What Is the Difference: Viruses, Worms, Trojans, and Bots?

Contents

Introduction

Viruses, worms, Trojans, and bots are all part of a class of software called malware. Malware or malicious code (malcode) is short for malicious software. It is code or software that is specifically designed to damage, disrupt, steal, or in general inflict some other “bad” or illegitimate action on data, hosts, or networks.

There are many different classes of malware that have varying ways of infecting systems and propagating themselves. Malware can infect systems by being bundled with other programs or attached as macros to files. Others are installed by exploiting a known vulnerability in an operating system (OS), network device, or other software, such as a hole in a browser that only requires users to visit a website to infect their computers. The vast majority, however, are installed by some action from a user, such as clicking an e-mail attachment or downloading a file from the Internet.

Some of the more commonly known types of malware are viruses, worms, Trojans, bots, back doors, spyware, and adware. Damage from malware varies from causing minor irritation (such as browser popup ads), to stealing confidential information or money, destroying data, and compromising and/or entirely disabling systems and networks.

Malware cannot damage the physical hardware of systems and network equipment, but it can damage the data and software residing on the equipment. Malware should also not be confused with defective software, which is intended for legitimate purposes but has errors or bugs.

Classes of Malicious Software

Two of the most common types of malware are viruses and worms. These types of programs are able to self-replicate and can spread copies of themselves, which might even be modified copies. To be classified as a virus or worm, malware must have the ability to propagate. The difference is that a worm operates more or less independently of other files, whereas a virus depends on a host program to spread itself. These and other classes of malicious software are described below.

Viruses

A computer virus is a type of malware that propagates by inserting a copy of itself into and becoming part of another program. It spreads from one computer to another, leaving infections as it travels. Viruses can range in severity from causing mildly annoying effects to damaging data or software and causing denial-of-service (DoS) conditions. Almost all viruses are attached to an executable file, which means the virus may exist on a system but will not be active or able to spread until a user runs or opens the malicious host file or program. When the host code is executed, the viral code is executed as well. Normally, the host program keeps functioning after it is infected by the virus. However, some viruses overwrite other programs with copies of themselves, which destroys the host program altogether. Viruses spread when the software or document they are attached to is transferred from one computer to another using the network, a disk, file sharing, or infected e-mail attachments.

Worms

Computer worms are similar to viruses in that they replicate functional copies of themselves and can cause the same type of damage. In contrast to viruses, which require the spreading of an infected host file, worms are standalone software and do not require a host program or human help to propagate. To spread, worms either exploit a vulnerability on the target system or use some kind of social engineering to trick users into executing them. A worm enters a computer through a vulnerability in the system and takes advantage of file-transport or information-transport features on the system, allowing it to travel unaided.

Trojans

A Trojan is another type of malware named after the wooden horse the Greeks used to infiltrate Troy. It is a harmful piece of software that looks legitimate. Users are typically tricked into loading and executing it on their systems. After it is activated, it can achieve any number of attacks on the host, from irritating the user (popping up windows or changing desktops) to damaging the host (deleting files, stealing data, or activating and spreading other malware, such as viruses). Trojans are also known to create back doors to give malicious users access to the system.

Unlike viruses and worms, Trojans do not reproduce by infecting other files nor do they self-replicate. Trojans must spread through user interaction such as opening an e-mail attachment or downloading and running a file from the Internet.

Bots

"Bot" is derived from the word "robot" and is an automated process that interacts with other network services. Bots often automate tasks and provide information or services that would otherwise be conducted by a human being. A typical use of bots is to gather information (such as web crawlers), or interact automatically with instant messaging (IM), Internet Relay Chat (IRC), or other web interfaces. They may also be used to interact dynamically with websites.

Bots can be used for either good or malicious intent. A malicious bot is self-propagating malware designed to infect a host and connect back to a central server or servers that act as a command and control (C&C) center for an entire network of compromised devices, or "botnet." With a botnet, attackers can launch broad-based, "remote-control," flood-type attacks against their target(s). In addition to the worm-like ability to self-propagate, bots can include the ability to log keystrokes, gather passwords, capture and analyze packets, gather financial information, launch DoS attacks, relay spam, and open back doors on the infected host. Bots have all the advantages of worms, but are generally much more versatile in their infection vector, and are often modified within hours of publication of a new exploit. They have been known to exploit back doors opened by worms and viruses, which allows them to access networks that have good perimeter control. Bots rarely announce their presence with high scan rates, which damage network infrastructure; instead they infect networks in a way that escapes immediate notice.

Best Practices for Combating Viruses, Worms, Trojans, and Bots

The first steps to protecting your computer are to ensure that your OS is up to date. This means regularly applying the most recent patches and fixes recommended by the OS vendor. Secondly, you should have antivirus software installed on your system and download updates frequently to ensure that your software has the latest fixes for new viruses, worms, Trojans, and bots. Additionally, you want to make sure that your antivirus program can scan e-mail and files as they are downloaded from the Internet. This will help prevent malicious programs from reaching your computer. You may also want to consider installing a firewall.

Additional Definitions and References

Exploit

An exploit is a piece of software, a command, or a methodology that attacks a particular security vulnerability. Exploits are not always malicious in intent—they are sometimes used only as a way of demonstrating that a vulnerability exists. However, they are a common component of malware.

Back Door

A back door is an undocumented way of accessing a system, bypassing the normal authentication mechanisms. Some back doors are placed in the software by the original programmer and others are placed on systems through a system compromise, such as a virus or worm. Usually, attackers use back doors for easier and continued access to a system after it has been compromised.

Technical Definition Sites

http://en.wikipedia.org/wiki/

http://www.sans.org/resources/glossary.php

This document is part of the Cisco Security Intelligence Operations.

This document is provided on an "as is" basis and does not imply any kind of guarantee or warranty, including the warranties of merchantability or fitness for a particular use. Your use of the information on the document or materials linked from the document is at your own risk. Cisco reserves the right to change or update this document at any time.

Back to Top

Cisco Security Intelligence Operations

Information For
Small Business
Midsize Business
Service Provider
Executives
Home (Linksys)

Industries

Contacts
Contact Cisco
Find a Partner

News & Alerts
Newsroom
Blogs
Field Notices
Security Advisories

Technology Trends
Cloud
IPv6
Mobility
Open Network Environment
Trustworthy Systems

Support
Downloads
Documentation

Communities
Developer Network
Learning Network
Support Community

Video Portal

About Cisco
Investor Relations
Corporate Social Responsibility
Environmental Sustainability
Tomorrow Starts Here
Career Opportunities

Programs
Cisco Designated VIP Program
Cisco Powered
Financing Options

Contacts | [+] Feedback | Help | Site Map | Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks