Malware-2

Ed Zaluska

COMP6230:
Implementing Cybersecurity

Review of Malware-1

- what is malware?
- why does it exist?
- case studies and examples
  - Trojan horse
  - viruses
  - worms (to be concluded)

SQL Slammer worm

- January 2003
- exploited buffer overflow in Microsoft SQL server (patch to fix this had been released six months earlier…)
- infected 90% of vulnerable hosts inside 10 minutes
- very small: just 376 bytes, fits inside a single IP packet (hence can use UDP)
- Internet denial of service because internet routers collapsed under very high traffic: some crashed or became unusable (over 15% packet loss at peak)

Conficker worm

- November 2008 (but still active, because propagation/update strategy continually changes – still over 1 million?)
- propagates using flaws in Windows software and dictionary attacks on admin passwords
- some military systems infected!
- self-defence – e.g. disables Windows update, kills anti-malware software, scans every second to detect patches or diagnostic utilities
- later versions designed to install *botnet client*

Bots and Botnets

- First detected 2001, serious problem since 2009
- once a host machine has been compromised by malware (e.g. virus or worm), it installs malware to become a *botnet client* (or *bot*, or *zombie*)
- a large number of such bots will be created…
- a botnet master (or *bot herder*) will send commands to the clients from a *command-and-control (C&C) server* (originally using *Internet Relay Chat* (IRC), now usually twitter or HTTP)

Bots and Botnets (continued)

- a botnet is typically used for DDOS attacks… or sending email spam… or running spyware… or hosting illegal content… or mining bitcoins
- the botnet can be *hired out* to other criminals

  (entire “black economy” created, with infrastructure and marketplaces)
- modern botnets now using P2P messages, distributed and replicated C&C, greater emphasis on stealth to avoid detection – and can detect attempts to disable the network (possible countermeasures?)

Adware and Spyware

- aware is any software advertising something
- legitimate if with user's consent and knowledge
- **malware** when unwanted
- is it a serious problem, or just annoying?
- what if user activity is recorded and reported back (spyware)?

Scareware

- e.g. “We have detected that your computer has been infected with a virus! Click here for a removal package”
- usually the claimed virus is bogus (as is the downloaded package)
- the victim either pays for the worthless package or (if it was “free”) unwittingly installs dangerous malware

Hoaxware

typically “there is a dangerous virus going around! Quickly, email all your friends to warn them about this…”

E.g. http://www.snopes.com/computer/virus/jdbgmgr.asp

“I got this message about a virus that can produce lot of dammage [sic] to your computer. If you follow the instructions which are very easy, you would be able to "clean" your computer. Apparently the virus spreads through the adresses book .

I got it, then may be I passed it to you too, sorry. The name of the virus is jdbgmgr.exe and is transmitted automatically through the Messanger and addresses book of the OUTLOOK.

The virus is neither detected by Norton nor by Mc Afee. It remains in lethargy ("sleeping") for 14 days and even more, before it destroys the whole system. It can be eliminated during this period.”

Ransomware

- restricts access to infected computer (or files): computer held “hostage”
- payment required to criminals to restore access – money needs to be untraceable (for obvious reasons), usually international:

  e.g. Western Union, bitcoins, premium-rate telephone numbers
- ‘simple’ ransomware little more than scareware
- more advanced ransomware a serious problem:

  files encrypted with ‘hard’ cryptography (need good back-ups, recover files rather than pay?)

Ransomware (continued)

- Example - Cryptlocker
  http://www.theregister.co.uk/2013/11/15/cryptolocker_menace_triggers_nca_alert/
- Control server generates a 2048-bit RSA key pair, sends the public half to the malware.
- The malware generates a new 256-bit random key for each file on the computer, encrypts the file using 256-bit AES, encrypts each random key with the asymmetric public key and stores the encrypted key before deleting the unencrypted random key and your original files.
- Ransom of 2 bitcoins ($2k?) to release the private key
- (exchange rate from http://preev.com/)

Backdoor/(Trapdoor)

- anything that avoids the normal authentication mechanism (hence allowing illegal access without a password)
- e.g. Ken Thompson Unix backdoor (master password hard-coded into system)
- e.g. unauthorised “Back Orifice” (designed for remote system administration), but often incorporated into malware)

  (“server” installed into target system and controlled by remote client - usually listens for TCP/UDP commands on specific port)

Keylogging

- ‘keystroke logging’, recording keystrokes as keys are pressed on a keyboard - without the user being aware
- can capture passwords as they are typed
- software mechanisms can use several different mechanisms
- also network keyloggers and hardware keyloggers
- all need a mechanism to communicate the captured keystrokes to whoever installed the keylogger *without being detected*

Tempest (codename)

- can detect computer activity by the EM (electromagnetic) radiation emitted by all hardware (not just wireless devices) if sufficiently close – without any hardware connection
- not new: military and national security agencies have been actively using since the 1970's
- military etc. computers are specifically hardened to prevent such eavesdropping
- 'Tempest' now usually refers to the entire field of emission security

Rootkits

- usually malware, but not always

  (Sony 2005 DRM rootkit – was this malware? Not fully disclosed in EULA)
- key objective is *stealth*: existence of rootkit and payload hidden and undetectable
- typically modifies OS kernel together with system tools capable of detecting changes
- (e.g. in Unix there would be modified versions of ps, who, ls, passwd etc.)
- removal difficult: re-install OS from scratch?

Additional topics…

- drive-by download
- zero-day exploit
- spear phishing
- man-in-the-middle attacks
- timing attacks
- covert channels
- logic bomb and time bomb
- virus detection (early anti-virus used ‘signature detection’, but modern viruses are polymorphic: multiple detection techniques now used)
- IPv6: address scanning no longer attractive

Conclusions

- overview of a complex topic
- many different malware attacks possible
- wide variety of malware mechanisms

- difficult or impossible to prevent attacks
- countermeasures:
  - apply patches immediately
  - configure systems correctly
  - user education