Malware: Past, Present, and Future – Notes

Introduction

- Malware = Malicious Software – software designed to harm or exploit systems.
- Can hide inside seemingly harmless programs.
- Evolved from harmless pranks → billion-dollar crimes (like ransomware).
- Too many types exist — focus on key examples & trends.

Malware of the Past

General Traits

- Early malware was mostly for mischief or fame, not money.
- Motivations: curiosity, ego, disruption.
- Types included viruses, worms, Trojans, boot sector malware, macro viruses, and rootkits.

Viruses

- Attach to files and require user action to spread (like opening or running something).
- Example: ILOVEYOU Virus (2000)
- Spread via email attachments.
- Looked like a love letter (VB script).
- Overwrote image files and caused billions in damage.
- Required users to double-click to activate.

Worms

- Self-replicating malware that spreads across networks without user action.
- Example: Morris Worm (1988)
- Spread via early internet (ARPANET).
- Exploited system vulnerabilities.
- A bug caused it to replicate uncontrollably, crashing systems.
- Showed how a “mistake” could cripple the internet.

Trojan Horses

- Malware disguised as legitimate software.
- Trick users into running them.
- Example: Zeus Trojan (2007)
- Banking Trojan; used “man-in-the-browser” attacks.

- Stole credentials and intercepted data.
- Could alter transactions invisibly.

Boot Sector Malware

- Infects the boot sector of disks; runs when the computer starts.
- Spread mainly via floppy disks.
- Example: Michelangelo Virus (1991) – infected DOS systems.
- Rare today because we no longer boot from floppies.

Macro Viruses

- Embedded in Office documents (Word, Excel).
- Trigger when the file is opened.
- Example: Concept (1995) – first proof-of-concept macro virus.
- Example: Melissa (1999) – emailed itself to 50 contacts.
- Mixed virus + worm features.

Rootkits

- Hide deep inside the operating system, altering core behavior.
- Make malware invisible to users and antivirus tools.
- Often very persistent and hard to detect.

Summary of Past Malware

- Loud and visible – crashed systems, displayed weird messages.
- Easier to spot.
- Decline due to:
- Better OS security.
- Improved antivirus tools.
- Widespread multi-factor authentication (MFA).

Malware of the Present

General Traits

- Modern malware = stealthy + profitable.
- Focus: money, data theft, control.
- Key types: ransomware, info stealers, RATs, IoT botnets, cryptojackers.

Ransomware

- Encrypts or steals data and demands payment.
- Two main types:
- Encrypts your files — pay to unlock.
- Steals your data — pay to stop leaks.
- Example: WannaCry (2017)
- Hit hospitals & companies worldwide.
- Demanded Bitcoin ransom.
- Estimated $4–8 billion in damages.

Info Stealers

- Steal sensitive data like passwords or IDs.
- Collect:
- Login credentials
- Credit card numbers
- Personal or business information
- Attackers use or sell the data for fraud or identity theft.
- Increasingly common (IBM X-Force report).

RATs (Remote Access Trojans)

- Trojan that gives attackers remote control of your system.
- Can:
- Spy on screen activity.
- Use webcam or mic.
- Track GPS on mobile.
- Example: Pegasus – highly advanced mobile RAT used to spy on journalists.
- Very invasive and hard to remove.

IoT Malware

- IoT = Internet of Things (smart devices, cameras, DVRs, etc.)
- Every device = a small computer → all can be hacked.
- Example: Mirai Botnet (2016)
- Infected IoT devices worldwide.
- Used them to perform massive DDoS attacks.
- Owners often didn’t know their devices were part of attacks.

Cryptojackers

- Hijack your computer's CPU/GPU to mine cryptocurrency secretly.
- Slows your system, uses power — attacker gets the profit.

Malware of the Future

AI-Driven Malware

- Uses artificial intelligence to adapt, plan, and evade defenses.
- Can:
- Read vulnerability reports (CVEs) and generate exploit code automatically.
- Learn from defenses and alter itself.
- Target weak systems intelligently.
- Study showed GPT-4 could write exploit code for 87% of CVEs tested.

Polymorphic & Adaptive Malware

- Changes code slightly each time it spreads → hard to detect.
- AI could make this much smarter and faster.

Deepfake-Based Attacks

- Use AI to fake voices or videos (e.g., your boss calling you).
- Combine social engineering + malware for scams and data theft.
- Highly realistic and dangerous in corporate environments.

Protecting Yourself (and Organizations)

1.Keep Systems Patched

- Update OS, apps, and devices.
- Most attacks exploit known, unpatched vulnerabilities.

2. User Training

- Avoid downloading untrusted software or clicking strange links.
- Educate employees about phishing and unsafe behavior.

3. Use Antivirus / EDR

- Traditional antivirus = signature based.

- Modern EDR (Endpoint Detection & Response) = behavior-based, detects unknown threats.

4. Backups

- Keep regular backups of important data.
- Store backups offline or offsite.
- Check they aren't infected.

5. Limit Privileges

- Don't give admin access unless necessary.
- Malware run under limited accounts can't do much harm.

6. Firewalls

- Personal firewalls: block or monitor incoming/outgoing traffic.
- Network firewalls: stop self-replicating threats like worms.

7.Monitoring & Visibility

- Use SIEM (Security Information and Event Management) systems.
- Centralize logs and alerts — "You can't secure what you can't see."