Tackling Cyber Attacks From Within

Jezmynn Koh, 2014-23-01

An increasing number of organizations face serious security threats that are socially, politically and economically motivated. Conventional firewalls are no longer enough to prevent complex and frequent cyber attacks such as multi-layer distributed denial-of-service (DDoS)/application layer attacks and SQL injection vulnerabilities.

In the past year, the number of DDoS attacks targeting vulnerable spots in web applications has risen and attackers are using increasingly complicated methods to bypass defenses. Meanwhile, 75% of CISOs aware external attacks had increased – 70% of CISOs noticed that web applications represent an area of risk higher than the network infrastructure.

The challenge with application-layer attacks is to differentiate human traffic from bot traffic. DDoS mitigation providers frequently utilize browser fingerprinting techniques like cookie tests and JavaScript tests to verify if requests are coming from real browsers. However, most recently, it's become apparent that cybercriminals have launched DDoS attacks from hidden, but real browser instances running on infected computers. This type of complex cyber attack is incredibly hard to detect.

What organizations need is a security strategy that is flexible and comprehensive, much like F5's web application firewall (WAF) and security solution. F5 recently received the 2013 Frost & Sullivan Asia Pacific Web Application Firewall Market Share Leadership Award. This recognition demonstrates excellence in capturing the highest market share for WAF solutions in the region and its achievement in remarkable year-on-year revenue growth – a true testimony to the execution of F5's security strategy.

Christian Hentschel, (SVP, APJ) noted that cyber-attacks often result in the loss or theft of intellectual property, money, sensitive corporate information, and identity. An effective security strategy encompasses not only the enterprise infrastructure but also the devices, the applications, and even the networks through which users access mobile and web applications.

F5's ICSA-certified WAF and policy-based web application security address cyber-threats at the application level. In September 2013, F5 strengthened its security portfolio with the acquisition of Versafe Ltd. – a web anti-fraud, anti-phishing, and anti-malware solutions provider. The acquisition reinforces F5's commitment to provide organizations with holistic, secure access to data and applications any time, from any device.

F5's comprehensive security solutions combine DNS security and DDoS protection, network firewall, access management, and application security with intelligent traffic management. Its flexibility to provide WAF both as a standalone solution and as an integrated offering on its BIG-IP® Application Delivery Controller platform provides customers with options that best suit their businesses. F5's ability to provide end-to-end application protection, advanced monitoring, and centralized management without comprising performance make their WAF solutions the number one choice throughout the Asia Pacific region.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com