



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.

Main

Help

About

Statistics

IApps

Wizards

DNS

Local Traffic

Traffic Intelligence

Acceleration

Subscriber Management

Access

Device Management

Shared Objects

Security

Overview

Application Security

Protocol Security

Network Firewall

Network Address Translation

Zones

Packet Filter

Security > Options > Application Security > Threat Campaigns

Attack Signatures

Threat Campaigns

RegExp Validator

Integrated Services

Advanced Configuration

Synchronization

Order by Status ▾ Active First ▾

1 - 100 of 326 Entries | 1 2 ... 4

Threat Campaigns

Oracle WebLogic async Deserialization RCE - asa

Command Execution Reconnaissance

Active

High

CGI Remote Code Execution Reconnaissance - moo

Malware Spreading

Active

High

Oracle WebLogic async Deserialization RCE - Multistix

Vulnerable System Reconnaissance

Active

High

Bash ShellShock in User-Agent - Minimal Headers

Malware Spreading - DDoS

Active

High

Oracle WebLogic WLS Security Component RCE - plus

Malware Spreading - Crypto Currency Miner

Active

High

Bash ShellShock in User-Agent - XSSUCCESS

Malware Spreading - DDoS

Active

High

Bash ShellShock in User-Agent - realignup echo 2014

Command Execution Reconnaissance

Active

High

Oracle WebLogic WLS Security Component RCE - Corona

Malware Spreading - Generic

Active

High

Oracle WebLogic async Deserialization RCE - yaycve

Command Execution Reconnaissance

Active

High

Oracle WebLogic async Deserialization RCE - test2725

Vulnerable System Reconnaissance

Active

High

Bash ShellShock in User-Agent - H0m34b1t

Command Execution Reconnaissance

Active

High

Oracle WebLogic async Deserialization RCE - yayshell

Malware Spreading - Crypto Currency Miner

Active

High

Vulnerability Scanner - sleep+5

Command Execution Reconnaissance

Active

High

Oracle WebLogic async Deserialization RCE - ximcx cn

Vulnerable System Reconnaissance

Active

High

Name

Bash ShellShock in User-Agent - Minimal Headers

Status

Active

Intent

Malware Spreading - DDoS

Risk

High

Attack Type

Other Application Attacks

First Observed

2017-01-06

Description

This campaign aims to identify web servers vulnerable to the ShellShock vulnerability (CVE-2014-6271). The threat actor instructs the server to download and execute a malicious file.

Last Observed

2017-05-30

Target

CGI based webservers vulnerable to shellshock

Last Updated

2019-11-19

Payload Tactics

Download and Execute

Systems

Unix/Linux

Payload Analysis

Attacker instructs the attacked server to download and run DDoS malware that uses the 'wget' bash command for download and perl for execution.

Reference

CVE-2014-6271

Delivered Malware

Type

DDoS

Family

Unknown

Target System

Unix/Linux

Programming Language

Perl

Figure 1: F5 Threat Campaigns Console