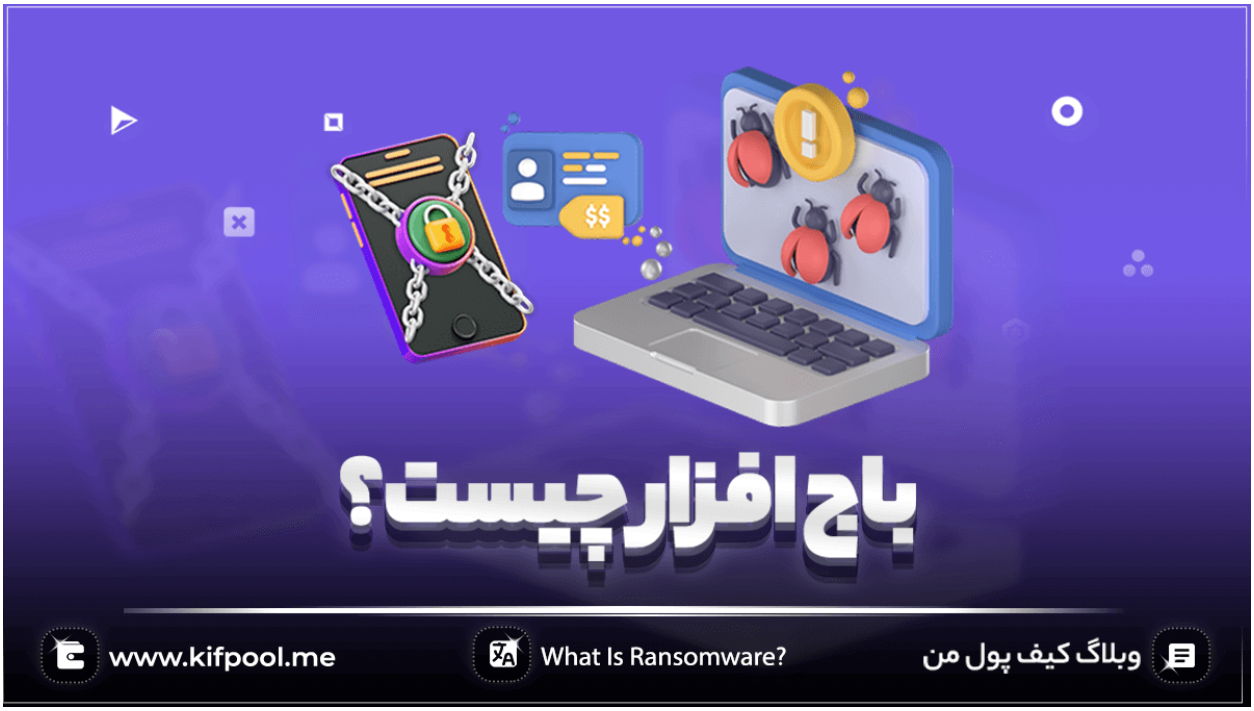


باج افزار چیست؟

گسترش و توسعه بازار ارزهای دیجیتال، بستر مناسبی برای هکرها و **حملات وحشتناک باج افزارها** فراهم کرده تا دارایی کاربران را به سرقت ببرند. روزانه افراد زیادی به دلیل عدم آگاهی، دارایی‌های خود را از دست می‌دهند و این مسئله از آنجایی مهم تلقی می‌شود که بسیاری از این دارایی‌های به سرقت رفته قابل بازگشت و بازیابی نیستند. باج افزارها اغلب به سمت کوین‌هایی با محور حفظ حریم خصوصی روی می‌آورند و یکی از خطرهایی که افراد فعال در حوزه ترید ارزهای دیجیتال را تهدید می‌کند، از دست دادن ارزهای دیجیتال از کیف پول خود توسط حمله باج افزارها است.

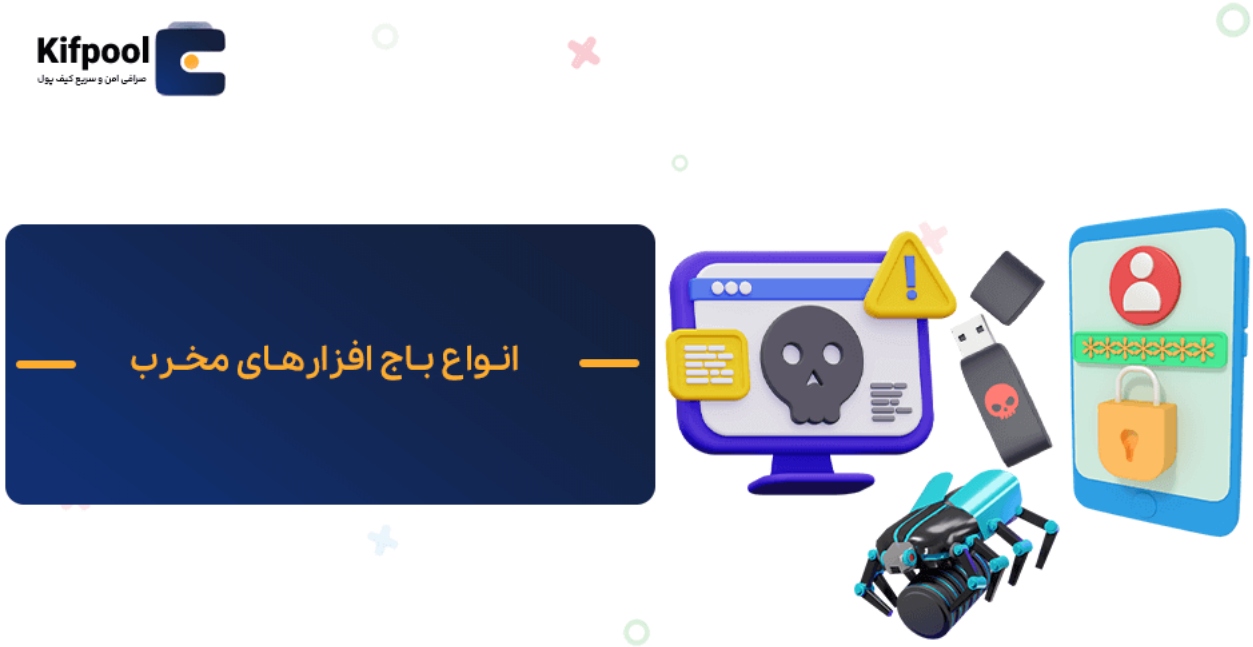
در پایان سال گذشته و حتی با شروع سال میلادی جدید، شاهد افزایش پرداختی ارز دیجیتال به مهاجمان باج افزارها بودیم و با گذشت زمان هم انتظار می‌رود که حملات سایبری افزایش پیدا کنند. اما **باج افزار چیست؟** چه راه‌هایی برای حفظ ارزهای دیجیتال و کیف پول ارزها در برابر هجوم باج افزارها وجود دارد؟ در ادامه این مطلب از وبلاگ کیف پول من، با مخرب‌ترین باج افزارها آشنا شده و راه‌های محافظت از کیف پول ارزهای دیجیتال در برابر حملات این بدافزارها را شرح می‌دهیم.

آشنایی با باج افزارها

باج افزارها (**Ransomware**) نوعی از بدافزارهای خطرناکی هستند که به اطلاعات و فایل‌های سیستم قربانی نفوذ کرده و این اطلاعات را با روش‌های مختلف رمزگذاری و قفل گذاری می‌کنند و به این طریق دسترسی افراد به اطلاعات خود محدود می‌شود. هکرها پس از رمزگذاری فایل‌ها و اطلاعات سیستم قربانی، درخواست باج می‌کنند و در قبال دریافت مبلغ و یا مقداری رمزارز، اجازه دسترسی به اطلاعات را به فرد قربانی می‌دهند.

در این حملات، این امکان وجود دارد که علاوه بر اطلاعات خود، ارزهای دیجیتالی که در کیف پول نرم‌افزاری نگهداری می‌کنید را هم از دست دهید. حملات شدید باج افزارها ابتدا در روسیه گزارش شدند؛ اما با گذشت زمان، شاهد آن هستیم که حملات هکرها افزایش یافته و به منطقه جغرافیایی خاصی ارتباط ندارد. به عبارتی دیگر، می‌توان گفت افرادی که در دنیای ارزهای دیجیتال فعالیت می‌کند، در معرض حمله باج افزارها قرار دارند؛ اما با این حال می‌توان با انجام برخی راهکارها احتمال این حملات را کاهش داد و از وقوع آن‌ها جلوگیری کرد.

انواع باج افزارهای مخرب



باج افزارهای بسیار زیادی وجود دارد که به سه دسته زیر طبقه‌بندی می‌شوند:

- ترس افزار (Scareware): این باج افزار با ایجاد ترس، کاربر را مجبور به انجام کاری می‌کند که در نظر دارد.

- قفل کننده صفحه نمایش (Screen lockers): مهاجم صفحه نمایش کاربر را قفل می‌کند و یک صفحه اخطار برای قربانی نشان داده می‌شود. کاربر برای دسترسی مجدد به سیستم باید جریمه‌ای که مدنظر هکر است را پرداخت کند.
- رمزگذار (Encryption ransomware): در ازای ارسال کلید رمزگشایی، از کاربر درخواست باج می‌کند.

در ادامه قصد داریم نمونه‌هایی از مخرب‌ترین باج افزارها را معرفی کنیم.

باج افزار DoppelPaymer

این باج افزار برای رمزگذاری فایل‌ها، جلوگیری از دسترسی کاربران به فایل‌های خود و تهدید قربانی برای پرداخت باج جهت رمزگشایی طراحی شده است. DoppelPaymer برای اولین بار در سال 2019 کشف شد و توسط گروهی به نام INDRIK SPIDER به کار می‌رود. در چند وقت اخیر، این باج افزار بیش از 200 گیگابایت داده را در حمله به شهر تورانس کالیفرنیا به سرقت برد و برای پس دادن این اطلاعات، درخواست 100 بیت کوین به عنوان باج کرد. همچنین گزارش دیگری نیز نشان می‌دهد که بدافزار DoppelPaymer برای حمله به سیستم فناوری اطلاعات ایالت آلاباما به کار رفته است. مهاجمان در این حمله تهدید کردند که اگر مبلغ 300000 دلار به‌صورت بیت کوین به آن‌ها پرداخت نشود، داده‌های خصوصی شهروندان را منتشر می‌کنند.

مطلب پیشنهادی: بررسی الگوریتم رمزنگاری در دنیای کریپتو

باج افزار Revil

باج افزار Revil برای اولین بار در آوریل 2019 کشف شد و بیش از 150000 رایانه منحصربه‌فرد در سراسر جهان را آلوده کرده است. مهاجمان از این باج افزار برای رمزگذاری سیستم‌های تجاری بسیار مهم استفاده می‌کنند و مبلغ هنگفتی از کاربران به عنوان باج دریافت می‌کنند. اخیرا این باج افزار حراجی را برای فروش داده‌های سرقت شده از شرکت‌هایی برپا کرده است که قادر به پرداخت باج 50000 دلاری به صورت مونرو نیستند. ناگفته نماند که این Ransomware رویکرد خود را از دریافت بین کوین به مونرو که یک کوین با محوریت حریم خصوصی بود، تغییر داد. از این باج افزار به عنوان یکی از پرخاشگرترین بدافزارهایی یاد می‌شود که در درجه اول به سیستم شرکت‌ها حمله می‌کنند و پس از رمزگذاری پرونده‌های آن‌ها، درخواست هزینه‌های نجومی می‌دهند.

باج افزار WastedLocker

این **باج افزار** از جدیدترین باج افزارهای گروه Evil Corp است که به عنوان یکی از کشنده‌ترین تیم‌های جرایم سایبری شناخته می‌شوند. دلیل نام گذاری این باج افزار به این باز می‌گردد که مخفف نام قربانی را به کلمه Wasted اضافه می‌کنند. با غیرفعال کردن برنامه‌ها و سرویس‌های پایگاه داده، باج افزار WastedLocker از توانایی قربانیان خود برای بازیابی پرونده‌ها در مدت زمان طولانی‌تر و تهیه نسخه پشتیبان به‌صورت آفلاین جلوگیری می‌کند.

باج افزار GrandCrab

باج افزار گرندکرب در ژانویه 2018 مشاهده شد و قبل از آنکه شناسایی شود، بیش از 50 هزار قربانی گرفت. باج افزار GrandCrab با سوء استفاده از تبلیغات و ایمیل‌های فیشینگ منتشر شد و به عنوان اولین باج افزاری محسوب می‌شود که باج خود را به‌صورت ارز دیجیتال دش طلب می‌کرد. باج‌های اولیه این بدافزار از 300 الی 1500 دلار متغیر بود.

باج افزار Cryptolocker

از مشهورترین و خطرناک‌ترین باج افزارهای شناخته شده کریپتولاکر است که در سال 2013 شناسایی شد. این باج افزار از کلید 2048 بیتی برای رمزنگاری فایل‌های سیستم کاربران استفاده می‌کرد و پس از انجام عملیات خرابکارانه خود، از کاربران باج می‌خواست. اگر فرد قربانی شده مبلغ مدنظر مهاجمان را پرداخت نمی‌کرد، پس از سه روز کلید رمزگشایی از بین می‌رود و دیگر فرد قادر به دسترسی و بازگشایی فایل‌های خود نبود و به همین دلیل است که از Cryptolocker به عنوان یکی از دردسرسازترین باج افزارهای موجود در میان سایر باج افزارها یاد می‌شود.

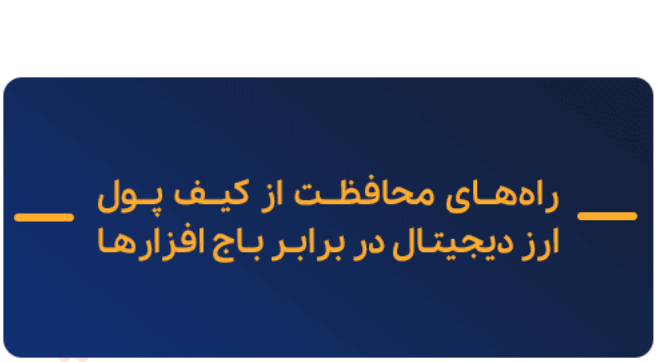
چگونه سیستم خود را برای خرید و فروش ارزهای دیجیتال در برابر باج افزارها ایمن کنیم؟

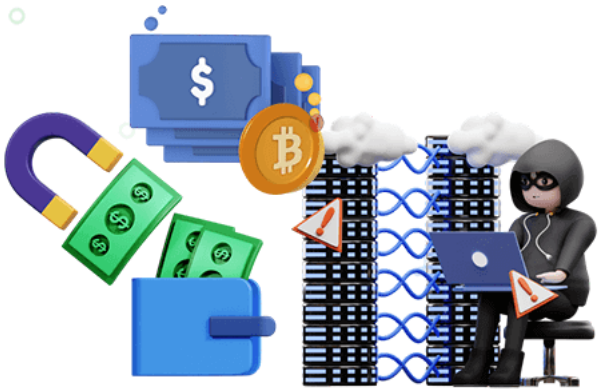
حملات باج افزارها برای سرقت ارزهای دیجیتال به این صورت است که رمز سیستم یا کیف پول ارز دیجیتال کاربران را با تکنیک‌های خاصی از سیستم دریافت می‌کنند. مهاجمان اقدام به تغییر رمز دریافتی می‌کنند و به دلیل اینکه کاربر از رمز جدید اطلاع ندارد، مجبور به پرداخت باج به مهاجمان می‌شود. اگر شما هم در حوزه ارزهای دیجیتال و بازار کریپتوکارنسی‌ها مشغول به فعالیت هستید، باید امنیت سایبری خود را بازبینی کنید و با استفاده از این روش در برابر حملات باج افزارهای مختلف ایمن بمانید.

برای حفظ دارایی‌ها و رمزارزهای دیجیتال خود باید از کلید خصوصی و کلمات بازیابی خود به درستی محافظت نمایید و اگر بتوانید این کار را به شیوه‌ای مناسب انجام دهید، احتمال قربانی شدن شما توسط باج افزارها به میزان قابل توجهی کاهش می‌یابد.

مطلب پیشنهادی: پس از گم شدن کلید خصوصی چگونه به کیف پول دیجیتال خود دسترسی پیدا کنیم؟

راه‌های محافظت از کیف پول ارز دیجیتال در برابر باج افزارها





کیف پول ارزهای دیجیتال به‌صورت نرم‌افزاری و سخت‌افزاری در دسترس هستند و دارایی دیجیتال کاربران را نگهداری می‌کنند. این موضوع یک گزینه مناسب برای باج افزارها و مهاجمانی محسوب می‌شود تا با طراحی حملات مختلف، کیف پول‌های کاربران را آلوده کنند. اگر دارایی و ارزهای دیجیتال شما بسیار زیاد است، باید ارزهای دیجیتال خود را در کیف پول یک صرافی معتبر محدود کرده و تنها مقداری که قصد معامله با آن دارید را در صرافی نگهداری کنید. همچنین نباید بدون تحقیق لینک‌هایی که دعوت به ایجاد کیف پول ارز دیجیتال می‌کنند را باز کنید؛ چراکه برخی اوقات این لینک‌ها طعمه باج افزارها و از طرف هکرها هستند. به عنوان مثال، بدافزاری به نام Echelon فایل آلوده‌ای در گروه‌های تلگرامی قرار داد و از این طریق توانست به کیف پول ارزهای دیجیتال حمله کند.

از صرافی‌های معتبر و کیف پول‌های مطمئن برای نگهداری رمزارزهای خود کمک بگیرید. برخی از کیف پول‌ها امنیت لازم را ندارند و حریم خصوصی کاربران ایرانی را به خطر می‌اندازند. همچنین برخی از کیف پول‌ها جعلی هستند و علاوه بر به خطر انداختن حریم خصوصی کاربران، دارایی‌ها و رمزارزهای دیجیتال آن‌ها را نیز نابود می‌کنند. متاسفانه در بسیاری از موارد حتی پرداخت باج به باج افزارها نیز منجر به رمزگشایی نشده است؛ این موضوع اهمیت انتخاب یک کیف پول مناسب را نشان می‌دهد.

مطلب پیشنهادی: **بهترین کیف پول های ارز دیجیتال ایران برای گوشی های اندروید و ios**

سرعت حملات باج افزارها در حوزه ارزهای دیجیتال افزایش یافته است!

تحقیقات و گزارش‌های به دست آمده نشان می‌دهند که در یک سال اخیر، سرعت حمله باج افزارها در حوزه ارزهای دیجیتال و بازار کریپتوکارنسی افزایش بسیار زیادی یافته است. اگر در حوزه ارزهای دیجیتال مشغول فعالیت هستید و سرمایه خود را وارد این مسیر کرده‌اید، باید از اطلاعات خود و دارایی‌های ارزی خود به دقت محافظت کنید. همچنین باید از باز کردن ایمیل‌های اسپم یا لینک‌های درون آن‌ها اجتناب کرده و فایل‌های موردنیاز خود را از سایت‌های معتبر دانلود نمایید.

پشتیبان‌گیری منظم، نصب و به روز کردن ضد ویروس‌های معتبر، استفاده از آپدیت‌های آنلاین برای سروها و غیره از جمله راهکارهایی هستند که می‌توانید از حملات باج افزارها تا حد زیادی در امان بمانید. در این مطلب از کیف پول من، با برخی از مخرب‌ترین باج افزارها آشنا شده و راه‌های محافظت از کیف پول ارزهای دیجیتال را شرح دادیم. اگر در رابطه با باج افزارها سوال یا نظری دارید، می‌توانید آن‌ها را در قسمت نظرات با کارشناسان ما در میان بگذارید تا در اسرع وقت به شما پاسخ دهند.