آنتی ویروس ATM-Shield

Dr.WEB®
www.drweb.com

Dr.WEB®
www.dwav.ir

امنیت اطلاعات مهمترین چالش در عصر تکنولوژی

امنیت بدون هیچ اغراق و بزرگنمایی مهمترین و پرچالش‌ترین مقوله در دنیای ارتباطات دیجیتال بوده و هست. با توجه به فراگیر شدن استفاده از رایانه، گوشی های هوشمند ، تبلت و ... در زندگی روزمره امروزی، تمامی شرکت‌های تجاری و شخصیت‌های حقیقی به دنبال راه کارهایی جهت ارتقاء امنیت در هنگام استفاده از ابزار دیجیتالی خود می باشند .

طی دهه اخیر حمله تروجان‌ها و بدافزارها به سیستم‌های رایانه ای شخصی، شرکتی و حتی بانکها و بعدتر از آن به گوشی‌های تلفن همراه به سرنوشت محتوم همه کاربران تبدیل شده است چرا که با گسترش اینترنت و نفوذ آن به همه ابعاد زندگی افراد راه چاره ای نیست جز آنکه با کمک یک آنتی ویروس از خودمان در برابر هزاران حمله بدافزاری که هر روزه در فضای مجازی گسترش پیدا می‌کند، مقابله کنیم.

ضرورت استفاده از آنتی ویروس ATM-Shield

با چند سوال زیر شروع می کنیم:

- از یک حافظه یو اس پی بدون اینکه آنرا توسط یک آنتی ویروس اسکن کنیم، استفاده می کنیم؟
- شما ایمیل های ارسال شده از یک منبع ناشناخته را باز می کنید؟
- شما تحت یک حساب کاربری مدیر در ویندوز کار می کنید؟
- شما به روز رسانی امنیتی نرم افزارهای مورد استفاده را انجام می دهید؟
- شما دسترسی به اینترنت را از طریق رایانه های محل کار خود که از برنامه هایی که حاوی خلا های امنیتی می باشند، انجام می دهید؟
- شما از رمزهای عبوری ضعیف استفاده می کنید که به راحتی هک می شوند؟

چه چیزی به ما این اطمینان را می دهد که کارکنان مسئول تعمیر و نگهداری ATM ها ، چنین اشتباهاتی را انجام ندهند؟

کمی صبر کنیم، مگر اصلا ویروسی برای ATM ها نیز داریم؟

- ویروس ATM متخصصی که قابلیت باز تولید از خود داشته باشد هنوز پیدا نشده است. اما این موضوع در مورد تروجان های مخصوص ATM قابل تامل است بطوری که فقط در ماه دسامبر ۲۰۱۳ چهار گونه جدید از تروجان های مخصوص ATM در دنیا شناسایی شد. Trojan.Ploutus1، Trojan.Ploutus2،

Dr.WEB®
www.dwav.ir

Trojan.Skimer19 و Trojan.PWS.OSMP.21 که این خود روند فزاینده تولید این نوع بدافزارها را از سال ۲۰۰۹ که اولین بدافزار مخصوص ATM ها کشف شد، نشان می دهد.

و اما خصوصیات خاص تروجان های مخصوص ATM چیست؟

- این نوع از بدافزارها از طریق کارتهای اعتباری ویژه (طراحی شده برای همین هدف) و یا دستگاههای تلفن همراه کنترل می شوند.
- رهگیری PIN کدهای وارد شده و رمزگشایی آنها " با استفاده از نرم افزارهای خود ATM که برای همین منظور تعبیه گردیده اند"
- هکرها با استفاده از این تروجان ها اطلاعات کارتهای بانکی را می دزدند، آنها اطلاعات دزدیده شده را بر روی کارتهای پلاستیکی خاصی که خود تولید کرده اند ذخیره و یا بر روی رسیدهای کاغذی خود دستگاه چاپ می کنند.
- مهاجمان با وارد کردن یک فرمان از طریق صفحه کلید ATM ها و یا ارسال یک SMS تعریف شده، اقدام به دریافت پول از ATM ها می کنند.

عملیات تعمیر و نگهداری ATM ها توسط افراد معتمد انجام می گیرد، پس چگونه نرم افزارهای مخرب وارد آنها می شوند؟

یک ATM می تواند به روشهای زیر آلوده شود:

- بصورت روتین از حافظه های قابل حمل جهت تعمیر و نگهداری ATM ها استفاده می شود، که اکثر اوقات این حافظه ها توسط پرسنل تعمیر و نگهداری برای کارهای شخصی نیز استفاده می شود.
- گاهی اوقات بدافزارها از طریق حافظه های قابل حمل تبهکارانی انتقال پیدا می کنند که به مناطق تعمیر دستگاههای ATM دسترسی دارند.
- توسط بدافزارهایی که در شبکه آلوده داخلی خود شرکت های ارایه دهنده خدمات ATM حضور دارند در صورتی که سیستم های Embeded به این شبکه های داخلی متصل باشند.
- با بهره برداری از آسیب پذیری در نرم افزار دستگاههای ATM.

حتی اگر یک ATM با هر یک از انواع بدافزارهای معمول آلوده گردد و تاثیری هم بر تراکنش های انجام گرفته ایجاد نگردد، تصاویری دیده شده و یا به اشتراک گذاشته در فضای مجازی از گزارشات خرابی ATM ها (مثل صفحات آبی BSOD ، هنگ کردن سیستم ها و ... که متاثر از فعالیت یک بدافزار در سیستم های کامپیوتری است) می تواند تاثیرات نامطلوبی بر شهرت کسب و کار شما داشته باشد. این مورد چیزی است که نه تنها ناخوشایند است بلکه پرهزینه نیز خواهد بود.

Dr.Web ATM Shield فقط یک آنتی ویروس نیست!

- Dr.Web ATM Shield بسته امنیتی کاملی می باشد که دارای ویژگیهای منحصر به فردی جهت جلوگیری از هر گونه نفوذ و آسیب رسانی به دستگاههای ATM می باشد، این ویژگیها شامل:
- نظاره گر فایل(File Monitoring)، اجرای نرم افزارهای مخرب بر روی دستگاههای خود پرداز را غیر ممکن می سازد.
- تکنولوژی Anti-Rootkit قادر به شناسایی بدافزارهای ناشناخته می باشد.
- ویژگی Office-Control سطح دسترسی به دایرکتوریها و وب سایتها را محدود می کند، از این طریق امکان ارسال اطلاعات به مجرمان و یا اتصال از طریق فرامین و یا کنترل سرور توسط بدافزار از بین خواهد رفت.
- با غیرفعال کردن دسترسی به حافظه های قابل حمل، امکان دسترسی بدافزارهای ناشناخته که از طریق حافظه های قابل حمل سعی در آلوده کردن ATM ها دارند، از بین خواهد رفت.
- نظاره گر HTPP به شما این اطمینان را می دهد که فقط برنامه های قابل اعتماد امکان دسترسی به اینترنت و یا شبکه داخلی را از طریق تعریف پورت های خاص دارند.

Dr.Web ATM Shield منحصرا جهت خنثی سازی بدافزارهای مخصوص ATM ها طراحی شده است.

چرا از یک راهکار جامع و تمام عیار مثل Dr,Web ATM-Shield به جای یک آنتی ویروس معمول جهت حفاظت از ATM ها استفاده می شود:

برای پاسخ به این سوال باید نگاهی به خصوصیات مخصوص سیستم های Embedded بیاندازیم که شامل:

- استفاده از RAM پایین و CPU نسبتا کند
- کارکرد بدون توقف
- دارای ویرایش خاصی از سیستم عامل به نام Embedded Edition

Dr.Web ATM Shield طوری خاص طراحی شده است که بر روی سیستم هایی با سخت افزار ضعیف کار کند.

Dr.WEB®
www.dwav.ir

برای اجرای Dr.Web ATM Shield به صورت نرمال، همان ۵۱۲ مگابایت رم مورد نیاز سیستم های Embedeed کافی است.

پایگاه داده ویروسی کم حجم و همچنین حجم پایین فایل های به روزرسانی ویروسها، این قابلیت را به این ویرایش خاص از آنتی ویروس های دکتر وب می دهد که برای بروزرسانی تمامی ایستگاههای کاری کمترین میزان از پهنای باند شبکه استفاده گردد.

Dr.Web ATM Shield تحت ویرایش Embedded سیستم عامل ها نیز کار می کند.

Dr.Web ATM Shield علاوه بر اینکه بر روی سیستم عامل های معمول مایکروسافت مانند: Windows® XP Professional ، Windows® Vista ، Windows® 7 و Windows® 8, مورد استفاده قرار می گیرد، امکان استفاده بر روی سیستم عامل های: Windows® XP Embedded ، Windows® 7 Embedded و Windows® 8 Embedded را دارد.

Dr.Web ATM Shield فقط یک آنتی ویروس نیست بلکه در بردارنده :

- فن آوری های نوین در به حداقل رساندن زمان بارگذاری و اسکن (چند وجهی با امکان تاخیر در اسکن فایل های که خوانده شده اند).
- عملیات پایدار در دستگاه های با سخت افزار ضعیف
- طراحی منحصر به فرد در موتور جستجوگر آنتی ویروس که این امکان را به آنتی ویروس های دکتر وب می دهند که بتوانند حتی ویروسهایی که به دیتابیس ویروسی اضافه نشده اند نیز، کشف و خنثی کند، حتی فایل های مخربی که تحت لوای هکرها مخفی شده اند.
- حفاظت قدرتمند از عملیات خود آنتی ویروس با استفاده از Self-Protection اختصاصی دکتر وب که مانع از اخلال در فرآیند خود آنتی ویروس می شود.

Dr.Web ATM Shield یک راه حل منحصر به فرد می باشد که طراحی شده است برای دستگاههای Embedded

بطور کلی بدافزارها به دنبال:

- به دنبال جمع آوری اطلاعات محرمانه ذخیره شده در رایانه ها می باشند.
- به دنبال تحمیل هزینه های خرابکارانه می باشند، هزینه هایی که به واسطه از بین رفتن اطلاعات ، نیاز به تعویض سیستم عامل و ... به آن مجموعه تحمیل می گردد.

Dr.WEB®
www.dwav.ir

- از کاربران جاسوسی کنند، اقدام به استراق سمع، دریافت اطلاعات مکانی و ... داشته باشند.
- به دنبال نفوذ به شبکه های دیگر مرتبط با شبکه آلوده می باشند.
- با گسترش آلودگی به شبکه های مختلف در پی بالا بردن میزان تخریب می باشند.
- گاها بدافزارها با آلوده کردن یک شبکه به دنبال برداشتن توجه از آلودگی در نقاط دیگر می باشند.
- بدافزارهای جدید با رمزگذاری بر روی اطلاعات، جهت رمزگشایی از شما اخاذی می کنند.
- و .....

و بدافزارهای مخصوص ATM به دنبال:

- سرقت اطلاعات پین کدهای ورودی دارندگان کارتهای بانکی می باشند.
- سرقت مبالغ ذخیره شده بر روی خود ATM ها می باشند.
- خرابکاری بر روی دستگاههای خودپرداز که نتیجه آن می تواند زیر سوال بردن امنیت خودپردازهای آن بانک خاص باشد.
- و .....

بیوگرافی از چند نمونه از بدافزارهای معروف ATM:

Trojan.Skimer.18: در دسامبر ۲۰۱۳ میلادی، این تروجان ATM های بیشماری را آلوده کرد. این تروجان تمامی اطلاعات کارت های بانکی، اعم از شماره کارت و شماره حساب را خوانده و در محل خاصی ذخیره می کرد. سپس پین کد واردی توسط دارنده کارت (با استفاده از صفحه کلید ATM) را رمزگشایی کرده و به اطلاعات ذخیره شده قبلی، جهت استفاده مهاجمان اضافه می کرد.

به منظور حفظ محرمانه بودن اطلاعات رد و بدل شده در دستگاه خودپرداز، تولید کنندگان این دستگاهها از یک تکنولوژی خاص جهت انتقال رمزگذاری شده پین کد وارد شده توسط کاربر به دستگاههای خودپرداز، بهره می

برند. پین کدها به هیچ وجه در یک فایل TXT و یا بر روی کارتهای بانکی و یا بر روی خود خودپرداز و یا حتی بر روی سرور بانکهایی که دارنده خودپرداز هستند ذخیره نمی شوند.

اما تروجان های خانواده Trojan.Skimer با دورزدن این حفاظت و با استفاده از نرم افزار رمزگشایی خود خودپرداز ها به اطلاعات پین کدهای ورودی دست پیدا می کنند.

Trojan.Skimerها از سال ۲۰۰۹ در حال فعالیت هستند

در حال حاضر بیش از ۲۵ نوع از این نوع تروجان ها در دیتابیس آنتی ویروس دکتر وب وجود دارند

Trojan.Plotus و Trojan. Plotus.2: این دو نوع تروجان که در دسامبر ۲۰۱۳ کشف گردیدند به آلوده کردن ATM ها به روش زیر پرداختند:

- این نوع بدافزار در زمانی که خودپردازها جهت تعمیرات باز می شدند، از طریق حافظه های قابل حمل وارد شده و خود را بر روی سیستم عامل خودپرداز نصب می کردند.
- به محض اینکه خودپرداز ریستارت می شد سرویس های مربوط به این نرم افزار مخرب فعال می شد و این امکان را به تولید کنندگان خود می داد که بتوانند انواع مختلف دستورات را بر روی ATM ها جهت نیل به اهداف خود اجرا کنند. یکی از این دستورات خالی کردن تمامی محتویات پول نقد درون ATMها بود. با اجرای این دستور تمامی محتویات پول نقد موجود بر روی ATM ها توسط مهاجمان برداشت می گردید.
- دستورات مهاجمان از دو طریق، استفاده از صفحه کلید خود ATM و یا ارسال از طریق SMS های خاص قابل اجراست.

امروزه امنیت یک سرویس بسیار مهم و حیاتی است :

امروزه نرم افزار ضد ویروس در تمامی فرآیندهای کسب و کار که شامل استفاد از رایانه، تبلت و ابزارهای هوشمند دیجیتالی دیگر در برنامه ریزی، مدیریت کسب و کار، حسابداری، تولید و ... می باشد مورد استفاده قرار می گیرد.یک ضد ویروس موثر، تضمین کننده عملکرد بی عیب و نقص سیستم های رایانه ای و ... در مواجه با نرم افرارهای مخرب و در مجموع باعث کاهش هزینه های مربوط تخریب ایجاد شده توسط بدافزاهاست.

پس این طور به نظر می رسد که داشتن یک آنتی ویروس به مسابه داشتن یک سرویس نگهداری می باشد که در مجموعه ها استفاده می گردد تا در نهایت از هزینه های گزاف تعمیر و بازسازی و گاهها جایگزینی سیستم های جدید جلوگیری گردد.

Dr.WEB®
www.dwav.ir

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 ۱۲۰ 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.

یکی از اهداف استراتژیک دکتر وب تولید نرم افزار های آنتی ویروسی می باشد که قابلیت مقابله با تمام تهدیدات بد افزاری را داشته باشند. همچنین از الویت های مهم دیگر این کمپانی توسعه تکنولوژی های جدید برای مقابله با تهدیدات بد افزاری جدید می باشد. این کمپانی طیف وسیعی از محصولات خود جهت مقابله با بدافزارها برای کاربران خانگی، شبکه های کوچک، متوسط، بزرگ، خیلی بزرگ و کاربران گوشی های هوشمند وغیره.... را به ارمغان آورده است.

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.

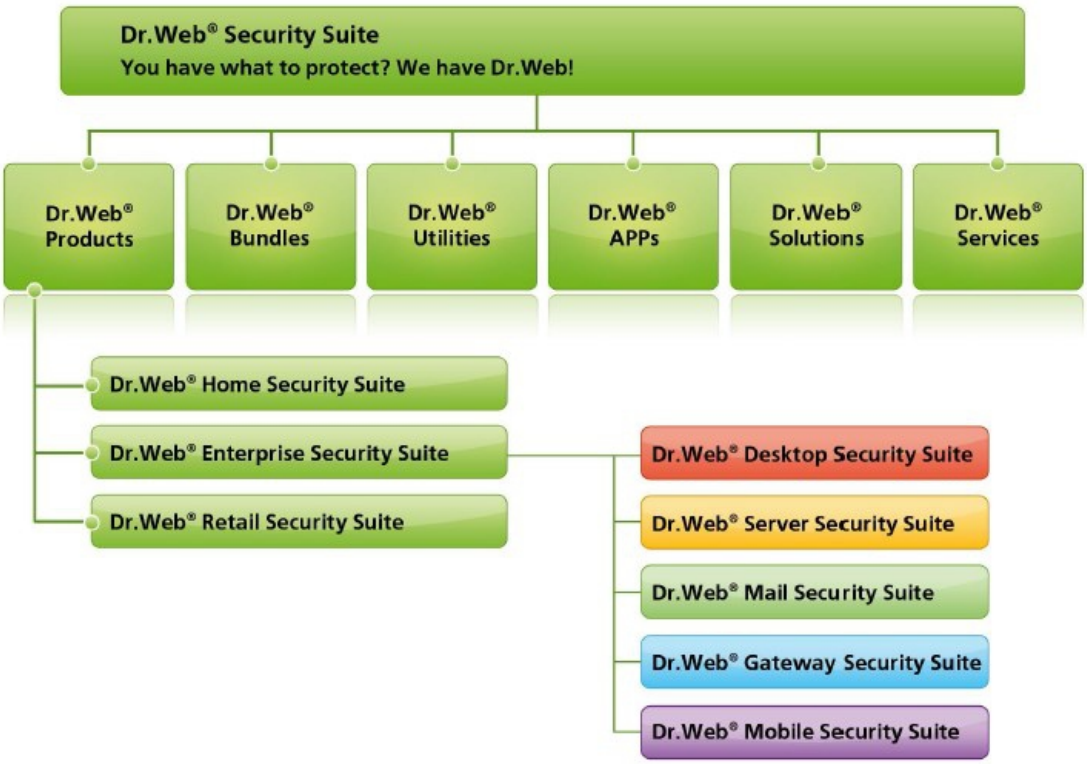
FLY-CODE: تکنولوژی منحصر به فرد کمپانی دکتر وب جهت رمزگشایی فایل هایی که توسط ویروس نویسان و هکرها **Encrypt** شده اند.

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 **Spam**ها و ویرایش خطرناکتری از **Spam**ها 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



چرا دکتر وب؟

- یکی از اولین آنتی ویروس های جهان
- دکتر وب دارای ۳۰ سال تجربه در زمینه توسعه نرم افزارهای ضد ویروس و تخصص گسترده است.
- دکتر وب فناوری های منحصر به فرد امنیت سایبری خود را توسعه می دهد که به طور مداوم بهبود می یابند تا قدرتمند، ایمن و مرتبط باشند، همچنین آزمایشگاه ویروس خود را توسعه می دهد.
- دکتر وب سطح بالایی از حفاظت را برای همه گروه های کاربر – بخش شرکتی، موسسات دولتی و کاربران خانگی ارائه می دهد.
- محصولات Dr.Web از تکنولوژی ها و فرآیندهای بسیار پیچیده ای استفاده می کنند و در عین حال استفاده از آن ها آسان است و با اعلان های غیر ضروری (پیچیده – داخلی، ساده – خارجی)مزاحم کاربران نمی شوند.
- دکتر وب قیمت های رقابتی برای همه دارد و پیشنهادهای ویژه ای برای موسسات تجاری کوچک، آموزشی و پزشکی، و برای شرکت هایی که از فروشندگان دیگر به محصولات Dr.Web مهاجرت می کنند را دارا می باشد.

Dr.WEB®
www.dwav.ir

- دکتر وب پشتیبانی آنلاین و کارآمد از کاربران و شرکای خود را مهیا کرده است.
- دکتر وب سیستم به روز رسانی جهانی را دارد که ارائه سریع و قابل اطمینان بروزرسانی ها به کاربران در سراسر جهان را بر عهده دارد.
- دکتر وب دیتابیس بی نظیری از بدافزارها دارا می باشد (تنها در یک روز، لابراتوار ویروس یاب دکتر وب، بیش از یک میلیون نمونه بالقوه مخرب را بررسی و به دیتابیس خود اضافه می کند.)
- دکتر وب دارای فناوری های حفاظتی پیشگیرانه منحصر به فردی می باشد که وظیفه محافظت از رایانه ها در مقابل جدیدترین و پیشرفته ترین برنامه های مخرب طراحی شده برای دور زدن شناسایی توسط امضای سنتی را در اختیار دارد. (بررسی و تحلیل اکتشافی)
- دکتر وب از جمله اولین شرکت های ارائه دهنده سیستم مدیریت متمرکز و مناسب کل شبکه تحت وب برای مشتریان شرکتی و دولتی می باشد.
- محصولات دکتر وب نه تنها از تهدیدات پیش گیری می کنند، بلکه در صورت پیدا شدن، آن ها را درمان (Cure) می کنند.
- دکتر وب مشتریان خود در برابر انواع تهدیدات مدرن محافظت می کند، مخاطراتی چون ماینرها، جاسوس افزارها، کلاه برداری های شبکه ای، فیشینگ، دسترسی غیرمجاز، باج افزار رمزگذاری،حملات هدفمند، سرقت اطلاعات محرمانه
- راه حل های Dr.Web توسط کاربران ۱۲۰ کشور انتخاب شده اند.

لیستی از بانکهایی که از ATM-Shield استفاده می کنند:

لیست این بانکها جز اطلاعات محرمانه دکتر وب می باشد. فقط بطور مختصر می توان به ۲ مورد زیر اشاره کرد:

- بانک Sberbank روسیه با بیش ۱۰۰ هزار دستگاه (شامل تمامی ATM ها و سیستم های دیگر این بانک می باشد)، این بانک بزرگترین بانک روسیه و سومین بانک بزرگ اروپا می باشد.
- بانک Russian Agricultural Bank با بیش از ۲۴ هزار دستگاه (شامل تمامی ATM ها و سیستم های دیگر این بانک می باشد)

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.