Overview of Attack Trends

CERT® Coordination Center

The CERT Coordination Center has been observing intruder activity since 1988. Much has changed since then, from our technology to the makeup of the Internet user community, to attack techniques. In this paper, we give a brief overview of recent trends that affect the ability of organizations (and individuals) to use the Internet safely.

Trend 1 – Automation; 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.

A. *Scanning for potential victims*. Widespread scanning has been common since 1997. Today, scanning tools are using more advanced scanning patterns to maximize impact and speed.

B. *Compromising vulnerable systems*. 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.

C. *Propagate the attack*. Before 2000, attack tools required a person to initiate additional attack cycles. Today, attack tools can self-initiate new attack cycles. We have seen tools like Code Red and Nimda self-propagate to a point of global saturation in less than 18 hours.

D. *Coordinated management of attack tools*. 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).

Trend 2 – Increasing sophistication of attack tools

Attack tool developers are using more advanced techniques than previously. 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 anitforensic nature, dynamic behavior, and modularity of the tools.

A. *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.

B. *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.

C. *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 (HyperText Transfer Protocol) 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.

Trend 3 – Faster discovery of vulnerabilities

The number of newly discovered vulnerabilities reported to the CERT/CC continues to more than double each year. 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.

Trend 4 – 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; for example, 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" (ActiveX controls, Java, and JavaScript) make it difficult for vulnerable systems to be protected and malicious software to be discovered. (See http://www.cert.org/reports/activeX_report.pdf.)

Trend 5 – Increasingly asymmetric 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.

Trend 6 – 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. Four types of infrastructure attacks are briefly described below.

Attack 1 – Distributed 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 with high-speed connections. 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 is comprised of limited and consumable resources, and Internet security is highly interdependent.

Attack 2 – 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. (Code Red infected more than 250,000 systems in just 9 hours on July 19, 2001.)

Some worms include built-in denial-of-service attack payloads (Code Red) or web site defacement payloads (sadmind/IIS, Code Red); and others have dynamic configuration capabilities (W32/Leaves). 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, and they cause much collateral damage (examples include DSL routers that crash; cable modem

ISPs whose networks are completely overloaded, not by the scanning itself but by the burst of underlying network management (ARP) traffic that the scanning triggers; and printers that crash or print reams of junk output).

Attack 3 – Attacks on the Internet Domain Name System (DNS)

DNS is the distributed, hierarchical global directory that translates names (www.example.com) to numeric IP addresses (192.168.13.2). The top 2 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", ".net", etc., as well as the country code top level domains (ccTLDs – ".us", ".uk", ".ru", etc.) Threats to DNS include

- *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/CC shows that over 80% of the TLD domains 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/CC survey indicates that at least 20% of TLD domains are running on vulnerable servers; another 70% are "status unknown."

- *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 co-opt the domain registration processes to take control of legitimate domains.

Attack 4 – Attacks against or using routers

Routers are specialized computers that direct traffic on the Internet (similar to mail routing facilities in the postal service). 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 the strong encryption and authentication features available on the routers.

Potential impact of infrastructure attacks

Denial of service

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 between 1 and 155 megabits per second (Mbps) of bandwidth available. Attacks have been reported in the hundreds of Mbps and up, more than enough to saturate nearly any system on the Internet.

Compromise of sensitive information

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).

Misinformation

Intruders might be able to modify news sites, produce bogus press releases, and conduct other activities, all of which could have economic impact.

Time and resources diverted from other tasks

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

Conclusion

The purpose of this paper was to raise readers' awareness of current trends in attack techniques and tools. The trends seen by the CERT/CC 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. The appendix of this paper lists sources of more information about the problems and steps that can be taken to address them, if only in a limited way. Further information is available on the Internet Security Alliance and CERT/CC web sites. Much work remains for all of us as we analyze the problems, evaluate our risks, and determine what we can do to mitigate them.

Appendix: References and additional information

Denial of service

http://www.cert.org/advisories/CA-1999-17.html
http://www.cert.org/incident_notes/IN-99-07.html
http://www.cert.org/reports/dsit_workshop.pdf
http://www.cert.org/advisories/CA-2000-01.html
http://www.cert.org/incident_notes/IN-2000-05.html
http://www.cert.org/archive/pdf/DoS_trends.pdf

Intruders targeting vulnerable address blocks

http://www.cert.org/advisories/CA-2001-20.html

Worms

Morris: Denning, P. J., (ed.), *Computers Under Attack: Intruders, Worms, and Viruses,* ACM Press, Addison-Wesley, New York, 1990.

1i0n: http://www.cert.org/incident_notes/IN-2001-03.html

cheese: http://www.cert.org/incident_notes/IN-2001-05.html

sadmind/IIS: http://www.cert.org/advisories/CA-2001-11.html

Code Red: http://www.cert.org/advisories/CA-2001-19.html
http://www.cert.org/advisories/CA-2001-23.html
http://www.cert.org/incident_notes/IN-2001-10.html

Code Red II: http://www.cert.org/incident_notes/IN-2001-09.html

Nimda: http://www.cert.org/advisories/CA-2001-26.html

BIND vulnerabilities

http://www.cert.org/advisories/CA-1997-22.html
http://www.cert.org/advisories/CA-1998-05.html
http://www.cert.org/advisories/CA-1999-14.html
http://www.cert.org/advisories/CA-2000-20.html
http://www.cert.org/advisories/CA-2001-02.html
http://www.menandmice.com/6000/6200_bind_research.html

Mobile code vulnerabilities

http://www.cert.org/reports/activeX_report.pdf

DNS Configuration Errors

http://www.menandmice.com/6000/61_recent_survey.html

DNS server compromises

http://www.cert.org/advisories/CA-2000-03.html
http://www.cert.org/incident_notes/IN-2000-04.html
http://www.cert.org/incident_notes/IN-2001-03.html

Sircam

http://www.cert.org/advisories/CA-2001-22.html

Misinformation

http://www.usatoday.com/life/cyber/invest/ina039.htm
http://www.usatoday.com/life/cyber/2001/09/25/yahoo-danger.htm
http://www.cnn.com/2000/TECH/computing/10/03/nashaq.idg/index.html

Code Red economic impact

http://www.computereconomics.com/cei/news/codered.html

9/11 IT economic impact

http://www.computereconomics.com/cei/news/terroristpr.html

“Window of vulnerability”

http://www.cs.umd.edu/~waa/pubs/Windows_of_Vulnerability.pdf

“CERT” and “CERT Coordination Center” are registered in the U.S. Patent and Trademark Office.

Copyright 2002 Carnegie Mellon University