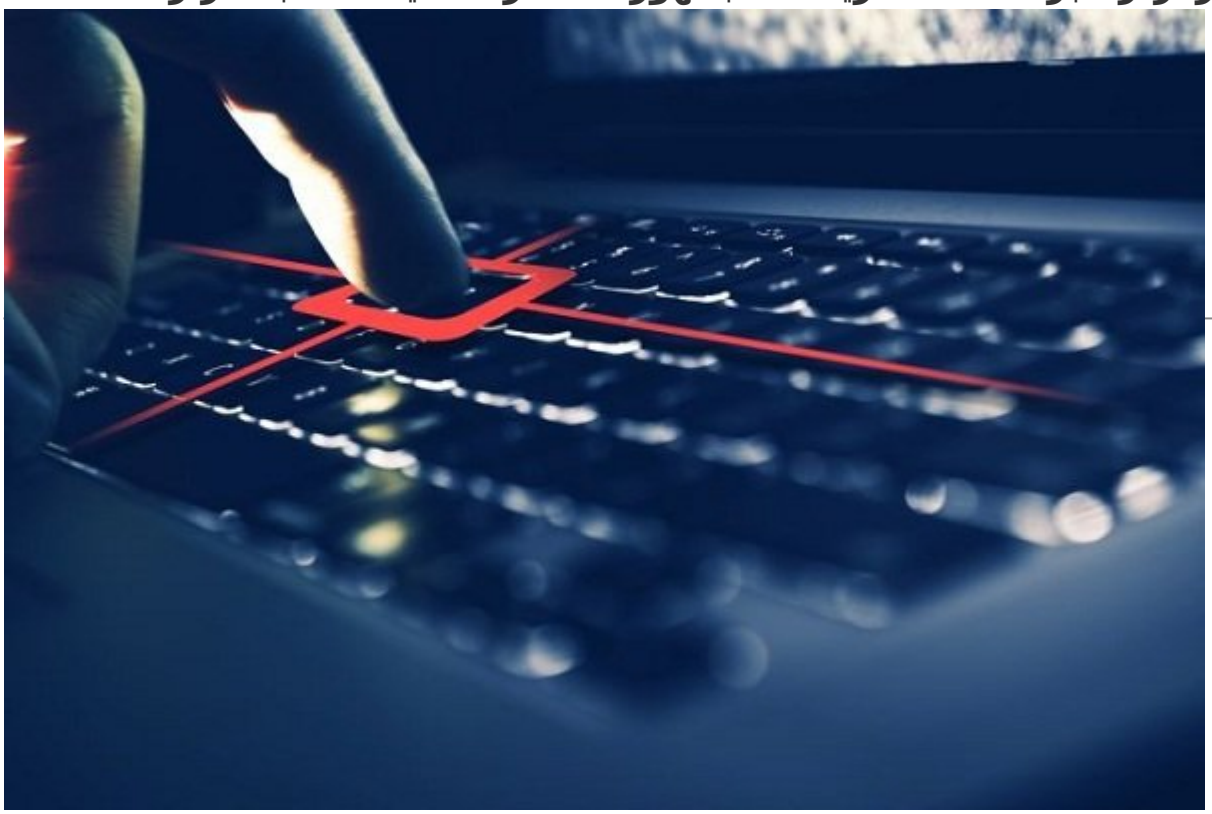
هشدار مرکز راهبردی افتای ریاست جمهوری خطر فعالیت 10 بدافزار



مرکز مدیریت راهبردی افتای ریاست جمهوری هشدار داد پژوهشگران در آمریکا بیش از هزار سرور را شناسایی کردند که از طریق عملیات فیشینگ مرتبط با بات‌نت Necurs، ده خانواده بدافزار مختلف را توزیع می‌کنند.

به نقل از روابط عمومی **مرکز مدیریت راهبردی افتای ریاست جمهوری**، پژوهشگران Bromium اعلام کردند در این سرورها پنج تروجان بانکی شامل Nymaim، IcedID، Gootkit، Dridex و Trickbot، دو باج‌افزار شامل Gandcrab و Hermes و سه بدافزار سارق اطلاعات شامل Neutrino، Fareit و Azorult مشاهده شده‌اند.
یکی از این سرورها متعلق به سیستمی مستقل است که سرویس میزبانی bulletproof نام دارد و ۱۱ سرور دیگر هم متعلق به یک شرکت در Nevada است که سرورهای خصوصی مجازی به فروش می‌رساند.
به گفته پژوهشگران، ایمیل‌های فیشینگ بُردار حمله اصلی حملات شناسایی شده و در این حملات از فایل‌های Word حاوی ماکروهای VBS مخرب استفاده شده است. ایمیل‌ها در قالب یک سازمان شناخته شده ارسال شده‌اند و محتوای آن‌ها مربوط به موقعیت‌های شغلی است.
کارشناسان معاونت بررسی **مرکز افتا** به نقل از پژوهشگران Bromium می‌گویند: از سرورها برای عملیات مختلف استفاده شده است، برای مثال در ۹ مارس یک سرور برای توزیع تروجان بانکی IcedID به کار گرفته و یک هفته بعد همان سرور برای میزبانی Dridex استفاده شده و وب سرور دیگری در مدت ۴۰ روز از ۶ خانواده بدافزاری مختلف میزبانی کرده است.

منبع:

منبع:
mehrnews
تاریخ انتشار:
21 فروردین 1398
mehrnews

تاریخ انتشار:
21 فروردین 1398

نشانی منبع:
https://www.shabakeh-mag.com/news/iran/14888/%D9%87%D8%B4%D8%AF%D8%A7%D8%B1-%D9%85%D8%B1%DA%A9%D8%B2-%D8%B1%D8%A7%D9%87%D8%A8%D8%B1%D8%AF%DB%8C-%D8%A7%D9%81%D8%AA%D8%A7%DB%8C-%D8%B1%DB%8C%D8%A7%D8%B3%D8%AA-%D8%AC%D9%85%D9%87%D9%88%D8%B1%DB%8C-%D8%AE%D8%B7%D8%B1-%D9%81%D8%B9%D8%A7%D9%84%DB%8C%D8%AA-10-%D8%A8%D8%AF%D8%A7%D9%81%D8%B2%D8%A7%D8%B1