Malware-1

Ed Zaluska

COMP6230:
Implementing Cybersecurity

Key issues

- what is malware?
- why does it exist?
- case studies and examples

What is malware?

- short for “malicious software”
- effect of malware is to cause something unexpected (and usually unwelcome) on your computer e.g.
  - disrupt computer operation
  - collect sensitive information (“spyware”)
  - access private computer system
- malware may take many forms: “virus” is simply the most well-known example (hence used for *all* malware?)
- often designed to remain *undetected*
- protect systems using firewalls, anti-virus, etc.

Why?

- malware can take control of your computer
  (without your consent, of course)
- usually only *partial* control (because otherwise the malware is revealed)
- usually for the benefit of somebody else and usually for money
  (maybe the hacker is merely doing it “just for kicks”)
- send spam to other users (using your address book?)?
- identity/password theft? (e.g. access your bank account)
- store illegal content (e.g. pornography) on your system?
- track user activity? (“spyware”)
- “ransom” your computer?
- launch DDOS (Distributed Denial Of Service) attacks?
- etc. (non-exhaustive list)

Malware variants

- virus
- worm
- Bots (i.e. *Botnet clients*)
- Trojan horse
- rootkit
- adware
- scareware
- ransomware
- backdoor/trapdoor
- keyloggers

Case study: a Trojan Horse

- Trojan war – 12th century BC?
- military tactic to defeat Troy defences
- hence, “something that is not what it appears to be and contains a hidden threat” (i.e. appearance + hidden payload)
- example – log onto your computer: it crashes, you reboot and successfully logon at the second attempt
- maybe the first logon screen you saw was generated by Trojan malware, not your operating system?
- now your password is safely stored away for later retrieval by the hacker: your account has been compromised
- many variants possible: the password could be passed on after a copy made, the Trojan could switch to the correct screen after it has copied your password?
- this exploit has been in common use since the 1970’s – long before networks became commonplace

Case study (continued)

- Ken Thompson demonstrated another Trojan horse technique in the 1970's when working on Unix
- He changed the Unix "login" command so that it would accept either the correct password or a preset (by him) master password
- Any review of the "login" source code would detect this without difficulty
- However, he modified the C compiler to insert this change automatically and then modified the source of the C compiler to insert *that* modification automatically.
- There are now two pieces of malware: the login program and the C compiler, both contain Trojans that cannot be detected by inspecting the source code

  see: http://cm.bell-labs.com/who/ken/trust.html

Case study (continued)

- modern examples of Trojan software range from simple to complex
- e.g. a “phishing” email that claims to have come from your bank, asking you to logon (usually some urgent reason given)
- the “logon” screen they provide looks exactly the same as your normal bank logon screen (but of course it isn’t)
- your password and other credentials are stolen as explained before
- very important that you are redirected smoothly to the correct banking site once they have your password, else you will simply change your password if you realize you have been conned
- more generally you will inadvertently install some software without realizing that it also contains malicious coding.

Example Phishing/Trojan spam email

Secure Your Account

From:Natwest Bank <personal@nwolb.com>

To: Recipients <personal@nwolb.com>

Date:Thu, 29 Aug 2013 10:59 AM

Dear NatWest Customer,

NatWest Bank is constantly working to increase security for all Online Banking users for the best security.

Sign In Here To Secure Your Account

[http://www.qastructures.com/modules/natwest.co.uk/www.nwolb.com/ibcarregister-natwst.html]

This web site is operated by NatWest Personal Banking

Are links safe to click on?

- Look at a simple Google search:
- Search for ECS

  Electronics and Computer Science (ECS) | Electronics and ...

  *www.**ecs**.soton.ac.uk/*
- Actually goes to:

  http://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&ved=0CDgQFjAB&url=http%3A%2F%2Fwww.ecs.soton.ac.uk%2F&ei=5eeMUq_6H8jI0wWZ6YCIBQ&usg=[deleted]&sig2=[deleted]

  (Man-in-the-Middle exploit, but one that the user *already agreed to* by using Google) (see Google T&C)

Computer viruses

- malware that attempts to spread by making copies of itself – into other programs, data files, memory, disk drives or over a network
- does not *always* have a malicious payload
- first reported virus was in 1982: ‘Elk Cloner’, running on Apple II machine
- first PC virus was in 1986 (MSDOS)
- all these early viruses propagated by floppy disk or programs shared on bulletin boards

Virus mechanisms

- infection mechanism: how does it spread?
- trigger mechanism – what causes the payload to be activated? (e.g. date?)
- payload – what does the virus actually do? (could be collecting information or installing software)
- virus may remain dormant until the trigger event

Email viruses

- Email attachments have now become a major mechanism for virus transmission
- Usually the recipient has to be tricked into opening the attachment
- An .exe file can be disguised in windows as (say) xyz.doc.exe
- Macro viruses exploit the active content available on some applications (e.g. Microsoft Word or Excel)

Virus example

- “I love you” 2000
  – email attachment “LOVE-LETTER-FOR-YOU.txt.vbs”
- .vbs often hidden on Windows systems
- Users thought they were opening a text file, instead they were running a VB script
- Image files over-written, copy of email sent to first 50 users in the Microsoft Outlook address book
- “social engineering” – emails appear to come from friends and relations, so safe to open?
- Damage estimated at over $5B worldwide
- 10% of all internet-connected computers worldwide?

Computer worms

- very similar to viruses - often confused
- ‘worm’ can propagate directly across network (i.e. self-contained)

  (also self-replicating)
- increasing trend to use either term?
- worm gains access to distant networks by exploiting vulnerabilities in services

The Morris worm

- first computer worm – November 1988
- Robert Morris Jnr – Cornell PGR student
- son of Robert Morris, responsible for original Unix password authentication system at Bell Labs and (at the time) working for the NSA
- ‘proof of concept’ – no malicious intent
- maybe 6,000 machines affected? (guess)

The Morris worm (2)

- Morris convicted of felony, $10,000 fine + 3 years probation + 400 hours community work
- just 99 lines of code!
- connected to another computer using vulnerabilities, run at new location, repeat
- buffer overflow in *fingerd*, password guessing, *sendmail* backdoor
- code error led to multiple infection: first ‘denial of service’ attack

More worms

- “Code Red” (July 2001) – attacks Microsoft IIS (Internet Information Services) web servers
- about 360k infected hosts at peak (in 14 hours)
- exploited vulnerability in IIS indexing software using a buffer overflow (security patch had been released a month earlier – but many customers had not installed the update)
- payload defaced the web site, then action depended on day-of-the-month
  - day 1-19 look for more IIS servers
  - day 20-27 launch DOS attacks on several fixed IP addresses (e.g. 198.137.240.91, www.whitehouse.gov)

Code Red buffer overflow

GET /default.ida?NNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNN
%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801
%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3
%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a HTTP/1.0

string of N’s to overflow buffer: payload follows
interpreted as computer instructions which will propagate the worm

Code Red 2 worm

- August 2001
- completely different software (despite comment “Code red 2” in code)
- exploited same vulnerability
- payload was boot-resistant backdoor
- pseudo-random choice of targets (prefers targets on own subnet)

Code Red 2 Backdoor

- replaced explorer.exe with modified copy on C: and D: drives
- copy “cmd.exe” to special directories
- modify registry to give special directories full system access (i.e. read/write/execute all files)
- full access now possible by running command window in special locations
- worm continues to run in background: every ten minutes resets registry entries

Nimda worm

- September 2001 (“admin” backwards)
- most widespread virus/worm – in just 22 minutes
- multi-mode propagation (five methods)
  - IIS servers from infected clients
  - direct copy via open network shares
  - email + virus payload to address book
  - modifying web pages on host server (attempt to infect webserver clients using Javascript exploit)
  - Code Red 2 backdoor

  (see http://www.cert.org/advisories/CA-2001-26.html)

To be concluded…

…in “Malware-2”