

رشد عجم لولسی لفرج

ویدر ویدر

نویسنده: ابراهیم آرام

استفاده از این کتاب به صورت رایگان میباشد

فهرست مطالب

۳	مقدمه
۴	ویروس کامپیوتری چیست؟
۶	خانه ویروس
۷	ویروسها شناخته شده
۷	انواع ویروسها
۸	انواع ویروس ها نسل جدید
۹	عملکرد ویروس
۱۲	ویروسهای ناشناخته:
۱۳	ساختار عمومی ویروسها و ضد ویروسها:
۱۳	تکنیک های آشکارسازی ویروس ها:
۱۶	پاکسازی ویروس ها
۱۵	روش های پاکسازی
۱۸	ابزارهایی برای افزایش امنیت و سرعت کامپیوتر

مقدمه

بیش از سه دهه از ساخت اولین ویروس کامپیوتری توسط فرد کوهن می گذرد. شاید در ابتدا کوهن هرگز تصور نمی کرد که روزی اختراع او به صورت یک فاجعه کامپیوتری در آمده و دنیای کامپیوتر را مورد تهدید قرار دهد (متأسفانه بسیاری از مشکلات بزرگ تکنولوژی همین گونه آغاز می شود). کوهن صرفاً به عنوان یک پروژه دانشجویی، برنامه ای را ساخت که می توانست خود را تکثیر کرده و انگل وار به دیگر برنامه ها بچسبد و نوعی تغییر در آنها بوجود آورد. با طرح ویژگیهای این نوع برنامه ها در مقالات و سخنرانیها بتدریج این مسئله توجه عده زیادی از برنامه نویسان را به خود جلب کرده و رفته رفته مسئله تولید ویروسهای کامپیوتری نضج گرفت. علت نامگذاری ویروس بر روی اینگونه برنامه ها، تشابه زیاد آنها با ویروسهای بیولوژیکی بود. چرا که ویروسهای کامپیوتری مانند ویروسهای بیولوژیکی بطور ناگهانی تکثیر می شوند و در حالی که ممکن است بر روی یک دیسک وجود داشته باشند تا زمانی که شرایط مناسب نباشند، فعال نخواهد بود. امروزه مسئله ویروسهای کامپیوتری به یک معضل بسیار جدی تبدیل شده است. حوزه عملکرد ویروسها، انواع کامپیوترها و سیستم های عامل را در بر می گیرد. و هر روز چندین ویروس جدید تولید شده و در فضای کامپیوتر جهانی رها می شود. بدون اینکه بتوان فرد سازنده آن را شناسایی و مواخذه کرد. برای یک کاربر معمولی PC ممکن است حداکثر ضرر ناشی از یک ویروس خطرناک، ناپدید کردن اطلاعات و برنامه های مهم موجود بر روی کامپیوتری باشد در حالی که ضرر یک ویروس مخرب بر روی شبکه ارتباطی ترمینالهای بانک های یک کشور ممکن است موجب تغییر و یا حذف اطلاعات مالی شرکتها و افراد صاحب حساب شده و خسارات مالی سنگینی را ببار آورد، آنچنان که تا کنون نیز مواردی از این دست، از رسانه های گروهی اعلام شده است. بنابراین اثر تخریب کنندگی ویروسها مرز خاصی نمی شناسد و هر جا که اثری از یک فعالیت کامپیوتری نرم افزاری وجود دارد، ممکن است ویروسها نیز حضور داشته باشند.

بدیهی است رشد سرطان گونه ویروسها متخصصین امر را بر آن می دارد که برنامه هایی برای نابودی آنها تهیه کنند. تا کنون برنامه های ضد ویروس زیادی ساخته شده است که هر یک گروهی از ویروسها را شناسایی و آنها حذف می کنند.

این برنامه ها هر يك ویژگیهاي خاصی داشته و براحتي نمي توان از آنها را به عنوان بهترین ضد ویروس معرفی کرد . متأسفانه به دلیل کمبود منابع ، عموم کاربران داخل کشور از کارايي و نحوه عملکرد برنامه هاي اطلاع کافي نداشته و لذا صرفاً از آنها به شکل ساده و بدون تنظیمات خاص استفاده کرده و از این رو در بسياري موارد مشکلات ناشي از وجود ویروسها به طور قطعي حل نمي شوند .

ویروس کامپیوتري چیست ؟

ویروس کامپیوتري برنامه اي است که مي تواند داده هاي موجود روي دیسک و حافظه RAM را معیوب نموده و در نتیجه از اجرای برنامه ها بطور صحیح جلوگیری به عمل مي آورد . بعضي از ویروسها ي کامپیوتري ضعیف بوده و فقط با نمایش پیغام خاصی خود را نشان داده و صدمه اي به دیسک وارد نمي سازند ولي نوع دیگر ویروس ها ممکن است به حد خطرناک باشند که کل اطلاعات دیسک را از بین برده و کاربر را مجبور به **format** نمودن دیسک مزبور کنند . ویروسها کامپیوتري به صورت مخفیانه و از طریق برنامه هايی که توسط دیسک هاي دیگر یا مودم به کامپیوترتان کپی مي کنید ، وارد کامپیوترتان مي شوند . این ویروسهاي کامپیوتري ممکن است مدتها در کامپیوتر شما موجود بوده و فقط به تکثیر خود پرداخته و هیچ صدمه اي وارد ننمایند و در ساعت و تاریخ و یا هنگام اجرای برنامه خاصی فعال شده و تمام کپی هاي خود را نیز فعال کنند که بستگی به ویروس مورد نظر ، صدمات غیرقابل جبراني را وارد مي کنند . ویروس ها اغلب روي فایل هاي اجرایی دیسک عمل نموده و آنها را معیوب مي کنند . ویروس هاي کامپیوتري به صورت برنامه جداگانه اي وجود ندارند بلکه خود را به فایل ها و برنامه هاي دیگر چسبانده و از کامپیوتري به کامپیوتر دیگر منتقل مي شوند .

تا کنون بیش از ۲۰۰۰۰ ویروس شناخته شده اند و متخصصین و کارشناسان پس از شناسایی هر يك از آنها ، نام خاصی را به آنها اطلاق کرده اند .

برای محافظت و سالم نگه داشتن دیسک ، کاربران بایستی از برنامه هاي موجود به طور مداوم استفاده نمایند که یکی از آنها و قویترین شان برنامه **Disk Monitor** است البته برنامه هاي دیگری در سیستم عامل **Dos** و دیگر برنامه هاي سودمند نیز تعبیه شده اند که عبارتند

از Vasfe و سنسورهاي مختلف برنامه Norton system Doctor در Un تحت ويندوز 95 و.....

اگر برنامه هاي حفاظت از ديسك هميشه استفاده نماييد، امكان ورود و پروس هاي كامپيوتري به كامپيوترتان كم شده و در نتيجه سيستم شما سالم خواهد ماند .
در انتها بطور خلاصه مي توان گفت : وپروس برنامه مخفي و كوچكي است كه باعث آلوده شدن برنامه هاي ديگرمي شود و مي تواند داده ها را دستكاري و ياتخريب نموده ، سرعت سيستم را کاهش داده باعث اغتشاش و عدم كارايي كامپيوتر شود .
مهمترين خصوصيت وپروس قدرت تكثير آن است ، وپروسها براي تكثير نياز به يك برنامه اجرايي دارند يعني بيشتروپروسها در فايلهاي اجرايي جاي مي گيرند و آنها را آلوده مي كنند .
كمتر وپروسي پيدا مي شود كه بتواند نسخه هاي اجرايي جاي مي گيرند و آنها را آلوده مي كنند و كمتر وپروسي پيدا مي شوند كه ابتدا نسخه هاي اجرايي از خود را در برنامه هاي ديگر قرار دهد . برنامه آلوده به وپروس مي تواند هر برنامه سيستمي با كاربردي باشد كه شرايط مورد نياز براي پذيرش وپروس را داشته باشد . برنامه آلوده قادر است برنامه هاي ديگر را آلوده كند .

خانه وپروس

ويروس هم مانند هر برنامه كامپيوتري نياز به محلي براي ذخيره خود دارد منتهي اين محل بايد به گونه اي باشد كه وپروسها را به وصول اهداف شوم خود نزديك تر كند . همانطور كه مي دانيد اكثر وپروسها به طور انگل مانندي به فايلهاي اجرايي مي چسبند و آنها را آلوده مي كنند. اصولاً در برخورد با وپروسها ، فايلهاي اجرايي و غير اجرايي تقسيم مي شوند عموم وپروسها در فايلهاي اجرايي جاي گرفته و آنها را آلوده مي كنند و واقعاً كمتر وپروسي هست كه در يك فايل غير اجرايي جاي بگيرد و بتواند از طريق آن تكثير پيدا كند. در ذيل، فهرست پسوندهاي رايج فايلهاي اجرايي ارائه شده است و اكثر نرم افزارهاي ضد وپروس در حالت عادي(بدون تنظيم خاص) تنها همين فايلها را وپروس ياب مي كنند(البته دربرخي برنامه هاي ضد وپروس ممكن است برخي پسوندها حذف و اضافه شوند).
EXE-COM-SYS-BIN-

OVL-DLL-SCR

بنابراين يكي از اصلي ترين خانه هاي وپروس فايلها آلوده به وپروس هستند. از طرف برخي وپروسها علاقه خاصي به قطاع بوت (Boot Sector) و جدول بخش بندي ديسك Master

(Boot record یا partition) دارند . قطاع بوت واحد راه اندازي Dos است که در قطاع شماره صفر سخت دیسک یا فلاپی دیسک قرار دارد و جدول بخش بندی شامل اطلاعات تقسیم بندی سخت دیسک است که در آن نیز در قطاع شماره صفر سخت دیسک قرار دارد . اینگونه ویروسها با قرار گرفتن در یکی از این دو محل به محض روشن شدن کامپیوتر می توانند به راحتی و به دلخواه کنترل تمامی برنامه هایی که اجرا می شوند را در دست بگیرند و حتی به گونه ای عمل کنند که شماتا مدتها متوجه به حضور آنها نشوید!

محل دیگر ویروسها که البته موقتی است در حافظه RAM کامپیوتر می باشد . به محض روشن کردن کامپیوتر و اجرای یک برنامه آلوده به ویروس و یا دسترسی به یک دیسک تا قطاع بوت و جدول بخش بندی آلوده ، ویروس همراه آن در حافظه جا می گیرد و برخی از آنها تا زمان خاموش کردن کامپیوتر همان جا مانده و فایلهاي دیگر را آلوده می کنند ولو آنکه شما حتی برنامه آلوده را حذف کرده و فلاپی دیسک آلوده را نیز از دیسک گردان مربوط بیرون بیاورند .

ویروسها شناخته شده

ویروس شناخته شده ویروسی است که قبلا توسط متخصصین کشف شده و مورد تجزیه و تحلیل قرار گرفته است .

بدین ترتیب نامی مانند Stoned یا Michelangelo برای آن انتخاب شده است . همچنین امضایی (Signature) دارد که یک سری بایت منحصر به فرد در برنامه ویروس بوده و در شناسایی آن کمک می کند .

همچنین ویروس ممکن است چند نژاد شناخته شده داشته باشد (یعنی گونه هایی در برنامه های اصلی آنها تفاوت جزئی وجود دارد).

تا کنون بیش از ۱۰۰۰۰ ویروس شناخته شده است . بسیاری از آنها مدتی است دیده نشده اند و احتمالاً معدوم شده اند ، اما با وجود این هیچ راهی برای پیش بینی زمان و محل ظهور مجدد آنها وجود ندارند .

انواع ویروسها

ویروس های کامپیوتری بسته به نوع تاثیر آنها به سه قسمت تقسیم می شوند :

الف) Boot Sector

Boot Sector بخشی از دیسک سخت شماست که به کنترل چگونگی آغاز سیستم عامل هنگام روشن کردن کامپیوتر می پردازد یک ویروس Boot Sector، Boot Sector اصلی دیسک را برداشته و خود جانشین آن می شود و ویروس را به حافظه انتقال می دهد و حضور ویروس در حافظه به مفهوم پخش شدن آن در دیسک های دیگر می باشد .

ب) File infector

ویروس تخریب کننده فایل، ویروس را برای فایلی که برنامه آن اجرا شده، اضافه می کند این اضافه شدن به گونه ای است که در هنگام اجرای برنامه ویروس فعال شده و فعالیت آن به مفهوم پخش آن در سایر فایل های برنامه نیز می شود .

پ) Trogen Hourse

ویروس Trogen Hourse به عنوان برنامه مخرب کامپیوتری می باشد . بدین ترتیب که فایل ها و دیسک ها را خراب کرده و قدرت آن سایر انواع ویروس ، بسیار بیشتر می باشد . فایل های دیسک ها را خراب کرده و قدرت آن از سایر انواع ویروس ، بسیار بیشتر می باشد . فایل ها یا دیسک هایی که با ویروس Trogen Hourse تخریب شده اند . ممکن است قابل بازیابی نباشند .

انواع ویروس ها نسل جدید

۱- ویروس های مقیم در حافظه (Memory Resident Virus)

برنامه مقیم در حافظه، برنامه ای است که پس از اتمام شدن اجرا ، جای خود را در حافظه از دست نمی دهد . بیشتر ویروسها پس از فعال شدن مانند برنامه های مقیم در حافظه عمل می کنند و در حافظه باقی می مانند .

۲- ویروس های استتاری یا نهان (Stealth)

این ویروسها با روشهای خاص و بدون تغییر وضعیت ظاهری، عملیات خود را انجام می دهند و به روشهای گوناگون ردپای خود را مخفی می کنند تا شناخته نشوند . یعنی فایل های آلوده به این ویروسها طوری نشان داده می شوند که فکر کنیم سالم هستند .

۳- ویروسهای رمزی (Encypting Virus)

این ویروسها برای جلوگیری از شناسایی خود را بصورت های مختلفی رمز می کنند .
ویروس در ۱۲۶۰ یا (Stealth) به صورت کد بوده و به طور تصادفی تغییراتی در کد
بندی خود ایجاد می کند تا روال شناسایی ویروسها را خنثی و بی اثر کند .
ویروس ایرانی ((آریا)) به صورت کد شده بر روی فایل های آلوده قرار می گیرد و در ابتدای
ویروس ، یک روال رمزگشا ویروس وجود دارد .

۴- ویروسهای چند شکلی یا هزار چهره (Polymorphic Virus)

کشف این ویروسها از همه مشکل تر است زیرا این ویروسها پس از هر بار آلوده سازی ،
ساختار داخلی خود را تغییر می دهند و یا شیوه های خود رمز استفاده می کنند . این
ویروسها هنگام تولید مثل شکل خود را تغییر و تکامل می دهند . برخی از آنها می توانند
رمز خود را به طور تصادفی تغییر دهند ، بدون آنکه در وظیفه آنها خللی وارد شود .

۵- ویروسهای انفجاری (Triggerdd event Virus)

این ویروسها بخشی از عملیات تخریب خود را در ساعت و یا در تاریخ خاصی انجام می
دهند ولی تکثیر و آلوده سازی فایل ها در تمام مدت فعال بودن ویروس در حافظه و اجرای
برنامه های دیگر صورت می گیرد .

به عنوان مثال ویروس ایرانی در TOPGUN چنانچه تاریخ سیستم برابر با روز دوم ماه
باشد ، ۶۴ بیت اول Ram CMOS را پاک می کند .

۶- ویروس خود شناخته (Self Modify Virus)

ویروسهایی که خود را با نسخه های قبلی خود در سیستم مطابقت می دهند و نسخه های قبلی
خود را Update می کنند .

۷- ویروسهای چند قسمتی (Multi partite Virus)

این نوع ویروسها دارای چندین قسمت هستند که هر کدام کار خاصی را انجام می دهد.
مانند برنامه ای که از چندین روال تشکیل شده است .

عملکرد ویروس

ویروسها عملکرد مختلفی دارند و آنچه در مورد همه آنها اشتراک دارد، عملکرد منفی آنها می
باشد. به این معنی که ویروسها عموماً در صدد ایجاد مزاحمت های کامپیوتری هستند. این
مزاحمتها گستردگی وسیعی دارند و به راحتی قابل تعریف نیستند . اما به طو کلی می توان
عملکرد ویروس ها را به صورت زیر تقسیم بندی کرد :

- ایجاد تاخیر وقفه و در حین عملیات سیستم اعم از اجرای برنامه ها و یا راه اندازی کامپیوتر و ...

- تخریب یا حذف برنامه ها و اطلاعات بخشهای مختلف دیسکها و یا حتی Format کردن دیسکها

- اشتغال حافظه و تکثیر در حافظه به نحوی که در حافظه جایی برای اجرای دیگر برنامه ها نمی ماند .

مزاحمتیهای فوق ممکن است به محض فعال شدن ویروس (یعنی قرار گرفتن ویروس در حافظه از طریق اجرای یک برنامه کاربردی آلوده و یا در یک تاریخ و زمان خاص و یا حتی با اجرای یک برنامه کاربردی خاص انجام شود).

علائم موجود در ویروس

علائم زیر معمولاً به وسیله ویروسها ایجاد می شوند . اما ممکن است در اثر عوامل غیر ویروسی نیز ظاهر شود .

(۱) قفل کردن و دادن پیامهای غیر عادی : بعضی از ویروس ها به محض ورود به حافظه، خودشان را چندین بار تکثیر می کنند این کار موجب میشود سیستم بسیار کند شود و گاهی نیز قفل کند . بعضی از ویروسها نیز پس از آلودگی پیامهای گوناگونی به نمایش می گذارند .

(۲) دادن پیامهای غیر عادی : پاره ای از ویروسها در مراحل از آلودگی خود پیامهایی را نمایش می دهند که نشانه آلودگی سیستم است .

(۳) اختلال در کار Printer: یکی از مواردی که نشان دهنده آلودگی احتمالی به ویروس است اختلال در کار چاپگر است . اعمالی مانند توقف عمل چاپ و عمل format موقع چاپ یا .. می تواند نشان دهنده آلودگی سیستم باشد .

(۴) صدای غیر عادی Speaker: برخی از ویروسها با ایجاد صداهای غیر عادی یا پخش یک موزیک و... آلودگی سیستم را اعلام می کنند. Atiavri باعث پخش شدن صدای هیس از بلندگوی کامپیوتر می شود .

(۵) کاهش سرعت سیستم : در صورتی که زمان بار کردن برخی از برنامه ها به نحوه قابل ملاحظه ای افزایش یابد و یا مدت زمان راه اندازی سیستم ، وقتی که از روی

HARD DISK راه اندازي مي شود، افزايش يابد، و... نشان دهنده احتمال آلودگي به ويروس است .

(۶) وقتي که صفحه کلید را فشار مي دهد دستوري را وارد مي کنيد پيامي مبني بر غلط بودن شکل دستور دريافت مي کنيد و علت آن ممکن است اين باشد که اگرکلید B را فشار مي دهيد علامت کيد مجاورش ، يعني N روي صفحه نمايش ظاهر مي شود، در اين صورت احتمالاً کامپيوتر آلوده به ويروس است .

(۷) خرابي **DISK**: ممکن است که احتمالاً بخشي ازديسک يا تمام آنها ازبين بروند و يا ديسک **Format** شود .

(۸) کاهش حجم حافظه : با وجودي که هيچ برنامه مقيم جديدي بر روي سيستم نصب نشده باشد ، ظرفيت حافظه کاهش يافته است .

(۹) تغيير در اندازه فايل ها : طول برنامه ها ي قابل اجرا ، يعني فايل هاي **EXE, CIM** به اندازه ۴۰۰ تا ۶۰۰۰ بابت تغيير مي کنند .

(۱۰) اختلال در صفحه نمايش : هنگام اجراي يك فايل يا کاراکتر ها و پيام هاي غير معمول روي صفحه نمايش ظاهر ميشود (ممکن است برخي از اين پيغام ها نام ويروس فعال در حافظه باشد).

(۱۱) اختلال در **SETUP**: برخي از ويروسها ، اطلاعات موجود در **Setup** کامپيوتر را از بين مي برند .

(۱۲) راه اندازي مجدد سيستم (**Restart**) : برخي از ويروسها موقع استفاده از برنامه باعث **RESTART** شدن سيستم مي شود .

(۱۳) خواص فايلهاي اجراي تغيير مي کند .

(۱۴) در حين اجراي يك برنامه ، بخشي از عمليات برنامه به طور عادي انجام نمي شود.

(۱۵) هنگام کار در محيط هاي گرافيكي تصاوير بر هم مي ريزند .

(۱۶) هنگام اجراي فايل ها پيغام **File is Damaged** يا **File is curropted** ظاهر مي شود .

(۱۷) امکان دسترسي به يکي ازديسک گردانها از بين مي رود .

۱۸) هنگام اجرای يك برنامه سیستم قفل می کند و گاهی فشردن کلیدهای ALT+DEL+CTRL نیز نمی تواند سیستم راه اندازی کند .

ویپر وین

ویروس‌های ناشناخته

شاید یافتن ویروس‌های ناشناخته مهمتر از ویروس‌های شناخته شده باشد، زیرا ویروس‌های جدید تا قبل از کشف شدن، مورد تجزیه و تحلیل قرار گرفتن، نامگذاری و توزیع ویروس‌یابها، مدتی ناشناخته می‌مانند.

ویروس‌یابها با جستجوی فایل‌های برنامه‌ای به دنبال تغییراتی در آنها احتمال آلودگی ویروسی را نشان می‌دهند، ویروس‌های ناشناخته را پیدا می‌کنند. بیشتر فایل‌های برنامه‌ای پس از نصب تغییر نمی‌کنند، بنابراین وجود هر گونه تغییری در آنها می‌تواند نشانگر آلودگی ویروسی باشد.

اولین باری که ویروس‌یابها میکروسافت را در درایوی مورد استفاده قرار دهید، فایلی به نام **CHKLIST.MS** در هر فهرستی ایجاد می‌کند و اندازه، صفات، تاریخ و ساعت تمام فایل‌های برنامه‌ای فهرست مزبور را در آن فایل ثبت می‌کند.

اولین باری که مقدار کنترلی (**Check sum**) یعنی مقدار منحصر به فردی که از محاسبه محتویات فایل بدست می‌آورد را نیز ثبت می‌کند. بدین ترتیب اگر محتویات فایل تغییر کند، مقدار کنترلی آن نیز تغییر می‌کند و ویروس‌یاب از روی آن می‌فهمد که فایل تغییر کرده است، حتی اگر اندازه، صفات و تاریخ و سرعت آن ثابت مانده است.

اگر هنگام ثبت داده‌ها **CHKLIST.MS** ویروس ناشناخته‌ای در سیستم وجود داشته باشد شناسایی نخواهد شد. خوشبختانه **VSAFE** می‌تواند با نظارت بر سیستم، جلوی فعالیت مخرب ویروس‌ها را بگیرد.

پس از تشکیل فایل‌های **CHKLIST.MS**، هر بار که عملیات ویروس‌یابی انجام شود، ویروس‌یابی داده‌های ثبت شده را با فایل‌های برنامه‌ای مقایسه می‌کند. هر گونه تفاوتی در آنها باعث می‌شود ویروس‌یاب داده‌های ثبت شده را با فایل‌های برنامه‌ای مقایسه می‌کند. وجود هر گونه تفاوتی در آنها باعث می‌شود که ویروس‌یاب امکان وجود یک ویروس ناشناخته را گزارش دهد که در این صورت باید فکری به حال سیستم بکنید. در این حالت می‌توانید به برنامه‌ی ویروس‌یاب بگویید که از تغییر صرف نظر کند، فایل **CHKLIST.MS** را با داده‌های جدید نوسازی کند، فایل آلوده را پاک کند، یا عملیات ویروس‌یابی را متوقف سازد.

ساختار عمومی ویروسها و ضد ویروسها :

سیستم عامل دارای امکاناتی است که به ویروس نویسان اجازه می دهد با استفاده از آنها کنترل سیستم را در دست بگیرید، خود را مخفی کنند ، در حافظه مقیم شوند و ویروسهای کامپیوتری با استفاده از این امکانات از روشهای مدرن و پیچیده ای برای آلوده سازی ، مخفی سازی خود و تخریب اطلاعات استفاده می کنند . یکی از این ویروسها One half است . اولین باری که برنامه آلوده به ویروس ، بر روی یک کامپیوتر سالم و غیر آلوده اجرا شود partition Table را آلوده کند . بعد از آن هر وقت که سیستم با hard disk آلوده راه اندازی می شود ، ویروس کنترل عملیات ورودی /خروجی را در دست می گیرد . در صورتی که اطلاعات partition Table به کلی از بین برود، بدیهی است که سیستم دیگر Boot نمی شود . وقتی ویروس partition Table را آلوده بعد از آن در هر بار روشن شدن سیستم دور سیلندر از انتهای hard disk راکد کرده و به آن ترتیب بعد از مدتی ، حجم زیادی از اطلاعات تخریب می شوند .

تکنیک های آشکار سازی ویروس ها :

یکی از اولین نرم افزارهایی که بر روی کامپیوتر نصب می شوند آخرین نسخه نرم افزارهای ضد ویروس است . هیچ کدام از ضد ویروس های زرنگ و باهوش اغلب می توانند آنها را فریب دهند ولی آنها احتمال آلودگی را به حداقل می رسانند و در صورت آسیب دیدن ، کار درمان را ، راحت تر می کنند .

۱- بررسی علامت مشخصه ویروس بانگ الگوی ویروس V irus Pattern database ساده ترین روش تشخیص ویروس ها نگاه کردن به برنامه آنهاست و بررسی پیام های موجود در آنهاست . راه دیگر گشتن به دنبال بایت های خاصی ، که مشخص کننده ویروس های خاص است ، می باشد . که به آنها رمز مشخصه (Signature) یا امضاء ویروس می گویند . بنابراین در این روش همه فایل ها جستجو می شوند تا علامت مشخص شده ویروس

را پیدا کنند در Boot Sector آلوده به ویروس ((مغز پاکستانی)) رشته های Virus shoe وجود دارد که ممکن است از این علامت برای شناسایی این ویروس استفاده کرد . در انتهای کلیه فایل‌های آلوده به ویروس 1,2 Mixer می توان رشته حرفی mixl را پیدا کرد . بنابراین در بانگ الگو می توان از این علامت ، برای شناسایی این ویروس استفاده کرد .

۲- بررسی تجربی یا مکاشفه ای (Heuristic Scan)

در این روش ضد ویروس به دنبال رفتار های ویروس می گردد مثلاً به دنبال قطعاتی که به صورت رمز بوده و خطر آفرین هستند می گردد . مانند کپی کردن فایل بر روی خودش ، یا به یک فایل دیگر ، یا حذف کردن خودش بدون هیچ اختطاری به کاربر ، در این روش ممکن است هشدار اشتباه نیز داده شود و نسبت به روش بانگ الگوی ویروس ، دارای دقت کمتری است اما برای تشخیص ویروس های جدید که رمز مشخصه آنها هنوز در نرم افزار های ضد ویروس وجود ندارد بسیار خوب عمل می کند .

۳- بررسی درستی مجموع (integrity Checking)

ویروس معمولاً اندازه تاریخ یا مشخصات فایل اجرایی را تغییر می دهد . بنابراین می توان با ضبط قبلی و قایسه آن با وضعیت فعلی (CHKLIST.MS) از تغییرات احتمالی که بوسیله ویروس ایجاد می شود آگاه شد. اگر ویروس جدید باشد و ضد ویروس آن در دسترس نباشد با این روش می توان به شناسایی ویروس های جدید نیز پرداخت .

۴- بررسی رمز ژنریک :

در این روش به جای جستجوی رمز مشخصه ویروس های خاص ، به دنبال الگوهایی مانند دستور العمل های پرش نامناسب می گردد که به برنامه های ویروسی شباهت دارد . این روش برای کشف ویروس های هزار چهره که می توانند رمز خودشان را هر بار که فایل جدیدی را آلوده می کنند ، تغییر دهند ، بسیار کارا و موثر است .

۵- رفتار نگرها :

به رفتار های غیر عادی و طبیعی داخل کامپیوتر توجه دارند . مانند فایلی که روی Boot Sector می نویسد یا HARD DISK را Format می کند . وقتی چنین اتفاقی می خواهد انجام شود ضد ویروس کاربر را آگاه می کند .

۶- بررسی فازی :

اساس این روش بر منطق فازی استوار است . با این روش می توان دقیقاً به وجود ویروسهای هم شکل و هزار چهره پی برد . ضد ویروسها یی که بر اساس بررسی فازی کار می کنند در

تشخیص ویروسها بسیار خوب عمل می کنند . اما عملیات جستجو را آهسته انجام می دهند و بروز اشتباه در آنها بسیار اندک است. ضد ویروس IBM بر این اساس کار می کند و بسیاری از ویروسها را تشخیص و نابود می کند .

روشهای کلی مبارزه :

جمله معروفی در علم پزشکی مطرح شده است که پیشگیری از بیماری به مراتب آسانتر از درمان آن است این سخن تا حدود زیادی در مورد ویروس های کامپیوتری نیز صدق می کند . به این معنی که در بسیاری از مواقع جلوگیری از ورود ویروس به کامپیوتر ساده تر از رفع آن است .

به طور کلی راههای اصلی برای مبارزه با ویروسها به دو دسته زیر تقسیم می شوند .

(۱) شناسایی ویروس ها و جلوگیری از ورود آنها به کامپیوتر

(۲) از بین بردن ویروسی که به سیستم وارد شده و در صورت ایجاد اختلال ،

بازگرداندن وضعیت سیستم کامپیوتر و برنامه های آن به حالت عادی

اجرای دو بند فوق مستلزم شناخت چهره واقعی ویروس ، یعنی کد مبدا آنها است هر روز ویروس های جدیدی با یک کد مبدا آنها شناخته شده و تا برنامه پاک کننده تهیه می شود ، هزاران برنامه در معرض حمله و تخریب این ویروس ها قرار گرفته اند .

شرکتها ی تولید کننده نرم افزار های ضد ویروس زمانی میتوانند برنامه های ضد ویروس خود را کامل تر و فراگیر تر کنند که حداقل به ویروس جدید ساخته شده توسط دیگران دسترسی پیدا کنند تا بتوانند با شناخت کد مبدا و نحوه کار آنها برنامه های ضد ویروسی مناسب را طراحی نمایند و همه این مراحل بسیار وقت گیر خواهد بود .

بنابراین اگر صرفاً به شناخت دقیق ویروس ها اکتفا کنید هرگز روش مطمئن و فراگیری را نخواهید یافت و هیچ یک از برنامه های ضد ویروس فعلی ادعای شناخت همه ویروسها را ندارند .

البته این به معنای عدم توجه به اثر فوق العاده روشهای مبارزه ای که مبتنی بر شناخت دقیق ویروس است . نخواهند بود . بلکه منظور آن است که اگر همین امروز کامپیوتر شما دچار ویروس مخربی بشود که هیچ ویروس یابی نتواند آن را بشناسد . آنگاه باید ضرر ناشی

format دیسک سخت ، از بین رفتن برنامه هایی که ساعتها مشغول طراحی و ویرایش آن بوده اید و یا حداقل ضرر اتلاف وقت خویش را تحمل کنید .

برای رفع این مشکل از دو نکته غیر قابل اجتناب زیر استفاده شده است :

۱- ویروسها هنگام ورود به سیستم ناچار باید روی حافظه ، برنامه و یا ناحیه سیستمی دیسک قرار گیرند و لذا معمولا در سیستم يك حالت نوشتن اطلاعات به وجود آید که این عمل (صرف نظر از نوع اطلاعات) تا حدودی قابل کنترل است .

۲- وقتی ویروسی بر روی ناحیه سیستمی دیسک و یا بر روی برنامه می نشینند ناچار اندازه، تاریخ یا مختصات فایل اجرایی را تغییر می دهد . بنابراین می توان ضبط وضعیت قبلی و مقایسه آن با وضعیت فعلی از تغییرات احتمالی که به واسطه ویروس ایجاد شده است، آگاه شد. بنابراین اگر کد مبدا ویروسهای ناشناخته و یا برنامه ضد ویروس مناسب آنها در دسترس نباشد می توان به جای شناسایی ویروس به شناسایی وضعیت فایل ها و مقایسه با حالت قبل پرداخت و از این رهگذر تا حدی می توان به وجود ویروس پی برد. از نکته اول فوق (خصوصیت نیاز به نوشتن اطلاعات) برای تکمیل روش اول مبارزه یعنی جلوگیری از ورود ویروس و از نکته دوم فوق (ضبط و مقایسه وضعیت) برای تکمیل روش دوم یعنی از بین بردن ویروس ها استفاده می شود توجه کنید که ضد ویروس های قدرتمند انواعی از ویروس های فریب دهنده مانند ویروس stealth و ویروس های poly Morphic که هیچ يك از دو اثر فوق ظاهر نمی کنند نیز شناسایی می کنند .

پاکسازی ویروس ها

پس از اطلاع از وجود ویروس در سیستم ، ادامه کار با سیستم صحیح نیست ، با وجودی که ممکن است سیستم آلوده به کار خود ادامه دهد . ولی دامنه تخریب آن افزایش پیدا می کند قبل از پاکسازی ویروس اعمال زیر را انجام دهید .

۱) کامپیوتر را برای مدت ۵ دقیقه خاموش کنید این کار دارای مزایای زیر است :

الف- توقف انتشار ویروس

ب- پاک شدن ویروس ها مقیم در حافظه

۲) برای محدود کردن دامنه فعالیت ویروس ، لازم است تنها دستگاههای جانبی که برای کار با کامپیوتر ضروری هستند به کامپیوتر متصل باقی بمانند و باید بقیه را قطع کنید .

۳) حتی دیگر ضد ویروس ها را به کار نبرید زیرا برخی از ویروس ها ، موقع باز کردن فایل ها ، برای ویروس یابی آنها آلوده می کنند .

۴) کلیه دیسکت ها را در حالت write protect نوشتن مصنوع ، قرار دهید .

۵) همواره برای انجام عملیات ویروس یابی ، راه اندازی را از Floppy Drive انجام دهید.

۶) با استفاده از نرم افزار های ضد ویروس ، به پاک سازی ویروس ها بپردازید
روش های پاکسازی

۱) **آلودگی فایل ها** : در صورتی که فایل ها hard disk آلوده به ویروس هستند
اعمال زیر را انجام دهید :

الف- راه اندازی کامپیوتر با استفاده از یک Floppy disk سالم

ب- بدون دادن هیچ دستوری ، دیسک حاوی ضد ویروس را درون درایو فلاپی دیسک قرار داده و دستور پاکسازی ویروس ها را صادر نمایید .

ج- پس از آن مجددا سیستم را خاموش و روش کرده و مجددا از فلاپی دیسک راه اندازی نمایید .

۲) **آلودگی فایل ها و BOOT SECTOR** : در این حالت در صورتی که hard disk آلوده باشد اعمال زیر انجام دهید :

الف- راه اندازی کامپیوتر با استفاده از یک Floppy disk سالم

ب- بکار بردن دستوری بای پاک کردن Boot Sector با استفاده از یک ضد ویروس

ج- راه اندازی مجدد با استفاده از Floppy disk سالم

د- بدون دادن هیچ دستور دیگری ، دیسک حاوی ضد ویروس را درون درایو Floppy disk قرار داده و دستور پاکسازی ویروس ها را صادر نمایید .

ز- برای اطمینان ، راه اندازی مجدد و جستجو برای وجود ویروس

۳) **آلودگی فایل ها ، PARTITION, BOOT SECTOR** : در این صورت
اعمال زیر را انجام دهید :

الف- راه اندازی کامپیوتر با Floppy disk سالم

ب- استفاده از یک ویروس پاک کننده BOOT Sector برای پاکسازی Boot Sector

ج- خاموش و روشن کردن و راه اندازی مجدد کامپیوتر از Floppy drive

د- با استفاده از یک ضد ویروس پاک کننده partitian Table

ر- بدون دادن هیچ دستور دیگری، دستور پاکسازی ویروس ها را از روی Floppy disk صادر نمایید .

ز- خاموش و روشن کردن و راه اندازی مجدد کامپیوتر Floppy drive

ژ- اجرای مجدد ضد ویروس برای جستجوی ویروس ها

۴) آلودگی فایل ها ، PARTITION TABLE, BOOT SECTOR و حافظه

: روش پاکسازی در این حالت ، عیناً مانند حالت سوم است . فقط وقتی حافظه

آلوده است به هیچ وجه نمی توانید از ضد ویروس موجود در hard disk

استفاده کنید .

۵) آلودگی به ویروس ناشناخته : در این حالت، در صورتی که موفق به

پاکسازی ویروس نشدید ، یکی از راه حل های زیر را انتخاب کنید .

الف- تغییر نام یا حذف فایل های ویروسی از روی disk

ب- استفاده از برنامه های ویرایش سکتر دیسک

ج- Format و partition بندی مجدد

ابزارهایی برای افزایش امنیت و سرعت کامپیوتر

WinSpeedUp 2.5.2 ابزارهای موثر در حل مشکلات و بالا بردن سرعت کامپیوتر

WinSpeedUp ابزارهایی را ارائه می دهد که میتواند به حل مشکلاتی همچون خرابی

Registry Editor بپردازد یا اینکه آیکن های راتریب نماید در صورتی که راه حلی برای

این مشکلات نداشته

باشید، همین مسائل کوچک و پیش پا افتاده میتوانند موجب رنجش خاطر شما شوند. قبل از آن

که کار با برنامه WinSpeedUp را آغاز کنید، از شما پرسیده می شود که آیا کاربر

مبتدی هستید یا حرفه ای . اگر کاربر مبتدی باشید، برخی گزینهها که ممکن است خطرات

بالفوه بیشتری را به دنبال داشته باشند، غیر فعال می شوند. در مورد تمام کاربران، این نرم

افزار از تنظیمات موجود پشتیبان میگیرد، به عبارت دیگر چنانچه با انجام هرگونه تغییری

وضعیت کامپیوتر نسبت به قبل بدتر شود، میتوانید آن را مجدداً به حالت اول بازگردانید. شما

میتوانید کامپیوتر خود را بهینه سازی کنید و فضای هارد دیسک را بیشتر

نمائید WinSpeedUp. پر از ابزارهای مفیدی است که می توانند همه نوع کاری را از

تغییر ظاهر Internet Explorer گرفته تا پاک کردن History انجام دهند و به شما در تنظیم

DirectX کمک نمایند یا اینکه به شما بگویند که چقدر از حافظه را استفاده کرده اید. این نرم افزار دارای یک ابزار برگشت به حالت قبل (roll back) است، به عبارت دیگر تغییراتی که شما انجام می دهید، آسیبی به کامپیوتر نمی‌رساند. با استفاده از بخش Advanced برنامه WinSpeedUp

میتوانید دستورالعمل‌های بیشتری را به Windows Explorer بیافزائید.

ابزارهای کمی ویندوز XPTuner 1.05 یک برنامه tweak کننده با امکانات بسیار زیاد از جمله مزایای ویندوز این است که راه‌های بسیاری برای tweak کردن آن وجود دارد، چه به طریق دستی و چه با نرم‌افزاری شبیه به XPTuner. زمانیکه این برنامه را باز می‌کنید، یک پنجره باز میشود که تقریباً تمام کارهایی که میتوانید با این برنامه انجام دهید را خلاصه میکند. علیرغم ماهیت پیچیده برخی از tweak ها، میتوان به وضوح آن‌ها را شرح داد. نمونه‌هایی از این tweak ها زمانی است که وارد تب Edit Other Settings می‌شوید. در این قسمت ابزار بسیار مفیدی وجود دارد که آیتها را از پنجره Add Remove Programs حذف میکند.

گاهی اوقات زمانیکه نرم‌افزاری را حذف میکنید، آیکن مربوط به آن در Add Remove Programs باقی‌مانده، اما با XPTuner میتوانید آیکن را حذف کنید طوری که دیگر اثری از آن باقی نماند. گرچه تمام این کارها را می‌توان به طور دستی انجام داد اما اگر نسبت به انجام آن مطمئن نیستید، XPTuner دارای ویژگی‌هایی است که u1605 میتواند به شما کمک کنند. اگر جرات و اطمینان لازم را دارید، گزینه‌هایی وجود دارند که با آنها میتوانید تنظیمات کش را در مور CPU خود تغییر دهید.

Security and Privacy Pack

از کامپیوتر خود در مقابل تهدیدات آنلاین محافظت کنید و فایل‌های خود را با این مجموعه امنیتی حفظ نمایید.

به عنوان یک کاربر کامپیوتر دیگر نمیتوانید نسبت به ایمنی آن بی‌تفاوت باشید. این کار درست همانند این است که والدین به فرزندان بگویند که بدون هیچ نگرانی از ورود افراد ناشناس به خانه می‌توانند منزل را بدون قفل کردن در، ترک کنند. خطراتی که حریم

خصوصی شما را تهدید میکنند، میتوانند از جانب منابع داخلی یا خارجی باشند. به محض اینکه به اینترنت وصل میشوید، سیستم شما در معرض حملاتی از جمله هکرها، ویروسها، جاسوس افزارها و برنامه های بدخواه افزار دیگر قرار میگیرد.

مایکروسافت امکانات امنیتی را در قالب Windows Firewall ارائه میدهد که در واقع مانع از نفوذ هکرها میگردد و همچنین Microsoft AntiSpyware را عرضه میکند که کامپیوتر شما را در مقابل جاسوسافزارها و دیگر برنامه های ناخواسته محافظت مینماید.

با وجود اینکه این دو ابزار از ابزارهای مفید و قدرتمندی به شمار میروند، بهتر است برای کامل کردن امنیت سیستم خود از برنامه های دیگر شرکتها نیز استفاده نمائید. به خاطر داشته باشید که تهدیدات امنیتی فقط منشأ خارجی و بیرونی ندارند. اگر اشخاص دیگری به طور فیزیکی به کامپیوتر شما دسترسی دارند، میتوانند فایل هایی را باز کنند که در واقع شما نمیخواهید این فایل ها در دسترس آنها باشد.

Security and Privacy Pack از بهترین نرم افزارهای طراحی شده در حفظ اطلاعات شخصی است که کامپیوتر شما را در برابر حملات و آلودگی های ناشی از ویروس و دیگر بدخواه افزارها ایمن می کند. شما می توانید برای ایمن کردن سیستم خود از برنامه های دیگری نیز استفاده کنید، اما ما به شرح ۳ برنامه از این دست اکتفا می کنیم.

AntiVir PE 6 محافظ ویروس

خطر حمله ویروسها همیشه سیستم ما را تهدید می کند و هیچ نشانهایی دال بر این موضوع وجود ندارد که در آینده نزدیک از این گونه حملات در امان خواهیم ماند. قبل از نصب این نرم افزار، حتماً باید به صورت يك کاربر با حقوق اجرا کننده وارد سیستم شوید و نکته مهم دیگر اینکه نرم افزار ضد ویروس دیگری در سیستم نصب نباشد، در این صورت ممکن است با AntiVir تداخل پیدا کند. اگر از ارتباط تلفنی استفاده می کنید، بالا: کاربرد XPTuner بسیار ساده است، همچنین از طریق آن میتوان به جزئیات بیشتری دست یافت.

اگر مطمئن نیستید که کار را از کجا آغاز کنید، ویزاردهایی وجود دارند که در این رابطه به

شما کمک می کنند. می توانید مولفه Dialer-Recognition را نصب کنید. این مولفه شما را در مقابل شمار هگیر های فریب دهنده که می توانند صورت حساب های تلفنی کلانی برایتان به ارمغان بیاورند، حفظ می کند. در صورتیکه تعاریف سیستم شما قدیمی و منسوخ شده باشند، برنامه AntiVir به شما

هشدار میدهد و از شما می خواهد آخرین نسخه ها را دانلود کنید، به این ترتیب سیستم شما در مقابل آخرین تهدیدات و حملات ایمن می گردد. گزینه زمانبندی این برنامه به این معنی است که شما می توانید کامپیوتر خود را در فواصل زمانی معین اسکن کنید تا از نظر وجود مشکل بررسی شود، بنابراین دیگر نیازی نیست که انجام این کار را به خاطر بسپارید.

Hide My Files 1.0 محدود نمودن دسترسی به فایل

درایو سخت هر کاربر شامل فایلها و اطلاعاتی است که اغلب بهتر است برای دیگران قابل دسترس نباشند. با استفاده از Hide My Files می توانید دسترسی به هر فولدری که میخواهید از دید دیگران پنهان بماند را کاملاً غیر ممکن نمایید. اولین باری که این برنامه را اجرا می کنید از شما خواسته میشود تا رمز عبوری را وارد نمایید. بنابراین هر بار که بخواهید از این برنامه استفاده کنید، باید این رمز عبور را وارد کنید. سپس می توانید ساختار درختی نوع Explorer برای پیمایش در میان فولدر های خود استفاده نمایید. بعد به راحتی فولدری را که می خواهید پنهان کنید، کلیک نموده و دکمه Lock را کلیک نمایید. اگر برنامه را ببندید و سعی کنید به فولدری که انتخاب کرده اید دسترسی پیدا کنید، خواهید دید که این فولدر به پیوندی به Control Panel تبدیل شده است. برای دسترسی مجدد، Hide My Folders را اجرا نمایید، رمز عبور خود را وارد کرده فولدر را انتخاب و Unlock را کلیک کنید.

Password Manager XP 1.99.254

ذخیره سازی رمز عبور

بسیاری از برنامه ها و وب سایتها از شما میخواهند که username و رمز عبوری را وارد کنید که پی بردن به آنها دشوار باشد. با استفاده از Password Manager XP 1.99.254 می توانید تمام اطلاعات رمز عبور خود را در یک بانک اطلاعاتی رمزگذاری شده که خود آن نیز توسط رمز عبور محافظت میشود ذخیره نمایید، به این ترتیب شما باید

برای دسترسی به تمام رمزهای عبور تنها یک رمز عبور را به خاطر داشته باشید. برنامه را اجرا کنید و **Database>Create New** را کلیک نمایید. تعریفی را برای بانک اطلاعاتی خود وارد کرده و قبل از کلیک کردن **Ok** یک رمز عبور انتخاب کنید. در کادر سمت چپ، نام بانک اطلاعاتی خود را راست کلیک کرده و **New Folder** را انتخاب نمایید. شما میتوانید برای مرتب کردن رمزهای عبور خود به صورت طبقه بندی شده از فولدرها استفاده کنید و همچنین کادر سمت راست را کلیک کرده و **New Password** را انتخاب نمایید. انتخاب آیکن از منوی **Title** جستجو و یافت رمزهای عبور را سادهتر میسازد.

Spyware Doctor 3.2

ابزار ضد جاسوس افزار

آیا نصب دیواره آتش و ابزار ضد ویروس به معنی ایمنی شما در زمان آنلاین بودن است؟ متأسفانه، خیر. جاسوس افزارها، مرورگر رباها و برنامههای آزار دهنده دیگری از این دست راههای زیادی برای هجوم و حمله به کامپیوتر شما دارند، به همین دلیل داشتن یک ابزار جاسوسی اختصاصی برای از بین بردن آن ها ضروری به حساب می آید. ابزارهای جامع ای همچون **Ad-Aware SE Personal** به طور رایگان در دسترس هستند، بنابراین نیازی به خریداری آن ها نیست. اما اگر ثابت شود که ابزار ضد جاسوس افزار **Spyware Doctor** در مقایسه با **Ad-Aware** موثر و کارآمدتر است، پس ارزشش را دارد که برای آن هزینه کنید. مقایسه اولیه این دو ابزار در مرحله اول آزمایشات ما نتیجه خوبی را به دنبال نداشت. تعداد امضاهای **SpyWare Doctor** در بانک اطلاعاتی آن کمتر است (۲۶۸۴۰ در مقایسه با ۳۰۱۲۲ امضاء). **Ad-Aware** بعلاوه اجرای **Quick Scan** در **Spyware Doctor** حدود ۲۵ دقیقه طول می کشد، در حالیکه اجرای **Smart System can** متعلق **Ad-Aware** در ۶ دقیقه کامل می شود. امضا در کل بیانگر همه چیز نیست. گرچه **Spyware Doctor** کندتر است، اما بعضاً به این دلیل می باشد که اکثر آبجکت ها را اسکن می کند (۱۴۸۵۰۷ در مقایسه با **Ad-Aware** ۸۹۸۱۶ **Spyware Doctor** حدود ۱۱۴۱ مشکل را شناسایی میکند و این در مقایسه با ۱۴۶ مشکلی است که **Ad-Aware** بررسی مینماید، به همین دلیل است که اسکن کردن در **Spyware Doctor** بیشتر طول میکشد. برای از بین بردن کامل جاسوس افزار، ابتدا باید آن را شناسایی کنید، در این صورت تعداد خطرات احتمالی را که می یابید حائز اهمیت میگردد. آیا این به معنی برتری **Spyware Doctor** است به این دلیل که این ابزار ۱۱۴۱ مشکل را شناسایی و

لیست میکند. ضرورتاً خیر، زیرا در بررسی گزارش اسکن مشاهده کردیم که این تعداد شامل چندین ورودی به ازای یک خطر یا تهدید مشابه است. برای مثال، Spyware Doctor به ما اطلاع داد که NS Keylogger را در سیستم یافته است و اینکه نصب شامل 215 registry

key متفاوت می باشد. سپس این ابزار آن ها را به عنوان ۲۱۵ آلودگی شمارش کرده ولی تنها یک برنامه را یافته بود. مطمئن یا مشکوک؟

تصمیم گرفتیم که بررسی کنیم آیا این Keylogger اصلاً نصب شده است یا خیر. Spyware Doctor وجود Keylogger را در فایلی به نام jmail.dll و ورودیهایی Registry مربوط به آن شناسایی کرد، که به عقیده ما یک فایل قانونی بود Ad-Aware. این keylogger را شناسایی نکرد، Norton AntiVirus نیز هیچ مشکلی را تشخیص نداد. بعلاوه، Spyware Doctor برنامه بیخطر دیگری تحت عنوان TrojanIRC.Comiz را شناسایی کرد که Ad-Aware یا Norton AntiVirus آن را شناسایی نکردند. به نظر میرسید اسکن به درستی یا به طور کاملاً صحیح صورت نگرفته است. آیا Spyware Doctor میتواندست با آخرین ترند خود ما را فریب دهد؟

در اکثر ردیابهای جاسوس افزار، شما باید هر چند وقت یک بار اسکن را اجرا کنید، در غیر این صورت شما را بدون هیچ محافظی رها می کنند. اما این مسئله در مورد Spyware Doctor صادق نیست. Spyware Doctor شامل OnGuard است که بطور اختیاری تمام وقت کامپیوتر شما را تحت نظر دارد و آلودگیها را به محض تشخیص آنها بلوکه می کند. مزیت خوبی به نظر میرسد به خصوص که Spyware Doctor دارای ترکیب معقولانهایی از ابزارها است:

بررسی برای یافتن Cookie های خطرناک، نصب خودکار برنامه ها برای اجرا در Startup یا شناسایی فرایندها جاسوس افزار از همان ابتدا. همچنین یک pop-up blocker و ردیاب eylogger نیز در آن وجود دارد.

استفاده بیش از حد از منابع

متأسفانه، این مسئله به دلیل اجرای ضعیف Spyware Doctor که آن هم به دلیل کنترل دائمی تعدادی فایل و رجیستری است، ارزش خود را از دست داده است. بررسی نهایی بیانگر این است که Spyware Doctor هر چند ثانیه حدود ۵۰ درصد از منابع CPU را مصرف میکند و به این ترتیب موجب کندهای عملکردهای دیگر می گردد. شما می توانید با

کاهش بررسیهایی که توسط ActiveGuard صورت میگیرد، این میزان مصرف از CPU را محدود نمائید. مسئله دیگر اینکه هنگام اجرای SpywareDoctor متوجه شدیم، (Smartstore.biz یک ابزار (e-commerce دیگر به درستی در صفحه نمایش اصلی به نمایش در نمیآید. این ابزار از یک پنجره مرورگر پنهان استفاده میکند که به نظر میرسد Spyware Doctor به طریقی آن را بلوکه مینماید. در دسرهایی نظیر این فاجعه است و اگر در مورد برنامه های مشابهی نظیر آن تکرار شود این ذهنیت را به وجود می آورد که مشکلات Spyware Doctor نسبت به مزایای آن بیشتر است.

DisKeeper 9.0

پراکندگی دیسک هرگز

اسکن جاسوس افزار، بلوکه کردن کنترلرهای خاص ActiveX و محافظت زمان اجرا همگی از یک رابط ساده و مشابه راه اندازی میشوند. سرعت اسکن کردن زیاد نیست اما حداقل زمانبندی آن به این معناست که این برنامه به طور خودکار اجرا میشود. Spyware Doctor ادعا میکند که ۱۰۹۰ آلودگی را یافته، پس چرا تنها ۶ آلودگی در اینجا لیست شده است؟ Diskeeper شامل گرافهای نمایشی است که نشان میدهند که پراکندگیها چگونه سرعت و اطمینان پذیری را تحت تاثیر قرار میدهند. اینقدر ساده، دقیق و سریع نبوده است.

پراکندگی درایو دیسک سخت یکی از دلایلی اصلی مشکلات اجرایی است. ویندوز خود دارای برنامه کمکی یکپارچه سازی است، اما نیازمند یک فرآیند دستی بوده تا از میزان پراکندگی آگاهی یابد و اجرای آن در درایوهای سخت بزرگ مدت زیادی طول می کشد. Diskeeper 9.0 سریع، ساده و موثر است و دارای امکانات زمانبندی و زمان راه اندازی میباشد. DisKeeper درایورهای شما را پاک میکند و آنها را به همان صورتی که هستند یعنی به صورت فشرده سازیشده یا رمز گذاری شده حفظ نموده و فایل ها را در دیسکهای NTFS پراکنده میکند. همچنین میتوان DisKeeper را زمانبندی کرد تا به طور پنهان و غیر قابل رویت به صورت یک برنامه زمینهای اجرا گردد یا به عنوان یک یکپارچهساز (defragmenter دستی، فایلها را دو باره مرتب کند و فضای دیسک را خالی نماید. این رابط مرتب و کار با آن ساده میباشد. مولفه های موجود این امکان را فراهم میسازند تا وجوه مختلف وضعیت دیسک خود را ببینند و در زمان اجرای DisKeeper آن ها را کنترل نمائید و به ویژگی ها و میان برهایی که معمولاً استفاده میشوند، دسترسی یابید.

انتقال دادهها

ویژگی " Set it and Forget it " یکی از مفیدترین ویژگی های این نرم افزار است. با این ویژگی DisKeeper به طور خودکار با یک زمانبندی از پیش تعیین شده در زمینه اجرا میگرد. همچنین میتوانید از گزینه SmartScheduling استفاده کنید تا این نرم افزار به طور خودکار بهترین زمانبندی یکپارچهسازی را برای دیسک های شما تعیین کند. شما میتوانید مطابق با نیاز خود روشهای مختلف یکپارچه سازی را انتخاب نمایید. از جمله ویژگیهای دیگر این نرم افزار Boot-Time defragmentation است که دایرکتوریها را به یک محل منتقل میکند. این ویژگی اهمیت خاصی دارد زیرا ویندوز دایرکتوریها را در محلهاي اتفاقي در سراسر يك دیسک مینویسد و در حقیقت، فضای خالی دیسک را تکه تکه می کند. با گروه بندی تمام دایرکتوریها در یک محل، امکان دسترسی به فضاهای خالی بزرگتر و پیوسته بیشتر میگردد. بنابراین، فایلهاي جدید به طور پیوسته در دیسک نوشته میشوند. این کار همچنین موجب یکپارچه سازی Master File Table میگردد که بخش مهم و حساس پارتیشنهای دیسک NTFS ویندوز است.

Registry Machanic 4.0

پاک کردن رجیستری موجب بهبود عملکرد و افزایش ثبات کامپیوتر می گردد. زمانیکه برنامههاي کاربردي زيادي را نصب میکنید، این برنامهها u1608 و رودیهاي جدید زيادي را به Registry شما میافزایند: تنظیمات برنامه، پیوندهاي فایل، فونتها، ورودی Add/Remove Programs و بسیاری دیگر.

البته اگر در صورت حذف برنامه کاربردي تمام این موارد همگی حذف شوند بسیار خوب و عالی است. متأسفانه، چنین چیزی ندرتاً اتفاق میافتد و نتیجه نهایی Registry ای است که با استفاده از کامپیوتر بزرگ تر و کندتر میگردد. نیازی نیست این وضعیت را تحمل کنید. با اجرای Registry Machanic ، رجیستری شما اسکن شده، خطاها برطرف و تمام ورودیهاي ببرد نخود حذف میگردند. همچنین این برنامه منوی Start شما را چک میکند تا میانبرهاي احتمالي به این فایل را حذف نماید. معمولاً وجود برنامههاي که با رجیستری ما سرو کار دارند و آن را دست کاری میکنند موجب رنجش ما میگردد، اما Registry

Mechanic در این رابطه دارای دو لایه محافظتی است. اولاً این برنامه از تمام کلیدهای رجیستری که تغییر داده میشوند پشتیبانگیری میکند، بنابراین میتوانید در صورت نیاز دوباره آنها را برگردانید. دوماً، کاربران ویندوز XP میتوانند قبل از هرگونه اصلاح یا تغییری یک **System Restore** تنظیم کنند تا در صورت بروز مشکل آنها را بازیابی کنند.

فرآیند اسکن

برای آزمایش، از این برنامه در کامپیوتر خود استفاده کردیم، اسکن کامل کامپیوتر حدود ۱۴ دقیقه

طول کشید و بالاخره ۱۹۲ مشکل را گزارش کرد. اگر بخواهید بررسیهای کمتری صورت بگیرد،

اسکن سریع تر انجام میشود. در مقایسه با این برنامه، **Aid RegistryFirst** (www.rosecitysoftware.com) تقریباً در ۶ دقیقه ۱۲۲۵ مشکل را در ارتباط با رجیستری ما شناسایی کرد. بعلاوه، **Registry TuneUp** (www.ace-logix.com) ظرف ۳ دقیقه و ۲۹ ثانیه در صورت بروز هرگونه اشتباهی، از پشتیبانهای **Registry Mechanic** میتوان برای بازگرداندن رجیستری استفاده کرد. مدعی تشخیص ۱۳۲۵ مشکل رجیستری گردید. **Registry Mechanic** از نظر سرعت نسبت به دو برنامه دیگر پائین تر است، اما شمارش مشکلات نمایانگر بالا بودن کیفیت برنامه نیست.

Registry First Aid و **Registry TuneUp** با این فرض که کلیدهای خالی رجیستری خطا

هستند و میباید حذف شوند، مشکلات بیشتری را شمارش میکنند. یک برنامه کاربردی ممکن است

با بررسی وجود یک کلید، اطلاعات مفیدی بدست بیاورد. بنابراین روش **Registry Mechanic** که کاری به کار این ورودیها ندارد مطمئن تر است.

کار پر مخاطره

پس از اتمام کار اسکن، **Registry Mechanic** مشکلات را در گروههای مختلف نشان میدهد. سپس کاربر ممکن است بخواهد هر مشکل را به نوبت مرور کند و مشکل هر ورودی را حل و یا آن را به همان صورت باقی بگذارد. اگر برنامه صدها u1605 مشکل را بیابد، احتمالاً گزینه ساده تر را انتخاب خواهید کرد، **Repair** را کلیک کنید و **Registry Mechanic** را فعال نمایید تا تمام مشکلات را حل کند. آیا روش خوبی است؟ احتمالاً خیر. **Registry Mechanic** تنها پاک کنندهایی است که یک ورودی برنامه (**dumprep**)

(Startup) را نادرست شناسایی می کند و آن را برای حذف کردن علامت گذاری می نماید. شاید علت آن این است که برنامه Registry Mechanic به دنبال فایلی به نام dumperp.exe است، در حالیکه نام واقعی dumperp.exe می باشد؟

گرچه ویندوز اهمیتی به این موضوع نمی دهد: این فایل يك فایل قانونی است که برای گزارش فایل خطا به کار می رود، با این وجود Registry Mechanic در زمان راه اندازی کامپیوتر اجرای آن را متوقف میکند. البته این مورد خیلی مهم نیست، اما اگر موارد مهم تری را بدون اطلاع شما حذف کند چه؟ باید گفت که مزایای حذف این ورودیهایی اضافی رجیستری بسیار مهمتر از مشکلاتی است که ممکن است با یک حذف نادرست به وجود بیاید.

System Mechanic 5

کامپیوتر خود را برای اجرای راحتتر و روان تر، تنظیم کنید

حتی سرعت عمل ما نیز با گذشت زمان و بالا رفتن سن، پائین میآید و ویندوز XP مایکروسافت نیز از این قاعده استثناء نیست. دادههای ناخواسته ی که پس از هر بار استفاده از کامپیوتر در آن اثبات شده می شوند، اگر دست نخورده باقی بمانند حقیقتاً میتوانند مشکلاتی را به دنبال داشته باشند. بنابراین لازم است فرصتی به کامپیوتر داده شود تا بقایای دیجیتالی را پاک کند و درایو سخت و حافظه کامپیوتر شما را به شکل اولیه خود بازگرداند. ده ها بلکه هم صدها برنامه برای انجام این کار وجود دارند و ممکن است شما نیز یکی دو برنامه از این دست در کامپیوتر خود نصب کرده باشید. پس System Mechanic 5 باید امکان خاصی را ارائه دهد تا آن را از دیگر برنامهها متمایز نماید. این برنامه کارهای ارزشمندی همچون tweak کردن رجیستری، پاک کردن فایل های موقت و یکپارچه سازی

دیسک سخت را انجام می دهد که البته این ویژگیها را میتوان در برنامههای دیگری نیز یافت. ویژگیهای دیگری همچون ابزارهای ضد جاسوس افزار، پاک کردن تاریخچه اینترنت و بلوکه کردن pop-up ها را نیز میتوان در Sevice Pack2 و بتای برنامه ضد جاسوس افزار جدید مایکروسافت یافت. بهرحال، این نسخه شامل ویژگی های جدیدی است. یکپارچه ساز جدید زمان راه اندازی که قبل از راه اندازی ویندوز فایل های اصلی سیستم را مرتب میکند يك ویژگی عالی و ماهرانه است، و در صورتیکه با برنامه های کمکی دیگر همراه شود، موجب ارتقاء عملکرد سیستم شما می گردد.

مهمترین ویژگی Service Mechanic 5 این است که تمام این ویژگی ها را در يك رابط ساده ادغام میکند. در این صورت دیگر مشکل نصب برنامههای مختلف و مجزا را ندارید. بعلاوه این برنامه قابل اطمینان بوده و شامل تمام آن چیزهایی است که شما نیاز دارید و

اجرای آن مقرون به صرفه می باشد. اسکن کامل رجیستری حدود ۱۴ دقیقه طول می کشد.
برای آنکه کار مرور کردن ساده تر شود، مشکلات در گروه های مختلف گروه بندی می
شوند.

ویژگی و متن

منابع:

www.persian blog.com
www.irandevolvers.com
www.zendagi.com
www.frontpageworld.com

وبلاگ و هنر

انتقاد و پیشنهاد را به ایمیل ebrahimaram40@yahoo.com
ارسال کنید

با تشکر از دانلود این کتاب