

رسم عجم لولسی الفرج

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 يك 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 يك پروژه دانشجویی ، برنامه ای را ساخت که می توانست خود را تکثیر کرده وانگل 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 زاد 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 يك دیسک وجود داشته باشند. تا زمانی که شرایط مناسب نباشند، فعال نخواهد بود. امروزه مسئله ویروسهای کامپیوتری به يك معضل بسیار جدی تبدیل شده است. حوزه عملکرد ویروسها، انواع کامپیوتر ها 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 يك کاربر معمولی PC ممکن است حداکثر ضرر ناشی از يك ویروس خطر ناک ، نابود کردن اطلاعات و برنامه های مهم موجود بر روی کامپیوتری باشد در حالی که ضرر يك ویروس مخرب بر روی شبکه ارتباطی ترمینالهای بانک های يك 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 يك 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 يك 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 معرفي كرد . متأسفانه به دليل كمبود منابع ، عموم کاربران داخل كشور از كارايي و نحوه عملکرد برنامه هاي اطلاع كافي نداشته و لذا صرفاً از آنها به شكل ساده و بدون تنظیمات خاص استفاده کرده و از این رو در بسياري موارد مشكلات ناشي از وجود ویروسها به طور قطعي حل نمي شوند .

ویروس كامپیوتري چیست ؟

ویروس كامپیوتري برنامه اي است كه مي تواند داده هاي موجود روي ديسك و حافظه RAM را معيوب نموده و در نتیجه از اجراي برنامه ها بطور صحيح جلوگیری به عمل مي آورد . بعضي از ویروسها ي كامپیوتري ضعيف بوده و فقط با نمایش پیغام خاصی خود را نشان داده و صدمه اي به ديسك وارد نمي سازند ولي نوع ديگر ویروس ها ممكن است به حد خطرناك باشند كه كل اطلاعات ديسك را از بين برده و كاربر را مجبور به format نمودن ديسك مزبور كنند . ویروسها كامپیوتري به صورت مخفيانه و از طريق برنامه هايي كه توسط ديسك هاي ديگر يا مودم به كامپیوترتان كپی مي كنيد ، وارد كامپیوترتان مي شوند . این ویروسهاي كامپیوتري ممكن است مدتها در كامپیوتر شما موجود بوده و فقط به تكثير خود پرداخته و هيچ صدمه اي وارد ننمایند و در ساعت و تاريخ و يا هنگام اجراي برنامه خاصی فعال شده و تمام كپی ها ي خود را نيز فعال كنند كه بستگی به ویروس مورد نظر ، صدمات غيرقابل جبراني را وارد مي كنند . ویروس ها اغلب روي فايل هاي اجرايي ديسك عمل نموده و آنها را معيوب مي كنند . ویرس هاي كامپیوتري به صورت برنامه جداگانه اي وجود ندارند بلکه خود را به فايل ها و برنامه هاي ديگر چسبانده و از كامپیوتري به كامپیوتر ديگر منتقل مي شوند .

تا كنون بیش از ۲۰۰۰۰ ویروس شناخته شده اند و متخصصين و كارشناسان پس از شناسايي هر يك از آنها ، نام خاصی را به آنها اطلاق کرده اند .

براي محافظت و سالم نگه داشتن ديسك ، کاربران بايستي از برنامه هاي موجود به طور مداوم استفاده نمایند كه يكي از آنها و قويترين شان برنامه Disk Monitor است البته برنامه هاي ديگري در سيستم عامل Dos و ديگربرنامه هاي سودمند نيز تعبيه شده اند كه عبارتند

از Vasfe و سنسورهای مختلف برنامه Norton system Doctor در Un تحت ویندوز 95 و.....

اگر برنامه های حفاظت از دیسک همیشه استفاده نمایید، امکان ورود ویروس های کامپیوتری به کامپیوترتان کم شده و در نتیجه سیستم شما سالم خواهد ماند .

در انتها بطور خلاصه می توان گفت : ویروس برنامه مخفی و کوچکی است که باعث آلوده شدن برنامه های دیگری شود و می تواند داده ها را دستکاری و یاتخریب نموده ، سرعت سیستم را کاهش داده باعث اغتشاش و عدم کارایی کامپیوتر شود .

مهمترین خصوصیت ویروس قدرت تکثیر آن است ، ویروسها برای تکثیر نیاز به یک برنامه اجرایی دارند یعنی بیشتر ویروسها در فایل های اجرایی جای می گیرند و آنها را آلوده می کنند . کمتر ویروسی پیدا می شود که بتواند نسخه های اجرایی جای می گیرند و آنها را آلوده می کنند و کمتر ویروسی پیدا می شوند که ابتدا نسخه های اجرایی از خود را در برنامه های دیگر قرار دهد . برنامه آلوده به ویروس می تواند هر برنامه سیستمی با کاربردی باشد که شرایط مورد نیاز برای پذیرش ویروس را داشته باشد . برنامه آلوده قادر است برنامه های دیگر را آلوده کند .

خانه ویروس

ویروس هم مانند هر برنامه کامپیوتری نیاز به محلی برای ذخیره خود دارد منتهی این محل باید به گونه ای باشد که ویروسها را به وصول اهداف شوم خود نزدیک تر کند . همانطور که می دانید اکثر ویروسها به طور انگل مانندی به فایل های اجرایی می چسبند و آنها را آلوده می کنند. اصولاً در برخورد با ویروسها ، فایل های اجرایی و غیر اجرایی تقسیم می شوند عموم ویروسها در فایل های اجرایی جای گرفته و آنها را آلوده می کنند و واقعاً کمتر ویروسی هست که در یک فایل غیر اجرایی جای بگیرد و بتواند از طریق آن تکثیر پیدا کند. در ذیل، فهرست پسوند های رایج فایل های اجرایی ارائه شده است و اکثر نرم افزار های ضد ویروس در حالت عادی (بدون تنظیم خاص) تنها همین فایل ها را ویروس یاب می کنند (البته در برخی برنامه های ضد ویروس ممکن است برخی پسوندها حذف و اضافه شوند). -EXE-COM-SYS-BIN-

OVL-DLL-SCR

بنابراین یکی از اصلی ترین خانه های ویروس فایل ها آلوده به ویروس هستند. از طرف برخی ویروسها علاقه خاصی به قطاع بوت (Boot Sector) و جدول بخش بندی دیسک 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 بندي شامل اطلاعات تقسیم بندي 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 موقتي است در حافظه RAM کامپیوتر می باشد . به محض روشن کردن کامپیوتر و اجرای يك برنامه آلوده به ویروس و یا دسترسی به يك دیسک تا قطاع بوت و جدول بخش بندي آلوده ، ویروس همراه آن در حافظه جا می گیرد و برخي 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 ویروسي 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 امضايي (Signature) دارد که يك سري 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 (یعني گونه هایی در برنامه هاي اصلي آنها تفاوت جزيي وجود دارد).

تا کنون بیش از ۱۰۰۰۰ ویروس شناخته شده است . بسیاری از آنها مدتي 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 می 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 TOPGUN چنانچه تاریخ سیستم برابر با روز دوم ماه
باشد ، ۶۴ بایت اول Ram CMOS را پاک می کند .

۶- ویروس خود شاخه (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 .

مزامتهای 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 مرحله ای 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 وپروس است .

(۶) وقتي كه صفحه كليد را فشار مي دهد دستوري را وارد مي كنيد پيامي مبني بر غلط بودن شكل دستور دريافت مي كنيد و علت آن ممكن است اين باشد كه اگر كليد B را فشار مي دهيد علامت كيد مجاورش ، يعني N روي صفحه نمايش ظاهر مي شود، در اين صورت احتمالاً كامپيوتر آلوده به وپروس است .

(۷) خرابي DISK: ممكن است كه احتمالاً بخشي ازديسك يا تمام آنها ازبين بروند و يا ديسك Format شود .

(۸) کاهش حجم حافظه : با وجودي كه 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 كنند .

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

(۱۱) اختلال در SETUP: برخي از وپروسها ، اطلاعات موجود در Setup كامپيوتر را از بين مي برند .

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

(۱۳) خواص فايلهاي اجراي تغيير مي كند .

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

(۱۵) هنگام كار 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) امكان دسترسي به يكي ازديسك گردانها از بين مي رود .

١٨) هـځام اءراي يـك برنامـه سـيستم قفل مـي كـند و گاهـي فـشردن كـليدهـاي
ALT+DEL+CTRL نـيز نـمي تـواند سـيستم رـاه اندازي كـند .

ويژر ورس

ویروسهای ناشناخته

شاید یافتن ویروس های ناشناخته مهمتر از ویروس های شناخته شده باشد، زیرا ویروس های جدید تا قبل از کشف شدن، مورد تجزیه و تحلیل قرار گرفتن، نامگذاری و توزیع ویروس یابها، مدتی ناشناخته می مانند.

ویروس یابها با جستجوی فایل های برنامه ای به دنبال تغییراتی در آنها احتمال آلودگی ویروسی را نشان می دهند، ویروس های ناشناخته را پیدا می کنند. بیشتر فایل های برنامه ای پس از نصب تغییر نمی کنند، بنابراین وجود هر گونه تغییری در آنها می تواند نشانگر آلودگی ویروسی باشد.

اولین باری که ویروس یابها میکروسافت را در درایوی مورد استفاده قرار دهید، فایلی به نام CHKLIST.MS در هر فهرستی ایجاد می کند و اندازه، صفات، تاریخ و ساعت تمام فایل های برنامه ای فهرست مزبور را در آن فایل ثبت می کند.

اولین باری که مقدار کنترلی (Check sum) یعنی مقدار منحصر به فردی که از محاسبه محتویات فایل بدست می آورد را نیز ثابت می کند. بدین ترتیب اگر محتویات فایل تغییر کند، مقدار کنترلی آن نیز تغییر می کند و ویروس یاب از روی آن می فهمد که فایل تغییر کرده است، حتی اگر اندازه، صفات و تاریخ و سرعت آن ثابت مانده است.

اگر هنگام ثبت داده ها CHKLIST.MS ویروس ناشناخته ای در سیستم وجود داشته باشد شناسایی نخواهد شد. خوشبختانه VSAFE می تواند با نظارت بر سیستم، جلوی فعالیت مخرب ویروس ها را بگیرد.

پس از تشکیل فایل های CHKLIST.MS، هر بار که عملیات ویروس یابی انجام شود، ویروس یابی داده های ثبت شده را با فایل های برنامه ای مقایسه می کند. هر گونه تفاوتی در آنها باعث می شود ویروس یاب داده های ثبت شده را با فایل های برنامه ای مقایسه می کند. وجود هر گونه تفاوتی در آنها باعث می شود که ویروس یاب امکان وجود یک ویروس ناشناخته را گزارش دهد که در این صورت باید فکری به حال سیستم بکنید. در این حالت می توانید به برنامه ویروس یاب بگویید که از تغییر صرف نظر کند، فایل CHKLIST.MS را با داده های جدید نوسازی کند، فایل آلوده را پاک کند، یا عملیات ویروس یابی 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 آشکارسازی 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 Virus Pattern database ساده ترین روش تشخیص ویروس ها نگاه کردن به برنامه آنهاست و بررسی پیام ها ی 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 فایل های 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 يك فایل دیگر ، یا حذف کردن خودش بدون هیچ خطاري 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 ویروس های هم شکل و هزار چهره پی برد . ضد ویروس های 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 معمولاً 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) حتي ديگر ضد ويروس ها را به كار نبريد زيرا برخي از ويروس ها ، موقع باز كردن فايل ها ، براي ويروس يابي آنها آلوده مي كنند .
- (۴) كلييه ديستكت ها را در حالت write protectنوشتن مصنوع ، قرار دهيد .
- (۵) همواره براي انجام عمليات ويروس يابي ، راه اندازي را از Floppy Drive انجام دهيد.
- (۶) با استفاده از نرم افزار هاي ضد ويروس ، به پاك سازي ويروس ها بپردازيد
روش هاي پاكسازي
- (۱) *آلودگي فايل ها* : در صورتي كه فايل ها hard disk آلوده به ويروس هستند اعمال زير را انجام دهيد :
- الف- راه اندازي كامپيوتر با استفاده از يك Floppy disk سالم
- ب- بدون دادن هيچ دستوري ، ديستك حاوي ضد ويروس را درون درايو فلاپي ديستك قرار داده و دستور پاكسازي ويروس ها را صادر نماييد .
- ج- پس از آن مجدداً سيستم را خاموش و روش كرده و مجدداً از فلاپي ديستك راه اندازي نماييد .
- (۲) *آلودگي فايل ها و BOOT SECTOR* : در اين حالت در صورتي كه hard disk آلوده باشد اعمال زير انجام دهيد :
- الف- راه اندازي كامپيوتر با استفاده از يك Floppy disk سالم
- ب- بكار بردن دستوري باي پاك كردن Boot Sector با استفاده از يك ضد ويروس
- ج- راه اندازي مجدد با استفاده از Floppy disk سالم
- د- بدون دادن هيچ دستور ديگري ، ديستك حاوي ضد ويروس را درون درايو Floppy disk قرار داده و دستور پاكسازي ويروس ها را صادر نماييد .
- ز- براي اطمينان ، راه اندازي مجدد و جستجو براي وجود ويروس
- (۳) *آلودگي فايل ها ، PARTITION, BOOT SECTOR* : در اين صورت اعمال زير را انجام دهيد :
- الف- راه اندازي كامپيوتر با ي Floppy disk سالم
- ب- استفاده از يك ويروس پاك كننده BOOT Sector براي پاكسازي Boot Sector
- ج- خاموش و روشن كردن و راه اندازي مجدد كامپيوتر از Floppy drive
- د- با استفاده از يك ضد ويروس پاك كننده 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 سکتور 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 گزینه ها که ممکن است خطرات

بالقوه 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 نرم افزاری شبیه به XPTuner. زمانیکه این برنامه را باز می کنید، 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 آن ها را شرح داد. نمونههایی از این tweak ها زمانی است که وارد تب Edit Other Settings می شوید. در این قسمت ابزار بسیار مفیدی وجود دارد که آیتمها را از پنجره Add or Remove Programs حذف میکند.

گاهی اوقات زمانیکه نرم افزاری را حذف میکنید، آیکن مربوط به آن در Add or Remove Programs باقی میماند، اما با XPTuner میتوانید آیکن را حذف کنید طوری که دیگر اثری از آن باقی نماند. گرچه تمام این کارها را می توان به طور دستی انجام داد اما اگر نسبت به انجام آن مطمئن نیستید، XPTuner دارای ویزاردهایی است که u1605 میتواند به شما کمک کنند. اگر جرات و اطمینان لازم را دارید، گزینه هایی وجود دارند که با آنها میتوانید تنظیمات کش را در مورد CPU خود تغییر دهید.

Security and Privacy Pack

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

به عنوان یک کاربر کامپیوتر دیگر نمیتوانید نسبت به ایمنی آن بی تفاوت باشید. این کار درست همانند این است که والدین به فرزندان بگویند که بدون هیچ نگرانی از ورود افراد ناشناس به خانه می توانند 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 نمایید. 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. میتوانید مولفه Dialer-Recognition را نصب کنید. این مولفه شما را در مقابل شمار هگیر های فریب دهنده که میتوانند 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 میگردد. گزینه زمانبندی این برنامه به این معنی است که شما میتوانید 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 میتوانید دسترسی به هر فولدری که میخواهید از دید دیگران پنهان بماند را کاملاً غیر ممکن نمائید. اولین باری که این برنامه را اجرا می کنید از شما خواسته میشود تا رمز عبوری را وارد نمائید. بنابراین هر بار که بخواهید از این برنامه استفاده کنید، باید این رمز عبور را وارد کنید. سپس میتوانید از ساختار درختی نوع Explorer برای پیمایش در میان فولدر های خود استفاده نمائید. 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 نمائید، 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 آن ها دشوار باشد. با استفاده از Password Manager XP 1.99.254 میتوانید تمام اطلاعات رمز عبور خود را در یک بانک اطلاعاتی رمزگذاری شده که خود آن نیز توسط رمز عبور محافظت میشود ذخیره نمائید، 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 يك 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 يك 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 ورودیهای 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 ترفند خود ما را فریب دهد؟

در اکثر رد یابهای جاسوس افزار، شما باید هر چند وقت يك بار اسکن را اجرا کنید، در غیر این صورت شما را بدون هیچ محافظتی 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 معقولانه ای 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 يك pop-up blocker و رد یاب 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 کندی 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 يك ابزار (e-ommerce) دیگر به درستی در صفحه نمایش اصلی به نمایش در نمیآید. این ابزار از يك 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 يك 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 زمینه ای اجرا گردد یا به عنوان یک یکپارچه ساز (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 ویژگی‌های این نرم افزار است. با این ویژگی DisKeeper به طور خودکار با یک زمانبندی از پیش تعیین شده در زمینه اجرا می‌گردد. همچنین می‌توانید از گزینه SmartScheduling استفاده کنید تا این نرم افزار به طور خودکار بهترین زمانبندی یکپارچه‌سازی را برای دیسک‌های شما تعیین کند. شما می‌توانید مطابق با نیاز خود روش‌های مختلف یکپارچه‌سازی 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 محل‌های اتفاقی در سراسر یک دیسک مینویسد و در حقیقت، فضای خالی دیسک را تکه تکه می‌کند. با گروه بندی تمام دایرکتوری‌ها در یک محل، امکان دسترسی به فضاهای خالی بزرگ‌تر و پیوسته بیشتر می‌گردد. بنابراین، فایل‌های جدید به طور پیوسته در دیسک نوشته می‌شوند. این کار همچنین موجب یکپارچه‌سازی 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 می‌گردد. زمانیکه برنامه‌های کاربردی زیادی را نصب می‌کنید، این برنامه‌ها u1608 و رودیهایی جدید زیادی را به Registry شما می‌افزایند. تنظیمات برنامه، پیوندهای فایل، فونتها، ورودی را به Add/Remove Programs و بسیاری دیگر.

البته اگر در صورت حذف برنامه کاربردی 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 بزرگ‌تر و کندتر می‌گردد. نیازی نیست این وضعیت را تحمل کنید. با اجرای Registry Machanic ، رجیستری شما اسکن شده، خطاها برطرف و تمام ورودیهایی بدرد نخود حذف می‌گردند. همچنین این برنامه منوی Start شما را چک می‌کند تا میانبرهای احتمالی به این فایل را حذف نماید. معمولاً وجود برنامه‌هایی 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، Registry First Aid (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 (dumpprep)

(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 dumpprep 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 ای که پس از هر بار استفاده از کامپیوتر در آن انباشته 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.

رجیستری و اسکن

منابع:

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

وبلاگ

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

با تشکر از دانلود این کتاب