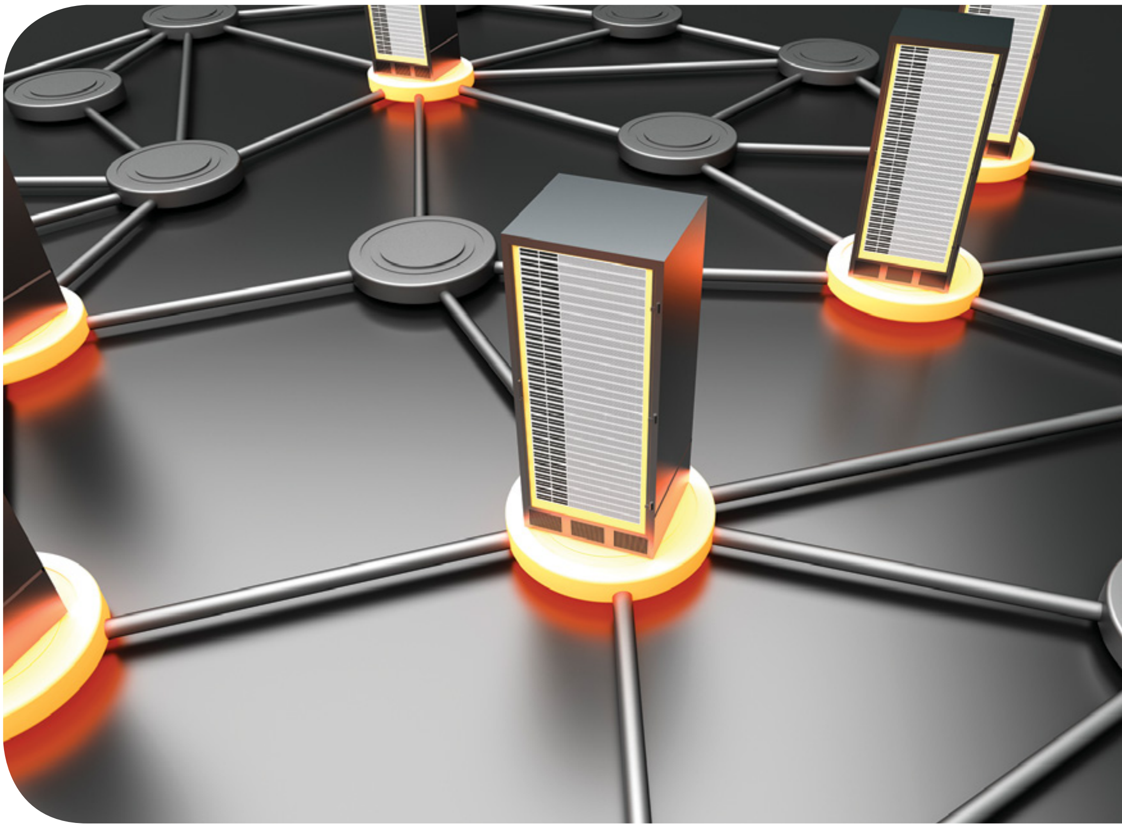
Technical Series



A Prolexic White Paper

Distributed Reflection Denial of Service (DrDoS) Attacks

An Introduction to the DrDoS White Paper Series

PROLEXIC
DDoS Attacks End Here.

In 2012, there was a significant increase in the use of a specific distributed denial of service (DDoS) methodology known as Distributed Reflection Denial of Service attacks (DrDoS). DrDoS attacks have been a persistent and effective type of DDoS attack for more than 10 years. The technique shows no signs of obsolescence; it continues to grow in effectiveness and popularity.

Prolexic has observed many DrDoS attacks across a range of industries. The Prolexic Security Engineering and Response Team (PLXsert) is producing a series of white papers that analyze Reflection and Amplification DDoS Attacks. The four types of DrDoS attacks are:

- DNS
- SYN
- SNMP/NTP/CHARGEN
- Gaming server attacks

The white paper series will detail real-world case studies of DrDoS attacks observed by PLXsert through the Prolexic global DDoS mitigation network. Their purpose is to:

- Bring more attention to this often overlooked DDoS attack method
- Make system administrators aware of potential security exploits against their servers
- Help victims of DrDoS attacks understand the technical aspects of what took place

DrDoS techniques usually involve multiple victim host machines that unwittingly participate in a DDoS attack on the attacker's primary target. Requests to the victim host machines are redirected, or reflected, from the victim hosts to the target.

Anonymity is one advantage of the DrDoS attack method. In a DrDoS attack, the primary target appears to be directly attacked by the victim host servers, not the actual attacker. This approach is called spoofing.

Amplification is another advantage of the DrDoS attack method. By involving multiple victim servers, the attacker's initial request yields a response that is larger than what was sent, thus increasing the attack bandwidth.

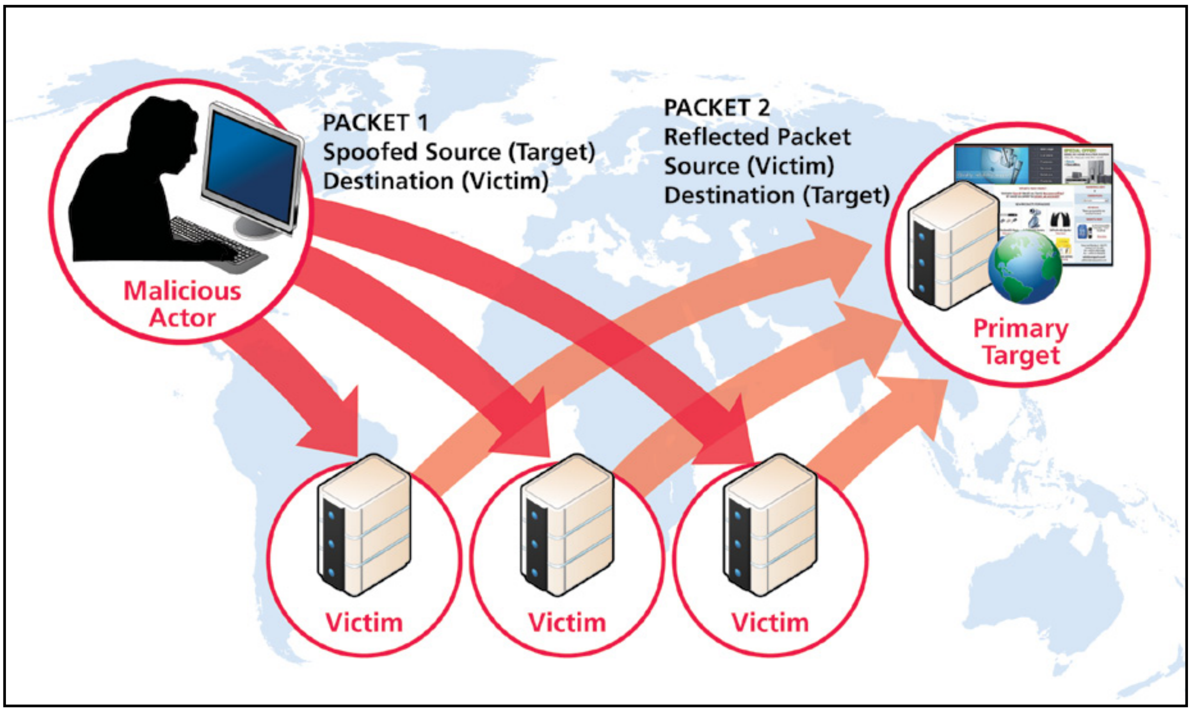


Figure 1: The DrDoS attack method amplifies the attacker's original request by involving multiple victim hosts in a spoofed attack against the primary target.

In Figure 1, a malicious actor is shown making a DrDoS attack. The malicious actor makes it appear to a victim host server that the primary target is contacting them with a request. The victim host servers therefore respond back to the primary target, which they mistakenly think made the initial request (a spoof). The reflected denial of service attack is called distributed because of the involvement of multiple victim host servers. The attacker may be a single actor or multiple actors.

Glossary for DrDoS white paper series

The glossary defines terms used in the white paper series. Familiarity with these DrDoS terms will allow the reader a better understanding of DrDoS attack concepts.

Distributed Reflection Denial of Service (DrDoS) Attack – A DDoS attack that uses spoofed requests to victim host servers to produce responses directed at a primary target. A distributed attack involves multiple victim host servers.

Malicious Actor – The originating source of spoofed requests that generate the DrDoS attack traffic.

Victim – A host server with an application service that responds to the actor's spoofed requests and thus participates in the attack.

Primary target – The server receiving the majority of the attack traffic initiated by the malicious actor.

Spoofing – Creation of TCP/IP packets using a third party's IP address (typically the destination IP) to mask the source IP address.

About Prolexic Security Engineering & Response Team (PLXsert)

PLXsert monitors malicious cyber threats globally and analyzes DDoS attacks using proprietary techniques and equipment. Through digital forensics and post attack analysis, PLXsert is able to build a global view of DDoS attacks, which is shared with our customers. By identifying the sources and associated attributes of individual attacks, the PLXsert team helps organizations adopt best practices and make more informed, proactive decisions about DDoS threats.

About Prolexic

Prolexic Technologies is the world's largest, most trusted distributed denial of service (DDoS) protection and mitigation service provider. Able to absorb the largest and most complex DDoS attacks ever launched, Prolexic protects and restores within minutes mission-critical Internet-facing infrastructures for global enterprises and government agencies. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel, hospitality, gaming and other industries at risk for DDoS attacks rely on Prolexic for DDoS protection. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida, and has DDoS scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, call +1 (954) 620 6002 or follow @Prolexic on Twitter.