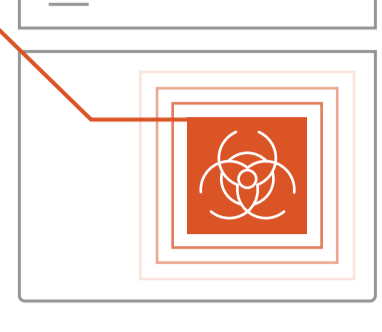


# MALICIOUS TRAFFIC

## HIDES BEHIND ENCRYPTION.

Encrypting data in motion is a necessary step towards securing sensitive data. Yet, it is an equal opportunity protector, hiding malware and other attacks just as easily as lawful activity.



## MALVERTISING & DOMAIN SHADOWING

USE SSL TO APPEAR LEGITIMATE

# 6.9 BILLION

MONTHLY VISITORS ON YAHOO!

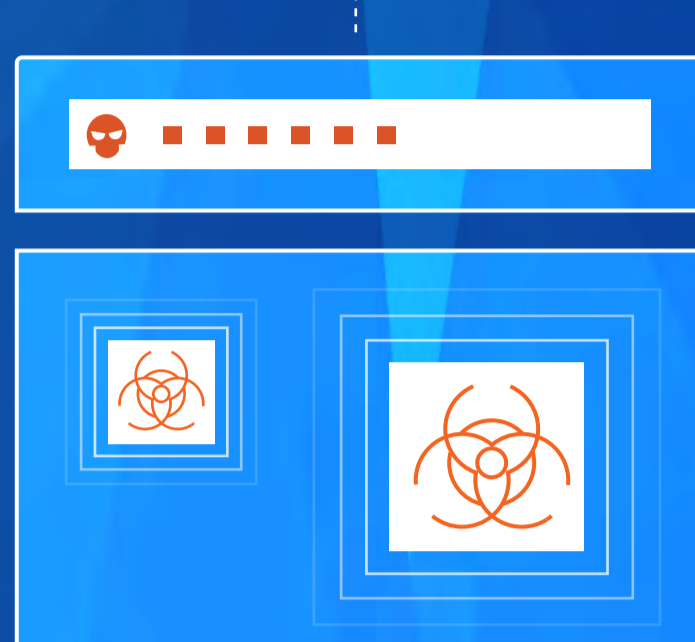
were exposed to a malvertising campaign that used Yahoo!'s own ad network to distribute malicious links.<sup>1</sup>



## DOMAIN SHADOWING

USES LET'S ENCRYPT

which provides free SSL/TLS certificates, is now being exploited to create secure, malicious subdomains tied to legitimate domains.<sup>2</sup>



## MALWARE & INSIDER THREATS

ARE USING SSL TO DISGUISE ACTIVITY

MORE THAN **50%**

OF ALL NETWORK ATTACKS

ARE USING SSL/TLS ENCRYPTION TO AVOID DETECTION AS OF 2018<sup>3</sup>



**60%**

OF COMPANIES

GO OUT OF BUSINESS WITHIN SIX MONTHS AFTER BEING VICTIM OF CYBER ATTACK<sup>4</sup>



# 197 DAYS

IS THE AVERAGE TIME IT TAKES TO DETECT A DATA BREACH.

Once identified it takes on average **69 days** to contain a breach.<sup>5</sup>



## INTRUDERS CAN AVOID DETECTION

BY USING ENCRYPTED COMMUNICATIONS

(Gmail, Yahoo!, etc.)

& SECURE CLOUD STORAGE

(Box, Dropbox, etc.)<sup>6</sup>



## MAJOR TYPES OF ATTACKS

HIDE BEHIND SSL ENCRYPTION

### RANSOMWARE

USES SSL TO HIDE ITS COMMUNICATION, DOWNLOADING ENCRYPTION KEYS AND WITHHOLDING INFECTED MACHINES' DATA UNTIL A FEE IS PAID TO OBTAIN THE KEY.

WannaCry ransomware attack was estimated to have affected **more than 200,000 computers across 150 countries**, with total damages ranging from **hundreds of millions to billions of dollars**.<sup>7</sup>

### WANNACRY

AFFECTED FEDEX, TELEFONICA, HONDA, RENAULT, PARTS OF BRITISH NATIONAL HEALTH SERVICE (NHS), RUSSIAN INTERIOR MINISTRY AND RUSSIAN TELECOM MEGAFON AMONG SEVERAL OTHERS.

## THE SOLUTION



## A10 THUNDER SSLI

The A10 Thunder<sup>®</sup> SSLI<sup>®</sup> product enables organizations to analyze all data, including encrypted data, by intercepting SSL communications and sending it to third-party security devices such as firewalls, threat prevention platforms and forensic tools for inspection.

To learn more about how A10 Thunder SSLI can help enterprises make security devices more effective please visit:

[A10NETWORKS.COM/SSLI](http://A10NETWORKS.COM/SSLI)



1. [blog.malwarebytes.org/threat-analysis/2015/08/large-malvertising-campaign-takes-on-yahoo/](http://blog.malwarebytes.org/threat-analysis/2015/08/large-malvertising-campaign-takes-on-yahoo/)  
2. [thenextweb.com/insider/2016/01/07/lets-encrypts-free-https-certificates-are-already-being-used-to-distribute-malware/](http://thenextweb.com/insider/2016/01/07/lets-encrypts-free-https-certificates-are-already-being-used-to-distribute-malware/)  
3. [www.venafi.com/blog/most-cyber-attacks-now-use-encryption-are-you-prepared-for-good-bad-and-ugly](http://www.venafi.com/blog/most-cyber-attacks-now-use-encryption-are-you-prepared-for-good-bad-and-ugly)  
4. [www.denverpost.com/2016/10/23/small-companies-cyber-attack-out-of-business/](http://www.denverpost.com/2016/10/23/small-companies-cyber-attack-out-of-business/)  
5. [securityboulevard.com/2018/07/survey-finds-breach-discovery-takes-an-average-197-days/](http://securityboulevard.com/2018/07/survey-finds-breach-discovery-takes-an-average-197-days/)  
6. [www.scmagazine.com/encryption-increasingly-used-to-hide-attacks-says-new-report/article/478532/](http://www.scmagazine.com/encryption-increasingly-used-to-hide-attacks-says-new-report/article/478532/)  
7. [en.wikipedia.org/wiki/WannaCry\\_ransomware\\_attack](http://en.wikipedia.org/wiki/WannaCry_ransomware_attack)