

SECURITY TERMS:

Advisory - A formal notice to the public on the nature of security vulnerability. When security researchers discover vulnerabilities in software, they usually notify the affected vendor well in advance of the public. When the vendor has had a chance to create a fix, they usually collaborate with the researchers to publish an advisory.

Backdoor - A secret program installed by a hacker, worm or virus in order to grant unauthorized access to the infected computer at any point in the future. Backdoors usually allow attackers to connect back to the compromised system over the network, using a secret network protocol.

Blended Threat - A marketing term for attacks that use a variety of techniques to achieve the attacker's objective. By the conventional definition, all worms are blended threats. They use exploits, scanning techniques, and backdoors to take over massive numbers of hosts.

Blind Worm - For certain vulnerabilities, such as the UDP Microsoft SQL hole, an extremely skilled worm author can create a worm that requires the delivery of only a single packet to completely infect a target. These blind worms do not need to establish communications with their targets, but rather spray infected packets blindly across a network.

Bootstrapped Worm - These worms propagate by illicitly installing small file transfer programs, such as TFTP servers, to copy a relatively large and ungainly worm program to newly-infected machine. A bootstrapped worm, as such as Sasser, can be designed more simply and quickly, but often lacks in speed and efficiency.

Bot - A hybrid of backdoors and worms, bots are malware programs that are designed to turn a victim computer into platforms for network attacks, typically installed by a human attacker. Bots can be much larger and slower than worm programs, as they typically include advanced hacker tools such as network sniffers, keystroke loggers, and chat programs.

Coordinated Scanning - A variety of random-number-generated techniques where multiple worm instances avoid scanning the same addresses, without requiring the infected computers to communicate.

Denial of Service (DOS) - An attack involving floods of traffic that overwhelm the network or computing resources of target, cutting off services and rendering the network unavailable to a user or organization.

Distributed Denial of Service - DDoS attacks are coordinated assaults by hundreds, or thousands of compromised systems, thereby forcing the targeted system to shut down, denying service to legitimate users. DDoS attacks can be very effective and are difficult to defend against.

Enabling Factors - A blanket term for a variety of factors (other than susceptibility) that influences whether a vulnerability will be used to create a new network worm. Enabling factors include how well-known the vulnerability is, whether exploits programs for the vulnerability have been published, and how hard it is to program the target computer system.

Exploit - Computer programs written to automate the exploitation of vulnerabilities. A well-written exploit for severe vulnerability, such as a Windows security hole, can provide an attacker with push-button remote access to every vulnerable machine exposed on the network.

Flash Worm - A theoretical design for a worm that can infect a majority of vulnerable machines within seconds, before any human intervention could reasonably mitigate the attack. The basic technique used by a flash worm is to pre-scan the Internet to generate a hit-list of the most potentially vulnerable servers.

High-Speed Worm - Modern worms, such as SQL Slammer and MS Blaster, are capable of propagating themselves with surprising speed and effectiveness, using one or more of a variety of techniques, including local address scanning, self-containment, and hit-lists.

Hit-List - Instead of starting with a single patient zero, a hit-list-enabled worm might start with thousands; reducing the time it takes for the worm to achieve rapid infection from hours, to minutes or seconds. Generating a large list for vulnerable computers in advance becomes a much more effective means for worm authors to kick-start a worm outbreak.

Mail Worm - More of a virus and not an actual worm, mail worms are programs which infect computers by copying themselves within email messages to other computers. Mail worms are often successful by tricking email readers into clicking on them (and running embedded infection programs), or by exploiting bugs in mail-reading software.

Malware - Malicious software. A blanket term used to describe any program or file that is harmful to a system, e.g. worms, viruses, bots, backdoors, etc.

Multi-Vector Worm - A worm that uses multiple mechanisms to compromise and infect computers. Multi-vector worms, like the 2001 Nimda worm, are harder to stop because they have more susceptibility and require multiple steps to guard against.

Network Hardening - The process in which network operators can discover the legitimate relationships between users, machines, and applications and segment the network, locking it down before new vulnerabilities are announced and reducing exposure to outages and availability problems.

Patient Zero - During a global worm outbreak, patient zero is the first computer ever to be infected “in the wild” by a new worm. The global patient zero for a worm can provide clues as to the origin of the worm. In any specific enterprise worm outbreak, patient zero is the first host on the network to carry the infection into the network.

Payload - The code in a worm or virus designed to inflict harm or further the aim of the attacker. Virus payloads are often designed to disable infected computers and destroy information. In contrast worm payloads tend to be more subtle. Well-known worm payload techniques include: slowly removing all the data on a hard drive and installing backdoor programs.

Polymorphic Malware - Uses an unlimited number of encryption routines to prevent detection. Polymorphic viruses actively mutate themselves as they spread, changing their code structure in ways that don't substantially affect the way they function.

Propagation - One of the three basic elements of a worm, propagation is the means by which a worm finds susceptible hosts to infect and spread throughout a network.

Scanning - The simplest method of finding hosts susceptible to infections is to attempt to probe every computer on the network. A typical worm program scans the network randomly, which spreads the worm across the network faster and mitigates the effect of multiple infected computers wasting time scanning the same host.

Scavenger Worm - A worm that takes advantage of damage done by previous attacks. As an example, the 2004 Dabber worm functioned by exploiting a vulnerability in

backdoor installed by Sasser worm. Because worm outbreaks worldwide, scavenger attacks are an emerging threat to Internet.

Seed Infection - Mail-borne seed infections can vault a multi-vector worm past perimeter security, enabling it to attack services that are not usually exposed on the Internet, like printers and IP telephones. Because even a small fraction of the vast email-using population amounts to a large number of hosts, mail worms provide a powerful means for beginning a worm infection.

Self-Contained Worm - Self-contained worms build the entire functionality of the worm into the initial exploit, allowing it to completely infect a host with a single transaction. Self-contained worms, are faster than bootstrapped worms, but are harder for the worm authors to write.

Stealth Scanning - A scan that is designed to go undetected by auditing tools. Scanning very slowly (taking a day or more) becomes a stealth technique.

Stealth Worm - Involves slow-scanning techniques, hit-lists, and traffic analysis countermeasures which mask probe traffic with legitimate-looking fake traffic. A stealth worm is created to be as quiet as possible, so that several hosts are infected before defenders even become aware of the worm.

Susceptibility - A measure of the number of hosts vulnerable to an attack. A hole that affects any computer running Microsoft Windows has a very large susceptible population. A hole that only affects Cray XMP Supercomputers has a very small susceptible population. The larger the susceptible population, the more damage a worm can do to it.

Targeted Worm - An attack aimed at specific networks or computers. Once a worm has injected itself into a victim, it can check the identity of its new host and act accordingly, locating susceptible hosts and leveraging them to further infection.

Topology-Aware Worm - Only scans hosts which are likely to be susceptible. A worm could discover likely candidates for infection in a variety of ways, including: sniffing the network for active hosts; examining browser caches for server addresses; or bombing entire hard drives for IP addresses.

Variant Worm - When an attacker takes an existing worm and modifies it slightly. A variant worm infects computers in the same manner as the original, but will appear different and may have a different payload.

Vector - The means by which a worm infects a single target host. The vector of a modern worm is almost always an exploit program for a recently published security vulnerability; through older worms have used network file shares or even password guessing to spread themselves.

Virulence - Not all security holes provide suitable vehicles for new worms,. Virulence is a metric that expresses the likelihood of a vulnerability being used by a worm. Virulent vulnerabilities, of which tens or hundreds are announced every year, are likely to become new worm attacks.

Virus - A computer program that infects other computers by creating copies of itself in files, programs, disk boot sectors, and email messages. Viruses are passive agents: to become infected, a system must come in contact with an infected program.

Vulnerability (security hole) - A software bug that allows an attacker to trick a computer into doing something unauthorized. Vulnerabilities in operating systems and network systems and network services often allow attackers to take control of computer systems from across the Internet.

Warhol Worm - A theoretical worm design that is likely to infect a majority of all vulnerable hosts in under 15 minutes. A Warhol worm that targets a Microsoft Windows vulnerability would infect thousands of computers in seconds, worldwide. Warhol worms use two acceleration techniques: hit-lists and coordinated scanning.

Whack-a-Mole - The phenomenon in which a worm defenses are outpaced by the worm infection rate, so that any infected computer is likely to spread the worm to at least one other host before the host is disabled or disinfected. The whack-a-mole phenomenon is common to virtually all worm defense mechanisms that operate by finding and disabling infected hosts or switch ports.

Worm - Unlike viruses, which can only be spread by unwitting users, a worm infects other computers by actively attacking them, propagating through the network by duplicating itself repeatedly. Worms can invade vulnerable machines anywhere on the Internet, at any time, with no end-user intervention, often within minutes, or seconds, of the first appearing on the network.

Zero-Day - The day the public becomes aware of a vulnerability is the zero-day. Vulnerabilities are disclosed either intentionally, as when a vendor or research team publishes an advisory, or unintentionally, as when hackers with insider knowledge use previously unknown vulnerabilities to launch visible attacks. Zero-day exploits refer to attacks that use previously-unknown vulnerabilities.

Zombie - The most devastating denial of service attacks are distributed across thousands, or even millions of attacking computers. To accomplish this, attackers create zombie armies of compromised computers, which communicate with their masters via chat networks. Worms and viruses are notorious for generating zombies that are used to attack high-profile targets, like Microsoft and SCO Systems.