نویسنده

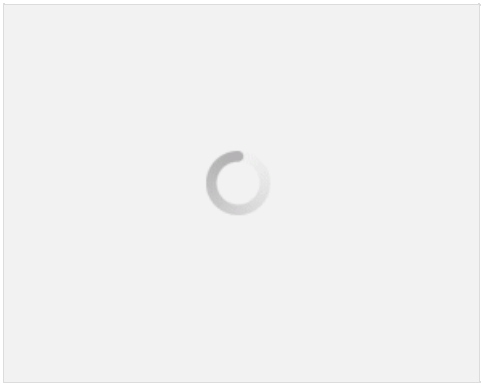
علیرضا عارف

۵۶۱ | ۰ | ۲۸ | ۴۰۶

کارشناس نرم افزار-کارشناس ارشد فناوری اطلاعات-مدرس کامپیوتر-مدیر فناوری اطلاعات -net+,mcse,ccna,ceh certificate

حملات سایبری MassMiner

۳۲۷



ظهور ارزهـای دیجیتـال و شـیوع به یکباره و گسترده اون در سـطح فضای سایبر و علاقه منـدی ای که به ماننـد سونامی در فضای سایبر نسـبت به آنها بوجود آمد، در کنار حملات باج افزارها، فضای اینترنت را دچار التهاب و تب چهل درجه کرد. اخیرا هم گروهی از متخصصـین موفق به کشف بـدافزاری شده اند که اقدام به نفوذ به سیسـتم های قربانیان کرده و از منابع سـخت افزاری آنها در جهت استخراج ارز دیجیتال مونرو برای خود اقدام می کند. این متخصصان که از شرکت امنیتی AlienVault هستند موفق به کشف این گونه از بدافزار شده اند. AlienVault جزء شرکت های بزرگ امنیتی محسوب می گردد که در حوزه soc فعالیت و نرم افزار ارائه می دهد. در ادامه، طبق گفته های این متخصصین، این حملات ناشی از آسیب پذیری های اعلام شده CVE-۲۰۱۷-۱۰۲۷۱ (مربوط به CVE-۲۰۱۷-۰۱۴۳ ،Oracle WebLogic) (مربوط به Windows SMB) و CVE-۲۰۱۷-۵۶۳۸ (مربوط به Apache Struts) است که هر کدام اختلالات زیادی را قبل از کشف و ارائه patch امنیتی برای آنها در شرکت های مالی دنیا بوجود آوردند.

نحوه ورود آنها به سیستم از طریق حملات brute-force علیه پایگاه‌داده‌های SQL مایکروسافت است به این ترتیب که پس از نفوذ به پایگاه داده، مهاجم می‌توانـد اسـکریپت SQL دلخواه خود را اجرا کنـد و اسـتخراج‌کننـده ارز را نصب کنـد.البته این بـدافزار از چندین روش برای نفوذ به سیستم قربانی استفاده می کند.

گزینه **پسندیدم**، اعلام رضایت شما از این مطلب.

منبع : alienvault

منبع : مرکز افتا

نویسنده : علیرضا (ARAF)

منبع : انجمن تخصصی فناوری اطلاعات ایران

۰ نظر

هیچ نظری ارسال نشده است! اولین نظر برای این مطلب را شما ارسال کنید...

نظر شما

برای ارسال نظر باید وارد شوید.

از سرتاسر توسینسو