Malicious code - Malware

Khái niệm cơ bản

- **Malware (Malicious Software)**: Tập lệnh hoặc chương trình chạy trên máy tính và khiến hệ thống thực hiện điều mà kẻ tấn công muốn.
- **Phân loại theo cách lây lan**:
    - **Virus** – cần sự hỗ trợ từ con người (chạy file nhiễm).
    - **Worm** – tự động lây lan không cần tương tác người dùng.
- **Phân loại theo cách ẩn nấp**:
    - **Rootkit** – chỉnh sửa OS để che giấu sự tồn tại.
    - **Trojan** – ngụy trang dưới chức năng hợp pháp nhưng thực hiện hành vi độc hại.
- **Payloads**: Hành vi cụ thể của malware (phá hoại, đánh cắp dữ liệu, cài backdoor…).

Các loại malware phổ biến

Virus

- **Định nghĩa**: Đoạn mã tự chèn vào chương trình host để lây lan, không thể tự chạy.
- **4 giai đoạn**:
    - Dormant (ngủ).
    - Propagation (lây lan).
    - Triggering (kích hoạt).
    - Execution (thực thi).
- **Các loại**:
    - Parasitic (ký sinh).
    - Memory-resident.
    - Boot sector.
    - Macro virus.
    - Stealth virus.
    - Polymorphic virus (biến đổi hình thái để tránh signature-based detection).

Malware (Mã độc)

- **Định nghĩa**: Phần mềm độc hại được thiết kế để gây hại, đánh cắp dữ liệu hoặc chiếm quyền kiểm soát hệ thống.
- **Cách lây**: Email, web, USB, tải phần mềm lậu.
- **Phòng chống**: Antivirus, cập nhật hệ thống, cảnh giác link/file lạ.

Computer Virus

- **Đặc điểm**: Gắn vào file/chương trình, cần người dùng chạy để kích hoạt.
- **Lây lan**: Khi file bị nhiễm được sao chép/chia sẻ.
- **Phòng chống**: Không mở file lạ, dùng phần mềm quét virus.

Virus Hoax

- **Đặc điểm**: Tin nhắn/cảnh báo giả về virus để lừa người dùng làm hành động gây hại.
- **Lây lan**: Email, mạng xã hội, tin nhắn.
- **Phòng chống**: Kiểm chứng thông tin trước khi hành động.

Worm

- **Đặc điểm**: Tự nhân bản, lây qua mạng không cần người dùng.
- **Tác hại**: Chiếm băng thông, lây nhanh chóng.
- **Phòng chống**: Vá lỗ hổng, firewall, IDS/IPS.

Ransomware

- **Đặc điểm**: Mã hóa dữ liệu, đòi tiền chuộc.
- **Lây lan**: Phishing, lỗ hổng RDP, phần mềm crack.
- **Phòng chống**: Backup offline, không click link lạ, cập nhật bản vá.

Trojan

- **Đặc điểm**: Giả dạng phần mềm hợp pháp nhưng có mã độc.
- **Tác hại**: Mở backdoor, đánh cắp dữ liệu.
- **Phòng chống**: Cài phần mềm từ nguồn tin cậy, dùng sandbox kiểm tra.

RAT (Remote Access Trojan)

- **Đặc điểm**: Trojan cho phép kẻ tấn công điều khiển máy từ xa.
- **Tác hại**: Xem màn hình, lấy file, điều khiển webcam.
- **Phòng chống**: Antivirus, chặn cổng không cần thiết, giám sát lưu lượng.

Cryptojacker

- **Đặc điểm**: Sử dụng tài nguyên máy để đào tiền ảo trái phép.
- **Tác hại**: Hao CPU/GPU, giảm hiệu suất.
- **Phòng chống**: Chặn script đào coin, quét hệ thống.

Keylogger

- **Đặc điểm**: Ghi lại thao tác bàn phím.
- **Tác hại**: Lộ mật khẩu, thông tin cá nhân.
- **Phòng chống**: Antivirus, phần mềm anti-keylogger.

Logic Bomb

- **Đặc điểm**: Kích hoạt khi điều kiện nhất định xảy ra (ngày giờ, sự kiện).
- **Phòng chống**: Giám sát file và script bất thường.

Malvertising

- **Đặc điểm**: Quảng cáo chứa mã độc trên web.

- **Phòng chống**: Chặn quảng cáo, duyệt web an toàn.

Wiper Virus

- **Đặc điểm**: Xóa sạch dữ liệu, làm hỏng hệ thống.
- **Phòng chống**: Backup định kỳ, phân quyền hợp lý.

Adware

- **Đặc điểm**: Hiển thị quảng cáo không mong muốn, có thể thu thập dữ liệu.
- **Phòng chống**: Chỉ cài phần mềm từ nguồn tin cậy.

Spyware

- **Đặc điểm**: Theo dõi hoạt động, thu thập dữ liệu bí mật.
- **Phòng chống**: Anti-spyware, cập nhật hệ điều hành.

RAM Scraper

- **Đặc điểm**: Đọc dữ liệu nhạy cảm từ RAM (thường là thẻ tín dụng tại POS).
- **Phòng chống**: Mã hóa dữ liệu, vá lỗ hổng ứng dụng.

Rootkit

- **Đặc điểm**: Ẩn tiến trình/mã độc, khó bị phát hiện.
- **Phòng chống**: Dùng tool rootkit detection, cài lại OS khi bị nhiễm.

Backdoor

- **Đặc điểm**: Tạo lối vào bí mật vào hệ thống.
- **Phòng chống**: Kiểm tra dịch vụ và cổng mở, giám sát nhật ký.

Botnet

- **Đặc điểm**: Mạng máy bị chiếm quyền, điều khiển tập trung.
- **Tác hại**: DDoS, spam, phát tán malware.
- **Phòng chống**: IDS/IPS, chặn IP C2.

Fileless Malware

- **Đặc điểm**: Chạy trong bộ nhớ, không lưu file trên đĩa.
- **Phòng chống**: EDR giám sát hành vi, vô hiệu hóa macro/script không cần thiết.

Malicious Macro

- **Đặc điểm**: Macro trong file Office chứa mã độc.
- **Phòng chống**: Tắt macro mặc định, quét file trước khi mở.

Vị trí malware ẩn nấp

- Email (file đính kèm, link).
- Nội dung web (JavaScript, drive-by download).
- Website hợp pháp bị xâm nhập.
- File tải về từ nguồn không tin cậy.

Kỹ thuật phát hiện và phòng chống

Detection

- **Signature-based**: So khớp chuỗi đặc trưng (virus fingerprint).
  Heuristic analysis: Phân tích hành vi khả nghi (mở file hệ thống, sửa boot sector).
- **Sandboxing**: Chạy file trong VM và quan sát hành vi.
- **White/Blacklist**: Danh sách cho phép/chặn.

Prevention

- Chỉ cài phần mềm từ nguồn tin cậy.
- Test trong môi trường cách ly.
- Backup định kỳ.
- Cập nhật bản vá, firewall, antivirus.

Quy trình xử lý sự cố malware

1. **Detection** – Phát hiện và xác định vị trí nhiễm.
2. **Identification** – Nhận diện chủng loại.
3. **Removal** – Loại bỏ mã độc.
4. **Recovery** – Khôi phục hệ thống.

Malware Analysis

- **Static analysis**: Phân tích mã, chuỗi, cấu trúc file PE/ELF mà không chạy.
- **Dynamic analysis**: Thực thi trong môi trường an toàn để quan sát network, file I/O, registry.
- **Kỹ thuật nâng cao**: Reverse engineering (IDA, Ghidra), unpacker, memory dump.

Kiến thức mở rộng & xu hướng

- **APT (Advanced Persistent Threat)**: Chiến dịch tấn công lâu dài, có mục tiêu rõ, thường dùng nhiều loại malware kết hợp.
- **Fileless malware**: Chạy trực tiếp trong bộ nhớ, khó phát hiện bằng signature.
- **Polymorphic/Metamorphic malware**: Tự biến đổi code để né detection.
- **Living off the land (LotL)**: Lợi dụng công cụ hợp pháp của OS (PowerShell, WMI) để hoạt động.
- **Supply chain attack**: Cấy mã độc vào phần mềm hợp pháp trong quá trình phát triển/phân phối.
- **IoT malware**: Nhắm tới thiết bị IoT bảo mật kém (ví dụ Mirai botnet).

Best Practices phòng chống malware

- **Defense in depth**: Nhiều lớp bảo vệ (network, endpoint, email filter).
- **MFA** để hạn chế khai thác tài khoản bị lộ.
- **Application whitelisting**: Chỉ cho phép app đã duyệt chạy.
- **User awareness training**: Huấn luyện nhận biết phishing & link độc.
- **EDR/XDR**: Giám sát hành vi endpoint và phản ứng sự cố tự động.
- **Network segmentation**: Hạn chế lây lan trong mạng nội bộ.

DDoS

DoS (Denial of Service)

- DoS là hành vi cố ý làm cho hệ thống mạng, hệ thống máy tính hoặc ứng dụng **không thể được sử dụng** bởi người dùng hợp lệ.
    - Cách tấn công thường gặp: làm cạn kiệt tài nguyên như **CPU**, **RAM**, **băng thông**, **dung lượng đĩa**.
- **Mục tiêu:**
  Không cần chiếm quyền, chỉ cần khiến dịch vụ bị gián đoạn hoặc ngừng hoạt động.

Các loại tài nguyên có thể bị tấn công

- **Băng thông mạng (Network bandwidth)** → Gửi lượng lớn dữ liệu khiến kênh truyền bị nghẽn, gói tin hợp lệ không tới nơi.
- **Tài nguyên hệ thống (System resources)** → CPU, RAM, số lượng file handle, số kết nối socket.
  Tài nguyên ứng dụng (Application resources) → Ép ứng dụng xử lý các tác vụ tốn kém, dẫn đến chậm hoặc treo.

Các dạng tấn công DoS

- **Classic DoS** → Một máy tấn công trực tiếp một máy.
- **Source Address Spoofing** → Giả mạo địa chỉ IP nguồn để che giấu danh tính và gây khó khăn cho việc truy vết.
- **SYN Spoofing** → Lợi dụng quá trình bắt tay 3 bước của TCP.
  Flooding Attacks → Gửi lượng lớn gói tin làm nghẽn hệ thống.
- **DDoS** → Nhiều máy cùng tấn công (phân tán).
- **Application-based bandwidth Attacks** → Tấn công tầng ứng dụng, ép xử lý nhiều hơn lượng tài nguyên yêu cầu từ attacker.
- **Reflector & Amplifier Attacks** → Dùng hệ thống trung gian để phản xạ hoặc khuếch đại lưu lượng.

Flooding Attacks

- Mục tiêu: làm quá tải đường truyền mạng.
- Các dạng phổ biến:
    - **ICMP Flood** → Gửi liên tục lệnh ping.
    - **UDP Flood** → Gửi nhiều gói UDP tới cổng ngẫu nhiên.
    - **TCP SYN Flood** → Lợi dụng handshake TCP.

SYN Flooding Attack

- **Cách hoạt động:**
    - Attacker gửi gói SYN mở kết nối TCP.
    - Server trả SYN-ACK.
    - Attacker không gửi ACK cuối hoặc IP nguồn giả.
- **Hậu quả:**
  Kết nối "half-open" bị giữ trong hàng đợi. Khi hàng đầy, kết nối hợp lệ bị từ chối.
- **Cách giảm thiểu:**
    - Lọc gói tin (filtering).
    - Tăng kích thước hàng đợi.
    - Giảm thời gian chờ (timeout) cho kết nối chưa hoàn tất.
    - Giới hạn số kết nối half-open từ 1 IP.
    - **SYN Cookies**.

SYN Cookies

- **Ý tưởng:** Không lưu trạng thái kết nối khi chưa nhận ACK.
- **Cách hoạt động:**
    - Server mã hóa thông tin (thời gian, MSS, hash bí mật) vào số thứ tự (sequence number) trong gói SYN-ACK.
    - Khi nhận ACK, server kiểm tra lại thông tin và mới tạo kết nối thực.
- **Ưu điểm:** Chống tốn bộ nhớ với kết nối giả.
- **Nhược điểm:** Sequence number tăng nhanh, MSS bị giới hạn, không gửi được dữ liệu trong SYN ban đầu.

DDoS (Distributed DoS)

- **Tại sao dùng DDoS?**
  Một máy tấn công có giới hạn, nhiều máy tấn công sẽ mạnh hơn.
- **Cách triển khai:**
    - Lây nhiễm malware vào nhiều máy (PC, server, IoT).
    - Các máy này trở thành **zombie**.
    - Attacker điều khiển đồng loạt để tấn công mục tiêu.

Application-based Bandwidth Attacks

- **Ý tưởng:** Bắt server làm việc nặng hơn attacker.
- **Ví dụ:**
    - **SIP Flood** → Tấn công hệ thống VoIP qua SIP request.

    - **HTTP Flood** → Gửi hàng loạt request HTTP GET/POST.
    - **Slowloris** → Giữ kết nối HTTP mở thật lâu bằng cách gửi header nhỏ giọt → làm cạn thread xử lý.

Reflector & Amplifier Attacks

- **Reflector Attack:** Attacker gửi gói tin tới server thứ 3, nhưng giả mạo IP nguồn là IP nạn nhân → server trả lời về nạn nhân.
- **Amplifier Attack:** Chọn dịch vụ có phản hồi lớn hơn request (DNS, NTP, ICMP), giúp khuếch đại lưu lượng.
- **Hiệu quả:** Lượng dữ liệu nạn nhân nhận được có thể gấp hàng chục lần lượng attacker gửi.

Phòng chống & Giảm thiểu

4 hướng chính:

1. **Ngăn ngừa & phòng tránh (trước tấn công)**
    - Cập nhật vá lỗi, tránh bị chiếm quyền.
    - Lọc gói tin giả IP.
    - Tắt IP-directed broadcast.
    - Dự phòng hệ thống ở nhiều nơi (mirroring, CDN).
2. **Phát hiện & lọc (trong lúc tấn công)**
    - Dùng SYN Cookies.
    - Xóa kết nối chưa hoàn tất khi bảng kết nối đầy.
    - Xác thực người dùng bằng CAPTCHA.
3. **Truy vết nguồn tấn công (trong & sau tấn công)**
    - Kết hợp với ISP để tìm nguồn.
4. **Phản ứng & khôi phục (sau tấn công)**
    - Khôi phục dịch vụ, vá lỗ hổng, xử lý pháp lý.