ناشناخته، اما قدرتمند و کاربردی

پنج ابزار جادویی امنیتی که هیچ‌گاه روی سیستم خود نصب نکرده‌اید

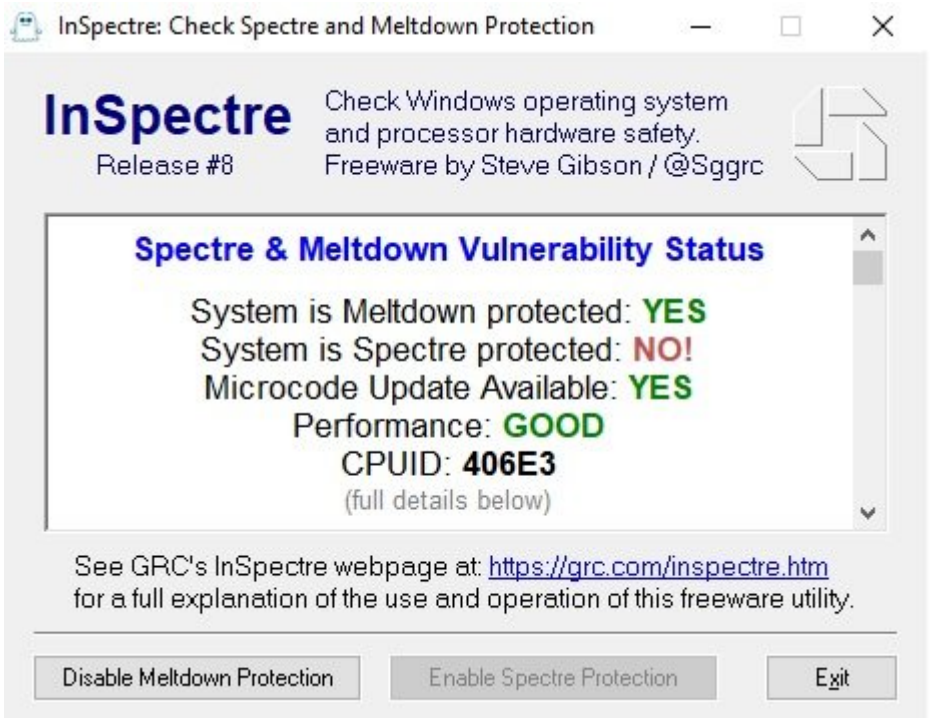
هر زمان سخن از ابزارهای امنیتی به میان می‌آید، منتظر هستیم تا مطالبی درباره ضدویروس‌ها و دیوارهای آتش بشنویم. درست است که ابزارهای یاد شده از سامانه ما در برابر تهدیدات محافظت می‌کنند، اما محافظت از سامانه‌های کامپیوتری محدود به ابزارهای فوق نیست و شما باید از ابزارهای قدرتمند اما کمتر شناخته شده‌ای که وجود دارند برای محافظت از سامانه‌های کامپیوتری خود استفاده کنید. در این مقاله با پنج ابزار امنیتی آشنا خواهید شد که ممکن است خبری در مورد آن‌ها نخوانده باشید.

برخی بر این باور هستند که نصب یک بسته امنیتی کامل برای محافظت از سامانه‌ها کافی است و دیگر لزومی ندارد تا ابزارهای جانبی دیگری نصب شوند. اما یک کارشناس امنیتی به خوبی می‌داند که حتا قدرتمندترین ضدویروس‌های حال حاضر هیچ‌گونه تضمینی در اختیارتان قرار نمی‌دهند که از سامانه شما در برابر تهدیدات محافظت کنند. درست است که ضدویروس‌ها می‌توانند به خوبی از سامانه‌ها در برابر ویروس‌ها، بدافزارها و در برخی موارد باج‌افزارها مراقبت کرده و در ترکیب با دیوار آتش سپر خوبی پیرامون یک سامانه قرار دهند، اما این محصولات نیز کاستی‌هایی دارند که لزوم به‌کارگیری ابزارهای مکمل را دوچندان می‌کنند. در ادامه با پنج مورد از ابزارهای قدرتمند رایگان امنیتی آشنا خواهید شد.

مطلب پیشنهادی

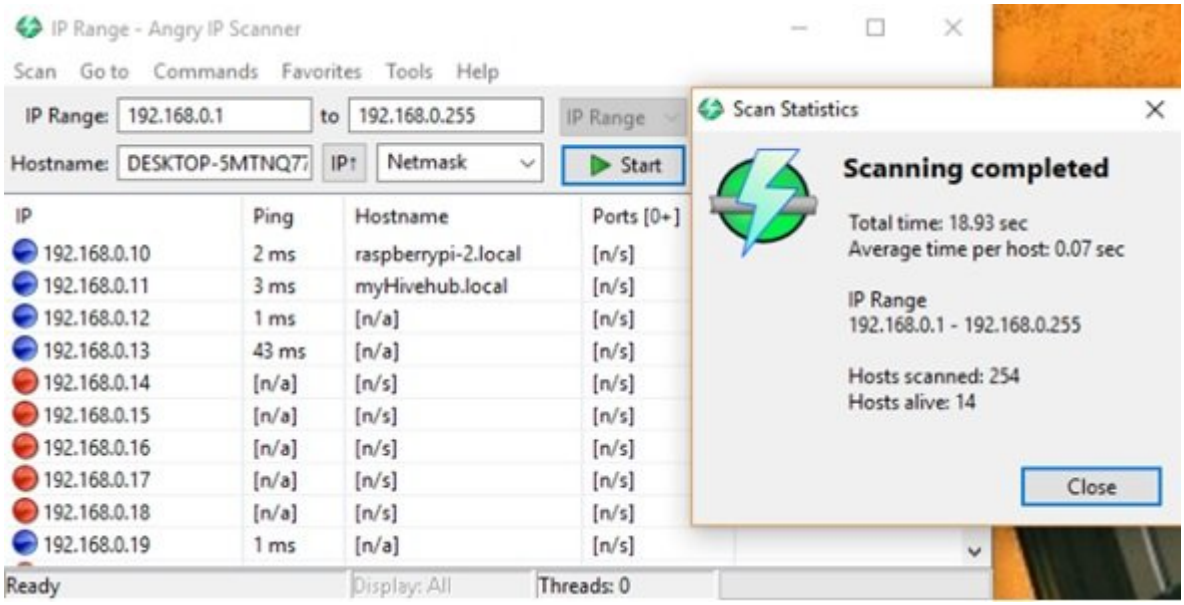
SamSam و Maktub باج‌افزارهایی تکامل‌یافته و نوین
شروع عصر باج‌افزارها؛ هر سال خطرناک‌تر و پیچیده‌تر

1. ابزار پویش‌گر Inspectre



به احتمال زیاد به خوبی می‌دانید که باگ‌های Spectre و Meltdown چه هستند و چگونه به هکرها اجازه می‌دهند اطلاعات شخصی شما را به سرقت ببرند. دو آسیب‌پذیری فوق در سطح سخت‌افزار سیستم و پردازنده مرکزی به هکرها اجازه می‌دهند به سامانه‌های قربانیان نفوذ کنند. درست است که این فرضیه در حد تئوری باقی مانده است، اما پیاده‌سازی یک چنین حمله‌ای دور از انتظار نیست. تنها تعداد محدودی از سامانه‌های کامپیوتری در برابر آسیب‌پذیری‌های فوق ایمن هستند و حتا وصله‌ها و به‌روزرسانی‌های امنیتی در سطح سیستم‌عامل‌ها نیز تنها فرآیند آسیب‌پذیری را کمی کند می‌کنند. مایکروسافت ابزار خاص خود را برای بررسی این دو آسیب‌پذیری ارائه کرده است، اما به دلیل پیچیده بودن همه کاربران نمی‌توانند از این ابزار استفاده کنند. اما ابزار ساده و قدرتمند دیگری به نام InSpectre به شکل رایگان در اختیارتان قرار دارد که قادر است وضعیت یک سیستم را ارزیابی کرده و اطلاع دهد چه تهمیداتی را برای به‌روزرسانی سخت‌افزاری و نرم‌افزاری سامانه خود باید در نظر بگیرید تا سطح ایمنی سامانه‌تان افزایش پیدا کند. ابزار Inspectre به سادگی قابل استفاده بوده و به خوبی می‌تواند آسیب‌پذیری‌های پردازنده مرکزی سامانه را تشخیص داده و هر زمان وصله یا به‌روزرسانی امنیتی ارائه شد شما را مطلع کند. با فعال‌سازی این ابزار تا حد زیادی سامانه شما در مقابل دو آسیب‌پذیری فوق مصون خواهد بود، اما اگر پس از اجرای این نرم‌افزار احساس کردید که سرعت سیستم شما کاهش پیدا کرد گزینه غیر فعال کردن برای شما در نظر گرفته شده است. برای دانلود نرم‌افزار فوق به آدرس **InSpectre** مراجعه کنید.

2. Angry IP Scanner



نرم‌افزار Angry IP Scanner با بیش از 23 میلیون بار دانلود در پلتفرم‌های مختلف یکی از مهم‌ترین ابزارهایی است که حتما باید روی سامانه خود داشته باشید. یک نرم‌افزار چندسکویی متن‌باز و رایگان که شبکه‌های محلی را بر مبنای آدرس آی‌پی که برایش تعیین کرده‌اید پویش می‌کند. در ادامه آدرس‌های آی‌پی پینگ شده و هرگونه داده‌ای که در پاسخ ارسال کرده‌اند جمع‌آوری می‌شود. خروجی این پویش در قالب یک فایل متنی یا فرمت‌های XML و CSV در اختیارتان قرار می‌گیرد. این ابزار به شما اعلام می‌دارد که چه دستگاه‌هایی روی شبکه شما قرار دارند. اگر مشکوک هستید که همسایه شما به شبکه‌تان نفوذ کرده این ابزار به راحتی این مسئله را برای شما بررسی می‌کند. دقت کنید که شناسایی و کشف گذرواژه شبکه وای‌فای برای برخی از افراد کار چندان پیچیده‌ای نیست، در نتیجه با پویش مرتبط تجهیزاتی که به شبکه شما متصل شده‌اند، اطمینان حاصل خواهید کرد همسایه شما به شکل غیرقانونی به شبکه شما نفوذ نکرده است. توجه داشته باشید که ابزار فوق از جاوا استفاده کرده و در نتیجه باید جدیدترین نسخه جاوا روی سیستم شما نصب شده باشد. برای دانلود نرم‌افزار فوق به آدرس **Angry IP Scanner** مراجعه کنید.

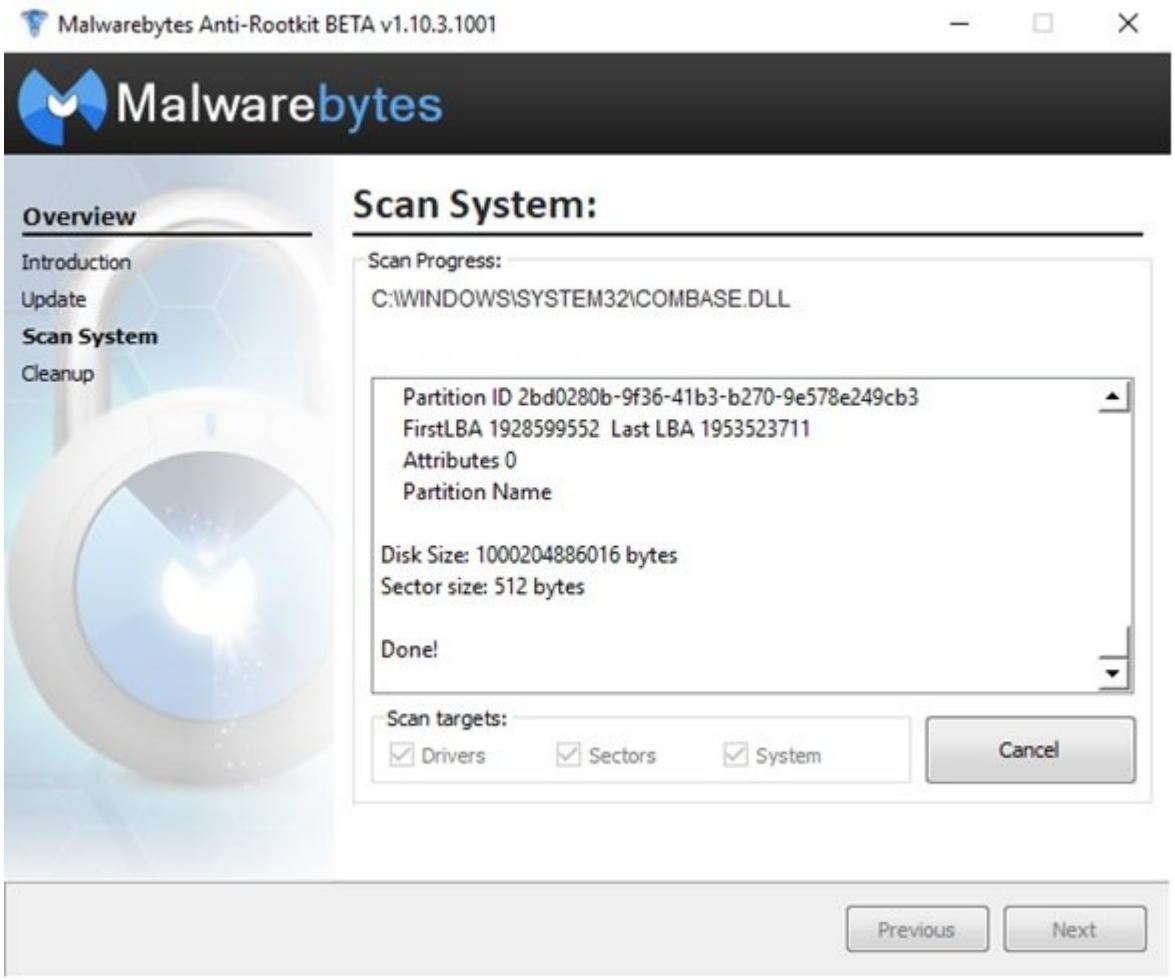
3. Cybereason RansomFree

می‌دانید که باج‌افزارها چه هستند؟ باج‌افزارها گونه‌ای از بدافزارها هستند که سامانه‌ها و فایل‌ها را رمزگذاری کرده و مادامی که قربانیان باج درخواست شده را به هکرها پرداخت نکنند داده‌ها همچنان در وضعیت قفل باقی خواهند ماند. این مشکل نه تنها برای کاربرانی که تصاویر و فایل‌های شخصی روی سامانه خود دارند وضعیت بغرنجی را ایجاد می‌کند، بلکه برای شرکت‌ها که اسناد و قراردادهای تجاری دارند مشکل‌ساز خواهد بود. RansomFree from Cybereason ابزار قدرتمندی است که بنابر ادعای سازنده آن تا 99 درصد قادر است از سامانه‌ها در برابر باج‌افزارها محافظت کند. این ابزار با ایجاد فایل‌هایی موسوم به canary قادر است رفتارهای باج‌افزاری را تشخیص دهد. ابزار فوق این فایل‌ها را در مکان‌هایی قرار می‌دهد که باج‌افزارها ابتدا کار خود را از آن بخش‌ها آغاز می‌کنند. در نتیجه در همان آغاز فرآیند رمزگذاری به سرعت به کاربر هشدارهای لازم را خواهد داد. این ابزار بدون مشکل در کنار سایر بسته‌های امنیتی قابل استفاده است. برای دانلود نرم‌افزار فوق به آدرس **RansomFree** مراجعه کنید.

4. Disconnect

زمانی که گشت‌وگذار در وب را آغاز می‌کنید، کامپیوتر شما تنها سایت‌هایی که به آن‌ها وارد شده‌اید متصل نمی‌شود. تبلیغات مختلفی که درون یک سایت قرار دارند یا اسکریپت‌هایی که یک سایت اجرا می‌کند باعث می‌شوند تا کامپیوتر شما به سایت‌های مختلفی متصل شود. افزونه Disconnect زمانی که روی مرورگر کامپیوترتان نصب شود به شما اجازه می‌دهد به رهگیری نرم‌افزارهایی بپردازید که فعالیت‌های شما را ردیابی می‌کنند. ابزار فوق با شناسایی و مسدود کردن، سایت‌های رهگیر قادر است تا 44 درصد سرعت مرورگر شما را افزایش داده و امنیت آنلاین سامانه شما را بهبود بخشد. افزونه فوق اجاز می‌دهد فهرست سفیدی ایجاد کرده و در آن مواردی که قرار است دانلود شوند را مشخص کنید. افزونه Disconnect برای مرورگرهای مختلف **کروم**، **فایرفاکس**، **اپرا** و **سافاری** عرضه شده است.

5. Malwarebytes Anti-Rootkit



روت‌کیت‌ها گونه ای خطرناک از بدافزارها هستند که قادر هستند فعالیت‌های ضدویروس‌ها را مختل کرده و به هکرها اجازه دهند مجوزهایی در سطح مدیر یک سیستم به دست آورده تا کنترل کاملی روی سامانه قربانیان داشته باشند. دقت کنید که روت‌کیت‌ها در سطح سخت‌افزار کار می‌کنند. در نتیجه روت‌کیت‌ها می‌توانند کنترل بایوس و سیستم‌عامل را به دست آورند. یکی از بهترین ابزارهایی که برای مقابله با روت‌کیت‌ها عرضه شده است، Malwarebytes Anti-Rootkit است. با نصب ابزار فوق فرآیند پویش سیستم آغاز می‌شود. برای دانلود نرم‌افزار فوق به آدرس **Malwarbytes Anti-Rootkit** مراجعه کنید.

تاریخ انتشار:
24 فروردین 1398

نشانی منبع:
https://www.shabakeh-mag.com/security/14901/%D9%BE%D9%86%D8%AC-%D8%A7%D8%A8%D8%B2%D8%A7%D8%B1-%D8%AC%D8%A7%D8%AF%D9%88%DB%8C%DB%8C-%D8%A7%D9%85%D9%86%DB%8C%D8%AA%DB%8C-%DA%A9%D9%87-%D9%87%DB%8C%DA%86%E2%80%8C%DA%AF%D8%A7%D9%87-%D8%B1%D9%88%DB%8C-%D8%B3%DB%8C%D8%B3%D8%AA%D9%85-%D8%AE%D9%88%D8%AF-%D9%86%D8%B5%D8%A8-%D9%86%DA%A9%D8%B1%D8%AF%D9%87%E2%80%8C%D8%A7%DB%8C%D8%AF