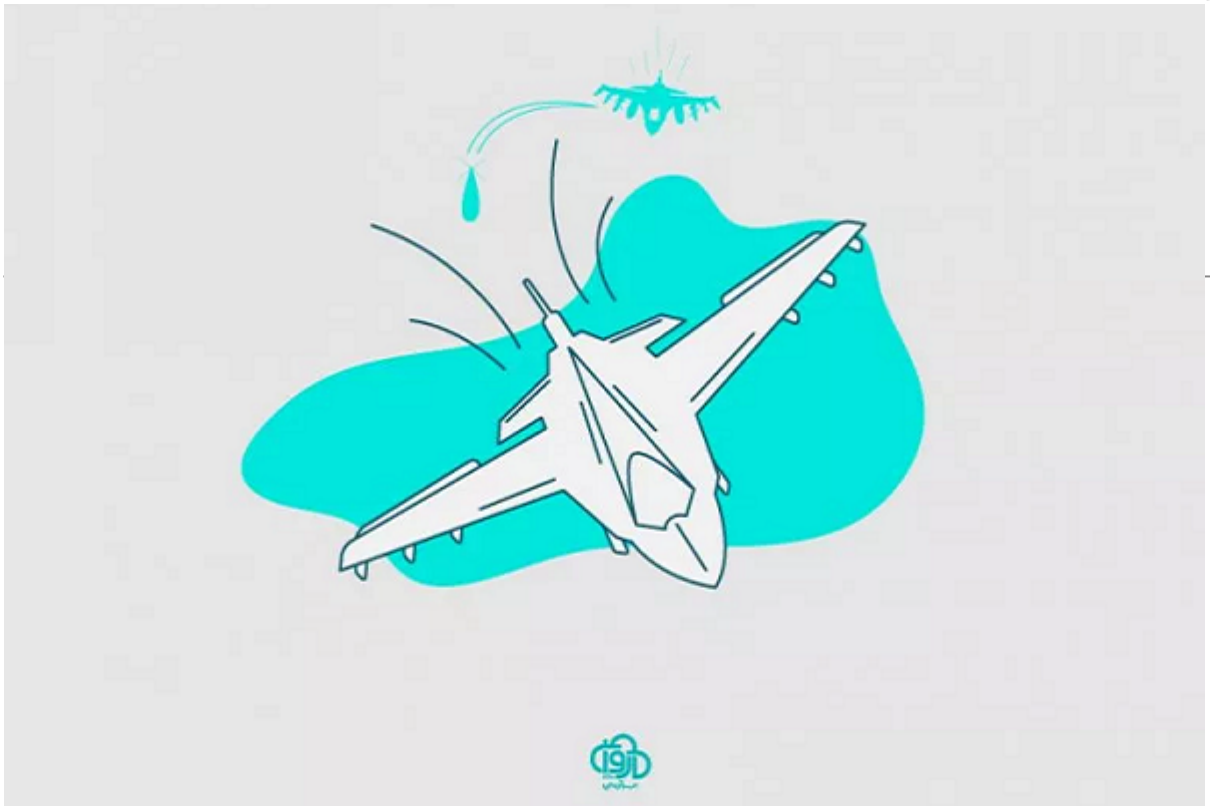
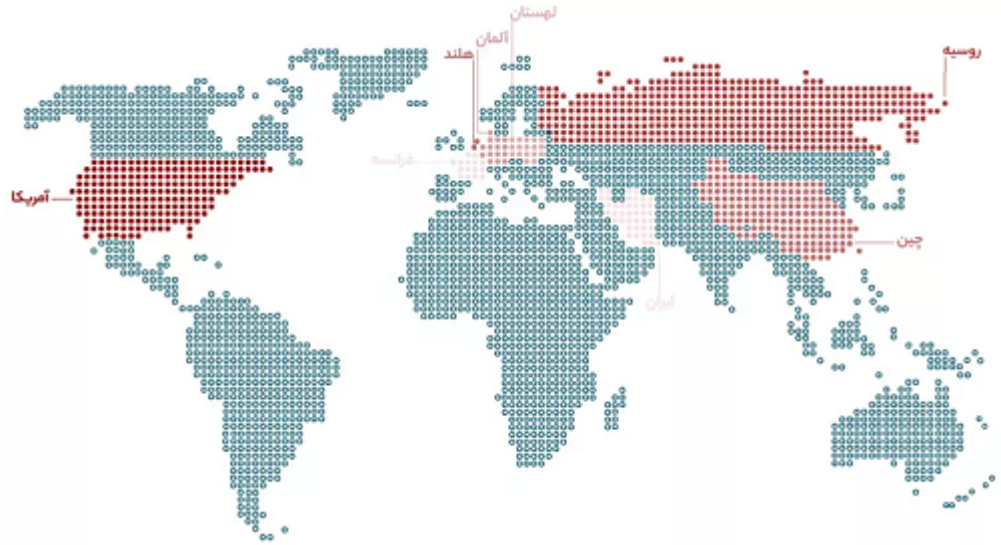
حملات گسترده‌ی DDoS در یک هفته‌ی گذشته؛ زامبی‌ها علیه کسب‌وکارهای آنلاین ایرانی

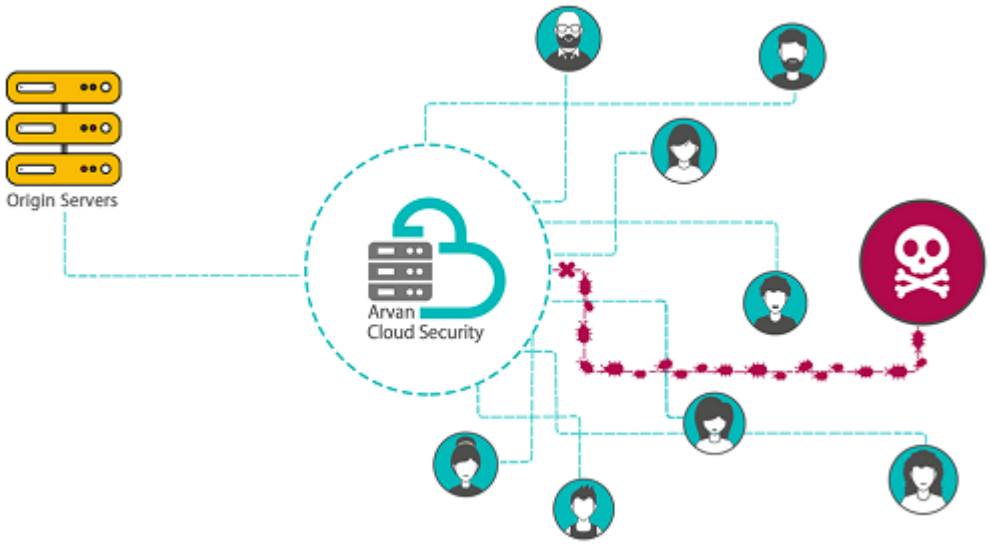


در روزهای اخیر برخی کسب‌وکارهای آنلاین با حملات منع سرویس توزیع‌شده یا (DDoS) و به‌دنبال آن باج‌خواهی هکرها روبه‌رو شدند. از آن جمله حملات و باج‌خواهی از دو وب‌سایت زرین پال و علی بابا رسانه‌ای شدند که از این بین، زرین پال با انتقال به سامانه‌های امنیت ابری آروان توانست با این حملات مقابله کند.

براساس گزارش‌های زیرساختی آروان، این حملات برخلاف گذشته که تنها منشا خارجی داشتند، این بار با حملاتی از داخل و خارج کشور روبه‌روست که شامل حملات DDoS لایه شبکه و لایه‌ی ۷ می‌شوند.
به زبان ساده، حملات منع سرویس توزیع‌شده (Distributed denial-of-service یا DDoS) به مجموعه حملاتی گفته می‌شود که هکرها تلاش می‌کنند یک سرویس یا یک سیستم خاص را با ارسال حجم بالایی درخواست از سیستم‌ها یا دستگاه‌های کاربران عادی، از دسترس خارج و اتصال کاربران به آن را با مشکل مواجه ساخته یا کامل مختل کنند.
در روزهای اخیر برخی کسب‌وکارهای آنلاین با حملات منع سرویس توزیع‌شده یا (DDoS) و به‌دنبال آن باج‌خواهی هکرها روبه‌رو شدند. از آن جمله حملات و باج‌خواهی از دو وب‌سایت زرین پال و علی بابا رسانه‌ای شدند که از این بین، زرین پال با انتقال به سامانه‌های امنیت ابری آروان توانست با این حملات مقابله کند.
براساس گزارش‌های زیرساختی آروان، این حملات برخلاف گذشته که تنها منشا خارجی داشتند، این بار با حملاتی از داخل و خارج کشور روبه‌روست که شامل حملات DDoS لایه شبکه و لایه‌ی ۷ می‌شوند.

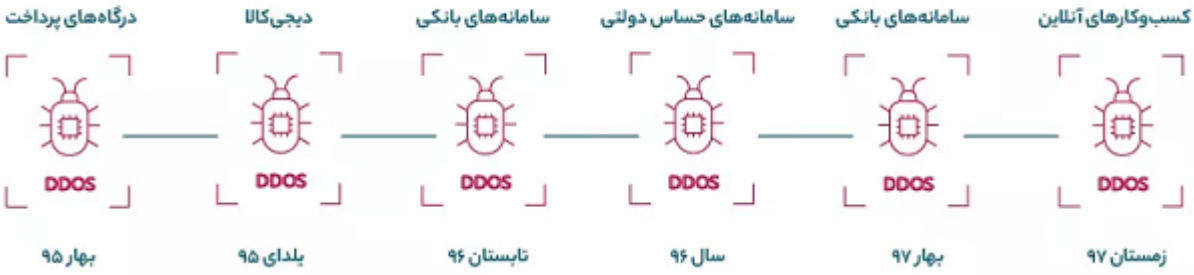


به زبان ساده، حملات منع سرویس توزیع‌شده (Distributed denial-of-service یا DDoS) به مجموعه حملاتی گفته می‌شود که هکرها تلاش می‌کنند یک سرویس یا یک سیستم خاص را با ارسال حجم بالایی درخواست از سیستم‌ها یا دستگاه‌های کاربران عادی، از دسترس خارج و اتصال کاربران به آن را با مشکل مواجه ساخته یا کامل مختل کنند.



این دست حملات، اتفاق تازه‌ای نیست؛ نگاهی به تاریخچه‌ی این حملات و مقابله‌ی آروان با آن‌ها نشان می‌دهد که؛

- در ابتدای سال ۹۵، درگاه‌های پرداخت از جمله زرین پال، مهرپال، آزادپی و... مورد این نوع حمله قرار گرفتند.
- یلدای همان سال، دیجیکالا به مدت ۴۵ ساعت مورد حمله قرار گرفت و حجم این حمله تا مرز Gb/s ۷۹ رسید.
- تابستان ۹۶ شاهد حملات گسترده‌ی DDoS به سامانه‌های بانکی کشور بودیم که آروان با بزرگ‌ترین حمله‌ی سایبری کشور با حجم Gb/s ۵۶ به بانک پاسارگاد مقابله کرد.
- سامانه‌های حساس دولتی هدف بعدی حملات DDoS در سال ۹۶ بودند.
- بهار امسال دوباره سامانه‌های بانکی از جمله سامان و آینده مورد حمله قرار گرفتند.
- و در تازه‌ترین اتفاق، این کسب‌وکارهای آنلاین هستند که مورد حملات گسترده‌ی DDoS قرار گرفتند.



مقابله‌ی آروان با حملات گسترده و بی‌سابقه‌ی DDoS

در یک هفته‌ی گذشته آروان با بیش از ۲۰ حمله‌ی لایه ۳ و ۴ با حجم بیش از ۵۰ Gb/s و با ۵۰ حمله‌ی لایه ۷ هر کدام با بیش از ۲ میلیون درخواست در دقیقه، مقابله کرده است.
گزارش‌های زیرساختی آروان نشان می‌دهد در یک هفته‌ی گذشته ۲۰ کسب‌وکار آنلاین از جمله لست سکند، ایسام، اقامت ۲۴، فروشگاه اینترنتی خانمی، زرین پال، سامانه‌ی اعتبارسنجی مرآت، خانه سرمایه، گیفت کارت، نت بانک سامان و... مورد حملات DDoS قرار گرفتند. حجم و گستردگی این حملات بیش از ۵۰ گیگابیت بر ثانیه بوده است که آروان با **۲۰۰ برابر ظرفیت مقابله** با همگی مقابله کرده است و هیچ‌یک از این کسب‌وکارها با مشکلی مواجه نشدند.

در مواجهه با حملات DDoS چه باید کرد؟

اگر وب‌سایت، وب‌سرویس یا اپلیکیشن شما مورد حمله‌ی منع سرویس توزیع‌شده یا DDoS قرار گرفته است لازم است کارهای زیر را انجام دهید:

1. از یک سامانه‌ی امنیت ابری استفاده کنید چرا که زیرساخت‌های محدود شما توانایی مقابله با حجم بالای حملات را ندارد.
2. IPهای سرور اصلی‌تان را پشت شبکه‌ی ابری مخفی کنید.
3. از مکانیزم‌های تشخیص ربات از انسان برای مقابله با حملات لایه ۷ استفاده کنید.
4. مکانیزم‌های محدودیت دسترسی (Rate Limit) را به‌کار بگیرید.

و توجه داشته باشید که حملات سایبری ناغافل به سراغ شما می‌آیند و همیشه پیش‌گیری بهتر از درمان است. با قطع پیاپی سرویس‌های امنیت ابری به‌راحتی طعمه‌ی حملات سایبری و حملات DDoS خواهید شد.

برای آگاهی از ویژگی‌های راهکار امنیت ابری آروان، وب‌سایت آروان را ببینید و برای استفاده از این راهکار در مقابله با حملات سایبری و حملات منع سرویس‌توزیع شده یا DDoS مراحل زیر را انجام دهید:

1. مطمئن شوید که رکوردهای NS شما روی آروان تنظیم شده باشد؛ وگرنه، هم‌چنان درخواست‌هایی که به‌سمت وب‌سایت شما می‌آید مستقیم به سرورهای اصلی وب‌سایت یا وب‌سرویس شما می‌رسد و از سامانه‌ی ابری آروان عبور نمی‌کند. با این تغییر رکوردهای NS، تمام ترافیک وب‌سایت شما نخست از فیلتر آروان می‌گذرد. «راهنمای به‌روزرسانی رکوردهای NS وب‌سایت» در این مورد به شما کمک می‌کند.
2. مطمئن شوید که هیچ رکورد DNS ندارید که تیک ابر نداشته باشد (یعنی ابر CDN برای آن فعال باشد که از طریق آن IP سرور اصلی شما کشف نشود).
3. مطمئن شوید که سرور Mail شما با سرور وب شما یکی نباشد.
4. مطمئن شوید که پس از انتقال به آروان، IP سرور اصلی خودتان را عوض کرده باشید. زمانی‌که استفاده از سامانه‌ی ابری آروان را آغاز می‌کنید، دیگر کاربران و هکرها آدرس IP سرور اصلی شما را مشاهده نمی‌کنند و تنها آروان را می‌بینند. اما اگر از همان IP قدیمی استفاده می‌کنید یا سرویس ابر خود را پیش‌تر خاموش کرده‌اید، آدرس IP شما در پایگاه‌های اینترنتی ثبت شده و هکرها می‌توانند مستقیم آدرس IP سرور اصلی شما را هدف قرار دهند.

مقابله با حملات DDoS

تاریخ انتشار:

29 بهمن 1397

نشانی منبع:
https://www.shabakeh-mag.com/ads-report/14658/%D8%AD%D9%85%D9%84%D8%A7%D8%AA-%DA%AF%D8%B3%D8%AA%D8%B1%D8%AF%D9%87%E2%80%8C%DB%8C-ddos-%D8%AF%D8%B1-%DB%8C%DA%A9-%D9%87%D9%81%D8%AA%D9%87%E2%80%8C%DB%8C-%DA%AF%D8%B0%D8%B4%D8%AA%D9%87%D8%9B-%D8%B2%D8%A7%D9%85%D8%A8%DB%8C%E2%80%8C%D9%87%D8%A7-%D8%B9%D9%84%DB%8C%D9%87-%DA%A9%D8%B3%D8%A8%E2%80%8C%D9%88%DA%A9%D8%A7%D8%B1%D9%87%D8%A7%DB%8C-%D8%A2%D9%86%D9%84%D8%A7%DB%8C%D9%86-%D8%A7%DB%8C%D8%B1%D8%A7%D9%86%DB%8C