Kaspersky Lab warns Retailers not to Give Cybercriminals a Discount in the Sales

According to the Kaspersky Lab IT Security Economics Report, over 77% of companies have suffered from some kind of attack during the last 12 months. An increase in attacks where DDoS and POS systems were the main vectors is making the situation even worse – especially during the Christmas sale season, when there are more shoppers in store than usual, and the boost in sales is making retailer revenues an attractive target for cybercriminals.

The research shows that over the past year there has been an explosion (up to 16%) in both attacks involving DDoS attacks, and attacks in which vulnerabilities in point-of-sale systems (POS-terminals) have been used. These figures indicate that whatever heists cybercriminals are planning this season, they are likely to start with, or include, DDoS or the exploitation of vulnerabilities in retailer POS systems.

In particular, 2017 has seen a series of high-profile cybersecurity breaches reported in the payment systems of major brands: from Chipotle to Hyatt Hotels and recently, Forever 21. Kaspersky Lab also registered a considerable increase and geographic spread in botnet DDoS attacks in the third quarter of 2017, with targets in 98 countries (compared to 82 in Q2), according to the latest DDoS Intelligence Report.

This situation is going to be extremely relevant to retail and e-commerce organizations during the intense period of sales around Christmas. As shoppers look to bag their bargains, retailers can expect increased revenues. This in turn makes retailers a lucrative prize, if cybercriminals can stage successful DDoS attacks against them for a ransom, or for dirty competition, use POS systems as an entry point for targeted attacks, or steal customer credentials and money.

“Given this year’s apparent increase in these types of attacks, we recommend businesses – retailers in particular – to stay alert during the Christmas season, when there are more risks of cybercriminals cashing-out, through the exploitation of payment systems or attacks that use DDoS. These can involve cybercriminals demanding a ransom, or simply preventing an organization from trading, making them lose income and clients as a result. But apart from the obvious risks, this is also a good opportunity for businesses to think about their protection in in general, by developing their cybersecurity culture and investing in the right technologies.” – said Alessio Aceti, Head of Enterprise Business Division, Kaspersky Lab.

To avoid ruining their revenues in the upcoming high sales season, retailers and e-commerce organizations can protect themselves with a range of solutions dedicated to meeting their specific requirements. Kaspersky Lab strongly recommends that retailers:

– Keep e-commerce platforms up-to-date because every new update may contain critical patches to make the system less vulnerable to cybercriminals;

– If possible, make sure that the POS terminals in use run the latest version of software and change the default passwords;

– Use a tailored security solution, like Kaspersky Embedded Systems Security, to protect point of sales terminals from malware attacks;

– Prepare for DDoS attacks by choosing a reliable service provider that is a cybersecurity expert and can protect against powerful and sophisticated DDoS attacks. This is not always possible using in-house resources or Internet providers. To learn about the specialist Kaspersky DDoS Protection offering for SMBs and enterprises, please visit our website.

– Educate customers about the possible cyberthreats they may encounter while shopping online and offline, as well as steps about how to minimize the risks.

To learn more about how Kaspersky Lab can help protect retail organizations from cyberthreats please visit our website.