شرکت آب و فاضلاب استان آذربایجان شرقی

دفتر حراست و امور محرمانه

ارز رمزی یا پول دیجیتال چیست؟

ارز رمزی یک دارایی دیجیتال است که برای مبادله‌ی تراکنش‌های مالی به صورت رمز شده‌ی قوی طراحی شده است. ارز رمزی نوعی از ارزهای جایگزین است که از سیستمی غیرمتمرکز برای کنترل تراکنش‌ها استفاده می‌کند که برخلاف سیستم مالی سنتی است که از روش بانکداری متمرکز برای آن استفاده می‌شود. در سیستم مالی سنتی دولت‌ها براساس پشتوانه‌هایی که دارند اقدام چاپ پول می‌کنند اما ارزهای دیجیتال پول چاپ نمی‌شود بلکه از یک معدن نامحدود استخراج می‌شود. کامپیوترهای سراسر جهان برای استخراج ارزهای رمزی باهم رقابت می‌کنند. در حال حاضر معروفترین ارز دیجیتال بیت کوین است. افراد در طول روز بیت کوین ها را از طریق شبکه بیت کوین برای یکدیگر ارسال می کنند، اما تا وقتی که از سوابق تراکنش‌ها نگهداری نشود، هیچ کس قادر به انجام تراکنش نخواهد بود. شبکه بیت کوین با جمع آوری تمام تراکنش‌های انجام شده در یک دوره زمانی معین آن را در یک لیست که بلاک نامیده می شود، ذخیره می کند. کار کامپیوتر های استخراج کننده تایید این تراکنش ها است و برای آن پاداش (بیت کوین) دریافت می کنند.

استخراج غیرقانونی ارزهای دیجیتال

گروهی از افراد و سازمانهایی هستند که تلاش می کنند با استفاده از روش های غیرقانونی از ارز رمزنگاری شده استفاده کنند و آنها را اسخراج کنند.

اکثر ارزهای دیجیتالی از طریق فرآیندی به نام "استخراج" تولید میشوند. ، این روش نیاز به استفاده از انرژی و منابع قوی برای تکمیل فرآیند استخراج است که به کسب ارز مورد نظر منتهی میشود. منظور از انرژی و منابع قوی، برق و محاسبات پیچیده است.

کد جاوا اسکریپت Coinhive

یکی از پیشگامان نرم افزارهای مخرب استخراج غیرقانونی ارز دیجیتال، یک نرم افزار قانونی به نام Coinhive بود . Coinhiveبر پایه‌ی جاوا اسکریپت بود که در اواخر سال ۲۰۱۷ توسعه یافت و استخراج Monero را به طور مستقیم در مرورگر وب فعال کرد. در حالی که هدف از این پروژه این بود که به کاربران برای انجام عملیات استخراج در کامپیوترهای شخصی خود اجازه داده شود، ولی این فنآوری به سرعت توسط مجرمان اینترنتی به کار گرفته شد. شاید ناامیدکننده باشد، هدف ایده آل برای این حمله ی غیرقانونی یک شبکه بزرگ سرور است. دلیل این امر این است که شبکه های سرور دارای بیشترین میزان توان محاسباتی هستند و ئر نتیجه قدرت محاسباتی بیشتری در دسترس است، و فرآیند استخراج می تواند سریع تر انجام شود. در حقیقت، این حمله ممکن است از قدرت پردازش رایانه‌ای سرپیچی کند و سیستم را خاموش کند و باعث به وجود آمدن خسارت شود. به همین دلیل، شرکت های امنیتی متمرکز بر فناوری در تلاش برای مبارزه با این نوع حملات هستند.

در هر وب سایتی که شما بازدید می کنید جاوا اسکریپت اجرا می شود بنابراین جاوا اسکریت مسئول ماینینگ است و نیاز به نصب هیچ برنامه ای ندارد. وقتی شما یک صفحه را لود می کنید کد ماینینگ تزریق شده به مرورگر اجرا می شود. اما شاید شما هم یکی از قربانیان این ماجرا باشید برای محافظت خود چه کاری انجام می دهید.

جهت پیشگیری از اجرای کدهای تزریق شده، مرورگرها در حال طراحی افزونه‌هایی برای تشخیص هستند، بنابراین از بروز بودن مرورگر مورد استفاده‌ی خود اطمینان حاصل کنید.

همچنین آنتی ویروس‌ها نیز تلاش می‌کنند از اجرای کدهای استخراج کننده جلوگیری کنند.

یکی از نشانه‌های احتمالی اجرا شدن کدهای استخراج کننده افزایش بار CPU و کارت گرافیکی و داغ شدن غیرمعمول سیستم است.

شایعترین نوع استخراج غیرقانونی ارز دیجیتال (کریپتوکارنسی ها) استفاده از نرم افزارهای مخرب‌است.

تروجان یکی از آنهاست که نرم افزاری مخفی است که می تواند به صورت مخفی روی کامپیوتر فردی بدون حضورش یا دانستن دانش موردنیاز او اجرا شود.

در مورد بدافزار استخراج این ارزها، این برنامه قدرت پردازش لازم را از کامپیوتر به منظور تکمیل فرآیندهای الگوریتمی پیچیده که به استخراج منتهی میشود میگیرد. همه این کارها بدون اینکه کاربر کامپیوتر از چیزی با خبر باشد انجام می شود. و در آخر کنترل کننده بدافزار، نه کامپیوتر، ارز دیجیتال را به عنوان جایزه به دست می آورد.