حملات DDoS بر علیه سایت‌های ایران

## جزئیات حمله دیروز به چند وب‌سایت دولتی اعلام شد

روز گذشته برخی از سایت‌ها و پورتال‌های دولتی مانند سایت بانک مرکزی، پست، ایرانسل و غیره مورد حمله سایبری قرار گرفتند و از کار افتادند.

براساس اعلام سازمان فناوری اطلاعات ایران، عصر روز گذشته، تعدادی از وب‌سایت‌ها و پورتال‌های سازمان‌ها و دستگاه‌های اجرایی بر اثر حوادث امنیتی، از دسترس خارج شدند یا با بار پردازشی بسیار زیاد و غیرطبیعی روی سرویس‌دهنده‌های وب خود رو به رو بودند که تیم عملیاتی و پاسخگویی به حوادث امنیتی مرکز ماهر، ضمن بررسی موضوع اقدامات لازم و ضروری را اجرایی کرد.

طبق اعلام مرکز ماهر (مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه ای)، هدف حمله، منع سرویس توزیع شده، سیستم‌عامل‌های ویندوز با سرویس‌دهنده‌های وب IIS بوده است و تمامی اهداف مورد حمله قرار گرفته تاکنون، از شرایط فنی یکسان برخوردار بوده‌اند.

آناتومی حمله، شامل ارسال زیاد درخواست‌های HTTP به سمت وب‌سرورها با حجم و تعداد بالا است که باعث ایجاد پردازش سنگین روی سرویس‌دهنده‌ها شده و به اعتقاد کارشناسان، هدف اولیه این حمله پهنای باند شبکه نبوده است، لذا تشخیص اولیه با سیستم‌های مانیتورینگ و پایش معمولی، به سختی قابل انجام است و با تاخیر تشخیص حاصل می شود.

برهمین اساس، پیکربندی صحیح سرویس‌دهنده‌های وب که میزبان برنامه‌های کاربردی تحت وب هستند، باید به دقت صورت پذیرد و رعایت نکات امنیتی در آنها، امنیت کل سیستم‌ها و برنامه‌های کاربردی را تحت تاثیر قرار می‌دهد.

با توجه به اعلام مرکز ماهر، استفاده از دیواره‌های آتش اختصاصی لایه کاربرد یا WAF و پیکربندی موثر آن به تناسب تعداد کاربران و نیز شرایط برنامه کاربردی هر سازمان از جمله روش های موثر برای مقابله با این دست از حملات است.

**منبع:**

Mehrnews

**تاریخ انتشار:**

08 خرداد 1396

---

**نشانی منبع:**

https://www.shabakeh-mag.com/news/iran/8070/%D8%AC%D8%B2%D8%A6%DB%8C%D8%A7%D8%AA-%D8%AD%D9%85%D9%84%D9%87-%D8%AF%DB%8C%D8%B1%D9%88%D8%B2-%D8%A8%D9%87-%DA%86%D9%86%D8%AF-%D9%88%D8%A8%E2%80%8C%D8%B3%D8%A7%DB%8C%D8%AA-%D8%AF%D9%88%D9%84%D8%AA%DB%8C-%D8%A7%D8%B9%D9%84%D8%A7%D9%85-%D8%B4%D8%AF