Lecture 3: Malicious Software (Malware)

Theme: Malware and Social Engineering
Technical University of Moldova
Lecturer: Maxim Masiutin, Associate Professor

Introduction

Hello, everyone. Today we enter the world of malicious software, commonly known as malware. This is one of the most dynamic areas of cybersecurity, with new threats emerging daily and attackers constantly evolving their techniques.

Let me start with some numbers that illustrate the scale of the problem. According to SonicWall, a network security company, there were over 783 million ransomware attack attempts recorded globally in 2025, up from 658 million in 2024. Projections for 2026 suggest this number could exceed one billion attempts. And ransomware is just one type of malware.

Cyble, a cyber threat intelligence company, observed 57 new ransomware groups and 27 new extortion groups in 2025, along with over 350 new ransomware strains. The malware ecosystem is vast, sophisticated, and highly profitable for criminals. Understanding how malware works is essential for defending against it.

Part 1: Malware Taxonomy

Malware is any software intentionally designed to cause damage to a computer, server, network, or user. The term combines "malicious" and "software." Let us examine the major categories.

Viruses

A **virus** is malware that attaches itself to a legitimate program or file and spreads when that program is executed. Like biological viruses, computer viruses cannot propagate without a host.

Characteristics:

- Requires user action to spread (running infected program)

- Attaches to legitimate files
- May damage or modify files
- Can spread via infected media, email attachments, downloads

Types of viruses:

- **File infectors**: Attach to executable files
- **Boot sector viruses**: Infect the master boot record
- **Macro viruses**: Hide in document macros (Word, Excel)
- **Polymorphic viruses**: Change their code to avoid detection
- **Metamorphic viruses**: Completely rewrite themselves

Historical note: Viruses were dominant in the 1990s and early 2000s but have become less common as other malware types have proven more effective for attackers.

Worms

A **worm** is self-replicating malware that spreads automatically across networks without requiring user action or a host program. This makes worms particularly dangerous because they can spread rapidly.

Characteristics:

- Self-replicating
- Spreads automatically via network
- No host program required
- Can consume bandwidth and system resources
- Often exploits vulnerabilities for propagation

Famous examples:

- **Morris Worm (1988)**: One of the first worms, crashed 10% of internet-connected computers
- **Code Red (2001)**: Exploited IIS vulnerability, infected 359,000 computers in 14 hours
- **SQL Slammer (2003)**: Infected 75,000 servers in 10 minutes
- **Conficker (2008)**: Infected millions of computers, still active today
- **WannaCry (2017)**: Combined worm spreading with ransomware payload

Trojans

A **Trojan** (or Trojan Horse) is malware disguised as legitimate software. Users are tricked into installing it, thinking they are getting something useful.

Named after the Greek myth where soldiers hid inside a wooden horse to enter Troy, Trojans appear harmless but contain hidden malicious functionality.

Characteristics:

- Disguised as legitimate software
- Requires user to install
- Does not self-replicate
- Often provides backdoor access
- May have legitimate-appearing functionality

Types of Trojans:

- **Remote Access Trojans (RATs)**: Provide remote control to attackers
- **Banking Trojans**: Steal financial credentials
- **Downloader Trojans**: Download additional malware
- **Spy Trojans**: Monitor user activity
- **Game-thief Trojans**: Steal gaming account credentials

Ransomware

Ransomware encrypts victim files or locks systems, demanding payment (usually in cryptocurrency) for restoration. This has become the dominant malware threat in recent years.

Characteristics:

- Encrypts files or locks systems
- Demands ransom payment
- Often uses strong encryption
- May have time-limited demands
- Increasingly targets organizations over individuals

Evolution of ransomware:

- **Early ransomware**: Simple screen lockers
- **CryptoLocker (2013)**: First widely successful encryption ransomware
- **Double extortion (2019+)**: Steal data before encrypting, threaten to publish
- **Triple extortion**: Add DDoS (Distributed Denial of Service) attacks or contact victims' customers
- **Ransomware-as-a-Service**: Criminal business model

The statistics are alarming: according to Cyble, publicly reported ransomware attacks rose to 7,200 in 2025 compared to 4,900 in 2024, a 47 percent increase. According to

Coveware, a ransomware incident response firm, over 60 percent of ransomware attacks now include data exfiltration components.

According to the IBM/Ponemon Cost of a Data Breach Report 2025, the average total cost of a ransomware attack, including downtime, recovery, and reputational damage, ranges between 1.8 million and 5 million dollars per incident. Healthcare and manufacturing face the highest costs due to operational disruption.

Spyware

Spyware secretly monitors user activity and collects information without consent. It may track browsing habits, capture keystrokes, or gather personal information.

Characteristics:

- Operates covertly
- Collects user information
- May slow system performance
- Often bundled with free software
- Difficult to detect

Types:

- **Keyloggers**: Record keystrokes to capture passwords
- **Screen capture**: Take screenshots of user activity
- **Browser hijackers**: Modify browser settings, redirect searches
- **Tracking cookies**: Monitor browsing behavior
- **Commercial spyware**: Tools like Pegasus used for surveillance

Rootkits

A **rootkit** is malware designed to provide privileged access while hiding its presence from detection tools. The name comes from Unix systems where "root" is the administrator account.

Characteristics:

- Hides from operating system
- Provides persistent access
- Extremely difficult to detect
- May modify OS components
- Often requires complete system reinstallation to remove

Types:

- **User-mode rootkits**: Operate at application level
- **Kernel-mode rootkits**: Operate at OS kernel level
- **Bootkits**: Infect boot process, load before OS
- **Firmware rootkits**: Hide in hardware firmware

Detection of rootkits often requires booting from clean media and scanning the system from outside.

Bootkits

A **bootkit** is an advanced rootkit that infects the boot process, loading before the operating system. This allows it to evade detection by security software that loads after the OS.

Bootkits target:

- Master Boot Record (MBR)
- Volume Boot Record (VBR)
- UEFI firmware

Because bootkits load before the OS, they can intercept and modify any OS function, making them extremely dangerous.

Adware

Adware displays unwanted advertisements on user systems. While sometimes considered less dangerous than other malware, adware can degrade system performance, track user behavior, and serve as a vector for more dangerous malware.

Characteristics:

- Displays unwanted ads
- May track browsing behavior
- Often bundled with free software
- Can redirect search results
- May install additional unwanted software

Cryptojacking Malware

Cryptojacking malware uses victim systems to mine cryptocurrency without consent. While not destructive, it consumes computing resources and electricity.

Characteristics:

- Mines cryptocurrency

- Consumes CPU/GPU resources
- Increases electricity costs
- May cause hardware damage from overuse
- Often delivered through browser-based exploits

Part 2: Infection Vectors and Propagation

Understanding how malware reaches systems helps us implement effective defenses.

Email-Based Delivery

Email remains the most common malware delivery mechanism:

- **Malicious attachments**: Documents with macros, executable files
- **Malicious links**: Leading to exploit kits or malware downloads
- **Archive files**: ZIP, RAR files containing malware
- **HTML smuggling**: Encoding malware in HTML attachments

Drive-By Downloads

Users become infected simply by visiting compromised websites:

- Exploit kits target browser vulnerabilities
- No user interaction required beyond visiting the page
- May use legitimate sites that have been compromised
- Malvertising delivers malware through advertising networks

Software Vulnerabilities

Malware exploits vulnerabilities in software:

- Unpatched operating systems
- Outdated applications
- Browser plugin vulnerabilities
- Zero-day exploits

Removable Media

USB drives and other removable media can spread malware:

- Autorun functionality (largely disabled now)
- Social engineering to run malicious files
- Firmware-level infections

Network Propagation

Worms and some other malware spread across networks:

- Exploiting vulnerable services
- Using stolen credentials
- Leveraging trust relationships

Supply Chain

Malware can be introduced through the software supply chain:

- Compromised software updates
- Infected open-source components
- Trojanized development tools

According to the Verizon Data Breach Investigations Report (DBIR) 2025, 29 percent of ransomware infections originated through third-party vendors, up from 17 percent in 2024.

Part 3: Ransomware Deep Dive

Given the prevalence and impact of ransomware, let us examine it in more detail.

Ransomware-as-a-Service (RaaS)

The RaaS model has transformed ransomware into a criminal industry:

How RaaS works:

1. Developers create ransomware and infrastructure
2. Affiliates pay for or rent access to the platform
3. Affiliates conduct attacks using the tools
4. Profits are split (typically 70-80% to affiliate)

Benefits for criminals:

- Developers profit without conducting attacks
- Affiliates need minimal technical skills

- Scalable criminal operations
- Shared infrastructure and support

As Europol notes in the Internet Organised Crime Threat Assessment (IOCTA), this model has "democratized cybercrime to an unprecedented degree." Anyone with basic internet knowledge can use these services.

Double and Triple Extortion

Modern ransomware goes beyond simple encryption:

Double extortion:

1. Attackers steal sensitive data
2. Attackers encrypt files
3. Demand payment to decrypt AND prevent data publication
4. Even if backups exist, data exposure threat remains

Triple extortion:

1. All of the above
2. Plus DDoS attacks against victims
3. Plus contacting victims' customers or partners
4. Additional pressure tactics

According to the State of Ransomware Report 2025 by Sophos, a cybersecurity company, over 60 percent of ransomware attacks now include data exfiltration. The majority of new ransomware groups adopt double extortion immediately because it increases return on investment and reduces victim negotiation leverage.

Ransomware Attack Lifecycle

Typical ransomware attack progression:

1. **Initial access**: Phishing, vulnerable services, RDP (Remote Desktop Protocol)
2. **Persistence**: Install backdoors, create accounts
3. **Privilege escalation**: Gain administrator access
4. **Defense evasion**: Disable security tools
5. **Credential harvesting**: Steal passwords
6. **Lateral movement**: Spread across network
7. **Data collection**: Identify and steal valuable data
8. **Data exfiltration**: Extract data to attacker infrastructure
9. **Impact**: Deploy ransomware, encrypt files

10. **Extortion**: Demand payment, threaten data release

Modern ransomware operators often spend days or weeks inside networks before deploying encryption.

Emerging Ransomware Tactics for 2026

New trends are emerging:

- **DDoS-as-a-Service offerings**: Additional pressure on victims
- **Insider recruitment**: Paying employees to provide access
- **Gig worker exploitation**: Recruiting accomplices online
- **AI-assisted attacks**: Automated victim selection and customization
- **Data-leak extortion without encryption**: Some groups skip encryption entirely

---

Part 4: Fileless Malware and Living-Off-the-Land

Traditional malware writes files to disk, but modern attackers increasingly use fileless techniques.

What is Fileless Malware?

Fileless malware operates entirely in memory without writing persistent files to disk. This makes it extremely difficult to detect with traditional antivirus.

Characteristics:

- No files written to disk
- Resides in memory
- Uses legitimate system tools
- Survives only until reboot (unless persistence achieved)
- Evades signature-based detection

According to the ENISA (European Union Agency for Cybersecurity) Threat Landscape Report 2025, fileless malware attacks increased by 33 percent from 2023 to 2025, targeting endpoint detection blind spots.

Living-Off-the-Land (LOtL) Techniques

Attackers use legitimate system tools for malicious purposes:

Commonly abused tools:

- **PowerShell**: Scripting and automation
- **WMI (Windows Management Instrumentation)**: System management
- **certutil**: Certificate utility misused for downloads
- **bitsadmin**: Background transfer service
- **mshta**: Executes HTA files
- **regsvr32**: Registers COM components

Why LOtL is effective:

- Tools are already present on systems
- Actions may appear legitimate
- Difficult to distinguish malicious use
- Cannot simply block these tools
- Traditional AV focuses on malicious files

Detection Challenges

Fileless and LOtL attacks require different detection approaches:

- Behavioral analysis instead of signatures
- Command-line monitoring
- Script block logging
- Memory analysis
- User and entity behavior analytics (UEBA)

Part 5: Malware Analysis Basics

Security professionals analyze malware to understand threats and develop defenses.

Static Analysis

Static analysis examines malware without executing it:

Techniques:

- **File metadata examination**: Headers, timestamps, compiler information
- **String extraction**: Look for URLs, IP addresses, commands
- **Code analysis**: Disassembly and decompilation
- **Hash calculation**: Generate IOCs (Indicators of Compromise) for detection

- **Packer detection**: Identify obfuscation methods

Tools:

- PEStudio (Windows executables)
- strings command
- IDA Pro, Ghidra (disassemblers)
- VirusTotal (multi-scanner analysis)

Advantages:

- Safe (malware not executed)
- Can reveal capabilities without triggering them

Limitations:

- Obfuscation and packing complicate analysis
- Cannot observe runtime behavior

Dynamic Analysis

Dynamic analysis executes malware in a controlled environment:

Techniques:

- **Sandbox execution**: Run in isolated virtual environment
- **Process monitoring**: Observe process creation and activity
- **File system monitoring**: Track file operations
- **Registry monitoring**: Watch for configuration changes
- **Network monitoring**: Capture communications
- **API monitoring**: Log system calls

Tools:

- Cuckoo Sandbox
- Any.Run (online sandbox)
- Process Monitor
- Wireshark
- API Monitor

Advantages:

- Reveals actual behavior
- Can observe unpacked code

Limitations:

- Malware may detect sandbox and alter behavior

- Some behaviors trigger only under specific conditions
- Risks if containment fails

Sandbox Evasion

Sophisticated malware detects analysis environments:

Detection techniques:

- Check for VM artifacts (drivers, registry keys)
- Timing attacks (sleep to outlast analysis)
- User interaction requirements
- Environment checks (username, machine name)
- Hardware fingerprinting

Countermeasures:

- Bare-metal analysis environments
- Realistic system configurations
- Extended analysis times
- Human interaction simulation

Part 6: Defensive Technologies

Now let us examine technologies that defend against malware.

Signature-Based Detection

Traditional antivirus relies on signatures:

- Database of known malware patterns
- Files compared against signatures
- Fast and accurate for known threats
- Requires regular updates

Limitations:

- Cannot detect new (zero-day) malware
- Easily evaded by modification
- Ineffective against fileless attacks

Heuristic Detection

Heuristics identify malware by behavior patterns:

- Rules based on suspicious characteristics
- Can detect variants of known malware
- May catch some new threats
- Higher false positive rate than signatures

Behavioral Detection

Modern solutions monitor behavior:

- Watch for suspicious actions in real-time
- Detect malware by what it does, not what it looks like
- Effective against fileless and LOtL attacks
- May intervene before damage occurs

Behavioral indicators:

- Mass file modification
- Encryption activities
- Process injection
- Registry modifications
- Network anomalies

Machine Learning Detection

AI/ML enhances malware detection:

- Train models on malware characteristics
- Identify patterns humans might miss
- Adapt to new threats
- Reduce reliance on signatures

Limitations:

- Requires quality training data
- Adversarial attacks can evade ML
- May produce false positives
- Explainability challenges

Endpoint Detection and Response (EDR)

EDR provides comprehensive endpoint protection:

- Continuous monitoring
- Behavioral analysis
- Threat hunting capabilities
- Incident response tools
- Forensic data collection

EDR goes beyond prevention to detect and respond to threats that evade initial defenses.

Sandboxing

Sandboxing isolates potentially dangerous content:

- Email attachments detonated safely
- Downloads analyzed before delivery
- Suspicious files executed in isolation
- Behavior observed without risk

Part 7: Practical Malware Defense Strategies

Let me share practical strategies for defending against malware.

Defense in Depth

Layer multiple protections:

1. Email security gateway
2. Web filtering
3. Endpoint protection
4. Network monitoring
5. User training
6. Backup and recovery

Patch Management

Keep systems updated:

- Prioritize critical vulnerabilities
- Test patches before deployment
- Use automated patching where possible
- Track patch status

Principle of Least Privilege

Limit user and process permissions:

- Users should not have admin rights for daily work
- Applications run with minimal permissions
- Reduces impact of successful malware

Application Whitelisting

Only allow approved applications:

- Block execution of unknown programs
- Very effective but requires management overhead
- Consider for high-security environments

Backup Strategy

Prepare for ransomware:

- Regular, automated backups
- Offline or air-gapped backup copies
- Test restoration procedures
- Immutable backups where possible
- 3-2-1 rule: 3 copies, 2 media types, 1 offsite

Network Segmentation

Limit malware spread:

- Separate critical systems
- Control traffic between segments
- Monitor lateral movement attempts

User Training

Humans are often the weakest link:

- Phishing awareness
- Safe browsing practices
- Reporting suspicious activity
- Regular refresher training

Conclusion

Today we covered the world of malicious software:

1. **Malware taxonomy**: Viruses, worms, Trojans, ransomware, spyware, rootkits, and more
2. **Infection vectors**: Email, drive-by downloads, vulnerabilities, removable media, supply chain
3. **Ransomware evolution**: RaaS model, double/triple extortion, emerging tactics
4. **Fileless malware**: Memory-resident threats and living-off-the-land techniques
5. **Analysis methods**: Static and dynamic analysis approaches
6. **Defensive technologies**: Signatures, heuristics, behavior, ML, EDR, sandboxing
7. **Defense strategies**: Layered approach, patching, least privilege, backups

In our next lecture, we will examine social engineering, where attackers target the human element rather than technical vulnerabilities.

Discussion Questions

1. Should organizations pay ransomware demands? What factors should influence this decision?
2. How can we balance security with usability when blocking potentially malicious content?
3. What role should governments play in combating ransomware?

Thank you for your attention. See you next time.

Review Questions

1. Distinguish between viruses, worms, and Trojans. How do their propagation methods differ?
2. Explain the Ransomware-as-a-Service (RaaS) model and why it has made ransomware more prevalent.
3. What is double extortion in ransomware, and how does it change the risk calculus for organizations?
4. Describe fileless malware and living-off-the-land techniques. Why are they difficult to detect?
5. Compare static and dynamic malware analysis. What are the strengths and limitations of each approach?
6. How do modern EDR solutions differ from traditional signature-based antivirus?
7. What is sandbox evasion, and what techniques do malware authors use to avoid analysis?
8. Outline a defense-in-depth strategy specifically for malware protection.

Key Terms

- **Adware**: Software that displays unwanted advertisements
- **Bootkit**: Malware that infects the boot process to load before the operating system
- **Cryptojacking**: Unauthorized use of computing resources to mine cryptocurrency
- **Double Extortion**: A ransomware tactic combining data encryption with data theft, threatening to publish stolen data if ransom is not paid
- **Drive-By Download**: Malware downloaded automatically when visiting a compromised website
- **Dynamic Analysis**: The process of analyzing malware behavior by executing it in a controlled environment
- **EDR**: Endpoint Detection and Response, advanced endpoint security providing visibility and response
- **Fileless Malware**: Malware that operates entirely in memory without writing files to disk
- **Living off the Land (LOtL)**: Using legitimate system tools for malicious purposes
- **Ransomware**: Malware that encrypts data and demands payment for decryption
- **Ransomware-as-a-Service (RaaS)**: A criminal business model providing ransomware tools to affiliates

- **Rootkit**: Malware designed to hide its presence and provide continued privileged access
- **Sandbox**: An isolated environment for safely analyzing suspicious code
- **Sandbox Evasion**: Techniques used by malware to detect and avoid analysis in sandboxed environments
- **Spyware**: Software that covertly collects information about a user
- **Static Analysis**: The process of analyzing malware without executing it, examining code structure and signatures
- **Trojan**: Malware disguised as legitimate software
- **Virus**: Malware that attaches to programs and replicates when the host program executes
- **Worm**: Self-replicating malware that spreads across networks without user interaction

References and Further Reading

- NIST SP 800-83: Guide to Malware Incident Prevention and Handling for Desktops and Laptops
- MITRE ATT&CK for Enterprise (attack.mitre.org)
- CISA Stop Ransomware Resources (stopransomware.gov)
- AV-TEST Institute Reports (av-test.org)
- VirusTotal Documentation (virustotal.com)