(PRLEAP.COM) Prolexic Technologies, the global leader in Distributed Denial of Service (DDoS) protection services, today issued a high alert DDoS attack threat advisory on the DNS Flooder v1.1 toolkit. The toolkit makes it faster and easier for malicious actors to launch crippling reflection attacks and will likely be widely adopted in the DDoS-as-a-Service market, potentially increasing the number of attacks.

This new toolkit enables malicious actors to purchase, set up and use their own DNS servers to launch reflection attacks without the need to find open and vulnerable DNS servers on the Internet. This expedites the availability of the DNS botnet, enabling malicious actors to launch large cyber attacks without having to spend considerable time and resources building an army of bots through malware infections.

"As the DNS Flooder toolkit uses reflection and amplification techniques, attackers can anonymously launch powerful DDoS attacks with just a handful of servers," said Stuart Scholly, president of Prolexic. "Widespread usage in the DDoS-as-a-Service market is likely and the security community needs to be aware and closely monitor this emerging threat."

Prolexic has observed the DNS Flooder toolkit in multiple DDoS attack campaigns against its global client base over the last six months. In some cases, the campaigns have had amplification factors of 50 times the originating bandwidth.

The DNS Flooder toolkit uses a multi-step process to launch DDoS attacks:

1. The toolkit spoofs the IP address of the intended target and creates a DNS request, which is sent to attacker's DNS botnet.2. The attacker's DNS botnet sends an extended DNS (EDNS) response back. The EDNS response includes more data than the DNS request (amplification). Because the IP address used in the request was spoofed, the response is reflected back to the attacker's target. 3. The toolkit loops multiple times, reflecting and amplifying the response to the target with each loop.

Prolexic's DNS Flooder threat advisory provides a detailed analysis of the toolkit, sample payloads, recommended DDoS protection and mitigation techniques, as well as case studies on two DNS Flooder campaigns directed against Prolexic clients. A complimentary download of the threat advisory is available at www.prolexic.com /dns-flooder.

Prolexic Threat AdvisoriesDesigned to provide early warnings of new or modified DDoS denial of service attack signatures and scripts, recently observed by PLXsert, each threat advisory contains a detailed description of the type of DDoS attack, a list of attack signatures, and the specific network infrastructure or application that it targets. In addition, Prolexic's DDoS mitigation experts also offer insight into the nature of each type of attack, as well as provide specific warnings as to how the attack will affect businesses and enterprises of different sizes and infrastructures.

About the Prolexic Security Engineering & Response Team (PLXsert)PLXsert monitors malicious cyber threats globally and analyzes DDoS attacks using proprietary techniques and equipment. Through data forensics and post attack analysis, PLXsert is able to build a global view of DDoS attacks, which is shared with 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.

Details of Prolexic's DDoS mitigation activities and insights into the latest tactics, types, targets and origins of global DDoS attacks are provided in quarterly reports published by the company. Prolexic's global DDoS attack reports are available at www.prolexic.com/attackreports.

About ProlexicProlexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider.
Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming, energy and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Fort Lauderdale, Florida, and has 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
, follow us on LinkedIn, Facebook, Google+, YouTube, and @Prolexic on Twitter.