radware

THE BIG 3 CYBER-ATTACKS TARGETING PROXY SERVERS

Today, many organizations are now realizing that DDoS defense is critical to maintaining an exceptional customer experience. Why? Because nothing diminishes load times or impacts the end user's experience more than a cyber-attack.

As a facilitator of access to content and networks, proxy servers have become a focal point for those seeking to cause grief to organizations via cyber-attacks due to the fallout a successful assault can have. Based on research from Radware's *2017-2018 Global Application & Network Security Report*, here are three types of attacks that organizations can expect to target their proxies.

Attacking the CDN Proxy

New vulnerabilities in content delivery networks (CDNs) have left many wondering if the networks themselves are vulnerable to a wide variety of cyber-attacks. Here are five cyber "blind spots" that will be attacked in 2018—and how to mitigate the risks:

1. **Increase in dynamic content attacks.** Attackers have discovered that treatment of dynamic content requests is a major blind spot in CDNs. Since the dynamic content is not stored on CDN servers, all requests for dynamic content are sent to the origin's servers. Attackers are taking advantage of this behavior to generate attack traffic that contains random parameters in HTTP GET requests. CDN servers immediately redirect this attack traffic to the origin—expecting the origin's server to handle the requests. However, in many cases the origin's servers do not have the capacity to handle all those attack requests and fail to provide online services to legitimate users. That creates a denial-of-service situation. Many CDNs can limit the number of dynamic requests to the server under attack. This means they cannot distinguish attackers from legitimate users and the rate limit will result in legitimate users being blocked.

2. **SSL-based DDoS attacks.** SSL-based DDoS attacks leverage this cryptographic protocol to target the victim's online services. These attacks are easy to launch and difficult to mitigate, making them a hacker favorite. To detect and mitigate SSL-based attacks, CDN servers must first decrypt the traffic using the

customer's SSL keys. If the customer is not willing to provide the SSL keys to its CDN provider, then the SSL attack traffic is redirected to the customer's origin. That leaves the customer vulnerable to SSL attacks. Such attacks that hit the customer's origin can easily take down the secured online service.

During DDoS attacks, when web application firewall (WAF) technologies are involved, CDNs also have a significant scalability weakness in terms of how many SSL connections per second they can handle. Serious latency issues can arise. PCI and other security compliance issues are also a problem because they limit the data centers that can be used to service the customer. This can increase latency and cause audit issues.

Keep in mind these problems are exacerbated with the massive migration from RSA algorithms to ECC and DH-based algorithms.

3. **Attacks on non-CDN services.** CDN services are often offered only for HTTP/S and DNS applications. Other online services and applications in the customer's data center, such as VoIP, mail, FTP and proprietary protocols, are not served by the CDN. Therefore, traffic to those applications is not routed through the CDN. Attackers are taking advantage of this blind spot and launching attacks on such applications. They are hitting the customer's origin with large-scale attacks that threaten to saturate the Internet pipe of the customer. All the applications at the customer's origin become unavailable to legitimate users once the Internet pipe is saturated, including ones served by the CDN.

4. **Direct IP attacks.** Even applications that are served by a CDN can be attacked once attackers launch a direct hit on the IP address of the web servers at the customer's data center. These can be network-based flood attacks such as UDP floods or ICMP floods that will not be routed through CDN services and will directly hit the customer's servers. Such volumetric network attacks can saturate the Internet pipe. That results in degradation to application and online services, including those served by the CDN.

5. **Web application attacks.** CDN protection from threats is limited and exposes web applications of the customer to data leakage and theft and other threats that are common with web applications. Most CDN-based WAF capabilities are minimal, covering only a basic set of predefined signatures and rules. Many of the CDN-based WAFs do not learn HTTP parameters and do not create positive security rules. Therefore, these WAFs cannot protect from zero-day attacks and known threats. For companies that do provide tuning for the web applications in their WAF, the cost is extremely high to get this level of protection. In addition to the significant blind spots identified, most CDN security services are simply not responsive enough, resulting in security configurations that take hours to manually deploy. Security services are using technologies (e.g., rate limit) that have proven inefficient in recent years and lack capabilities such as network behavioral analysis, challenge-response mechanisms and more.

Finding the Watering Holes

Waterhole attack vectors are all about finding the weakest link in a technology chain. These attacks target often forgotten, overlooked or not intellectually attended to automated processes. They can lead to unbelievable devastation. What follows is a list of sample watering hole targets:

- App stores
- Domain name services
- Web analytics platforms
- Open source code commonly used by vendors
- Security update services
- Public code repositories to build websites
- Identity and access single sign-on platforms
- Third-party vendors that participate in the website

The DDoS attack on Dyn in 2016 has been the best example of the water-holing vector technique to date. However, we believe this vector will gain momentum heading into 2018 as automation begins to pervade every aspect of our life.

Attacking from the Side

In many ways side channels are the most obscure and obfuscated attack vectors. This technique attacks the integrity of a company's site through a variety of tactics:

- DDoS the company's analytics provider
- Brute-force attack against all users or against all of the site's third-party companies
- Port the admin's phone and steal login information
- Massive load on "page dotting"
- Large botnets to "learn" ins and outs of a site

DOWNLOAD THE *2017-2018 GLOBAL APPLICATION & NETWORK SECURITY REPORT* TO LEARN MORE

LEARN MORE AT DDOS WARRIORS

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.