DDoS Tools & Traffic Signature Reference Guide

This reference guide provides detailed information on common Distributed Denial of Service (DDoS) tools, their traffic signatures, and how to detect and defend against them. It is designed to help learners and defenders recognize tools used in both testing and real-world attack scenarios.

LOIC (Low Orbit Ion Cannon)

• Type: Open-source stress testing tool, often used in coordinated voluntary attacks

• Traffic Pattern:
Launches high volumes of TCP, UDP, or HTTP requests.
Payloads are non-random and easy to fingerprint.

• Signature Example:
User-Agent: LOIC
Host: target.com

• Detection Tips:
Look for large numbers of identical HTTP requests from a single IP.
Common identifiers like the "LOIC" User-Agent header are easy to spot in web server logs.
High connection rates from one or more sources without meaningful application interaction.

• Real-World Notes: LOIC does not spoof IPs, so attackers can be traced if logs are retained.

HOIC (High Orbit Ion Cannon)

• Type: Upgraded version of LOIC that supports customizable attack scripts (called booster files)

• Traffic Pattern:
Generates highly randomized HTTP floods using booster scripts.
Harder to detect using simple signature matching.

• Signature Example:
Unusual or inconsistent HTTP headers.
Bursts of randomized GET/POST traffic from the same or multiple clients.

• Detection Tips:
Look for anomalies in User-Agent strings and header combinations.
High rate of TCP sessions being created and dropped quickly.
Payload entropy can help detect randomized content.

• Real-World Notes: More evasive than LOIC but still detectable with behavioral analysis.

hping3

• Type: Command-line packet crafter for testing and offensive security use

• Traffic Pattern:
Can generate SYN, FIN, ICMP floods, and more.
Often used to simulate DDoS or test firewall responses.
Supports spoofed source IPs.

• Signature Example:
Flags: SYN Seq: 0 Win: 512

• Detection Tips:
Analyze TCP flags (e.g., high volume of SYNs with no corresponding ACKs).
Track for inconsistent TTL values and sequence numbers.
Sudden spike in small, uniform packets from many IPs.

• Real-World Notes: Must be paired with network-level anomaly detection to effectively identify.

Slowloris

• Type: Low-and-slow denial-of-service tool targeting HTTP servers

• Traffic Pattern:
Opens many simultaneous connections and sends partial HTTP headers very slowly.
Ties up server resources by never completing the request.

• Signature Example:
Connections held open for unusually long times.
No full HTTP request ever delivered.

• Detection Tips:
Watch for abnormally high connection times with minimal data transfer.
Analyze for large numbers of open connections in WAITING or ESTABLISHED state.
Enable timeouts and connection limits on your web server.

• Real-World Notes: Very effective against servers with high connection limits and minimal idle timeouts.

Metasploit DDoS Modules

• Type: Framework for penetration testing, includes optional flood modules

• Traffic Pattern:
Custom TCP/UDP floods, HTTP flooding, DNS amplification.

• Signature Example:
Spoofed or malformed requests (varied)

• Detection Tips:
Monitor for high rate of incomplete TCP handshakes.
Detect outbound DNS traffic to known reflector IPs.
Log anomalies or malformed requests from unexpected services.

• Real-World Notes: Detection is reliant on baselining known-good traffic and alerting on outliers.

Detection Techniques Summary

Tool	Likely Protocols	Detection Approach
LOIC	TCP, UDP, HTTP	Repetition, known user-agent
HOIC	HTTP	Header fuzzing, entropy anomalies
hping3	TCP, ICMP	Flag anomalies, spoofed IPs
Slowloris	HTTP	Idle/open connections, no requests
Metasploit	Mixed	Correlation, spoofing detection

Prepared by: Charles J. Wasson