Review

- Chapter 6 – Malware
  - History of malware
  - Malware terminology
- Virus
  - Virus design
  - Virus classification
  - Virus concealment strategies

Virus Countermeasures

- Prevention - ideal solution but difficult
- Realistically need:
  - Detection
  - Identification
  - Removal
- If detection attempted but can’t identify or remove, must discard and replace infected program
Anti-Virus Evolution

- Virus & antivirus technology have both evolved
- Early viruses simple code, easily removed
- As becoming more complex, so must the countermeasures

Antivirus Generations

- **First-generation** scanner
  - Requires a virus signature to identify a virus
  - Virus may contain "wildcards" but has essentially the same structure and bit pattern in all copies
  - Signature-specific scanners are limited to the detection of known viruses

Antivirus Generations

- **Second-generation** scanner
  - Uses heuristic rules to search for probable virus infection
    - e.g. to look for fragments of code that are often associated with viruses.
  - Can use integrity checking, using a hash function rather than a simpler checksum.
Antivirus Generations

- **Third-generation** scanners
  - Memory-resident programs that identify a virus by its actions rather than structure in an infected program.
  - Not necessary to develop signatures / heuristics, but only to identify the small set of actions indicating an infection is attempted and then intervene.

Antivirus Generations

- **Fourth-generation** scanner
  - Packages consisting of a variety of antivirus techniques used in conjunction
  - Include scanning and activity trap components
  - Include access control capability, which limits the ability of viruses to penetrate a system
    - Limits the ability of a virus to update files in order to pass on the infection.

Behavior Blocking Software

- Seeks to identify virus by monitoring behavior of programs in real-time
  - Attempts to open, view, delete, and/or modify files;
  - Attempts to format disk drives and other unrecoverable disk operations;
  - Modifications to the logic of executable files or macros;
  - Modification to critical system settings, such as start-up settings;
  - Scripting of e-mail and instant messaging clients to send executable content; and
  - Random initiation of network communications.
Behavior-Blocking Software

1. Administrator sets up e-mail blocking software on server.
2. Administrator sends e-mail through firewall.
3. Server reads e-mail.
4. Server blocks e-mail if it contains malware.

Generic Decryption Based Antivirus

• Runs executable files through GD scanner:
  – CPU emulator to interpret instructions
  – Virus scanner to check known virus signatures
  – Emulation control module to manage process
• Lets virus decrypt itself in interpreter
• Periodically scan for virus signatures
  – Various exposes itself
• Issue is long to interpret and scan
  – Tradeoff chance of detection vs time delay

Digital Immune System
Worms

- Replicating program that propagates over net
  - Using email, remote exec, remote login
- Has phases like a virus:
  - Dormant, propagation, triggering, execution
  - Propagation phase: searches for other systems, connects to it, copies self to it and runs
- May disguise itself as a system process
- Implemented first by Xerox Palo Alto labs in 1980's
  - Non malicious. Search for idle systems to run a computationally intensive task

Morris Worm

- One of the best known worms
- Released by Robert Morris in 1988
- Various attacks on UNIX systems
  - Cracking password file to use login/password to logon to other systems
  - Exploiting a bug in the finger protocol
  - Exploiting a bug in sendmail
- If succeed have remote shell access
  - Send bootstrap program to copy worm over

Worm Components

- Warhead
- Propagation Engine
- Target Selection Algorithm
- Scanning Engine
- Payload
Worm Warhead

- Code that exploits some vulnerability to break into a target system
- Most popular techniques
  - Buffer overflow attacks
  - File-sharing attacks
  - Email systems allowing executable attachments
  - Common misconfiguration most notably use of default password

Propagation Engine

- Warhead opens the door to the target system.
  The Propagation Engine transfers the rest of the body of the worm into the system
- Most popular
  - FTP (uses clear-text user-id and password)
  - TFTP (allows unauthenticated access)
  - HTTP
  - SMB (Server Message Block protocol used for Windows file sharing. Unix servers running SAMBA support SMB)

Target Selection Algorithm

- Looks for new victims to attack
- Popular
  - Email addresses
  - Host lists (from /etc/hosts or LMHOSTS)
  - Trusted systems (from .rhosts or equivalent files)
  - Network neighborhood (using NetBIOS or SMB protocol)
  - DNS Queries
  - Randomly selecting target network address
Scanning Engine

- Scans the network for suitable victim using the list of targets generated by the target selection engine
- Most popular
  - Open ports scanning
  - Vulnerability scanning

Worm Payload

- Code designed to implement some specific action on the target system
- Most popular
  - Plant a Backdoor (to allow remote control of system)
  - Plant a DDoS Flood Agent (to allow launching a DDoS attack remotely)
  - Perform complex mathematical operation (typically cracking crypto keys)

Worm Propagation Model
Newer Worm Technology

• Multiplatform
  – Newer worms are not limited to Windows machines but can attack a variety of platforms, especially the popular varieties of UNIX.

• Multi-exploit
  – Newer worms penetrate systems in a variety of ways, using exploits against Web servers, browsers, email, file-sharing, and other network based applications.

Newer Worm Technology

• Ultrafast spreading
  – One technique to accelerate the spread of a worm is to conduct a prior Internet scan to accumulate Internet addresses of vulnerable machines.

• Polymorphic
  – To evade detection, skip past filters, and foil real-time analysis, worms adopt the virus polymorphic technique. Each copy of the worm has new code generated on the fly using functionally equivalent instructions and encryption techniques.

Newer Worm Technology

• Metamorphic
  – In addition to changing their appearance, metamorphic worms have a repertoire of behavior patterns that are unleashed at different stages of propagation.

• Transport vehicles
  – Because worms can rapidly compromise a large number of systems, they are ideal for spreading other distributed attack tools, such as distributed denial of service bots.

• Zero-day exploit
Worm Countermeasures

- Overlaps with anti-virus techniques
- Once worm on system A/V can detect
- Worms also cause significant net activity
- Worm defense approaches include:
  - Detection approaches
  - Prevention

Detection Approaches (1)

- Signature-based worm scan filtering:
  - Generates a worm signature, which is then used to prevent worm scans from entering/leaving a network/host.

Detection Approaches (2)

- Filter-based worm containment:
  - Focuses on worm content rather than a scan signature. The filter checks a message to determine if it contains worm code.
Detection Approaches (3)

- Payload-classification-based worm containment:
  - Examine packets to see if they contain a worm using anomaly detection techniques

Detection Approaches (4)

- Threshold random walk (TRW) scan detection:
  - Exploits randomness in picking destinations to connect to as a way of detecting if a scanner is in operation

Prevention Approaches (1)

- Rate limiting:
  - Limits the rate of scanlike traffic from an infected host.
Prevention Approaches (2)

- Rate halting:
  - Immediately blocks outgoing traffic when a threshold is exceeded either in outgoing connection rate or diversity of connection attempts.
  - Rate halting can integrate with a signature- or filter-based approach so that once a signature or filter is generated, every blocked host can be unblocked.
    - Rate halting techniques are not suitable for slow, stealthy worms.

Proactive Worm Containment

Network Based Worm Defense
Bots

- Program taking over other computers
- To launch hard to trace attacks
- If coordinated then form a botnet
- Characteristics:
  - Remote control facility
    - via IRC/HTTP etc
  - Spreading mechanism
    - attack software, vulnerability, scanning strategy
- Various counter-measures applicable

Rootkits

- Set of programs installed for admin access
- Malicious and stealthy changes to host O/S
- May hide its existence
  - Subverting report mechanisms on processes, files, registry entries etc
- May be:
  - Persistent or memory-based
  - User or kernel mode
- Installed by user via Trojan or intruder on system
- Range of countermeasures needed

Summary

- Introduced types of malicious software
  - backdoor, logic bomb, Trojan horse, mobile
- Virus types and countermeasures
- Worm types and countermeasures
- Bots
- Rootkits