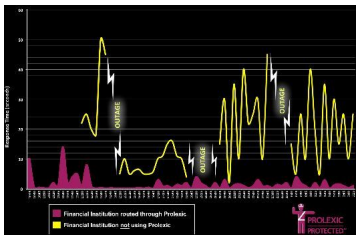

(PRLEAP.COM) Hollywood, FL – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, announced today that its secure socket layer (SSL) key sharing tools allow customers to maintain control of their SSL keys at all times, while making it easier for Prolexic to detect and stop encrypted Layer 7 (application layer) DDoS attacks. The SSL key sharing tools are provided with the Prolexic Application-Based Monitoring (PLXabm) service and PLXproxy , Prolexic's on-demand, symmetric DDoS mitigation service.

"Malicious actors are employing more sophisticated attack techniques, and as a result we anticipate the frequency of encrypted Layer 7 DDoS attacks will rise," said Stuart Scholly, president at Prolexic. "It is especially challenging to stop DDoS attacks in encrypted flows, because they can only be examined using a customer's encryption key."

Monitoring encrypted traffic with PLXabm SSL Hardware Security Module

An encrypted Layer 7 DDoS attack is detected and analyzed by examining packet headers, which require a customer's unique SSL key to unlock. For quicker and easier DDoS analysis and detection, Prolexic developed the PLXabm SSL Hardware Security Module. Compliant with FIPS-140-2 Level 2 key management standards, the SSL Hardware Security Module facilitates decryption of SSL traffic bi-directionally and enables automated alerting when a DDoS attack is detected.

"This enhancement to PLXabm allows our engineers to identify and isolate the source IP address, which they can use to block encrypted Layer 7 attacks," said Scholly. "Best of all, this approach ensures that our customers can maintain control over their SSL keys at all times."

Stopping DDoS attacks in encrypted traffic with PLXproxy

Prolexic can mitigate encrypted DDoS attacks using its PLXproxy service once the customer's SSL keys and certificates are uploaded and deployed to Prolexic. Customers can elect to have these items stored securely for reuse or to provide temporary certificates and keys that are revoked after an encrypted DDoS attack is stopped. To aid in this process, PLXproxy SSL Manager, a secure and efficient way to upload SSL keys and certificates, can be accessed through the PLXportal, an online resource devoted to giving Prolexic customers greater visibility into their Prolexic DDoS mitigation services and activity.

For additional details, please visit the Prolexic DDoS Protection Services at http://www.prolexic.com/services-dos-and-ddos-protection.html
to download data sheets on Prolexic's SSL capabilities, the PLXabm monitoring service and the PLXproxy mitigation service.

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.