Finding Hidden Threats by Decrypting SSL

Sponsored by Blue Coat Systems, Inc.

Finding Hidden Threats by Decrypting SSL

November 2013

A SANS Analyst Whitepaper

Written by J. Michael Butler

Introduction

SSL encryption is crucial to protecting data in transit during web transactions, email communications and the use of mobile apps. Data encrypted with this common method can sometimes pass uninspected through almost all the components of your security framework, both inbound and outbound. As such, SSL encryption has become a ubiquitous tool for the enemy to hide sensitive data transfers and to obfuscate their command and control communications.

For example, suppose a user has succumbed to one of the many phishing emails she receives every day, has followed a bad URL link and inadvertently downloaded encrypted Zeus malware to the financial officer's computer used for ACH bank transfers. Under the cover of encryption, Zeus sends that password information and other sensitive data to an external user, making it possible for the remote attacker to capture a login session, use the transmitted password and deposit the organization's money in an offshore account. With all commands and traffic transmitted into and out of the network via SSL, the company's security tools were blind to these activities.

Now companies are accepting even more encrypted traffic as they shift toward greater use of cloud services. This means malware will find more innovative ways to take advantage of this common form of transport encryption. For example, attackers can use cloud services to bypass the firewall and synchronize malware from one computer to another, as described in an August 2013 article in "Technology Review News."[1]

With the good guys and bad guys both using encryption, making malicious traffic visible through decryption—and inspecting it—becomes essential. The decryption must be conducted in a way that doesn't interfere with legitimate network traffic, while working with other security systems for optimum accuracy and performance. Then, the traffic must be re-encrypted before sending it on to its destination to protect sensitive information that might be caught up in the packets being decrypted.

This whitepaper describes the role of SSL, the role SSL decryption/inspection tools play in security, options for deploying inspection tools, and how the information generated by such inspection can be shared with other security monitoring systems.

[1] www.technologyreview.com/news/518506/dropbox-and-similar-services-can-sync-malware

About SSL

SSL, also known as *transport layer security* (TLS), is a general-purpose PKI (public key infrastructure) encryption protocol that works between the underlying transport protocol (TCP) and the application containing data we are trying to protect. It can be a part of any application commonly including web browsers or email apps, and it protects data by making it unreadable by unintended recipients. Whenever we mention SSL in this paper, we are also including, by implication, TLS. (Any secure SSL server these days should be running at least TLS 1.1.)

This protocol is used to protect health care, financial, proprietary and other sensitive data transferred through e-commerce applications, workforce applications such as SalesForce, public clouds such as Amazon, and social networking applications such as Twitter and Facebook. It is also used for secure VPN to remote clients and secure FTP, among other forms of transport.

SSL involves the exchange of public keys that are used to encrypt a symmetric key that can only be decrypted by the other party's private key. Such an exchange takes place initially in communications between two entities, in order to pass the symmetric encryption key that is used to protect the data that follows. Figure 1 represents a simplified version of how this works.

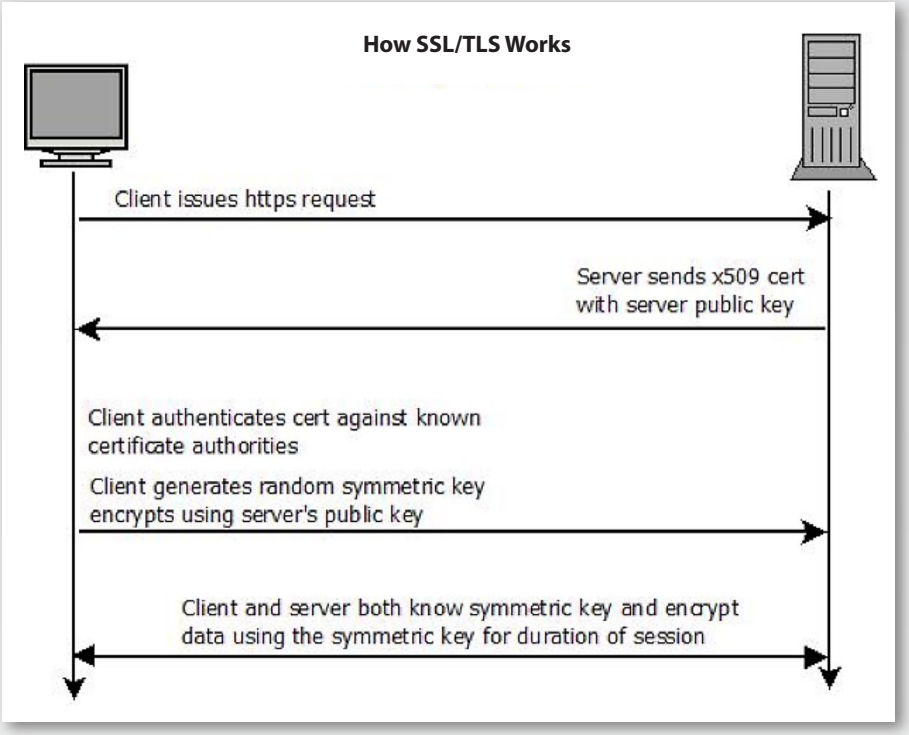

Figure 1. SSL/TLS Process[2]

The benefits of SSL extend beyond encryption and data protection to assuring data integrity and nonrepudiation, which are key tenets of any risk management program. However, it is important to note that it is possible to use SSL without true authentication, such as in the use of self-signed server certificates.

[2] http://tools.ietf.org/html/rfc5246

Widespread Use

Since its introduction in the mid-1990s, the level of protection SSL (and then TLS) offers has been improved by, for example, increasing the length of keys used during the SSL handshake to 2048 bits. Even more significant benefits are offered to those who use Diffie-Hellman Exchange (DHE)[3] rather than RSA during the SSL handshake.[4]

SSL has become ubiquitous as the de facto encryption standard for web and email transactions. Google measured 17 million SSL-encrypted pages as of May 2010.[5] The Electronic Frontier Foundation (EFF) scanned the entire IPv4 space in that time frame and located 16.2 Million IP addresses[6] listening on port 443, and of those, 10.8 million started an SSL "handshake."

This doesn't count the unknown number of sites offering SSL connections on an obscure port or the growth in IPv6 addresses. Therefore, we can assume that well over 10 million active IP addresses are listening for SSL traffic.

According to NSS Labs, SSL traffic now accounts for an average of 25 percent to 35 percent of a typical enterprise's network traffic.[7] One network technician reports that SSL traffic makes up 50 percent to 70 percent of the traffic within her organization. The rate for financial and other organizations handling large amounts of sensitive data will, of course, be higher.

NSS Labs also predicts an average increase of around 20 percent in SSL traffic per year. This growth will be fed by the increasing use of HTTPS (encrypted HTTP) and other protocols running on top of SSL to support social networking applications (including Twitter and Facebook) and search engines. Corporate migration to cloud services, especially external clouds, will also cause a jump in the use of these protocols to protect data in transit to and from the cloud.

Ripe for Abuse

Even though SSL helps protect an organization's sensitive data from prying eyes while meeting compliance demands for data protection, there is a dark side to data encryption. The criminal element, for example, is using encryption to hide its activities. In the next section, we discuss abuse cases, followed by how SSL traffic inspection can help protect against and respond to malicious activity hiding within SSL sessions.

---

[3] http://searchsecurity.techtarget.com/definition/Diffie-Hellman-key-exchange

[4] http://wiki.openssl.org/index.php/Elliptic_Curve_Diffie_Hellman

[5] https://developers.google.com/speed/articles/web-metrics

[6] www.eff.org/files/DefconSSLiverse.pdf

[7] https://nsslabs.com/system/files/public-report/files/2013-06%20AB%20SSL%20Performance%20Problems%20130605c.pdf

Encryption Gone Bad

Encryption has not gone unnoticed by external attackers and abusive employees. As NSS Labs said in a recent report, "Ironically, increased use of SSL in attempt to make our online lives more secure can create 'blind spots' that can actually reduce security…"[8]

Even with all the usual enterprise security practices in place, monitoring tools can only see the destinations and, in some cases, the host name within the unencrypted portion of the SSL handshake. They can't see the full path, content type or content itself. That can be a problem when the command and control channels or the exfiltration of sensitive data are hidden by encryption.

Hiding Malicious Actions and Messages

Bad actors can and do use SSL to mask malicious actions and data exfiltration in the following ways (among others):

- Sending an encrypted stream of protected, sensitive and other critical data outbound through your firewall over "normal" ports, such as 443 or 80, which the firewall is tuned to accept because they are approved ports.
- Obfuscating malware communications when a worm, virus or botnet "phones home" to send stolen data to a master computer or download instructions or more malicious code.
- Making phishing threats look even more legitimate, as even informed recipients would think the SSL usage makes it secure. Clicking the link, however, takes them to an SSL server loaded with malware that infects the client because the malware traffic is encrypted and not recognized by an IPS.

These real threats make it possible for us to develop the following scenarios, all of which play out again and again across all verticals, according to multiple media reports.

Hiding the Initial Infection

An initial infection coming through an approved port and a seemingly secure browser is the most common way infections are launched beneath the radar of a firewall and/or IPS. According to CGISecurity, it's actually easier to attack an organization through applications that use encryption than those that don't. In a FAQ on cross-site scripting attacks, it said:

> **Websites that use SSL (https) are in no way more protected than websites that are not encrypted. The web applications work the same way as before, except the attack is taking place in an encrypted connection. People often think that because they see the lock on their browser it means everything is secure. This just isn't the case.[9]**

In other words, the use of encryption provides the perfect cover and also makes a convincing phish that users could fall for.

Through cross-site scripting, malicious users can steal cookies that can be used for a number of things, including account or session hijacking, changing user settings, cookie poisoning or false advertising. All of this can be accomplished while hiding within SSL-encrypted traffic.

---

[8] https://nsslabs.com/news/press-releases/nss-labs-research-finds-ssl-traffic-causes-significant-performance-problems-next

[9] www.cgisecurity.com/xss-faq.html

Hiding the Command and Control Channel

Malware families such as Zeus are notorious for using encryption and other tricks to hide their command and control (C&C) communications from security-monitoring devices. One recent example is the "Gameover" banking Trojan that opens an SSL connection from compromised web servers and uses that channel for command and control operations. The initial infection is sent via spam, and once the user's browser touches the infected website, the channel is automatically opened. Gameover has been linked to DDoS and banking credential theft attacks.[10]

Hiding Data Exfiltration

An increasing number of malware families also use encryption to hide any network information, including passwords or sensitive data (such as stolen bank account information) they are sending out to SSL servers.

In this hypothetical case, the initial phish went undetected because the infrastructure protection programs did not include SSL inspection on the outbound response to the email, and its firewalls were not sounding any alarms to block the packets. Then, the malware set up connections to a command and control server from deep inside the network and started sending financial account data out of the organization under SSL-encrypted sessions that looked perfectly legitimate to the edge network security.

The encryption blinded the monitoring systems to these internal network activities, so the attack went on for nine months until an external party alerted the organization that thousands of accounts linked to the organization's processing systems had been exploited and abused.

[10] www.scmagazine.com/gameover-trojan-hides-activity-in-encrypted-ssl-connections-to-defraud-victims/article/315215

Making SSL-Encrypted Traffic Visible

To counter these threats, organizations need visibility into SSL-encrypted traffic. That means using SSL inspectors that work with secure network gateways and other advanced edge security to inspect the traffic once it's decrypted. Visibility into SSL-encrypted sessions must include inspection of inbound, outbound and even suspect internal SSL traffic to detect command and control communications, outbound sensitive data and malware distribution.

Any solution providing visibility into SSL/TLS traffic must meet a number of criteria:

- It should sit inline so it can immediately and automatically react to suspicious inbound and outbound traffic. (There may be use cases where out-of-band inspection is preferred, which we discuss later.)
- It should send decrypted traffic to network and endpoint security devices such as IDS, IPS, network forensics devices and advanced network gateways for immediate inspection and analysis as needed.
- It must decrypt inbound and outbound traffic in compliance with a policy based on what is known good and known or suspected bad activity, as well other considerations.
- It must be able to decrypt both inbound and outbound communications, including the web and email communications from which many external attacks originate.
- It must be able to whitelist or filter certain data that must be kept encrypted, such as patient information protected by HIPAA. This avoids revealing the very data we are attempting to keep safe.
- It must process large amounts of data quickly.
- Decryption must help to accelerate the analysis of suspect traffic, rather than getting in the way of these processes.

Providing visibility into SSL traffic is not the same as analyzing the data. While the SSL inspection may be able to follow some rules governing what traffic to decrypt upon inspection, the real analysis of the decrypted packets occurs through other tools working with the SSL inspection device. These include IDS/IPS, firewalls, secure web gateways, data loss prevention (DLP) and other monitoring systems, as well as forensics tools based on a coordinated policy among devices. We show how decryption works with and enhances the capabilities of other monitoring and analysis devices in the next section.

Deployment Options

Security tools can be either active (usually inline) or passive (tapped into the line.) Passive monitoring involves simple detection and logging after decryption, along with the possible use of alerting. When the SSL-inspection device is in a passive (tap) configuration, it can only feed passive security tools. Passive tools, such as IDSs, can report on analyzed traffic and possibly send alerts, but they cannot block threats.

Active monitoring tools, such as IPSs, allow more actions, including segmenting the data into a secure zone for further analysis and/or blocking suspect traffic. Active monitoring is supported by the "in-line" model, which is the ideal for most SSL-inspection capabilities. This is particularly true during a live investigation, when time is of the essence, or when SSL inspectors pull the suspect traffic off the network to prevent damage. When considering whether to use an active or passive tool, remember that passive tools consume the decrypted data sent to them and never forward it to active tools such as an IPS. On the other hand, a tool in an active configuration can feed data "downstream" to both active and passive security tools.

Figure 2 shows a device used in line to decrypt internal traffic between a server and client PC within the corporate firewall.

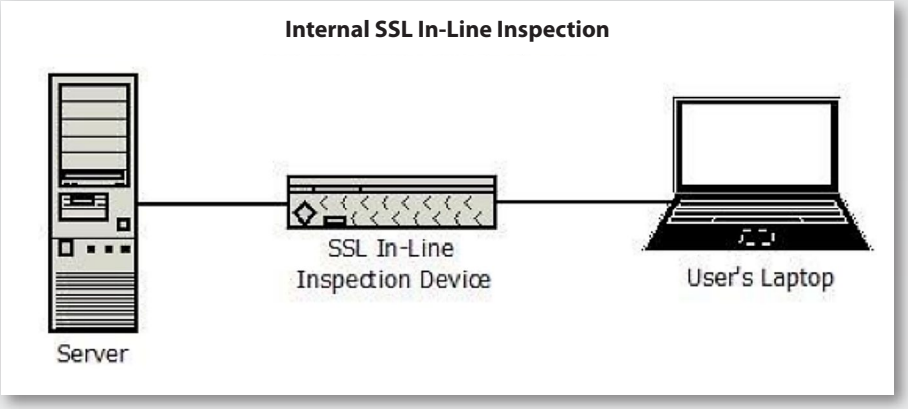

Figure 2. Inline Packet Inspection for Internal Systems

Internal communications between servers are common among many malware families that also use encryption to protect these communications. For example, malware could be sniffing sensitive data off the network or copying it off infected devices and parking it on an internal server before sending the data out of the network.

Assisting Other Monitoring Tools

The inline SSL-inspection appliance detects the SSL session and consults its policy to determine whether the session should be inspected. In this case, the sessions could raise a flag if the types of applications and servers talking to one another are abnormal. If the session requires decryption, it decrypts the data at high speeds and sends the decrypted data to the security tool(s) to which this data is designated to go.

Another option is deploying the inspection appliance outside the firewall. Figure 3 shows such a configuration, with the links to associated security tools.

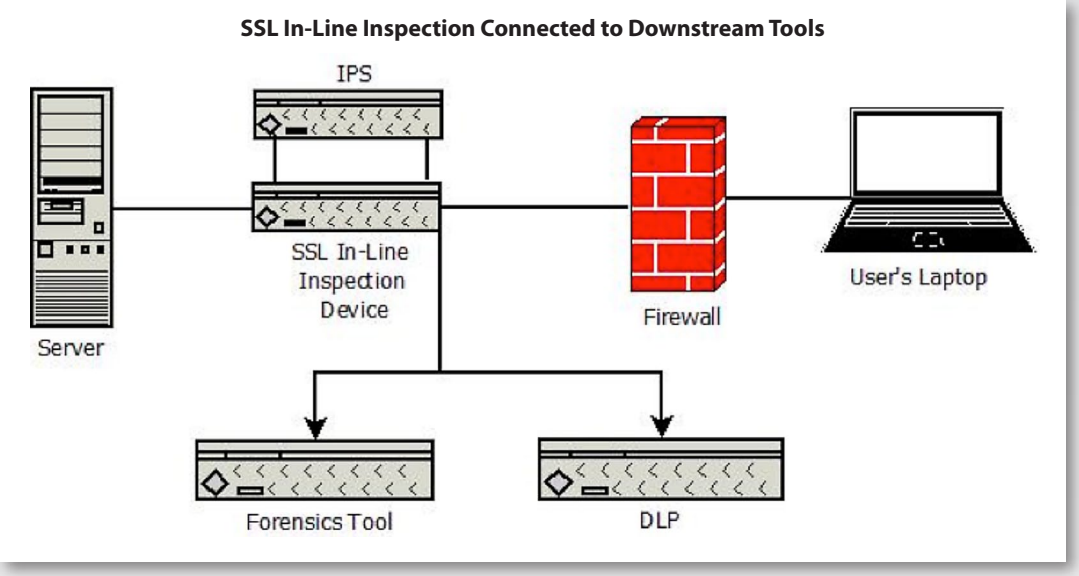

Figure 3. SSL Inspection Working with Other Security Tools for Analysis

Policies are required to coordinate the actions taken by the SSL-inspection device and its associated IDS, proxy or NGFW devices. For example, outbound commands detected by the SSL-inspection device might be sent directly to a malware analysis tool. In another example, outbound SSL traffic containing sensitive customer financial data may go to the DLP and/or to an audit and compliance reporting system.

All in One

Another choice is using a multifunctional gateway that can also perform decryption. The advantage is a reduction in the number of devices an organization must buy and manage. The downside is that, given current processor limitations, asking one device to do too many tasks can and does slow network performance or the detection of possible threats. This is particularly true when decryption is involved.

In addition, using a security device with built-in SSL inspection means tearing out and writing off your investments in existing IPS, secure network gateways and other security infrastructure, and creating new IT policy and support issues around certificate authorities (CAs) and key management.

Figure 4 shows such an all-in-one network security and SSL decryption configuration using a multifunction gateway/firewall capable of SSL inspection.

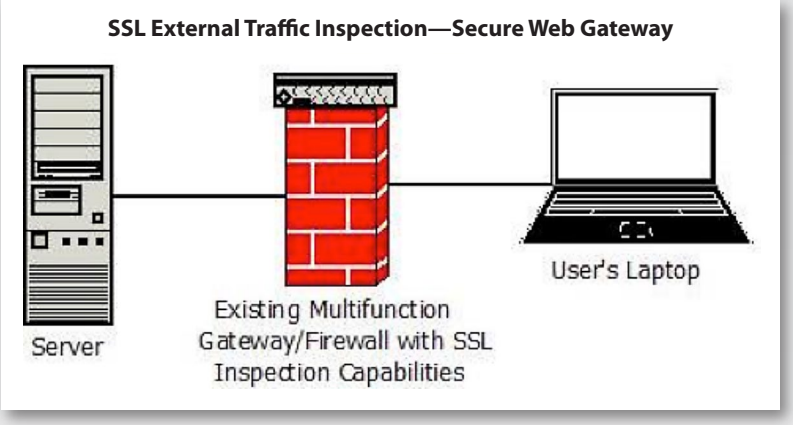

Figure 4. External Traffic Inspection

Sharing Decrypted Data

The decrypted data is useful only if it is analyzed to determine what is valid and what contains threats. This requires sharing it with downstream devices quickly and completely enough that attacks can be found and stopped before they do damage. Downstream sharing with systems could include the following:

- **IDS/IPS, firewalls and network gateways.** Pairing an SSL-inspection appliance with an IPS allows the IPS to see and block malware and other threats in both unencrypted and encrypted traffic. The SSL-inspection appliance feeds the decrypted stream through the IPS, which decides to drop packets it sees as a threat. The inspection appliance detects this and, instead of sending re-encrypted traffic to the destination, kills the SSL session.
- **Email filtering.** Because email filtering is a basic tool that most organizations use religiously, the ability of a decryption/inspection system to work with email security is important. This is especially true of the growing number of enterprises that rely on cloud-based email or other solutions that bypass standard corporate email servers with email filtering solutions.
- **Data loss prevention.** These tools are high on the list for security practitioners because data loss prevention is the top priority for the legal, compliance, and contracts departments to which they report. DLP policies must be applied to all information, whether encrypted or not. When the data is encrypted, being able to see what is inside is critical to the legal, compliance and contracts departments, as well as information security. With an SSL-inspection device, the DLP system can go about its job of pattern-matching, looking for data such as Social Security, credit card, bank account and routing numbers that otherwise might escape into the wild.
- **Forensics.** Forensics and investigative tools, which are increasingly converging into the realms of security intelligence and analytics, need ready access to decrypted traffic for further analysis.

Advice for Getting Started

Organizations should tap legal counsel to ensure SSL decryption doesn't violate corporate, industry or governmental regulations around data confidentiality. Some of these determinations hinge on where the hardware lives and/or where the transaction takes place.

Organizations also need to know where their critical systems are and what data could be exfiltrated from them. In addition, they need to know these things:

- Whether those systems connect to trusted or untrusted networks
- Whether the organization would face a greater threat from failing "open" (allowing potential threats through but allowing business to continue) or failing "closed" (ensuring total security but blocking all transactions when the security systems are unavailable)
- Current and future levels of traffic that must be decrypted
- The number of encryption protocols the organization uses
- The downstream systems with which the organization wishes to share the decrypted data

Capabilities to consider when choosing an SSL-inspection solution include depth, performance, scalability and management.

Depth

The depth of a device is the number of encryption protocols and algorithms it supports and can decrypt. For this discussion, a tool must be able to intercept and decrypt SSL/TLS protocols using asymmetric and symmetric ciphers, varying hashing algorithms, key lengths and digital signatures, and support multiple versions of SSL or TLS, including TLS extensions.

Another measure of depth is whether the tool can detect SSL-encrypted traffic on any port. SSL is usually associated with the ports shown in Table 1.

Table 1. Typical Ports Used for Encrypted Traffic

Protocol[11]	Clear Text	Explicit Port	Implicit Port
FTP	21	21	990
HTTP	80		443
IMAP	143	143	993
POP3	110	110	995
SMTP	25 or 587	25 or 587	465

Finding malware and commands in commonly approved ports is critical, because most network monitoring devices allow traffic through them. In addition, the tool must be able to detect and decrypt SSL traffic on any port, even if an application is using a nonstandard port that is not listed in Table 1.

[11] www.rebex.net/kb/tls-ssl-explicit-implicit/default.aspx

Performance

Performance is a critical metric. For both application performance and security reasons, it is essential that traffic be decrypted and forwarded to an organization's analysis tools as quickly as possible. It is also important that a tool keep up with the traffic so that inspection is done without slowing communications between the client and server.

To assess your speed requirements, determine the number of TCP active connections and teardowns that occur in your network on a regular and, more importantly, on a peak basis. Other factors are the number of simultaneous connections (and SSL sessions) that must be supported and the rate of new SSL session setups/teardowns, which may not always be the same as the rate of TCP connection setups/teardowns.

Scalability

Plan for the future. How soon will you upgrade to faster speeds and more SSL connections? Do you support a different speed between devices in the trusted server network than "on campus" among users? How many servers do you currently have in your data center? What is your internal "client" population and the size of your customer base that might access your servers? What is your organization's anticipated growth in these areas? The more users and devices, the more packets pass over the network. All of this affects the bandwidth your decryption/inspection and analysis tools will need to handle.

Consider also whether your SSL-inspection solution must be adequately redundant (highly available), in which case your organization will require devices capable of operating in a high-availability configuration.

Manageability

A tool is pretty much useless if it is difficult and/or frustrating to manage. Consider not only the user interface, but also its ability to provide console and/or email alerts. The tool also needs to generate robust reports that deliver actionable data to the information security team and management. Reports not only can be leveraged to improve security, but can also help prove the ROI of SSL inspection to the business managers who pay for it.

Preconfigured, canned reports can be useful if they were optimized by the vendor for the highest speed and least possible impact on the reporting system. However, the ability to customize reports is also crucial, because managers in every organization have unique needs for security-related information.

Depending on their deployment strategy, customers may also want to evaluate whether a solution allows reporting to be split off as a separate function, possibly using a separate (virtual) server, which should lessen the impact of report generation on the SSL-inspection and analysis devices.

Conclusion

As SSL usage has grown, clever hackers have been subverting this vital security tool by using it to hide their actions from traditional network detection devices that allow this traffic to pass into and out of the network because they cannot read it. Bad actors are after our data, our customers, our resources, our company secrets and our money, and encrypting that data is the best way to hide their transfers and malware communications from security devices.

To counter this threat, SSL decryption and inspection technology is critical for organizations managing threats and sensitive data on their networks. SSL inspection includes the ability to decrypt and forward SSL traffic to other tools for analysis and timely reaction to find and stop attacks hiding under the cover of encryption. When these tools are chosen and deployed properly, organizations can find the threats hiding within encrypted data without degrading business-critical communications.

Like a black hole that sucks the light out of the space surrounding it, "dark" communications can suck the life out of our organizations. Inspecting SSL traffic will bring light to the darkness and show organizations exactly what communications are happening on their networks, uncovering dangers such as malicious commands and the theft of sensitive data.

About the Author

J. Michael Butler, GCFA CISA GSEC EnCE, is an information security consultant with a leading provider of technical services for the mortgage industry. Butler's responsibilities have included computer forensics, information security policies (aligned to ISO and addressing federal and state disclosure laws), enterprise security incident management planning, internal auditing of information systems and infrastructure, service delivery and distributed systems support. He has also been involved in authoring SANS security training courseware, position papers, articles and blogs.

SANS would like to thank its sponsor:

BLUE COAT®

Last Updated: June 23rd, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Cyber Defence Canberra 2017	Canberra, AU	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MDUS	Jun 26, 2017 - Jul 01, 2017	Live Event
SEC564:Red Team Ops	San Diego, CAUS	Jun 29, 2017 - Jun 30, 2017	Live Event
SANS London July 2017	London, GB	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, JP	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS ICS & Energy-Houston 2017	Houston, TXUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, SG	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Los Angeles - Long Beach 2017	Long Beach, CAUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, DE	Jul 10, 2017 - Jul 15, 2017	Live Event
SANSFIRE 2017	Washington, DCUS	Jul 22, 2017 - Jul 29, 2017	Live Event
Security Awareness Summit & Training 2017	Nashville, TNUS	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS San Antonio 2017	San Antonio, TXUS	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Hyderabad 2017	Hyderabad, IN	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MAUS	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, CZ	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UTUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NYUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, ILUS	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, AU	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VAUS	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CAUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FLUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Network Security 2017	Las Vegas, NVUS	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS Dublin 2017	Dublin, IE	Sep 11, 2017 - Sep 16, 2017	Live Event
SANS Paris 2017	OnlineFR	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced