Global DNS Threat Survey Report from EfficientIP estimates DNS-based attacks cost businesses more than $2M annually

Submitted by: EfficientIP
Tuesday, 27 June 2017

New research reveals global organisations gamble their business future on poorly designed network security solutions

London, UK, 27th June 2017 - EfficientIP (http://www.efficientip.com/), a leading provider of network services, today announced the results of its 2017 Global DNS Threat Survey Report (http://www.efficientip.com/resources/white-paper-dns-security-survey-2017/). It explored the technical and behavioural causes for the rise in DNS threats and their potential effects to businesses across the world. Major issues highlighted by the study in its third year, include a lack of awareness as to the variety of attacks, a failure to adapt security solutions to protect DNS and poor responses to vulnerability notifications. These concerns will not only be subject to regulatory changes, but also create a higher risk of data loss, downtime or compromised public image.

According to the report, carried out among 1,000 respondents across APAC, Europe and North America, 94% of respondents claim DNS security is critical for this business. Yet, 76% of organisations have been subjected to a DNS attack in last 12 months and 28% suffered data theft. The Global DNS Threat Survey Report also estimates the yearly average costs of the damages caused by DNS attacks to be $2.236 million (for organisations with 3,000+ employees). The leading causes were Malware (35%), DDoS (32%), Cache Poisoning (23%), DNS Tunnelling (22%) or Zero-Day Exploits (19%).

“The results once again highlight that despite the evolving threat landscape and the increase in cyber-attacks, organisations across the globe and their IT departments still don’t fully appreciate the risks from DNS-based attacks,” said David Williamson, CEO at EfficientIP. “In less than a year, GDPR will come into effect, so organisations really need to start rethinking their security in order to manage today’s threats and save their business from fines of up to £20 million or 4% of global revenue."

Globally, the results varied widely. 39% of respondents from the UK and US demonstrated more awareness of the top 5 DNS-based attacks than Spain (38%), Australia (36%), Germany (32%) and France (27%), but less than India (50%) and Singapore (47%). In the UK, the attacks organisations are the most aware of include: DNS-based Malware (52%), DDoS (43%), DNS Tunnelling (39%), Cache Poisoning (34%) and Zero-Day Exploits (28%).

Other key UK findings include:

- A quarter of organisations have been subjected to DDoS (26%) with 41% of those over 5Gb/sec, Cache Poisoning (25%) or Zero-Day attacks (25%) in the past year while almost a third have been vulnerable to Phishing (32%) or DNS-based Malware (29%) attacks.
- Almost a third (29%) of organisations surveyed experienced Data Exfiltration via DNS. Of those, 16% had sensitive customer information stolen and 15% intellectual property stolen. This could be social security numbers, job assignments or even bank details.
- A third (34%) stated they have experienced more than five attacks in the last 12 months.
- By taking the measure of closing down affected applications to mitigate an attack, 38% of

organisations achieved what the attacker intended to do.
For 50% of those who experienced a DNS attack, it took more than six hours, almost a full business day to mitigate it, requiring more than four members of staff in 34% of cases which for many organisations may be their entire network security team.
Most worryingly, many believe they are protected, but they are not. Almost all organisations (99%) in the UK did not apply the necessary security patches, compare to 83% globally.

Recommendations from the report
The following steps can be taken by organisations to ensure continuity of service and data protection for them, their users and clients:

1. Replace useless firewall and load balancers with purpose-built DNS security technology
2. Keep their DNS security up to date by patching DNS servers more often
3. Enhance their threat visibility by using deep DNS transaction analysis

The 2017 Global DNS Threat Survey report
The report was conducted by Coleman Parkes from February to March 2017. The results are based on 1,000 respondents in three regions. Respondents included CISOs, CIOs, CTOs, IT Managers, Security Managers and Network Managers.

To read the full report please visit:
http://www.efficientip.com/resources/white-paper-dns-security-survey-2017/ (http://www.efficientip.com/resources/white-paper-dns-security-survey-2017/)

About EfficientIP

As one of the world's fastest growing DDI vendors, EfficientIP helps organisations drive business efficiency through agile, secure and reliable network infrastructures. Its unified management framework for DNS-DHCP-IPAM (DDI) and network configurations ensures end-to-end visibility, consistency control and advanced automation. Additionally, its unique 360° DNS security solution protects data confidentiality and application access from anywhere at any time. Companies rely on EfficientIP to help control the risks and reduce the complexity of challenges they face with modern key IT initiatives such as cloud applications, virtualization, and mobility.

Institutions across a variety of industries and government sectors worldwide depend on its offerings to assure business continuity, reduce operating costs and increase the management efficiency of their network and security teams. For further information, please visit: www.efficientip.com

PRESS CONTACT:
Florie Lhuillier / Verena Franco
Positive Marketing
0203 637 0632
efficientip@positivemarketing.com