هشدار مرکز افتا در خصوص بدافزار سرقت ارزهای دیجیتالی DarkGate

[ad_1]

به گزارش خبرنگار روابط عمومی گروه تجاری ققنوس، مرکز افتای ریاست جمهوری در اطلاعیه‌ای از کشف بد افزار جدیدی با نام DarkGate با قابلیت توزیع از طریق فایل‌های تورنت و دور زدن فرآیندهای شناسایی نرم افزارهای آنتی ویروس و شناسایی آلودگی سایبری خبر داد و اعلام کرد که این بدافزار فعالیت‌های مخربی از جمله حملات باج افزاری، سرقت اطلاعات هویتی و استخراج ارز دیجیتالی را به صورت برنامه ریزی شده پیگیری می‌کند و نیاز است تا اقداماتی برای جلوگیری از آن توسط کاربران انجام شود؛ در واقع فایل‌های تورنت آلوده، کدهای مخرب VBscript را در رایانه قربانی اجرا، پس از آن با سرور C&C ارتباط برقرار و فرایند کاوش ارز را آغاز می‌کند. سپس فعالیت‌های مخرب دیگری توسط بدافزار اجرا می‌شود.

این بدافزار در کشورهای فرانسه و اسپانیه به سرعت توسعه یافته و در سایر کشورهای جهان نیز در حال گسترش و ایجاد آلودگی سایبری است؛ این بدافزار به دنبال سرقت اطلاعات هویتی و تاریخچه و کوکی‌های مرورگر، و اطلاعات گفتگوهای برنامه اسکایپ است و قصد دارد تا با آلودگی در سیستم کاربران نسبت به برداشت غیر مجاز و سرقت اط کیف پول‌های ارزهای رمزنگار سیستم‌های آلودگی شده قربانیان اقدام کند که خطر بزرگی برای صاحبان حساب‌های رمز ارز و سرمایه

گذاران در این حوزه به شمار می‌رود.

از جمله نشانه‌های آلودگی (IoC) این بدافزار در دامنه‌های زیر قرار دارد:

- **akamai.la**
- **hardwarenet.cc**
- **ec۲-۱۴-۱۲۲-۴۵-۱۲۷.compute-۱.amazonaws.cdnprivate.tel**
- **awsamazon.cc battlenet.l**
- **a۴۰-۷۷-۲۲۹-۱۳.deploy.static.akamaitechnologies.pw**

همچنین، مرکز افتای ریاست جمهوری در گزارشی تاکید کرده است که فیشینگ از طریق نوعی جدید از بدافزار TrickBot و توسط My Online Security به عنوان تروجانی بانکی در حال گسترش است و کاربران باید ایمیل‌های خود با محتوای بانکی را بررسی و پس از آن به انجام عملیات‌های بانکی بپردازند چرا که برخی از ایمیل‌ها با لوگوی بانک به صورت جعلی طراحی شده و حاوی کد مخبر ماکرو است که اطلاعات کارت بانکی کاربران را سرقت می‌کند و سارقان می‌توانند از مالباختگان برداشت غیز مجاز داشته باشند.

[ad_2]