F5 THREAT CAMPAIGNS

CHALLENGES

Targeted attack campaigns can be sophisticated and hard to detect

Threat hunting in-house is costly, time-consuming and less effective

Overly restrictive security policies can block legitimate users

KEY BENEFITS

Cost-effective model for confident risk mitigation

Improved web application security with near-zero false positives

Live updates with actionable threat intelligence from F5

Cyber adversaries are smart, fast and growing in number. The cyber-attacks they launch continuously threaten businesses and challenge security professionals. Standard security tools protect against a wide range of cyber-attacks but often cannot keep up with skillful threat actors. Web applications remain the top target of these attacks.

While a web application firewall (WAF) serves as an essential security control point, sophisticated attacks can evade baseline WAF security policies and configurations. To defend against these advanced threats, organizations need a WAF with tactical threat intelligence specifically designed to identify and mitigate sophisticated, targeted attacks.

F5® Threat Campaigns is an add-on threat intelligence subscription for F5® Advanced WAF™. The service provides intelligence that contains contextual information about the nature and purpose of the active threat campaign. In contrast, although a WAF may detect a syntax error in a web application form, without threat intelligence, it cannot correlate the singular attack incident as part of a more extensive and sophisticated threat campaign.

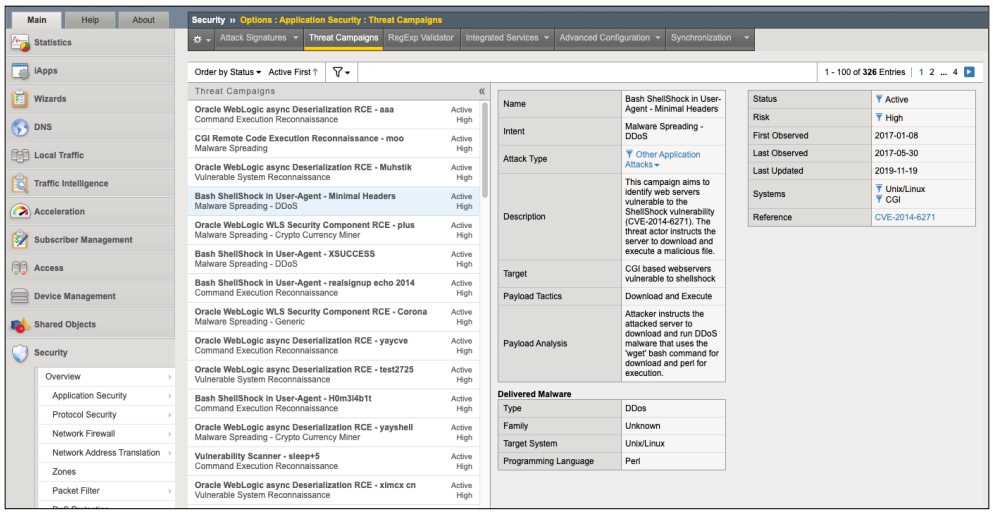

Figure 1: F5 Threat Campaigns Console