

Cyber attacks leave Telcos on hold for two days

Submitted by: Positive Marketing

Wednesday, 21 November 2018

EfficientIP's 2018 DNS Threat Report reveals telecom organizations took average of 18 hours to mitigate each attack

London, 21 November 2018: EfficientIP, a leading specialist in network security, today revealed in its 2018 Global DNS Threat Report (<http://www.efficientip.com/resources/dns-security-survey-2018/>) that the telecommunications sector ranks as one of the worst businesses sectors in its handling of cyber threats. The report revealed that 43% of telco organizations suffered from DNS-based malware over the past 12 months. The report also highlighted 81% took three days or more to apply a critical security patch after notification.

Time & Money

DNS attacks cost telco organizations significant time and money. According to this year's report, telcos took too long to mitigate an attack, requiring an average of 3 employees to collectively spend over 17 hours per attack. Due to how time-intensive the mitigation process can be, the average cost per DNS attack is rising for the telco sector. Last year, a single DNS attack cost a telco organization \$622,100. This year the research shows telcos lose an average of \$886,560 from each DNS attack, an increase of 42% in just 12 months.

Commenting on the reason behind these attacks, David Williamson, CEO of EfficientIP states:

"Telco organizations attract complex, sophisticated cyber attacks as they hold sensitive customer data, and are also critical for providing unified communication services to businesses. With a large part of their customer base operating online, strong network security has become a business necessity for the entire telco sector in general. Ensuring consistency and reliability in service is a crucial step towards providing elevated customer satisfaction."

Brand Erosion

The 2018 Global DNS Threat Report also revealed the ramifications on telcos' brands while undergoing cyber attacks. Brand reputation was likely to suffer due to service issues:

45% had to close down specific affected processes and connections.

38% suffered cloud service downtime.

33% reported a compromised website.

31% endured in-house application downtime.

30% reported sensitive customer information stolen.

Recommendations for telcos

Working with some of the world's largest telecommunication brands such as Orange and Vodafone to protect their networks, EfficientIP recommends five best practices:

Rethink and simplify DNS architectures by replacing intermediary security layers with an adapted DNS security solution (<http://www.efficientip.com/resources/dns-security-survey-2018/>).

As well as reducing administration and maintenance costs, this helps guarantee availability of service.

Augment your threat visibility using real-time, context-aware DNS transaction analytics for behavioral threat detection. Businesses can detect all threat types, and prevent data theft to help meet regulatory compliance such as GDPR and US CLOUD Act.

Apply adaptive countermeasures relevant to threats. The result is ensured business continuity, even when the attack source is unidentifiable, and practically eliminates risks of blocking legitimate users.

Decentralize DNS architecture to cope with heavy growth of traffic. In addition to enhancing user experience, placing purpose-built, high performance DNS servers in points of presence significantly improves security against DDoS attacks.

Incorporate DNS into a global network security solution to recognize unusual or malicious activity and inform the broader security ecosystem. This allows holistic network security to address growing network risks and protect against the lateral movement of threats.

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 - North America, Europe and Asia Pacific. Respondents included CISOs, CIOs, CTOs, IT Managers, Security Managers and Network Managers. 96 telco organizations were interviewed across 9 countries for the survey.

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. We enable IP communication and simplify network management with end-to-end visibility and smart automation, while our patented technology secures DNS services to safeguard data and ensure application access. Companies in all sectors rely on our offerings to face the challenges of key IT initiatives such as cloud applications and mobility. For further information, please visit: [<http://www.efficientip.com/http://www.efficientip.com/>].

Press contacts

Positive Marketing for EfficientIP

(UK)

Eisha Sharma|Jordan Ratcliffe

efficientip@positivemarketing.com

+44 (0)203 637 0643