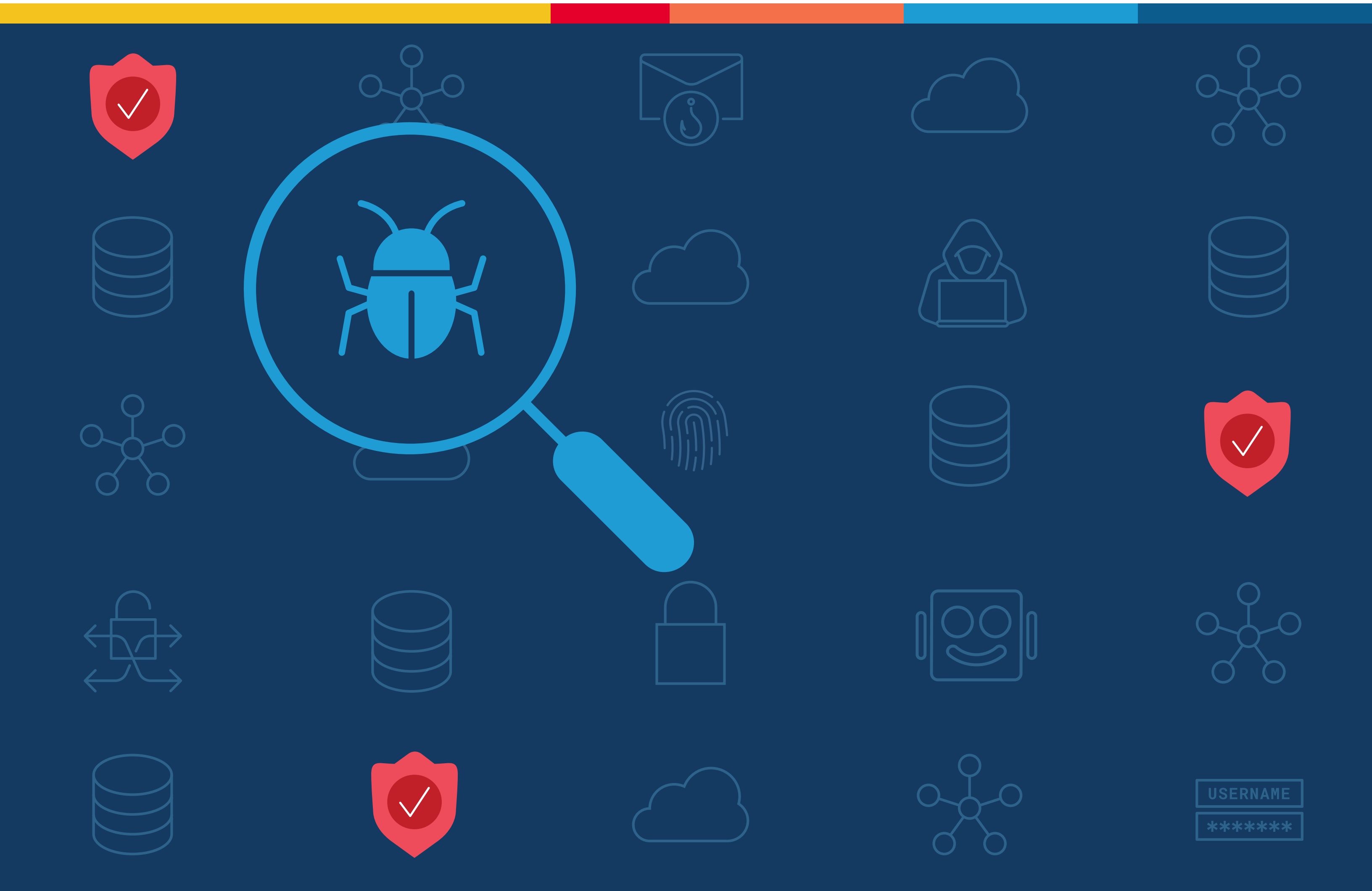
SOLUTION OVERVIEW

Detecting and Mitigating Cyberattack Campaigns

Prevent real-world attacks by detecting and mitigating the risk.



KEY BENEFITS

Mitigate Threats Cost-Effectively
Eliminate the need for internal threat hunting, which can be time-consuming and less effective.

Improve Web Application Security
Proactively block attack campaigns to strengthen web application security.

Simplify Deployment
Ensure fast and simple deployment through as-a-Service delivery.

Utilize Tactical Threat Intelligence
Get real-time, automated threat intelligence to help identify the individual actions of active attack campaigns.

Achieve Near-Zero False Positives
Rely on F5 threat researchers to monitor attack campaigns.

Access Through as-a-Service Delivery
Benefit from the convenience of a subscription service.

Why Cyberattack Campaigns Pose a Threat

Cyber adversaries are intelligent, fast, and increasing in number, posing a constant threat to businesses and security professionals. While standard security tools protect against a wide range of cyberattacks, they often struggle to keep up with skilled threat actors. Among these attacks, web applications remain the primary target.

Enterprise organizations typically rely on a wide array of applications, ranging from 200 to 1,000 (Figure 1), spread across multiple public clouds, private clouds, and data centers. This complex landscape presents a challenge for organizations in terms of ensuring both availability and security for these applications. While many organizations have mature vulnerability management programs in place, often these are simply not enough to defend against the number of vulnerabilities reported—and unreported—over a year. Unfortunately, security operations (SecOps) teams don't have the luxury of downtime.

Application Portfolio Sizes

We asked:
How many applications does your organization have today?

We learned:
Portfolios are trending to encompass from 200 to 1,000 applications, on average.

■ 2017
■ 2022

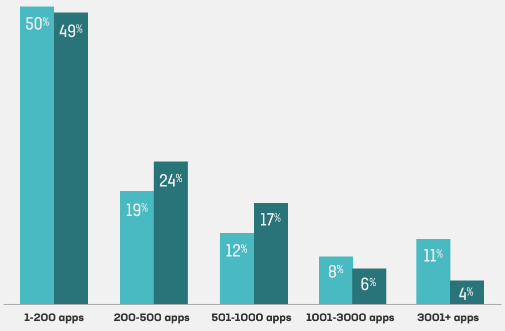


Figure 1: F5 2022 State of Application Strategy Report

Targeted threat campaigns can leverage known and used vulnerabilities to launch exploits and coordinate attacks. These threats can be sophisticated and difficult to detect. This is either because campaigns are designed cleverly to evade standard WAF rules and signatures or because detecting them requires comprehensive and coarse security policies that may increase false positives, overwhelming a security team and risking that attacks will go unnoticed in the deluge of alerts.

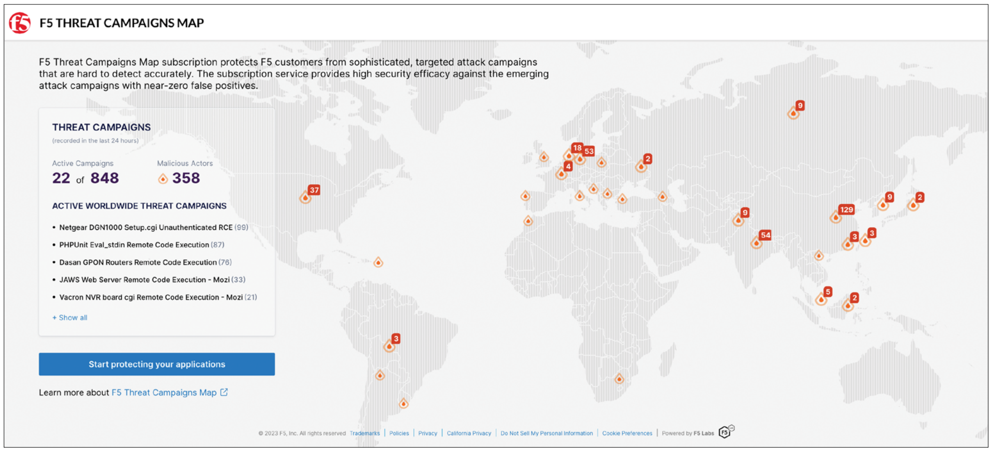
Addressing Sophisticated, Targeted Cyberattack Campaigns

The best way to mitigate the coordinated exploits of cyberattacks on applications and APIs via vulnerable code is by deploying a web application firewall (WAF). But sophisticated attacks can be difficult to detect with baseline WAF security policies and configurations. Therefore, organizations need a WAF with tactical threat intelligence specifically designed to identify and mitigate sophisticated, targeted attacks. Even if organizations are slow in patching a known vulnerability, a WAF with tactical intelligence can protect most critical apps and vital APIs from the attacks and exploits of coordinated threat campaigns.

F5 Threat Campaigns is an add-on threat intelligence service for F5 BIG-IP® Advanced WAF®, and is included in F5 NGINX® App Protect WAF and F5 Distributed Cloud WAF as well. F5 Threat Campaigns provides intelligence with contextual information about the nature and purpose of active threat campaigns. A standard WAF may detect a combination of identifiers in a web application form, but without threat intelligence, it cannot specifically search for certain payloads or unique identifiers. These highly specific identifiers surpass traditional signatures, leading to a significant reduction in false positives.

Organizations today require live and actionable threat intelligence that can enhance the efficacy of existing security controls, including WAFs. F5 Threat Campaigns achieves this with controls that automatically detect and block active threat campaigns, bolstering security measures.

THE F5 THREAT CAMPAIGNS SERVICE USES METADATA AND MULTI-VECTOR THREAT INTELLIGENCE TO HELP IDENTIFY THE INDIVIDUAL ACTIONS OF AN ACTIVE ATTACK CAMPAIGN. F5 THREAT CAMPAIGNS HELPS BIG-IP ADVANCED WAF IDENTIFY AN ATTACK INDICATOR AS PART OF A THREAT CAMPAIGN SO THAT MITIGATION CAN BE PERFORMED.



F5 THREAT CAMPAIGNS MAP

F5 Threat Campaigns Map subscription protects F5 customers from sophisticated, targeted attack campaigns that are hard to detect accurately. The subscription service provides high security efficacy against the emerging attack campaigns with near-zero false positives.

THREAT CAMPAIGNS

(recorded in the last 24 hours)

Active Campaigns: 22 of 848

Malicious Actors: 358

ACTIVE WORLDWIDE THREAT CAMPAIGNS

- Netgear DGN1000 Setup.cgi Unauthenticated RCE (99)
- PHPUnit Eval_stdin Remote Code Execution (87)
- Dasan GPON Routers Remote Code Execution (76)
- JAWS Web Server Remote Code Execution - Mozi (33)
- Vacron NVR board cgi Remote Code Execution - Mozi (21)

Learn more about F5 Threat Campaigns Map

© 2023 F5, Inc. All rights reserved

+ Show all
Start protecting your applications
Trademarks | Policies | Privacy | California Privacy | Do Not Sell My Personal Information | Cookie Preferences | Powered by F5 Labs
37
3
18
53
4
2
9
9
2
129
9
54
3
3
5
2

Figure 2: F5 Threat Campaigns Map

FULLY VETTED ATTACK SIGNATURES FROM F5 THREAT RESEARCHERS ENABLE SECURITY ADMINISTRATORS TO ACTIVATE MITIGATIONS WITH CONFIDENCE. THIS REDUCES EXPOSURE AND HELPS BLOCK ATTACKS BEFORE ANY DAMAGE IS DONE.

The F5 Threat Campaigns service leverages a team of security experts who are dedicated to finding, analyzing, and dissecting real ongoing attacks in the wild. With an arsenal of resources that include a worldwide network of honeypots and more, the service is automatically updated with the latest campaign information released by F5. This ensures enterprises receive rapid and preemptive protection against current attack campaigns before they can have an effect. The insight collected helps security operators gain a comprehensive understanding of potential threats to their apps or infrastructure, including attack methods, perpetrators, and risk assessment.

To enhance visibility into cyberattack campaigns, the F5 Threat Campaigns world map is available on f5.com for anyone to see and use. This interactive map can be viewed at scale, delivering details into ongoing threat campaigns.

Conclusion

F5 Threat Campaigns is easy to use and requires only a simple activation with no need for additional configuration. The F5 Threat Campaigns service provides an additional layer of protection against real-world attack campaigns without false positives. As an add-on to F5 BIG-IP Advanced WAF (and included with F5 NGINX App Protect WAF and F5 Distributed Cloud WAF), it enables organizations to cover any security gaps that attackers might otherwise get through.

To learn more, visit f5.com/products/security/advanced-waf or contact an F5 representative.