US Signal ‘State of Web and DDoS Attacks’ Survey Reveals that 83 Percent of Organizations Have Been Hit with a DDoS Attack in the Last Two Years

US Signal, today released its 2019 State of Web and DDoS Attacks survey. The study revealed that a staggering 83 percent of organizations have experienced a DDoS attack within the last two years, and more than half of them experienced multiple.

GRAND RAPIDS, Mich. (PRWEB) July 24, 2019 -- US Signal, a leading data center services provider, today released its 2019 State of Web and DDoS Attacks survey. The study—which included data derived from more than 100 IT decision makers in U.S.-based companies with up to 750 employees—revealed that a staggering 83 percent of organizations have experienced a DDoS attack within the last two years, and more than half of them experienced multiple.

The majority of these organizations also stated that, on average, a DDoS attack caused 12 hours of downtime, and a further 30 percent said that it caused around 20 hours of downtime. These periods of downtime have major negative impacts on companies. More than a third of those surveyed considered revenue loss the most dire consequence caused by DDoS attacks. Other impacts reported by respondents included a decrease in IT staff productivity (34 percent) and reputational damage (20 percent). Despite this, 17 percent of the respondents did not have, or were not sure if they had a DDoS protection provider or tool.

The survey also showed that 81 percent of respondents had experienced a cyberattack on their web applications in the past two years, and nearly half experienced several cyberattacks. It went on to discover that the average financial impact of affected companies’ most recent cyberattacks totaled to approximately $152,000. Despite this, 91 percent of respondents still consider their website and application security performance to be satisfactory, with nearly 3 in 5 saying it’s highly satisfactory.

To combat these threats, many respondents are turning to managed service providers to help implement, monitor and maintain a mixture of cybersecurity technologies, including cloud-based firewalls (73 percent), DDoS protection (71 percent) and email security (62 percent). In addition, 97 percent of participating organizations scan and test for vulnerabilities within their web applications.

“The number of respondents that have experienced DDoS and application attacks is jarring, demonstrating that there is always room for improvement in keeping up with modern cyberthreats. While the survey showed that there is a clear culture of investing in IT security solutions across organizations, there seems to be a need for more robust security tools and managed services to help resource-strapped technical teams,” said Trevor Bidle, vice president of Information Security and compliance officer, US Signal. “The reputational and financial damage that an online attack can cause a company is immense, and we hope security vendors and service providers can use this data to enhance their offerings and further protect their customers’ websites and applications.”


About US Signal
US Signal is a provider of data center services, offering connectivity, cloud hosting, colocation, data protection,
and disaster recovery solutions – all powered by its wholly owned and operated, robust, fiber network. US Signal also helps customers optimize their IT resources through managed and professional services.
Contact Information
Alyssa Pallotti
Touchdown PR
http://www.touchdownpr.com
5123738500

Online Web 2.0 Version
You can read the online version of this press release here.