Malicious Software

Malicious Software

Malicious software: programs exploiting system vulnerabilities

- Need a host program or independent
  - program fragments: viruses, logic bombs, backdoors
  - self contained programs: worms, bot programs
- Self replicating or activated by trigger
  - viruses, worms
  - logic bombs, back doors, bot programs
- Action/payloads once a target is reached

Malware Terminology

- Virus: malware that tries to replicate into other programs. When that program is ran the virus is executed as well.
- Worm: program that can run independently and replicate to other systems through the network
- Logic bomb: code inserted from intruder. Lies dormant until precondition is met and then executes
- Trojan horse: a computer program that seems useful but also contains malware in it
- Backdoor (trapdoor): any mechanism that bypasses security check to allow unauthorized functionality
- Mobile code: software that can be shipped out to any platform
- Spammers and Flooder programs: Use to send large volume of emails
- Keyloggers: capture keystrokes
- Rootkit: set of hacker tools after attacker has root-level access
- Zombie, bot: program activated on infected machine that will attack other machines

Viruses

Virus: piece of software that infects other programs

- modifying them to include a copy of the virus
- executes secretly when host program is ran

Specific to operating system and hardware

- taking advantage of their details and weakness

A typical virus goes through four phases:

1. dormant: virus is idle, activated by some event, not all viruses go through this phase
2. propagation: virus copies itself to other programs, copy may not be identical, it morphs sometimes to evade detection
3. triggering: virus is activated and performs what it was suppose to do
4. execution: function is performed

Virus Structure

Components:

- infection mechanism: enables replication
- trigger: event that makes payload activate
- payload: what it does, malicious or benign

Components are prepended / postpended / embedded to host program

Systems can block:

- initial infection (difficult)
- propagation (with access control)a

Virus Classification

Classification by infection target:

- boot sector: affects master boot record
- file infector: infects file in OS
- macro virus: infect scripting code

Classification by concealment strategy

- encrypted virus (virus body: infection, trigger, payload)
- polymorphic virus (mutates its encryption/decryption code with every infection without changing semantics and engine)
- metamorphic virus (mutates with every infection with complete rewriting including engine)

Macro Virus

Macro virus: common in mid-1990's

- platform independent
- infect documents
- easily spread (by email)

Exploit macro capability of office apps

- executable program embedded in office doc
- often a form of Basic
- more recent releases include protection

Recognized by many anti-virus programs

Virus Countermeasures

Prevention: ideal solution but difficult

Realistically: detection, identification, removal

- if detect but can't identify or remove, must discard and replace infected program
- detection or identification techniques
  - signature scanners
  - heuristics

Generic Decryption

Run executable files through **generic decryption** scanner:

- CPU emulator to interpret instructions
- virus scanners to check known virus signatures
- emulation control module to manage process

Let virus decrypt itself interpreter

Periodically scan for virus signatures

Issue is long to interpret and scan

Worms

Worms: replicating program that propagates over network

- Uses email, remote exec, remote login

Has phases:

- dormant → propagation → triggering → execution
- propagation phase: actively searches for other systems, connects to it, copies self to it and runs

May disguise itself a system process

Morris Worm

Best known worm, released by Robert Morris. Various attacks on UNIX systems:

- discover other hosts known to current host
- crack password file to log on to remote hosts
- exploit a bug in the finger protocol
- exploit a backdoor in sendmail

If succeeded: have remote shell access

- can send bootstrap program to copy worm over

Worm Technology and Countermeasures

Multiplatform, multi-exploit, ultrafast spreading, polymorphic, metamorphic, transport vehicles for other attacks, zero-day exploit

Countermeasures overlap with anti-virus techniques

- signatures, heuristics
- worms also cause significant network activity, thus activity and usage monitoring can be helpful
- requirements on generality, timeliness, resiliency, minimal denial-of-service costs, transparency.

Bots

Program taking over other computers

If coordinated from a botnet:

- bots execute attack routines
- control module sends commands to active/update bots, etc

Characteristics:

- remote control facility (internet relay chat, http)
- attack network construction (attack software, vulnerability, scanning strategy)

Rootkits

Set of programs installed for admin access

Makes malicious and stealthy changes to host OS

- may hide its existence: subverting report mechanisms in process
- may be: persistent or memory based
- installed via trojan or intruder on system
- range of counter measures: IDS, file integrity check, etc