Trends in Denial of Service Attack Technology

CERT® Coordination Center

Kevin J. Houle, CERT/CC
George M. Weaver, CERT/CC

In collaboration with:
Neil Long
Rob Thomas

v1.0
October 2001

1 Abstract

In November of 1999, the CERT® Coordination Center (CERT/CC) sponsored the Distributed Systems Intruder Tools (DSIT) Workshop where a group of security experts outlined the emerging threat of distributed denial of service (DDoS) attack technology. Since then, denial of service (DoS) attack technology has continued to evolve and continues to be used to attack and impact Internet infrastructures.

Advances in intruder automation techniques have led to a steady stream of new self-propagating worms in 2001, some of which have been used to deploy DoS attack technology. Windows end-users and Internet routing technology have both become more frequent targets of intruder activity. The control mechanisms for DDoS attack networks are changing to make greater use of Internet Relay Chat (IRC) technology. The impacts of DoS attacks are causing greater collateral damage, and widespread automated propagation itself has become a vehicle for causing denial of service.

While DoS attack technology continues to evolve, the circumstances enabling attacks have not significantly changed in recent years. DoS attacks remain a serious threat to the users, organizations, and infrastructures of the Internet.

The goal of this paper is to highlight recent trends in the deployment, use, and impact of DoS attack technology based on intruder activity and attack tools reported to and analyzed by the CERT/CC. This paper does not propose solutions, but rather aims to serve as a catalyst to raise awareness and stimulate further discussion of DoS related issues within the Internet community.

2 Introduction

The traditional intent and impact of DoS attacks is to prevent or impair the legitimate use of computer or network resources. Regardless of the diligence, effort, and resources spent securing against intrusion, Internet connected systems face a consistent and real threat from DoS attacks because of two fundamental characteristics of the Internet.

- The Internet is comprised of limited and consumable resources

  The infrastructure of interconnected systems and networks comprising the Internet is entirely composed of limited resources. Bandwidth, processing power, and storage capacities are all common targets for DoS attacks designed to consume enough of a target's available resources to cause some level of service disruption. An abundance of well-engineered resources may raise the bar on the degree an attack must reach to be effective, but today's attack methods and tools place even the most abundant resources in range for disruption.

- Internet security is highly interdependent

  DoS attacks are commonly launched from one or more points on the Internet that are external to the victim's own system or network. In many cases, the launch point consists of one or more systems that have been subverted by an intruder via a security-related compromise rather than from the intruder's own system or systems. As such, intrusion defense not only helps to protect Internet assets and the mission they support, but it also helps prevent the use of assets to attack other Internet-connected networks and systems. Likewise, regardless of how well defended your assets may be, your susceptibility to many types of attacks, particularly DoS attacks, depends on the state of security on the rest of the global Internet.

Defending against DoS attacks is far from an exact or complete science. Rate limiting, packet filtering, and tweaking software parameters can, in some cases, help limit the impact of DoS attacks, but usually only at points where the DoS attack is consuming fewer resources than are available. In many cases, the only defense is a reactive one where the source or sources of an ongoing attack are identified and prevented from continuing the attack. The use of source IP address spoofing during attacks and the advent of distributed attack methods and tools have provided a constant challenge for those who must respond to DoS attacks.

Early DoS attack technology involved simple tools that generated and sent packets from a single source aimed at a single destination. Over time, tools have evolved to execute single source attacks against multiple targets, multiple source attacks against single targets, and multiple source attacks against multiple targets.

Today, the most common DoS attack type reported to the CERT/CC involves sending a large number of packets to a destination causing excessive amounts of endpoint, and possibly transit, network bandwidth to be consumed. Such attacks are commonly referred to as packet flooding attacks. Single source against single target attacks are common, as are multiple source against single target attacks. Based on reported activity, multiple target attacks are less common.

The packet types used for packet flooding attacks have varied over time, but for the most part, several common packet types are still used by many DoS attack tools.

TCP floods – A stream of TCP packets with various flags set are sent to the victim IP address. The SYN, ACK, and RST flags are commonly used.

ICMP echo request/reply (e.g., ping floods) – A stream of ICMP packets are sent to a victim IP address.

UDP floods – A stream of UDP packets are sent to the victim IP address.

Because packet flooding attacks typically strive to deplete available processing or bandwidth resources, the packet rate and volume of data associated with the packet stream are important factors in determining the attack's degree of success. Some attack tools alter attributes of packets in the packet stream for a number of different reasons.

Source IP address – In some cases, a false source IP address, a method commonly called IP spoofing, is used to conceal the true source of a packet stream. In other cases, IP spoofing is used when packet streams are sent to one or more intermediate sites in order to cause responses to be sent toward a victim. The latter example is common for packet amplification attacks such as those based on IP directed broadcast packets (e.g., "smurf" or "fraggle").

Source/destination ports – TCP and UDP based packet flooding attack tools sometimes alter source and/or destination port numbers to make reacting with packet filtering by service more difficult.

Other IP header values – At the extreme, we have seen DoS attack tools that are designed to randomize most all IP header options for each packet in the stream, leaving just the destination IP address consistent between packets.

Packets with fabricated attributes are easily generated and delivered across the network. The TCP/IP protocol suite (IPv4) does not readily provide mechanisms to insure the integrity of packet attributes when packets are generated or during end-to-end transmission. Typically, an intruder need only have sufficient privilege on a system to execute tools and attacks capable of fabricating and sending packets with maliciously altered attributes.

In June of 1999, multiple source DoS, or DDoS, tools began to be deployed. It is from that point in time forward that we evaluate trends in DoS attack technology. Though the focus of this paper is the continuing evolution of DoS attack technology, it is important to note that older tools are still successfully employed by intruders to execute DoS attacks.

3 Timeline

What follows is a brief timeline to highlight some of the major trend events in attack technology evolution. A more granular timeline is required to capture all trend events since July 1999, but that is not the purpose here. For our purposes, we are only interested in a timeline that highlights trends associated with widespread Internet activity based on reports received by the CERT/CC.

1999

July

Widespread deployment of DDoS networks based on tools like 'trinoo' and 'Tribe Flood Network' via various RPC related vulnerabilities. Many of the initial deployments were done manually, with intruders carefully testing for and selecting hosts positioned with high bandwidth availability.

DDoS networks used classic handler/agent control topology with direct communication via custom TCP, UDP, and ICMP protocols. Packet flooding attacks used UDP floods, TCP SYN floods and ICMP echo request floods.

DDoS networks were linked together with hard-coded handler lists in the agents, and with local files at the handler containing agent IP addresses.

DDoS agents listened for inbound commands from the handler. IDS signatures and network scanners were able to detect the presence of these types of DDoS agents on networks.

CERT® Incident Note IN-99-07
Distributed Denial of Service Tools
http://www.cert.org/incident_notes/IN-99-07.html

August

Stacheldraht DDoS tool found in isolated incidents. Stacheldraht combined features of ‘trinoo’ and TFN and added encrypted communications between the attacker and the stacheldraht handlers. Stacheldraht also provided for automated update of agents.

Again, deployment involved selective targeting based on the packet generating capability of the target systems.

DOCKET
ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | sales@docketalarm.com | 1-866-77-FASTCASE

fastcase®
Smarter legal research.