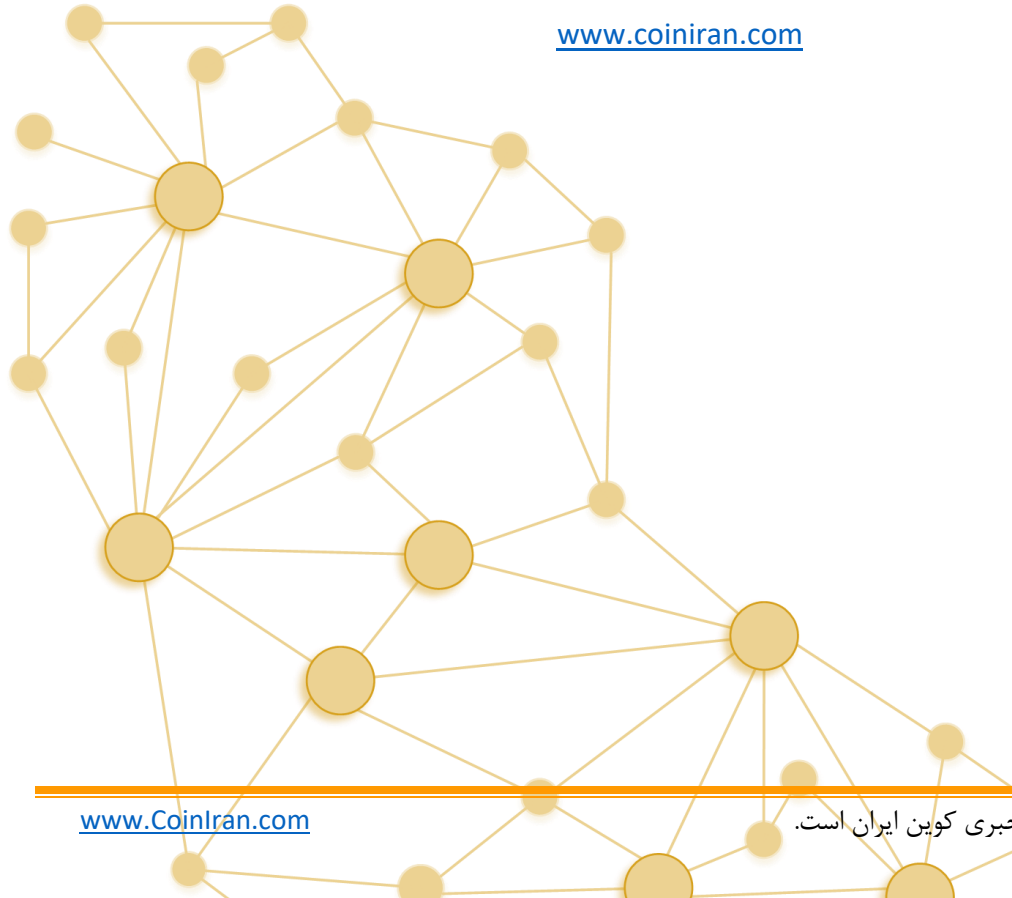
نام نویسنده: ایوب کریمی
ایمیل نویسنده: ayubkarimi587@gmail.com

منتشر شده توسط

کوین ایران

کوین ایران بزرگترین پایگاه خبری فارسی زبان در حوزه فناوری بلاکچین، ارزهای رمزنگاری شده و پلتفرم های مرتبط با بلاکچین است. این وب سایت در سال ۱۳۹۲ توسط بابک جلیلوند و آرش محبوب، با هدف اطلاع رسانی، آموزش و مشاوره به جامعه فارسی زبان علاقه مند به رمز ارزها راه اندازی شد و اولین مقاله آن در ۱۴ دی ماه همان سال، با عنوان «بیت کوین چیست؟» منتشر گردید . هدف کوین ایران از معرفی این فناوری ایجاد محیطی پژوهشی و آموزشی در راستای استفاده صحیح از این فناوری جهت ارائه تسهیلات و رفاه به جوامع فارسی زبان است.

www.coiniran.com



بد افزار های استخراج رمز ارز (Mining Malwares)

یک بدافزار استخراج رمز ارز به یک برنامه نرم افزاری گفته می شود که برای در اختیار گرفتن منابع یک کامپیوتر و استفاده از آنها برای استخراج رمز ارز بدون اجازه مالک کامپیوتر توسعه یافته است. مجرمان سایبری به طور فزاینده ای به این روش روی آورده اند تا قدرت پردازش تعداد زیادی از کامپیوتر ها، گوشی ها و دیگر وسایل الکترونیک را در کنترل خود در آورند.

تنها یک botnet استخراج رمز ارز می تواند برای مجرمان سایبری ماهانه بیش از 300000 دلار درآمد داشته باشد. در حالی که 2017 سال باج افزار ها بود امسال یعنی سال 2018 را می توان سال بدافزار های استخراج نامید که با استفاده از آنها مجرمان از کامپیوتر دیگران برای استخراج انواع رمز ارز ها استفاده می کنند.

این جرم آنچنان رایج شده که سازمان AdGuard تخمین می زند که بیش از 500 میلیون کاربر بر روی دستگاه هایشان رمز ارز استخراج می- شود بدون اینکه خودشان تشخیص دهند. این کاربران یا توسط بدافزار های استخراج آلوده گشته اند و یا از وب سایت هایی دیدن کرده اند که از طریق این وب سایت ها مخفیانه نرم افزار استخراج رمز ارز را در پیش زمینه اجرا کرده اند بدون این که کاربر متوجه شود و نسبت به این امر رضایت داشته باشد.

در حالی که تعداد زیادی از این بدافزار ها دسکتاپ ها و لپ تاپ ها را مورد هدف قرار می‌دهند، تعدادی دیگر نیز گوشی های هوشمند و تبلت ها را آلوده می‌کنند. یکی از این بدافزار های قدرتمند که توسط لابراتوار های Kaspersky، Loapi نامیده شده است برای دزدیدن پردازنده یک گوشی آندرویدی طراحی شده تا با استفاده از آن به استخراج رمز ارز بپردازد که این بدافزار آنچنان هجوم شدیدی را به گوشی می کند که باتری گوشی را بیش از حد داغ کرده و حتی می تواند به طور فیزیکی به گوشی صدمه نیز بزند.

Source

گسترش استخراج رمز ارز با استفاده از مرورگر

علاوه بر بدافزار های مذکور، مجرمان سایبری در حال روی آوردن به استخراج با استفاده از مرورگر می باشند و این کار به آنها کمک می کند که از استخراج کسب درآمد کنند. این جرم از 2011 مطرح بوده اما این اواخر بسیار شایع گشته است که دلیل این امر نیز رشد خیره کننده رمز ارز ها در 2017 بوده است.

Coinhive یک برنامه نرم افزاری است که همه ابزار های مورد نیاز را برای صاحبان وب سایت فراهم می کند تا بازدید کنندگان از سایت را مجبور کنند که به استخراج برای آنها بپردازند. در حالی که بحث هایی مطرح است در مورد اینکه Coinhive بدافزار است یا فقط به وب سایت ها کمک می‌کند که برای خودشان درآمد اضافی ایجاد کنند؛ اما در اینجا این موضوع مطرح می شود که وقتی Coinhive برای استخراج رمز ارز بدون اجازه ملاقات کننده سایت به کار می رود باید آن را به عنوان نوع دیگری از بدافزار های استخراج تعبیر کرد.

Source

چرا باید تهدید بدافزار های استخراج را جدی گرفت؟

متقلبان فضای سایبری همیشه در جستجوی ابزار های جدیدی برای پول در آوردن هستند. آنها در دو سال گذشته باج افزار ها (ransomwares) را انتخاب کرده بودند ولی اخیرا باج افزار ها را کنار گذاشته اند و شیوه جدیدی را برای کسب درآمد آغاز کرده اند که این شیوه جدید استفاده از بدافزار های استخراج رمز ارز می باشد.

این مجرمان فضای مجازی، پتانسیل استفاده از قدرت پردازشی کامپیوتر ها را برای استخراج رمز ارز هایی مانند بیت کوین و مونرو درک کرده اند و می دانند که این روش راه خوبی برای کسب ثروت است. این مجرمان به جای آنکه هزینه کنند و سخت افزار بخرند و سپس به طور قانونی و مشروع شروع به کار استخراج کنند، از بدافزار ها برای استفاده از قدرت سیستم افراد استفاده می کنند.

این عمل مکانیسم ساده ای دارد. قربانیان ناآگاه، کامپیوتر و یا گوشی هوشمندشان با بدافزار آلوده می شود که این بدافزار از قدرت CPU ابزار آنها برای استخراج رمز ارز استفاده می کند و سود حاصل از این کار به والت مهاجم سرازیر می شود. این بدافزار ها علاوه بر اینکه از فن کامپیوتر استفاده زیادی می کنند و هزینه انرژی را بالا می برند، خود را آشکار نمی سازند و قربانی معمولا تشخیص نمی دهد که بدافزار ها در سیستم او مشغول به کار استخراج هستند.

این متقلبان سایبری یک مدل کسب و کار را برای خود راه اندازی کرده اند و با کمترین ریسک به کار خود ادامه می دهند. این روش بر خلاف باج افزار ها نیاز به تعامل با قربانی نداشته و مزایای زیادی برای متقلبان دارد. این عملکرد متقلبانه در این روش برای مدت زیادی می تواند ادامه پیدا کند. این روش بازار گسترده ای را در اختیار کلاهبرداران قرار می دهد و فرقی نمی کند که قربانی در کجای جهان ساکن باشد.

در مورد باج افزار ها، فرد قربانی مجبور بود مبلغ سنگینی را بپردازد اما این کار همیشه صورت نمی گرفت و یک کامپیوتر آلوده در آفریقا به احتمال زیاد این مبلغ را نمی پرداخت و یا در برخی از مناطق جهان مردم اصلا باج نمی دهند. در این کلاهبرداری جدید احتیاجی به این موارد نیست و هر کامپیوتری در هر جای جهان می تواند هدف باشد. این مزایا همگی دست به دست هم داده اند تا متقلبان فضای سایبری تغییر روش دهند و از باج افزار به بدافزار ماینینگ روی بیاورند.

در این کار چون سود به صورت رمز ارز دریافت می‌شود، استفاده از این سود برای مجرمان آسان تر است و نیازی به ایجاد سیستمی برای پنهان سازی این سود نامشروع و پول شویی نیست. قابلیت ردیابی متقلبین با این روش به مراتب سخت تر از روش های سنتی است و این موارد کلا سبب جذاب شدن این نوع جرم در میان مجرمان سایبری شده است.

مونرو رمز ارزی است که بسیار برای این متقلبان جالب است، زیرا طوری طراحی شده که استخراج آن آسان بوده و با اکثر دستگاه ها انجام می‌شود و پیچیدگی های بیت کوین را هم ندارد، و از طرف دیگر انتقال آن نیز امن و امکان ردگیری آن کم است. در این موارد اغلب قربانی متوجه حمله نشده و معمولا بعضی از آنها زمانی که سخت افزارشان خراب می شود، به این قضیه شک می کنند.

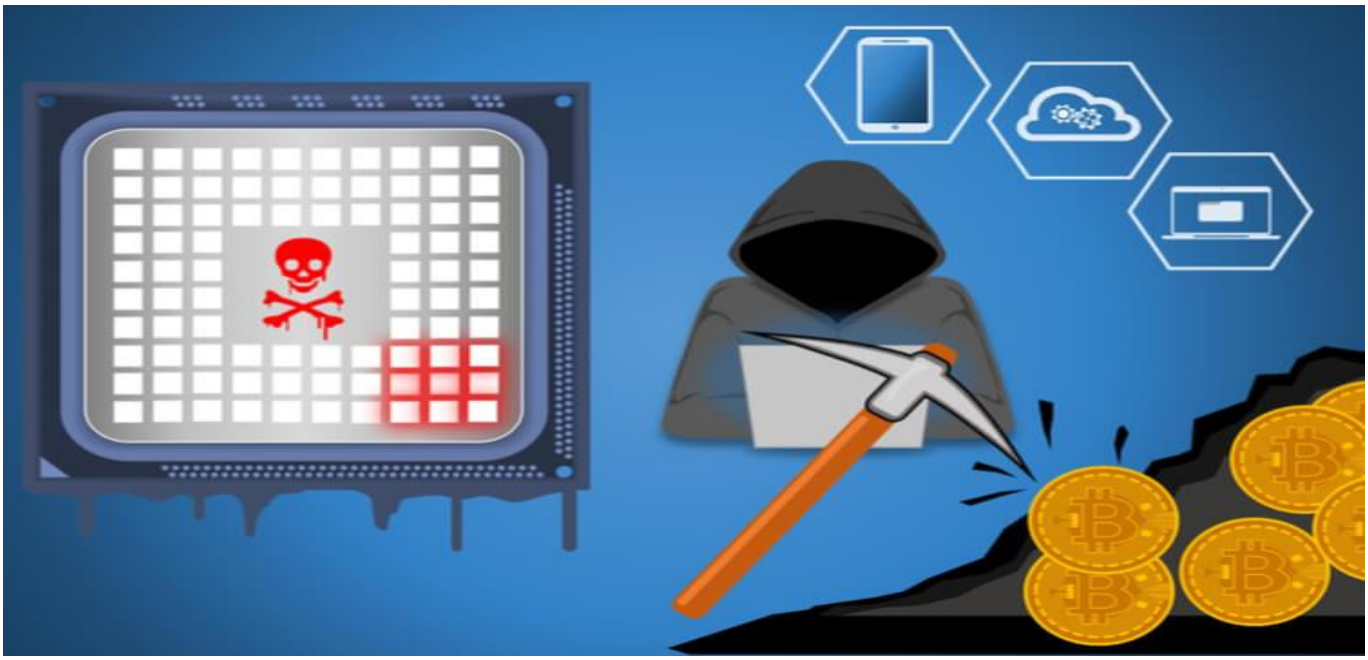
Source

این بدافزار ها بدون فایل (fileless) هستند

همچنان که باج افزار ها تکامل پیدا کردند، استفاده از روش های دیگری برای گسترش بدافزار های بدون فایل مشاهده شد. به عنوان مثال Coinhive را می توان نام برد که در آن 10 تا 20 استخراج گر فعال در یک وب سایت می توانند یک سود ماهانه 0.3 مونرو را ایجاد کنند و هر چه این مجموعه سیستم بزرگتر باشد، سود بیشتری را نصیب مجرمان می کند.

یک بدافزار استخراج مونرو به نام Adylkuzz از اولین بدافزار هایی بود که از EternalBlue قبل از Wannacry بهره برداری کرد. هر اندازه که سیستم و شبکه بیشتر بدون تعمیر بماند، به همان اندازه بیشتر در معرض آلودگی مجدد خواهد بود. یک نوع آلودگی شایع که این بدافزار های بی فایل ایجاد می کنند، بارگذاری یک کد آسیب رسان در حافظه سیستم می باشد.

تنها رد پایی که از این آلودگی بر جای می ماند وجود یک فایل batch آسیب رسان، یک سرویس WMI نصب شده و یک PowerShell قابل اجرا می باشد. در واقع آسیب پذیری های سیستم، دروازه هایی برای ورود این بدافزار ها هستند. این موضوع در تلاش های تهاجمی اخیر و بر روی سیستم های مدیریت پایگاه داده Apache CouchDB خود را نشان داد. یک تروجان که حامل استخراج گر مونرو است سرور های Jenkins را هدف قرار داده بود و برای متصدیان خود بیش از 3 میلیون دلار مونرو را به ارمغان آورد.



Source

تفاوت بدافزار های Cryptojacking با نسخه های قدیمی تر

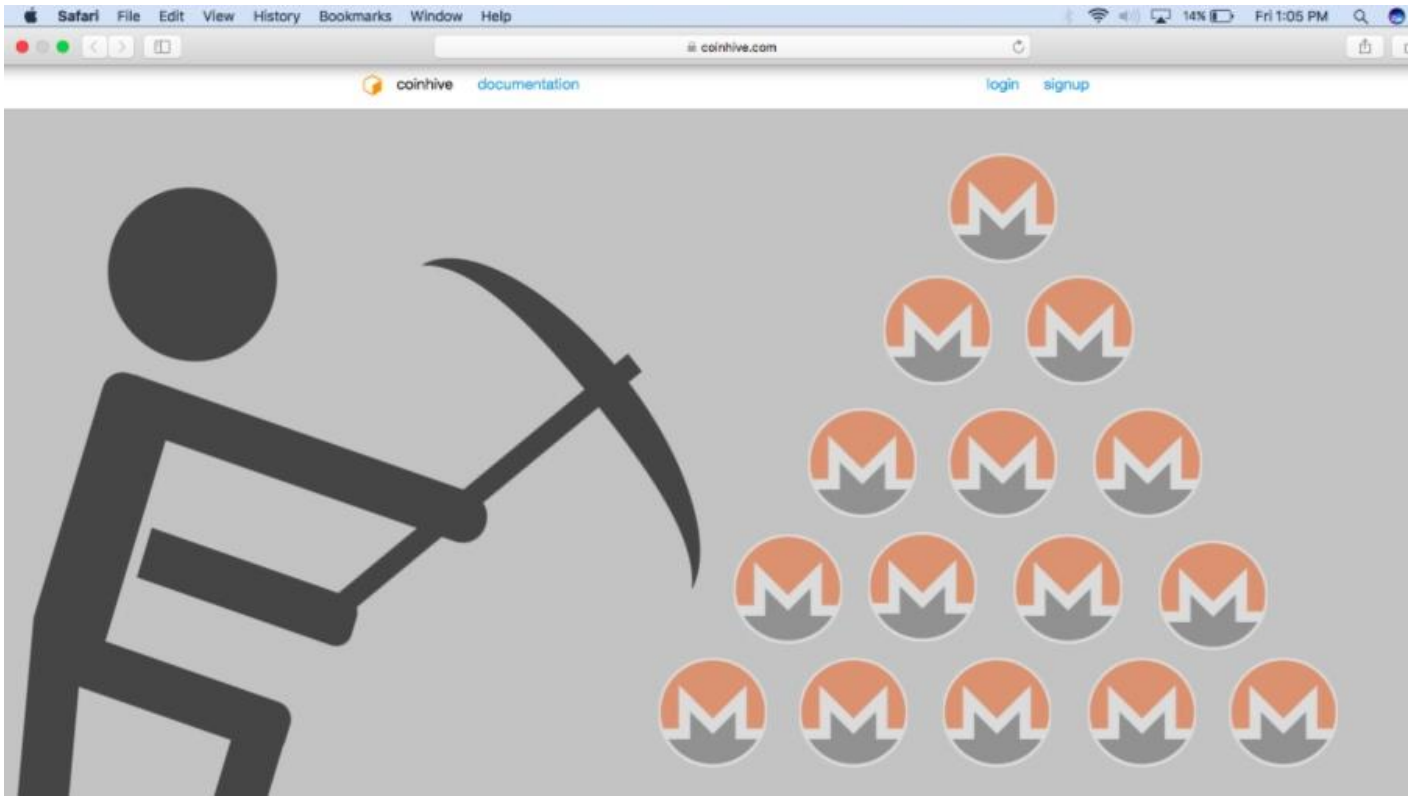
اگرچه فرآیند استخراج رمز ارز با استفاده از سیستم دیگران قبلا هم مطرح بوده اما در گذشته فرد می بایست یک فایل آلوده را نصب کرده و در سیستم قرار دهد. این Cryptojacking مدرن احتیاجی به نصب و قرار دادن فایل آلوده ندارد و به محض ملاقات کردن وب سایتی که چنین ترفندی را به کار می برد، فرد قربانی گرفتار شده و همه کار ها به صورت خودکار انجام می گیرد.

در Cryptojacking تمام کد هایی که وظیفه استخراج را به عهده دارند به زبان Javascript نوشته شده اند؛ به همین دلیل تنها با بازکردن وب سایت آلوده، تمام آن کدها درون مرورگر شما اجرا می شوند. بسیاری از اوقات این بدافزار ها چنان هوشمندانه نوشته شده اند که با استفاده مقطعی از پردازنده شما حتی شما را دچار شک هم نمی کنند. در بسیاری از موارد شما حتی مصرف غیر عادی منابع سخت افزاری خود را تشخیص نمی دهید؛ ولی به هر حال فردی به طور پنهانی از قدرت سخت افزار و هزینه برق شما برای کسب درآمد خود استفاده می کند.

Source

پیدایش Cryptojacking

تمام ماجرا از جایی شروع شد که شرکت Coinhive یک سرویس استخراج مونرو (XMR) را برای وب مستر ها فراهم آورد تا با JavaScript در مرورگر استخراج کنند و با این کار بتوانند از بازدید های خود درآمد داشته و از طریق استخراج رمز ارز درآمدی جانبی را برای خود ایجاد کنند. The Pirate Bay که یک وب سایت دانلود غیر قانونی تورنت است، اولین وب سایتی بود که از این سرویس سوء استفاده کرد و بعد از لو رفتن آن در مدت کمی اینترنت مملو از چنین سایت هایی شد.



Source

Cryptojacking می تواند مفید باشد

اگرچه فرآیند Cryptojacking در حال حاضر غیر قانونی است و سایت های متقلب و هکر ها از آن سوء استفاده کرده اند اما در آینده این روش می تواند جایگزین آگهی های آزار دهنده موجود در وب سایت ها شود. Pirate Bay هم بعد از لو رفتن ماجرا از کاربرانش نظر خواهی کرده بود و اکثرا کاربران، استخراج را به آگهی های آزار دهنده ترجیح داده بودند؛ اما اگر قرار باشد هر وب سایتی چنین کند کاربران در هنگام بازدید وب سایت ها بسیاری از توان پردازشی CPU خود را از دست خواهند داد و در این مورد باید تمهیداتی اندیشید.

به طور کلی کسب درآمد از طریق استخراج رمزارز توسط سخت افزار بازدید کننده های یک وب سایت، روش نوین و خلاقانه ای برای کسب درآمد وب مسترها می باشد. بسیاری به این موضوع به چشم بدافزار نگاه می کنند، ولی از منظر بسیاری از وب مستر ها و حتی کاربران، این روش جایگزین بسیار خوبی برای تبلیغات آزار دهنده و گاها بدون استفاده ی وب سایت ها می باشد.

Source

چگونه می توان بدافزار ها را تشخیص داد و از آنها جلوگیری کرد؟

هکر ها بدافزار های استخراج را بر روی ابزار ها، شبکه ها و وب سایت ها به میزان زیادی قرار می‌دهند. این کار برای هکر ها یک منبع درآمد دائمی و خوب را ایجاد می کند و آنها خیلی هوشمندانه بدافزار های خود را پنهان می کنند. بنگاه های اقتصادی با وسواس زیادی مراقب باج افزار ها هستند اما حمله بدافزار ها مخفی تر است و ممکن است تشخیص آن برای این شرکت های اقتصادی مشکل باشد.

خسارت های ناشی از این بدافزار ها واقعی است اما همیشه مشهود نیست. این صدمات ممکن است تاثیرات مالی داشته باشند و به قبض برق قربانی وارد شوند. همچنین این بدافزار ها می‌توانند دستگاه را کند کرده و عملکرد آن را تحت تاثیر قرار دهند. ممکن است CPU های دستگاه شما مخصوص استخراج نباشند و این موضوع باعث خسارت های جبران ناپذیری برای دستگاه شود.

به همین دلائل است که بعضی از ارائه دهندگان سرویس های امنیتی از یادگیری ماشینی و دیگر فناوری های هوش مصنوعی می خواهند برای مبارزه با این بدافزار های استخراج استفاده کنند. بسیاری از این ارائه دهندگان سرویس های امنیتی دارند روی تشخیص فعالیت این بدافزار ها در سطح شبکه کار می کنند.

هر نوع بدافزار استخراج در سطح شبکه نیاز به برقراری ارتباط دارد تا هش جدیدی دریافت کرده و آنها را محاسبه کند و سپس آنها را به سرور ها برگرداند و در والت مناسب بگذارد. بنابراین بهترین کار برای تشخیص این فعالیت های مجرمانه این است که بر هر فعالیت مشکوکی در شبکه نظارت داشت و آن را کنترل کرد.

Source

متاسفانه ترافیکی که برای این فعالیت های مجرمانه ایجاد می گردد، بسیار مشکل تشخیص داده می شود و هکر ها اغلب از پیام هایی خلاصه و مبهم استفاده می کنند. مشکل بسیاری از سازمان ها این است که حجم داده های آنها بسیار زیاد می باشد و نظارت بر همه این داده ها مشکل است. فناوری بررسی مستقل SecBI این مشکل را هدف قرار داده و از طریق یادگیری ماشینی با الگو های مشکوک در داده های شبکه های سازمانی مقابله می کند.

SecBI عوامل متعددی را مورد ملاحظه قرار می دهد. به عنوان مثال ترافیک استخراج رمز ارز به صورت دوره ای است و اگرچه سازندگان بدافزار ها سعی می کنند که ماهیت واقعی ارتباط را پنهان کنند اما SecBI فواصل را تصادفی کرده و این مشکل را حل می کند. این فناوری برای ساختار هایی بزرگ مانند آمازون و غیره می تواند بسیار مثمر ثمر باشد.

در این حالت حتی اگر ترافیک رمز گذاری هم شود این تناوب ارتباطات، طول پیام ها و دیگر شاخص های ظریف با هم ترکیب می شوند تا به سیستم کمک کنند که آلودگی ها را تشخیص دهد. در خلال چند ماه گذشته، سیستم SecBI مجهز به تشخیص Cryptojacking شده است و آن را به درستی طبقه بندی می کند و اقدام اصلاحی فوری را نیز انجام می دهد.

از دیگر ارائه دهندگان سرویس های امنیتی برای مقابله با Cryptojacking می توان DarkTrace را نام برد که از فناوری سیستم ایمنی سازمان های اقتصادی استفاده می کند. این سیستم هر نوع ناهنجاری را در شبکه تشخیص داده و با آن مقابله می کند. در زمینه مقابله با Cryptojacking مبتنی بر مرورگر یک روش تضمین شده این است که JavaScript را خاموش کنیم.

این کار شدید ترین پاسخ به این گونه جرایم می باشد و گرنه javaScript در واقع برای مقاصد قانونی در شبکه به کار می رود. نرم افزار آنتی ویروس نیز می تواند بعضی از حملات مبتنی بر مرورگر را مسدود کند. افزونه دیگری که برای مقابله با این جرایم مفید است NoCoin می باشد که عملکردی عالی در زمینه مسدود کردن Coinhive و کلون های آن دارد.

WatchGuard نیز یک استراتژی دفاعی دیگر می باشد که شبکه محور است و می تواند به جستجوی رفتار های مشکوک بپردازد. رویکرد مفید دیگری برای تشخیص Cryptojacking محافظت از endpoint می باشد. این فناوری به قدری هوشمندانه عمل می کند که نه تنها فعالیت مشکوک کنونی بلکه فعالیت های قبلی را نیز شناسایی می کند.

خطر نصب این بدافزار ها توسط کارمندان داخلی شرکت ها به ویژه آنهایی که به دلایلی می خواهند از شرکت جدا شوند و زیاد آنجا نمانند نیز مطرح است و تشخیص این بدافزار ها که خودی ها اعمال کرده اند بسیار مشکل است.

Source

نتیجه گیری

بدافزار های استخراج را اگر بتوان مهار کرد و از ایده نیکویی که در ابتدا پشت آنها بود یعنی ایجاد درآمد برای وب مستر ها و صاحبان سایت ها، بشود استفاده کرد، این امر کمک زیادی را به مالکان سایت ها و وبلاگ های پر بازدید می کند. همان طور که گفته شد می توان به جای تبلیغات آزار رسان اینترنت از فرآیند استخراج استفاده کرد و این کار برای کاربران نیز خوشایند تر خواهد بود. استخراج با استفاده از سیستم دیگران و آن هم بدون اجازه آنها قطعا جرم است و برای مقابله با این جرایم باید تمهیداتی اندیشیده شود و cryptojacking را در خدمت صاحبان وبلاگ ها و وب سایت های پر بازدید قرار داد. البته این ایده در عمل دشوار است و اگر قرار باشد هر وب سایتی از قدرت پردازشی CPU شما استفاده کند، کار در اینترنت بسیار سخت خواهد بود.

منابع

https://www.zdnet.com/article/cryptocurrency-mining-malware-why-it-is-such-a-menace-and-where-its-going-next/

https://www.zdnet.com/article/why-cryptocurrency-mining-malware-is-the-new-ransomware/

https://blog.trendmicro.com/trendlabs-security-intelligence/cryptocurrency-mining-malware-2018-new-menace/

https://www.webopedia.com/TERM/C/cryptomining-malware.html

https://www.csoonline.com/article/3267572/encryption/how-to-detect-and-prevent-crypto-mining-malware.html

https://coiniran.com//?s=%D8%A8%D8%AF%D8%A7%D9%81%D8%B2%D8%A7%D8%B1+%D9%87%D8%A7