Cybersecurity report finds wide majority of organisations have been victimised by cyber attacks, attributes half of attacks to hidden malware in encrypted traffic

Submitted by: C8 Consulting
Tuesday, 30 August 2016

The risk to financial services, healthcare and other industries stems from growing reliance on encryption technology, says network security study from A10 Networks and Ponemon Institute

Key findings include:

• 80% of organisations were victims of cyber-attacks during past year
• Nearly half of cyber-attacks used malware hidden in encrypted traffic to evade detection
• 75% of IT experts surveyed admit malware could steal employee credentials from their networks

Reading, UK – 30th August 2016 – A surprising outcome of the growing use of encryption technology is an increase in cyber-attacks, according to a new report from A10 Networks (https://www.a10networks.com) (NYSE: ATEN), a technology leader in application networking and security. Conducted in partnership with Ponemon Institute (https://www.ponemon.org), the network security study Hidden Threats in Encrypted Traffic: A Study of North America & EMEA surveyed 1,023 IT and IT security practitioners in North America and Europe, highlighting the overwhelming challenges these professionals face in preventing and detecting attacks on encrypted traffic in and out of their organisations' networks.

A growing number of organisations are turning to encryption technology to keep their network data safe. For many security managers, however, the cost of inspecting this rising tide of encrypted traffic is degraded network performance—an incorrect assumption depending on solution and technology choice that can carry costly consequences. At issue is the fact that SSL encryption not only hides data traffic from would-be hackers, but also from common security tools. The encryption technology that is crucial to protecting sensitive data in transit, such as web transactions, emails and mobile apps, can allow malware hiding inside that encrypted traffic to pass uninspected through an organisation's security framework.

Almost half of respondents (47 percent) cited a lack of enabling security tools as the primary reason for not inspecting decrypted web traffic—closely followed by insufficient resources and degradation of network performance (both 45 percent). Yet 80 percent of survey respondents say their organisations have been victims of a cyber-attack or malicious insider during the past year. And nearly half say that the attackers used encryption to evade detection.

Although 75 percent of survey respondents say their networks are at risk from malware hidden inside encrypted traffic, roughly two-thirds admit that their company is unprepared to detect malicious SSL traffic (https://www.a10networks.com/secure), leaving them vulnerable to costly data breaches and the loss of intellectual property. Among the IT professionals responding to the survey, the largest percentage work in financial services, followed by healthcare and the public sector — three industries most in need of protecting sensitive data.

Moreover, the threat is expected to get worse as the volume of encrypted data traffic continues to grow, with the majority of respondents expecting network attackers to increase their use of encryption over the

coming year to evade detection and bypass controls. Many companies may be caught off guard, as their security solutions collapse under the weight of tremendous SSL vulnerabilities.

“IT decision makers need to think more strategically,” said Dr. Chase Cunningham, director of cyber operations at A10 Networks. “The bad guys are looking for ROI just like the good guys, and they don’t want to work too hard to get it. Instead of focusing on doing everything right 100 percent of the time, IT leaders can be more effective by doing a few things very strategically with the best technology available. It’s the cyber security equivalent of the zombie marathon — as long as you can avoid being the slowest in outrunning the zombies, you minimise risk.”

“The Hidden Threats in Encrypted Traffic study sheds light on important facts about the malicious threats lurking in today’s corporate networks,” said Dr. Larry Ponemon, chairman and founder, Ponemon Institute. “Our goal is to help organisations better understand the risks to help them better address vulnerabilities in their networks.”

-END-

Notes to editors:

About A10 Networks

A10 Networks (NYSE: ATEN) is a leader in application networking and security, providing a range of high-performance application networking solutions that help organisations ensure that their data centre applications and networks remain highly available, accelerated and secure. Founded in 2004, A10 Networks is based in San Jose, Calif., and serves customers globally with offices worldwide. For more information, visit: www.a10networks.com (https://www.a10networks.com) and @A10Networks (https://twitter.com/a10networks).

Trademarks

Media Contacts:

Paula Elliott
C8 Consulting
01189 497 736
paula@c8consulting.co.uk

Lucille Dancer
C8 Consulting
01189 497 750
lucille.dancer@c8consulting.co.uk

Tom Hindle
C8 Consulting
01189 497 763
tom.hindle@c8consulting.co.uk