آنتی ویروس Dr.Web Katana

(ضد باج افزار)

معرفی شرکت دکتر وب

دکتر وب، شرکتی روسی در زمینه توسعه نرم افزارهای امنیتی می باشد که در سال ۱۹۹۲ میلادی تاسیس گردیده است. این کمپانی همواره جزء برترین ها در زمینه شناسایی و حذف بد افزارها بوده است بطوریکه جهت دست یابی به این هدف نرم افزارهای متنوعی در زمینه امنیت اطلاعات تولید کرده است. در حال حاضر دکتر وب در بیش از ۹۰ کشور جهان دارای نمایندگی فعال می باشد.محصولات دکتر وب جزء محدود محصولاتی می باشد که از تکنولوژی های منحصر به فرد خود کمپانی دکتر وب جهت شناسایی و حذف بد افزارها بهره می برد. این کمپانی با دارا بودن سرویس های قدرتمند مانیتورینگ بد افزاری ولابراتوار قدرتمند تحلیل رفتارهای بد افزارها، این امکان را به این کمپانی عظیم داده است که در کمترین زمان ممکن مشکلات بوجود آمده توسط بدافزارها را حل و فصل نماید.

Dr.WEB®
www.dwav.ir

دکتر وب و تکنولوژی های منحصر به فرد :

دکتر وب در تولیدات محصولات نرم افزاری از تکنولوژی های منحصربه فرد خود جهت تولید آنتی ویروس دکتر وب استفاده می کند، همچنین تمام تلاش خود را معطوف به بهبود روش های جدید درکشف بدافزارهای جدید و پیچیده نموده است که از آن جمله می توان به موارد زیر اشاره کرد:

Self-protection: محافظت چند لایه از خود آنتی ویروس و جلوگیری از غیر فعال شدن آن توسط بدافزارها.

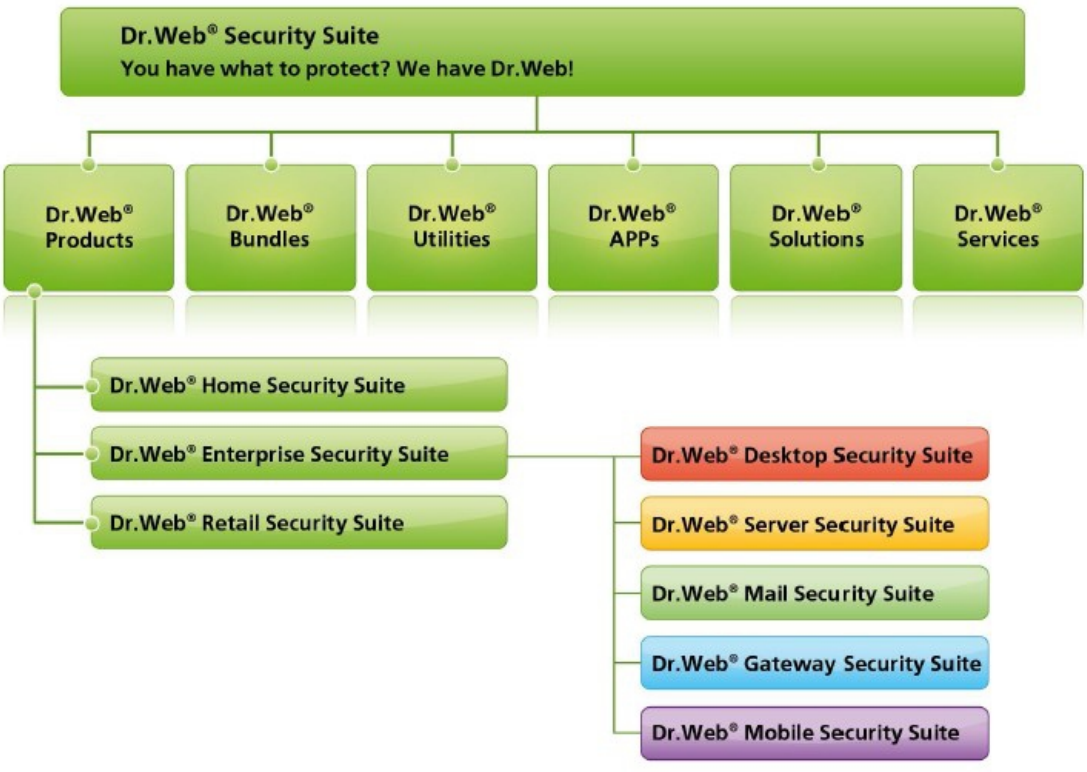
FLY-CODE: تکنولوژی منحصر به فرد کمپانی دکتر وب جهت رمزگشایی فایل هایی که توسط ویروس نویسان و هکرها Encrypt شده اند.

Heuristic analysis: تکنولوژی هوش مصنوعی دکتر وب که توانایی شناسایی انواع مختلف بدافزارهای ناشناخته را به این آنتی ویروی اضافه کرده است.

Anti-spam technologies & Anti-scam technologies: تکنولوژی شناسایی و جلوگیری از فعالیت Spamها و ویرایش خطرناکتری از Spamها که معروف به Scam می باشند.

Unique updating system: استفاده از تکنولوژیهای منحصر به فرد در فشرده سازی آپدیت ها در سیستم به روز رسانی آنتی ویروس دکتر وب، باعث کاهش حجم دانلود بر روی سیستم ها می گردد.

نمایی کلی از محصولات دکتر وب



Dr.WEB®
www.dwav.ir

محصول جدید و منحصر به فرد دکتر وب به نام "کاتانا"

Dr.Web Katana: کاتانا آنتی ویروس بدون پایگاه داده ویروسی دکتر وب می باشد که با تکنولوژیهای منحصر به فرد خود حفاظت پیشگیرانه ای در مقابل تهدیدات فعال، حملات هدفمند و تلاش تروجان ها و Exploit ها و بخصوص باج افزارها برای استفاده از آسیب های امنیتی موجود، بویژه Zero-Day ها که مترصد نفوذ به سیستم های شما می باشند و برای آنتی ویروس ها ناشناخته می باشند، به ارمغان آورده است. این نرم افزار دارای خصوصیاتی چون:

* حفاظت از بخشهای اساسی و حیاتی سیستم و جلوگیری از تغییر آنها توسط بدافزارها.

* شناسایی و متوقف کردن فعالیت بدافزارها، نرم افزارهای مشکوک، اسکریپت های نا مطمئن و پروسسهای آلوده.

* تشخیص تغییر ناخواسته فایلها، نظارت بر کلیه فعالیتهای سیستم به منظور شناسایی انواع تهدیدات امنیتی و جلوگیری از تزریق کدهای مخرب به فعالیتهای جاری سیستم.

* شناسایی و خنثی کردن تهدیدات امنیتی جدید که هنوز مورد شناسایی قرار نگرفته اند و در مخزن ویروس دکتر وب وجود ندارند.

* حفاظت در مقابل سوء استفاده کدهای مخرب از حفره های امنیتی موجود در نرم افزارهای کاربردی مورد استفاده در رایانه.

* کنترل و بررسی عملکرد کلیه مرورگرهای معروف و مورد استفاده کاربران و پلاگین های مورد استفاده در آنها.

امکانات Dr.Web Katana چیست؟

ضد ویروس بدون پایگاه داده ویروس (مخزن ویروس) یک راهکار حفاظتی جدید و ارائه شده توسط شرکت دکتر وب می باشد که می تواند رایانه کاربران را در مقابل انواع تهدیدات، تروجانها و نفوذها و بخصوص باج افزارها مورد حفاظت قرار دهد.

محصول "Dr.Web Katana" نسل نوین و بعدی نرم افزارهای حفاظتی بوده و این اطمینان را به کاربران می دهد تا با بهره گیری از تکنولوژی های جدید کلیه تهدیدات امنیتی جدید و ناشناخته را در بدو گسترش شناسایی و حذف نماید. این تکنولوژی جدید دارای خصوصیات زیر می باشد:

موارد کلی

- شناسایی و خنثی سازی کلیه تهدیدات امنیتی جدید و ناشناخته با بهره گیری از جدیدترین فن آوری ها و الگوریتم های شناسایی.

Dr.WEB®
www.dwav.ir

- "Dr.Web. Katana" یک محصول امنیتی جدید بوده و به منظور شناسایی و مقابله با برنامه های آلوده ای طراحی شده اند که قصد دارند نرم افزار ضد ویروس و الگوریتم های شناسایی سنتی آنها (مانند به کارگیری مخزن ویروس و استفاده از هوش مصنوعی) را دور زده و به رایانه کاربر آسیب برسانند.

- "Dr.Web Katana" فعالیت خود را به محض روشن شدن رایانه و در حین بوت شدن آن بر خلاف محصولات ضد ویروس رایج آغاز می کند.

قابلیت های پنهان

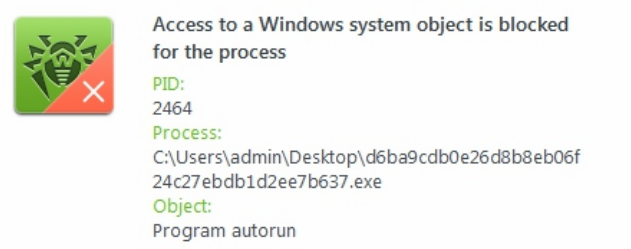
قابلیتها و امکانات یک نرم افزار ضد ویروس باید به طور مداوم با رشد برنامه های مخرب تغییر پیدا کرده و تکمیل گردد. یک محصول امنیتی قدرتمند باید توانایی پیش بینی و مقابله بدون وقفه با یک حمله حتمی را داشته باشد. این تغییرات و پیشرفتها اغلب موجب کاهش راندمان رایانه می گردد و آن دسته از کاربران را که نیاز به راندمان بالا در اجرای برنامه های خود را دارند مجبور می نماید تا نرم افزار ضد ویروس خود را موقتا غیر فعال کنند. طراحان و توسعه دهندگان "Dr.Web Katana" موارد فوق را در طراحی محصول ضد ویروس مدنظر قرار داده اند و محصولی را به کاربران ارائه نموده اند تا با پنهان شدن در لایه های زیرین سیستم و استفاده از کمترین منابع آن راندمان رایانه کاربران را بطور قابل ملاحظه و چشمگیر افزیش دهند.

کاتانا کلیه تهدیدات امنیتی را به سرعت و بدون ایجاد وقفه در راندمان رایانه شناسایی و خنثی می نماید.

"Dr.Web Katana" قابلیت نصب همزمان با آنتی ویروس های دیگر را دارد.

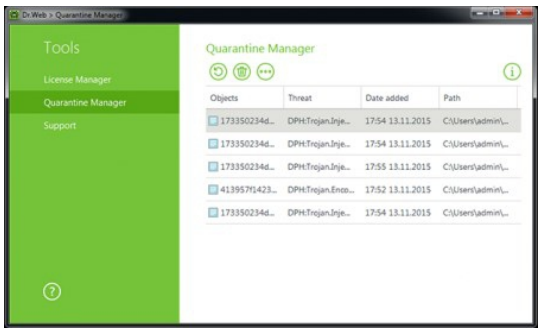
وجه تمایز برجسته

- آنالیز رفتار هر کد مخرب بصورت بلادرنگ و پاکسازی اسکریپت های آلوده و خنثی کردن پروسس های آنها در حالی که نرم افزار ضد ویروس شما حتی قادر به شناسایی آنها نیست از برجسته ترین قابلیتهای این محصول می باشد. محصول "Dr.Web Katana" بر پایه شناسایی بدون استفاده از پایگاه داده (مخزن ویروس) و بهره گیری از فن آوری های نوین تشخیص و حفاظت ابری طراحی شده است. این نرم افزار کلیه پروسس های سیستم را مورد تجزیه و تحلیل قرار داده و به محض مشاهده هرگونه پروسه مشکوک اقدام به بلوکه کردن آن می نماید. در تصویر زیر می توانید هشدار شناسایی را ببینید:



Dr.WEB®
www.dwav.ir

- نرم افزارهای ضد ویروس رسمی و سنتی بر اساس مجموعه ای از الگوریتم های شناسایی از قبل تعریف شده به منظور شناسایی و برخورد با تهدیدات امنیتی استفاده می نمایند که این روشها و الگوریتم ها برای تبهکاران و مجرمان سایبری شناخته شده می باشد. محصول "Dr.Web Katana" متفاوت عمل می کند. این محصول رفتار هر برنامه فعال در رایانه را بصورت بلادرنگ با متدهای انحصاری موجود در فضای ابری دکتر وب که مرتبا در حال به روز رسانی می باشد مقایسه نموده و در صورت مشاهده هرگونه تهدید نسبت به بلوکه کردن و خنثی سازی آن اقدام می نماید.



باج افزار (Ransomware)

باج‌افزارها گونه‌ای از بدافزارها هستند که دسترسی به سیستم را محدود می‌کنند و ایجادکننده آن برای برداشتن محدودیت درخواست باج می‌کند. برخی از انواع آنها روی فایل‌های هارددیسک رمزگذاری انجام می‌دهند و برخی دیگر ممکن است به سادگی سیستم را قفل کنند و پیام‌هایی روی نمایشگر نشان دهند که از کاربر می‌خواهد مبالغی را واریز کنند.

نحوه عملکرد باج افزار

باج افزارها از طرق مختلف مانند کرمها منتشر می‌شوند و پس از نصب و اجرا شروع به اعمالی مانند رمزگذاری بر روی هارددیسک و اطلاعات موجود در آن می‌کنند. باج افزارهای پیشرفته تر با استفاده از کلید عمومی فایلها را رمز نگاری می‌کنند و کلید خصوصی لازم برای بیرون آوردن فایلها از حالت رمز شده تنها در دستان طراح باج افزار است. این روش رمزگذاری را RSA می گویند. کاربر برای باز کردن فایلهایش مجبور به پرداخت وجه به حساب طراح باج افزار می‌شود.

تفاوت باج افزارها و بدافزارهای دیگر

- ❖ استفاده از الگوریتم های غیر قابل رمزگشایی
- ❖ امکان رمزنگاری انواع مختلف فایل ها مانند فیلم، عکس و.....
- ❖ تغییر نام فایل به اسامی نامربوط که باعث سردرگمی می شود
- ❖ اضافه کردن پسوندی خاص به انتهای فایل ها
- ❖ نمایش عکس و یا یک نوشته به معنی اینکه اطلاعات شما رمزنگاری شده است و درخواست باج

Dr.WEB®
www.dwav.ir

- درخواست باج بصورت بیت کوین
- دارای محدودیت در زمان پرداخت باج جهت تحت فشار قراردادن قربانی
- استفاده از مجموعه هایی از روشها برای فرار از شناسایی توسط آنتی ویروس ها
- در اغلب موارد سیستم های آلوده شده جزیی از یک بات نت می شوند جهت حمله به پروژه های بزرگتر
- امکان گسترش از یک سیستم آلوده به دیگر سیستم های موجود در شبکه
- معمولا اطلاعات دیگر سیستم مانند رمز عبور، نام کاربری، ایمیل و ... را برای مقاصد بعدی ارسال می کنند.
- گاهی اوقات نیز با توجه به مکان جغرافیایی خاص زبان آن منطقه را بکار می برند

روش های گسترش باج افزار

- ایمیل های اسپم که حاوی لینک ها و یا پیوست های مخرب می باشند
- سوء استفاده از نرم افزارهای آسیب پذیر (استفاده از خلاهای امنیتی بر روی نرم افزارهایی مثل مرورگرهای اینترنتی)
- تغییر مسیر ترافیک اینترنت به سمت وب سایت های مخرب
- وب سایت های قانونی که در صفحات وب خود سهوا کد مخرب تزریق کرده اند
- Malvertising campaigns: استفاده از تبلیغات آنلاین برای گسترش بدافزارها
- پیامهای (SMS) این روش بیشتر گوشیهای هوشمند را هدف قرار می دهند
- بات نت ها
- خود انتشاری: انتشار از یک سیستم آلوده به سیستم دیگر
- Affiliate schemes in ransomware-as-a-service: کسب درآمد با انتشار باج افزار
- Drive-by downloads

با توجه به اطلاعات مطرح شده جهت جلوگیری از آلوده شدن به تهدیدات بالقوه و خطرناک باج افزاری علاوه بر آموزش کاربران، به روزرسانی نرم افزارهای سیستم عامل و نرم افزارهای کاربردی و .... نیاز به مسلح کردن رایانه ها به تکنولوژی های نوین محافظت پیشگیرانه در زمینه باج افزار ها می باشد.

آماری از دکتر وب

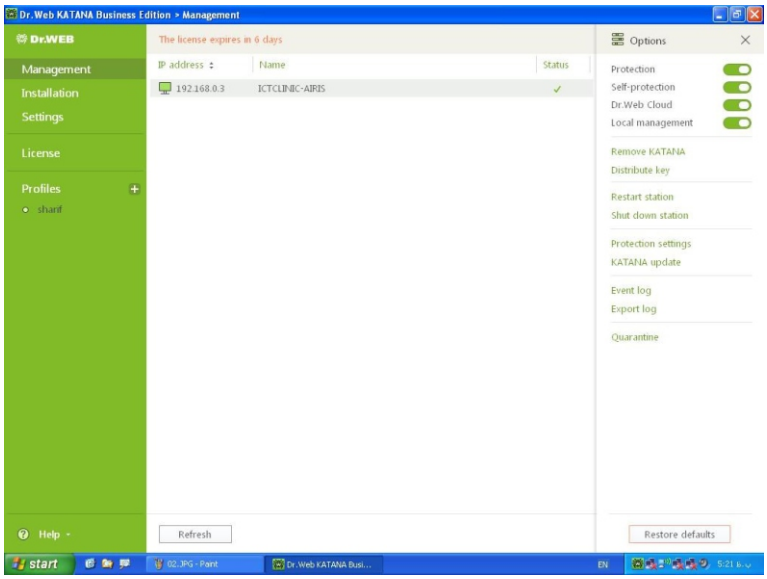
- طبق آمار کمپانی دکتر وب، درصد رشد باج افزارها از سال ۲۰۰۹ تا به حال ۱۹۰۰٪ می باشد.
- از اواسط آوریل ۲۰۱۳ تا پایان سال ۴۰۰۰۰ قربانی باج افزارها به دکتر وب مراجعه کرده اند.
- در سال ۲۰۱۵، ۶۰ درصد درخواست کنندگان خدمات پشتیبانی از دکتر وب مربوط به باج افزارها بوده است، عمده این افراد استفاده کنندگان از آنتی ویرس های برندهای دیگر بوده اند.

پیشنهاد دکتر وب پیشگیری و استفاده از راه کار جدید Dr.web Katana می باشد

Dr.WEB®
www.dwav.ir

ویرایش های مختلف کاتانا

دکتر وب کاتانا دارای دو نسخه کاربران خانگی (Home Edition) و نسخه کاربران شبکه ای (Business Edition) می باشد. هم نسخه خانگی و هم نسخه شرکتی قابل نصب به همراه آنتی ویروس های دیگر می باشند. نصب کاتانا بر روی شبکه های توسط یک نرم افزار مدیریت مرکزی به نام کنترل سنتر انجام می گیرد. تصاویری از نرم افزار کاتانا و نرم افزار مدیریت مرکزی کاتانا را در زیر مشاهده فرمایید.



Dr.WEB
www.dwav.ir

ناوک هوشمند پویان

Edge Intelligent Enterprise

جهت اطلاعات بیشتر در راستای راه حل فوق با ما در ارتباط باشید

navak-ai.ir

021-88109330

info@navak-ai.ir

اطلاعات جمع آوری شده توسط تیم تحقیقات **شرکت ناوک هوشمند پویان** به انجام رسیده است.