The CERT Coordination Center has been observing intruder activity since 1988. Much has changed since then, including our technology, the Internet user community, attack techniques, and the volume of incidents (depicted in Figure 1, next page). In this article, we give a brief overview of recent trends that affect the ability of organizations (and individuals) to use the Internet safely.

**Automation and Speed of Attack Tools**

The level of automation in attack tools continues to increase. Automated attacks commonly involve four phases, each of which is changing. These phases include scanning for potential victims, compromising vulnerable systems, propagating the attack, and coordinated management of attack tools.

Widespread scanning has been common since 1997. Today, scanning tools are using more advanced scanning patterns to maximize impact and speed. Previously, vulnerabilities were exploited after a widespread scan was complete. Now, attack tools exploit vulnerabilities as a part of the scanning activity, which increases the speed of propagation.

Before 2000, attack tools required a person to initiate additional attack cycles. Today, attack tools can initiate new attack cycles themselves. We have seen tools like Code Red and Nimda propagate themselves to a point of global saturation in fewer than 18 hours.

Since 1999, with the advent of distributed attack tools, attackers have been able to manage and coordinate large numbers of deployed attack tools distributed across many Internet systems. Today, distributed attack tools are capable of launching denial of service attacks more efficiently, scanning for potential victims and compromising vulnerable systems. Coordination functions now take advantage of readily available, public communications protocols such as Internet Relay Chat (IRC) and instant messaging (IM).

**Increasing Sophistication of Attack Tools**

Attack tool developers are using more advanced techniques. Attack tool signatures are more difficult to discover through analysis and more difficult to detect through signature-based systems such as antivirus software and intrusion detection systems. Three important characteristics are the anti-forensic nature, dynamic behavior, and modularity of the tools.

- **Anti-forensics.** Attackers use techniques that obfuscate the nature of attack tools. This makes it more difficult and time consuming for security experts to analyze new attack tools and to understand new and rapidly developing threats. Analysis often includes laboratory testing and reverse engineering.
- **Dynamic behavior.** Early attack tools performed attack steps in single defined sequences. Today’s automated attack tools can vary their patterns and behaviors based on random selection, predefined decision paths, or through direct intruder management.
- **Modularity of attack tools.** Unlike early attack tools that implemented one type of attack, tools now can be changed quickly by upgrading or replacing portions of the tool. This causes rapidly evolving attacks and, at the extreme, polymorphic tools that self-evolve to be different in each instance. In addition, attack tools are more commonly being developed to execute on multiple operating system platforms.

As an example of the difficulties posed by sophisticated attack tools, many common tools use protocols like IRC or HTTP to send data or commands from the intruder to compromised hosts. As a result, it has become increasingly difficult to distinguish attack signatures from normal, legitimate network traffic.

**Faster Discovery of Vulnerabilities**

The number of newly discovered vulnerabilities reported to CERT continues to more than double each year, as indicated...
in Figure 2. It is difficult for administrators to keep up to date with patches. Additionally, new classes of vulnerabilities are discovered each year. Subsequent reviews of existing code for examples of the new vulnerability class often lead, over time, to the discovery of examples in hundreds of different software products. Intruders are often able to discover these exemplars before the vendors are able to correct them.

Because of the trend toward the automated discovery of new vulnerabilities in technologies, the so-called time to patch is becoming increasingly small.

**INCREASING PERMEABILITY OF FIREWALLS**

Firewalls are often relied upon to provide primary protection from intruders. However, technologies are being designed to bypass typical firewall configurations, such as IPP (the Internet Printing Protocol) and WebDAV (Web-based Distributed Authoring and Versioning). Some protocols marketed as being “firewall friendly” are, in reality, designed to bypass typical firewall configurations. Certain aspects of mobile code (including ActiveX controls, Java, and JavaScript) make it difficult for vulnerable systems to be protected and malicious software to be discovered.

**INCREASINGLY SYMMETRIC THREAT**

Security on the Internet is, by its very nature, highly interdependent. Each Internet system’s exposure to attack depends on the state of security of the rest of the systems attached to the global Internet. Because of the advances in attack technology, a single attacker can relatively easily employ a large number of distributed systems to launch devastating attacks against a single victim. As the automation of deployment and the sophistication of attack tool management both increase, the asymmetric nature of the threat will continue to grow.

**INCREASING THREAT FROM INFRASTRUCTURE ATTACKS**

Infrastructure attacks are attacks that broadly affect key components of the Internet. They are of increasing concern because of the number of organizations and users on the Internet and their increasing dependency on the Internet to carry out day-to-day business. The main four types of attacks include denial-of-service, worms, DNS, and router attacks.

**DENIAL OF SERVICE**

Denial-of-service attacks use multiple systems to attack one or more victim systems with the intent of denying service to legitimate users of the victim systems. The degree of automation in attack tools enables a single attacker to install their tools and control tens of thousands of compromised systems for use in attacks.

Intruders often search address blocks known to contain high concentrations of vulnerable systems. Cable modem, DSL, and university address blocks are increasingly targeted by intruders planning to install their attack tools. Denial-of-service attacks are effective because the Internet consists of limited and consumable resources, and Internet security is highly interdependent.

**WORMS**

A worm is self-propagating malicious code. Unlike a virus, which requires a user to do something to continue the propagation, a worm can propagate by itself. The highly automated nature of the worms coupled with the relatively widespread nature of the vulnerabilities they exploit, allows a large number of systems to be compromised within a matter of hours. The Code Red worm infected more than 250,000 systems in just 9 hours on 19 July 2001.

Some worms, such as Code Red, include built-in denial-of-service attack payloads. Others, such as sadmind/IIS, contain Web site defacement payloads. Still others, such as W32/Leaves, have dynamic configuration capabilities. But the biggest impact of these worms is that their propagation effectively creates a denial of service in many parts of the Internet because of the huge amounts of scan traffic generated. Examples include DSL routers that crash and ISPs whose networks are completely overloaded, not by the scanning itself but by the burst of underlying network management traffic that the scanning triggers.

**DNS ATTACKS**

The Domain Name System is the distributed, hierarchical global directory that translates names to numeric IP addresses. The top two layers of the hierarchy are critical to the operation of the Internet. In the top layer are 13 root name servers. Next are the top-level domain (TLD) servers, which are authoritative for .com and .net, as well as for the country code top level domains (ccTLDs) such as .us, .uk, and so forth.
Threats to DNS include cache poisoning, compromised data, denial of service, and domain hijacking.

- **Cache poisoning.** If DNS is made to cache bogus information, the attacker can redirect traffic intended for a legitimate site to a site under the attacker’s control. A recent survey by the CERT Coordination Center shows that over 80 percent of the TLDs are running on servers that are potentially vulnerable to this form of attack.

- **Compromised data.** Attackers compromise vulnerable DNS servers, giving them the ability to modify the data served to users. Many of the TLD servers run a software program called BIND, in which vulnerabilities are discovered regularly. A CERT Coordination Center survey indicates that at least 20 percent of TLDs are running on vulnerable servers.

- **Denial of service.** A large denial-of-service attack on some of the name servers for a TLD (for example, .com) could cause widespread Internet slowdowns or effective outages.

- **Domain hijacking.** By leveraging insecure mechanisms used by customers to update their domain registration information, attackers can take over the domain registration processes to hijack legitimate domains.

**ROUTER ATTACKS**

Routers are specialized computers that direct traffic on the Internet in a manner similar to mail routing facilities in the postal service. Router threats fall into the following categories:

- **Routers as attack platforms.** Intruders use poorly secured routers as platforms for generating attack traffic at other sites or for scanning or reconnaissance.

- **Denial of service.** Although routers are designed to pass large amounts of traffic through them, they often are not capable of handling the same amount of traffic directed at them. (Think of it as the difference between sorting mail and reading it.) Intruders take advantage of this characteristic, attacking the routers that lead into a network rather than attacking the systems on the network directly.

- **Exploitation of trust relationship between routers.** For routers to do their job, they have to know where to send the traffic they receive. They do this by sharing routing information between them, which requires the routers to trust the information they receive from their peers. As a result, it would be relatively easy for an attacker to modify, delete, or inject routes into the global Internet routing tables to redirect traffic destined for one network to another, effectively causing a denial of service to both (one because no traffic is being routed to them, and the other because they’re getting more traffic than they should). Although the technology has been widely available for some time, many networks (Internet service providers and large corporations) do not protect themselves with available strong encryption and authentication features.

Because of the asymmetric nature of the threat, denial of service is likely to remain a high-impact, low-effort modus operandi for attackers. Most organizations’ Internet connections have 1 to 155 Mbps of bandwidth available. Attacks have been reported in the hundreds of Mbps and up, which is more than enough to saturate nearly any system on the Internet.

Additionally some viruses attach themselves to existing files on the systems they infect and then send the infected files to others. This can result in confidential information being distributed without the author’s permission (Sircam is an example). Also, intruders might be able to modify news sites, produce bogus press releases, and conduct other activities, all of which could have economic impact.

Perhaps the largest impact of security events is the time and resource requirements to deal with them. Computer Economics estimates that the total economic impact of Code Red was $2.6 billion, while Sircam cost another $1.3 billion. For comparison, most experts estimate that the 9/11 attacks will cost around $15.8 billion to restore IT and communication capabilities.

The trends seen by the CERT Coordination Center indicate that organizations relying on the Internet face significant challenges to ensure that their networks operate safely and that their systems continue to provide critical services even in the face of attack. Much work remains for all of us as we analyze the risks and determine what we can do to mitigate them.

**ACKNOWLEDGMENTS**

The authors thank Sven Dietrich, Jeffrey Havrilla, Shawn Hernan, Marty Lindner, Jeff Carpenter, and Linda Pesante for their ideas and assistance. They also thank Nancy Mead for coordinating the submission and production of this article.