بسمه تعالی

مرکز تخصصی آپا دانشگاه رازی گزارش می‌دهد

راهکارهای مقابله و پیشگیری از باج‌افزار BTCWare PayDay

گروه خبری:

مقالات آموزشی

نسخه‌ی کامل خبر

آذر ماه ۱۳۹۶

چگونه متوجه شویم سیستم ما توسط باج‌افزار PayDay آلوده شده است؟

هنگامی که باج‌افزار BTCWare کامپیوتر شما را آلوده می‌کند تمام درایوهای شما را جهت یافتن فایل‌های مورد هدف اسکن می‌نماید، آن‌ها را رمز نموده و سپس پسوند PayDay را به آن‌ها اضافه می‌کند. زمانی که فایل‌ها رمزگذاری شدند دیگر توسط برنامه‌های معمولی باز نخواهند شد.

پیغامی که پس از رمز شدن فایل‌ها به شما نشان داده می‌شود شامل دستورالعمل نحوه‌ی اتصال به سرویس رمزگشایی است، جایی که شما می‌توانید بفهمید چه اتفاقی برای فایل‌های شما افتاده و اینکه چگونه باید باج را پرداخت نمایید تا فایل‌های شما رمزگشایی شوند.

آیا امکان رمزگشایی فایل‌های رمز شده با پسوند .PayDay*وجود دارد؟

خیر، اکنون امکان بازیابی فایل‌های رمز شده با پسوند .PayDay وجود ندارد!

باج‌افزار BTCWare PayDay به خاطر نحوه‌ی رمزگذاری فایل‌های کاربر قابل توجه است_ یعنی این باج‌افزار از شیوه رمزنگاری AES-265 و RSA استفاده می‌کند_ برای اینکه مطمئن شود کاربر هیچ راهی جز پرداخت باج و خرید کلید خصوصی ندارد. کلید عمومی RSA تنها با کلید خصوصی مربوطه رمزگشایی می‌گردد. از آنجا که کلید AES با استفاده از رمزنگاری RSA مخفی شده است و کلید خصوصی RSA در دسترس نیست، رمزگشایی فایل‌ها آن‌طور که گفته شده میسر نیست.

با توجه به مدت زمانی که برای شکستن کلید رمزنگاری AES مورد نیاز است، ادعای Brute force نمودن کلید رمزگشایی واقع‌بینانه نیست. متأسفانه زمانی که کار رمز نمودن داده‌ها توسط BTCWare PayDay به پایان رسید، دیگر رمزگشایی بدون پرداخت باج امکان‌پذیر نخواهد بود. از آنجا که کلید خصوصی مورد نیاز برای باز کردن فایل‌های رمز شده تنها از طریق مجرمان سایبری امکان‌پذیر است، ممکن است قربانیان وسوسه شده و بخواهند با پرداخت باج مورد نظر، کلید را خریداری نمایند. با این وجود، انجام این کار ممکن است افراد سودجو

را به ادامه‌ی این عمل و حتی افزایش مبلغ درخواستی تشویق نماید. توصیه‌ی ما این است که شما هیچ پولی به این مجرمان سایبری پرداخت نکنید، و در عوض به آژانس اجرای قانون در کشور خود (پلیس فتا در ایران) این حمله را گزارش دهید.

نحوه حذف باج‌افزار PayDay

توجه داشته باشید که طی فرآیند حذف باج‌افزار خطر از دست دادن فایل‌ها وجود دارد، ما نمی‌توانیم تضمین کنیم که فایل‌های شما قطعاً بازیابی خواهند شد. علاوه بر این، هنگام حذف باج‌افزار یا تلاش برای بازیابی فایل‌های رمز شده این فایل‌ها ممکن است برای همیشه تسخیر شوند.

این مطلب یک راهنمای جامع است که باج‌افزار BTCWare PayDay را از کامپیوتر شما حذف می‌کند، با این وجود ما نمی‌توانیم تضمین کنیم که فایل‌های شما بازیابی خواهند شد. ما مسئولیت حذف اسناد و فایل‌های شخصی شما را طی فرآیند حذف باج‌افزار به عهده نخواهیم گرفت.

برنامه‌های Malwarebytes و HitmanPro می‌توانند این آلودگی را شناسایی و حذف کنند اما نمی‌توانند فایل‌های رمز شده‌ی شما را بازگردانند.

گام اول: استفاده از Malwarebytes برای حذف باج‌افزار BTCWare PayDay

برنامه‌ی ضدبدافزار Malwarebytes یک اسکنر قدرتمند مبتنی بر درخواست است که PayDay را از دستگاه شما حذف خواهد نمود. توجه داشته باشید که این برنامه‌ی ضدبدافزار می‌تواند همراه با آنتی‌ویروس بر روی سیستم، بدون هیچ تداخلی، اجرا شود.

۱. شما می‌توانید ضدبدافزار Malwarebytes را از لینک زیر دانلود نمایید:

https://www.malwarebytes.com/mwb-download

۲. پس از دانلود، تمامی برنامه‌های خود را ببندید، سپس بر روی آیکون موجود بر روی دسکتاپ خود به نام " mbam-setup " دابل کلیک کنید تا نصب آغاز گردد.

ممکن است هنگام نصب با پیغام User Account Control به صورت زیر مواجه گردید که از شما می‌پرسد آیا می‌خواهید این فایل اجرا شود یا خیر، اگر این اتفاق افتاد باید بر روی "Yes " کلیک کنید تا نصب ادامه یابد.

۳. زمانی که نصب آغاز شد، صفحه‌ی نصب ضدبدافزار Malwarebytes را خواهید دید که شما را از طریق فرآیند نصب راهنمایی خواهد نمود.

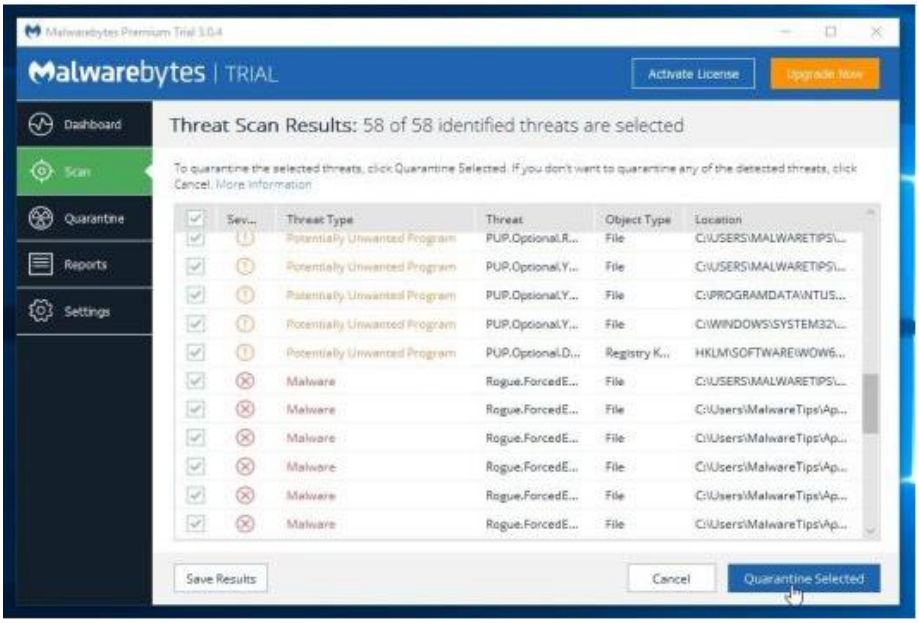
جهت نصب ضدبدافزار Malwarebytes بر روی سیستم دستورات زیر را با کلیک بر روی "Next" دنبال کنید.

۴. پس از نصب، Malwarebytes به طور خودکار شروع به کار کرده و پایگاه داده‌ی آنتی‌ویروس را آپدیت خواهد کرد. جهت آغاز اسکن سیستم، می‌توانید بر روی دکمه‌ی "Scan Now" کلیک کنید.

۵. با کلیک بر روی دکمه‌ی "Scan Now" ضدبدافزار شروع به اسکن کرده و کامپیوتر شما را برای یافتن بدافزار BTCWare PayDay. اسکن خواهد نمود. زمانی که ضدبدافزار Malwarebytes در حال اسکن است صفحه‌ای مانند تصویر زیر نشان داده خواهد شد.

۶. زمانی که اسکن به پایان رسید، شما با صفحه‌ای مطابق تصویر زیر که نشان‌دهنده‌ی آلودگی‌های بدافزاری (آلودگی ناشی از باج‌افزار PayDay) شناسایی شده توسط این ضدبدافزار است مواجه خواهید شد.

به منظور حذف برنامه‌های مخربی که توسط این برنامه یافت شده است، بر روی دکمه‌ی " Remove Selected" کلیک نمایید.



ضدبدافزار Malwarebytes اکنون تمامی فایل‌های مخرب و کلیدهای رجیستری را که یافته است قرنطینه می‌کند. هنگام حذف فایل‌ها، ضدبدافزار ممکن است جهت حذف برخی از فایل‌ها نیاز به راه‌اندازی مجدد داشته باشد. بنابراین اگر پیغامی در خصوص ریستارت کردن سیستم به شما نشان داده شد اجازه‌ی این کار را بدهید.

پس از اینکه سیستم ریستارت شد، شما باید ضدبدافزار Malwarebytes را باز کرده و مجدداً اسکن را بزنید تا مطمئن شوید خطری سیستم شما را تهدید نمی‌کند.

گام دوم: با HitmanPro سیستم خود را دوباره بررسی نمایید

HitmanPro بدافزارها، ابزارهای تبلیغاتی مزاحم، بات‌ها و سایر تهدیدات را یافته و آن‌ها را حذف می‌نماید، در حدی که حتی ممکن است بهترین آنتی‌ویروس‌ها را نیز از بین ببرد. این برنامه برای اجرا در کنار آنتی‌ویروس‌ها، فایروال‌ها و دیگر برنامه‌های امنیتی طراحی شده است.

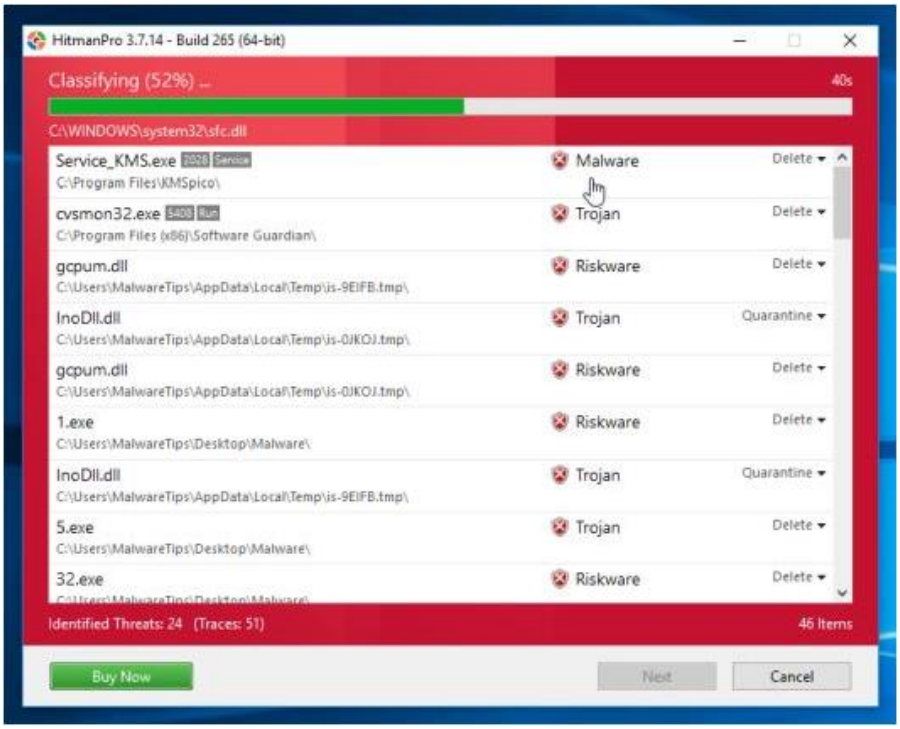
۱. می‌توانید HitmanPro را از لینک زیر دانلود نمایید:

https://www.hitmanpro.com/en-us/hmp.aspx

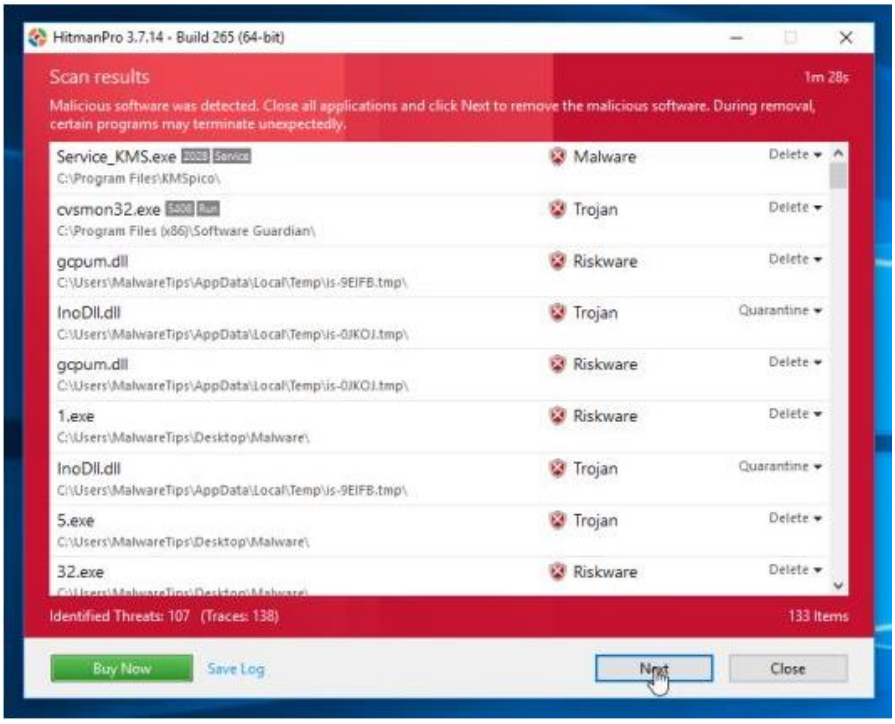
۲. بر روی فایل به نام "HitmanPro.exe" (برای نسخه‌های ۳۲ بیتی ویندوز) یا "HitmanPro_x64.exe" (برای نسخه‌های ۶۴ بیتی ویندوز) دابل کلیک کنید.

برای نصب HitmanPro بر روی کامپیوتر، روی دکمه‌ی "Next" کلیک کنید.

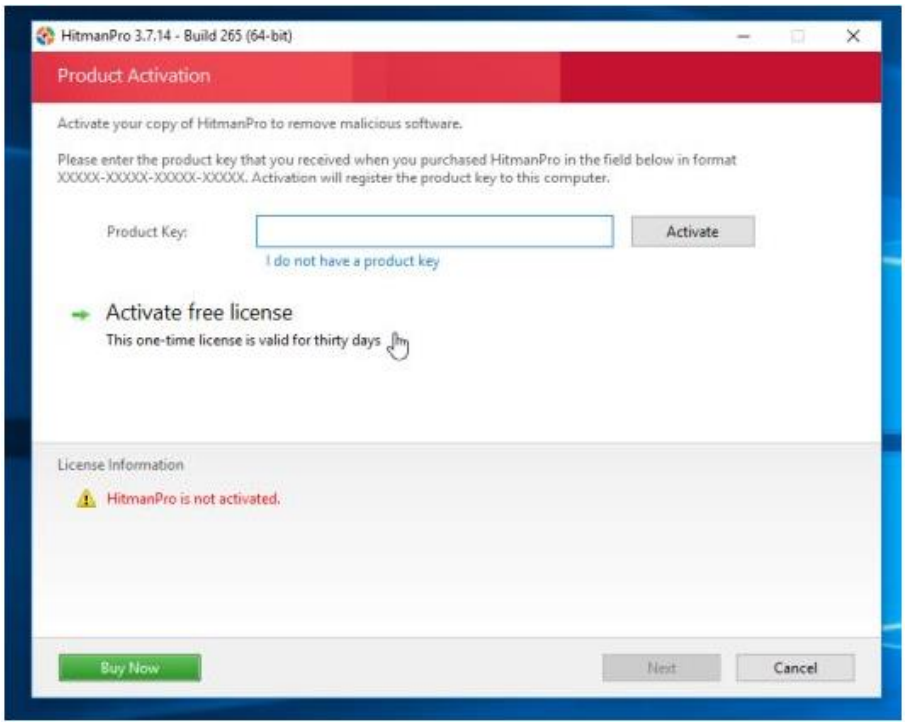
۳. اکنون HitmanPro شروع به اسکن سیستم شما، جهت یافتن بدافزارها خواهد نمود.



۴. زمانی که اسکن به پایان رسید، مطابق تصویر زیر لیستی از تمام بدافزارهایی که برنامه شناسایی کرده به شما نشان داده خواهد شد. برای حذف بدافزار بر روی دکمه‌ی "Next" کلیک کنید.



۵. برای اینکه برنامه به مدت ۳۰ روز به صورت آزمایشی فعال شود بر روی دکمه‌ی " Activate free license" کلیک کنید، و تمامی فایل‌های مخرب را از سیستم خود حذف کنید.



گام سوم: بازگردانی فایل‌های رمز شده توسط BTCWare PayDay با نرم‌افزارهای بازیابی

روش اول: بازگردانی فایل‌های رمز شده توسط BTCWare PayDay با ShadowExplorer

BTCWare PayDay تلاش می‌کند تمام کپی‌های Shadow را زمانی که شما برای اولین بار پس از آلوده شدن، هرگونه فایل اجرایی را باز می‌کنید حذف نماید. خوشبختانه، این آلودگی همیشه قادر به حذف کردن کپی‌های Shadow نیست، بنابراین شما باید سعی کنید فایل‌های خود را با استفاده از این روش بازگردانید.

۱. شما می‌توانید ShadowExplorer از لینک زیر دانلود نمایید:

http://www.shadowexplorer.com/downloads.html

۲. زمانی که ShadowExplorer را دانلود و نصب کردید، می‌توانید با دنبال کردن ویدئوی راهنمایی که در لینک زیر آمده است نحوه‌ی بازگردانی فایل‌های رمز شده را با استفاده از این روش ببینید:

https://www.youtube.com/watch?v=oaXtQ6rbvxA

روش دوم: بازگردانی فایل‌های رمز شده توسط BTCWare PayDay از طریق نرم‌افزار بازگردانی فایل Recuva

هنگامی که فایل‌ها توسط BTCWare PayDay. رمز شدند، باجافزار ابتدا یک کپی از فایل‌ها ایجاد می‌کند، کپی را رمز کرده و سپس فایل‌های اصلی را پاک می‌کند. بنابراین شما می‌توانید از نرم‌افزارهای بازگردانی فایل مانند Recuva استفاده کنید.

می‌توانید با دنبال کردن ویدئوی راهنمایی که در لینک زیر آمده است نحوه بازگردانی فایل‌های رمز شده را با استفاده از Recuva ببینید:

https://www.youtube.com/watch?v=LeEICG0zWqY

چگونه از آلوده شدن کامپیوتر خود توسط این باج‌افزار جلوگیری کنیم؟

به منظور حفاظت از سیستم در مقابل باج‌افزار BTCWare PayDay همیشه باید یک آنتی‌ویروس بر روی سیستم نصب داشته باشید و نیز همیشه از فایل‌های شخصی خود بک‌آپ بگیرید. روش حفاظتی دیگر این است که از برنامه‌ای به نام HitmanPro.Alert استفاده کنید که از اجرای هر گونه بدافزار رمزکننده‌ی فایل جلوگیری می‌کند.

در ویدئویی که در لینک زیر آمده است نحوه‌ی نصب و کار با این برنامه توضیح داده شده است:

https://www.youtube.com/watch?v=XrSP-CMjuFk

منبع:

https://malwaretips.com/blogs/remove-btcware-payday-ransomware/#prevent