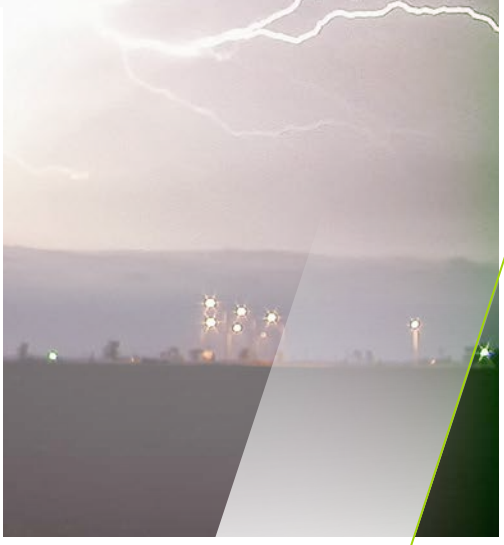
WEB SERVICE ENCRYPTION: ESSENTIAL, BUT INSUFFICIENT



Online services like banking and e-commerce can only succeed if users trust that their transactions and sensitive, personal data are truly secure.

Encryption is what makes those services possible. It only stands to reason, however, that encrypted services are among the prime targets of DDoS attacks. After all, what could be more attractive to an attacker than those assets that are the most difficult to attain? Think of Goldfinger's obsession with breaking into Fort Knox. The very fact that something is encased in a powerful protective shield denotes its value.

To add insult to injury, bad actors often use encryption themselves to infiltrate encrypted traffic, making their attacks extremely difficult to detect.

SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are the most common cryptographic protocols used to secure money transfers, online purchases and other financial transactions, as well as email and remote access. Increasingly, social media platforms such as Facebook and Twitter are also using SSL to protect user privacy. With more and more services dependent on SSL encryption, we are seeing more DDoS attacks targeting encrypted services. In our 12th Annual Worldwide Infrastructure Security Report, 52% of security professionals surveyed said they had experienced attacks on secure web services (HTTPS) in 2016, up from 47% the previous year.

ARBOR® NETWORKS

The Security Division of NETSCOUT

A VARIETY OF ATTACK METHODS

In general, attacks on SSL encryption simply try to overwhelm the capacity of SSL servers to authenticate communication attempts. Our annual survey found these attacks tend to fall into four categories:

1. Attacks that target the SSL or TLS negotiation, more commonly known as the "handshake."

In one common example, the attacker starts the handshake process, then attempts to renegotiate the encryption key multiple times until server resources are exhausted, making services unavailable to legitimate users.

2. Protocol or connection attacks against the SSL or TLS port.

Typically, the attacker bombards the SSL server with garbage data, overloading the server's processing capacity.

3. Volumetric attacks that simply flood traffic at service ports.

An entire data center can be cut off from the outside world through very high volume traffic floods that saturate the incoming links from the internet.

4. Application-layer attacks that target the underlying service directly over fully negotiated SSL or TLS connections.

HTTPS services are among the most common targets of sophisticated, stealthy application-layer attacks. These "low and slow" attacks can be very effective, with as few as one attacking machine generating traffic at a low rate.

This variety of methods underscores the need for security measures that cover the spectrum of today's attack types, from brute-force floods to the more precise and insidious application-level attacks that slither through defenses and bide their time before striking.

WHAT'S HIDING IN YOUR ENCRYPTED TRAFFIC?

The challenge of attacks on SSL is compounded when the attacks themselves are encrypted. SSL encryption works by recoding user data so that unauthorized users or devices cannot read it as it moves between servers. This is what ensures the security and integrity of online business transactions and confidential communications. It also poses risks, however. Network security devices such as firewalls and IPSs do not normally inspect encrypted traffic. A high volume of Internet traffic simply moves onto the network without being seen. What better place for malware or botnets to hide, waiting to unleash devastating attacks? This enables hackers to take advantage of SSL and leverage malicious browser-based tools to direct attacks to HTTPS services, essentially hidden from detection.

The most effective way to inspect SSL traffic is to decrypt it — which, of course, puts legitimate services at the risk of being compromised or, at a minimum, disrupted. This calls for a solution that can inspect encrypted traffic securely and attest to its authenticity without slowing the traffic queue or exposing authorized traffic to intruders.

Without question, encryption is an essential, fundamental component of online security. But the job of securing critical services does not end with encryption, as malicious actors will devise ever more clever methods to try and break it. Robust, comprehensive capabilities encompassing threat intelligence, detection and mitigation are needed to ensure the integrity and unimpeded availability of secure services.

• • ○

Learn More about Arbor DDoS protection solutions.

ARBOR NETWORKS
The Security Division of NETSCOUT

arbornetworks.com

AI/ENCRYPTION/EN/0617-LETTER

Corporate Headquarters
76 Blanchard Road
Burlington, MA 01803 USA
Toll Free USA: +1 866 212 7267
T: +1 781 362 4300

North American Sales
Toll Free: +1 855 773 9200

Europe
T: +44 207 127 8147

Asia Pacific
T: +65 6664 3140

Latin & Central America
T: +52 55 4624 4842