post/79453081001/mastering-4-stages-of-malware-analysis

malware and threat intel

Phase
Reconnaissance
Weaponization
Delivery
Exploitation
Installation
C2
Actions on Objectives

- malware can provide incredible insight into the operational capabilities of an adversary
- the more you know about your enemy, the better you can prepare your defense
- More info on the Intrusion Kill Chain: http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

intel-driven defense

- The Exploit Intelligence Project by Dan Guido
  - http://vimeo.com/31548167
  - Takeaways
    - There are many vulnerabilities
    - Mass malware only exploits a handful of vulns
    - You can mitigate the majority of attacks by implementing your security around the relatively small number of exploitable vulnerabilities

security research

- research the latest threats and security trends
  - rss/blogs
  - mailing lists
  - social media
- analyze network traffic, exploits, vulnerabilities, malware
  - file hashes / characteristics
  - url structures / traffic patterns and anomalies
- write signatures to expand detection capabilities
  - network-based
  - file-based