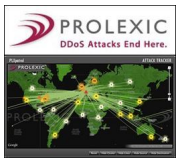

(PRLEAP.COM) Hollywood, FL – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, today shared attack signatures and details that are helpful to detect and stop DDoS attacks from the Drive DDoS toolkit, an attack tool often used as a source of distraction while criminals break into customer accounts at finance firms and e-Commerce businesses.

DDoS attacks from the Drive DDoS toolkit and other variants of the Dirt Jumper toolkit can sidetrack IT security personnel while criminals attempt to transfer funds out of bank accounts, gather passwords for later use, or place unauthorized orders. Because attacks from this criminal DDoS toolkit are associated with identity theft, recognizing the Drive toolkit as the source of a DDoS attack can lead financial institutions, banking, insurance, investment firms, brokerages or e-Commerce firms to suspect and investigate possible fraudulent access of customer accounts that may have occurred during the attack.

"During the confusion of a DDoS attack, malicious actors can break into the financial and e-Commerce accounts of customers without being noticed," warned Stuart Scholly, President at Prolexic. "IT departments are typically so focused on the damage caused by the DDoS attack that they don't realize it may merely be a planned distraction while criminals loot customer accounts."

New signatures, communication patterns

The Drive toolkit, which is being leaked in underground hacking forums, has been the source of multiple recent DDoS attacks observed by the Prolexic Security Engineering and Response Team (PLXsert). The tool is a newer variant of the Dirt Jumper family of DDoS toolkits, one of the most popular denial of service attack tools in use today.

"In recent weeks, Prolexic has detected, stopped and mitigated DDoS attacks launched against our clients from the Drive DDoS toolkit," said Scholly. "Although these attacks are cousins to Dirt Jumper DDoS toolkit, they have new signatures and communication patterns. In all cases, Prolexic mitigated attacks from the new toolkit in minutes, as promised in our service level agreement."

Attacks target Web applications

Six types of DDoS attacks are built into the Drive toolkit, allowing attackers to launch a variety DDoS attacks. The tool features GET floods , POST floods , POST2 floods, IP floods and IP2 floods directed at the application layer as well as UDP floods , which target network infrastructure. Encryption allows malicious actors to hide their identities.

"Companies often don't realize they are under attack from the Drive toolkit, because application attacks increase server utilization without excessive network traffic," Scholly added. "The information in the threat advisory can help detect these attacks quickly."

DDoS threat advisory

An analysis of the Drive threat, including screenshots, launch commands, sample payloads and identifying signatures to enable DDoS mitigation techniques, is available free of charge in Prolexic's Drive DDoS Threat Advisory at http://www.prolexic.com/drive-ddos .

Prolexic Threat AdvisoriesDesigned to provide early warnings of new or modified DDoS attack signatures and scripts recently observed by PLXsert, threat advisories contains descriptions of the type of attack, attack signatures, and the 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 and provide warnings as to how the attack will affect businesses and enterprises of different sizes and infrastructures. PLXsert also provides tips to help subscribers not only recognize the new attack signatures, but also proactively defend against them. The latest threat advisories, including itsoknoproblembro and Pandora, are available to the public at http://www.prolexic.com/threatadvisories .

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.