گزارش در مورد تاریخچه و ماهیتِ حملاتِ DDoS

تهیه و تنظیم: مبین خیری

شماره دانشجویی: 994421017

استاد راهنما: دکتر میرسامان تاجبخش

چکیده:

هدف از این تحقیق، معرفیِ شیوه‌ی عملکردِ حملاتِ DDoS و چگونگیِ گسترش و توسعه‌ی آن‌هاست. علاوه بر این، در گزارش پیش‌رو قصد داریم نگاهی گذرا به تاریخچه‌ی این حملات انداخته و سیر تطور آن‌ها را بررسی کنیم.

برای این منظور ابتدا به معرفیِ جامع و کاملِ این نوع از حملات پرداخته و سپس به تفاوت‌های میان این نوع حملات و سایر حملات مرسوم در سطح شبکه اشاره خواهیم کرد. علی‌رغمِ وجود منابع پرشمار و معتبری که به زبان انگلیسی و در سطح اینترنت یافت می‌شوند، این گزارش، تماما به زبان فارسی تهیه و تدوین شده است.

انواع حملات DDoS و تشریح ۵ تهاجم بزرگ در دنیا

حملات DDoS، تلاشی برای ایجاد اختلال در ترافیک عادی یک سرور، سرویس یا شبکه هستند. این حملات در گذشته توسط یک کامپیوتر و این روزها با استفاده از چندین سیستم کامپیوتری برای ایجاد ترافیک در شبکه ایجاد می‌شوند. ماشین‌های مورد استفاده می‌توانند رایانه یا سایر دستگاه‌های IoT باشند. به بیانی دیگر، می‌توان گفت که حمله‌ی DDoS مانند یک ترافیک غیرمنتظره است که یک بزرگراه را مسدود می‌کند و از حرکت سایر اتوموبیل‌ها جلوگیری می‌نماید.

حمله‌ی DoS چیست؟

حمله‌ی DoS (Denial-of-Service) تهاجمی است که با هدف خاموش کردن یا از کار انداختن یک ماشین یا شبکه انجام می‌شود و آن را برای کاربران دیگر دسترس ناپذیر یا بسیار کند می‌کند.

هر ماشین یا شبکه‌ای دارای حجم مشخصی از منابع پردازشی است. هر کاربر با ورود و ارسال درخواست به شبکه، بخشی از این منابع پردازشی را به خود مشغول می‌کند. وقتی که تعداد این درخواست‌ها افزایش یابد، منابع پردازشی به شکل کامل پر شده و شبکه از ارایه خدمات به سایر کاربران ناتوان خواهد شد. در حمله‌ی DoS، مهاجم با یک ماشین و با یک IP ثابت بخش قابل توجهی از منابع شبکه را درگیر می‌کند. در این موارد با بستن IP مهاجم می‌توان ترافیک ایجاد شده در شبکه را از بین برد.

حمله DDoS چیست؟

در حمله‌ی DDoS (Distributed Denial-of-Service) که گاهی به آن حمله‌ی تکذیب سرویس نیز گفته می‌شود، تهاجم به شکل توزیع‌شده انجام خواهد شد. یعنی مهاجم به جای استفاده از یک ماشین و یک IP ثابت، چندین ماشین و IP را به کار می‌گیرد. در حمله-ی DoS، با مسدود کردن ماشین مهاجم می‌توانستیم با آن مقابله کنیم، اما در حملات سایبری DDoS، از بین بردن خطر سخت‌تر است برای این که حمله به شکل توزیع شده انجام می‌شود و ترافیک دریافتی از هر ماشین قابل توجه نیست. در این نوع حملات، تشخیص مهاجم از کاربر واقعی سخت-تر است و امکان دارد در زمان مقابله با حمله، به اشتباه جلوی ترافیک دریافتی از سوی کاربران واقعی گرفته شود.

انواع حملات DDoS

به شکل کلی، انواع حملات DDoS را می‌توان به ۳ دسته تقسیم کرد:

دسته‌ی اول: در این دسته، حمله به شبکه، منجر به کندی شدید سرویس برای کاربران و یا قطعی کامل خواهد شد. این کار با استفاده از ارسال ترافیک در حجم بسیار بالا به زیرساخت شبکه انجام می‌شود. در چنین حالتی پهنای باند شبکه به شکل کامل اشغال خواهد شد.

دسته دوم: در این دسته، حمله به شکلی رخ می-دهد تا منابع پردازشی سرور مانند CPU، RAM و دیسک درگیر شوند. این اتفاق در نهایت سبب می‌شود تا سرور توانایی پاسخ‌گویی به درخواست کاربران را نداشته باشد.

دسته سوم: در این دسته، فرد مهاجم با هوشمندی، یک نقطه‌ی آسیب‌پذیر در برنامه را پیدا کرده و از طریق آن اجرای وب‌سرویس را مختل و یا در آن مشکلاتی ایجاد می‌کند.

انواع حملات DDoS اجزای مختلف اتصال شبکه را هدف قرار می‌دهد. برای درک شیوه‌ی عملکرد حملات سایبری DDoS لازم است بدانیم که چگونه یک اتصال در شبکه ایجاد می‌شود. یک اتصال شبکه در اینترنت از اجزای مختلف یا لایه‌ها تشکیل شده است. مانند ساختن یک خانه از پایه، هر لایه از اتصال، هدف متفاوتی دارد. برای مثال مدل OSI که یک چارچوب مفهومی است، می‌تواند به درک بیش‌تر انواع حملات کمک کند.

حمله‌ی SYN Flood

حمله‌ی SYN Flood یا نیمه‌باز، یکی از انواع حملات DDoS است که با هدف اشغال کلیه منابع سرور و بر اساس عملکرد TCP اجرا می‌شود. وقتی که کلاینت و سرور بخواهند با یکدیگر داده تبادل کنند، عملیاتی به نام Three-Way Handshake اتفاق می--افتد. در طی این فرآیند: کلاینت پیامی به نام SYN، یا همان هماهنگ‌سازی را، به شکل یک درخواست به سرور ارسال می‌کند. بعد از آن، سرور با پیامی به نام SYN-ACK به کلاینت اعلام می‌کند که درخواست پذیرفته شد. سپس، نوبت کلاینت است که با ارسال یک پیام ACK به SYN-ACK به سرور پاسخ دهد. وقتی که پیام ACK کلاینت به سرور رسید، اتصال TCP برای برقراری داده باز خواهد شد.

در حملات SYN Flood، سرور پس از فرستادن پیام SYN-ACK، در انتظار دریافت پیام ACK از سوی کلاینت، یک پورت را برای دریافت پیام باز می‌گذارد. این مساله منجر به اتلاف منابع پردازشی سرور خواهد شد. حال، فرض کنید که کلاینت، هرگز ACK را برای سرور ارسال نکند و این کار را به دفعات و با تعداد بسیاری از ماشین‌ها انجام دهد. نتیجه این خواهد شد که بیش‌تر پورت‌ها در حالت انتظار و مشغول باقی خواهند ماند. بعد از اشغال تمامی پورت‌ها، سرور دیگر قادر به خدمت‌رسانی نخواهد بود.

حمله‌ی Slowloris

حمله-ی Slowloris از پروتکل HTTP که برای ایجاد ارتباط و انتقال داده بین سرور و کلاینت استفاده می‌شود، بهره می‌گیرد. طی این حمله، درخواست-های HTTP بسیاری را می‌سازد و آن‌ها را با سرعت بسیار کم به سرور ارسال می‌کند. وقتی که این اتصالات با سرعت کمی انجام می‌شود، سرور دچار ازدحام شده و در نهایت توانایی خود را برای سرویس‌دهی از دست می‌دهد.

در این حمله، مهاجم اتصالی را بین خود و سرور برقرار می‌کند و پس از آن تمام تلاشش را خواهد کرد تا این اتصال را باز نگه دارد. برای این کار، مهاجم درخواست‌های خود را به شکل ناقص و با سرعت کم ارسال کرده و سرور هیچ‌گاه درخواست کاملی را از کلاینت دریافت نمی‌کند. در نتیجه، بخش قابل توجهی از منابع سرور هدر خواهد رفت.

حمله‌ی DNS Flood

حمله‌ی DNS Flood یکی از انواع حملات DDoS است که در آن مهاجم یک یا چند DNS متعلق به یک منطقه‌ی خاص را هدف قرار می‌دهد و تلاش می‌کند تا عملکرد آن-ها را مختل کند. سرورهای DNS «نقشه‌ی راه اینترنت» هستند و به درخواست‌کنندگان کمک می‌کنند تا سرورهای مورد نظر خود را بیابند. در یک حمله‌ی DNS Flood، مهاجم سعی می‌کند تا یک یا چند سرور DNS خاص را با ترافیک به- ظاهر معتبر، تحت فشار قرار دهد. این فشار تا حدی انباشته می‌شود که سرورهای DNS قادر به هدایت Requestهای واقعی نشوند.

در این حملات، مهاجم بسته‌های کوتاه را ارسال و پاسخ‌های دراز را دریافت می‌کند. این موضوع باعث می‌شود تا بخش قابل توجهی از منابع سرور DNS درگیر و در نهایت تلف شوند. مهاجم با استفاده از مکانیزم IP Spoofing درخواست‌های بسیاری را برای سرور DNS ارسال کرده و اقدام به ایجاد اختلال در سرور می-کند.

معرفی پنج مورد از معروف‌ترین حملات DDoS

در این بخش، قصد داریم تا برخی از برجسته‌ترین حملات DDoS در تاریخ را شرح دهیم. انتخاب این ۵ مورد بر اساس مقیاس، تاثیر و پیامدهای آن‌ها بوده است.

حمله‌ی گوگل، ۲۰۱۷

در ۱۶ اکتبر ۲۰۲۰، گروه تجزیه و تحلیل تهدیدات گوگل (TAG) یک پست وبلاگی درباره تغییرات تاکتیکی تهدیدگر-ها در نزدیکی انتخابات ریاست جمهوری ۲۰۲۰ آمریکا منتشر کرد. در پایان این پست، این گروه در یادداشتی نوشت:

"در سال ۲۰۱۷، تیم امنیتی ما یک رکورد در حمله‌ی نوع UDP Amplification از سوی چندین ISP چینی را استخراج و اندازه‌گیری کرد که بزرگ‌ترین حملات سایبری DDoS است که ما از آن آگاه هستیم."

حمله به هزاران آدرس IP گوگل که از چهار ISP چینی نصب شده بود، شش ماه طول کشید و با سرعت خیره کننده ۲.۵۴ ترابیت بر ثانیه به اوج خود رسید! دامیان منشر، مهندس ایمنی در گوگل، نوشت: «مهاجم از چندین شبکه برای جعل میلیون‌ها بسته در ثانیه به ۱۸۰هزار سرور DNS، CLDAP و SMTP استفاده و در ادامه پاسخ‌های حجیمی را برای ما ارسال کرد. این حجم چهار برابر بزرگ‌تر از حمله‌ی Mirai در یک سال قبل بود.»

حمله AWS، فوریه ۲۰۲۰

سرویس وب آمازون (AWS) در فوریه ۲۰۲۰ مورد حمله‌ی DDoS شدیدی قرار گرفت. این یکی از بزرگ‌ترین حملات سایبری DDoS بود که در آن، یک مشتری ناشناس، AWS را با استفاده از تکنیکی به نام Connectionless Lightweight Directory Access Protocol (CLDAP) هدف قرار داد. این تکنیک به سرورهای آسیب‌پذیر CLDAP شخص ثالث متکی است و مقدار داده ارسال شده به آدرس IP قربانی را بین ۵۶ تا ۷۰ برابر افزایش می‌دهد. این حمله به مدت سه روز به طول انجامید و با سرعت خیره کننده‌ی ۲.۳ ترابایت در ثانیه به اوج خود رسید.

با این-که اختلال ایجاد شده به‌وسیله‌ی AWS DDoS Attack بسیار کم‌تر از آن چیزی بود که می‌توانست باشد، این حمله آسیب گسترده‌ای به مشتریان و برند AWS وارد کرد.

حملات Mirai Krebs و OVH DDoS، سپتامبر ۲۰۱۶

در ۲۰ سپتامبر ۲۰۱۶، وبلاگ یک کارشناس امنیت سایبری به نام برایان کربس، توسط یک تهاجم DDoS با قدرت ۶۲۰ گیگابیت بر ثانیه مورد حمله قرار گرفت. کربس با حملات سایبری DDoS بیگانه نبود و از ژوئیه ۲۰۱۲، ۲۶۹ حمله‌ی سایبری DDoS را روی سایت خود تجربه کرده بود. هرچند این حمله، تقریبا سه برابر بیش‌تر از هر آن-چه بود که سایت او قبلا دیده بود.

منبع این حمله Mirai Botnet که در آگوست ۲۰۱۶ کشف شد و در اوج خود، یعنی اواخر همان سال، بیش از ۶۰۰هزار دستگاه اینترنت اشیا مانند دوربین-های مدار بسته، روترهای خانگی و سیستم‌های ویدیویی را مورد تهاجم قرار داد. حمله به وب‌سایت کربس، اولین اقدام بزرگ آن بود.

حمله‌ی بعدی Mirai Botnet در ۱۹ سپتامبر با هدف تخریب OVH که یکی از بزرگترین ارایه‌دهندگان سرویس میزبانی در اروپاست انجام شد. این سرویس‌دهنده، میزبانیِ ۱۸میلیون برنامه از حدود یک میلیون

مشتری را انجام می‌داد. این حمله روی یک مشتری ناشناس OVH و به وسیله‌ی حدود ۱۴۵هزار ربات هدایت شد. بار ترافیکی ایجاد شده به وسیله‌ی آن ۱.۱ ترابیت در ثانیه بود و حدود ۷ روز طول کشید. OVH آخرین قربانی Mirai Botnet در سال ۲۰۱۶ نبود.

Mirai Botnet گام بسیار مهم در افزایش قدرت انواع حملات DDoS بود. اندازه و پیچیدگی شبکه Mirai و مقیاس حملات آن‌ها بی‌سابقه به نظر می‌رسید و به همین دلیل اهمیت بسیاری پیدا کرد.

حمله Mirai Dyn DDoS، اکتبر ۲۰۱۶

در ۲۱ اکتبر ۲۰۱۶، Dyn که یکی از ارایه‌دهندگان DNS است، با سیل ترافیک یک ترابیت در ثانیه مورد حمله قرار گرفت. این تهاجم باعث شد تا رکورد جدیدی برای انواع حملات DDoS ثبت شود. شواهدی وجود دارد که نشان می‌دهد این حمله در واقع به نرخ ۱.۵ ترابیت در ثانیه دست یافته باشد. سونامی ترافیک، خدمات Dyn را با مشکل مواجه و منجر به آفلاین شدن آن شد. طی این رویداد تعداد زیادی از سایت‌های مطرح مانند GitHub، HBO، Twitter، Reddit، PayPal، Netflix و Airbnb از دسترس خارج شدند. کایل یورک، مدیر ارشد استراتژی Dyn گزارش کرد: ما ۱۰ میلیون آدرس IP مجزا و مرتبط با Mirai botnet را مشاهده کردیم که بخشی از حمله بودند.

حملات Mirai botnet از پیچیده-ترین حملاتی بود که دنیای اینترنت آن را مشاهده کرد. در اواخر سپتامبر ۲۰۱۶، کد منبع Mirai به -شکل همگانی منتشر شد و برای هر کس با مهارتی به- نسبت متوسط در حوزه‌ی فناوری اطلاعات، امکان انجام حملات DDoS را فراهم کرد. به این ترتیب، روش‌های مقابله با حملات DDoS به سختی می‌توانستند در برابر این تهاجم‌ها از خود مقاومت نشان- دهند.

حمله GitHub، فوریه ۲۰۱۸

در ۲۸ فوریه ۲۰۱۸، GitHub که یک پلتفرم برای توسعه‌دهندگان نرم‌افزار است، با یک حمله‌ی DDoS با سرعت ۱.۳۵ ترابیت بر ثانیه و برای ۲۰ دقیقه مورد تهاجم قرار گرفت. طبق گفته‌ی GitHub، ترافیک به بیش از هزار سیستم مستقل مختلف (ASN) در ده‌ها هزار نقطه‌ی پایانی رسیده بود.

با این که GitHub به خوبی برای انواع حملات DDoS آماده شده بود، خدمات آن‌ها به هر روی تحت تاثیر قرار گرفت. GitHub در یکی از گزارش‌های خود بیان کرد که در طول سال‌های گذشته به حجم منابع پردازشی خود افزوده‌اند تا بتوانند روش‌های مقابله با حملات منع سرویس توزیع شده را عملی کنند.

حمله‌ی سایبری DDoS که روی GitHub انجام گرفت به خاطر مقیاس آن و این واقعیت که تهاجم با استفاده از استاندارد Memcached که یک سیستم کش پایگاه‌داده برای سرعت بخشیدن به وبسایت‌های صحنه‌سازی شده بود، قابل توجه است.

بررسی 12 نوع از مشهورترین انواع حملات DDoS

این روزها در خبرهای حوزه امنیت، بسیاری از خبرها متعلق به انجام حملات DDoS به زیر ساخت ها است و بسیاری از سازمان ها در حال حاضر متوجه شده اند، هر گونه کسب و کار، صرف نظر از اندازه و مکان آن، یک هدف برای حملات انکار سرویس توزیع شده (DDoS) است.

حملات DDoS شامل حملاتی است که بصورت سیل آسا، وب سایت سازمان را با حجم زیادی از ترافیک مورد حمله قرار میدهند، با این هدف که سایت سرویس دهنده را آفلاین نمایند که منجر به قطع دسترسی به سرویس مورد نظر میگردد. کسانی که تحت تأثیر حملات DDoS قرار می گیرند، اغلب از زمان خراب شدن رنج می برند، که منجر به زیان مالی و صدمه به شهرت آنها می شود.

یکی از گسترده ترین حملات DDoS که تا کنون رخ داده است، در سال 2016 اتفاق افتاد، زمانی که سرویس دهنده های DNS ارائه کننده Dyn آنلاین نبودند. از آنجایی که Dyn یک ارائه دهنده DNS است، بسیاری از سازمان های جهانی بر روی دسترسی به سرویس های خود متکی بودند تا اطمینان حاصل شود که وبسایت ها قادر به اجرای آن هستند. این در نهایت به این معنی بود که وقتی Dyn به صورت آفلاین قرار گرفته شد، بر روی بسیاری از سازمان های دیگر نیز تاثیر مستقیم گذاشت. وب سایت های مهم که تحت تاثیر این حمله قرار داشتند شامل نیویورک تایمز، توییتر Pinterest، Reddit، Tumblr، GitHub، Etsy، Spotify، PayPal و Verizon بود. این حملات نه تنها موجب ناراحتی زیادی برای سازمانها و مشتریان آنها شد، بلکه می تواند به طور قابل توجهی از لحاظ مالی هم همه آنها را تحت تاثیر قرار دهد.

به علت آسیب قابل توجهی که ممکن است یک حمله DDoS ایجاد شود، بسیاری از تیم های فناوری اطلاعات در مقابل تهدید قرار می گیرند. با این حال، چه بسیاری از تیم های فناوری اطلاعات ممکن است کاملا ناآگاه از آن باشد که مجرمان سایبری انواع مختلفی از انواع حملات DDoS را در مشت خود دارند و به فراخور زمان ممکن است از یک یا ترکیبی از انها استفاده نمایند.

در زیر به 12 نوع از مهمترین حملات DDoS اشاره شده است که از خطرناک ترین و مضرترین حملات هستند و دانستن در مورد آنها به تیم های امنیتی کمک می کند تا با داشتن برنامه های مناسب برای دفاع و مقابله با آنها، از خود محافظت نمایند:

1 - DNS Amplification: این حمله یک نوع "انعکاس" حمله است که در آن یک عامل مرتکب شده اقدام به زدن کوئری هایی میکند که از آدرس آی پی تقلبی قربانی مورد نظر استفاده می کنند. استفاده از آسیب پذیری ها در سرورهای نام دامنه (DNS) ، پاسخ ها را به بسته های UDP بسیار بزرگتر کرده و سرورهای هدف، فلود می شوند.

2 - UDP Flood : در این حمله، مهاجم از بسته های IP حاوی دیتاگرام UDP برای قرار دادن پورت های تصادفی در یک شبکه هدف استفاده می کند. سیستم قربانیان تلاش می کند تا هر یک از استراتژی های دیتاگرام را با یک برنامه مطابقت دهد، اما نمیتواند و دائم تلاش می کند که جلوی پاسخ بسته ی UDP را بگیرد که این تلاش، بزودی سیستم هدف را خسته کرده و از پاری درخواهد آورد.

3 - DNS Flood : شبیه به حمله UDP Flood است، این حمله شامل عواملی اس که با استفاده از مقادیر جمعی از بسته های UDP برای از بین بردن منابع سرور تلاش میکنند. با این حال، در اینجا، هدف این است که سرورهای DNS و مکانیزم های حافظه پنهان خود را با هدف جلوگیری از تغییر مسیر درخواست های قانونی ورودی به منابع منطقه DNS، فلج نمایند.

4 - HTTP Flood : این حمله به منظور هدف قرار دادن یک برنامه یا وب سرور با استفاده از تعداد زیادی از درخواست HTTP GET یا POST، ظاهرا قانونی انجام میگردد. این درخواستها اغلب برای جلوگیری از تشخیص مجرمان با به دست آوردن اطلاعات مفید در مورد هدف قبل از حمله ساخته شده است.

5 - IP Fragmentation Attack : این حمله اکسپلویت نمودن MTU جهت سرزیر نمودن سرور هدف است. این حمله را می توان با ارسال بسته های ICMP و UDP جعلی که بیش از MTU شبکه است به مقصد ارسال نمود تا منابع سرور به سرعت مصرف شوند تا سیستم نتواند بسته ها را بازسازی نماید و از دسترس خاج شود. مجرمان همچنین می توانند یک حمله Teardrop یا گاز اشک آور را اجرا کنند که با جلوگیری از بازسازی بسته های IP / TCP کار می کند. این حمله نیز شامل ارسال بسته‌های آی پی است که با هم تداخل دارند یا بسته‌هایی با سایز بزرگ یا بسته‌هایی با ترتیب نامناسب می‌باشند. این حمله می‌تواند سیستم عامل‌های مختلف را به علت اشکالی که در کد بازسازی مجدد بخش‌های TCP/IP دارند crash کند.

6 - NTP Amplification: دستگاه های متصل به اینترنت از پروتکل های زمان شبکه (NTP) برای هماهنگ سازی ساعت استفاده می کنند. همانند حمله متمرکز DNS، در اینجا نیز حمله کنندگان از تعداد زیادی از سرورهای NTP استفاده میکنند تا توسط انها بسته های UDP زیادی را به سمت مقصد ارسال کنند تا مقصد از دسترس خارج شود.

7 - Ping Flood - یکی دیگر از حملات سیلاب معمولی که از اکو شدن تعداد زیادی از درخواست های ICMP استفاده میکند. برای هر پینگ فرستاده شده، باید یک پاسخ متقاطع که حاوی همان تعداد بسته است بازگشت شود، لذا سیستم هدف تلاش می کند تا به درخواست های بی شماری پاسخ دهد، در نهایت پهنای باند شبکه خود را مسدود می کند. همچنین ping of death که نوع دیگری از این حمله است نیز، به ارسال‌هایی از بسته‌های ping با فرمت و شکل نامناسب یه سمت قربانی گفته می‌شودکه باعث crash شدن سیستم عامل می گردد.

8 - SNMP Reflection: پروتکل SNMP به مدیران سیستم کمک میکند که اطلاعات مهمی را از سرورهای داخل شبکه کسب نموده و یا دستورات ساده ای را برای این سرورها ارسال نمایند.در این نوع حمله با استفاده از یک آدرس IP جعلی قربانی، یک حمله کننده می تواند بسیاری از درخواست های SNMP را بصورت انفجاری به دستگاه ها بفرستدد، که در ازای هر درخواست، انتظار می رود که به طور صریح پاسخ داده شود. تعداد دستگاه های متصل شده می تواند به صورت دستی به سمت بالا حرکت کند، به طوری که سرعت و کیفیت شبکه در نهایت توسط مقدار پاسخ های SNMP کاهش می یابد.

SYN Flood - 9 : هر جلسه TCP نیاز به برقراری ارتباط سه جانبه بین دو سیستم دارد. با استفاده از یک سیل SYN، مهاجم به سرعت به هدف با درخواست های اتصال بسیاری می پردازد که نمی تواند آن را حفظ کند و منجر به اشباع شبکه شود. در واقع زمانی اتفاق می افتد که میزبانی از بسته‌های سیل آسای TCP/SYN استفاده کند که آدرس فرستنده آن‌ها جعلی است. هر کدام از این بسته‌ها همانند یک درخواست اتصال بوده و باعث می‌شود سرور درگیر اتصالات متعدد نیمه باز بماند و با فرستادن یا برگرداندن بسته‌های TCP/SYN ACK، منتظر بسته‌های پاسخ از آدرس فرستنده بماند ولی چون آدرس فرستنده جعلی است هیچ پاسخی برگردانده نمی‌شود. این اتصالات نیمه باز تعداد اتصالات در دسترس سرور را اشباع می‌کنند و آن را از پاسخگویی به درخواست‌های مجاز تا پایان حمله بازمیدارد. بنابر این منابع سرور به اتصال‌های های نیمه باز اختصاص خواهد یافت. وامکان پاسخ گویی به درخواستها از سرور منع می‌شود.

Smurf Attack - 10 : این نوع حمله به پیکربندی نامناسب تجهیزات شبکه که اجازه ارسال بسته‌ها به همه کامپیوترهای میزبان روی یک شبکه خاص با آدرس‌های همه پخشی را می دهد، متکی است. در چنین حمله‌ای مهاجمان با یک آی پی جعلی یک تقاضای ping به یک یا چندین سرور همه پخشی ارسال کرده و آدرس آی پی ماشین هدف (قربانی) را ست می‌کنند .سرور همه پخشی این تقاضا را برای تمام شبکه ارسال می‌کند. تمام ماشین‌های شبکه پاسخ را به سرور، ارسال همه پخشی می‌کنند. سرور همه پخشی پاسخ‌های دریافتی را به ماشین هدف هدایت یا ارسال می‌کند. بدین صورت زمانی که ماشین حمله‌کننده تقاضائی را به چندین سرور روی شبکه‌های متفاوت همه پخشی می نماید، مجموعه پاسخ‌های تمامی کامپیوترهای شبکه‌های گوناگون به ماشین هدف ارسال می گردند و آن را از کار می اندازند. بنابراین پهنای باند شبکه به سرعت استفاده می‌شود و از انتقال بسته‌های مجاز به مقصدشان جلوگیری به عمل خواهد آمد.برای مبارزه با حمله منع سرویس در اینترنت سرویس‌هایی مانند Smurf Amplifier Registry توانایی تشخیص پیکربندی‌های نامناسب شبکه وانجام عملیات مناسب مثل فیلترینگ را می دهند.

Ping of Death - PoD - 11 : یک شیوه است که هکرها بسته های غیر عادی یا بادکنکی (به وسیله pinging) ارسال میکنند تا حافظه سرور سرریز کرده و کرش کند. سرریز حافظه زمانی اتفاق می افتد که در تلاش برای بازسازی بسته های داده بزرگ باشد. مهاجمان میتوانند از هر نوعی از IP datagram ، از جمله ICMP echo، UDP، IDX و TCP برای حمله استفاده کنند.

Fork Bomb - 12: این حمله DoS از داخل یک سرور هدف آغاز می شود. در یک محیط مبتنی بر یونیکس، یک Fork،یک کپی از والد خود را برای فرزند فراخوانی میکند. هر دو فرآیند می توانند وظایف همزمان را در هسته سیستم مستقل از یکدیگر انجام دهند. با استفاده از یک بمب انفجاری (a.k.a, rabbit virus"")، یک حمله کننده مرتکب بسیاری از Forkهای بازگشتی می شود که سیستم هدف به طور داخلی غرق شده و از دسترس خارج میگردد.

حملات DDoS بسیار قدرتمند هستند و می توانند باعث آسیب مالی و مالی زیادی به سازمان ها شوند. با این حال، در حالی که اهداف و انگیزه های مهاجمین DDoS همیشگی باقی مانده است، روش هایی که استفاده می کنند، به طور مداوم در حال پیشرفت هستند. لذا مدریان شبکه های حتما باید اطلاعات کامل و جامعی از این نوع از حملات داشته باشند تا بتوانند پیشگیری مناسبی را داشته باشند. همچنین بد نیست

که به سایت http://map.norsecorp.com مراجعه کرده و به‌صورت انلاین حملات DDoS انجام شده در دنیا را مشاهده نمایید.

حمله dos چیست؟

قبل از آن‌که حمله انکار سرویس توزیع شده (DDoS) را بررسی کنیم، بهتر است نیم نگاهی به حمله انکار سرویس (DoS) داشته باشیم. تصور کنید سروری، در حال ارایه یک سرویس کاربردی است و به درخواست‌های مختلف کاربران پاسخ می‌دهد. هر سرور، ظرفیت محدودی برای پاسخ‌گویی به درخواست‌های کاربران دارد و اگر به آستانه اشباع برسد، قادر نیست در زمان مناسب به درخواست‌ها پاسخ دهد.

یکی از اصلی‌ترین روش‌هایی که هکرها برای مختل کردن عملکرد یک سرویس از آن استفاده می‌کنند، سوءاستفاده از ظرفیت محدود سرورها است. اگر کاربری، به‌شکل مستمر برای یک سرور درخواست‌های مکرری ارسال کند، بخشی از ظرفیت سرور را به خود اختصاص می‌دهد و با توجه به محدود بودن منابع سیستمی و ظرفیتی سرور، سرویس از دسترس سایر کاربران خارج می‌شود.

دومین روشی که هکرها برای مختل کردن عملکرد یک سرویس از آن استفاده می‌کنند، ارسال بسته‌های درخواست به گونه‌ای است که بخش عمده‌ای از منابع شبکه را هدف دهند. در دنیای امنیت به این بردار حمله انکار سرویس (DoS) سرنام Denial of Service می‌گویند.

معمولا DoS attack از طریق یک کامپیوتر و آدرس آی‌پی ثابت پیاده سازی می‌شود، به همین دلیل در برخی موارد امکان اضافه کردن آدرس آی‌پی حمله‌کننده به فهرست سیاه وجود دارد.

هدف از هر دو نوع حمله dos و ddos خارج کردن سرور از دسترس کاربران است.

حمله ddos چیست؟

اکنون که با عملکرد حمله DoS آشنا شدید، اجازه دهید به نسخه تکامل یافته‌تر این بردار حمله نیم نگاهی داشته باشیم و ببینیم حمله های از کار انداختن سرویس پخش شده ddos چیست. تصور کنید هکری در نظر دارد عملکرد سرویسی را مختل کند، اما برای مخفی شدن از دید ابزارهای امنیتی به جای استفاده از یک کامپیوتر و آدرس آی‌پی ثابت از چند کامپیوتر که آدرس‌های آی‌پی مختلفی دارند استفاده می‌کند. ویژگی مهم حمله ddos اجرای آن از چند Host مختلف به صورت همزمان است حتی ممکن است هکر از سرور شما برای حمله به سرور دیگری استفاده کند.

مهم‌ترین تفاوت حملات dos و ddos این است که حمله به جای آن‌که از یک نقطه متمرکز انجام شود از مکان‌های مختلفی انجام می‌شود. به این نوع حمله، انکار سرویس توزیع شده (DDoS) می‌گویند. حالا ddos مخفف چیست؟ ddos مخفف Distributed Denial of Service است.

سازمان‌ها و زیرساخت‌های ارتباطی اگر از مکانیزم‌های دفاعی استفاده نکرده باشند بسته به شدت حمله ممکن است در چند دقیقه یا چند ساعت قادر به پاسخ‌گویی به درخواست‌های کاربران نباشند. و شرکت‌هایی

که مکانیزم‌های دفاعی برای مقابله با این حمله ارایه می‌کنند در این زمینه با محدودیت‌های ظرفیتی روبرو هستند.

در یک حمله ddos به دلیل این‌که تعداد درخواست‌های ارسالی از جانب هر ماشین حمله‌کننده، کم‌تر از بردار حمله DoS است، تشخیص ترافیک حمله‌کنندگان سخت‌تر می‌شود. علاوه بر این، ضریب خطا در شناسایی درست ماشین‌هایی که ترافیک مخرب را تولید می‌کنند زیاد است، به همین دلیل اگر ترافیک یک ماشین به اشتباه مخرب شناسایی شود، دسترسی کاربر به یک سرویس یا سایت قطع می‌شود.

ddos به زبان ساده از دسترس خارج کردن منابع و برنامه‌های کاربردی و سرویس‌های یک شبکه برای کاربران مجاز آن شبکه است.

انگیزه هکر از انجام حمله ddos اغلب در امور مربوط به سیاست و ایدئولوژی افراد و خرابکاری و بازی‌های آنلاین است. مثلا شرکت یوبی سافت یکی از تولیدکنندگان بازی‌های کامپیوتری استرالیایی است، که بازی محبوب رینبو (Rainbow Six Siege) آن مورد حمله دیداس قرار گرفته است. در حملات مربوط به بازی‌های کامپیوتری ممکن است مهاجم فقط برای یک برد و باخت ساده اقدام به انجام حملات ddos کند.

انواع حملات ddos چیست؟

حملات دیداس عموما در سه گروه گسترده دسته بندی می‌شوند، حملات حجمی، حملات بر پایه TCP و حملات لایه کاربردی که تفاوت‌های زیادی با هم دارند:

حملات حجمی یا Volumetric: روش این نوع حمله از کار انداختن زیرساخت شبکه با استفاده از اشغال کل پهنای باند شبکه است. رایج ترین نوع حملات ddos از نوع حجمی هستند.

حملات بر پایه TCP: در این روش با سو استفاده از حالت Stateful طبیعی پروتکل TCP، منابع سرورهای Load-Balancer و فایروال‌ها مختل می‌شوند.

حملات لایه‌ی برنامه‌های کاربردی یا حملات Application Layer: در این روش به قسمتی از یک برنامه کاربردی یا سرویس لایه هفتم حمله می‌شود.

حملات جدیدی که از ترکیب هر سه روش و افزایش مدت زمان و مقیاس استفاده می‌کنند، در حال افزایش هستند.

اکنون که دانستیم حملات dos و ddos چیست و با کلیت این بردار حمله آشنا شدیم می‌توانیم درباره جزییات فنی این بردار حمله اطلاعاتی ارایه دهیم. برای آن‌که مطلب روال خسته‌کننده‌ای پیدا نکند و همزمان با مباحث فنی، اطلاعات کامل‌تری نیز به دست آورید، جزییات فنی این بردار حمله در قالب انواع مختلف بردارهای حمله ddos بررسی شده‌اند.

حمله icmp flood چیست؟

حمله icmp flood بیشتر مبتنی بر حمله dos است. به این معنا که حمله‌کننده پیام‌های سیل‌آسایی برای قربانی ارسال می‌کند تا سرور از دسترس خارج شود. اگر پیام‌ها از ماشین‌های متفاوتی ارسال شوند، حمله رویکرد ddos به خود می‌گیرد. به‌طور معمول، هکرها از روش‌های مختلفی برای پیاده سازی این حمله استفاده می‌کنند. ساده‌ترین روش، ارسال متوالی پیام‌های پینگ از طریق خط فرمان برای سرور هدف است. البته روش فوق این عیب را دارد که ظرفیت و پهنای باند دستگاه هکر را نیز مصرف می‌کند.

چون در حمله سرریز پروتکل icmp پیام‌ها در قالب پینگ ارسال می‌شوند. برخی منابع از اصطلاح ping flood attack برای توصیف این حمله استفاده می‌کنند. به‌طور معمول پینگ برای بررسی ارتباط دو دستگاه و محاسبه زمان رفت و برگشت بسته‌ها میان دو دستگاه استفاده می‌شود مثلا هنگامی که قصد داریم وضعیت ارتباط دو شبکه محلی با یکدیگر یا وضعیت متصل بودن یک سرور به سرور دامین کنترلر را بررسی کنیم.

کارشناسان امنیتی برای مقابله با حمله icmp flood، پروتکل icmp روی شبکه را غیر فعال می‌کنند که البته این‌کار امکان استفاده از فرمان پینگ را غیرممکن می‌کند.

دومین روش پر کاربرد برای پیاده سازی حمله icmp flood سواستفاده از ماشین‌های دیگر است که مبتنی بر بردار حمله بات‌نتی است. در این روش، هکر به دستگاه‌های تسخیر شده (زامبی) فرمان می‌دهد به یک آدرس مشخص پیام پینگ ارسال کنند. در این حالت، حجم بالایی از بسته‌ها توسط دستگاه‌های قربانی برای هدف ارسال می‌شوند و هکر نیز هویت خود را پنهان باقی نگه می‌دارد.

سومین روش پیاده‌سازی، حمله اسمورف – Smurf attack است. این روش نیز شباهت زیادی به حالت قبل دارد. حمله smurf چیست؟ این نوع حمله سه محور اصلی دارد؛ سایت مبدا، سایت پرش یا Bounce، سایت هدف. مهاجم از سایت مبدا بسته اطلاعاتی از نوع ping را برای آدرس سایت پرش Broadcast می‌کند، اطلاعات در کل شبکه پخش می‌شود، تمام سیستم‌ها پاسخ را به جای فرستادن به سایت مبدا به سایت هدف ارسال می‌کنند. در نتیجه سایت هدف به دلیل عدم آمادگی و ناشناس بودن بسته‌های ارسالی امکان پاسخگویی ندارد و Crash خواهد کرد.

syn flood چیست؟

حمله syn flood بر مبنای پروتکل TCP پیاده سازی می‌شود. فرض کنید قرار است یک کلاینت و سرور بر مبنای پروتکل TCP بسته‌های اطلاعاتی را مبادله کنند. برای آن‌که ارتباط فوق برقرار شود، پروتکل TCP از مکانیزم دست‌دهی سه مرحله‌ای (three-way handshake) استفاده می‌کند.

در این مکانیزم ابتدا کلاینت یک عدد را با پیام SYN برای سرور ارسال می‌کند تا سرور از این عدد برای شماره‌گذاری بسته‌های ارسالی به سمت کلاینت استفاده کند. در ادامه سرور پاسخ خود را در قالب، یک پیام ACK در تایید دریافت SYN و یک پیام SYN با هدفی مشابه پیام SYN قبلی برای کلاینت ارسال

می‌کند. در انتها اگر کلاینت پاسخ ACK را ارسال کند، اتصال TCP برقرار می‌شود. شما روزانه بر مبنای این مکانیزمِ ارتباطی با سرورها و سایت‌ها ارتباط برقرار می‌کنید.

اکنون حالتی را تصور کنید که کاربر پیام SYN اولیه را ارسال و پاسخی از سرور دریافت می‌کند، اما ACK نهایی مورد نیاز برای برقراری ارتباط را برای سرور ارسال نمی‌کند. سرور این ارتباط را باز نگه می‌دارد و برای دریافت پاسخ به انتظار می‌نشیند.

اگر این کار ادامه پیدا کند و درخواست‌ها زیاد شوند، سرور همواره در حالت انتظار برای دریافت پاسخ برای هر کانال ارتباطی قرار می‌گیرد و با توجه به محدودیت در منابع به سایر درخواست‌های کاربران پاسخ نخواهد داد و سرویس دهی دچار اختلال می‌شود. این بردار حمله، پیام‌های سیل‌آسا (SYN Flood) نیز نام دارد که مبتنی بر ارسال حجم گسترده‌ای از بسته‌های SYN برای یک سرور و عدم دریافت پاسخ ACK هستند.

این حمله به دلیل نقص ذاتی پروتکل TCP به وجود می‌آید و راه‌حلی برای آن وجود ندارد، زیرا هنگامی که پروتکل tcp ابداع شد، اینترنت به شکل امروزی آن نبود و هیچ کارشناسی تصور نمی‌کرد، روزگاری هکرها بتوانند از این نقطه ضعف ذاتی سواستفاده کنند.

udp flood چیست؟

حمله udp flood در هر دو بردار حمله‌های dos و ddos قابل استفاده است. در این بردار حمله بسته‌های udp به تعداد زیاد به پورت‌های یک سرور ارسال می‌شوند و سرور را مجبور به پاسخ‌گویی می‌کنند. در شرایط عادی، هنگامی که سرور یک بسته udp دریافت کند، برنامه‌ای که مربوط به پورت مقصد بسته است را پیدا می‌کند و بسته را تحویل می‌دهد. اگر پورت مقصد بسته متعلق به هیچ برنامه‌ای نباشد، سرور یک پیام ICMP با عنوان مقصد در دسترس نیست (Destination Unreachable) برای مبدا ارسال می‌کند.

اگر مهاجم به شکل مداوم بسته ICMP را به شکل تصادفی برای پورت‌های مختلفی از سرور ارسال کند ، منابع سرور به سرعت هدر می‌روند و دیگر فرصتی برای پاسخ‌گویی به درخواست‌های کاربران باقی نمی‌ماند.

گاهی در حمله‌های udp flood، از تغییر آدرس آی‌پی برای عدم شناسایی آدرس اصلی استفاده می‌شود. در این روش، شناسایی مبدا حمله تقریبا ناممکن است و هنگامی که پیام‌های icmp از جانب سرور ارسال می‌شوند برای آدرس‌های آی‌پی دیگری می‌روند و در عمل شبکه‌ای که هکر برای این منظور از آن استفاده کرده به مرز اشباع نمی‌رسد و حمله تداوم پیدا می‌کند.

برای پیش‌گیری از بروز حمله udp flood، می‌توان ارسال پیام‌های ICMP را تا حد امکان محدود کرد یا به‌طور کل سرویس فوق را روی سرور غیرفعال کرد. پیام‌های ICMP بیشتر برای اطلاع‌رسانی وضعیت شبکه استفاده می‌شوند و غیرفعال کردن آن‌ها تاثیری بر عملکرد سایر سرویس‌ها ندارد.

فایروال‌ها نیز تا حدودی قادر به مقابله با این حمله هستند. می‌توان در زمان حمله، بسته‌هایی که از پروتکل udp استفاده می‌کنند را محدود کرد و مانع ورود آن‌ها به شبکه شد. البته در شرایطی که حمله فراگیر باشد، پردازش تمام این بسته‌ها می‌تواند دیوار آتش را زمین‌گیر کند.

به‌طور کلی بهتر است سرویس‌های غیرضروری که از پروتکل udp استفاده نمی‌کنند را غیرفعال کرد و پورت‌های مربوط به آن‌ها را بسته نگه داشت و تنها تعدادی از آن‌ها که ضروری هستند مثل پورت ۵۳ که سرویس dns از آن استفاده می‌کند را باز نگه داشت.

حمله http flood چیست؟

حمله http flood با هدف مصرف بیش از اندازه منابع سرور از طریق ارسال درخواست‌های مبتنی بر پروتکل http انجام می‌شود. این حمله بیشتر با هدف از دسترس خارج کردن یک سرویس استفاده می‌شود و بیشتر از طریق دستورات GET و POST پیاده سازی می‌شود. در این روش، درخواست‌ها شباهت زیادی به درخواست‌های عادی دارند. این حمله به پهنای باند کمی نیاز دارد در نتیجه شناسایی و پیشگیری از بروز آن کار مشکلی است. حمله‌های http flood به روش‌های مختلفی انجام می‌شوند مثلا استفاده از get و post. این دو دستور پرکاربردترین دستورات پروتکل http هستند که هکرها برای مشغول نگه‌داشتن سرور از آن استفاده می‌کنند.

روش GET: متد get به منظور دریافت اطلاعات از سرور استفاده می‌شوند. هنگامی که هکرها تصمیم می‌گیرند از آن استفاده کنند، شروع به ارسال تعداد زیادی درخواست می‌کنند. حمله با متد get نسبت به متد post به منابع بیش‌تری برای پیاده سازی نیاز دارد، اما پیچیدگی کمی دارد. در بیشتر موارد برای پیاده‌سازی حمله فوق از بات‌نت‌ها استفاده می‌شود.

روش POST: دومین دستوری که هکرها به سوء استفاده از آن می‌پردازند، متد POST است. این متد برای ارسال یک فرم یا اطلاعات برای سرور استفاده می‌شود. هر فرمی که برای سرور ارسال می‌شود باید در یک پایگاه داده ثبت شود که این فرآیند، زمان‌بر و از نظر پردازشی سنگین است. هنگامی که هکرها تصمیم می‌گیرند از این متد سواستفاده کنند، به اندازه‌ای درخواست‌های post برای سرور می‌کنند که پهنای باند سرور برای درخواست‌های ورودی پاسخ‌گو نباشد یا سرور منابع زیادی را صرف درخواست‌های مرتبط با پایگاه داده کند و دیگر منابعی برای پاسخ‌گویی به درخواست‌های دیگر نداشته باشد.

روش‌های مقابله با حمله http flood عبارتند از:

برای مقابله با حمله http flood بهترین ابزاری که در دسترس شرکت‌ها قرار دارد به‌کارگیری الگوی کپچا است که برای شناسایی کاربر واقعی استفاده می‌شود.

دومین روش پر کاربرد، دیوارهای آتش وب‌محور (WAF) سرنام web application firewall هستند که قادر به ارزیابی الگوهای رفتاری کاربران هستند و مانع ورود ترافیک مشکوک به زیرساخت‌ها می‌شوند. این دیوارهای آتش با نمونه‌های سنتی تفاوت‌هایی دارند و در لایه کاربرد کار می‌کنند.

این دیوارهای آتش، ترافیک ورودی یک برنامه وب و آی‌پی کاربران ارسال‌کننده را زیر نظر می‌گیرند و آدرس‌های آی‌پی را درون یک بانک اطلاعاتی ذخیره می‌کنند. با استفاده از این اطلاعات، خط‌مشی‌ها و الگوهایی که از قبل برای فایروال تعریف شده، هر وقت دیوارآتش رفتاری شبیه به حمله را مشاهده کند، ترافیک ورودی را مسدود می‌کند و مانع شکل‌گیری موفقیت‌آمیز حمله می‌شود. علاوه بر این، دیوارهای

آتش می‌توانند با تحلیل محتوای درخواست‌های http، مانع بروز حمله‌های دیگری نظیر تزریق کد اس‌کیوال شوند.

حمله dns flood چیست؟

حمله سرریز سامانه نام دامنه یکی از پیچیده‌ترین انواع حمله دیداس است. برخی منابع از اصطلاح حمله تقویت شده -amplification attack برای توصیف آن استفاده می‌کنند. در حمله dns flood، هکر بسته‌هایی با اندازه بسیار کم ارسال می‌کند که سرور را مجبور به پاسخ‌گویی می‌کند، پاسخ‌گویی که زمان‌بر هستند و توالی آن‌ها باعث می‌شود منابع سرور بیهوده هدر روند.

در حمله dns flood، هکر درخواست‌های dns زیادی را بر مبنای مکانیزم جعل آدرس آی پی (ip spoofing) برای سرور ارسال می‌کند. البته در روش فوق هدف سرورهای DNS هستند که نقش دامین کنترلرها را عهده‌دار هستند. سرور dns مجبور است به محاوره‌های مرتبط با dns که شامل پیدا کردن نام دامنه هستند پاسخ دهد که زمان زیادی از سرور می‌گیرد و باعث می‌شوند سرور نتواند به سایر درخواست‌های مرتبط با dns که شامل تبدیل نام‌ها به آدرس‌های آی‌پی و بالعکس می‌شوند، پاسخ دهد، زیرا منابع بیهوده هدر رفته‌اند.

حمله slowloris چیست؟

حمله slowloris در لایه کاربرد پیاده سازی می‌شود و در تعامل با پروتکل http است. مکانیزم حمله slowloris به این صورت است که بعد از ایجاد یک کانال ارتباطی موفق میان هکر و سرور، هکر تا حد امکان ارتباط را باز نگه دارد. برای این منظور، درخواست‌های ناقص و با سرعت کم برای سرور ارسال می‌کند. در این حالت سرور مجبور است بخشی از منابع پردازشی را برای باز نگه داشتن این کانال ارتباطی اختصاص دهد و صبر کند تا پاسخ‌هایی از جانب کاربر ارسال شوند که هیچ‌گاه این اتفاق نمی‌افتد.

اگر هکر حجم زیادی از درخواست‌ها را ارسال کند، بخش عمده‌ای از منابع سرور هدر می‌روند. خوشبختانه برای این حمله slowloris مکانیزم دفاعی خوبی وجود دارد. به احتمال زیاد، بارها مشاهده کردید، هنگامی که یوتیوب را باز می‌کنید، صفحه کپچا را مشاهده می‌کنید که یوتیوب اعلام می‌کند ترافیک غیرعادی از طرف آدرس آی‌پی شما ارسال شده و برای حل این مشکل باید به سوال امنیتی پاسخ دهید. این مکانیزم برای دو منظور استفاده می‌شود. اول آن‌که اگر حمله‌ای قرار است اتفاق بیفتد با تاخیر روبرو شود، اگر کاربر بات است با مکانیزم کپچا شناسایی شود یا اگر روند حمله قرار است تداوم پیدا کند، آدرس ip به فهرست سیاه منتقل شود.

حمله ترموکس چیست؟

حمله ترموکس یکی از خطرناک‌ترین حملات دیداس است که ضریب موفقیت آن از تمامی انواع حمله ddos بیشتر است. بردار حمله DDoS به روش‌های مختلف قابل انجام است، به‌طور مثال از سامانه‌های آلوده به تروجان برای پیاده سازی حملات dos و ddos استفاده می‌شود. در این بردار حمله سامانه قربانیان

(تسخیر شده) و اهداف به‌طور کامل تحت کنترل هکر قرار می‌گیرند و مالکان سایت‌ها در عمل کار چندان خاصی نمی‌توانند انجام دهند مگر آن‌که هدف آسیب دیده را به‌طور کامل از شبکه جدا کرده و اقدام به پاک‌سازی آن کنند.

در حمله ترموکس، ترافیکی اجماع شده توسط ماشین‌های مختلف به سمت هدف ارسال می‌شود. حمله‌ای که ممکن است بالغ بر صدها هزار یا بیشتر کلاینت در آن شرکت داشته باشند و منابع مختلف سرور را به سرعت مصرف کنند؛ یعنی cpu، حافظه اصلی یا دیسک‌های جانبی قربانی مورد حمله قرار می‌گیرند.

سرپرستان شبکه نمی‌توانند با مسدود کردن یک آدرس آی‌پی این حمله را متوقف یا مهار کنند. علاوه بر این، تشخیص ترافیک کاربر مشروع از ترافیک مخرب با توجه به کثرت آدرس‌های آی‌پی کار سختی است. این حمله با هدف مصرف تمام پهنای باند موجود بین هدف و اینترنت پیاده‌سازی می‌شود.

در حالت کلی هکرها از بات نت‌ها برای پیاده سازی این حمله استفاده می‌کنند، هرچند امکان پیاده‌سازی آن از طریق یک دستگاه واحد مثل گوشی اندرویدی نیز وجود دارد. از نظر فنی، تکنیک‌هایی وجود دارد که شدت این حمله را کم می‌کنند، اما قادر به متوقف کردن کامل آن نیستند. به‌طور مثال، با افزایش پهنای باند می‌توان تا حدودی از شدت این حمله کم کرد تا سرور به‌طور کامل از مدار خارج نشود.

حمله دیداس ترموکس چگونه پیاده سازی می‌شود؟

در ابتدا هکر برنامه Termux را از پلی‌استور دانلود و نصب می‌کند. هنگامی که ابزار فوق را اجرا کنید، یک صفحه خط فرمان در اختیارتان قرار می‌گیرد که اجازه اجرای دستورات لینوکسی را می‌دهد. اکنون باید دستورات زیر را اجرا کنید:

```
$ apt update && upgrade
$ pkg install git
$ pkg install paython2
$ git clone https://github.com/ujjawalsaini3/hulk
```

پس از نصب ملزومات اولیه در ادامه دستورات زیر را اجرا کنید:

```
$ cd hulk
$ chmod + x hulk.py
$ python2 hulk.py “Url Target
```

در آخرین دستور باید آدرس سایت موردنظر را وارد کنید تا حمله آغاز شود. به‌طور معمول، سایت‌هایی که از پروتکل HTTP به شکل گسترده استفاده کنند با اجرای این حمله از کار خواهند افتاد. دقت کنید

سایت‌هایی که توسط زیرساخت‌های قدرتمندی نظیر کلادفلیر پشتیبانی می‌شوند از ویژگی شناسایی آدرس حمله‌کننده برخوردار هستند با شکست روبرو می‌شوند.

دیداس رینبو چیست؟

در ژانویه ۲۰۲۰ شرکت بازی‌سازی یوبی‌سافت علیه اپراتورهای SNG.one شکایتی ثبت کرد. وب‌سایتی که ادعا می‌شود حملات دیداس علیه بازی‌های آنلاین از جمله Rainbow Six Siege را ترتیب داده است. در حکم اولیه که اوایل سال ۲۰۲۰ تصویب شد، دادگاه منطقه‌ای ایالات متحده رای را به نفع یوبی‌سافت صادر کرد و این شرکت توانست مبلغ ۱۵۳۰۰۰ دلار غرامت از SNG.one دریافت کند. تا قبل از ثبت شکایت، وب‌سایت SNG.one خود را به‌عنوان یک سرویس آزمایش دیوارهای آتش در برابر حمله‌های سایبری معرفی کرده بود، اما یوبی‌سافت ادعا کرد که اپراتورهای این شرکت خدمات خود را در اختیار سایت‌هایی مثل r6s.support قرار داده‌اند که به‌طور خاص حمله Rainbow Six Siege که یک بردار حمله DDoS است را علیه زیرساخت‌های این شرکت ترتیب داده‌اند.

علاوه بر این، ادعا شد که هنگام تشکیل پرونده، متهمان به سرعت شواهد مربوط به دخالت خود در حمله را پنهان کردند. یوبی‌سافت در شکوایه خود به این نکته اشاره کرد که شرکت مذکور مجوزهای دسترسی به خدماتی که برای پیاده سازی حملات دیداس استفاده می‌شوند را به قیمت ۱۰ یورو (۱۱.۱۱ دلار) برای ۳۰ روز دسترسی و یک حمله همزمان در اختیار کاربران عمومی قرار داده است و در صورتی که متقاضیان مبلغ ۲۷۰ یورو (۲۹۹.۸۵ دلار) را پرداخت کنند دسترسی مادام‌العمر به یک شبکه VIP و حداکثر سه مورد پیاده‌سازی حمله همزمان را خواهند داشت.

یوبی‌سافت در شکوایه خود علیه شرکت SNG.one به پنج اتهام بزرگ از جمله نقض قانون، کلاهبرداری و سوء استفاده از کامپیوترها، نقض قانون دسترسی به اطلاعات رایانه‌ای، تقلب و مداخله عمدی در کانال‌های ارتباطی این شرکت اشاره کرد. بد نیست بدانید که حملات DDoS دردسرهای زیادی برای بازی‌های Rainbow Six Siege به وجود آوردند و ضرر مالی زیادی به شرکت یوبی‌سافت وارد کردند، با این‌حال شرکت یوبی‌سافت اوایل فروردین‌ماه، اعلام کرد از مکانیزم‌های امنیتی قدرتمندی برای بهبود زیرساخت‌های خود استفاده کرده و توانسته است تا ۹۳ درصد از شدت حملات به زیرساخت‌های خود کم کند.

نرم افزار حمله ddos

حمله‌های انکار سرویس با هدف از دسترس خارج کردن سرویس‌های مورد استفاده کاربران به مرحله اجرا در می‌آیند. این حمله‌ها می‌توانند دسترسی به خدمات وب‌محور مهمی مثل وب‌سایت، زیرساخت‌های ارتباطی، ایمیل، شبکه‌های اجتماعی و غیره را مختل کنند. در تمامی موارد، این حمله‌ها سیلی از بسته‌های اطلاعاتی را به سمت قربانیان هدایت می‌کنند، به‌طوری که سرورها پس از گذشت چند ساعت از کار خواهند افتاد.

هکرها برای پیاده سازی حملات ddos به ابزارهایی نیاز دارند که قابلیت ارسال بسته‌های اطلاعاتی را داشته باشند. این ابزارها به دو گروه رایگان و غیر رایگان تقسیم می‌شوند:

ابزارهای غیر رایگان در بازارهای دارک‌وب به فروش می‌رسند و در قالب کیت‌های مخرب در دسترس هکرها قرار می‌گیرند.

گروه دوم ابزارهایی هستند که جنبه عمومی دارند و با کمی جست‌وجو قادر به پیدا کردن این ابزارها هستید.

نکته‌ای که باید در مورد ابزارهای عمومی و بعضا رایگان به آن‌ها اشاره کرد این است که برخی از این ابزارها برای پیاده سازی حملهات داس طراحی نشده‌اند و برای انجام کارهایی نظیر تحلیل وضعیت شبکه استفاده می‌شوند، اما اگر به شکل معکوس استفاده شوند، قادر به پیاده سازی بردارهای حمله مخربی مثل داس هستند. از ابزارهای مهمی که در دسترس عموم کاربران قرار دارد عبارتند از:

HTTP Unbearable Load King: شبکه‌ای مجازی از کامپیوترها است که هیچ‌گونه پیوند فیزیکی میان آن‌ها وجود ندارد و تمامی ارتباطات از طریق سوییچ‌ها و سرورهای مجازی انجام می‌شود. به بیان دقیق‌تر، این ابزار مبتنی بر الگوی وب‌سرور است. ابزار hulk با هدف تولید و ارسال حجم گسترده‌ای از ترافیک‌ها در یک وب‌سرور و ارسال آن‌ها برای هدف طراحی شده است.

از قابلیت‌های جالب توجه این نرم افزار حمله ddos باید به توانایی آن در دور زدن سرور کش اشاره کرد. ابزار هالک، به هکرها اجازه می‌دهد تا یک ترافیک مبتنی بر الگوی نظیر به نظیر را پیاده‌سازی کنند که همین مسئله مبدا پیاده‌سازی این حمله را با مشکل روبرو می‌کند. کدهای این ابزار متن‌باز به شکل رایگان در گیت‌هاب در دسترس کاربران قرار دارد.

PyLoris: این ابزار بیشتر برای شناسایی آسیب‌پذیری‌های مستتر در شبکه‌ها استفاده می‌شود، اما قابلیت پیاده سازی حملات ddos را نیز دارد. کاری که انجام می‌دهد این است که ارتباطات ضعیف و کانال‌های ارتباطی که به درستی محافظت نشده‌اند را شناسایی می‌کند. از از قابلیت‌های مهم این نرم افزار حمله ddos وجود یک رابط گرافیکی قدرتمند است که گزارش لحظه‌ای درباره حمله‌ها ارایه می‌کند.

کاری که نرم افزار pyloris انجام می‌دهد این است که از سرآیندهای پروتکل HTTP برای پیاده سازی حملات DDoS استفاده می‌کند، بنابراین اگر در زمان کدنویسی وب‌سایت‌ها به این نکته دقت نکرده باشید، سایت به راحتی قربانی این ابزار می‌شود. این ابزار قابلیت کار با اسکریپت‌های پایتون را دارد بنابراین از کدهای بهینه و مختصری برای پیاده سازی حمله‌ها استفاده می‌کند. این ابزار چند پلتفرمی می‌تواند به راحتی به کانال‌ها و پورت‌ها حمله کند.

Tor’s Hammer: از لایه کاربرد استفاده می‌کند و هکرها از آن برای حمله به هر دو گروه برنامه‌های وب‌محور و وب‌سایت‌ها استفاده می‌کنند. عملکرد این نرم افزار حمله دیداس متفاوت از ابزارهایی است که در ادامه با آن‌ها آشنا می‌شوید، زیرا حمله‌های مبتنی بر مرورگر را انجام می‌دهد.

این ابزار می‌تواند به شکل خودکار آدرس‌های اینترنتی را به لینک‌هایی تبدیل کند و با متن‌های ساده‌ای قالب‌بندی می‌کند و در ادامه از طریق اتصالات مبتنی بر پروتکل TCP حجم گسترده‌ای از حمله‌ها را پیرامون

هدف انجام دهد. برای انجام این‌کار ابزار فوق از دستور POST پروتکل HTTP استفاده می‌کند تا بتواند حجم بسیار بالایی از بسته‌ها را برای حمله به قربانیان گسیل کند.

DAVOSET: یک ابزار خط فرمان در اختیار هکرها قرار می‌دهد. این ابزار عملکردی تقریبا متفاوت از سایر ابزارها دارد و قادر است از کوکی‌ها برای پیاده سازی حملات دیداس استفاده کند.

DDoS Simulator: این ابزار به زبان سی پلاس‌پلاس نوشته شده و به همین علت سرعت زیادی دارد و قابلیت اجرا روی سکوهای مختلف مثل ویندوز و لینوکس را دارد. این ابزار به‌طور ویژه برای پیاده سازی حملات دیداس علیه هدف‌های خاصی استفاده می‌شود.

عملکرد این نرم افزار حمله ddos مبتنی بر پروتکل TCP است، این توانایی را دارد تا حمله‌های سیلابی یا سرریز بافر را به بهترین شکل پیاده سازی کند و به راحتی وب‌سایت‌ها و حتا مکانیزم‌های مقابله با حمله‌های DDoS را با مشکل روبرو کند.

ابزار DDoSIM قادر به پیاده سازی طیف گسترده‌ای از حمله‌های تحت شبکه است، انواع مختلفی از بردارهای حمله را پیاده سازی می‌کند که همگی آن‌ها مبتنی بر کانال‌های ارتباطی پروتکل TCP هستند. بنابراین مکانیزم‌های امنیتی به صورت طبیعی در برابر حمله‌های پیاده‌سازی شده توسط این ابزار آسیب‌پذیر هستند.

OWASP HTTP POST: یکی دیگر از ابزارهای مخربی است که برای پیاده سازی حمله ddos از پروتکل http استفاده می‌کند. هرچند کارکرد اصلی آن آزمایش عملکرد شبکه است اما قادر است دسترسی به خدمات ارایه شده توسط یک وب‌سایت را مختل کند. به لحاظ فنی، حمله‌هایی که توسط ابزار فوق انجام می‌شوند از لایه کاربرد پروتکل TCP/IP استفاده می‌کنند تا به سرعت منابع سرور را مصرف کنند.

RUDY: برای پیاده سازی حمله‌های DDoS به نشست‌هایی که وب‌سرورها و کاربران ایجاد می‌کنند حمله می‌کند، هرچند قابلیت حمله به برنامه‌های ابرمحور را نیز دارد، به‌طوری که حتا شرکت‌های ارایه‌دهنده خدمات ابری نیز از گزند ابزار فوق مصون نیستند.

یکی از دلایل مهمی که باعث شده نرم افزار rudy نزد هکرها و کاربران مورد توجه قرار گیرد سهولت استفاده است. برای کار با ابزار فوق به دانش فنی خاصی نیاز ندارید و همه چیز آماده استفاده است. کافی است وب‌سایت قربانی را مشخص کنید و صفحاتی که قرار است به آن‌ها حمله کنید را تعیین کنید و تمام؛ ابزار حمله را پیاده‌سازی می‌کند.

rudy به جای آن‌که وب‌سرور را در حالت انتظار قرار دهد از فیلدها و پیام‌های طولانی برای ارسال بسته‌های سیل‌آسا استفاده می‌کند. رابط کاربری آن می‌تواند فرم‌هایی که برای ارسال اطلاعات در سایت‌ها قرار دارد را شناسایی کند.

Low Orbit Ion Cannon: ابزار چندسکویی قابل استفاده در سیستم‌عامل‌هایی مثل ویندوز، لینوکس مک، اندروید و iOS است که در اصل برای نظارت بر وضعیت شبکه طراحی شده است، اما هکرها برای پیاده‌سازی حملات دیداس از آن استفاده می‌کنند. این ابزار که مبتنی بر دات‌نت و Mono است و به زبان

سی شارپ نوشته شده است، اولین بار در سال ۲۰۱۴ میلادی منتشر شد. ابزاری که برای ارسال درخواست‌های مبتنی بر پروتکل‌های HTTP، TCP و UDP برای سرورها از آن استفاده می‌شود.

از مهم‌ترین قابلیتی که LOIC در اختیار کاربران قرار می‌دهد آزمایش عملکرد و وضعیت شبکه است اما امکان پیاده سازی حمله DDoS قدرتمند را بر علیه هر وب‌سایتی می‌دهد. این ابزار خالی از اشکال نیست و آدرس آی‌پی حمله کنند را پهنان نمی‌کند، حتا اگر حمله‌کننده از پروکسی سرور استفاده کرده باشد، زیرا در اصل برای آزمایش وضعیت شبکه طراحی شده تا تسترهای شبکه بتوانند پایداری شبکه و خدمات را ارزیابی کنند. کارشناسان امنیت از این نرم افزار برای شناسایی برنامه‌هایی که هکرها برای حمله به شبکه‌ها از آن‌ها بهره می‌برند استفاده می‌کنند.

High Orbit ION cannon: ابزار متن‌باز رایگان دیگری است که کاربردی دوگانه دارد و برای ارزیابی وضعیت شبکه یا پیاده سازی حمله‌های DDoS از آن استفاده می‌شود. می‌تواند به فراتر از یک هدف حمله کند و به‌طور همزمان به آدرس‌های اینترنتی مختلفی حمله کند. این ابزار برای پیاده سازی حملات ddos از پروتکل انتقال ابر متن ساده HTTP استفاده می‌کند.

از مهم‌ترین امکانات ابزار فوق باید به پیاده‌سازی بالغ بر ۲۰۰ حمله به‌طور همزمان اشاره کرد. رابط کاربری آن به هکرها کمک می‌کند در زمان پیاده‌سازی حمله‌ها، شدت تاثیرگذاری آن‌ها را مشاهده و ارزیابی کنند. این ابزار چندسکویی است و قابلیت اجرا روی سیستم‌عامل‌های ویندوز، لینوکس و مک را دارد. یکی از تفاوت‌های ابزار فوق با نمونه‌های مشابه در این است که به حمله‌کنندگان اجازه می‌دهد تا شدت حمله‌ها را تنظیم کنند.

جلوگیری از حملات ddos

تشخیص حملات ddos و مقابله با آنها کار مشکلی است، اما این امکان وجود دارد که بتوان ترافیک هکر را به شکل دقیق‌تری شناسایی کرد و به میزان قابل توجهی جلوی حمله را گرفت.

محافظت کامل شبکه در برابر حملات ddos تقریبا غیر ممکن است، زیرا کاربر مهاجم با داشتن حداقل امکانات نیز می‌تواند تداخل شدیدی در شبکه ایجاد کرده و آن را از دسترس خارج کند، بهترین روش برای محافظت در برابر حملات ddos تنظیم دقیق سرورهای شبکه و قراردادن پروتکل‌های مانند NTP و DNS و SSDP و SNMP و Chargen روی سرورهای اختصاصی با امنیت بالاست.

سرورهای شبکه باید طی یک برنامه ریزی منظم و مداوم تست و آزمایش شوند تا آسیب پذیری‌های احتمالی شبکه مشخص و رفع شوند، استفاده از فیلترهای Anti-Spoofing یکی دیگر از روش‌های محافظتی در برابر حملات ddos از نوع Spoofed Source IP است. (حمله به شبکه با ایجاد ترافیک زیاد با استفاده از IPهای گمراه کننده) این نوع حمله با کمترین منابع قابل انجام است و حتی امکان از دسترس خارج کردن سایت‌های بزرگ با امنیت بالا را نیز دارد. یک سازمان باید روی ایجاد بالاترین سطح امنیت در شبکه تمرکز کند.

روش ساده و کارآمد برای شناسایی حملات ddos تهیه سه چک لیست برای شبکه سازمان است:

چک لیست نظارت و تحلیل ترافیک وب سایت: در این روش گزارش‌های مربوط به ترافیک وب سایت کنترل و هرگونه ترافیک غیرعادی بررسی می‌شود.

چک لیست بررسی تاخیر وب سایت: در صورتی که به دفعات متعدد بارگیری وب سایت با تاخیر انجام شود نشانه‌ای از حملات ddos است.

چک لیست تاخیرهای طولانی مدت: ترافیک نامشخص، افزایش ناگهانی و غیرعادی بارکاری پردازنده تا حدود ۱۰۰% و هر عملیات مشکوک دیگری نشانه‌ای از حمله ddos است.

راهکارهای ایجاد امنیت در مقابل اختلال سرویس

در این مقاله به راهکارهای موثری برای مقابله با این حمله‌ها اشاره کردیم، اما برای مقابله با حمله‌های فوق به دو نکته زیر نیز دقت کنید:

اول اینکه برای غلبه بر این بردار حمله باید به فکر تشخیص ترافیک هکر باشید. برای این منظور باید خط‌مشی و تعریف مشخصی برای الگوی ترافیک عادی داشته باشید تا بر مبنای آن، امکان تشخیص ترافیک کاربر واقعی از هکر فراهم شود. این راهکار در کنار تکنیک‌های دیگر کمک می‌کند تا ترافیک واقعی را از ترافیک تولید شده توسط بات‌های حمله‌کننده متمایز کرد. دوم اینکه برای تشخیص حملات ddos از مکانیزم فیلترینگ استفاده کنید. فیلتر ترافیک در لایه شبکه و فایروال مانع رسیدن ترافیک به سرور می‌شود.

در مجموع ایجاد امنیت و دفاع در برابر حملات ddos به دو بخش تقسیم می‌شود:

۱- دفاع قبل از حمله ddos که از راه حل‌های زیر می‌توان استفاده کرد:

پیکربندی قوی فایروال

به کارگیری ارائه دهنده امنیت وب

زیرساخت‌هایHoneypot

امنیت حرفه‌ای شبکه

۲- دفاع از سیستم در زمان حمله ddos که از روش‌های زیر ممکن است:

فیلتر ترافیک ورودی شبکه

فیلترینگ IP براساس تاریخچه

تغییر آدرسIP

Load balancing

راه‌حل‌های این چنینی به میزان چشم‌گیری مانع بروز حمله‌ها می‌شوند، اما به شکل قاطع نمی‌توانند از سرویس‌ها در برابر حمله‌ها محافظت کنند. به همین دلیل کارشناسان امنیتی پیشنهاد می‌کنند از راه‌حل‌هایی

مثل proxy server و انتقال سرویس استفاده کنید تا اگر هکری موفق شد از فیلترها عبور کند، خسارت کمتری به زیرساخت‌ها وارد شود و دسترسی به خدمات مختل نشود.

حمله ddos با cmd

نرم افزار حمله ddos نرم افزار رایگان ترموکس است که به عنوان یکی از روش‌های ایجاد حمله ddos استفاده می‌شود اما روش ساده تر، استفاده از محیط cmd ویندوز است، برای این کار مراحل زیر را انجام دهید:

منو Start داخل قسمت Run کلمه cmd را سرچ کنید.

در پنجره ظاهر شده دستور Ping را برای یافتن آدرس IP سایت یا سرور هدف خود تایپ کنید. Ping را با آدرس سایت هدف بدون http:// یا https:// وارد کنید.

با دستور Ping Ip -t -i 0 حمله ddos شروع خواهد شد: به جای Ip، آی پی هدف و به جای 0 حجم بسته‌های ارسالی به سمت سایت هدف را مشخص کنید.

پایان.