Akamai Warns of Large DDoS Attacks from Spike DDoS Toolkit

Botnet builders target a wider range of Internet-capable devices

Akamai Technologies, Inc. (NASDAQ: AKAM), the leading provider of cloud services for delivering, optimising and securing online content and business applications, today released, through the company's Prolexic Security Engineering & Response Team (PLXsert), a new cybersecurity threat advisory. The advisory alerts enterprises to a high-risk threat of powerful distributed denial of service (DDoS) attacks from the Spike DDoS toolkit. With this toolkit, malicious actors are building bigger DDoS botnets by targeting a wider range of Internet-capable devices. The advisory is available for download from Prolexic (now part of Akamai) at www.prolexic.com/spike.

"This summer Akamai mitigated huge multi-vector DDoS attack campaigns that we traced to bots controlled by the new Spike DDoS toolkit," said Stuart Scholly, senior vice president and general manager, Security Business Unit, Akamai. "This DDoS kit is designed to build botnets from devices and platforms that system administrators may not have thought to be at risk for botnet infection in the past. Enterprises need system hardening to prevent initial infection and DDoS protection to stop DDoS attacks from the Spike bots."

Huge, multi-vector attack peaked at 215 Gbps, 150 Mpps

The multi-vector toolkit can launch infrastructure-based and application-based DDoS payloads. Attacks include SYN flood, UDP flood, Domain Name System (DNS) query flood, and GET floods. Several campaigns have been reported against hosts in Asia and the United States. DDoS attack campaigns launched from the botnet have targeted Akamai customers. One DDoS attack campaign mitigated by Akamai peaked at 215 gigabits per second (Gbps) and 150 million packets per second (Mpps).

Botnet builders use more types of Internet-capable devices

The Spike DDoS toolkit runs on a Windows system, but it can communicate and execute commands to Windows, Linux and ARM-based devices infected with its binary payloads. The ability to generate an ARM-based binary payload suggests that the authors of this malicious tool are seeking to control devices such as routers and Internet of Things (IoT) devices (i.e., smart thermostat systems and washer/dryers). The capability to infect and control a broader range of devices could allow DDoS attackers to propagate botnets in a post-PC era.

DDoS mitigation of Spike DDoS attacks

Most the infrastructure DDoS attacks launched by the Spike DDoS toolkit can be mitigated by implementing access control lists (ACLs) that filter out unwanted traffic. To mitigate against the toolkit's application-layer GET flood attack, PLXsert has produced a SNORT signature, which is available in the threat advisory.

System hardening recommended

The multi-platform infection code in this kit increases the threat's complexity and sophistication and makes it necessary to apply system hardening measures to each of the targeted operating systems and platforms. Links to industry recommended hardening techniques are provided to system administrators in the advisory. The advisory also provides a YARA rule to identify bot payloads used to infect devices and make them part of the botnet.

PLXsert anticipates further infestation and the expansion of this DDoS botnet.

Get the Spike DDoS Toolkit Threat Advisory to learn more

In the advisory, PLXsert shares its analysis and details about the Spike DDoS toolkit, including:

- Indicators of binary infection
- Command and control panel
- Toolkit variations
- Bot initialisation
- DDoS payloads
- Details of an observed attack campaign
- DDoS mitigation, including a SNORT rule to stop the GET flood attack

- System hardening resources
- YARA rule for preventing bot infection

A complimentary copy of the threat advisory is available for download at www.prolexic.com/spike.

About Akamai

Akamai® is the leading provider of cloud services for delivering, optimising and securing online content and business applications. At the core of the Company's solutions is the Akamai Intelligent Platform™ providing extensive reach, coupled with unmatched reliability, security, visibility and expertise. Akamai removes the complexities of connecting the increasingly mobile world, supporting 24/7 consumer demand, and enabling enterprises to securely leverage the cloud. To learn more about how Akamai is accelerating the pace of innovation in a hyperconnected world, please visit www.akamai.com or blogs.akamai.com, and follow @Akamai on Twitter.