radware

FRIEND TURNED ENEMY:
SSL-Based Cyber-Attacks

SSL-based cyber-attacks are the posterchild for the idiom “a wolf in sheep’s clothing.” A cryptographic protocol turned enemy, SSL improves privacy and integrity, but can also create a blind spot in corporate defenses when hackers leverage it to mask cyber-attacks and malware.

SSL-based cyber-attacks are growing in popularity, and for good reason: over half of all Internet traffic today is encrypted and that figure is only expected to rise, according to a study by the Georgia Institute of Technology.[1] Not surprisingly, the security challenges posed by encrypted traffic are poised to get worse, as Gartner has noted: “The continued growth of SSL/TLS traffic will be amplified by the adoption of HTTP 2.0. It creates a new attack surface for malware infection, data exfiltration and call back communication.”[2]

Research by Netcraft, a leading provider of internet security research and services, further vindicates this. Use of SSL by the top one million websites has increased by more than 48% over the past two years, according to Netcraft.[3] As the percentage of inbound and outbound traffic increases, so does the effectiveness of encryption as a smokescreen for hackers.

[1] http://www.iisp.gatech.edu/working-paper-online-privacy-and-isps
[2] “Security Leaders Must Address Threats From Rising SSL Traffic” Gartner Research, January 8, 2015
[3] https://news.netcraft.com/archives/2014/01/03/january-2014-web-server-survey.html

More Frequent, More Virulent

DDoS and advanced Web application attacks continue to plague businesses as they transition to online operations. With both types of attacks, those leveraging encrypted traffic as an attack vector are on the rise. This increase is further challenging many incumbent solutions for detecting and mitigating cyber threats. Most do not actually inspect SSL traffic, as it requires decrypting the encrypted traffic. According to Radware's *2016-2017 Global Application & Network Security Report*, 39% of respondents confirmed they have been targeted by SSL or encrypted vectors—a 10% increase compared to the prior year. Only one in four businesses reported feeling protected against SSL flood attacks.

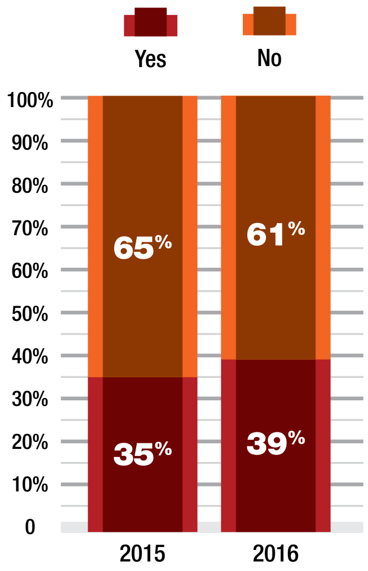

Figure 1: Have you experienced an SSL-based attack this year?

SSL-based attacks take many forms. Among them:

- **Encrypted SSL floods**. These attacks are similar in nature to standard, non-encrypted SYN flood attacks in that they seek to exhaust the resources in place to complete the SYN-ACK handshake. Encrypted SSL floods complicate the challenge by encrypting traffic and forcing resource use of SSL handshake resources.
- **SSL renegotiation**. These attacks work by initiating a regular SSL handshake and then immediately requesting the renegotiation of the encryption key. The tool continuously repeats this renegotiation request until all server resources have been exhausted.
- **HTTPS floods**. These attacks generate floods of encrypted HTTP traffic, often as part of multi-vector attack campaigns. Compounding the impact of "normal" HTTPS floods, encrypted HTTP attacks add the burden of encryption and decryption mechanisms.
- **Encrypted Web application attacks**. Multi-vector campaigns also increasingly leverage non-DoS, Web application logic attacks. By encrypting the traffic that masks these attacks, they often pass undetected through both DDoS and Web application protections.

Complicating Detection, Stressing Mitigation

Identifying attack traffic within encrypted traffic flows is akin to finding a black cat in a black room – blindfolded. Most cyber-attack solutions struggle to identify potentially malicious traffic from encrypted traffic sources and to isolate that traffic for further analysis (and potential mitigation).

SSL attacks offer attackers another advantage: the ability to put significant computing stress on the network and application infrastructures they target. The process of decrypting and re-encrypting SSL traffic increases the requirements of processing the traffic—in many cases beyond the functional performance of devices used for attack mitigation. Most devices are inline, stateful and unable to handle SSL encrypted attacks, making them vulnerable to SSL floods. Fewer still can be deployed out of path—a necessity for providing protection while limiting the impact on legitimate users.

Many solutions that can do some level of decryption tend to rely on limiting the rate of request, which results in legitimate traffic being dropped and effectively completes the attack. Finally, many solutions require the customer to share actual server certificates. That requirement complicates implementation and certificate management and forces customers to share private keys for protection in the cloud.

Visibility into encrypted traffic isn't the only challenge related to SSL/TLS. When surveyed about the ability of existing security solutions to decrypt, inspect and re-encrypt traffic, most are similarly working blind. Specifically, 75% of industry practitioners doubt their security solutions provide full encrypted attack protection.[4] According to Gartner, less than 20% of organizations decrypt inbound traffic at the network perimeter; less than half inspect encrypted traffic leaving the network. Further, more than 90% with public websites decrypt inbound Web traffic (often through a Web Application Firewall); however, many of the encrypted attack vectors are doing their damage before traffic gets this deep into the network or application infrastructure.[5]

Cloud Complexity

Traditional data center environments aren't the only place where encrypted traffic creates challenges of visibility and security. As volumetric attacks that saturate Internet pipes or overwhelm data center resources continue to grow, many are turning to cloud-based attack mitigation solutions.

Cloud-based services vary in capabilities but generally allow an attack target to rely on purpose-built resources outside of its network to scrub traffic—that is, removing attack traffic and returning what's legitimate. However, rerouting encrypted traffic to a third party creates a new set of challenges related to private key management and coordination. On one hand, decryption by the cloud DDoS provider is necessary to provide protection from encrypted threats (some providers simply pass encrypted traffic along to the customer). On the other, enabling a third party to decrypt traffic by sharing private keys sometimes means the customer must coordinate any certificate management changes with the cloud DDoS provider. It also means potential loss of end-user data privacy and confidentiality.

Given these challenges, organizations looking to handle volumetric attacks within encrypted traffic flows need to identify vendors with the ability to support wildcard certificates that do not need to match the server certificates. This does two things. First, it eliminates the need to share private keys with the cloud DDoS vendor, which will be against most organizations' security policies. Second, it dramatically reduces the administrative burden for coordinating changes and updates to the server certificates and also eliminates the additional risk of exposing server certificates to the network perimeter.

Encrypted Attack Protection: "Keys" To Success

SSL is both a blessing and a curse: blessing because it solves the privacy problem and secures the communication of sensitive information, curse because it creates new blind spots and vulnerabilities into an enterprise IT infrastructure. To address SSL challenges, implement a strategy that considers the following:

- **Visibility**. Aim to decrypt and re-encrypt SSL sessions to enable security inspection of both clear and encrypted traffic while maintaining privacy of content en-route.

- **Service chaining**. Any SSL inspection solution needs to be able to selectively forward traffic to one or more security solutions.

- **Flexible traffic inspection**. How can a solution support efficiency while inspecting encrypted traffic that's masquerading as clear traffic? It must dynamically define filters that intercept and open traffic for inspection—even if it flows through non-standard TCP ports (such as HTTPS port 443).

- **Security**. To avoid turning the SSL traffic inspection solution into a target itself, a solution must not perform like a proxy or have its own IP address.

[4] "Security Leaders Must Address Threats From Rising SSL Traffic" Gartner Research, January 8, 2015
[5] "Security Leaders Must Address Threats From Rising SSL Traffic" Gartner Research, January 8, 2015

- **Scalability**. As the amount of traffic/SSL traffic continuously grows, SSL traffic inspection solutions must seamlessly scale to reduce or eliminate the need for forklift upgrades.

- **High availability**. To avoid downtime due to outages in the security solution, the SSL traffic inspection solution should always ensure traffic is forwarded to the fastest-responding available security servers, automatically bypassing out-of-service servers.

Download the 2016-2017 Global Application & Network Security Report to learn more.

www.radware.com/ert-report-2016

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.