radware

THE RADWARE DDOS ATTACK CHECKLIST

The cyberattack threat landscape has never been more complex. Thanks to the growing array of online marketplaces, attack tools have never been easier to access and execute. From burst attacks to internet of things (IoT) botnets and encrypted attacks, the sheer quantity of attack vectors has never made safeguarding your organization and customers more difficult.

The threat landscape is unforgiving and preys on those organizations with cybersecurity architectures that are unprepared to mitigate the wide array of cyberattacks they will face. Ensure your DDoS mitigation solution can protect your organization, applications and customers from current and future cyberattacks.

This checklist provides an overview of the attack vectors that Radware's DefensePro detects and mitigates.

NETWORK-LAYER ATTACKS

Network-layer attacks target network resources and attempt to consume all of a victim's network bandwidth by using a large volume of illegitimate traffic to saturate the company's internet pipe. These attacks are simple yet effective.

THREAT	ATTACK TYPE	VULNERABILITY	DETECT?	MITIGATE?
TCP FLOOD	TCP (ACK, PSH, RST, FIN Flood, Mirai-originated)	Host exhaustion/link consumption	Yes	Yes
	SYN Flood	Host exhaustion/link consumption	Yes	Yes
	TCP NULL (no flags set)/Packet Anomaly Flood (Non-RFC Compliant)	Host exhaustion/link consumption	Yes	Yes
	Xmas Flood TCP packets (all flags set on)	Host exhaustion/link consumption	Yes	Yes
	STOMP Flood	Host exhaustion/link consumption	Yes	Yes
	Empty Connection Flood	Host exhaustion/link consumption	Yes	Yes
UDP FLOOD (NON-DNS)	UDP Flood (Mirai-originated, high-rate small packets, large packets, Garbage, DNS and NTP reflective floods)	Host exhaustion/link consumption	Yes	Yes
ICMP FLOOD	ICMP Echo Request, Unreachables, Source Quench	Host exhaustion/link consumption	Yes	Yes
IGMP FLOOD		Host exhaustion/link consumption	Yes	Yes
BURST ATTACK (TCP, UDP, ICMP, IGMP)	Bursts of volumetric, short-lived floods arriving with silent periods between waves	Host exhaustion/link consumption	Yes	Yes
GRE IP FLOOD	IP packets flood traffic tunneled in GRE, included in Mirai	Link consumption	Yes	Yes
GRE ETHERNET FLOOD	Ethernet packets flood traffic tunneled in GRE, included in Mirai	Link consumption	Yes	Yes

ENCRYPTION-BASED THREATS

Encryption-based threats are cyberattacks that use encryption protocols, such as SSL and TLS, to hide malicious payloads inside of network traffic. Encryption-based attacks have risen dramatically in recent years.

THREAT	ATTACK TYPE	VULNERABILITY	DETECT?	MITIGATE?
SSL COMPUTING	SSL renegotiation	SSL vulnerability	Yes	Yes
	SSL traffic	HTTPS flooding/CPS limits/bypass detection	Yes	Yes
	SSL handshake	Computation power	Yes	Yes

APPLICATION-LAYER ATTACKS

Recent years have brought a rise in DDoS attacks targeting applications. They primarily target application protocols that possess exploitable weaknesses, including HTTP and HTTPS protocols, DNS, SMTP, FTP, VoIP and others.

THREAT	ATTACK TYPE	VULNERABILITY	DETECT?	MITIGATE?
HTTP (GET/POST) FLOOD ATTACK	HTTP Get/Put/Post flooding	Host exhaustion/link consumption	Yes	Yes
		Processing power	Yes	Yes
	HTTP vulnerability	Protocol/RFC	Yes	Yes
HTTP FLOOD	Get request	Host exhaustion	Yes	Yes
	Post request — variable values	Host exhaustion	Yes	Yes
	Put request	Host exhaustion	Yes	Yes
	Search engine flood	Backend database	Yes	Yes
	Login page flood	Backend authentication	Yes	Yes
	Brute Force	Confidentiality/backend authentication server	Yes	Yes
SMTP FLOOD	Email spoofing and backscatter	Host exhaustion/link consumption	Yes	Yes
FTP FLOOD	Establishing a large number of TCP connections with the victim and sending requests for heavy processing through FTP communication	Host exhaustion/link consumption	Yes	Yes
FTP BRUTE FORCE	FTP Credential Brute Force attack	FTP authentication integrity	Yes	Yes
DNS	DNS volumetric attack (Query Flood)		Yes	Yes
	DNS Water Torture (Mirai)	Host exhaustion/link consumption	Yes	Yes
	DNS amplification and reflection (Response Flood)	Host exhaustion/link consumption	Yes	Yes
	DNS cache poisoning	Integrity/availability	Yes	Yes
SIP/VOIP	Register/Invite floods	Application-layer attack on the Session Initiation Protocol (SIP) in use in VoIP services, targeted at causing denial of service to SIP servers. A SIP Register flood consists of sending a high volume of SIP Register or Invite packets to SIP servers (indifferently accepting endpoint requests as first step of an authentication process), thereby exhausting their bandwidth and resources.	Yes	Yes
	SIP Brute Force attack	Detecting and mitigating attackers to try to brute force login or create processing load on SIP servers	Yes	Yes
SIP MALFORMED PACKET	A SIP malformed attack consists of sending any kind of nonstandard messages (e.g., malformed SIP Invite) with an intentionally invalid input, thereby making the system unstable		Yes	Yes
MIRAI — VALVE SOURCE SPECIFIC FLOOD	A targeted attack on Valve Source gaming servers	Link consumption	Yes	Yes
SLOW-RATE ATTACK (AKA RUDY OR SLOWLORIS)	Slow HTTP Get or Post requests	Processing power	Yes	Yes
		Connections/sessions	Yes	Yes
		Memory	Yes	Yes

ATTACK TECHNIQUES

Hackers leverage a wide array of attack vectors to either bypass or overwhelm DDoS mitigation defenses.

THREAT	ATTACK TYPE	DETECT?	MITIGATE?
VOLUMETRIC ATTACK	Reflective/Amplification attacks (DNS, NTP)	Yes	Yes
	TCP/UDP/ICMP/IGMP Flood	Yes	Yes
	SYN/Push/ACK Flood	Yes	Yes
	Malformed DNS queries/packets	Yes	Yes
	High-volume, properly formatted DNS queries	Yes	Yes
	DNS amplification/reflection attacks	Yes	Yes
RFC/COMPLIANCE ATTACK	Invalid Protocol, etc.	Yes	Yes
COMPUTE-INTENSIVE ATTACK	HTTP Slow Request	Yes	Yes
	HTTP Slow Post	Yes	Yes
	HTTP Slow Read	Yes	Yes
	Encrypted HTTP traffic flood	Yes	Yes
	Empty Connection Flood	Yes	Yes
	Hash DoS	Yes	Yes
	SSL renegotiation	Yes	Yes
	Search engine and login page attacks exploiting backend databases	Yes	Yes
BRUTE FORCE ATTACK	HTTP Brute Force/web scan (login invalid/40x errors storm)	Yes	Yes
	SMTP/FTP/SQL/MySQL/IMAP Brute Force	Yes	Yes
	Invalid website input parameters attack	Yes	Yes
	Search engine request attack	Yes	Yes
	DNS Brute Force (dictionary/zone enumeration — nonexistent domain)	Yes	Yes
	SIP Brute Force attack (SIP Request flood — Forbidden/Not Acceptable, etc.)	Yes	Yes
	SMB/LDAP Brute Force	Yes	Yes
INTRUSION/INFORMATION GATHERING	Vulnerability exploit, buffer overflow, SQL injection, XSS, CSRF, etc.	Yes	Yes
RECONNAISSANCE — SCANNING	Vertical scanning, horizontal scanning	Yes	Yes
RECONNAISSANCE — VULNERABILITY	Identification of vulnerable application, host fingerprinting, etc.	Yes	Yes
COMMON ATTACK TOOLS	Sockstress (Layer 4 connection flood, zero window)	Yes	Yes
	Slowloris/Pyloris (Slow HTTP Request)	Yes	Yes
	LOIC or variants (HTTP, TCP, UDP Flood)	Yes	Yes
	HOIC or variants (HTTP flooding with multithreading and booster scripting)	Yes	Yes
	nkiller2 (TCP Persist)	Yes	Yes
	SIP call-control flood	Yes	Yes
	THC-SSL (SSL renegotiation)	Yes	Yes
	Recoil	Yes	Yes
	RUDY (Slow HTTP Post)	Yes	Yes
	Hulk	Yes	Yes
	XerXeS DoS	Yes	Yes
	#RefRef DoS	Yes	Yes
	Dirt Jumper	Yes	Yes
	Apache Killer	Yes	Yes
	SIPVicious, Sundayddr, SipP, SipCrack	Yes	Yes

radware

THE RADWARE DDOS ATTACK CHECKLIST

RADWARE DEFENSEPRO

DefensePro is part of Radware's Attack Mitigation Solution and is an award-winning, real-time perimeter DDoS defense and attack mitigation device, which secures organizations against emerging network and application threats. DefensePro provides automated DDoS defense and protection from high-volume, encrypted or short-duration threats, including IoT-based, pulse, burst, DNS and TLS/SSL attacks and those attacks associated with permanent denial-of-service and ransom denial-of-service techniques.

DefensePro includes a comprehensive set of four essential security modules — anti-DDoS, network behavioral analysis, intrusion prevention system and SSL attack protection — to fully protect the application infrastructure against known and emerging network security attacks. It employs multiple detection and mitigation modules, including adaptive behavioral analysis, challenge/response technologies and automatic real-time signature creation, against emerging network, zero-day, DoS/DDoS and application misuse attacks, network scanning and malware spreading. It eliminates the need for human intervention and does not block legitimate user traffic.

Learn More About Radware's DDoS Protection Solutions

Contact Your Radware Sales Representative to Learn More

About Radware

Radware® (NASDAQ: RDWR) is a global leader of cybersecurity and application delivery solutions for physical, cloud and software-defined data centers. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application and corporate IT protection and availability services to enterprises globally. Radware's solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt quickly to market challenges, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.

Radware encourages you to join our community and follow us on: Radware Blog, LinkedIn, Facebook, Twitter, SlideShare, YouTube, Radware Connect app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis of DDoS attack tools, trends and threats.