FOR IMMEDIATE RELEASE

Media Contact:
John Gates
Elevate Communications
o-617.861.3651, c-617.548.8972
corero@elevatecom.com

Loss of Customer Trust and Decreased Revenues Most Damaging Consequences of DDoS Attacks According to IT Security Pros and Network Operators

Corero Network Security Releases Second Annual DDoS Impact Study; Highlights Current Business Trends for Handling DDoS Threats and Market Demand for Protection Services from Internet Service Providers

HUDSON, MA – March 23, 2016 – What is the most damaging consequence of DDoS attacks to businesses? Losing the trust and confidence of your customers, according to nearly half of IT security professionals participating in Corero Network Security's (LSE: CNS) second annual DDoS Impact Survey, which was released today by the company. The industry study polled technology decision makers, network operators and security experts attending the recent 2016 RSA Conference about key DDoS issues and trends that Internet service providers and businesses face in 2016.

"Network or website service availability is crucial to ensure customer trust and satisfaction, and vital to acquire new customers in a highly competitive market," said Dave Larson, COO at Corero Network Security. "When an end user is denied access to Internet-facing applications or if latency issues obstruct the user experience, it immediately impacts the bottom line."

Nearly half (45 percent) of the IT security professionals who responded said loss of customer trust and confidence were the most damaging consequences of DDoS attacks for their businesses, while 34% said lost revenues were the worst effect.

DDoS attacks get the most attention when a firewall fails, service outage occurs, a website goes down or customers complain, but Larson warns that companies should be concerned about DDoS attacks even when the attacks are not large-scale, volumetric attacks that saturate a company's network and associated server infrastructure. Approximately one third (32%) of survey respondents indicated that DDoS attacks on their network occur weekly or even daily. "That is a troubling, yet not surprising, statistic because DDoS attacks are incredibly inexpensive to create, and relatively easy to deploy," said Larson.

"Industry research, as well as our own detection technology, shows that cyber criminals are increasingly launching low-level, small DDoS attacks," said Larson. "The problem with such attacks is two-fold: small, short-duration DDoS

attacks still negatively impact network performance, and—more importantly, such attacks often act as a smokescreen for more malicious attacks. While the network security defenses are degraded, logging tools are overwhelmed and IT teams are distracted, the hackers may be exploiting other vulnerabilities and infecting the environment with various forms of malware."

Larson noted that small DDoS attacks often escape the radar of traditional scrubbing solutions. Many organizations have no systems in place to monitor DDoS traffic, so they are not even aware that their networks are being attacked regularly.

The survey also asked participants about their current methods of handling the DDoS threat; nearly one third (30%) of respondents rely on traditional security infrastructure products (firewall, IPS, load balancers) to protect their businesses from DDoS attacks. "Those companies are very vulnerable to DDoS attacks because it's well-documented that traditional security infrastructure products aren't sufficient to mitigate DDoS attacks," said Larson.

Interestingly, 30% of respondents currently rely on their upstream service providers to eliminate the attacks, yet an overwhelming majority (85%) of respondents indicated they believe upstream Internet Service Providers should offer additional security services to their subscribers to remove DDoS attack traffic completely. Furthermore, 51% responded that they would be willing to pay their Internet Service Provider(s) for a premium service that removes DDoS attack traffic before it is delivered to them, and 35% indicated they would allocate 5-10% of their current ISP spend to subscribe to this type of service.

"Clearly the majority of organizations need and are willing to pay for a service that protects them from DDoS attacks," said Larson. "Fortunately we offer the industry-leading in-line, real-time DDoS mitigation solution that allows Internet Service Providers to easily meet that demand. The Corero SmartWall Threat Defense System can be deployed at the very edge of the network or Internet peering points to effectively inspect all Internet traffic and mitigate DDoS attacks in real-time before they can inflict damage downstream."

About Corero Network Security
Corero Network Security is the leader in real-time, high-performance DDoS defense solutions. Service providers, hosting providers and online enterprises rely on Corero's award winning technology to eliminate the DDoS threat to their environment through automatic attack detection and mitigation, coupled with complete network visibility, analytics and reporting. This next-generation technology provides a First Line of Defense® against DDoS attacks in the most complex environments while enabling a more cost effective economic model than previously available. For more information, visit www.corero.com

# # #