6 DISCOVERIES

IT SECURITY PROS NEED TO KNOW ABOUT SSL INSPECTION

FINDINGS FROM THE PONEMON STUDY ON THREAT ACTORS, DEFENSE ABILITIES AND BARRIERS TO DECRYPTION CONTROLS.

EXECUTIVE SUMMARY

Encryption is necessary to protect online data in transit from being compromised. But the threat is continuously evolving. Bad actors are now leveraging SSL-based encryption to hide malicious activity from existing security controls and technology. Most security professionals recognize this growing threat, but few feel they are adequately equipped to address the problem.

So how concerned should we be about this growing threat vector?

In a study commissioned by A10 Networks, the Ponemon Institute surveyed 1,023 IT and IT security practitioners in North America and EMEA who are involved in detecting and/or preventing Web-based threats and are familiar with their organization's network traffic inspection. The detailed study evaluated organizational understanding of threat actor behavior changes, abilities to detect and defend against attacks hiding in SSL traffic, barriers to entry for implementing needed decryption solutions, and critical features for solution selection.

After carefully analyzing the data, A10 identified six key outlooks that may help your organization make smart and proactive security and business decisions.

OUTLOOK 1

SSL-BASED EVASION IS MORE COMMON THAN YOU THINK.

In just the past 12 months, of the 81 percent of respondents who were victims of a cyberattack or malicious insider activity, 41 percent suffered an attack where actors evaded detection by obfuscating their activities and/or payload within SSL encryption.

41% SUFFERED AN ATTACK WHERE ACTORS EVADED DETECTION BY USING SSL ENCRYPTION

ONLY 36% BELIEVES THEIR ORGANIZATION CAPABLE OF LEVERAGING SSL ENCRYPTION AND INSPECTION

OUTLOOK 2

ORGANIZATIONS ARE NOT PREPARED TO PROTECT THEMSELVES AGAINST MALICIOUS SSL TRAFFIC.

Of all respondents, only a third (36 percent) believed their organization capable of properly leveraging SSL decryption and inspection to prevent a costly data breach.

ENCRYPTED TRAFFIC WILL INCREASE

OUTLOOK 3

THE VOLUME OF ENCRYPTED WEB TRAFFIC WILL ONLY INCREASE.

Both inbound and outbound encrypted Web traffic — up to 80 percent[1], respectively — is expected to increase as a percentage of all traffic over the next 12 months. As such, threat actors will continue to leverage SSL-encrypted traffic for the foreseeable future.

[1] https://transparencyreport.google.com/https/overview?hl=en

OUTLOOK 4

COMPANIES AREN'T DECRYPTING WEB TRAFFIC. HERE'S WHY.

Organizations locked on to three core reasons why they had not yet implemented decryption solutions: lack of security tools (47 percent), insufficient resources (45 percent) and concerns over performance degradation (45 percent).

47%	LACK OF SECURITY TOOLS
45%	INSUFFICIENT RESOURCES
45%	CONCERNS OVER PERFORMANCE DEGRADATION

80%

ADMIT TO BEING A VICTIM OF A CYBERATTACK

OUTLOOK 5

SSL TRAFFIC INSPECTION IS GROWING IN IMPORTANCE.

With 80 percent of respondents admitting they were a victim of a cyberattack, and the high percentage of those incidents leveraging encryption to avoid detection, it's not a surprise that 57 percent say that SSL inspection is important to the safety of their business.

OUTLOOK 6

PERFORMANCE STILL DICTATES BUSINESS DECISIONS.

Security concerns aside, network performance remains a top requirement for organizations. In fact, 61 percent of respondents stated that concerns about the impact on their network is the primary reason they don't yet decrypt SSL traffic.

61% STATE THAT NETWORK IMPACT IS THE REASON THEY DON'T YET DECRYPT SSL TRAFFIC

DISCOVER SSL DECRYPTION

Ready to learn more about SSL decryption and inspection? Visit **a10networks.com/SSLi** to implement stronger security and performance capabilities for your organization.

LEARN MORE

ABOUT A10 NETWORKS

CONTACT US

a10networks.com/contact

Part Number: A10-MS-23178-EN-04 AUG 2018