ثبت بزرگترین حمله DDoS با رکورد Gbps 500

نویسنده : علی جعفری 1395-02-08 - 9:27 صبح

طبق گزارش Arbor Networks، در سال گذشته شاهد بزرگترین حمله DDoS با رکورد Gbps 500 بودیم؛ و این در حالی است که هکرها هر روز بیش از پیش تکنیک‌های چند برداری را برای اخاذی از قربانیان خود بکار می‌بندند.
براساس 11امین گزارش سالیانه امنیت زیرساخت جهانی (WISR) به نقل از این شرکت امنیت شبکه، اندازه این حمل DDoS 60 برابر بیش از اولین باری شده است که این مطالعه انجام گرفته است؛ و این در حالی است که برخی قربانیان چنین حملاتی در سال 2015 حملات DDoS به بزرگی Gbps 425 ،Gbps 450 و Gbps 337 را نیز گزارش کرده اند.

از طرفی پیچیـدگی این حملـات نیز در حـال افزایش است بطوریکه بیش از نصف (56%) حملات به اصـطلاح «چند برداری» گزارش شده بطور همزمان لایه‌های زیرساخت، برنامه‌های کاربردی و خدمات را هدف قرار داده بودند.

تقریبا در کلیه (93%) حملات لایه کاربرد گزارش شـده، DNS متداول ترین سـرویس هدف بوده که با HTTP در گذشته قابل قیاس است.

بعلاوه خـدمات مبتنی بر ابر بطور اخص زیر آتش این حملات قرار دارنـد. درصـد موارد قطع برق گزارش شده که بر این لایه اثر گذاشته نیز از رقم 19% دو سال گذشته به یک سوم (33%) افزایش یافته است.

از سوی دیگر، بیش از نصف پاسـخ دهنـده‌ها (57%) اذعان داشـتند که قصـد دارنـد تا فناوری را برای تسـریع روند پاسخ به رویـداد را اتخـاذ کننـد؛ و این در حالی است که 52% از ارائه دهنـدگان خـدمات مـدعی شدند امروزه می‌توانند ظرف یک ماه تهدیدات پیشرفته APT را کشف و مهار نمایند.

از طرفی سه چهارم نیز امروز مدعی شده اند که برنامه رسمی برای پاسخ به رویداد دارند.

با این وجود نرخ تهدیـد از داخل سازمان از 12% در سال گذشته به 17% افزایش یـافته است؛ و این در حالیکه است که در کمال تاسف 40% از سازمان‌ها هنوز فاقد ابزار مناسب برای پایش BYOD در شبکه‌های خود هستند.

به گفته دارن انستی کارشناس ارشد امنیت، «مقابله با تهدیدات پیچیده و پنهانی امروز سخت تر شده است.»
وی افزود، «هر سال بر تعداد پاسخ دهنده‌های این نظرسـنجی افزوده می‌شود که شاهد حملات لایه کاربردی در شـبکه‌هایشان بوده انـد. البته امسال سـهم تعداد حملات چند برداری گزارش شده افزایش قابل ملاحظه ای را نشان داده است. حملات چند

برداری پیچیـده تر از آن هسـتند که به آسـانی بتوان با آنها مقابله کرد، ولی قطعا توسـعه ابزارهای مناسب رونـد بازی را تغییر خواهد دارد.»

«خوشـبختانه، سهم پاسخ دهنده‌هایی که از سیستم‌های هوشمند مقابله با حملات DDos (یا به اختصار، «IDMS») استفاده می‌کننـد افزایش معنی داری در سـطح بنگاه‌های اقتصادی و ارائه دهنـدگان خـدمات نشان داده است. لـذا این خبر می‌تواند امیدوارکننده باشد در حالیکه بر فراوانی حملات افزوده می‌شود.»
بنا بر اسـتدلال دیوید اِم محقق ارشد امنیت در Kaspersky، «حملات DDoS امروز ارزان تر و ساده تر از گذشـته شده اند که فرصتی عالی را برای وارد کردن حداکثر خسارت به هدف مدنظر در اختیار رقبا، هکرها و افرادی با نیات سوء قرار می‌دهد.»

به گفته وی، «در واقع درحـالیکه هزینه ای کسب و کارها که بخاطر این نوع حملات متحمل می‌شونـد بطور متوسط 291000 پونـد است، ولی ساده ترین حملات DDoS نیز را فقط با صـرف هزینه ای بالغ بر 32.30 پوند می‌توان بطور ناشناس سفارش داد و خریداری کرد. در نتیجه حجم حملات با سرعت بی سابقه ای طی سال‌های گذشته افزایش یافته است و از اینرو، کسب و کارها باید راهکاری موثرتر برای حفظ امنیت خود در برابر چنین حملاتی را در سال 2016 اتخاذ نمایند.»

«به این منظور، شـرکت‌ها می‌توانند از همکاری متخصـص داخلی با یک ارائه دهنده خدمات اینترنت برای فیلتراسیون فعال و مقابله با این نوع حملات خام و متعاقبا کاهش هزینه حفظ امنیت مشتری و کاهش ریسک وارد شدن ضـرر و زیان به شـرکت سود ببرند.»