ماجرای حمله DDoS به زیرساخت اینترنت ایران چه بود؟

داستان یک هجوم سایبری

آرش جهانگیری

شاید شما هم در هفته گذشته متوجه اختلالات به‌وجود آمده در اینترنت ایران شده باشید. شاید هم آن را پای کند شدن‌های گاه و بی‌گاه اینترنت کشور گذاشته باشید، اما واقعیت این است که در روزهای گذشته زیرساخت اینترنت کشـــور دچار بی‌سابقه‌ترین حمله دی‌داس شده بود. این حمله به گفته مدیرعامل شرکت ارتباطات زیرساخت، بزرگ‌ترین حمله دی‌داسی است که به این سیستم وارد شده و تعداد درخواست‌ها به ۱۸۰ میلیون در ثانیه هم رسیده است. البته این حملات کنترل شده و به غیر از کندی مقطعی در شبکه اینترنت کشور، تاثیر دیگری نداشته است. اما حمله دی‌داس چیست؟ چه مشکلاتی ایجاد می‌کند و چطور می‌توان جلوی آن را گرفت؟ اینها سؤالاتی است که در این گزارش به دنبال جواب آن هستیم.

حمله دی‌داس چیست؟

فرض کنید شما یک مغازه با اندازه معمولی در یک کوچه دارید و در هر دقیقه یک‌مشتری به مغازه شـما سـر می‌زند. حـالا فرض کنید تمام مشـتریان یک فروشـگاه زنجیره‌ای در زمانـی مشـخص به مغازه شـما سـر بزنند. تبریک می‌گوییم؛ به مغازه شما حمله دی‌داس شده اسـت! در واقع حمله DDoS یا همان Distributed Denial of Service یک حمله به سـرورهای شماسـت که بر اثر حجم درخواست بسـیار بالا اتفاق می‌افتد. این درخواسـت بیش از حد را با شلوغ شدن مغازه خود در ساعت‌های شـلوغ روز اشتباه نگیرید. در واقـع حملـه دی‌داس با درخواسـت‌های کاذب، مخـرب و غیرطبیعی اتفـاق می‌افتد. این درخواسـت بالا باعث کندی سیستم و در درجـه بالا از کار افتادن آن می‌شـود. معمولا این حملات برای باجگیری از صاحب سرویس انجام می‌شـود، اما هکرهایی هستند که فقط بـا هدف تخریب و اختلال دسـت به حملات این‌چنینی می‌زنند.

وقتی این حمله در ابعـاد ملی، مثل اتفاقی که برای زیرسـاخت اینترنت ایران افتاد، انجام می‌شود، دیگر ماجرا فقط یک خرابکاری ساده نیست.

ابزاری برای آزمایش

باورتان می‌شـود که بسـیاری از شرکت‌ها به زیرسـاخت خودشان حمله می‌کنند؟ باورش سخت اسـت، اما واقعیتی است که هر شرکتی اگر اصولی عمل کند، باید به این کار تن دهد. در واقع تسـت دی‌داس، یک آزمایش رایج در شـرکت‌های مختلف اسـت که قبل از انتشار محصولات آنلاین مانند یک سـرویس، سایت یا نرم‌افزار، آن را انجام می‌دهند.

ایـن آزمایش بـرای سـنجش مقاومت و توانایی یک سـرویس انجام می‌شود تا بتواند تحمل بار پیش‌بینی شـده از سـمت کاربران یا حتی حمله‌های پیش‌فرض را داشـته باشد. همان‌طور کـه گفتیم، نتیجه حملات دی‌داس غیرقابل بازگشت نیسـت و بیشتر باعث از کار افتادن یا اختلال می‌شـود. در واقع در آزمایش دی‌داس آنقدر میزان درخواسـت‌ها بالا می‌رود که بار قابل تحمل توسـط سیستم اندازه‌گیری شود.

برای همین بیشتر سرویس‌دهنده‌ها از قبل آمـاده چنین حملاتی هسـتند و همین باعث شـد حمله به زیرساخت اینترنت کشور در ابعاد بزرگی دیده نشود و فقط باعث کند شدن شبکه برای بعضی از کاربران و سایت‌ها شود.

راه مقابله چیست؟

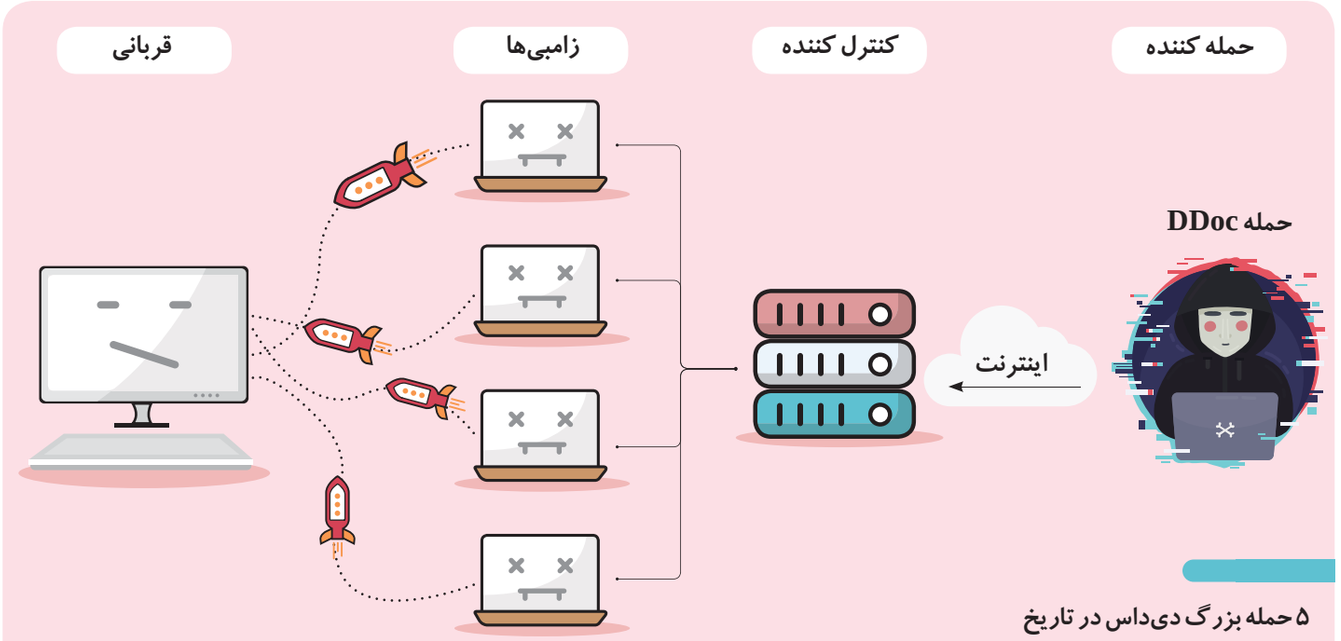
زمانی که یک هکر یا گروه هکری دست به حمله دی‌داس می‌زند، این کار را با دسـتگاه‌ها و آی‌پی‌های کاربران عادی انجام می‌دهد: در واقع دسـتگاه کاربران عادی تبدیل به زامبی‌هایی می‌شـوند که مانند فیلم‌های علمی ـ تخیلـی، هیچ اختیاری از خود ندارند و فقط به هدف خود حمله می‌کنند.

همان‌طـور که در اینفوگرافیک زیر می‌بینید، هکر درخواسـت‌های مخـرب را به یـک هندلر یـا کنترل‌کننده می‌فرسـتد. کنترل‌کننده، درخواسـت‌های مخـرب را به هدف‌هـای اولیه یا همـان کاربران و آی‌پی‌های محافظت نشـده می‌فرسـتد. از اینجای کار این کاربران به بات‌نت یا همان زامبی‌های کنترل شـونده‌ای تبدیل می‌شوند و بدون این‌که خودشـان اطلاع داشته باشند، شـروع به ارسال درخواست‌های زیاد و بی‌شـمار به هدف اصلی می‌کنند. این درخواسـت‌های مخرب و بی‌شـمار، بار روی سـرور هدف مورد نظر را بـالا می‌برند و باعث اختلال‌های بعدی می‌شوند. روش معمول برای مقابله با حمله دی‌داس معمولا به شکل خودکار اتفاق می‌افتد. به این شکل که وقتی سرویس متوجه درخواسـت‌های زیاد از یک آی‌پی خاص به سـرورش می‌شود، آن آی‌پی خاص را می‌بندد تا دیگر درخواسـتی برایش ارسـال نشود.

اما در حمله‌ای که به‌طور مثال به زیرسـاخت ایران شد، هکرها از روش پیچیده‌تری استفاده کرده‌اند و با استفاده از آی‌پی‌های گسترده این کار را پیـش بردند، یعنی همان بات‌نت‌ها یـا زامبی‌هایی که قبل‌تر به آن اشاره کرده‌ایم. در چنین حالتی سرویس مورد نظر در قدم اول باید توان سروس‌های خود را افزایش دهد تا بتواند بار بیشتری را تحمل کند. بعد باید از مسیر درخواسـت‌های مخرب، آی‌پی کنترل‌کننده را پیدا کند و جلوی حمله را بگیرد. اگر شما صاحب یک برنامه، وب‌سایت یا سرویس آنلاین هستید یا به‌عنوان یک کاربر عادی دوست ندارید که دستگاه شما به یک زامبی تبدیل شود، می‌توانید با استفاده از روش‌های ایمن جلوی چنین سوءاستفاده‌ای را بگیرید.

استفاده از سرویس‌ها Virtual Private Network یک روش مناسب برای بیمه شدن در برابر حمله دی‌داس است.

Virtual Private Network اطلاعات دسـتگاه یا سرویس شـما را رمزگذاری می‌کند و در واقع آی‌پی شـما را مخفی می‌کند. در چنین حالتی یک هکر با توجه به این‌که دسترسـی به آی‌پی شما ندارد، امکان اسـتفاده از شـما به‌عنوان زامبی یا هدفی برای حمله را نخواهد داشت و این به معنی بیمه‌شدن شما در برابر حملات دی‌داس است.



۵ حمله بزرگ دی‌داس در تاریخ

GitHub	() Dyn	Hong Kong	Cloudflare	Spamhaus
2018	2016	2014	2014	2013
وسعت حمله	وسعت حمله	وسعت حمله	وسعت حمله	وسعت حمله
1.3	800	500	400	300
ترابایت در ثانیه	گیگابایت در ثانیه	گیگابایت در ثانیه	گیگابایت در ثانیه	ترابایت در ثانیه

اگر مطالب این صفحه را می‌پسندید، عدد ۷۴۳۲ را به شماره ۳۰۰۰۱۱۲۲۶ پیامک کنید