efficient iP®

Press Release

# Enterprises Plagued by DNS Attacks: Organisations suffering seven attacks a year, costing $942,000 per attack

*New research reveals the impact of DNS attacks on global organisations, with 7 in 10 enterprises experiencing application downtime*

**Paris, France -- June 1, 2022** -- EfficientIP, the specialist in DDI security and automation (DNS, DHCP, IPAM), has today announced the findings of its eighth annual '2022 Global DNS Threat Report', conducted by leading market intelligence firm IDC. The research, commissioned by EfficientIP, reveals the damaging impact Domain Name System (DNS) attacks have had on global organisations' operations over the past 12 months. The report uncovers how despite 73% of organisations knowing that DNS security is critical to their business, cyber criminals are still infiltrating the network and causing significant business disruption, resulting in the shutdown of cloud and on-premise applications and theft of data.

As enterprises continue to strike a balance between supporting remote workers and mitigating the network security risks posed by the rise in hybrid work models and reliance on cloud applications, the results show that 88% of organisations have experienced one or more DNS attacks on their business. Each successful attack costs the business, on average, $942,000. Securing the DNS and ensuring the integrity of the network so that threats are detected and mitigated before they propagate becomes even more critical to guaranteeing continuous business operations, with organisations detailing how they have, on average, been hit by seven attacks in the past 12 months.

A DNS attack does not just result in an inconvenient business disruption but can be a costly expense for organisations. In the past 12 months, APAC has become the region with the highest average cost of a successful attack at $1,036,040, an increase of 14% when compared to 2021, while EMEA and North America's average cost of successful attack has decreased by 4% and 7% respectively. Malaysia (21%), Germany (18%) and both India and the UK (14% each) experienced the highest increase in the cost of an attack, while Spain saw its cost of damages plummet by almost half (48%) when compared to 2021. France and the US were the only other countries that saw a decline in the average cost with 21% and 5% respectively.

Cybercriminals are continuing to use all available tools to gain access to networks, disrupt the business and steal data by specifically targeting the hybrid workforce, with DNS-based attacks becoming increasingly pervasive across all industries. In the last year, 70% of organisations suffered with in-house and cloud application downtime, with the average time to mitigate these threats increasing to 6 hours and 7 minutes, meaning that employees, partners, and customers were unable to access any services. The top five DNS-based attacks experienced by organisations are; Phishing (51%), Malware (43%) DDoS (30%) DNS tunnelling (28%) and hijacking/credential attack (28%).

Jean-Yves Bisiaux, CTO and co-founder of EfficientIP commented: "Weaponizing the DNS is crucial. DNS is a critical foundation to any organisations' network security strategy, yet each year we keep seeing the same alarming trends and data, revealing that organisations aren't taking these risks seriously. In an era where we all expect a hybrid environment so that we can work from anywhere, business leaders should now be insisting that this environment is secure against hackers who are continuing to take advantage of this weak spot in defences. DNS does not need to be an organisation's Achilles heel; it should be the backbone of a resilient network security strategy designed to keep attackers firmly on the outside."

Maintaining DNS resiliency to secure networks, applications and data are always available and accessible is key for enterprises that want to maintain operations and protect their reputation among customers, partners, and employees. With an increased reliance on cloud-based services and applications, the risk of downtime can be even more catastrophic for organisations if they are taken 'offline'. 56% of respondents acknowledge that DNS is a critical component of their cloud strategy, helping to build in resilience and intelligently direct app traffic to ensure availability and improve the user experience. In the last year, 44% of organisations were hit by cloud service downtime and 27% suffered a DNS attack that abused a cloud misconfiguration. These impacts can be mitigated by using automation as part of the DNS solution to enable the provisioning and deprovisioning of IP resources and eliminating the risk of misconfigurations.

Additional key findings from the research include:

- 43% of organisations do not use a security solution built into a DNS server and 62% are still not using auto-remediation to ensure the security of the services.
- Almost a quarter (24%) had Intellectual Property (IP) or sensitive data stolen as a result of a DNS attack.
- 43% of respondents were victims of Ransomware
- Despite the risks posed by employees accessing unsanctioned cloud applications, 61% have not made Shadow IT a priority for its business in 2022. DNS has been proven as a primary solution to detect shadow IT in 51% of organisations.

"The continued rise of digital transformation projects, which have been significantly accelerated in the past two years, and the adoption and migration to multi-cloud infrastructures while supporting an increasingly remote workforce, has caused greater complexity for IT security teams" says Romain Fouchereau, Research Manager European Security at IDC. "We know that organisations recognise the importance of leveraging DNS capabilities to mitigate attacks, yet there are still weak spots in cyber defences as attackers continue to diversify and deploy new attack techniques to infiltrate businesses and inflict damage. Effective DNS tools and a proactive security strategy will ensure business continuity and greater agility and visibility when supporting the hybrid workforce."

The research, commissioned by EfficientIP and conducted by market intelligence firm International Data Corporation (IDC), surveyed CISOs, CIOs, CTOs, IT Managers, Security Managers and Network Managers from companies with 500 or more employees across North America, Europe, and Asia Pacific.

To download a copy of the IDC Infobrief 'The 2022 Global DNS Threat Report', sponsored by EfficientIP, please click HERE

**About EfficientIP**

EfficientIP is a network automation and security company, specialising in DNS-DHCP-IPAM (DDI) solutions. Their goal is to help organisations across all industries improve operational efficiency through agile, secure, and reliable infrastructure foundations. The company's solutions simplify network management with end-to-end visibility and intelligent automation, while patented DNS technology protects against malware, secures access to applications and optimises application performance. Companies around the world rely on EfficientIP offerings to meet the IT challenges of their digital transformation. For more information, please visit www.efficientip.com

**Press Enquiries**

Kim Smith

Press Release

Code Red Communications for EfficientIP
EfficientIP@CodeRedComms.com
T: +44 (0) 1276 486000