39% of EU businesses suffering data theft, and paying €734,000 per DNS attack

Submitted by: EfficientIP

Tuesday, 12 June 2018

EfficientIP 2018 DNS Threat Report proves European organizations suffer most from global network attacks

Paris, France - Tuesday 12th June 2018 - EfficientIP, a leading specialist in DNS security to ensure service continuity, user protection and data confidentiality, revealed the European results of its 2018 DNS Threat Report. The research explored the technical causes and behavioral responses towards DNS-based threats and their potential effects on businesses across the world. Globally, 77% of organizations faced DNS attacks in the past year with each attack costing European businesses an average of €734,000. The consequences of not securing DNS increases the risk of data loss, service downtime, compliance failure or compromised public image.

David Williamson, CEO of EfficientIP summarized the research, saying, “New regulation made it necessary for every organization to ensure the data they keep is secure. Surprisingly, our research shows European organizations have invested the least globally in technology, which can prevent data theft. This could be a reason as to why the region had the most data stolen. In the year ahead, it will be interesting to see how European companies will prevent data theft and avoid regulatory fines."

DNS attacks cost European businesses the most

DNS is the gateway to every corporate network and malicious actors are targeting it as a way to steal sensitive information. The research shows the average cost per DNS attack for European organizations has risen by 43% over the past year to €734,000, much higher than their North American and Asia Pacific counterparts. French organizations had the highest cost per attack at €847,000 and the UK had highest cost increase at 105% to €684,000. German organizations have reduced the impact of DNS attacks over the last year, increasing only by 15% this year.

Attacks dent revenue, but cloud services are better protected

On average, European companies suffered the most data theft at 39%, higher than the global average at 33%. Nearly half of French organizations admitted to losing sensitive data (48%) and UK companies suffered the least in the region at 32%. A third of European organizations had their websites compromised, with nearly half (48%) of Spanish organizations admitted to website downtime. A quarter (25%) of French organizations suffered loss of business as a consequence of DNS attacks.

European organizations are more effective than their global peers at protecting their cloud services. On average, a third (34%) of European businesses suffered cloud downtime, lower than the global average at 40%. Within the region, France has the most cloud outages due to DNS attacks at 41%, whereas Germany was the lowest at 28%.

DNS-based malware most prevalent in Europe

The top five DNS-based attacks in Europe reflect the global top five, with DNS-based malware (39%) being the most popular attack faced in the region, followed by phishing at 34%, DNS DDoS attacks at 20%, DNS tunneling at 19%, domain lock-up at 18%. DNS-based malware were more prevalent than anywhere else in world, with Germany facing the most attacks at 44%. Spanish organizations faced more DNS tunneling attacks at 24% than their European peers.

European businesses underinvest in keeping data confidential

DNS is recognized as a prime target for data exfiltration. Protecting the DNS requires monitoring and analysis of traffic to identify threats once they enter the corporate network. Conventional end-point and firewall technologies primarily focus on protecting the perimeter of every corporate network, therefore they are redundant once the threat moves inside.

European companies prioritized investment in securing network endpoints (38%), the monitoring and analysis of DNS traffic at 36%, and followed by firewalls at 20%. It’s positive to see DNS investment move into the top three, but more can be done in this area, and it maybe why European organizations had the most data stolen within the last year.

[ENDS]

Notes to Editors
The 2018 Global DNS Threat Report
The report was conducted by Coleman Parkes from January to April 2018. The results are based on 1,000 respondents in three regions - 300 respondents in North America, 400 respondents in Europe and 300 respondents in Asia Pacific. Respondents included CISOs, CIOs, CTOs, IT Managers, Security Managers and Network Managers.

Want to learn how to ensure business continuity and data confidentiality?
Download the full report (http://www.efficientip.com/resources/dns-security-survey-2018/)

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 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: http://www.efficientip.com.

Press contact

Positive Marketing for EfficientIP
Charles Parant|Sam Ashcroft
efficientip@positivemarketing.com
(0)203 637 0646

Distributed via Press Release Wire (https://pressreleases.responsesource.com/) on behalf of EfficientIP