(PRLEAP.COM) Hollywood, FL – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, today detailed the rampant problem of denial of service attacks within and from online gaming communities. The DDoS attacks, which can pack a powerful punch by the use of reflection and amplification (DrDoS) techniques, have been used against other gamers, gaming platforms and even third party targets such as financial services and other non-gaming businesses.

The availability and accessibility of online gaming infrastructures and devices creates opportunities for malicious actors to launch DDoS attacks and steal login credentials. Denial of service attacks have a long tradition in the community, occur frequently and keep evolving.

"DDoS attacks fueled by rivalries, poor password security protocols and readily available DDoS tools are widespread and harm gaming and non-gaming targets alike," said Stuart Scholly, president of Prolexic. "There are serious repercussions for every industry from denial of service attacks that feed off the explosive growth of online gaming infrastructures."

A Prolexic customer in the financial industry was the target of a DrDoS attack that reached 5 Gbps and made use of misconfigured game servers as intermediary victims to reflect and amplify network traffic to the financial services target, in an effort to stop it with a DDoS attack.

As is common in DrDoS attacks, the malicious actors increased the power of their DDoS attack against the financial services firm with reflection and amplification techniques. Sending a small request to one gaming server produced an outsized response that was five times larger than the initial request. The attackers co-opted hundreds of gaming servers to produce the same outsized response at once, and repeatedly, against the targeted financial services firm.

The attack was stopped by Prolexic's DDoS mitigation service .

"This attack targeted Call of Duty 2 gaming servers across the globe – in South Africa, Europe, Asia and the United States," explained Scholly. "PLXsert has replicated the attack in our lab."

In the white paper, the culminating piece in a series explaining DrDoS attacks , the Prolexic Security Engineering & Response Team (PLXsert) explains:

Why DDoS attacks occur in online gaming communities The history of DrDoS attacks in online gaming DrDoS attack tools that use gaming servers – including Quake, Half Life, and Call of Duty – to attack non-gaming targets A case study of a DrDoS attack against a financial services firm The underground market for stressors, booters and other DDoS-as-a-Service tools that target online gaming communities The white paper, the concluding piece in Prolexic's DrDoS series, is available free of charge at www.prolexic.com/gaming .

The laboratory-created proof-of-concept attack script will be available to the public on the official PLXsert GitHub page
located at
http://www.github.com/plxsert
.

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. A complimentary copy of Prolexic's most recent Global DDoS Attack Report is 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 Hollywood, 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 and follow us on LinkedIn, Facebook, Google+, YouTube, and @Prolexic on Twitter.