حمله گسترده DDOS به زیرساخت های اَبر دِراک دفع شد

زیرساخت سرویس های اَبری اَبر دراک روز شنبه ۱۵ بهمن به مدت **۳۰ ساعت** هدف حمله DDOS گسترده در لایه شبکه قرار گرفت و بدون از دسترس خارج شدن سرویس های مورد حمله با موفقیت دفع شد.

به گزارش روابط عمومی ابر دراک این حمله که ابعاد آن حدود **۱۰ برابر** بزرگ تر از بزرگ ترین حمله صورت گرفته بر بستر ابر دراک گزارش شده است، با هدف از دسترس خارج کردن دو وبسایت مالی سرویس گیرنده از سرویس CDN ابر دراک و از خارج از ایران صورت گرفت و اثرات آن توسط سرویس امنیت اَبری اَبر دِراک و بدون از دسترس خارج شدن این وبسایت ها دفع شد.

در گزارش فنی تیم عملیات و پشتیبانی اَبر دِراک، این حمله گسترده از ساعت ۱۳:۱۵ روز شنبه ۱۵ بهمن آغاز شد و تا ساعت ۱۸:۵۰ روز یکشنبه ۱۶ بهمن ادامه داشته است. ماهیت این حمله **UDP Flood** و **DNS Amplification** عنوان شده است و در طول مدت حمله جمعا حدود **۱۸۰ هزار** آدرس آلوده **۸ میلیارد** بسته را به سمت سرورهای لبه زیرساخت ابر دراک ارسال نموده اند. در نقاط اوج حمله **۳۵۰ میلیون** درخواست در ثانیه ارسال شده است و حدود **۴۵۰ گیگابیت** بر ثانیه از پهنای باند شبکه ابر دراک را به این بسته های آلوده اختصاص داده اند. سهم آدرس های آلوده ایرانی در این حمله **۲.۵ درصد** بوده است و بر این اساس میتوان با اطمینان گفت که این حمله این بار، از خارج از ایران اتفاق افتاده است.

اقدامات اَبر دِراک جهت دفع این حمله عمدتا شامل توزیع ترافیک UDP مربوط به حمله بروی شبکه Anycast اَبر دراک بوده است. با وجود گستردگی و حجم حمله صورت گرفته سرویس امنیت اَبری اَبر دِراک به خوبی توانست تاثیرات این حمله را کاهش دهد و در نتیجه هیچ یک از وبسایت های سرویس گیرنده از سرویس امنیت اَبری اَبر دِراک در اثر این حمله از دسترس خارج نشدند. اگرچه در زمان های اوج حمله افت کیفیت مقطعی در برخی از سرویس های ابری مشاهده شده است ، تیم پشتیبانی اَبر دِراک تمام تلاش خود را برای کاهش این تاثیرات بر سرویس های اَبری کاربران با جا به جایی سرویس ها در زمان های مشخص انجام داده است.

سینا سلطانی مدیرعامل اَبر دِراک، با اشاره به اینکه شبکه اَبر دِراک در پاسخ به این حمله ظرفیت خوبی از خود نشان داده است و دفع این حمله و کاهش تاثیرات آن توسط تیم عملیات و پشتیبانی و همکاری با مراکز داده ی خارج از کشور که اَبر دِراک در آن نقاط پاپ سایت دارد، به خوبی مدیریت شده است، معتقد است با کاهش امنیت در شبکه داخلی ایران ناشی از محدودیت های اینترنت در ماه های اخیر و توسعه حملات سایبری در سال های گذشته در سطح جهانی، قطعا برنامه ریزی هایی جهت افزایش ظرفیت فعلی پاسخگویی به حملات سایبری مخصوصا در داخل ایران ضروری خواهد بود. در هفته گذشته و پس از وقوع این حمله تا زمان انتشار خبرحمله، با بررسی های انجام شده بر روی گراف ها و شبکه ابر دراک در پاپ سایت های مختلف و همچنین پارتنرهای زیرساختی و تشخیص نوع حملات صورت گرفته، نقاط نا امن سرویس های مورد حمله نیز مجددا ارزیابی شد. و در همین راستا افزایش ظرفیت مورد نیاز به زودی در برنامه عملیاتی توسعه زیرساخت قرار خواهد گرفت، این اقدامات شامل افزایش سرورهای لبه در دیتاسنتر های موجود و همچنین تجهیز دیتاسنترهای فعلی و افزایش ظرفیت Disaster Site های بخش عملیات و پشتیبانی خواهد بود.

شرکت ابر دراک ارائه دهنده سرویس های اَبری است و فعالیت خود را به صورت رسمی در سال ۹۸ با رونمایی از سرویس شبکه توزیع محتوا (CDN) آغاز کرد.در حال حاضر شبکه اَبری اَبر دراک با ۷۵ پاپ سایت در سراسر دنیا، در حال ارائه و توسعه سرویس های اَبری و شبکه ای امن و پایدار برای کسب و کارهای آنلاین است. شبکه توزیع محتوا (CDN)، امنیت اَبری و سرورهای آبری، استریمینگ و پخش زنده ازجمله سرویس های این شرکت هستند.