

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.

Mathematics 🏷		🔅 🗸 Attack Signatures 👻 Threat Campaigns RegExp Valid	lator Integ	grated Services - Advanced Co	onfiguration - Synchronization	·	
iApps		Order by Status - Active First↑ 🖓 -					1 - 100 of 326 Entries 1 2 4
Wizards		Threat Campaigns	Name	Bash ShellShock in User-	Status	T Active	
S DNS		Oracle WebLogic async Deserfalization RCE - aaa Command Execution Reconnaissance CGI Remote Code Execution Reconnaissance - moo Malware Spreading		Name	Agent - Minimal Headers	Risk	T High
				Intent	Malware Spreading - DDoS	First Observed	2017-01-08
Local Traffic				Attack Type	✓ Other Application Attacks → This campaign aims to identify web servers vulnerable to the ShellShock vulnerability (CVE-2014-6271). The threat actor instructs the server to download and	Last Observed	2017-05-30
Traffic Intelligence		Oracle WebLogic async Deserialization RCE - Muhstik Vulnerabie System Reconnaissance Bash SheliShock in User-Agent - Minimal Headers Malware Spreading - DOS Oracle WebLogic WLS Sacurity Component RCE - plus Malware Spreading - Crypic Currency Minar				Last Updated	2019-11-19
						Systems	T Unix/Linux CGI
				Description		Reference	CVE-2014-6271
Subscriber Management							
		Bash ShellShock in User-Agent - XSUCCESS Malware Spreading - DDoS	Active High		execute a malicious file.		
		Bash ShellShock in User-Agent - realsignup echo 2014 Command Execution Reconnaissance	Active High	Target	CGI based webservers vulnerable to shellshock		
				Payload Tactics	Download and Execute		
K Shared Objects		Oracle WebLogic WLS Security Component RCE - Corona Malware Spreading - Generic	Active High		Attacker instructs the attacked server to		
Security		Oracle WebLogic async Deserialization RCE - yaycve Command Execution Reconnaissance		Payload Analysis	download and run DDoS malware that uses the 'wget' bash command for		
Overview	w >	Oracle WebLogic async Deserialization RCE - test2725 Vulnerable System Reconnaissance	Active High		download and peri for execution.		
Applica	ation Security >	Bash ShellShock in User-Agent - H0m3l4b1t	Active	Delivered Malware			
Protoco	ol Security >	Command Execution Reconnaissance	High	Туре	DDos		
Networ	rk Firewall >	Oracle WebLogic async Deserialization RCE - yayshell Malware Spreading - Crypto Currency Miner	Active High	Family	Unknown		
Networ	rk Address Translation →	Vulnerability Scanner - sleep+5	Active	Target System Programming Language	Unix/Linux		
Zones		Command Execution Reconnaissance	High	Programming Language	Perl		
Packet	t Filter >	Oracle WebLogic async Deserialization RCE - ximcx cn Vulnerable System Reconnaissance	Active High				

Figure 1: F5 Threat Campaigns Console

F5 THREAT CAMPAIGNS

FEATURES:

Tactical Threat Intelligence

The F5 Threat Campaigns service uses metadata and multi-vector threat intelligence to help correlate the individual actions of an active attack campaign. This helps the F5 Advanced WAF identify an attack indicator as part of a threat campaign so that mitigation can be performed.

Near-Zero False Positives

Fully vetted attack signatures from F5 threat researchers enable security administrators to activate mitigations with confidence. This reduces exposure and helps block attackers before they can do damage.

As-a-Service Delivery

F5 Threat Campaigns, delivered as a subscription service, integrates with F5 Advanced WAF to consume intelligence on active attack campaigns being monitored by the threat researchers at F5. The F5 Advanced WAF can be configured to automate mitigation for these new and ongoing threats.

Learn more about F5 Advanced WAF.

F5 THREAT CAMPAIGNS PROVIDES VISIBILITY INTO AN ATTACKER'S PRELIMINARY APPROACH, TO HELP SECURITY ADMINISTRATORS PROACTIVELY BLOCK ATTACKS.

THE F5 ADVANCED WAF CAN BE CONFIGURED TO AUTOMATE

MITIGATION FOR THESE NEW

AND ONGOING THREATS.