Why Inspecting Encrypted Traffic Is A Must

By **Prakash Sinha** - June 23, 2021

What You Don't See Can Harm You

As we emerge from the COVID-19 lockdown, we see a rash of malicious ransomware attacks trying to shut down many sectors of the economy – Colonial Pipeline, J.B.S, C.N.A Financial – for profit. Why? Because crime pays. Even more threatening are the ones we don't hear about – those from the users inside of the organization.

The same encryption mechanism using a public key to secure our communication – transport level security (TLS) a.k.a Secure Sockets Layer (SSL) can be used by malicious users or programs to access sensitive information.

Initially, botnets were used for DDoS attacks. Now, some of these command-and-control malware use the resources of infected machines for ransom and profit (ransomware and crypto-mining), significantly affecting an enterprise's performance and increasing operating costs as well as wear on the commandeered machines. These attacks can also be a conduit for additional future malware delivery.

Most malware threatens the availability, integrity, and security of a network.

As we have seen recently, ransomware attacks can often result in information theft and hijacking in addition to disrupting an organization's mission-critical operations.

When the malware activates, it may open an encrypted session to an external server. The only information the malware requires to secure the communication with the external server is the external server's public key. Since the sending organization (of the user or malware program) does not have the private key to this encrypted communication, it cannot decipher this session and thus is blind to any information that is being sent outside.

As the usage of encrypted traffic increases, this challenge will become even more pervasive. We are already beginning to see such cyber-attacks on many organizations for financial gain and access to valuable confidential data.

Many traffic inspection solutions such as data leakage prevention (DLP), intrusion prevention systems (IPS), and firewalls may not have the ability to decrypt ***outbound*** encrypted traffic, and therefore are blind to cyber threats initiated from within the organization to external servers. Furthermore, even when they can decrypt, the ability comes with a steep cost-performance impact and expense, making these systems less scalable and thus uneconomical.

Inspection and Visibility – The Necessary Disinfectant

The key to protecting against such attacks is to inspect SSL traffic. So, how does the SSL traffic inspection work?

The SSL inspection systems take advantage of the fact that the security is between two endpoints and not end-to-end. Sometimes referred to as ***legitimate*** man-in-the-middle (MiTM), the SSL inspection solution intercepts and decrypts SSL sessions destined to and from the enterprise. These SSL inspection solutions appear as the intended external server for internal users or programs initiating secure communication to external servers. For the recipient servers, the SSL inspection system appears as the initiating user or malware program.

For ease of deployment, SSL inspection solutions may provide both transparent inspection without requiring the need to re-engineer the network or as explicit proxy that require all users to pass through a predefined SSL proxy configured via a user's browser.

Then, the decrypted traffic is steered to any content inspection solution such as firewalls, anti-malware, or data leakage protection systems already deployed in the enterprise to check against an organization's security policies. Sessions that pass the security inspection are then re-encrypted by the SSL inspection solution and forwarded to their destination server.

For efficiency, some traffic may be untouched if a particular site is trusted by the enterprise or is related to employee privacy (online banking, healthcare). For productivity reasons, other traffic may be blocked, typically online gaming or known malware servers.

Since SSL decryption and re-encryption are computationally intensive operations and may impact latency, use best practices such as hardware acceleration if you have many users and encrypted traffic. Be selective with decryption by using filtering and whitelists to bypass decryption for sites that you trust, and choose solutions that reduce the number of devices you require to scale and are cost-effective.

Decrypting, inspecting, and gaining visibility to network traffic using SSL inspection solution helps identify red flags that may indicate malware. Furthermore, adopting the best practices: least privilege access, multi-factor authentication while stopping web malware injections using web application firewalls, and protecting network perimeter against denial of service while educating the workforce on cybersecurity practices help reduce an enterprise's exposure to these malware threats.

[You may also like: How to Respond to a DDoS Ransom Note]

Prakash Sinha

Prakash Sinha is a technology executive and evangelist for Radware and brings over 29 years of experience in strategy, product management, product marketing and engineering. Prakash has been a part of executive teams of four software and network infrastructure startups, all of which were acquired. Before Radware, Prakash led product management for Citrix NetScaler and was instrumental in introducing multi-tenant and virtualized NetScaler product lines to market. Prior to Citrix, Prakash held leadership positions in architecture, engineering, and product management at leading technology companies such as Cisco, Informatica, and Tandem Computers. Prakash holds a Bachelor in Electrical Engineering from BIT, Mesra and an MBA from Haas School of Business at UC Berkeley.