



NCSIP Position Paper

NCSIP Position Paper on Malware Visibility

Prepared on behalf of NCSIP with input from Committee Members by

Gary Perkins/BRITISH COLUMBIA

2018-01-15

INTRODUCTION

Cybersecurity has never been as imperative as it is today. No organization globally is immune to attack. Cyberattacks are escalating in frequency, sophistication, and are more targeted than ever. Threat actors are taking additional steps to ensure their attacks and efforts to remain persistent go undetected. More than ever, the attacks, ongoing control, and ex-filtrated data are encrypted. The percentage of encrypted traffic has increased significantly over recent years and traditional security controls are incapable of inspecting the traffic to prevent, detect, and respond to attacks. Malware visibility refers to the decryption of encrypted network traffic so that it can be inspected by traditional security systems such as firewalls and intrusion prevention systems.

“The growing adoption of protocols to secure Internet traffic, including Secure Socket Layer (SSL), is paradoxically giving cyber criminals a way to evade network defences.”

<https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/web/ds-ssl-intercept.pdf>

POSITION

It is the position of NCSIP that organizations must implement some form of malware visibility to prevent, detect, and respond to attacks hidden by encryption.

The percentage of network traffic that is encrypted has risen significantly in recent years. This affords organizations additional security and privacy controls against would-be adversaries. Unfortunately adversaries are equally interested in concealing their attacks to ensure the attacks are successful and remain undetected. Organizations that do not “decrypt” potentially malicious traffic prior to being inspected by traditional security controls will not be able to prevent an increasing number of attacks.

Normally, network traffic between the users’ browser and the webserver is encrypted. In order to establish visibility, an intermediate system will essentially perform an authorized ‘Man in the Middle’ attack to capture traffic between the destination server and the intermediate system. The traffic will be decrypted on the intermediate system and can be passed through traditional security technology for inspection. Then the traffic is re-encrypted by the intermediate system and passed to the end users’ machine. The end user’s machine must be configured to trust the certificate of the intermediate system.

The primary concern with this solution is the threat to privacy. Whether the threat is real or perceived depends on how the system is used. In order to maintain privacy, the integrity of the system must be maintained similar to existing technology. With existing technology an event is detected and the traffic is prevented or an alert is generated. There is no human intervention until a suspicious event is identified. It should be the case that the inspection is performed by a system in much the same way as a firewall operates today.



Organizations must have a solution to provide visibility into malware and other attacks. In the absence of a solution, they will be subject to increasing undetected attacks in the safety of an encrypted tunnel, unaware whether information was ex-filtrated or how much.

“...the encrypted traffic that protects data from being viewed within these modern applications also creates a **blind spot** that can be exploited by advanced threats and malware, as indicated by numerous highly-publicized data breaches in well-known organizations. To identify hidden threats to your organization, it's clear you need complete visibility into the encrypted traffic coming into and out of your business. However, to comply with local privacy regulations that protect certain classes of data — such as financial or healthcare-related, as well as with corporate policies on the acceptable use of applications - organizations must be able to selectively decrypt network traffic. An encrypted traffic management strategy that considers the various business needs, the corporate policies established, and the compliance mandates for your industry is essential.”

<https://www.bluecoat.com/fr/node/17406>

Given the rise of encryption resulting in loss of visibility, legacy technology solutions are no longer able to provide the value they once did. Malware visibility through decryption of encrypted traffic, inspection, and re-encryption is required to preserve the value. Organizations may choose to exclude certain sites such as personal banking to avoid decrypting sites believed to be low risk. However, while the technique of decrypting traffic works well for many types of encrypted traffic it does not work for all. In some environments, depending on the level of traffic and the technology used, decrypting traffic may cause performance issues. In order to avoid performance issues this function should be performed on dedicated hardware rather than attempting to manage this through software. This solution is best applied when there are a small number of known ingress and egress points. Organizations may focus their spend on technologies to inspect the traffic once decrypted before it is re-encrypted and passed back to the client.

Finally, this solution should in no way be confused as humans inspecting the traffic. Malware visibility (or SSL decryption) functions in much the same way as firewalls and intrusion prevention systems work with systems performing the inspection and preventing known bad events and identifying other potentially bad events.

In summary, given the rise of encrypted traffic and the propensity for legitimate and illegitimate users to leverage this capability to hide traffic from prying eyes, it is completely unreasonable for organizations to not invest in malware visibility systems. There is no less intrusive way to provide the same level of protection. If you're not decrypting traffic in order to prevent and detect malware, “...you're leaving a large hole in your network where you cannot protect against threats coming in or sensitive data going out”. As such, **NCSIP recommends that all organizations implement malware visibility services in order to prevent and detect attacks occurring over encrypted channels.**

“The percentage of encrypted Internet traffic continues to grow creating a space where not only private information but also criminals can travel about undetected. In the last five years, the advent of SSL traffic from major companies like Google, YouTube, and Twitter has spawned an expansive movement toward encrypting Internet traffic for enterprises as well.

The risk in taking this security measure, though, is that while the exchange of information via the Internet is secured, bad guys can also linger unnoticed. Criminals, of course, know this and use it to their advantage, cloaking their attacks...”

<https://www.csoonline.com/article/3028031/data-protection/decrypt-ssl-traffic-to-detect-hidden-threats.html>