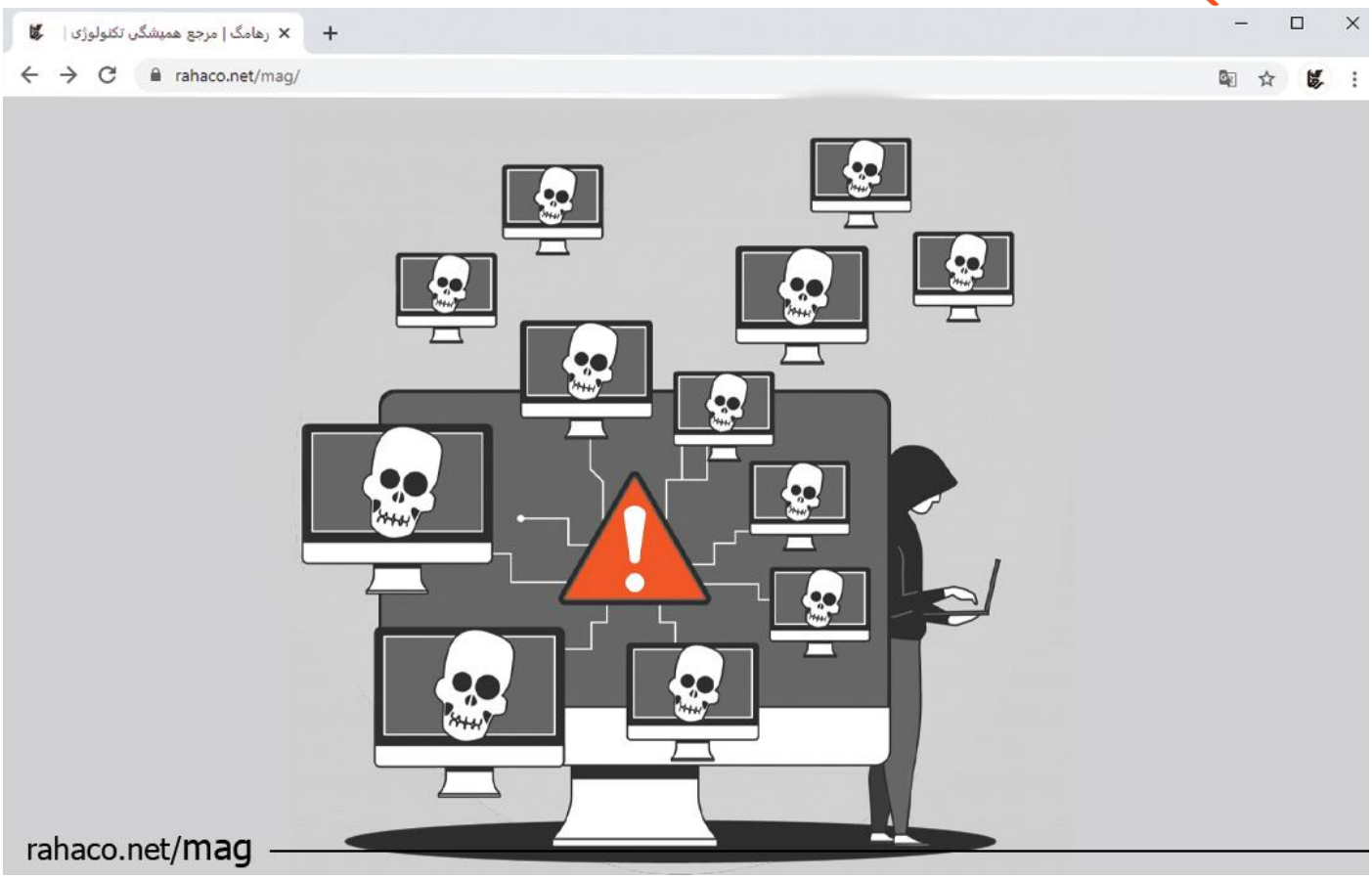
تعریف DDoS؛ رایج‌ترین تهدید داون کردن وبسایت‌ها

شرکت رهاکو

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net



فهرست

تعریف DDoS چیست؟ 3
تاریخچه تعریف DDoS 3
حملات DDoS چگونه بر مشاغل تاثیر می‌گذارد؟ 4
در طول حمله DDoS چه اتفاقی می افتد؟ 4
چگونه حملات DDoS را تشخیص دهیم؟ 5
چگونه حملات DDoS متوقف می‌شوند؟ 5
دلیل و انگیزه حمله DDoS چیست؟ 6
نتیجه گیری 7

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

برای درک تعریف DDoS، تصور کنید که در حال رفتن به سمت محل کار خود هستید. همه چیز خوب است، اما ناگهان ده‌ها ماشین در اتوبان جلوی شما ظاهر می‌شوند، سپس صدها و پس از آن هزاران. با ازدحام جمعیت و ترافیک سرعت ماشینتان را کند می‌کند و سپس به طور کامل متوقف می‌شود. چیزی که شما به عنوان یک کابوس ترافیکی در اتوبان مشاهده می‌کنید، همان کابوس DDoS و حملات سایبری در شبکه‌های کامپیوتری است.

صنعت فناوری اطلاعات اخیرا شاهد افزایش مداوم حملات DDoS بوده است. سال‌ها پیش، حمله DDoS مزاحمت‌های جزئی بودند که توسط هکرهای تازه کار انجام می‌شد. هکرها این کار را برای سرگرمی انجام می‌دادند و مهار آن نسبتا آسان بود. متاسفانه دیگر وضعیت به آن شکل نیست. اکنون حملات DDoS یک فعالیت پیچیده و در بسیاری از موارد یک معامله بزرگ است. در این مقاله در مورد تعریف DDoS و اینکه این حمله چگونه کار می‌کند بیشتر بخوانید.

تعریف DDoS چیست؟

حمله DDoS یا محروم سازی از سرویس برای ایجاد اختلال در وب سایت و شبکه طراحی می‌شود. با این حال، این تنها بخشی از این حملات DDoS است و کسب و کارهای آنلاین و مراکز داده باید در برابر این تهدیدات محافظت شوند. حملات DDoS لایه‌های شبکه را هدف قرار می‌دهد و با اسکن و مصرف منابع شبکه دسترسی کاربران را قطع می‌کند. لایه سرور نیز تحت تاثیر این حملات از طریق اسکن پورت، ابزارهای DoS و سوء استفاده از منابع سرور مختل می‌شود. در نهایت، لایه برنامه در برابر طیف گسترده‌ای از این حملات آسیب پذیر است. حمله DDoS در لایه برنامه از حفره‌های امنیتی سو استفاده می‌کند، منابع را مصرف کرده و دستورات مخرب را اجرا می‌نماید.

این حملات معمولا در سازمان‌های بزرگ رخ می‌دهند که افراد برای دریافت خدمات ضروری خود به آن‌ها وابسته هستند، مانند بانک‌ها و وب سایت‌های خبری و در برخی موارد حتی نیروگاه‌ها. هدف نهایی آن‌ها سرقت اطلاعات، از کار انداختن سیستم، فیشینگ و یا صرفا ایجاد هرج و مرج می‌باشد.

تاریخچه تعریف DDoS

اکنون که با تعریف DDoS آشنا شده اید بهتر است با تاریخچه آن نیز آشنا شوید. اولین حمله DDoS توسط هکر Khan C. Smithدر سال 1997 اتفاق افتاد. این حمله دسترسی اینترنت در لاس وگاس را برای بیش از یک ساعت مختل کرد. انتشار کد نمونه در طول این رویداد منجر به حملات بعدی در شرکت‌های بزرگ شد. در اوایل سال 2000، مایکل کالس، هکر نوجوان کانادایی حمله DDoS را ارتقا داد و با اختلال در یاهو تاثیر زیادی بر تجارت جهانی گذاشت! پس از آن سایر سایت‌های بزرگ مانند آمازون، CNNو eBay نیز با اختلال مواجه شدند. در نهایت،

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

همانطور که ما وارد عصر اینترنت اشیا (IoT) شده‌ایم، تقریبا هر دستگاه متصل به اینترنت مانند تلفن‌های هوشمند، دوربین‌های امنیتی، روترها و چاپگرها را می‌توان برای تاثیر بیشتر DDoS در یک بات نت جمع آوری کرد.

حملات DDoS چگونه بر مشاغل تاثیر می‌گذارد؟

با اطلاع از تعریفDDoS ، بدیهی است که شرکت‌ها و وب‌سایت‌های تجاری باید تهدیدات DDoS را جدی بگیرند. در سال 2018 مواردی از این قبیل وجود داشته است. حمله DDoS بسته به اندازه سازمان می‌تواند با روش‌های مختلف اعمال شود، از یک مزاحمت کوچک گرفته تا چیزی که می‌تواند در جریان درآمدزایی شما اختلال ایجاد کرده و برای همیشه به آن آسیب برساند. حمله DDoS برخی از کسب‌وکارهای آنلاین را در طولانی مدت فلج می‌کند و به طور قابل توجهی آن‌ها را از رقبا عقب می‌اندازد. بسته به نوع حمله، ممکن است این حملات به کسب و کار شما آسیب جدی وارد کنند. این مشکلات عبارتند از:

- کاربران ناامید
- از دست رفتن داده‌ها
- از دست دادن درآمد
- جبران خسارت
- کاهش بهره وری
- آسیب به شهرت و برندینگ

در طول حمله DDoS چه اتفاقی می افتد؟

در طول این حملات اختلال در دسترسی کاربران به داده‌های وب‌سایت، دسترسی به داده‌های خصوصی، کند کردن وبسایت یا داون کامل یک سرویس بر روی هر یک از لایه‌های ذکر شده در بالا وجود دارد. این حملات می‌تواند برای وبسایت‌ها و کسب و کارها در هر صنعتی رخ دهد - از بانک‌ها گرفته تا تجارت الکترونیک. مهاجمان در طول حمله شبکه را با حجم زیادی از درخواست‌ها و اطلاعات بمباران می‌کنند. همچنین ممکن است از برنامه‌ها و سرورها سو استفاده کنند یا تلاش کنند به داده‌های حساس سازمانی دسترسی یابند. انگیزه این حملات متفاوت است. از هک کردن تا اهداف مجرمانه، هرکدام از این حملات از روش‌های مختلفی استفاده می‌کنند. بنابراین داشتن یک سیستم امنیتی قوی برای اطمینان از اینکه شبکه‌ها و وبسایت‌های شما در برابر پیشرفته‌ترین حملات محافظت می‌شوند بسیار ضروری است.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

چگونه حملات DDoS را تشخیص دهیم؟

تعریف DDoS و تشخیص این حملات ساده است. شبکه‌ای که مورد حمله قرار بگیرد به کندی کار می‌کند و سرورها رو به خراب شدن می‌روند. همچنین دسترسی به شبکه با تاخیر بسیار زیاد امکانپذیر خواهد بود. این حملات عملکرد شبکه را کاهش داده و سرور را کاملا تحت تاثیر قرار می‌دهند. حملات DDoS اغلب از یک ترافیک یکسان در طول حمله استفاده می‌کنند که این امر می‌تواند به تشخیص وقوع حمله کمک کند. تعداد درخواست‌های غیرعادی از یک IP خاص نشانه خوبی است برای اینکه پی ببرید یک حمله DDoS در حال وقوع است.

سیستم‌ها و راهکارهای امنیتی به مدیران کمک می‌کند تا این ترافیک را شناسایی کنند و این راه‌حل‌های امنیتی می‌توانند درخواست‌های غیرعادی را تشخیص دهند. بنابراین، شناسایی برخی از حملات DDoS ممکن است دشوار باشد و به همین دلیل داشتن یک راهکار امنیتی جامع برای کسب و کارها به امری ضروری تبدیل شده است.

چگونه حملات DDoS متوقف می‌شوند؟

بهترین استراتژی برای کسب‌وکارها این است که از قبل برای حملات DDoS برنامه‌ریزی کنند. به عنوان مثال، یک فروشگاه آنلاین با کنترل حملات این امکان را برای کاربران فراهم می‌کند تا حتی هنگام حمله بدون توقف از وبسایت استفاده کنند. همچنین می‌توان از یک سیستم جایگزین برای مقابله با این حملات استفاده کرد. در واقع بخش فناوری اطلاعات سازمان باید در شناسایی و رهگیری هرگونه ارتباط مخرب با DDoS کاملا هوشیار عمل کند. چندین روش در مورد امنیت داخلی وجود دارد که باید در نظر بگیرید:

- پسوواردها را در جایی مطمئن نگه دارید
- رمز عبور دستگاه‌های اینترنت اشیا را تغییر دهید
- هنگام خروج رایانه خود را قفل کنید
- در پایان روز از سیستم خارج شوید
- رمز عبور خود را برای کسی فاش نکنید

در روش دوم، اگر به اشتراک گذاری اطلاعات ورود به سیستم ضروری است، اطمینان حاصل کنید که این اطلاعات از طریق کانال‌های رمزگذاری شده ارسال می‌شوند.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

دلیل و انگیزه حمله DDoS چیست؟

افراد عادی، کسب‌وکارها و حتی دولت‌ها با تعریف DDoS آشنا هستند و هر کدام انگیزه‌های خاص خود را برای انجام آن دارند. در ادامه دلایل مختلف این حملات را مشاهده می‌کنید.

هک

هکرها از حملات DDoS به عنوان ابزاری برای بیان انتقادات خود از دولت‌ها، سیاستمداران، سازمان‌ها و رویدادهای بزرگ استفاده می‌کنند. اگر هکرها با رویکرد شما موافق نباشند، وبسایت شما از بین می‌رود.(tango down)

هکرها از نظر فنی تسلط کمتری نسبت به سایر مهاجمان دارند و بیشتر از ابزارهای از پیش ساخته شده برای حمله استفاده می‌کنند. شاید یکی از معروف‌ترین هکرها Anonymous باشد. آن‌ها مسئول حمله سایبری در فوریه 2015 علیه داعش و همچنین حمله به دولت برزیل و اسپانسرهای جام جهانی در ژوئن 2014 هستند.

حمله سایبری

مهاجمان سایبری اغلب به عنوان «جوجه اسکریپت» شناخته می‌شوند. این هکرها اغلب نوجوانانی هستند که فقط آدرنالین می‌خواهند یا به دنبال تخلیه خشم یا ناامیدی خود علیه مدرسه و اهداف شخصی می‌باشند. در کنار ابزارها و اسکریپت‌های از پیش ساخته شده، هکر سایبری همچنین از سرویس‌های DDoS-for-hire (با نام مستعار بوترها) نیز استفاده می‌کند.

سرقت

یکی از انگیزه‌های محبوب حملات DDoS سرقت اطلاعات است؛ به این معنی که یک مجرم سایبری در ازای انجام ندادن یک حملهDDoS ، از هدف موردنظر درخواست پول می‌کند. چندین شرکت نرم‌افزاری از جملهMeetUp ، Bitly، Vimeoو Basecamp این نوع از تهدیدات را دریافت کرده‌اند و پس از قبول نکردن مورد حمله قرار گرفتند.

رقابت تجاری

حملات DDoS به عنوان یک ابزار رقابتی میان کسب و کارها شناخته می‌شوند. برخی از این حملات برای جلوگیری از فعالیت شرکت رقیب در یک رویداد مهم (مثلا بلک فرایدی) طراحی شده‌اند، در حالی که برخی دیگر با هدف تعطیلی کامل یک کسب و کار برای ماه‌ها و یا حتی سال‌ها انجام می‌شوند. در اینجا هدف اصلی ایجاد اختلال است تا مشتریان از رقیب شما دلسرد شوند که در نهایت باعث آسیب مالی و اعتباری آن‌ها خواهد شد. هزینه متوسط یک حمله DDoS برای سازمان می‌تواند به 40000 دلار در ساعت نیز برسد.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

جنگ سایبری

حملات DDoS توسط دولت برای ساکت کردن منتقدان و مخالفان داخلی استفاده می‌شود. همچنین به عنوان تهدیدی برای مختل کردن خدمات مالی، بهداشتی و زیرساختی در کشورهای دشمن محسوب می‌شود. این حملات توسط دولت پشتیبانی می‌شوند؛ به این معنی که آن‌ها پروژه‌هایی با بودجه خوب و سازمان‌دهی شده‌اند که توسط متخصصان فناوری اطلاعات اجرا می‌شوند.

رقابت شخصی

حملات DDoS برای تسویه حساب‌های شخصی یا ایجاد اختلال در بازی‌های آنلاین مورد استفاده قرار می‌گیرد. جایی که بازیکنان برای به دست آوردن برتری یا اجتناب از شکست با «تغییر جدول»، حملات DDoS را علیه یکدیگر و حتی علیه سرورهای بازی راه‌اندازی می‌کنند.

نتیجه گیری

اکنون که با تعریف DDoS آشنا شده‌اید، اگر کسب و کاری دارید یا شبکه‌ای را مدیریت می‌کنید باید از سرورهای خود در برابر حملات DDoS محافظت کنید .یکی از رایج‌ترین حملاتی است که در دنیای سایبری امروز وجود دارد. برای مدیر شبکه یا کسی که می‌خواهد به طور ایمن از اینترنت استفاده کند بسیار ضروری است که از انواع حملات و نحوه دفاع در برابر آن‌ها آگاهی داشته باشد. گذشته از تمام تکنیک‌های دفاعی می‌توانید از کمک افراد حرفه‌ای در زمینه امنیت سایبری نیز استفاده کنید تا کسب و کارتان همیشه ایمن بماند.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net