Uncovering Hidden Threats within Encrypted Traffic
Introduction

In a study commissioned by A10 Networks, Ponemon surveyed 1,023 IT and IT security practitioners in North America and EMEA who are involved in preventing and/or detecting Web-based attacks and are familiar with their organization’s network traffic inspection.

The detailed study evaluated understandings of threat actor behavior changes, abilities to defend attacks hiding in SSL traffic, barriers for implementing needed decryption controls and critical features for solution selection.
Survey Highlights

Survey Respondents Say:

- Half of all known cyberattacks used SSL encryption to evade detection in the last 12 months.
- The inability to inspect encrypted traffic will compromise capacity to meet existing and future compliance requirements.
- Most don’t believe their organization can properly inspect SSL traffic.
- Use of SSL encryption to mask malicious activity will parallel this growth.
- Encryption of inbound and outbound Web traffic will continue to increase.
- Three common barriers to implementing proper SSL inspection are a lack of security tools, insufficient resources and performance degradation.
- SSL bandwidth requirements diminish the effectiveness of existing security controls.

Introduction

Highlights

Audience

Findings

Attack Types

Takeaways

Recommendations
Target Audience

Most respondents (73 percent) are from organizations with 5,000 or more employees.

Core Focus
Survey targets were identified for their involvement or responsibility in preventing or detecting Web-based attacks in North America, Europe, Africa and the Middle East.

Industries
The survey was strategically distributed to 14 primary industries. Almost half of respondents (49 percent) were from financial services, health and pharmaceuticals, general services and the public sector.

Top 4 Roles
Of all respondents, 55 percent report directly to the CIO, CTO or head of corporate IT.

Organization Size
55% 5,001 - 25,000 employees
The Encryption Landscape

Of all the respondents who disclosed they were victims of a cyberattack in the preceding 12 months, nearly half claimed the attack leveraged SSL traffic to evade detection. Another 15 percent were unsure.

The majority of respondents also agree that SSL decryption and inspection is either “essential” or “very important” to the performance and security of their business.

- 80% Were Victims of a Cyberattack
- 41% Attacks Hid in SSL Traffic
- 89% Think SSL Decryption is Important
The Dividing Line

Of all respondents, only a third believe their organization can properly leverage SSL decryption and inspection to prevent a costly data breach.

Can You Detect Malicious SSL Traffic?

No
64%

Yes
36%
Today vs. Tomorrow

Will threat actors continue to hide malicious activity in SSL traffic? With the volume of encrypted inbound and outbound Web traffic increasing the next 12 months, it is the likely trend.

Today
39% Inbound
33% Outbound

Next Year
45% Inbound
41% Outbound
Top 3 Reasons for Not Inspecting SSL Traffic

More than half of all respondents (62 percent) admit that their organization does not currently decrypt Web traffic. Why?

- Lack of Enabling Security Tools: 47%
- Insufficient Resources: 45%
- Performance Degradation: 45%

Of this group, 51 percent say they will implement SSL decryption within the next 12 months.
Inspection Strategies

For organizations that are inspecting decrypted traffic, most haven’t found a seamless or cost-effective manner of implementing the process. Many are using a blend of commercial-grade solutions, in-house technology and labor-intensive manual inspection.
Performance is Big

The overwhelming concern in implementing SSL decryption solutions? Performance. The notion is confirmed by organizations currently decrypting and inspecting SSL traffic, as well as companies that haven’t yet invested in a solution.

Concerned

61%
Lack of performance a concern for organizations that don’t decrypt SSL traffic.

Confirmed

83%
Decryption results in some type of degradation within organizations currently decrypting and inspecting SSL traffic.
Features They Want

Organizations are looking for SSL decryption solutions that combine a wide range of attributes and capabilities. The most popular features — each acknowledged by more than 50 percent of respondents as important — focus on SSL certificate and key management, scalability, compliance and performance.

- **79%** SSL Certificate Management
- **68%** Scalability
- **63%** Compliance Requirements
- **62%** Uptime, Performance & Security
- **54%** Multi-Vendor Security Integration
Five Attacks Hiding in SSL Encryption

There are numerous approaches to masking malicious activity within SSL traffic. Below are common attack vectors, the likelihood each will occur and the ability of responding organizations to resolve the event.

Outbound Port Abuse

When asked: About the possibility of an attack hiding in “normal” port 443 traffic.

78% Thought they would likely be targeted by a similar attack.

30% Only a third were confident in their ability to resolve it.

79% Believe it’s highly likely this could occur within their organization.

17% Claim their organization has the ability to mitigate such an attack.

Phishing

When asked: If traffic from an SSL-secured malware server could be spotted by their intrusion prevention system (IPS).
Internal Hide & Seek
When asked:
About malware hiding outbound data (e.g., passwords, credentials, etc.) within encrypted traffic.
- **74%** Admit that this attack vector is highly likely.
- **16%** State that their organization could identify and mitigate the SSL-encrypted malware attack before data exfiltration.
- **66%** State that the likelihood of such an event is highly possible.
- **26%** Believe their organization could spot this behavior and prevent data loss.

Cookie Theft
When asked:
About the dangers of cross-site scripting (XSS) and how threat actors are able to steal cookies to highjack sessions, change user settings, poison cookies, etc.
- **62%** Acknowledge that XSS activity could hide within SSL-encrypted traffic.
- **19%** Assert that their organization could stop XSS attacks, even when concealed within encrypted traffic.

Phoning Home
When asked:
If an attacker could obfuscate outbound communications and/or stolen data to a command and control server.
- **26%** Believe their organization could spot this behavior and prevent data loss.
4 Key Takeaways

One thing is clear: threat actors will continue to leverage SSL-encrypted traffic to obfuscate malicious activity. While most organizations confirm that this is a concern, the urgency or understanding of the threat varies between respondents.

1. Organizations recognize threat actors’ evolving strategy of leveraging encrypted SSL traffic to hide activity.

2. Performance is a major barrier for deployment of SSL decryption solutions.

3. Respondents require a diverse range of necessary features and benefits.

4. Organizations are highly concerned that they aren’t able to detect and stop encrypted attacks, but aren’t sure where to start or how best to defend their business.
Recommendations for Inspecting SSL Traffic

1. **START NOW.** SSL decryption is rapidly becoming a necessity to properly inspect Internet traffic and stop potential attacks. Be proactive and expose the hidden threats within your environment.

2. **TAKE INVENTORY.** Assess your tools and determine which can benefit from adding SSL decryption and inspection capabilities. You’ll gain better visibility to what’s needed to protect the efficacy of your existing investment and avoid costly over-spending and redundancies.

3. **IDENTIFY CRITICAL NEEDS.** Prioritize the tools you need and what’s important to your business. Some organizations value scalability. Others require specific compliance controls. Many seek easier integration with third-party security vendors. Outline what’s important and build your plan.

4. **EVALUATE SSL DECRYPTION SOLUTIONS.** By mapping SSL decryption capabilities to a proven platform, you will be able to properly inspect and analyze encrypted traffic for malicious behavior — without hindering performance or significantly adding to your security program’s TCO.
A10 Networks Thunder SSLi

A10 Networks Thunder® SSLi® products feature A10’s SSL Insight® technology, which eliminates the blind spot imposed by SSL encryption by offloading CPU-intensive SSL decryption functions from third-party security devices. Thunder SSLi decrypts SSL traffic and forwards it to one or more third-party security devices.

To learn more about A10 Thunder SSLi, please visit a10networks.com/SSLi