SONICWALL®

UNDERSTANDING ENCRYPTED THREATS

How cyber criminals hide attacks on your network using SSL/TLS

Abstract

Encryption technology such as SSL/TLS and HTTPS offers protection against hacking, and its use is growing exponentially. But cyber-criminals have learned to leverage encryption as an effective method to hide malware, ransomware, spear-phishing, zero-day, data exfiltration, rogue sites and other attacks. Fortunately, advanced network security with deep packet inspection of SSL/TLS and HTTPS traffic is now available to protect against encrypted threats.

Types of encrypted threats

Encryption offers protection for legitimate traffic, as well as a means for cyber attacks to go undetected. In simple terms, SSL (Secure Sockets Layer) can create an encrypted tunnel for securing data over a VPN. TLS (Transport Layer Security) is an updated, more secure, version of SSL. HTTPS (Hyper Text Transfer Protocol Secure) appears in the URL when a website is secured by an SSL certificate.

There are a number of categories of encrypted threats. One category includes threats such as certificate vulnerabilities. In this case, when you are communicating with a site, you may see an alert in your browser or an application saying the connection is determined to be insecure or untrusted. In these situations, the certification has not passed muster. The Certificate Authority may be unreachable or the certificate is invalid. Or the encryption is less than desirable, whether it be an older form of SSL (which has all been depreciated at this point), a lower form of TLS, or signatures and hashes not matching up with what they should be using today's encryption standards.

Another category of encrypted threat includes malware that actually embeds all of its communications inside an encrypted tunnel so that it can circumvent your network's security. Examples of applications that deliberately obfuscate their traffic and communications include Psiphon, Tor and Ultrasurf.

And then there are the actual breaches of encrypted traffic, malware that steals credentials, such as DROWN, Heartbleed, PODDLE, and FREAK. These are exploits that take advantage of the encryption itself in order to play man-in-the-middle and intercept your emails, credentials, private information, online transaction data, etc. Once this type of attack compromises your network, it can use it against you later on, or it embeds the threat inside the communications themselves, sending you to third-party websites or injecting malicious applications into your browser connections.

The history of encrypted threats

To understand what it actually takes to secure against these threats, it helps to understand the history. The legacy firewall security model from the 1990s and early 2000s is Stateful Packet Inspection (SPI) technology. In fact, there are still millions of SPI-only firewalls still on the internet today.

SPI is analogous to a traffic officer who can stop or allow traffic through at an intersection. The officer can only see external information on the vehicles, such as make and model, license plate and the direction the vehicles are moving, but not anything hidden in the back seat, under the hood or in the trunk of the vehicles. So if there is anything malicious hidden in those places, the officer cannot see it.

> The internet is rapidly moving towards a completely encrypted model.

In contrast, Deep Packet Inspection (DPI), which forms the foundation for next-generation firewalls, allows firewalls to inspect at Layer 7. This is as if our traffic officer obtained x-ray vision to see those hidden places in the vehicles, and then decide which traffic can be allowed through the intersection or not.

However, using this analogy, the officer's x-ray vision still cannot see through lead (which in this case, is HTTPS). In order to overcome this limitation, DPI must include the ability to inspect encrypted SSL traffic (DPI-SSL).

The explosive growth of encrypted HTTPS traffic

Whether it's due to the "Snowden effect," the NSA spying scandal, or simply best efforts to safeguard online privacy from would-be attackers and thieves, a significant amount of internet traffic today is now encrypted via HTTPS.

An HTTPS connection is essentially a secure or private connection from the initiating application (usually a browser) all the way through the network and internet to the destination server or site. These HTTPS connections include webcasts, online searches, cloud-based productivity applications, web-based email, etc. HTTPS is basically a VPN. It is an encrypted web connection from your browser all the way to the destination. Because it is a VPN, you cannot see inside of it. You cannot inspect traffic traversing the HTTPS or determine whether it is harmful malware coming in, or sensitive data leaking out of your network.

The internet is rapidly moving towards a completely encrypted model. There are now major initiatives to "encrypt everything," and even leading search engines have altered their search algorithms to prioritize HTTPS sites in their search results. For example, one online retailer may have tens of thousands more clicks per month than another, but if they are not using HTTPS on their landing page, the search results will place them below the lower-performing competitor that uses HTTPS on their landing page.

Over half of web applications are now over HTTPS. Leading applications such as Office 365, YouTube, Amazon, SAP, Salesforce, Skype, Dropbox, Twitter and Gmail all use encryption. Leading analysts predict that by next year 65 percent of the world's internet traffic will be encrypted. To put that in perspective, if you have a 100 Mbps internet connection, about 65 Mpbs of that traffic would not be inspected. Over the course of an hour, that's roughly 4-7 DVDs of data being transferred without inspection. In some networks, the total amount of confidential personal and intellectual property data may be less than that. Consider the impact of not being able to see that much data coming in or out of your network.

And that's only typical internet traffic. The average implementation of HTTPS is 60-80 percent depending upon industry. For example, if you are finance, legal or healthcare industries, most of your sites are already encrypted.

Criminal use of encryption

While encrypted traffic has increased security in daily communications, cyber criminals are taking advantage of the privacy of HTTPS to hide their attacks. They have learned to manipulate encryption to circumvent most legacy firewall solutions. As a result, most HTTPS traffic today is not inspected, and even firewalls purchased recently may not be capable of inspecting the volume of today's encrypted traffic. With the majority of your traffic invisible to your firewall, it's not a matter of if or even when. You're network has likely already been compromised.

Headline breaches at Yahoo, the IRS and Ashley Madison all involved encryption. In one case, more than a billion email accounts that were compromised was a result a single encrypted spearfishing email to one single employee.[1] Likewise, the OPM breach (where more than 20 million individuals had their top-secret clearance information leaked online) originated in a single personal email download that was not inspected and contained malware.[2] Encrypted traffic might contain malware, accidentally or intentionally leaked confidential data, or a spear-phishing attack against the CFO to send a wire transfer payment. The following are just a few examples of threats hidden in encrypted traffic.

Encrypted email-borne malware

How do you stop a user from clicking on an email attachment that unleashes malware in your network? In the case of malware such as Cryptolocker, it contains a malicious payload downloaded inside webmail or other encrypted communications. If it is

[1] https://www.wsj.com/articles/yahoo-discloses-new-breach-of-1-billion-user-accounts-1481753131
[2] https://www.wsj.com/articles/opm-breach-exposed-19-7-million-background-clearance-forms-1436469626

encrypted, you can't inspect it, you can't control it and you can't block it. To block malicious emails, or their attachments or links being clicked on, you would need to be able to capture the encrypted traffic, decrypt it and inspect inside of it.

Encrypted ransomware

The biggest type of encrypted malware today is ransomware (such as WannaCry, CryptoLocker, Zeus, Chimera and Tesla). Ransomware makes use of encryption in a number of ways. The first is the actual delivery of the ransomware over an encrypted communication, whether that be web mail, social networking sites, instant messaging applications or text messages. Once it is delivered via encrypted communication, ransomware often executes and then phones home to a command and control (C&C) server inside yet another encrypted communication. So not only is the actual payload delivery encrypted, so is the communications back to the C&C server.

Encrypted spear-phishing attacks

In a typical spear-phishing attack, a user logs into their encrypted web mail, opens a spear-phishing email that appears to be from a trusted colleague, clicks an HTTPS link and executes a downloaded file. That user's laptop data is then immediately encrypted and no longer accessible. A prompt screen requests payment of a ransom to access the file.

According to US-CERT, over $5 billion have been siphoned out of companies this past year due to wire transfer spear-phishing and whaling attacks. The FBI estimates these losses have exceeded $1 trillion since 2014. FACC was compromised out of $54 million in a single spear-phishing attack alone.[3] And these attacks continue to happen daily.

Encrypted malicious websites

Just because a site is encrypted with HTTPS does not mean it is safe. Many encrypted sites are malicious, and contain zero-day threats that do not have corresponding firewall signatures. Without these signatures, the firewall may not recognize the corresponding malware on the site. Recently, US-CERT reported 19 new CVEs (Common Vulnerabilities and Exposures) inside the Google Android operating system in one week, including 11 high and 7 critical vulnerabilities.

> The major headline-grabbing breaches in the past five years all either targeted encryption or were delivered via encrypted payload.

Encrypted zero-day attacks

While you might have a very robust antivirus solution on your network, you are not going to always have the signatures there in time to protect against zero-day exploits. A zero-day malware is code that was written perhaps moments before the attack and has never been seen before, so no firewall has a signature for it and can be circumvented. Malware can actually enter the network and disable the antivirus client. The virus's first lines of code are designed to turn off the antivirus solution, and then the malware is detonated. US-CERT recently reported that even the built-in Microsoft Defender AV was compromised to allow outside exploitation.

Conclusion

Fortunately, there are solutions to counter the malicious exploitation of HTTPS, while retaining the ability to encrypt traffic from being viewed by hackers. Learn more about SonicWall's comprehensive and advanced encrypted threat solutions in our datasheet, Decryption and Inspection of Encrypted Traffic.

[3] http://www.securityweek.com/cybercriminals-steal-54-million-aircraft-parts-maker

About Us

SonicWall has been fighting the cyber-criminal industry for over 25 years, defending small, medium size businesses and enterprises worldwide. Our combination of products and partners has enabled a real-time cyber defense solution tuned to the specific needs of the more than 500,000 global businesses in over 150 countries, so you can do more business with less fear.

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

Refer to our website for additional information.
www.sonicwall.com

SONICWALL®