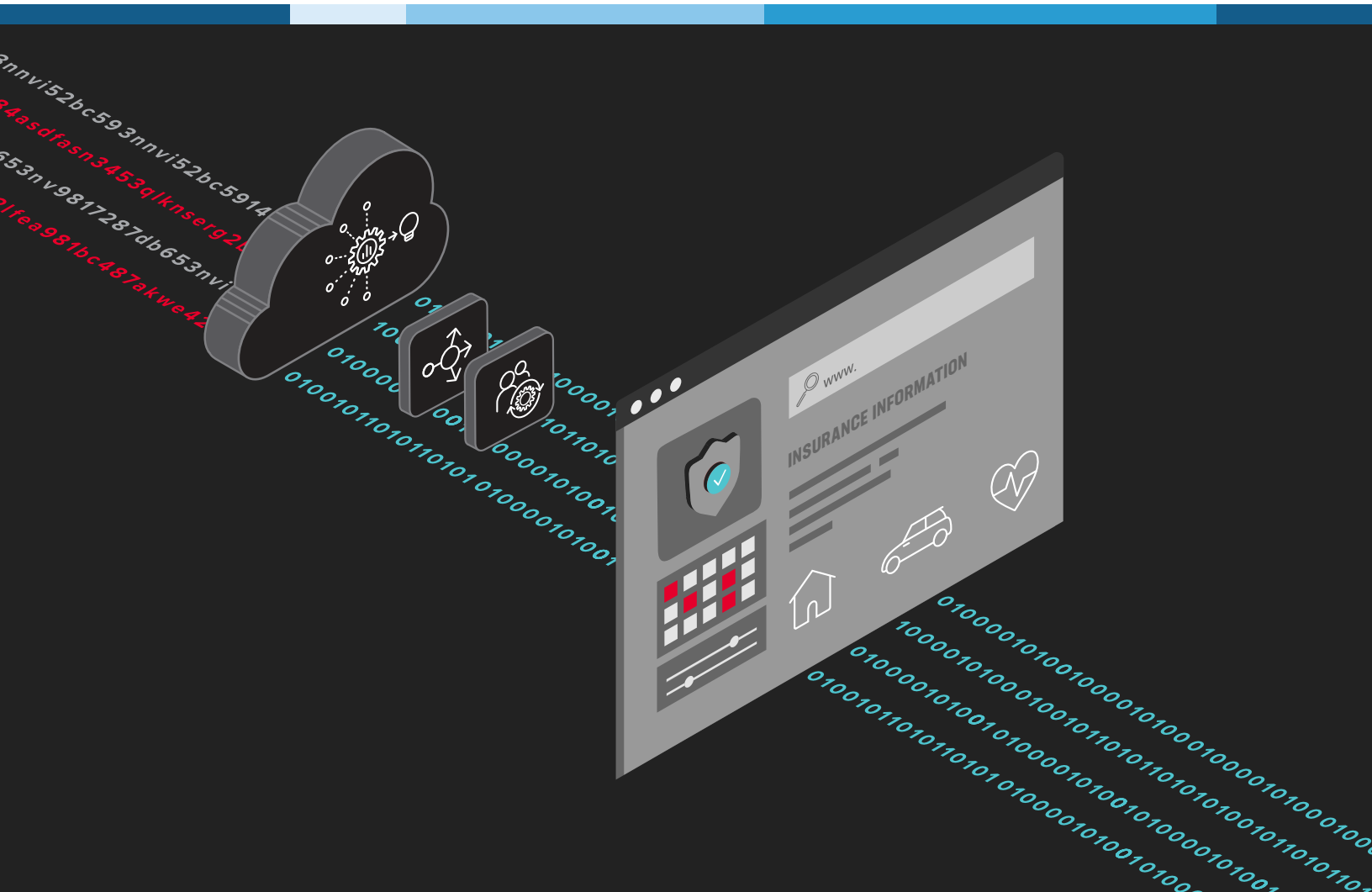
CASE STUDY

# Insurer Defeats Application Layer DDoS



NETWORK DDOS SOLUTIONS ARE EFFECTIVE AGAINST HIGH-VOLUME ATTACKS AT LOWER LAYERS OF THE APPLICATION STACK.

**Website taken down by application layer distributed denial-of-service.** A major insurer with over 20 million members relies on its website to deliver information on providers, benefits, and plans. Because the services offered by the insurer are complex and highly personalized, search is a popular and essential website component.

Recently, an attacker flooded the search function with queries for multiple days. The resulting application layer distributed denial-of-service (DDoS) caused the search function to fail and prevented members from using it. Other sections of the website also failed since web server resources are shared across website elements.

Cybercriminals often use DDoS attacks to extort targets or to mask other concurrent attacks. In this case, the attacker did not contact the company. However, F5 researchers observed low-level automated scraping activities occurring at the same time as the DDoS attack, indicating the DDoS attack may have been a diversionary tactic.

## Attack Target

The insurer's system architecture includes load balancers, DDoS defenses, web servers, application servers, and databases in a typical web services architecture. The adversary used a simple command line tool to exercise the search function at a rate sufficient to cause it to fail.

## Attack Methods

The attack, which appeared to come from thousands of unique IP addresses, targeted the application server with search queries that arrived at a rate high enough to overload the application server. But because the searches appeared to come from thousands of hosts, each host's query rate was low enough to evade network-layer DDoS detection.

## Attack Impact

Attack traffic volumes caused the search function to time out, at which point legitimate users could no longer use the search function. Other website components also failed as the attack consumed shared backend resources. At various points during the attack, the entire website was unavailable to members.

The diagram below (representative of the traffic recorded by the F5® Distributed Cloud Protection Manager) shows attack traffic directed at the insurer's website. Red indicates traffic reaching the origin servers before F5® Distributed Cloud Bot Defense was activated. Grey indicates traffic deflected by the service that did not reach the origin servers. The chart illustrates a typical app layer DDoS attack pattern that continued even after Distributed Cloud Bot Defense mitigated its damaging effects.

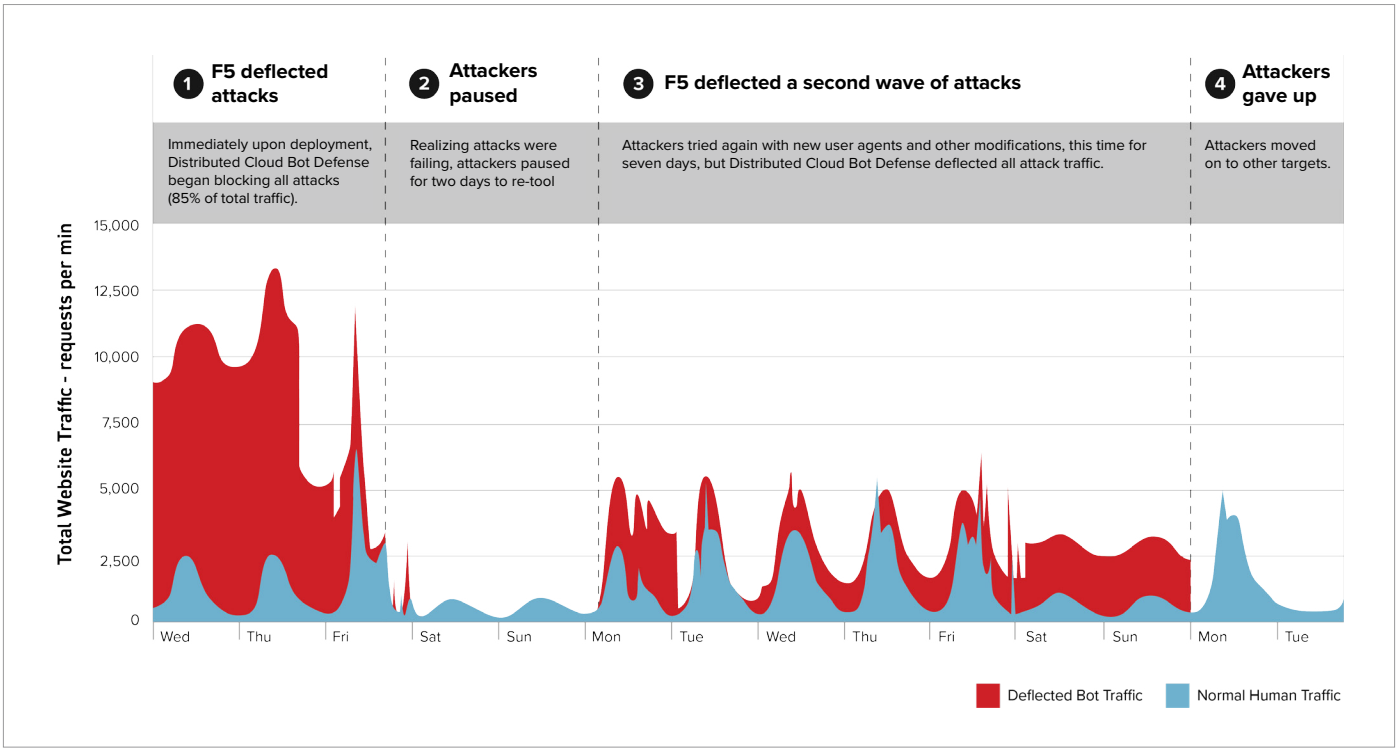



**Figure 1:** Attempted application layer attacks against major insurer

## Failure of Existing DDoS Mitigation Solutions

The insurer protects its website with an industry-leading DDoS mitigation solution. Although the solution worked as intended during the attack, it did not stop the app layer DDoS.

Network DDoS solutions are effective against high-volume attacks at lower layers of the application stack. They can also protect against certain attacks that rely on malformed traffic or connections that deviate from protocol norms. However, they are ineffective against attacks designed to look exactly like legitimate traffic.

The attacker's search queries were well-formed at layers three and four, conformed to all relevant protocols, and interacted with the website's search function as a human user would. As a consequence, the attack evaded the enterprise's existing DDoS protections.

## Attack Mitigation

Distributed Cloud Bot Defense, which recognizes automated traffic at any level and from any source, deflected all automated requests to the search function. The attacker continued to direct traffic at the site, but since this traffic was deflected and no longer reached the origin servers, site operations returned to normal.

## Conclusion

Existing network DDoS defenses are ineffective against automated adversaries masquerading as human visitors. This application layer DDoS attack is one of many types of automated attacks. New defensive approaches, focused on deflecting automation, reliably stop these website attacks.

**To learn more, contact your F5 representative, or visit f5.com.**