Report highlights rapid changes in DDoS threat landscape

Findings of a new report from Netscout have highlighted some key points around Distributed Denial of Service (DDoS) activity worldwide during 2018.

Netscout's Arbor Active Threat Level Analysis System (ATLAS) has actively monitored the global internet threat landscape since 2007 and today provides us with visibility into approximately one-third of the internet.

This is according to Hardik Modi, senior director of threat intelligence at Netscout, who says in a blog entry that the complexion of the threat landscape is moving more rapidly, expanding its footprint and changing tactics quickly.

Source: pixabay.com

He notes, "Methods that are commonplace in the DDoS threat tool kit have sprung to crimeware and espionage. This accelerating internet-scale threat paradigm changes the frontiers for where and how attacks can be launched, observed and interdicted."

Highlights

Highlights of the report, as outlined by Modi, include the following:

- **DDoS attacks have entered the terabit era**: During February 2018, Arbor Networks was able to mitigate the largest DDoS attack ever seen, a 1.7Tbps reflection/ amplification attack.

- **Attack volume is up while frequency is down**: From 2017 to 2018, we saw a slight drop in attack frequency accompanied by a dramatic increase in attack size and scale. However, the drop in frequency doesn't mean that DDoS attacks are abating. Netscout Arbor believes that as attack tools grow more sophisticated, attackers have found it easier and cheaper to launch larger, more effective attacks.

- **APT groups have expanded beyond the traditional arena**: More nations are operating offensive cyber programs and Netscout Arbor has observed a broader set of threat actors. Nation-state-sponsored activity has developed beyond the actors commonly associated with China and Russia, and today includes campaigns attributed to Iran, North Korea and Vietnam.

- **Crimeware actors are diversifying their attack methods**: While e-mail campaigns remain the primary form of attack, Netscout Arbor has observed notable changes in methods designed to accelerate malware proliferation. Inspired by 2017 worm events such as WannaCry, major crimeware groups added worm modules to other malware with distinct objectives such as credential-theft or traditional loaders. We also saw an increased focus on cryptocurrency mining in malware.

- **New DDoS attack vectors are rapidly leveraged**: The Memcached attack campaign used vulnerabilities in misconfigured Memcached servers to launch enormous DDoS assaults, a process that took very little time from initial reporting to the first attack tool being made available and used to cause global impact. Netscout Arbor says the vector remains exploitable and will continue to be used.

Bryan Hamman, territory manager for sub-Saharan Africa at Netscout Arbor

Bryan Hamman, territory manager for sub-Saharan Africa at Netscout Arbor, concludes, "Maintaining the availability of digital platforms, networks, applications and services is a business risk and a continuity issue. A successful DDoS attack aims to disrupt or cause the denial of an online service by overwhelming it with traffic from multiple sources. Motivations for planning a DDoS attack include extortion, competitive disruption by a business rival and even geo-political protest.

Against this background, businesses need to ensure that their e-commerce platforms are sufficiently protected against a potential DDoS attack using a multiple layer strategy to protect yourself from multi-vector attacks."