EXECUTIVE BRIEF: THE DARK SIDE OF ENCRYPTION

Why your network security needs to decrypt traffic to stop hidden threats

Abstract

Most of your users' web sessions are likely encrypted with Secure Sockets Layer/Transport Layer Security (SSL/TLS) encryption, or HTTPS. This is to achieve two key objectives:

- Make it more difficult for cyber-criminals to eavesdrop on web connections
- Keep personal information secure and private

Unfortunately, as the good guys increase their use of encryption protocol, encryption has become a favorite threat vector for hackers to mask their attacks, evade defense systems and ultimately open backdoors directly into your network. After all, your security measures cannot stop what they cannot see. If left untreated, any attacks utilizing SSL/TLS will have a 100 percent success rate in compromising your network, leading to loss of classified data, IP and reputation.

Encryption is everywhere

SSL/TLS is commonly used for everything from e-commerce to online banking. SSL/TLS secures a growing amount of enterprise traffic and makes up the majority of network traffic in some verticals. SSL protects data-in-motion by creating an encrypted channel over the public Internet or private networks, which keeps data from being captured or compromised.

In addition, SSL verifies that the data's final destination is not with a hacker spoofing a trusted destination. Crucial and sensitive data such as credit card information, user names and passwords are transported in a way that makes it difficult for anyone but the intended recipient to access that data. While websites and FTP and telnet servers were the original users of SSL, today a wide variety of applications use the protocol, including Java-based applications, application management services and cloud-based services. Facebook and Twitter are

> Legacy network security solutions typically either don't have the ability to inspect SSL/TLS-encrypted traffic or their performance is so low that they become unusable when conducting the inspection.

two of the most popular SSL-enabled applications. Browser add-ons that can force the use of SSL via HTTPS are also available.

In 2019, SonicWall Capture Labs threat researchers recorded 3.7 million malware attacks sent over TLS/SSL traffic, a 27.3% year-over-year increase.

Firewalls can be challenged when inspecting encrypted traffic

Using SSL/TLS, skilled attackers can cipher command and control communications and malicious code to evade intrusion prevention systems (IPS) and anti-malware inspection systems. These attacks can be extremely effective, simply because most organizations do not have the right infrastructure to detect them. Legacy network security solutions typically either don't have the ability to inspect SSL/TLS-encrypted traffic or their performance is so low that they become unusable when conducting the inspection. HTTPS traffic inspection by a next-generation firewall (NGFW) requires six additional compute processes compared to plain-text traffic inspection.

The two processes that affect performance most are:

- Establishing a secure connection
- Decrypting and re-encrypting the traffic for a secured data exchange

The performance penalty can be high in some cases, effectively prohibiting SSL/TLS inspection for companies operating on legacy security systems.

A majority of cyberattacks are opportunistic and most are financially motivated. This means that all organizations are at risk of becoming compromised.

Hiding among the pack

Malware comes in many flavors. While ransomware attacks, including Cerber, have commonly been encrypted the last two years, SonicWall Capture Labs threat researchers are seeing an influx of malicious packers encrypted by TLS or SSL standards.

Although intended for legitimate purposes, packers are used by malware authors to circumvent detection.

At a basic level, packers compress a range of files into a single executable, which is later decompressed to create the original file set. Common packers include Aspack, Armadillo and UPX.

For malware, however, packers are used to obfuscate the executable, evade detection and make it challenging for threat researchers to analyze a sample.

What this can mean to your organization

Encrypted traffic is a growing attack vector for cybercriminals. Unfortunately, there is a fear of complexity and a general lack of awareness around the need to responsibly inspect SSL and TLS traffic — particularly using deep packet inspection (DPI) — for malicious cyberattacks.

It's important to consult with your security or firewall provider to ensure you have this capability and that it is properly enabled.

Conclusion

Encryption is everywhere and is now a favorite threat vector for hackers. Your network security needs to decrypt traffic to stop hidden threats.

Learn more. Read the 2020 SonicWall Cyber Threat Report.

The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON- INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

About SonicWall

SonicWall has been fighting the cybercriminal industry for over 27 years defending small and medium businesses, enterprises and government agencies worldwide. Backed by research from SonicWall Capture Labs, our award- winning, real-time breach detection and prevention solutions secure more than a million networks, and their emails, applications and data, in over 215 countries and territories. These organizations run more effectively and fear less about security. For more information, visit www.sonicwall.com or follow us on Twitter, LinkedIn, Facebook and Instagram.

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

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

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