**MALICIOUS CODE**

**What Is Malicious Code?**

Malicious code is the term used to describe any code in any part of a software system or script that is intended to cause undesired effects, security breaches or damage to a system. Malicious code is an application security threat that cannot be efficiently controlled by conventional antivirus software alone. Malicious code describes a broad category of system security terms that includes attack scripts, viruses, worms, Trojan horses, backdoors and malicious active content.

Malicious code can take the form of:

* Java Applets
* ActiveX Controls
* Scripting languages
* Browser plug-ins
* Pushed content

Once inside your environment, malicious code can enter network drives and propagate. Malicious code can also cause network and mail server overload by sending email messages; stealing data and passwords; deleting document files, email files or passwords; and even reformatting hard drives.

### Malicious Code Threatens Enterprise Security

Malicious code can give a user remote access to a computer. This is known as an application backdoor. Backdoors may be created with malicious intent, to gain access to confidential company or customer information. But they can also be created by a programmer who wants quick access to an application for troubleshooting purposes. They can even be created inadvertently through programming errors. Regardless of their origin, all backdoors and malicious code can become a security threat if they are found and exploited by hackers or unauthorized users. As applications today tend to be built more and more often with reusable components from a variety of sources with varying levels of security, malicious code can pose a significant operational risk to the enterprise. That's why so many enterprises today are turning to Veracode to secure their applications.

### How to Avoid Malicious Code

One way to avoid malicious code in your applications is to add static analysis (also called [“white-box” testing](https://www.veracode.com/products/binary-static-analysis-sast)) to your software development lifecycle to review your code for the presence of malicious code. Veracode’s [static code analysis](https://www.veracode.com/products/static-analysis-sast/static-code-analysis) looks at applications in non-runtime environment. This method of security testing has distinct advantages in that it can evaluate both web and non-web applications and, through advanced modeling, can detect malicious code in the software’s inputs and outputs that cannot be seen through other testing methodologies.

# SPOOFING ATTACK: IP, DNS & ARP

### What Is a Spoofing Attack?

A spoofing attack is when a malicious party impersonates another device or user on a network in order to launch attacks against network hosts, steal data, spread [malware](https://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101/) or bypass access controls. There are several different types of spoofing attacks that malicious parties can use to accomplish this. Some of the most common methods include IP address spoofing attacks, [ARP spoofing](https://www.veracode.com/security/arp-spoofing) attacks and DNS server spoofing attacks.

### IP Address Spoofing Attacks

IP address spoofing is one of the most frequently used spoofing attack methods. In an IP address spoofing attack, an attacker sends IP packets from a false (or “spoofed”) source address in order to disguise itself. Denial-of-service attacks often use IP spoofing to overload networks and devices with packets that appear to be from legitimate source IP addresses.

There are two ways that IP spoofing attacks can be used to overload targets with traffic. One method is to simply flood a selected target with packets from multiple spoofed addresses. This method works by directly sending a victim more data than it can handle. The other method is to spoof the target’s IP address and send packets from that address to many different recipients on the network. When another machine receives a packet, it will automatically transmit a packet to the sender in response. Since the spoofed packets appear to be sent from the target’s IP address, all responses to the spoofed packets will be sent to (and flood) the target’s IP address.

IP spoofing attacks can also be used to bypass IP address-based authentication. This process can be very difficult and is primarily used when trust relationships are in place between machines on a network and internal systems. Trust relationships use IP addresses (rather than user logins) to verify machines’ identities when attempting to access systems. This enables malicious parties to use spoofing attacks to impersonate machines with access permissions and bypass trust-based network security measures.

### ARP Spoofing Attacks

ARP is short for Address Resolution Protocol, a protocol that is used to resolve IP addresses to MAC (Media Access Control) addresses for transmitting data. In an ARP spoofing attack, a malicious party sends spoofed ARP messages across a local area network in order to link the attacker’s MAC address with the IP address of a legitimate member of the network. This type of spoofing attack results in data that is intended for the host’s IP address getting sent to the attacker instead. Malicious parties commonly use [ARP spoofing](https://www.veracode.com/security/arp-spoofing) to steal information, modify data-in-transit or stop traffic on a LAN. [ARP spoofing](https://www.veracode.com/security/arp-spoofing)attacks can also be used to facilitate other types of attacks, including denial-of-service, session hijacking and [man-in-the-middle](https://www.veracode.com/security/man-middle-attack) attacks. ARP spoofing only works on local area networks that use the Address Resolution Protocol.

### DNS Server Spoofing Attacks

The Domain Name System (DNS) is a system that associates domain names with IP addresses. Devices that connect to the internet or other private networks rely on the DNS for resolving URLs, email addresses and other human-readable domain names into their corresponding IP addresses. In a DNS server spoofing attack, a malicious party modifies the DNS server in order to reroute a specific domain name to a different IP address. In many cases, the new IP address will be for a server that is actually controlled by the attacker and contains files infected with malware. DNS server spoofing attacks are often used to spread [computer worms](https://www.veracode.com/security/computer-worm) and viruses.

Spoofing Attack Prevention and Mitigation

There are many tools and practices that organizations can employ to reduce the threat of spoofing attacks. Common measures that organizations can take for spoofing attack prevention include:

* **Packet filtering:** Packet filters inspect packets as they are transmitted across a network. Packet filters are useful in IP address spoofing attack prevention because they are capable of filtering out and blocking packets with conflicting source address information (packets from outside the network that show source addresses from inside the network and vice-versa).
* **Avoid trust relationships:** Organizations should develop protocols that rely on trust relationships as little as possible. It is significantly easier for attackers to run spoofing attacks when trust relationships are in place because trust relationships only use IP addresses for authentication.
* **Use spoofing detection software:** There are many programs available that help organizations detect spoofing attacks, particularly [ARP Spoofing](https://www.veracode.com/security/arp-spoofing). These programs work by inspecting and certifying data before it is transmitted and blocking data that appears to be spoofed.
* **Use cryptographic network protocols:** [Transport Layer Security](https://www.veracode.com/security/insufficient-transport-layer-protection) (TLS), Secure Shell (SSH), HTTP Secure (HTTPS) and other secure communications protocols bolster spoofing attack prevention efforts by encrypting data before it is sent and authenticating data as it is received.