Neustar Neutralizes Fear of Ransom Note DDoS Attacks

Nov 9, 2015

With Proper Protections in Place, Organizations Can Confidently Ignore Extortion Attempts

STERLING, Va. — Neustar, Inc. (NYSE: NSR) **–** Businesses that protect their websites with a professional DDoS mitigation service are better prepared to defend against DDoS attacks. DDoS defense preparedness alleviates the fear, stress and worry caused by being on the receiving end of an extortion attempt or ransom note. The trend of blackmailing companies to send funds in order to gain back control continues to grow rapidly—with the total number of ransomware samples up 127% in the past year[1]. The impact is vast with DDoS attacks costing up to $1 Million or more if company's website is down for one hour during peak period[2].

"The best defense against extortion attempts is planning. Receiving a threat demanding payment when your business is at stake can cause fear and confusion about how to handle it. We are proud that our Neustar SiteProtect customers can confidently get focus on their core business and let Neustar handle DDOS defense if and when it's needed," said Margee Abrams, Director of IT Security Services Product Marketing for Neustar. "However, it's a different case for companies without professional DDoS protection – they must be very careful not to be drawn in to an ongoing extortion scenario. Experienced DDoS defenders can be mobilized within hours. It is this experience that counts when attack methods change during a DDOS crisis."

DDoS stands for distributed denial of service and an attack of this kind denies use of a website, server, network or other Internet services to its users. When these users are customers who are unable to access a website to browse, buy or compare prices, significant damage is done to the business, not only in terms of sales revenue but also to reputation – according to a recent Ponemon Institute study, 88 percent of consumers lose trust in a brand when the website is off-line or unavailable.

First seen in late 1990s, DDoS attacks have traditionally been big enough to take websites down for several hours if not days. However, the past 10 years have seen the rise of the extortion-type DDoS attacks where a relatively small but noticeable attack is quickly followed by an email ransom note claiming responsibility and threatening more to come unless money is paid. Often not much money, but there's the trap – if a susceptible a business is tempted to pay a small sum thinking the attacks will stop, all they have actually done is identified your website as one without professional DDoS protection and the attacks and requests for more and more money will continue.

When Team Internet, a leading provider of services in the direct navigation search market, experienced its first (and only) targeted attack, it was disconcerting.

“When the ransom note came, I went straight to my Neustar account manager who was unfazed and assured me that SiteProtect could handle the mitigation. This meant I could ignore the ransom note and sure enough, after the first attack there was nothing more. It was the best possible outcome and without Neustar, I would probably have paid,” says Mario Witte, Founder and CTO at Team Internet.

Read the latest Neustar DDoS Attacks and Protection report, including seven key DDoS trends here: https://www.neustar.biz/lp/security/oct-ddos-report/index.php

###

About Neustar, Inc.

Neustar, Inc. (NYSE:NSR) is the first real-time provider of cloud-based information services, enabling marketing and IT security professionals to promote and protect their businesses. With a commitment to privacy and neutrality, Neustar operates complex data registries and uses its expertise to deliver actionable, data-driven insights that help clients make high-value business decisions in real time, one customer interaction at a time. More information is available at www.Neustar.biz.

[1] *McAfee Labs Threats Report, August 2015*

[2] *Neustar DDoS Attacks and Protection Report, September 2015*