Average DNS Attack Cost Rises 49% to $1,070,000

New EfficientIP report, in partnership with IDC, shows 34% increase in attacks

Tuesday, 18th June 2019 - Paris, France - EfficientIP, a leading specialist in DNS security for service continuity, user protection and data confidentiality, today announced the results of its 2019 Global DNS Threat Report, sponsored research conducted by market intelligence firm IDC.

Over the past year, organizations faced on average more than nine DNS attacks, an increase of 34%. Costs too went up 49%, meaning one in five businesses lost over $1 million per attack and causing app downtime for 63% of those attacked. Other issues highlighted by the study, now in its fifth year, include the broad range and changing popularity of attack types, ranging from volumetric to low signal, including phishing, 47%, malware-based attacks, 39%, and old-school DDoS, 30%.

Also highlighted were the greater consequences of not securing the DNS network layer against all possible attacks. No sector was spared, leaving organizations open to a range of advanced effects from compromised brand reputation to losing business.

Romain Fouchereau, Research Manager European Security at IDC, says *"With an average cost of $1m per attack, and a constant rise in frequency, organisations just cannot afford to ignore DNS security and need to implement it as an integral part of the strategic functional area of their security posture to protect their data and services."*

DNS is a central network foundation which enables users to reach all the apps they use for their daily work. Most network traffic first goes through a DNS resolution process, whether this is legitimate or malicious network activity. Any impact on DNS performance has major business implications. 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.

The top impacts of DNS attacks — damaged reputation, business continuity and finances (See Figure 1 in 'Detailed Findings')
Three-in-five, 63%, of organizations suffered application downtime, 45% had their websites compromised, and one-quarter, 27%, experienced business downtime as a direct consequence. These could all potentially lead to serious NISD (Network and Information Security Directive) penalties. In addition, one-quarter, 26%, of businesses had lost brand equity due to DNS attacks.

Data theft via DNS continues to be a problem. To protect against this, organizations are prioritizing securing network endpoints, 32%, and looking for better DNS traffic monitoring, 29%.

David Williamson, CEO of EfficientIP summarized the research *"While these figures are the worst we have seen in five years of research, the good news is that the importance of DNS is at last being widely recognized by businesses. Mainstream organizations are now starting to leverage DNS as a key part of their security strategy to help with threat intelligence, policy control and automation, thus building a good foundation for their zero trust plan."*

[ENDS]

Detailed Findings follow.

Notes to Editors
The 2019 Global DNS Threat Report
The research was conducted by IDC from January to April 2019. The results are based on 904 respondents in three regions - North America, Europe and Asia Pacific. Respondents included CISOs, CIOs, CTOs, IT Managers, Security Managers and Network Managers.

To read the full report please click here.

About EfficientIP
EfficientIP is a network automation and security company, specializing in DNS-DHCP-IPAM solutions (DDI), with the goal of helping organizations worldwide drive business efficiency through agile, secure and reliable infrastructure foundations. Integrated solutions enable IP communication and simplify network management with end-to-end visibility and smart automation, while patented technology secures DNS services to safeguard data and ensure application access. Companies in all sectors rely on EfficientIP offerings to face the challenges of key IT initiatives such as cloud applications and mobility. For further information, please visit: https://www.efficientip.com.

Press contact
Positive Marketing for EfficientIP
Jordan Ratcliffe | Camilla Holroyd
efficientip@positivemarketing.com
0203 637 0640

Detailed Findings

The increasing cost per attack - varies country by country
(See Figure 2)
More than three-quarters, 82%, of the organizations surveyed were subject to a DNS attack. The global average cost per DNS attack increased by 49% year-on-year, to $1.07M, and was highest in Europe at $1,190,200. 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 108% and also the highest cost at $1,635,400. In North America, USA organizations faced the highest cost at $1,127,200 but Canadian organizations had the highest cost increase at 80%. In Asia-Pacific, Singapore had the highest cost at $924,750 per attack as well as the highest cost increase at 30%.

The five most popular DNS-based attacks in 2019
(See Figure 3)
The most popular DNS threats have changed compared with last year. Phishing, 47%, is now more popular than last year's favorite DNS-based malware, 39%, followed by DDoS attacks, 30%, False positive triggering, 26%, and Lock-up domain attacks, 26%.

No industry is safe from DNS attacks
Utilities is the sector with the highest cost per attack, 25% of attacks costing over $1.1M. Financial services was the most-targeted of any industry with 88% hit last year. Retail by comparison saw the highest business loss, 35%, particularly worrying in the current high street climate. Half of all healthcare organizations, 50%, had their website compromised in an attack, reducing patient access to online resources. Worryingly governments had the highest occurrence of sensitive information being stolen, 19%, and also took the longest to patch vulnerabilities, 74% taking two days or more.

Data Privacy & Compliance, One Year After GDPR
(See Figure 4)
Since May of last year GDPR regulation has been enforced with important investments having been made by organizations in all countries, notably in strengthening network security defenses.

One year on, organizations are focused on investing in analysis to improve security. Securing network endpoints, 32%, and better monitoring of DNS traffic, 29%, are where respondents see the most effective solutions to data confidentiality risks, over and above adding firewalls, 22%.

In addition to improving security, organizations also see other improvements from GDPR and other data privacy compliance initiatives (CLOUD Act, PDPA, etc.). These have been

beneficial in educating employees on data privacy, 81%, putting it on par with network security upgrades and innovation, 79%, and above heightening customer trust, 64%.

Zero Trust in the Spotlight

Security challenges brought by digital transformation, multi-cloud deployments, and mobility are causing perimeter network security to evolve to a zero-trust mindset. DNS security, fueled by threat intelligence and network automation, is key to a successful zero-trust strategy.

The research showed that 48% of organizations are planning to use zero-trust architecture, and 45% use predictive analytics. However, there is much room for improvement on the automation side as only 14% have adopted automation for their network security policy management.

[ENDS]

See Index below for data.

Index

Figure.1 'Top Impacts'

The top impact of attacks of DNS-based attacks in 2019	
In-house application downtime	63%
Loss of business	27%
Brand damage	26%

Figure.2 'Increasing Cost'

Increasing cost per attack, country by country			
	Country	Cost per attack in 2019 report	Cost per attack increase from 2018 report
1	UK	$1,635,400	105%
2	USA	$1,127,200	72%
3	Germany	$1,050,800	16%
4	France	$1,050,000	8%
5	Canada	$982,500	80%
6	Spain	$970,400	37%
7	Singapore	$924,800	30%
8	India	$835,500	27%

Figure.3 'Most Popular DNS-based attacks'

Top five DNS-based attacks suffered in 2019	
Phishing	47%
DNS-based malware	39%
DNS DoS/DDoS	30%
False positive triggering	26%
Lock-up domain attacks	26%

Figure. 4 'Data Privacy and Compliance'

Top Technology Investment to ensure data confidentiality

Securing network endpoints	32%
Better monitoring and analysis of DNS traffic	29%
Adding more firewalls	22%
Increasing the number of filtering rules	7%