efficient iP™
DEFINING SMART DDI

Press Release

EfficientIP DNS Threat Report reveals the cost per attack has increased by 57% to $715,000 for organizations globally

- 2018 research ushers a new era of network attacks

PARIS -- May 16, 2018 -- EfficientIP, a leading specialist in DNS security to ensure service continuity, user protection and data confidentiality, today announced the results of its 2018 Global DNS Threat Report. It explored the technical causes and behavioral responses towards DNS-based threats and their potential effects on businesses across the world. Over the past year, organizations on average faced seven DNS attacks, which cost some businesses more than $5 million in damages.

The major issues highlighted by the study in its fourth year include the increase in cost of DNS attacks, the evolving popularity of attacks, a failure to adapt security solutions to protect DNS on-premise or in the cloud and investment priorities to ensure data confidentiality. The consequences of not securing the DNS creates a higher risk of data loss, service downtime, compliance failure or compromised public image.

David Williamson, CEO of EfficientIP summarized the research, saying, “Worryingly, the frequency and financial consequences of DNS attacks have risen and businesses are late in implementing purpose-built security solutions to prevent, detect and mitigate attacks. On the positive side, business and IT leaders globally now have a better understanding on why DNS is fundamental to ensuring business continuity and data confidentiality, so securing DNS has become a top priority for them.»

The increasing cost per attack - varies country by country

More than three-quarters (77%) of organizations surveyed were subject to a DNS attack in 2018. The global average cost per DNS attack increased by 57% year-on-year, standing at $715,000. However, the cost per attack and its growth vary country by country.

A regional overview of cost per DNS attack shows in Europe, UK respondents witnessed the highest year-on-year increase in cost per DNS attack at 105%, whereas French organizations had the highest cost at $974,000. In North America, USA organizations faced the highest cost at $654,000 and the highest cost increase at 82%. In Asia-Pacific, Singapore had the highest cost at $710,000 per attack as well as the highest cost increase at 85%.

The five most popular DNS-based attacks in 2018

The most popular DNS threats has changed compared with last year. DNS-based malware has remained the joint most popular alongside Phishing (36%), followed by DDoS attacks (20%), Lock-up Domain attacks (20%) and DNS Tunneling (20%).

The top impacts of DNS-attacks, damaging reputation and the bottom line

Well-publicized cyber attacks such as WannaCry and NotPetya caused financial and reputational damage to organizations across the world. The impact caused by DNS-based attacks is as important due to its mission-critical role. Two-in-five (40%) organizations suffered cloud outages and one-third (33%) of respondents were victims of data theft. One-in-five (22%) businesses had lost business due to DNS attacks.

Organizational investments on GDPR compliance, DNS protection is the priority

With less than 10 days to go to the EU GDPR deadline on 25th May 2018, organizations are investing to comply with the new data protection regulation which has a global remit. DNS is recognized as a prime target for data exfiltration.

To ensure data confidentiality, respondents are prioritizing technology investment on the monitoring and analysis of DNS traffic (38%) over conventional security solutions such as firewalls (21%) and endpoint protection (35%). EU GDPR has been framed around the location of the data subject, rather than the data controller or data processor, leading to a global impact. This is reflected in the investment for GDPR compliance as organizations based outside the EU have spent over $1 million on average. US organizations have spent more on average at $1,417,000 than some EU member counterparts such as the UK ($1,165,000) and Spain ($1,223,000). German businesses lead the European and global rankings with each spending $1,752,000 on average. In Asia-Pacific, Singaporean businesses lead the way with each spending $1,361,000 on average.

EU GDPR has been framed around the location of the data subject, rather than the data controller or data processor, leading to a global impact. This is reflected in the investment for GDPR compliance as organizations based outside the EU have spent over $1 million on average. US organizations have spent more on average at $1,417,000 than some EU member counterparts such as the UK ($1,165,000) and Spain ($1,223,000). German businesses lead the European and global rankings with each spending $1,752,000 on average. In Asia-Pacific, Singaporean businesses lead the way with each spending $1,361,000 on average.

ABOUT EFFICIENTIP

As one of the world’s fastest growing DDI vendors, EfficientIP helps organizations 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 rely on EfficientIP 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

USA
EfficientIP Inc.
1 South Church Street
West Chester, PA 19382
+1 888-228-4655

EUROPE
EfficientIP SAS
90 Boulevard National
92250 La Garenne Colombes
FRANCE
+33 1 75 84 88 98