Malicious Code | Malicious Code Examples & Definition | Snyk

6-8 minutes

Everyone hears about the vulnerabilities of websites generated by malicious viruses and code, but just exactly what is malicious code, and how does it impact application users and developers? Let’s start from getting the definition of malicious code right.

What is malicious code?

Malicious code is defined as a piece of code or malware that can exploit common system vulnerabilities. Attacks may be launched through various means including viruses, worms, script attacks, backdoors, active content, and Trojan horses. Malware can be picked up from email attachments, untrustworthy websites and suspicious links, as well as other sources.

Malicious code attackers or malware code perpetrators have a few basic intentions in spreading their venomous code throughout business applications, including:

- Steal confidential data for financial gain such as selling credit card information
- Create mischief that causes alerts and minimal damage to servers as a technical challenge
- Take revenge against a business, as by a disgruntled current or former employee
- Implement a terroristic attack such as holding the digital assets of a government agency or business for ransom

Malicious code can penetrate website defenses in many forms, such as:

- ActiveX controls
- Scripting languages that embed scripts or commands through injection techniques
- Java Applets

- Browser plug-ins
- Pushed content that can reach a single user, or a large volume of users

  Malicious code is not unique to servers, networked computers, or laptops. Attackers are just as comfortable exploiting tablets, smartphones, and mobile devices.

  Enterprise systems that often utilize reusable components may be especially vulnerable to malicious code since a single flaw or coding error that opens the door to attackers can provide a weakness that extends to multiple applications, causing a severe security issue.

Safeguard Against Malicious Code

Automatically find, prioritize and fix vulnerabilities in the open source dependencies used to build your cloud native applications

What are malicious code examples?

Malicious code examples include backdoor attacks, scripting attacks, worms, trojan horse and spyware. Each type of malicious code attack can wreak havoc on a defenseless IT infrastructure very quickly or wait on servers for a predetermined amount of time or a trigger to activate the attack. Industry studies have revealed that detection of malicious code often takes weeks or months before the damage is noticed and threats are defeated.

Backdoor Attacks

With a backdoor attack, the offending code can take over an application to extract trade secrets from business databases, steal employee information for identity theft, erase critical files, and spread from one server to another. Seeds can be planted that go unnoticed for days or even months, gathering information and sending it back to the attacker without detection.

Scripting Attacks

Script injection can modify application functionality to reroute applications to another server, use different databases, retrieve additional unauthorized data, and modify web pages.

Trojan Horse and Spyware

Malicious code may go undetected on infected computers, simply monitoring applications and websites accessed. Once critical information is stolen, such as bank accounts or passwords, the information is forwarded to the perpetrator.

Worms

Worm attacks are designed to self-replicate across multiple computers or enterprise networks, often stealing or even destroying files and critical data.

Examples of Malicious Code Attacks

Hackers are continuously working to compromise technical defenses against malicious code. Some of the better-known examples of malicious attacks include:

- **Trojan Horse** – Emotet – appears as applications a user would benefit from
- **Worms** – Stuxnet – replicated through network computers

- **Bots** – Echobot – launched a flood of attacks
- **Ransomware** – RYUK – disables access to company assets until the ransom is paid

How Do You Know You Have Malicious Code?

For computer users, there are several hints that malicious code is lurking on the system:

- Performance issues for no known reason (no new software loaded)
- Frequent system crashes
- Changes to browser home page or account passwords
- Unfamiliar programs running in the taskbar or at system startup

Detecting malicious software on web applications or enterprise networks is significantly more complicated. Analyzing network assets and website sources for malware or different types of malicious code involves continuous monitoring, auditing of system logs, and the use of sophisticated security tools.

How Do You Safeguard Against Malicious Code?

Enterprise management and security teams have their work cut out for them in protecting against web application vulnerabilities and malware code.

Providing continuous protection includes a comprehensive approach to application, network and data security that includes:

- Stress to employees the importance of never opening unexpected emails from external sources. It’s especially important to avoid opening attachments or clicking links from such sources.
- Install and update antivirus software on all computers as a first defense
- Block pop-ups to prevent some incidents of intentional or accidental clicking on potentially harmful links
- Use minimal permissions on web applications to limit the authority and prevent hackers from having the potential to spread malicious code to critical systems

- Keep software updated to ensure any applicable security patches or improvements are included
- Scan websites and code for malicious code regularly
- Implement secure firewalls for all network traffic
- Utilize software tools to monitor suspicious activity, especially any use of unauthorized web sites, access to bank accounts, or emails to or from unrecognized email accounts
- Utilize secure VPN software for mobile employees who may utilize business systems from home, customer or job sites, or on public networks

Overall, ensure that there are authorized and accountable resources that monitor system logs for suspicious activity to be proactive in detecting potential security issues or the presence of malicious software.