چطور از سرور خود در مقابل حملات DDoS محافظت کنیم

چگونه از سرور خود در مقابل حملات DDoS محافظت کنیم

در حوزه‌ی دیجیتال، اشخاص یا صاحبان مشاغل به هر میزان که داده را بصورت آنلاین میزبانی می‌کنند، باید هوشیار باشند. روش‌های متفاوت بسیاری وجود دارند که موجب از کار افتادن سرورهای چندگانه یا خصوصی می‌شوند. یکی از شایعترین روش‌های حمله به کسب‌وکارهای آنلاین از طریق حملات DDoS انجام می‌شود.

در سال 2017 یک حمله DDoS در سرورهای پلی استیشن، چندین سرور اصلی را از کار انداخت، موجب مسدود شدن دسترسی کاربران به نتفیلیکس و آمازون و چندین سیستم دیگر در جنوب شرقی آمریکا شد.

اما حمله DDoS چیست؟ چگونه مدیران سرورها و کسب‌وکارها می‌توانند از DDoS جلوگیری کنند تا کسب‌وکارشان شکست نخورد؟در این مقاله همه آنچه که برای یادگیری حمله DDoS و تأثیرات آن بر کسب‌و کارها و این که چگونه امروزه با آن مقابله می‌کنند را می‌آموزید.

حمله DDoS چیست؟

قبل از آن که با نحوه مقابله با حمله DDoS آشنا شویم باید ابتدا بدانیم که این حمله چیست. DDoS مخفف (Distributed Denial of Service) به معنی منع سرویس توزیع شده است. نوعی حمله سازمان یافته است که علیه یک سرور یا یک شبکه، توسط دهها، یا صدها یا هزاران دستگاه با ارسال ترافیک فیک به یک سرور انجام می‌شود، تا شبکه یا سرور را از کار بیندازد. چگونگی انجام این امر بسته به نوع حمله DDoS متفاوت است ، که در ادامه بررسی خواهیم کرد.

در حمله DDoS وقتی کاربران واقعی وبسایت تلاش می‌کنند سایت را بازدیدکنند، به دلیل این که سرور با درخواست‌های زیادی روبرور شده است، با خطای سرور مواجه می‌شوند و دیگر نمی توانند سایت را بازدید کنند. در این شرایط دیگر کاربران واقعی نمی توانند به محصولات یا سرویس دسترسی پیدا کنند یا نمی توانند حساب کاربری خود را سازماندهی کنند که این وضعیت برای یک کسب و کار هزینه بسیاری دارد.

حملات DDoS دارای شدت و طول حمله هستند. می‌توانند به اندازه چند گیگابایت در ثانیه باشند یا صدها گیگابایت. هرچه حمله DDoS بزرگتر باشد مقابله با آن دشوارتر خواهد بود.

چرا حملات DDoS وجود دارد؟

هدف اصلی از یک حمله DDoS حمله علیه یک سازمان و باج گیری است. هکرها با سازمان‌ها تماس می‌گیرند و درخواست پرداخت پول می‌کنند (معمولا بصورت بیت کوین). در صورتی که سازمانی از

دادن پول امتناع کند گروه شروع به حمله DDoS علیه شرکت می‌کند. اغلب این تهدیدها بلوف هستند ولی گاهی هم این گروه‌ها همانطور که ادعا کرده‌اند حمله را شروع می‌کنند.

به کسب و کارها توصیه نمی‌شود که باجی به این گروه‌ها پرداخت کنند، چون اگر این گروه‌ها با سازمانی که مایل به پرداخت باج است مواجه شوند، احتمالاً برای دریافت مبالغ بیشتر باز می‌گردند. اگر چنین پیغامی دریافت کردید، از فرصت استفاده کنید و راهکارهای مقابله با حمله DDoS را بر سرورهای خود اجرا کنید، تا سرور را از هر گونه خرابی که ممکن است به واسطه این حمله در سیستم بروز دهد، محافظت کنید.

تأثیرات حمله DDoS چیست؟

برای درک اهمیت مقابله با حملات DDoS در کسب‌وکارتان، به عواقبی که ممکن است با از دسترس خارج شدن سایتتان برای ساعت‌ها یا حتی روزها رخ دهد فکر کنید. این که چقدر می‌تواند در میزان فروش شما تأثیرگذار باشد؟ چندین مشتری احتمالی را ممکن است از دست دهید؟

اگر یک شرکت تولیدی بطور میانگین روزانه 5000 دلار در روز فروش داشته باشد، یک حمله DDoS می‌تواند بیشتر از 15000 دلار هزینه داشته باشد. و این برای یک شرکت کوچک ضربه بزرگی خواهد بود. معمولا این حملات در زمان ساعات پیک کسب و کار انجام می‌شوند و مهاجمان سعی می‌کنند حمله را تا زمانی که امکان دارد ادامه دهند.

حملات DDoS به شهرت برند شما لطمه می‌زند. کاربران نمی‌دانند که شما قربانی این حمله بودید. تنها چیزی که آنها می‌دانند این است که به سایت شما مراجعه کردند ولی سایت شما خارج از سرویس بوده است.

حمله DDoS چگونه کار می‌کند؟

روش‌های استفاده شده در انجام حمله DDos بر اساس نوع حمله متفاوت است. اینجا متداول‌ترین روشهای مورد استفاده برای حمله به سرور را نام بردیم:

جریان SYN

در این روش سرور قربانی درخواست‌های جعلی از IP آدرس‌های تقلبی دریافت می‌کند. در این نوع حمله منابع سیستم مصرف می‌شود و سرور مدام در حال تفسیر حجم زیاد بسته‌های دریافتی است.

جریان SYN-ACK

در این نوع حمله سیستم قربانی بسته‌های **SYN-ACK** جعلی دریافت می‌کند، در نتیجه منابع سیستم تخلیه می‌شود چون سیستم مدام سعی میکند به این بسته‌ها پاسخ دهد.

Session تقلبی

این حمله یک ارتباط کامل TCP را جعل می‌کند. این حمله برای دور زدن ابزارهای دفاعی جدید طراحی شده است که فقط ترافیک ورودی به شبکه را کنترل می‌کنند.

مهاجمان DDoS از انواع مختلف حمله یا ترکیبی از آنها را استفاده می‌کنند و در تلاشند که یک سرور را از دسترس خارج کنند و روش‌های مقابله ای را دور بزنند. به همین دلیل باید مقابل چنین حمله‌هایی برنامه محافظتی داشته باشید.

چگونه از سرور خود در مقابل حملات DDoS محافظت کنیم؟

همانطور که دیدید حملات DDoS نسبتاً رایج هستند و گاه تأثیر جبران ناپذیری بر کسب‌وکارها دارد. خوشبختانه چند روش برای مقابله با حملات DDoS وجود دارد که با آن می‌توان یک حمله را متوقف کرد.

میزبانی محافظت شده DDoS

بهترین راه برای جلوگیری از حمله DDoS قبل از شروع آن تجهیز سرورها به حفاظ DDoS است. میزبان محافظت شده DDoS یک دستگاه سخت افزاری است که بین سرور و اینترنت شما قرار می‌گیرد و تمام ترافیک را فیلتر می‌کند تا از بروز هر نوع حمله DDoS جلوگیری کند.

ServerMania DDoS Protection وسیله ای است که ریوری (RioRey) برای کاهش این حملات طراحی کرده است. معمولا حملات DDoS تا 90 ثانیه قابل تشخیص و کاهش است. این وسیله اجازه می‌دهد تا ترافیک قانونی همچنان ادامه یابد حتی زمانی که حمله همچنان ادامه دارد.

میزبانی محافظت شده DDoS را می‌توان با هزینه کم بصورت ماهیانه اجاره کرد، قبل از اینکه بعد از حمله مجبور شوید به حالت دفاعی بروید،این سیستم از سرور شما در مقابل این حملات محافظت می‌کند و این نوعی روش فعال است.

سرویس حفاظت DDoS درجه سازمانی ما در برابر متداول‌ترین انواع حمله DDoS محافظت می‌کند ، از جمله این حمله‌ها :

- جریان UDP
- جریان SYN
- جریان SYN-ACK
- جریان ICMP
- جریان انعکاسی DNS
- Sessions جعلی
- IP های تکراری
- حملات Misused Application

اگر بدنبال بهترین روش برای محافظت در مقابل حملات DDoS هستید، استقرار سیستم تشخیص و مقابله با حمله DDoS بصورت همیشگی یکی از مؤثرترین روش‌ها است. در برخی از کسب‌وکارها فقط پس از شروع حمله از سخت افزارهای کاهش دهنده حملات استفاده میکنند، اما اغلب تا دستگاه مستقر شود ممکن است ساعت‌ها طول بکشد و صدماتی که نباید در سیستم رخ می‌دهد.

بهترین روش های حفظ امنیت سرور

علاوه بر روش های سرمایه گذاری در میزبان محافظت شده، حفظ رویه‌های امنیتی مناسب در سرور، روش دیگری برای محدود کردن تأثیرات حمله DDoS است مانند:

- محدود کردن سطح دسترسی دستگاه‌های خارج از شبکه به سیستم‌های داخلی.
- بروز نگهداشتن سیستم
- حفظ و مدیریت رمز عبور با راهکارهای مناسب

هزینه محافظت در مقابل حملات DDoS چقدر است؟

هزینه سرورهای محافظت شده DDoS اختصاصی، متناسب با نیاز و بودجه شما تعیین می‌شود و بدون جزئیات نمی توان دقیق تعیین کرد.

تا چه حد به محافظت DDoS نیاز داریم؟

شرکت‌های هاست اخیراً در حال تجهیز کردن سرورها به امکانات محافظتی اولیه در مقابل DDoS هستند. اما امکانات اولیه ممکن است برای نیازهای شما کافی نباشد. معمولا براساس میانگین میزان ترافیکی که وبسایت شما دریافت می‌کند می‌توانید تصمیم بگیرید که تا چه میزان به امکانات محافظتی

DDoS نیاز دارید. تخمیناً میانگین حملات DDoS در 14.1Gbps رخ می‌دهد. بنابراین اغلب برنامه‌های حفاظتی DDoS بازه 10 الی 20Gbps را محافظت می‌کنند.

البته باید هزینه خرابی سرورهای خاص را در نظرگرفت. اگر سرور، سرور پایگاه داده مرکزی برای فعالیت‌های کسب و کار باشد، منطقی است که سرمایه گذاری بیشتری برای محافظت آنها لازم است. اگر سرور دارای مأموریت‌های حیاتی نباشد احتمالاً به میزان محافظت استاندارد کمتری نیاز دارد.

می‌توانید با شرکت ارائه دهنده هاستینگ خود در رابطه با این که چه برنامه‌ای مناسب است مشورت کنید. با محافظت DDoS می‌توانید برای انواع حمله DDoS آماده باشید و با این کار هنگام وقوع حمله می‌توانید از ایجاد خرابی جلوگیری کنید و اعتبار خود را حفظ کنید.

چه نوع برنامه محافظتی DDoS برایتان مناسب خواهد بود؟

هر سیستم آنلاینی نیاز به محافظت DDoS دارد. ممکن است این، خرید آسانی نباشد ولی هر مدیر سیستمی که یک حمله DDoS را مدیریت کرده باشد به شما خواهد گفت که این شرایط می‌تواند بسیار آسیب رسان باشد. پس سرمایه گذاری در حفاظت مناسب مقابل DDoS بهترین راه حل جلوگیری از مشکلات است.