خبرنامه امنیت رایانه ای
کمیته امداد امام خمینی (ره)

سال اول، شماره هفدهم نیمه دوم آذر هشتاد و شش

دفتر آمار و فناوری اطلاعات

در ادامه بررسی ابزارهای افزایش امنیت رایانه ای، در این شماره نرم افزار ThreatFire محصول PC Tools را به شما معرفی می کنیم.
با وجود سادگی آموزشهای این بولتن، لطفاً آنها را فقط تحت نظارت یکی از کارشناسان دفتر آمار و فناوری اطلاعات انجام دهید. تلاش شده است تا حد امکان مطالب به زبان ساده و قابل فهم برای همه بیان شود و با این وجود برای افراد با تجربه نیز مطالب جدیدی در این خبرنامه وجود داشته باشد.
شما نیز می توانید نیازهای خود را جهت طرح و پاسخ و یا مطالب و مقالات خود را جهت درج با نام خود در این خبرنامه با ارسال به دفتر آمار و فناوری اطلاعات مرکز با ما در میان بگذارید.

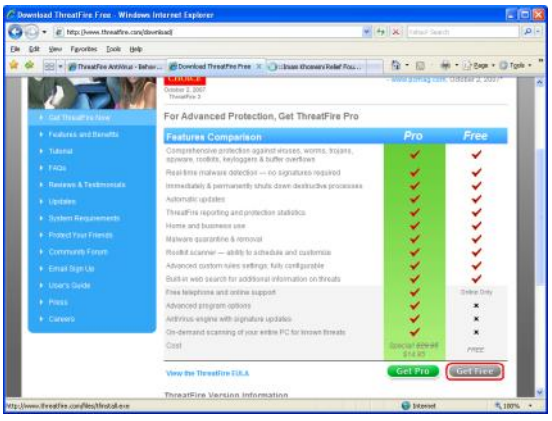
آشنایی با ThreatFire

نرم افزار ThreatFire که ابتدا به نام Cyber Hawk محصول شرکت Novatix به بازار عرضه شده بود و پس از آنکه PC Tools آنرا خریداری نمود به این نام عرضه شد یکی از بهترین نرم افزارهای هوشمند مقابله با ویروس، اسب تروا، کرم و هر نوع برنامه ناخواسته می باشد که به صورت مکمل همراه با نرم افزارهای ضد ویروس قابل استفاده می باشد.

برای دریافت نسخه رایگان این نرم افزار کافیست به آدرس زیر بروید و روی لینک Free Download کلیک فرمایید:

http://www.ThreatFire.com

پس از آن صفحه ای مشابه زیر ظاهر می شود:

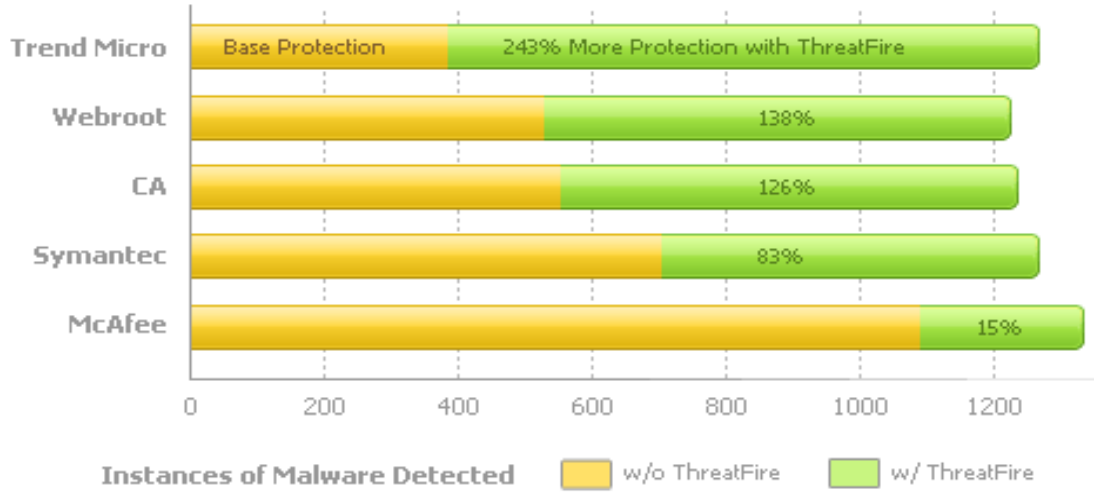


در صفحه فوق، روی Get Free کلیک فرمایید تا دانلود نرم افزار با باز شدن صفحه ای مانند زیر آغاز شود. مطابق معمول روی Save کلیک کنید تا آنرا در محل مناسبی ذخیره نمایید و در انتها اجرا نمایید. پس از یک بار دانلود، فایل را می توانید کپی نموده و روی چندین رایانه نصب نمایید.

پس از نصب کامل Threat Fire، شما یک آیکون به شکل آتش که نماد این نرم افزار می باشد در کنار ساعت روی Task Bar ویندوز خود خواهید داشت.

حال در زمانی که منتظر دانلود شدن هستید، بیایید کمی بیشتر با هدف این نرم افزار و چگونگی کمک آن به امنیت رایانه ما آشنا شویم.

آشنایی با ThreatFire



به شکل بالا دقت کنید، این شکل نشان می دهد که با وجود داشتن نرم افزارهای خوب ضد ویروس باز هم این نرم افزار می تواند به شما کمک کند. چرا؟ چون نرم افزارهای ضد ویروس اغلب بر اساس شناسایی یک ویروس شناخته شده کار می کنند یعنی پس از تولید و انتشار یافتن ویروس جدید، این ویروس به نوعی به دست متخصصان شرکت ضد ویروس شما می رسد و سپس در آزمایشگاه شرکت ضد ویروس، مشخصات آن شناسایی می شود که به این مشخصات امضای ویروس می گوییم و به همین دلیل است که به ضد ویروسهای معمول که به شناسایی بدافزارها بر مبنای این امضاها می پردازند، Signature-based گفته می شود.

Threat Fire اصولاً از سیستم امضاها استفاده نمی کند (البته نسخه غیر رایگان آن امکاناتی در این زمینه هم دارد) بلکه بر اساس رفتارهای خطرناک و غیر معمول به شناسایی بدافزارها می پردازد.

یک بدافزار معمولاً سعی می کند به طریقی خود را روی سیستم شما بنشاند تا همواره اجرا شود، احتمالاً از یک سیستم Packing استفاده کرده است تا امضای آن توسط ضدویروس دیده نشود و رفتارهای خطرناک دیگری مثل ارسال ایمیل، دخالت در سایر برنامه ها، تلاش در دزدیدن رمزهای عبور از طریق گوش کردن به کلیدهای تایپ شده و... از خود بروز می دهد که همگی توسط Threat Fire بررسی و در صورت بروز رفتار غیر معمول جهت اجرا یا عدم اجرای آن از شما اجازه می گیرد.

استفاده از این نرم افزار به عنوان مکمل ضد ویروسهای معمول بسیار مفید است چرا که:

۱. همیشه ابتدا ویروسها و بدافزارها تولید می شوند و ضد ویروسها با فاصله زمانی می توانند آنها را شناسایی کنند و به روز رسانی به شما ارائه کنند که ممکن است شما هم با فاصله زمانی آنرا نصب کنید در نتیجه گاهی روزها بعد از تولید یک بدافزار رایانه شما با ضد ویروسهای معمول نسبت به آن ایمن می شود در حالی که Threat Fire در این مدت نیز به شما کمک می کند.

۲. در برخی موارد یک بدافزار ایرانی یا نوشته شده مخصوص صدمه زدن به شما آنقدر کم در دنیا پخش می شود که اصولاً پس از چند ماه هم ضد ویروس شما قادر به شناسایی آن نخواهد بود و اینجا هم Threat Fire تا حد زیادی به شما یاری می رساند.

۳. سازندگان بدافزارها همواره با تغییرات کوچک کاری می کنند که امضای بدافزارشان تغییر کند و در نتیجه دوباره باید توسط ضد ویروس معمول از ابتدا شناسایی شده و به روز رسانی آن تولید شود که سبب می شود به صرف نصب داشتن نرم افزارهای ضد ویروسهای معمول، حتی در برابر ویروسهای شناخته شده هم کاملاً ایمن نباشید.

آشنایی با ThreatFire

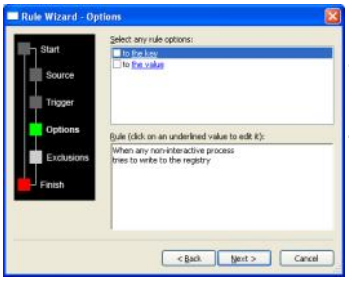
تصویر بالا با دوبار کلیک سریع روی آیکون آتش کنار ساعت که پیشتر گفته شد ظاهر می شود.

به طور پیش فرض Security Status از منوی سمت چپ انتخاب شده است و لذا جدول بزرگ نشان داده شده در صفحه آماری را نشان می دهد که بر حسب شرایط زمانی انتخاب شده تعداد موارد مورد بررسی قرار گرفته و مشکلات و نتایج کار نرم افزار را به شما نشان می دهد.

با انتخاب Start Scan صفحه زیر ظاهر می شود که در آن با انتخاب Basic یا Full تعیین می کنید که تنها بخشهای حساس یا تمام بخشهای دیسک سخت رایانه شما به دنبال Rootkit یعنی بد افزارهای سطح هسته جستجو شود.

در بخش Threat Control که سومین گزینه منو می باشد ضمن مشاهده Log و تاریخچه آنچه Threat Fire یافته و بازخورد نشان داده شده به آن، می توانید تغییراتی در آنچه از نرم افزار خواسته اید همواره به آن اجازه دهد یا ندهد ایجاد نمایید.

بخش Advanced Rules جهت ساختن قواعد خاص برای این نرم افزار به کار می رود که اگرچه ساده است، استفاده از آنرا تنها برای متخصصین توصیه می کنیم. در این بخش به سادگی می توانید رفتارهای غیر طبیعی و خطرناکی را که احتمال می دهید نرم افزار به خودی خود قادر به شناسایی و جلوگیری از آنها نباشد به آن معرفی کنید و در حقیقت به سادگی آنرا برنامه ریزی و برای نیاز خود سفارشی نمایید.



آشنایی با ThreatFire

بخش تنظیمات یا همان Settings که در شکل رو به رو مشاهده می کنید، برای روشن یا خاموش کردن بخشهای مختلف نرم افزار و تنظیم سطح حساسیت آن (بخشی که در شکل انتخاب شده) به کار می رود.

حالت مشابه تصویر نشان داده شده تنظیمات مطلوب را نشان می دهد اما با افزایش حساسیت به عدد ۴ می توانید آنرا حساستر کنید که اگرچه ممکن است کمی ایمنی را بالا ببرد، سبب خواهد شد با سؤالات بیش از حد برای اجازه گرفتن از شما جهت انجام امور معمول نرم افزارهایتان مواجه شوید.

پیشنهاد می کنیم با رفتن به بخش Quarantine (قرنطینه) و تیک زدن مربع مربوط به Restore Point، ساختن یک Restore Point قبل از هر اقدام به قرنطنه را تقاضا نمایید که البته ضروری نمی باشد.

امیدواریم با معرفی این نرم افزار قدرتمند جهت نصب به عنوان مکمل ضد ویروس فعلی شما توانسته باشیم سطح امنیت رایانه و شبکه شما را باز هم بالاتر ببریم. منتظر خبرنامه های بعدی ما باشید.

پرسشهای خود را در هر زمینه مرتبط با IT و رایانه از طریق پست الکترونیک یا نامه به دفتر آمار و فناوری اطلاعات مرکز با ما در میان بگذارید تا پاسخ آنها را در همین خبرنامه دریافت کنید.

همچنین در صورتی که علاقمند به همکاری با این خبرنامه می باشید، می توانید مقالات و مطالب خود را اعم از تألیف یا ترجمه در قالب یک فایل Word به صورت پست الکترونیک یا بر روی CD به دفتر آمار و فناوری اطلاعات ارسال نمایید تا پس از بررسی با نام خود شما در این خبرنامه درج شود.

تهیه شده در دفتر آمار و فناوری اطلاعات

با همکاری شرکت گسترش فناوری اطلاعات و ارتباطات خاورمیانه

سردبیر و نظارت علمی: احسان ریاضی اصفهانی

آدرس اینترنتی

http://www.Emdad.ir/security

کمیته امداد امام خمینی (ره)
لجنة امداد الامام الخمینی (ره)
Imam Khomeini Relief Foundation