EfficientIP: New Data Shows How Healthcare Suffered from Cyberattacks More than Other Industries During Pandemic

Cost per DNS attack increased by 12% in healthcare, the sharpest rise; healthcare also most likely industry to suffer other non-monetary types of damages, such as application downtime

July 8, 2021 -- PARIS: A new report from EfficientIP and International Data Corporation (IDC) shows how the healthcare industry experienced devastating effects from DNS attacks during the COVID-19 pandemic, more so than other industries. The 2021 Global DNS Threat Report shows that the average cost per attack in healthcare increased to $862,630, a rise of 12% from last year and the sharpest increase seen by any industry.

The Threat Report shows that healthcare is more vulnerable than other industries to a variety of consequences from attacks: Healthcare is the most likely industry to suffer application downtime, with 53% of healthcare companies in the survey reporting that. Healthcare also saw the highest rate of compromised websites at 44% and the highest rate of brand damage at 31%. During a time when the health industry is already experiencing other stressors related to the pandemic, downtimes in apps and services or cloud accessibility could have heavy consequences for both patients and providers.

Other negative effects include cloud service downtime (46%), loss of business (34%), and stolen customer information (23%) -- up from 13% last year. Customer information is particularly sensitive in the healthcare sector, which makes it an attractive target--particularly so during a time of high-stress for the industry.

“We all knew that the healthcare industry would be a prime target for cyberattacks during the pandemic,” says Ronan David, VP of Strategy for EfficientIP, “But it really is fascinating--and useful--to see the data in black and white. Fascinating because we finally have a clear quantitative picture, and useful because we see where companies like EfficientIP can help healthcare companies improve their defenses.”

Healthcare suffered an average of 6.71 DNS attacks over a 12-month period, and it took an average 6.28 hours to mitigate each attack, which is higher than the all-industry average of 5.62 hours.

The most common DNS attack type in healthcare, like many other industries, is phishing; 49% of the healthcare companies surveyed experienced a phishing attack, which matches the average for all industries. DNS-based malware is also popular in healthcare at 36%, as is DNS tunneling at 29% and DNS domain hijacking at 28%. Compared to the all-industry average, healthcare saw relatively low rates of things like DDoS attacks (the all-industry average was 29% while the healthcare average was 19%). The consequences of attacks on healthcare infrastructure can be extreme, directly affecting patient care and well-being.

This makes defense strategies incredibly important. In order to protect themselves, healthcare companies have turned both to Zero Trust and to smarter DNS security. The Threat Report shows that the healthcare industry is planning, implementing or running Zero Trust initiatives more than other industries (79%, compared to an all-industry average of 75%), and is the strongest believer that DNS domain deny-and-allow lists are valuable for Zero Trust (82%, compared to 79%).

Like many industries, healthcare sees DNS security as critical for protecting a remote workforce (54% of healthcare companies surveyed agreed with that statement). A full 78% agreed that DNS security was a critical component of network architecture. 27% of healthcare companies put better monitoring and analysis of DNS traffic as their top priority for preventing data theft.

For more on the impact of DNS attacks on healthcare and how companies can shore up their defenses, please read the full report.The 2021 Global DNS Threat Report is available online at www.efficientip.com/resources/idc-dns-threat-report-2021/.

efficient iP™

As one of the world’s fastest growing DDI vendors, EfficientIP helps organizations drive business efficiency through agile, secure and reliable network infrastructures. Our unified management framework for DNS-DHCP-IPAM (DDI) and network configurations ensures end-to-end visibility, consistency control and advanced automation. Additionally, our unique 360° DNS security solution protects data confidentiality and application access from anywhere at any time. Companies rely on us 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 our offerings to assure business continuity, reduce operating costs and increase the management efficiency of their network and security teams.

Copyright © 2021 EfficientIP, SAS. All rights reserved. EfficientIP and SOLIDserver logo are trademarks or registered trademarks of EfficientIP SAS. All registered trademarks are property of their respective owners. EfficientIP assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document.