Distributed Denial of Service (DDOS)

دیداس چیست؟

حمله دیداس نوعی حمله سایبری است که در آن فرد مهاجم با ارسال حجم سنگینی از ترافیک اینترنتی به سمت هدف خود باعث از کار افتادن و یا ایجاد اختلال در عملکرد عادی آن شده و در نتیجه کاربران و یا بازدیدکنندگان برای دسترسی به آن دچار مشکل خواهند شد. حملات دیداس از طریق بات‌نت‌ها انجام می‌شوند که در واقع مجموعه‌ای از دستگاه‌ها و سیستم‌های آلوده و متصل به‌هم هستند .

حملات دیداس چگونه انجام می‌شوند؟

1 – ساختن بات نت ها : هکر با استفاده از تکنیک **مهندسی اجتماعی** و یا ارسال **بدافزار** به صدها، هزاران و گاها صدها هزار یا میلیون دستگاه کامپیوتر شخصی، سرور مجازی، تبلت، تلفن هوشمند و یا حتی دستگاه‌های مبتنی برسیستم‌های امنیتی هوشمند و ... اقدام به هک کردن آن‌ها کرده و از آن‌ها یک بات‌نت می‌سازد. در حملات دیداس به هر دستگاه، بات گفته می‌شود .

2- انتخاب هدف : هکرها برای انجام حملات دیداس انگیزه‌های مختلفی را دنبال می‌کنند که از میان آن‌ها می‌توان به ضربه‌زدن به کسب‌وکارهای رقیب، باج‌خواهی و هکتیویسم اشاره کرد. فرد مهاجم در این مرحله هدف مورد نظر خود را انتخاب کرده و شروع به جمع‌آوری اطلاعات در مورد آسیب‌پذیری‌های امنیتی و سایر نقاط ضعف آن می‌کند.

3- راه اندازی C&C **:** فرد هکر برای مدیریت بات‌نت و ارسال دستورالعمل‌های مورد نظر خود به آن، اقدام به راه‌اندازی سی‌اندسی می‌کند . C&CمخففCommand and Control)) و سیستم یا سروری است که هکرها با استفاده از آن می‌توانند بات‌نت‌ها را مدیریت و دستورالعمل‌های مورد نظر خود را به آن ارسال کنند.

4 – ارسال دستورالعمل : فرد مهاجم نوع حمله را مشخص کرده و دستورالعمل‌های خود را به سمت بات‌نت ارسال می‌کند.

5 – انجام حمله : اتنت طبق دستورالعمل‌های دریافتی اقدام به ایجاد حجم سنگینی از ترافیک کرده و آن را به سمت هدف مورد نظر ارسال می‌کند که این عمل باعث از کار افتادن و یا کندی آن می‌شود.

۶ -مانیتورینگ حمله : هکر فرآیند حمله را با دقت مورد بررسی و ارزیابی قرار داده و در صورت نیاز حجم بیشتری از ترافیک را به سمت سیستم هدف می‌فرستد.

مقایسه DOS و DDOS

DOS مخفف (Denial Of Service) نوعی حمله سایبری است که در آن فرد هکر با ارسال حجم زیادی از درخواست‌های غیرقانونی به سمت هدف خود، منابع آن را مصرف کرده و در نهایت مانند حملات دیداس باعث ایجاد اختلال در عملکرد عادی آن می‌شود. افراد مهاجم معمولا برای انجام حملات DoSتنها از یک دستگاه یا اتصال شبکه استفاده می‌کنند اما حملات DDoS قدرت بیشتری داشته و در آن هکرها با استفاده از باتنت حجم بسیار سنگینی از درخواست‌های جعلی را به سوی هدف مورد نظر خود ارسال می‌کنند. حملات دیداس ماهیت پیچیده و توزیعی داشته و ممکن است از چندین مکان جغرافیایی مختلف انجام شوند که همین موضوع باعث می‌شود تا شناسایی و مقابله با آن‌ها نسبت به حملات DoS دشوارتر باشد. توجه داشته باشید که انجام حملات DoS نیز مانند حملات DDoS غیر قانونی هستند.

هدف انجام حملات DDOS

هکتیویسم :هکتیویست‌ها ممکن است به منظور جلب توجه، افزایش آگاهی افراد جامعه، مقابله با حکومت‌ها و یا ابراز مخالفت خود با برخی از سیاست‌های دولت‌ها، اقدام به انجام حملات DDoS کنند Anonymous .یکی از مهم‌ترین گروه هکری هکتیویست می‌باشد که در سطح جهانی فعالیت می‌کند.

باج‌خواهی :برخی از هکرها با انگیزه باج‌خواهی اقدام به انجام حملات DDoS کرده و معمولا تا زمانی که پول درخواستی آن‌ها پرداخت نشود، به حملات خود ادامه می‌دهند.

جنگ سایبری :در این نوع حمله دیداس ممکن است کشوری به دلایل مختلفی (ایجاد اختلال در روند انتخابات، رساندن زیان‌های مالی، ساکت‌کردن منتقدان و مخالفان داخلی، رساندن یک پیام خاص و...) وب‌سایت‌ها و زیرساخت‌های شبکه کشور دیگری را مورد هدف قرار دهند.

ضربه زدن به شرکت‌های رقیب :گاهی اوقات ممکن است کسب‌وکارها و شرکت‌ها با هدف ضربه‌زدن به رقبای خود، آن‌ها را مورد حملات دیداس قرار دهند.

استفاده پوششی :هکرها ممکن است از حملات DDoS به عنوان پوششی برای منحرف کردن توجه‌ها از سایر عملیات‌های سایبری (نقض داده‌ها، هک کردن مؤسسات مالی و...) استفاده کنند.

نارضایتی از خدمات :گاهی اوقات ممکن است فردی به دلیل نارضایتی از خدمات شرکت، سازمان و یا وب‌سایتی، آن را مورد حمله DDoS قرار دهد.

سرگرمی :برخی از افراد (بیشتر نوجوانان) صرفا برای سرگرمی و بدون هیچ دلیل خاصی وب‌سایت، سرور و یا سرویس آنلاینی را از طریق DDoS مورد حمله سایبری قرار می‌دهند.

آزمایش تکنیک‌ها و ابزارها :گاهی‌اوقات هکرها به منظور آزمایش تکنیک‌ها و ابزارها و همچنین بررسی میزان تأثیرات حملات خود اقدام به انجام حملات دیداس می‌کنند.

سوالات متداول

آیا می‌توان هکرهایی که از حمله دیداس استفاده می‌کنند را شناسایی کرد؟

شناسایی این افراد به دلیل ماهیت توزیعی حملات دیداس بسیار دشوار است. با این حال انجام کارهایی IP و تجزیه‌وتحلیل رفتار شبکه و آدرس‌های و پلیس امنیت سایبری، فارنزیک ISP مانند همکاری با می‌توانند به شما در شناسایی باتنت‌ها و فرد استفاده‌کننده از آن‌ها کمک بسیاری کند

در هنگام وقوع حملات دیداس چکار کنیم؟

حفظ آرامش، تماس فوری با ISPیا شرکت ارائه‌دهنده خدمات میزبانی، فعال‌سازی سرویس‌های مقابله با حملاتDDoS ، شناسایی و جمع‌آوری مدارک مرتبط با حمله، گرفتن کمک از کارشناسان امنیت سایبری، مطلع ساختن شرکای مالی و کارمندان از جمله موارد مهمی هستند که باید در هنگام وقوع چنین حملاتی به آن‌ها توجه کنید.

آیا حملات DDoS قابل پیشگیری هستند؟

پیشگیری کامل از حملات DDoS عملا غیرممکن است اما با استفاده از راهکارهایی که در بخش **راهکارهای پیشگیری و مقابله با حملات DDoS** به آن‌ها اشاره شد، می‌توان تا حد زیادی اثرات چنین حملاتی مخربی را کاهش داد.

حملات دیداس چقدر زمان می‌برند؟

این نوع حملات می‌توانند بین چند ثانیه تا چندین ساعت (حتی روزها) زمان ببرند و عواملی مانند پیچیدگی و حجم حمله، انگیزه فرد هکر، پهنای‌باند شبکه و روش‌ها و رویکردهای دفاعی استفاده شده بر مدت زمان حمله تأثیر می‌گذارند.

منابع : MaralHost , Radware , Cloudflare , IBM

سوالات امتحانی

1 – دیداس را تعریف کنید ؟

2 – 3 تا ازهدف های دیداس را نام ببرید ؟

3 – فرق DOS و DDOSچیست ؟

4 – بات نت چیست ؟

5 – ایا حملات دیداس قانونی است ؟