Fixing the HTTPS Security Blind Spot

It's time to secure network traffic you thought was secure

Rapidly increasing encrypted HTTPS web traffic is creating a security blind spot in business computer networks, allowing destructive malware to slip by unnoticed by conventional network defenses. Although HTTPS encryption does a good job of protecting privacy, email and website user data, the security of the organization can be threatened.

The problem exists because files downloaded and websites accessed over HTTPS may be transporting malicious content that is hiding behind TLS and SSL encryption. Network security appliances, such as unified threat management (UTM) firewalls are not concerned with the encrypted traffic and therefore fail to detect the threats.

Hackers know about the HTTPS blind spot and work aggressively to exploit it. They see that the growing amount of HTTPS traffic creates an ever-larger opportunity to profit from cyber-crime.

What is HTTPS?

When you access a URL beginning with HTTPS (Hypertext Transfer Protocol Secure), you are invoking the Secure Sockets Layer (SSL), or newer Transport Layer Security (TLS) protocols to encrypt the data and files transferred between your browser and the website. The encryption is intended to prevent interception by unauthorized individuals that may be monitoring the traffic.

HTTPS is being used by a growing number of major web services, including Google, Facebook, Twitter, and LinkedIn. According to an April 30, 2015 report from Canadian networking equipment company Sandvine, encrypted web traffic currently makes up 30% of web traffic in North America and may pass 50% by year's end.

The potential for HTTPS attacks is huge since, "…less than 20% of organizations with a firewall, an intrusion prevention system (IPS) or a unified threat management (UTM) appliance decrypt inbound or outbound SSL traffic," according to a December, 2013 report from Gartner. The report also estimates that in 2017, more than half of the network attacks targeting enterprises will use encrypted traffic to bypass controls.

Types of Threats

IT security engineers at eMazzanti Technologies, a NYC area IT consultant and MSP, report that, "a significant amount of malware is coming through the HTTPS channel," including viruses, ransomware and other types of threats. A majority of it slips through as email attachments or website data. If an organization is not decrypting and monitoring the traffic, network security devices can't see the threats.

"Viruses, ransomware, just about anything that you can imagine can get through," stated Almi Dumi, Project Lead, eMazzanti Technologies. "Firewalls are blind to threats coming in with encrypted data when not setup properly to inspect this traffic."

"Viruses, ransomware, just about anything that you can imagine can get through. Firewalls are blind to threats coming in with encrypted data when not setup properly to inspect this traffic."

For example: Some versions of the Cryptowall virus come through HTTPS and surface as ransomware. It may look like an invoice or document, but once inside the network it encrypts critical files, making them unusable. Ironically, businesses using HTTPS encryption to protect data transmissions then have to pay the hackers to decrypt their files.

Other HTTPS-borne threats (with curious names but serious consequences) include FREAK, BREACH, CRIME, BEAST, Lucky 13, and SSLStrip. These, and new threats that appear daily, continue to erode the integrity of the HTTPS encryption scheme, the basis of nearly all Web, e-mail and Internet services security.

Security Technology Battle

The HTTPS security battle is heating up. Hackers are increasingly taking advantage of malware toolkits that exploit HTTPS to prevent malware detection by firewalls and other network defenses. Organizations must bolster their defenses by decrypting and inspecting HTTPS traffic, or fall victim to these types of malware attacks.

eMazzanti's engineers report that most organizations don't employ deep packet inspection (DPI) technology to detect threats coming through HTTPS. Rapidly increasing business web traffic and connection speeds make the processor-heavy DPI task difficult.

A Workable Solution

Deep packet inspection works by means of a security appliance designed to intercept inbound advanced malware and prevent outbound data loss (DLP). It performs HTTP proxy inspection on encrypted traffic by decrypting and applying security rules and algorithms to the data.

Implementing DPI is challenging and requires expert assistance. Security-trained engineers have to set up equipment, generate certificates, and deal with effects throughout the network, including performance and functionality impacts.

"The nature of DPI requires on-site implementation to effectively prevent future attacks while preserving user service levels," stated Ariel Perez, eCare Team Lead, eMazzanti Technologies.

Privacy laws and regulations, as well as pushback from employees, represent another obstacle to successful implementation. Organizations should review privacy policies prior to implementing a DPI solution.

HTTPS Security Checklist

HTTPS security attacks will continue to increase as encrypted web traffic increases. Criminals will go where the opportunities exist. Organizations that are interested in preventing attacks by intercepting threats might consider these steps:

1. Work with an experienced data security professional to assess the threat to your organization.
2. Review privacy laws and regulations, the organization's privacy policies, and employee concerns.
3. Implement a DPI solution with on-site assistance from qualified IT security professionals.
4. Adopt a security-first mindset and use state-of-the-art data security as a competitive advantage.

HTTPS security threats represent a real and growing threat to enterprise data security. It's time to fix the HTTPS blind spot to make once secure internet traffic secure again.