SWINBURNE UNIVERSITY OF TECHNOLOGY

ICT30010 eForensic Fundamentals

Lecture 7

Malware and Hacking

Troy PRETTY

Digital Forensic Analyst

Outline and learning goals

- Hacking motivations
- Definition of 'malware'
- Some notable examples of malware
- Detection and dealing with malware

Background

- Evolution of hacking (cracking) over the past 20 years
- Original hackers driven by need for peer recognition
- Motivation was curiosity or a desire to demonstrate their abilities to others
  - Examples include the Morris Worm and the WANK worm
  - Moderately benign

Background

- When the Internet became commercialised motivation became more ideological
  - Big denial of service attacks on Microsoft, eBay
  - Much less benign
- Now attacks are driven by profit as much as anything else
  - Identity theft, fraud, theft of trade secrets, competitor plans
  - Information warfare
- Quite a lot of 'Hactivism' in few years
  - Anonymous
  - LulzSec
  - LizardSquad

Notable exploits over the last few years

- 2002 Bank of California:
  - 265,000 customer details stolen
- 2004 BJ's wholesale club
  - several million customer credit card numbers stolen
- 2005 Choicepoint (a company who collect private information on American consumers)
  - allowed access to their database by hackers posing as representatives from legitimate companies – used data for extensive identity theft
- 2006 DSW Shoe Warehouse
  - lost 1.4 million credit card numbers
- 2008 Conficker worm infects an estimated 9-15 million Windows systems

Notable exploits over the last few years

- 2009 Zeus (Trojan)
  - compromised over 74,000 FTP accounts on websites of such companies as the Bank of America, NASA, Monster, ABC, Oracle, Cisco, Amazon, and BusinessWeek
- 2010 Iran Stuxnet worm
  - Believed to be combined effort of US and Israeli military
  - Target Iranian nuclear programme
- 2011 Sony Playstation Network hacked.
  - Possible loss of 70 million credit card numbers
- 2014 Target compromise
  - Malware infected POS machines, RAM scraping credit card numbers
- 2016 Yahoo
  - Estimated 1 billion user accounts compromised
- 2018 Marriott Hotel
  - 383 Million Customer Records – Credit Card, Passport, Personal Details

Issues in dealing with attacks

- Organisations reluctant to release details of attacks
  - ‘Copycat’ attacks
  - Loss of trust in organisation
- Much easier to mount attacks than in the past
  - ‘script kiddies’
  - Software tools readily available
  - Malware for sale
- A big problem is the large number of naïve home users connected to broadband connections
  - Do not understand the problem
  - Do not understand that they are targets, eg as zombies in DDoS attack
  - Do not have the technical understanding to secure their machines

Some malware terminology

- Threat
  - Any potential danger to information or systems
- Vulnerability
  - A weakness in software, hardware or procedures that may provide an opportunity for attack
- Exploit
  - A particular security breach that makes use of a vulnerability
- Zero day exploit
  - An exploit that uses a vulnerability before the developer or user of the target software knows about the vulnerability.

Issues in dealing with attacks

- Security of TCP/IP
  - TCP/IP (version 4) designed in 1970s when security much less an issue for the Internet than it is now
  - TCP/IP (version 4) has no built-in security features but is used in most networks (including LAN, MAN and WANs) and in most applications (voice, email, multimedia, web etc)
    - Makes propagation of malware much easier than it should be

Issues in dealing with attacks

- Poor array bounds checking in widely used software
  - Computer memory is organised in contiguous blocks - executable code, data and stack space
  - Stack space contains return addresses from subroutines
  - If data passed to the routine exceeds the expected size, and there is no array bound checking, it can overwrite the stack and substitute a new return address
- With some clever programming the return address can be to a routine that contains some executable code
  - For example, starts a shell script
  - A 'Buffer Overflow' Attack

Malware

- Malicious Software that is designed to damage or gain unauthorised access to a computer or network
- Classification of malware
  - Infectious malware – Viruses, Worms
  - Concealment malware – Trojan horses, Rootkits and Backdoors
  - Malware for profit – Spyware, Botnets, Keystroke loggers, cryptolocker, cryptominer

Viruses

- A virus is a small application or piece of code that infects other applications or code
  - □ It cannot replicate on its own.
  - □ It uses an infected host to replicate and spread
- The virus vector is the mechanism by which the virus spreads
  - □ USB memory sticks
  - □ Word and Excel Macros
  - □ Downloaded or emailed executables

Viruses

- Capabilities
  - Erase files on your machine
  - Delete directory structures
  - Encrypt files making them impossible for you to access (a Denial of Service mechanism)
  - Copy and send files on your machine
  - Send files to emails in your address book
  - Load logic bombs
  - Display inappropriate message

Virus vectors

- Early viruses were spread mainly on floppy disks.
  - Main way of information exchange on early personal computers
- Online bulletin boards became main way of exchange in late 80s and early 90s
  - Viruses embedded in popularly traded software
- From mid-1990s main kinds of virus are macro viruses written in the VBA scripting languages of Microsoft programs such as Word and Excel
- USB flash drives
- Website drive by or email

Virus coding

- Easy to code viruses
  - ‘script kiddies’
- Can download viruses from websites
- Many viruses script based
  - Use Visual Basic
  - Embedded in EXCEL or WORD macros
- Often new viruses are derived from the notification of security weaknesses
  - A company identifies a weakness in its software and posts a patch
  - The virus writer exploits the weakness in the (reasonable) assumption that many users won’t install the patch

Worms

- A computer worm is a self-replicating computer program
- Self-contained and does not need to be part of another program to propagate itself
- Often designed to exploit the file transmission capabilities
- A worm uses a network to send copies of itself to other systems and it does so without any intervention

Worms

- Email and Instant messaging worms
  - Do not infect files, but propagate by a file transfer system
    - eg email attachments
- File sharing worms
  - Exploit peer-to-peer systems
  - Innocuous named file located in a shared folder
- Network aware worms
  - Exploit security vulnerabilities such as unprotected shared drives, FTP weaknesses
  - Earliest examples of these types of worms exploited buffer overflow

Trojan horses

- Simple Trojan Horse
  - Some inviting file name (use your imagination) with .exe suffix
  - User clicks on it
  - Program runs and (for example) deletes all files on c:\
  - Made easier by some Microsoft systems (eg. Microsoft Outlook Express) hiding file extension
    - eg. annakournikova.jpg.exe appears as annakournikova.jpg
- More sophisticated Trojan Horses
  - Rootkits

Rootkits

- A Trojan horse that allows administrator (root) access to the host while hiding its presence
- Circumvents normal access control mechanisms
- Hides processes, network connections, registry entries, files etc from ordinary observation

Backdoors

- Related to trojans and rootkits
  - Remote Access Trojan (RAT)
- Provides access without going through normal authentication
  - Netbus
  - Sub7
  - DarkComet

Spyware

- Collects information about users without their knowledge
  - Passwords, web surfing habits, email contacts...
  - Can be used for theft or blackmail
- Installed on user machines without their knowledge
- Usually as a result of a virus or worm but sometimes installed in a corporate network to monitor users
- An example is a 'key logger'
  - Captures keystroke information

Botnets

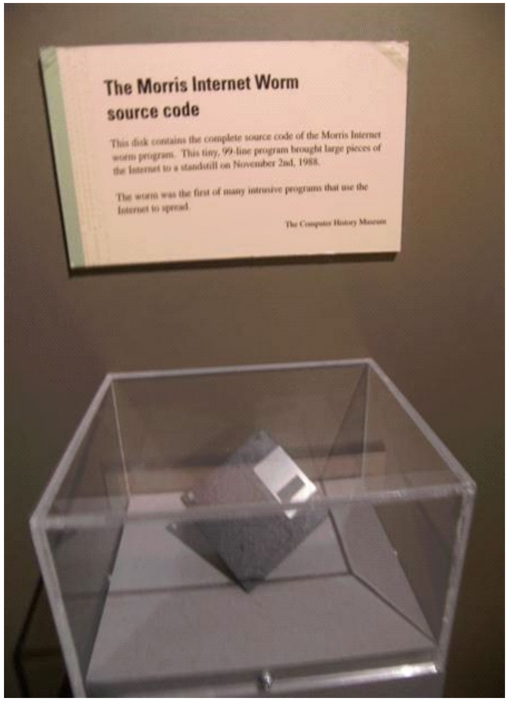
- A collection of compromised hosts (zombies) that can be marshalled for some (usually morally dubious) purpose
- Typically used in denial of service attacks, spam and phishing

Drive-by downloads

- Sometimes drive-by installs
- User visits a website
- Website causes a trojan (typically) to be loaded onto the victim’s computer without his or her knowledge
  - May trick the user into download by presenting a pop-up message
    - Clicking on the message causes the download to occur
  - May be an executable attached to an email

Notable examples of malware

- The Morris Worm in 1988
  - 99 lines of code
  - First known worm
  - Unix based (BSD and derivatives)
  - Exploited buffer overflows in sendmail, finger and rsh
  - Intent was not malicious, was meant to gauge the size of the internet.



The Morris Internet Worm source code

This disk contains the complete source code of the Morris Internet worm program. This tiny, 99-line program brought large pieces of the Internet to a standstill on November 2nd, 1988.

The worm was the first of many intrusive programs that use the Internet to spread.

The Computer History Museum

Notable examples of malware

- WANK worm (1989)
  - The first known ‘political’ worm, linked to protests around the Galileo spacecraft and it use of plutonium power
  - Attempted to attack VAX machines at NASA and USA Department of Energy
  - Refer to “In the Realm of the Hackers”
    - http://www.abc.net.au/tv/documentaries/stories/s853348.htm
- Melissa virus (1999)
  - Word macro virus
- Ramen worm (2001)
  - First known Linux worm
  - attacks Remote Procedure Call (RPC) service or ftp daemon
  - searches for vulnerable machines to propagate to

Notable examples of malware

- Annakournikova virus (Feb 2001)
  - Exploited Microsoft Outlook behaviour of hiding attachment suffix
  - If activated sends a copy of itself to everyone in the Outlook address book
- Welchia worm (August 2003)
  - A ‘good’ ish worm
  - The Welchia worm exploited a vulnerability in the Microsoft RPC service
  - it tried to help the user by downloading and installing security patches from Microsoft
  - Still causes lots of traffic, rebooted user’s machine and operated without user’s consent

Notable examples of malware

- Mydoom (January 2004)
  - email worm
  - The mail contains an attachment that, if executed resends the worm to email addresses found in local files such as a user's address book
  - Two versions Mydoom.A and Mydoom.B
  - Mydoom.A allowed a backdoor into the victim's computer with the aim of a Distributed Denial of Service Attack on SCO (Unix software company)
  - Mydoom.B targets Microsoft website, also blocks access MS and AV websites via modified host file

Notable examples of malware

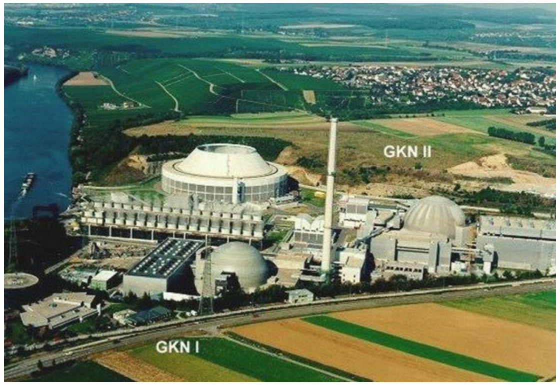
- Code-Red worm (2002)
  - A particularly nasty IIS worm
  - Attacked 359,000 machines in 14 hours (peaked at 2000/minute)
- Blaster worm (August 2003)
  - A malicious worm
  - Exploited a buffer overflow weakness in Microsoft DCOM architecture
  - Intended to do a SYN flood attack on Microsoft site windowsupdate.com
  - A distributed denial of service attack
  - Author went to prison for 18 months

Notable examples of malware

- Conficker (2008)
  - A computer worm that spreads itself to other computers across a network or via USB without human interaction
    - Five versions – A, B, C, D, E
  - Consumes resources, disables accounts, blocks DNS lookups, may load a more recent version of itself
    - Version E loads spam software
  - Attempts to spread itself in many different ways
    - Unpatched systems (exploits a buffer overflow vulnerability)
    - Weak passwords (uses a dictionary attack on password files)
    - Infects removable devices (USB memory sticks)

Notable examples of malware Stuxnet

- Stuxnet (2010)
  - Windows worm that attacks industrial systems
    - Transmitted via USB keys
  - Targets were Siemens Programmable Logic Controllers (PLCs) controlled by offline Windows machines
  - Targeted the Bushehar nuclear power station in Iran
  - Believed to be joint effort between US and Israeli
  - Motivation was sabotage



Notable examples of malware
Stuxnet

- So many things make this a fascinating exploit
  - The software itself
  - Multiple 0-day exploits involved (rare for its time)
  - Its sophistication, the mystery of its origin, the breadth of expertise it manifests...
  - First? Example of malware having real physical military effect
- A demonstration of how offline hosts can be targeted
- Questionable practices in some industrial plants
  - Contaminated USB keys used to transfer software in nuclear power plants
  - Siemen's default passwords not changed

Notable examples of malware
Stuxnet

- Very complex and sophisticated software
  - Estimated to have taken ten people six months to write
  - Required a knowledge of industrial processes
  - Used four zero day exploits
    - *very* unusual – 0-day exploits usually highly valued in hacker community
- Stole two legitimate digital certificates
  - An impressive attention to detail as well as technical breadth and depth
- Software was written to be difficult to detect
- An example of electronic warfare?
  - Despite denials by Iranian officials, appears to have succeeded

Notable examples of malware

- Cryptolocker (2013)
  - Ransomware Trojan
  - Distributed mainly via email
  - When executed, encrypts local files, network drives or MFT tables
  - Malware is easy to remove but files remain encrypted
  - Decryption key held on central malware control server
  - Paying a ransom via BitCoin or prepaid cash cards enables files to be decrypted
  - 2013 ZDNet research identified 4 BitCoin addresses that had $27M USD in transactions in 3 months

Notable examples of malware

- EternalBlue (2017)
  - Leaked by ShadowBrokers Group
  - Stolen NSA 0-Day malware
  - Every version of windows prior to 8 vulnerable
  - 200,000 machines estimated to be infected in first 14 days
  - Catalyst to a number of ransomware attacks such as WannaCry and Petya

Detection and eradication of malware

- Best advice is to not get infected
  - Use good practices to minimize risk of infection
  - Keep software releases up to date and install malware detection software
  - Don’t download pirated software
- Can be very challenging to detect good malware
  - Rootkits and trojans hide their existence
  - Viruses and worms can change their structure
  - An active area of research
- Cannot trust infected operating system
  - Wipe and re-install!

Finding Malware

- Anti-Virus Check
- Automated / Manual Memory Analysis
- Evidence of Persistence
- Packing/Entropy Check
- Event Logs and Timelining
- Third Party Lookups

Finding Malware on Windows OS

- Memory Forensics
  - Rogue Processes
  - Code Injection/Rootkits
  - Unusual Network Activity
- Operating System Forensics
  - Evidence of Persistence
  - Unusual OS Artifacts
  - Unknown Service

Manual Analysis

- Wrong parent process
- Known good .EXE is executed from a wrong path
- Misspelled processes

  lssass.exe vs lsass.exe

  scvhost.exe vs svchost.exe
- Processes that are running under the wrong account
- Processes with unusual start times
- Unusual command-line arguments
- Packed executables

Virus signatures

- A unique string of bits or the binary pattern of a virus
- Consist of sequences of bytes in the machine code of the virus
  - Similar to a fingerprint
- Usually many candidates for virus signatures
  - Goal of those writing systems to identify and deal with viruses is to minimize false negatives and false positives
  - Good signature is one found in every object infected by the virus but is unlikely to be found if the virus is not present;
- Usually obtained by manual inspection
  - slow and error prone
  - Some work being done on automatic extraction

Summary

- Looked at the different categories of malware
- Examined some notable examples
- Briefly discussed detection and eradication