نویسنده: ابراهیم آرام

فهرست مطالب

مقدمه

بيش از سه دهه ازساخت اولين ويروس كامپيوتري توسط فرد كوهن مي گذرد . شايد درابتدا كوهن هرگزتصورنمي كرد كه روزي اختراع اوبه صورت يك فاجعه كامپيوتري در آمده و دنياي كامپيوتر را مورد تهديد قرار دهد (متاسفانه بسياري از مشكلات بزرگ تكنولوژي همين گونه آغاز مي شود). كوهن صرفا به عنوان يك پروژه دانشجويي ، برنامه اي را ساخت كه مي توانست خود را تكثير كرده وانگل وار به ديگر برنامه ها بچسبد و نوعي تغيير در آنها بوجود آورد . با طرح ويژگيهاي اين نوع برنامه ها در مقالات و سخنرانيها بتدريجاين مسئله توجه عده زيادي از بر نامه نويسان را به خود جلب كرده و رفته رفته مسئله توليد ويروسهاي كامپيوتري نضج گرفت. علت نامگذاري ويروس بر روي اينگونه برنامه ها،تشابه زاد آنها با ويروسهاي بيولوژيكي بود. چرا كه ويروسهاي كامپيوتري مانند ويروسهاي بيولوژيكي بطور ناگهاني تكثير مي شوند و در حالي كه ممكن است بر روي يك ديسك وجود داشته باشند.تا زماني كه شرايط مناسب نباشند،فعال نخواهد بود.امروزه مسئله ويروسهاي كامپيوتري به يك معضل بسيار جدي تبديل شده است. حوزه عملكرد ويروسها، انواع كامپيوتر ها وسيستم هاي عامل را در بر مي گيرد. و هر روزچندين ويروس جديد توليد شده و در فضاي كامپيوتر جهاني رها مي شود. بدون اينكه بتوان فرد سازنده آن را شناسايي و مواخذه كرد.براي يك كاربر معمولي PC ممكن است حداكثر ضرر ناشي ازيك ويروس خطر ناك ، نابود كردن اطلاعات وبرنامه هاي مهم موجود بر روي كامپيوتري باشد درحالي كه ضرر يك ويروس مخرب بر روي شبكه ارتباطي ترمينالهاي بانك هاي يك كشور ممكن است موجب تغيير و يا حذف اطلاعات مالي شركتها و افراد صاحب حساب شده و خسارات مالي سنگيني را ببار آورد ، آنچنان كه تا كنون نيز مواردي از اين دست ، ازرسانه هاي گروهي اعلام شده است . بنابراين اثر تخريب كنندگي ويروسها مرز خاصي نمي شناسد و هر جا كه اثري ازيك فعاليت كامپيوتري نرم افزاري وجود دارد،ممكن است ويروسها نيز حضور داشته باشند .

بديهي است رشد سرطان گونه ويروسها متخصصين امر را بر آن مي دارد كه برنامه هايي براي نابودي آنها تهيه كنند.تا كنون برنامه هاي ضد ويروس زيادي ساخته شده است كه هر يك گروهي از ويروسها را شناسايي و آنها حذف مي كنند .

اين برنامه ها هر يك ويژگيهاي خاصي داشته و براحتي نمي توان ازآنها را به عنوان بهترين ضد ويروس معرفي كرد . متاسفانه به دليل كمبود منابع ، عموم كاربران داخل كشور ازكارايي و نحوه عملكرد برنامه هاي اطلاع كافي نداشته و لذا صرفاً ازآنها به شكل ساده و بدون تنظيمات خاص استفاده كرده و از اين رو در بسياري موارد مشكلات ناشي از وجود ويروسها به طور قطعي حل نمي شوند .

ويروس كامپيوتري چيست ؟

ويروس كامپيوتري برنامه اي است كه مي تواند داده هاي موجود روي ديسك و حافظه RAM را معيوب نموده و در نتيجه از اجراي برنامه ها بطور صحيح جلوگيري به عمل مي آورد .بعضي از ويروسها ي كامپيوتري ضعيف بوده و فقط با نمايش پيغام خاصي خود را نشان داده و صدمه اي به ديسك وارد نمي سازند ولي نوع ديگر ويروس 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. ويروسها كامپيوتري به صورت مخفيانه و از طريق برنامه هايي كه توسط ديسك هاي ديگر يا مودم به كامپيوترتان كپي مي كنيد ،وارد كامپيوترتان مي شوند . اين ويروسهاي كامپيوتري ممكن است مدتها در كامپيوتر شما موجود بوده و فقط به تكثير خود پرداخته و هيچ صدمه اي وارد ننمايند و درساعت و تاريخ و يا هنگام اجراي برنامه خاصي فعال شده وتمام كپي ها ي خود را نيز فعال كنند كه بستگي به ويروس مورد نظر ، صدمات غيرقابل جبراني را وارد مي كنند . ويروس ها اغلب روي فايل هاي اجرايي ديسك عمل نموده وآنها را معيوب مي كنند . ويرس هاي كامپيوتري به صورت برنامه جداگانه اي وجود ندارند بلكه خود را به فايل ها و برنامه هاي ديگر چسبانده و از كامپيوتري به كامپيوتر ديگر منتقل مي شوند .

تا كنون بيش از ۲۰۰۰۰ويروس شناخته شده اند و متخصصين و كارشناسان پس از شناسايي هر يك ازآنها ، نام خاصي را به آنها اطلاق كرده اند .
براي محافظت و سالم نگه داشتن ديسك ، كاربران بايستي ازبرنامه هاي موجود به طور مداوم استفاده نمايند كه يكي از آنها و قويترين شان برنامه Disk Monitor است البته برنامه هاي ديگري در سيتسم عامل Dos و ديگربرنامه هاي سودمند نيز تعبيه شده اند كه عبارتند

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

اگربرنامه هاي حفاظت ازديسك هميشه استفاده نماييد،امكان ورود ويروس هاي كامپيوتري به كامپيوترتان كم شده و در نتيجه سيستم شما سالم خواهد ماند .

در انتها بطور خلاصه مي توان گفت : ويروس 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 كاهش داده باعث اغتشاش و عدم كارايي كامپيوتر شود .

مهمترين خصوصيت ويروس قدرت تكثير آن است ، ويروسها براي تكثير نياز به يك برنامه اجرايي دارند يعني بيشترويروسها درفايلهاي اجرايي جاي مي گيرند و آنها را آلوده مي كنند . كمتر ويروسي پيدا مي شود كه بتواند نسخه هاي اجرايي جاي مي گيرند و انها را آلوده مي كنند و كمتر ويروسي پيدا مي شوند كه ابتدا نسخه هاي اجرايي ازخود را در برنامه هاي ديگر قرار دهد . برنامه آلوده به ويروس مي تواند هر برنامه سيستمي با كاربردي باشد كه شرايط مورد نياز براي پذيرش ويروس را داشته باشد . برنامه آلوده قادر است برنامه هاي ديگر را آلوده كند .

خانه ويروس

ويروس هم مانند هر برنامه كامپيوتري نياز به محلي براي ذخيره خود دارد منتهي اين محل بايد به گونه اي باشد كه ويروسها را به وصول اهداف شوم خود نزديك تر كند .همانطور كه مي دانيد اكثر ويروسها به طور انگل مانندي به فايلهاي اجرايي مي چسبند وآنها را آلوده مي كنند.اصولا دربرخورد با ويروسها ، فايلها ي اجرايي و غير اجرايي تقسيم مي شوند عموم ويروسها در فايلهاي اجرايي جاي گرفته و آنها را آلوده مي كنند و واقعاً كمتر ويروسي هست كه در يك فايل غيراجرايي 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 ويروس در حالت عادي(بدون تنظيم خاص)تنها همين فايلهارا ويروس ياب مي كنند(البته دربرخي برنامه هاي ضد ويروس ممكن است برخي پسوندها حذف و اضافه شوند).-EXE-COM-SYS-BIN-OVL-DLL-SCR

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

(Boot record يا partition) دارند . قطاع بوت واحد راه اندازي Dos است كه در قطاع شماره صفر سخت ديسك يا فلاپي ديسك قراردارد و جدول بخش بندي شامل اطلاعات تقسيم بندي سخت ديسك است كه درآن نيز در قطاع شماره صفر سخت ديسك قرار دارد . اينگونه ويروسها با قرار گرفتن در يكي از اين دو محل به محض روشن شدن كامپيوتر مي توانند به راحتي و به دلخواه كنترل تمامي برنامه هايي كه اجرا مي شوند را در دست بگيرند و حتي به گونه اي عمل كنند كه شماتا مدتها متوجه به حضور آنها نشويد!

محل ديگر ويروسها كه البته موقتي است در حافظه RAM كامپيوتر مي باشد . به محض روشن كردن كامپيوتر و اجراي يك برنامه آلوده به ويروس و يا دسترسي به يك ديسك تا قطاع بوت و جدول بخش بندي آلوده ، ويروس همراه آن در حافظه جا مي گيردو برخي ازآنها تا زمان خاموش كردن كامپيوتر همان جا مانده و فايلهاي ديگر را آلوده مي كنند ولو آنكه شما حتي برنامه آلوده را حذف كرده و فلاپي ديسك آلوده را نيز از ديسك گردان مربوط بيرون بياورند .

ويروسها شناخته شده

ويروس شناخته شده ويروسي است كه قبلا توسط متخصصين كشف شده و مورد تجزيه و تحليل قرار گرفته است .

بدين ترتيب نامي مانند Stonedيا Michelangeloبراي آن انتخاب شده است . همچنين امضايي (Signature) دارد كه يك سري بايت منحصر به فرد دربرنامه ويروس بوده و در شناسايي آن كمك مي كند .

همچنين ويروس ممكن است چند نژاد شناخته شده داشته باشد (يعني گونه هايي در برنامه هاي اصلي آنها تفاوت جزيي وجود دارد.)

تا كنون بيش از ١٠٠٠٠ ويروس شناخته شده است . بسياري ازآنها مدتي است ديده نشده اند و احتمالاً معدوم شده اند ، اما با وجود اين هيچ راهي براي پيش بيني زمان و محل ظهور مجدد آنها وجود ندارند .

انواع ويروسها

ويروس هاي كامپيوتري بسته به نوع تاثيرآنها به سه قسمت تقسيم مي شوند :

الف) Boot Sector

Boot Sectorبخشي ازديسك سخت شماست كه به كنترل چگونگي آغاز سيستم عامل هنگام روشن كردن كامپيوترمي پردازد يك ويروسBoot Sector، Boot Sector اصلي ديسك را برداشته و خود جانشين آن مي شود و ويروس را به حافظه انتقال مي دهد و حضور ويروس در حافظه به مفهوم پخش شدن آن در ديسك هاي ديگر مي باشد .

ب) File infector

ويروس تخريب كننده فايل،ويروس را براي فايلي كه برنامه آن اجرا شده، اضافه مي كند اين اضافه شدن به گونه اي است كه درهنگام اجراي برنامه ويروس فعال شده و فعاليت آن به مفهوم پخش آن درساير فايل هاي برنامه نيز مي شود .

پ)Trogen Hourse

ويروس Trogen Hourse به عنوان برنامه مخرب كامپيوتري مي باشد . بدين ترتيب كه فايل ها و ديسك ها را خراب كرده و قدرت آن ساير انواع ويروس ، بسيار بيشتر مي باشد . فايل هايا ديسك ها را خراب كرده و قدرت آن ازساير انواع ويروس ، بسيار بيشتر مي باشد .فايل ها يا ديسك هايي كه با ويروسTrogen Hourse تخريب شده اند . ممكن است قابل بازيابي نباشند .

انواع ويروس ها نسل جديد

۱- ويروس هاي مقيم در حافظه (Memory Resident Virus)

برنامه مقيم در حافظه، برنامه اي است كه پس از اتمام شدن اجرا ، جاي خود را در حافظه از دست نمي دهد . بيشتر ويروسها پس از فعال شدن مانند برنامه هاي مقيم در حافظه عمل مي كنند ودر حافظه باقي مي مانند .

۲- ويروس هاي استتاري يا نهان (Stealth)

اين ويروسها با روشهاي خاص و بدون تغيير وضعيت ظاهري، عمليات خود را انجام مي دهند و به روشهاي گوناگون رديابي خود را مخفي مي كنند تا شناخته نشوند .

يعني فايل هاي آلوده به اين ويروسها طوري نشان داده مي شوند كه فكر كنيم سالم هستند .

۳- ويروسهاي رمزي (Enctypting Virus)

اين ويروسها براي جلوگيري ازشناسايي خود را بصورت هاي مختلفي رمزي مي كنند . ويروس در ١٢٦٠ يا (Stealth) به صورت كد بوده و به طور تصادفي تغييراتي در كد بندي خود ايجاد مي كند تا روال شناسايي ويروسها را خنثي و بي اثر كند .

ويروس ايراني ((آريا)) به صورت كد شده بر روي فايلهاي آلوده قرار مي گيرد و در ابتداي ويروس ،يك روال رمزگشا ويروس وجود دارد .

٤-ويروسهاي چند شكلي يا هزار چهره (Polymorphic Virus)

كشف اين ويروسها ازهمه مشكل تر است زيرا اين ويروسها پس از هر بار آلوده سازي ، ساختار داخلي خود را تغيير مي دهند و يا شيوه هاي خود رمزي استفاده مي كنند . اين ويروسها هنگام توليد مثل شكل خود را تغيير و تكامل مي دهند . برخي از آنها مي توانند رمز خود را به طور تصادفي تغيير دهند ، بدون آنكه در وظيفه آنها خللي وارد شود .

٥-ويروسهاي انفجاري (Triggerdd event Virus)

اين ويروسها بخشي از عمليات تخريب خود را در ساعت و يا در تاريخ خاصي انجام مي دهند ولي تكثير وآلوده سازي فايل ها درتمام مدت فعال بودن ويروس در حافظه و اجراي برنامه هاي ديگر صورت مي گيرد .

به عنوان مثال ويروس ايراني درTOPGUN چنانچه تاريخ سيستم برابر با روز دوم ماه باشد ،٦٤ بايت اول Ram CMOS را پاك مي كند .

٦- ويروس خود شاخته (Self Modify Virus)

ويروسهايي كه خود را با نسخه هاي قبلي خود درسيستم مطابقت مي دهند ونسخه هاي قبلي خود را Update مي كنند .

٧-ويروسهاي چند قسمتي (Multi partite Virus)

اين نوع ويروسها داراي چند ين قسمت هستند كه هر كدام كار خاصي را انجام مي دهد. مانند برنامه اي كه از چندين روال تشكيل شده است .

عملكرد ويروس

ويروسها عملكرد مختلفي دارند و انچه در مورد همه آنها اشتراك دارد،عملكرد منفي آنها مي باشد. به اين معني كه ويروسها عموما در صدد ايجاد مزاحمت هاي كامپيوتري هستند.اين مزاحمتها گستردگي وسيعي دارند و به راحتي قابل تعريف نيستند . اما به طو كلي مي توان عملكرد ويروس ها را به صورت زير تقسيم بندي كرد :

-ايجاد تاخير وقفه و در حين عمليات سيستم اعم از اجراي برنامه ها و يا راه اندازي كامپيوتر و ...

- تخريب يا حذف برنامه ها و اطلاعات بخشهاي مختلف ديسكها و يا حتي Format كردن ديسكها

- اشتغال حافظه و تكثير در حافظه به نحوي كه در حافظه جايي براي اجراي ديگربرنامه ها نمي ماند .

مزاحمتهاي فوق ممكن است به محض فعال شدن ويروس (يعني قرار گرفتن ويروس در حافظه از طريق اجراي يك برنامه كاربردي آلوده و يا در يك تاريخ و زمان خاص و يا حتي با اجراي يك برنامه كاربردي خاص انجام شود.)

علائم موجود در ويروس

علائم زير معمولا به وسيله ويروسها ايجاد مي شوند . اما ممكن است در اثر عوامل غير ويروسي نيز ظاهر شود .

١) قفل كردن و دادن پيامها ي غير عادي : بعضي از ويروس ها به محض ورود به حافظه،خودشان را چندين بار تكثير مي كنند اين كار موجب ميشود سيستم بسيار كند شود و گاهي نيز قفل كند . بعضي از ويروسها نيز پس از آلودگي پيامهاي گوناگوني به نمايش مي گذارند .

٢) دادن پيامهاي غيرعادي : پاره اي از ويروسها در مراحلي از آلودگي خود پيامهايي را نمايش مي دهند كه نشانه آلودگي سيستم است .

٣) اختلال دركار Printer:يكي ازمواردي كه نشان دهنده آلودگي احتمالي به ويروس است اختلال در كار چاپگر است . اعمالي مانند توقف عمل چاپ و عمل format موقع چاپ يا .. مي تواند نشان دهنده آلودگي سيستم باشد .

٤) صداي غير عادي Speaker: برخي از ويروسها با ايجاد صداهاي غير عادي يا پخش يك موزيك و... آلودگي سيستم را اعلام مي كنند. Atiavri باعث پخش شدن صداي هيس ازبلندگوي كامپيوتر مي شود .

٥) كاهش سرعت سيستم : در صورتي كه زمان بار كردن برخي از برنامه ها به نحوه قابل ملاحظه اي افزايش يابد و يا مدت زمان راه اندازي سيستم ، وقتي كه ازروي

HARD DISKراه انداز ي مي شود،افزايش يابد، و... نشان دهنده احتمال آلودگي به ويروس است .

٦) 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 اگركليد B را فشار مي دهيد علامت كيد مجاورش ، يعني Nروي صفحه نمايش ظاهر مي شود، در اين صورت احتمالا كامپيوتر آلوده به ويروس است .

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

٨) كاهش حجم حافظه : با وجودي كه هيچ برنامه مقيم جديدي بر روي سيستم نصب نشده باشد ، ظرفيت حافظه كاهش يافته است .

٩) تغيير در اندازه فايل ها : طول برنامه ها ي قابل اجرا ،بعني فايل هاي EXE,CIM به اندازه ٤٠٠ تا ٦٠٠٠ بايت تغيير مي كنند .

١٠) اختلال در صفحه نمايش : هنگام اجراي يك فايل يا .... كاراكتر ها و پيا م هاي غير معمول روي صفحه نمايش ظاهر ميشود(ممكن است برخي از اين پيغام ها نام ويروس فعال در حافظه باشد.)

١١) اختلال در SETUP: برخي از ويروسها ، اطلاعات موجود در Setup كامپيوتر را از بين مي برند .

١٢) راه اندازي مجدد سيستم (Restart) : برخي از ويروسها موقع استفاده ازبرنامه باعث RESTART شدن سيستم مي شود .

١٣) خواص فايلهاي اجراي تغيير مي كند .

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

١٥) هنگام كار درمحيط هاي گرافيكي تصاويربر هم مي ريزند .

١٦) هنگام اجراي فايل ها پيغام Fileis Damagedيا File is curropted ظاهرمي شود .

١٧) امكان دسترسي به يكي ازديسك گردانها از بين مي رود .

۱۸) هنگـام اجـراي يـك برنامــه سيســتم قفـل مــي كنــد و گــاهي فشــردن كليـدهاي ALT+DEL+CTRl نيز نمي تواند سيستم راه اندازي كند .

ويروسهاي ناشناخته:

شايد يافتن ويروس هاي ناشناخته مهمتر از ويروس هاي شناخته شده باشد ،زيرا ويروس هاي جديد تا قبل از كشف شدن ، مورد تجزيه و تحليل قرار گرفتن ،نامگذاري و توزيع ويروس يابها ، مدتي ناشناخته مي مانند .

ويروس يابها با جستجوي فايل هاي برنامه اي به دنبال تغييراتي در آنها احتمال آلودگي ويروسي را نشان مي دهند ، ويروس ها ي ناشناخته را پيدا مي كنند . بيشتر فايل ها ي برنامه اي پس از نصب تغيير نمي كنند ، بنابراين وجود هر گونه تغييري در آنها مي تواند نشانگر آلودگي ويروسي باشد .

اولين باري كه ويروس يابها ميكروسافت را در درايوي مورد استفاده قرار دهيد، فايلي به نام CHKLIST.MS در هر فهرستي ايجاد مي كند و اندازه ، صفات ، تاريخ و ساعت تمام فايل هاي برنامه اي فهرست مزبور را درآن فايل ثبت مي كند.

اولين باري كه مقداركنترلي (Check sum) يعني مقدار منحصر به فردي كه از محاسبه محتويات فايل بدست مي آورد را نيز ثابت مي كند. بدين ترتيب اگر محتويات فايل تغيير كند ،مقدار كنترلي آن نيز تغيير مي كند و ويروس ياب ازروي آن مي فهمد كه فايل تغيير كرده است ، جتي اگراندازه ،صفات و تاريخ و سرعت آن ثابت مانده است .

اگر هنگام ثبت داده ها CHKLIST.MS ويروس ناشناخته اي در سيستم وجود داشته باشد شناسايي نخواهد شد . خوشبختانه VSAFE مي تواند با نظارت بر سيستم، جلوي فعاليت مخرب ويروس ها را بگيرد .

پس از تشكيل فايل هاي CHKLIST.MS، هر بار كه عمليات ويروس يابي انجام شود ، ويروس يابي داده هاي ثبت شده را با فايل هاي برنامه اي مقايسه مي كند. هر گونه تفاوتي در آنها باعث مي شود ويروس ياب داده هاي ثبت شده را با فايل هاي برنامه اي مقايسه مي كند . وجود هر گونه تفاوتي در آنها باعث مي شود كه ويروس ياب امكان وجود يك ويروس ناشناخته را گزارش دهد كه در اين صورت بايد فكري به حال سيستم بكنيد.در اين حالت مي توانيد به برنامه ويروس ياب بگوييد كه ازتغيير صرف نظر كند، فايل CHKLIST.MSرا با داده هاي جديد نوسازي كند ، فايل آلوده را پاك كند ، يا عمليات ويروس يابي را متوقف سازد .

ساختار عمومي ويروسها و ضد ويروسها :

سيستم عامل داراي امكاناتي است كه به ويروس نويسان اجازه مي دهد با استفاده از آنها كنترل سيستم را در دست بگيريد، خود را مخفي كنند ، در حافظه مقيم شوند و ....
ويروسهاي كامپيوتري با استفاده از اين امكانات از روشهاي مدرن و پيچيده اي براي آلوده سازي ، مخفي سازي خود و تخريب اطلاعات استفاده مي كنند . يكي از اين ويروسها One half است .
اولين باري كه برنامه آلوده به ويروس ، برروي يك كامپيوتر سالم و غيرآلوده اجرا شود partition Table را آلوده كند . بعد ازان هر وقت كه سيستم با hard disk آلوده راه اندازي مي شود ، ويروس كنترل عمليات ورودي /خروجي را در دست مي گيرد .
در صورتي كه اطلاعاتpartition Table به كلي از بين برود، بديهي است كه سيستم ديگر Bootنمي شود .
وقتي ويروس partition Table را آلوده بعد از آن در هر بار روشن شدن سيستم دور سيلندر از انتهاي hard disk راكد كرده و به ان ترتيب بعد ازمدتي ، حجم زيادي از اطلاعات تخريب مي شوند .

تكنيك هاي آشكارسازي ويروس ها :

يكي از اولين نرم افزارهايي كه بر روي كامپيوتر نصب مي شوند اخرين نسخه نرم افزارهاي ضد ويروس است. هيچ كدام از ضد ويروس هاي زرنگ و باهوش اغلب مي توانند آنها را فريب دهند ولي آنها احتمال آلودگي رابه حداقل مي رسانند و درصورت آسيب ديدن ، كار درمان را ، راحتر مي كنند .
۱-بررسي علامت مشخصه ويروس بانگ الگوي ويروسV irus Pattern database
ساده ترين روش تشخيص ويروس ها نگاه كردن به برنامه آنهاست و بررسي پيام ها ي موجود در انهاست . راه ديگر گشتن به دنبال بايت هاي خاصي ، كه مشخص كننده ويروس هاي خاص است ، مي باشد. كه به آنها رمز مشخصه (Signature) يا امضاء ويروس مي گويند . بنابراين در اين روش همه فايل ها جستجو مي شوند تا علامت مشخص شده ويروس

را پيدا كنند در Boot Sectorآلوده به ويروس ((مغز پاكستاني)) رشته هاي Virus shoe وجود دارد كه ممكن است از اين علامت براي شناسايي اين ويروس استفاده كرد . در انتهاي كليه فايلهاي آلوده به ويروس Mixer 1,2 مي توان رشته حرفي mixl را پيدا كرد . بنابراين در بانگ الگو مي توان از اين علامت ، براي شناسايي اين ويروس استفاده كرد .

٢- بررسي تجربي يا مكاشفه اي (Heuristic Scan)

در اين روش ضد ويروس به دنبال رفتارهاي ويروس مي گردد مثلا به دنبال قطعاتي كه به صورت رمز بوده و خطر آفرين هستند مي گردد . مانند كپي كردن فايل بر روي خودش ، يا به يك فايل ديگر ، يا حذف كردن خودش بدون هيچ اخطاري به كاربر ، در اين روش ممكن است هشدار اشتباه نيز داده شود و نسبت به روش بانك الگوي ويروس ، داراي دقت كمتري است اما براي تشخيص ويروس هاي جديد كه رمز مشخصه آنها هنوز در نرم افزارهاي ضد ويروس وجود ندارد بسيار خوب عمل مي كند .

٣-بررسي درستي مجموع (integrity Checking)

ويروس معمولاً اندازه تاريخ يا مشخصات فايل اجرايي را تغيير مي دهد . بنابراين مي توان با ضبط قبلي و قايسه آن با وضعيت فعلي (CHKLIST.MS)از تغييرات احتمالي كه بوسيله ويروس ايجاد مي شود آگاه شد. اگر ويروس جديد باشد و ضد ويروس آن در دسترس نباشد با اين روش مي توان به شناسايي ويروس هاي جديد نيز پرداخت .

٤- بررسي رمز ژنريك :

در اين روش به جاي جستجوي رمز مشخصه ويروس هاي خاص ، به دنبال الگوهايي مانند دستور العمل هاي پرش نامناسب مي گردد كه به برنامه هاي ويروسي شباهت دارد . اين روش براي كشف ويروس هاي هزار چهره كه مي توانند رمز خودشان را هر بار كه فايل جديدي را آلوده مي كنند ، تغيير دهند ، بسيار كارا و موثر است .

٥-رفتار نگرها :

به رفتارهاي غير عادي و طبيعي داخل كامپيوتر توجه دارند . مانند فايلي كه روي Boot Sector مي نويسد يا HARD DISKرا Format مي كند . وقتي چنين اتفاقي مي خواهد انجام شود ضد ويروس كاربررا آگاه مي كند .

٦-بررسي فازي :

اساس اين روش بر منطق فازي استوار است . با اين روش مي توان دقيقاً به وجودويروسهاي هم شكل و هزار چهره پي برد . ضد ويروسها يي كه بر اساس بررسي فازي كار مي كنند در

تشخيص ويروسها بسيار خوب عمل مي كنند . اما عمليات جستجو را آهسته انجام مي دهند و بروز اشتباه درانها بسيار اندك است.ضد ويروس IBM بر اين اساس كار مي كند و بسياري از ويروسها را تشخيص و نابود مي كند .

روشهاي كلي مبارزه :

جمله معروفي در علم پزشكي مطرح شده است كه پيشگيري از بيماري به مراتب آسانتر از درمان آن است اين سخن تا حدود زيادي درمورد ويروس هاي كامپيوتري نيز صدق مي كند . به اين معني كه در بسياري از مواقع جلوگيري از ورود ويروس به كامپيوتر ساده تر از رفع آن است .

به طور كلي راههاي اصلي براي مبارزه با ويروسها به دو دسته زير تقسيم مي شوند .

۱) شناسايي ويروس ها و جلوگيري از ورود آنها به كامپيوتر

۲) از بين بردن ويروسي كه به سيستم وارد شده و درصورت ايجاد اختلال ، بازگرداندن وضعيت سيستم كامپيوتر و برنامه هايآن به حالت عادي

اجراي دو بند فوق مستلزم شناخت چهره واقعي ويروس ، يعني كد مبدا آنها است هر روز ويروس هاي جديدي با يك كد مبدا آنها شناخته شده و تا برنامه پاك كننده تهيه مي شود ، هزاران برنامه در معرض حمله و تخريب اين ويروس ها قرار گرفته اند .

شركتها ي توليد كننده نرم افزار هاي ضد ويروس زماني ميتوانند برنامه هاي ضد ويروس خود را كامل تر و فراگير تر كنند كه حداقل به ويروس جديد ساخته شده توسط ديگران دسترسي پيدا كنند تا بتوانند با شناخت كد مبدا و نحوه كار آنها برنامه هاي ضد ويروسي مناسب را طراحي نمايند و همه اين مراحل بسيار وقت گير خواهد بود .

بنابراين اگر صرفا به شناخت دقيق ويروس ها اكتفا كنيد هرگز روش مطمئن و فراگيري را نخواهيد يافت و هيچ يك از برنامه هاي ضد ويروس فعلي ادعا ي شناخت همه ويروسها را ندارند .

البته اين به معناي عدم توجه به اثر فوق العاده روشهاي مبارزه اي كه مبتني بر شناخت دقيق ويروس است . نخواهند بود . بلكه منظور آن است كه اگر همين امروزكامپيوتر شما دچار ويروس مخربي بشود كه هيچ ويروس يابي نتواند آن را بشناسد . آنگاه بايد ضرر ناشي

format ديسك سخت ، از بين رفتن برنامه هايي كه ساعتها مشغول طراحي و ويرايش آن بوده ايد و يا حداقل ضرر اتلاف وقت خويش را تحمل كنيد .

براي رفع اين مشكل از دو نكته غير قابل اجتناب زير استفاده شده است :

۱- ويروسها هنگام ورودبه سيستم ناچار بايد روي حافظه ، برنامه و يا ناحيه سيستمي ديسك قرار گيرند و لذا معمولا در سيستم يك حالت نوشتن اطلاعات به وجود آيد كه اين عمل (صرف نظر از نوع اطلاعات) تا حدودي قابل كنترل است .

۲- وقتي ويروسي بر روي ناحيه سيستمي ديسك و يا بر روي برنامه مي نشينند ناچار اندازه، تاريخ يا مختصات فايل اجرايي را تغيير مي دهد . بنابراين مي توان ضبط وضعيت قبلي و مقايسه آن با وضعيت فعلي ازتغييرات احتمالي كه به واسطه ويروس ايجاد شده است،آگاه شد.بنابراين اگر كد مبدا ويروسهاي ناشناخته و يا برنامه ضد ويروس مناسب آنها در دسترس نباشد مي توان به جاي شناسايي ويروس به شناسايي وضعيت فايل ها و مقايسه با حالت قبل پرداخت و ازاين رهگذر تا حدي مي توان به وجود ويروس پي برد. از نكته اول فوق(خصوصيت نياز به نوشتن اطلاعات) براي تكميل روش اول مبارزه يعني جلوگيري از ورود ويروس واز نكته دوم فوق(ضبط ومقايسه وضعيت)براي تكميل روش دوم يعني ازبين بردن ويروس ها استفاده مي شود توجه كنيد كه ضد ويروس هاي قدرتمند انواعي از ويروس هاي فريب دهنده مانند ويروس stealth و ويروس هاي poly Morphic كه هيچ يك از دو اثر فوق ظاهر نمي كنند نيز شناسايي مي كنند .

پاكسازي ويروس ها

پس از اطلاع از وجود ويروس در سيستم ، ادامه كار با سيستم صحيح نيست ، با وجودي كه ممكن است سيستم آلوده به كار خود ادامه دهد . ولي دامنه تخريب آن افزايش پيدا مي كند قبل از پاكسازي ويروس اعمال زير را انجام دهيد .

۱)كامپيوتر را براي مدت ٥ دقيقه خاموش كنيد اين كار داراي مزاياي زير است :

الف- توقف انتشار ويروس

ب- پاك شن ويروس ها مقييم در حافظه

۲)براي محدود كردن دامنه فعاليت ويروس ، لازم است تنها دستگاههاي جانبي كه براي كار با كامپيوتر ضروري هستند به كامپيوتر متصل باقي بمانند و بايد بقيه را قطع كنيد .

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 .

٤) كليه ديسكت ها را در حالت write protectنوشتن مصنوع ، قرار دهيد .

٥) همواره براي انجام عمليات ويروس يابي ، راه اندازي را از Floppy Drive انجام دهيد.

٦) با استفاده از نرم افزار هاي ضد ويروس ،به پاك سازي ويروس ها بپردازيد روش هاي پاكسازي

۱) *آلودگي فايل ها* :درصورتي كه فايل ها hard disk آلوده به ويروس هستند اعمال زير را انجام دهيد :

الف- راه اندازي كامپيوتر با استفاده از يك Floopy disk سالم

ب- بدون دادن هيچ دستوري ، ديسك حاوي ضد ويروس را درون درايو فلاپي ديسك قرار داده و دستور پاكسازي ويروس ها را صادر نماييد .

ج- پس از آن مجددا سيستم را خاموش و روش كرده و مجددا از فلاپي ديسك 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 diskسالم

د- بدون دادن هيچ دستور ديگري ،ديسك حاوي ضد ويروس را درون درايو Floppy diskقرار داده و دستور پاكسازي ويروس ها را صادر نماييد .

ز- براي اطمينان ، راه اندازي مجدد و جستجو براي وجود ويروس

۳) آلودگي فايل ها ،PARTITON,BOOT SECTOR : در اين صورت اعمال زير را انجام دهيد :

الف- راه اندازي كامپيوتر با ي Floppy diskسالم

ب- استفاده از يك ويروس پاك كننده BOOT Sectir 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 هيچ دستور ديگري ،دستور پاكسازي ويروس ها را از روي Floppy disk صادر نماييد .

ز- خاموش و روشن كردن و راه اندازي مجدد كامپيوتر Floppy drive

ژ-اجراي مجدد ضد ويروس براي جستجوي ويروس ها

٤) *آلودگي فايل ها* ، PARTITON TABEL,BOOT SECTORو حافظه : روش پاكسازي در اين حالت ،عينا مانند حالت سوم است . فقط وقتي حافظه آلوده است به هيچ وجه نمي توانيد از ضد ويروس موجود درhard disk استفاده كنيد .

٥) *آلودگي به ويروس ناشناخته* : در اين حالت، درصورتي كه موفق به پاكسازي ويروس نشديد ، يكي از راه حل هاي زير را انتخاب كنيد .

الف-تغيير نام يا حذف فايل هاي ويروسي ازروي disk

ب- استفاده ازبرنامه هاي ويرايش سكتور ديسك

ج- Format وpatition بندي مجدد

ابزارهایی برای افزایش امنیت و سرعت کامپیوتر

WinSpeedUp 2.5.2ابزارهاي موثر در حل مشكلات و بالا بردن سرعت كامپيوتر WinSpeedUpابزارهايي را ارائه مي دهد كه ميتواندبه حل مشكلاتي همچون خرابي Registry Editorبپردازد يا اينكه آيكن هاي راتركيب نمايد.در صورتي كه راه حلی برای اين مشكلات نداشته

باشيد، همين مسائل كوچك و پيش پا افتاده ميتوانند موجب رنجش خاطر شما شوند.قبل از آن كه كار با برنامه WinSpeedUpرا آغاز كنيد، از شما پرسيده مي شود كه آيا كاربر مبتدي هستيد يا حرفها ي .اگر كاربر مبتدي باشيد،برخي گزينهها كه ممكن است خطرات بالقوه بيشتري را به دنبال داشته باشند، غير فعال مي شوند.در مورد تمام كاربران، اين نرم افزار از تنظيمات موجود پشتيبان ميگيرد، به عبارت ديگر چنانچه با انجام هرگونه تغييري وضعيت كامپيوتر نسبت به قبل بدتر شود، ميتوانيد آن را مجدداً به حالت اول بازگردانيد. شما ميتوانيد كامپيوتر خود را بهينه سازي كنيد و فضاي هارد ديسك را بيشتر نمائيد WinSpeedUp.پر از ابزارهاي مفيدي است كه مي توانند همه نوع كاري را از

تغيير ظاهر Internet Explorerگرفته تا پاك كردن Historyانجام دهند و به شما در تنظيم
DirectXكمك نمايند يا اينكه به شما بگويند كه چقدر از حافظه را استفاده كرده ايد.اين نرم افزار داراي يك ابزار برگشت به حالت قبل (roll back) است، به عبارت ديگر تغييراتي كه شما انجام مي دهيد،آسيبي به كامپيوتر نميرساند.با استفاده از بخش Advancedبرنامه WinSpeedUp
ميتوانيد دستورالعملهاي بيشتري را به WindowsExplorer بيافزائيد.

ابزارهای کمکی ویندوزXPTuner 1.05يك برنامه tweak كننده با امكانات بسيار زياد از جمله مزايای ويندوز اين است كه راههاي بسياري براي tweak كردن آن وجود دارد، چه به طريق دستي و چه با نرم افزاري شبيه به . XPTuner زمانيكه اين برنامه را باز مي كنيد،يك پنجره باز ميشود كه تقريباً تمام كارهايي كه ميتوانيد با اين برنامه انجام دهيد را خلاصه ميكند .عليرغم ماهيت پيچيده برخي از tweak ها،ميتوان به وضوح آن ها را شرح داد.نمونهاي از اين tweak ها زماني است كه وارد تب Edit Other Settingsمي شويد .در اين قسمت ابزار بسيار مفيدي وجود دارد كه آيتمها را از پنجره Add orRemove ProgramsدرControl Panel حذف ميكند.
گاهي اوقات زمانيكه نرم افزاري را حذف ميكنيد، آيكن مربوط به آن در Add orRemove Programsباقي ميماند، اما با XPTunerميتوانيد آيكن را حذف كنيد طوري كه ديگر اثري از آن باقی نماند .گرچه تمام اين كارها را می توان به طور دستي انجام داد اما اگر نسبت به انجام آن مطمئن نيستيد، XPTuner داراي ويزاردهايي است كه u1605ميتوانند به شما كمک كنند .اگر جرات و اطمينان لازم را داريد، گزينه هايي وجود دارند كه با آنها ميتوانيد تنظيمات كش را در مور CPUخود تغيير دهيد.

Security and Privacy Pack

از كامپيوتر خود در مقابل تهديدات آنلاين محافظت كنيد و فايلهاي خود را با اين مجموعه امنيتي حفظ نمائيد.
به عنوان يك كاربر كامپيوتر ديگر نميتوانيد نسبت به ايمني آن بي تفاوت باشيد .اين كار درست همانند اين است كه والدين به فرزندان بگويند كه بدون هيچ نگراني از ورود افراد ناشناس به خانه مي توانند منزل را بدون قفل كردن در، ترك كنند. خطراتی كه حريم

خصوصي شما را تهديد ميكنند، ميتوانند از جانب منابع داخلي يا خارجي باشند .به محض اينكه به اينترنت وصل ميشويد، سيستم شما در معرض حملاتي از جمله هكرها، ويروسها، جاسوس افزارها و برنامه هاي بدخواه افزار ديگر قرارميگيرد.

مايكروسافت امكانات امنيتي را در قالب Windows Firewallارائه ميدهد كه در واقع مانع از نفوذ هكرها ميگردد و همچنين Microsoft AntiSpywareرا عرضه ميكند كه كامپيوتر شما را در مقابل جاسوسافزارها و ديگر برنامه هاي ناخواسته محافظت مينمايد.

با وجود اينكه اين دو ابزار از ابزارهاي مفيد و قدرتمندي به شمار ميروند، بهتر است براي كامل كردن امنيت سيستم خود از برنامه هاي ديگر شركتها نيز استفاده نمائيد .به خاطر داشته باشيد كه تهديدات امنيتي فقط منشأ خارجي و بيروني ندارند.اگر اشخاص ديگري به طور فيزيكي به كامپيوتر شما دسترسي دارند، ميتوانند فايل هايي را باز كنند كه در واقع شما نميخواهيد اين فايل ها در دسترس آنها باشد.

Security and Privacy Packاز بهترين نرم افزارهاي طراحي شده در حفظ اطلاعات شخصي است كه كامپيوتر شما را در برابر حملات و آلودگي هاي ناشي از ويروس و ديگر بدخواه افزارها ايمن مي كند. شما مي توانيد براي ايمن كردن سيستم خود از برنامه هاي ديگري نيز استفاده كنيد، اما ما به شرح ۳ برنامه از اين دست اكتفا مي كنيم.

AntiVir PE 6 محافظ ويروس

خطر حمله ويروسها هميشه سيستم مارا تهديد مي كند و هيچ نشانهاي دال بر اين موضوع وجود ندارد كه در آينده نزديک از اين گونه حملات در امان خواهيم ماند .قبل از نصب اين نرم افزار، حتماً بايد به صورت يك كاربر با حقوق اجرا كننده وارد سيستم شويد و نكته مهم ديگر اينكه نرم افزار ضد ويروس ديگري در سيستم نصب نباشد، در اين صورت ممكن است با AntiVir تداخل پيدا كند. اگر از ارتباط تلفني استفاده می كنيد،بالا :كاربرد XPTunerبسيار ساده است،همچنين از طريق آ ن ميتوان به جزئيات بيشتری دست u1610يافت.

اگر مطمئن نيستيد كه كار را از كجا آغاز كنيد، ويزاردهايي وجود دارند كه در اين رابطه به

شما كمك مي كنند.ميتوانيد مولفهDialer-Recognition را نصب كنيد .اين مولفه شما را در مقابل شمارهگيرهاي فريب دهنده كه ميتوانند صورت حسابهاي تلفني كلاني برايتان به ارمغان بياورند، حفظ مي كند.در صورتيكه تعاريف سيستم شما قديمي و منسوخ شده باشند، برنامه AntiVir به شما
هشدار ميدهد و از شما مي خواهد آخرين نسخهها را دانلود كنيد، به اين ترتيب سيستم شما در مقابل آخرين تهديدات و حملات ايمن ميگردد .گزينه زمانبندي اين برنامه به اين معني است كه شما ميتوانيد كامپيوتر خود را در فواصل زماني معين اسكن كنيد تا از نظر وجود مشكل بررسی شود، بنابراين ديگر
نيازي نيست كه انجام اين كار را به خاطر بسپاريد.

Hide My Files 1.0 محدود نمودن دسترسی به فايل

درايو سخت هر كاربر شامل فايلها و اطلاعاتي است كه اغلب بهتر است براي ديگران قابل دسترس نباشند .با استفاده از Hide My Filesميتوانيد دسترسي به هر فولدري كه ميخواهيد از ديد ديگران پنهان بماند را كاملاً غير ممكن نمائيد .اولين باري كه اين برنامه را اجرا مي كنيد از شما خواسته ميشود تا رمز عبوري را وارد نمائيد .بنابراين هر بار كه بخواهيد از اين برنامه استفاده كنيد، بايد اين رمز عبور را وارد كنيد .سپس ميتوانيد از ساختار درختي نوعExplorer براي پيمايش در ميان فولدرهاي خود استفاده نمائيد .بعد به راحتي فولدري را كه مي خواهيد پنهان كنيد، كليك نموده و دكمه Lock را كليك نماييد .اگر برنامه را ببنديد و سعي كنيد به فولدري كه انتخاب كردها يد دسترسي پيدا كنيد، خواهيد ديد كه اين فولدر به پيوندي به Control Panel تبديل شده است .براي دسترسي مجدد، Hide My Foldersرا اجرا نمائيد، رمز عبور خود را وارد كرده فولدر را انتخاب و Unlock را كليك كنيد.

Password Manager XP 1.99.254

ذخيره سازي رمز عبور

بسياري از برنامه ها و وب سايتها از شما ميخواهند كه username و رمز عبوري را وارد كنيد كه پی بردن به آن ها دشوار باشد. با استفاده ازPassword Manager XP 1.99.254ميتوانيد تمام اطلاعات رمز عبور خود را در يك بانك اطلاعاتي رمزگذاري شده كه خود آن نيز توسط رمز عبور محافظت ميشود ذخيره نمائيد، به اين ترتيب شما بايد

براي دسترسي به تمام رمزهاي عبور تنها يك رمز عبور را به خاطر داشته باشيد .برنامه را اجرا كنيد و Database>Create New را كليك نمائيد .تعريفي را براي بانك اطلاعاتي خود وارد كرده و قبل از كليك كردن Ok يک رمز عبور انتخاب كنيد. در كادر سمت چپ، نام بانك اطلاعاتي خود را راست كليك كرده و New Folder را انتخاب نمائيد .شما ميتوانيد براي مرتب كردن رمزهاي عبور خود به صورت طبقه بندي شده از فولدرها استفاده كنيد و همچنين كادر سمت راست را كليك كرده و New Password را انتخاب نمائيد . انتخاب آيكن از منويTitle جستجو و يافت رمزهاي عبور را سادهتر ميسازد.

Spyware Doctor 3.2

ابزار ضد جاسوس افزار

آيا نصب ديواره آتش و ابزار ضد ويروس به معني ايمنی شما در زمان آنلاين بودن است؟ متاسفانه، خير .جاسوس افزارها، مرورگر رباها و برنامههاي آزار دهنده ديگري از اين دست راههاي زيادی براي هجوم و حمله به كامپيوتر شما دارند، به همين دليل داشتن يك ابزار جاسوسي اختصاصي براي از بين بردن آن ها ضروری به حساب می آيد .ابزارهاي جامع اي همچونAd-Aware SE Personal به طور رايگان در دسترس هستند، بنابراين نيازي به خريداري آن ها نيست .اما اگر ثابت شود كه ابزار ضد جاسوس افزار SpywareDoctorدر مقايسه با Ad-Aware موثر و كارآمدتر است، پس ارزشش را دارد كه براي آن هزينه كنيد.مقايسه اوليه اين دو ابزار در مرحله اول آزمايشات ما نتيجه خوبي را به دنبال نداشت. تعداد امضاهاي SpyWare Doctor در بانك اطلاعاتي آن كمتر است) ۲۶۸۴۰ در مقايسه با ۳۰۱۲۲ امضاء .(Ad-Aware بعلاوه اجراي Quick Scanدر Spyware Doctor حدود ۲۵ دقيقه طول مي كشد، در حاليكه اجراي Smart System canمتعلق Ad-Aware در ۶ دقيقه كامل مي شود .امضا در كل بيانگر همه چيز نيست .گرچه Spyware Doctor كندتر است،اما بعضاً به اين دليل مي باشد كه اكثر آبجكت ها را اسكن مي كند) ۱۴۸۵۰۷ در مقايسه با Ad-Aware).۸۹۸۱۶ Spyware Doctorحدود ۱۱۴۱ مشكل را شناسايي ميكند و اين در مقايسه با ۱۴۶ مشكلي است كه Ad-Awareبررسی مينمايد، به همين دليل است كه اسكن كردن در Spyware Doctor بيشتر طول ميكشد.براي از بين بردن كامل جاسوس افزار، ابتدا بايد آن را شناسايي كنيد، در اين صورت تعداد خطرات احتمالي را كه می يابيد حائز اهميت ميگردد .آيا اين به معني برتری Spyware Doctorاست به اين دليل كه اين ابزار ۱۱۴۱ مشكل را شناسايي و

ليست ميكند .ضرورتاً خير، زيرا در بررسی گزارش اسكن مشاهده كرديم كه اين تعداد شامل چندين ورودي به ازاي يك خطر يا تهديد مشابه است .براي مثال، Spyware Doctor به ما اطلاع داد كه NS Keylogger را در سيستم يافته است و اينكه نصب شامل 215 egistry

keyمتفاوت مي باشد .سپس اين ابزار آن ها را به عنوان ۲۱۵ آلودگي شمارش كرده ولی تنها يك برنامه را يافته بود.

مطمئن يا مشكوك؟

تصميم گرفتيم كه بررسي كنيم آيا اين Keyloggerاصلاً نصب شده است يا خير. SywareDoctorوجود Keylogger را در فايلي به نام jmail.dll و ورودیهاي Registryمربوط به آن شناسايي كرد، كه به عقيده ما يک فايل قانونی بودAd-Aware . اين keylogger را شناسايي نكرد، NortonAntiVirus نيز هيچ مشكلي را تشخيص نداد. بعلاوه، Spyware Doctor برنامه بيخطرديگري تحت عنوان TrojanIRC.Comiz را شناسايي كرد كه Ad-Aware يا Norton AntiVirus آن را شناسايي نكردند. به نظر ميرسيد اسكن به درستي يا به طور كاملا صحيح صورت نگرفته است .آيا Spyware Doctorميتوانست با آخرين ترفند خود ما را فريب دهد؟

در اكثر رد يابهای جاسوس افزار، شما بايد هر چند وقت يك بار اسكن را اجرا كنيد، در غير اين صورت شما را بدون هيچ محافظي رها مي كنند .اما اين مسئله در مورد SpywarDoctorصادق نيست Spyware Doctor.شامل OnGuard است كه بطور اختياري تمام وقت كامپيوتر شما را تجت نظر دارد و آلودگيها را به محض تشخيص آنها بلوكه مي كند.مزيت خوبي به نظرميرسد به خصوص كهSpyware Doctor دارای تركيب معقولانهاي از ابزارها است :

بررسي براي يافتن Cookie هاي خطرناك، نصب خودكار برنامه ها براي اجرا در Startupيا شناسايي فرآيندها جاسوس افزار از همان ابتدا .همچنين يك pop-up blockerو رد ياب eylogger نيز در ان وجود دارد.

استفاده بيش از حد از منابع

متاسفانه، اين مسئله به دليل اجراي ضعيف Spyware Doctorكه آن هم به دليل كنترل دائمي تعدادي فايل و رجيستري است، ارزش خود را از دست داده است .بررسی نهايي بيانگر اين است كه Spyware Doctor هر چند ثانيه حدود ۵۰ درصد از منابع CPU را مصرف ميكند و به اين ترتيب موجب كندي عملكردهای ديگر مي گردد.شما مي توانيد با

كاهش بررسيهايي كه توسط ActiveGuard صورت ميگيرد، اين ميزان مصرف از CPU را محدود نمائيد. مسئله ديگر اينكه هنگام اجراى SpywareDoctor متوجه شديم، Smartstore.biz (يك ابزار (e-ommerce ديگر به درستي در صفحه نمايش اصلي به نمايش در نميآيد. اين ابزار از يك پنجره مرورگر پنهان استفاده ميكند كه به نظر ميرسد Spyware Doctor به طريقي آن را بلوكه مينمايد .دردسرهايي نظير اين فاجعه است و اگر در مورد برنامه هاي مشابهاي نظير آن تكرار شود اين ذهنيت را به وجود می آورد كه مشكلاتSpyware Doctorنسبت به مزايای آن بيشتر است.

DisKeeper 9.0

پراكندگي ديسك هرگز

اسكن جاسوس افزار، بلوكه كردن كنترلهای خاصActiveX و محافظت زمان اجرا همگی از يک رابط ساده و مشابه راه اندازی ميشوند. سرعت اسكن كردن زياد نيست اما حداقل زمانبندی آن به اين معناست كه اين برنامه به طور خودكار اجرا ميشود. Spyware Doctorادعا ميكند كه ۱۰۹۰ آلودگی را يافته، پس چرا تنها ۶ آلودگی در اينجا ليست شده است؟ Diskeeperشامل گرافهای نمايشی است كه نشان ميدهند كه پراكندگيها چگونه سرعت و اطمينان پذيری را تحت تاثير قرار ميدهند.

اينقدر ساده، دقيق و سريع نبوده است.

پراكندگي درايو ديسك سخت يكي از دلايلي اصلي مشكلات اجرايي است .ويندوز خود داراي برنامه كمكي يكپارچه سازي است، اما نيازمند يك فرآيند دستي بوده تا از ميزان پراكندگي آگاهي يابد و اجرای آن در درايوهای سخت بزرگ مدت زيادي طول مي كشد. Diskeeper 9.0سريع، ساده و موثر است و داراي امكانات زمانبندي و زمان راه اندازي ميباشد . DisKeeperدرايورهاي شما را پاك ميكند و آنها را به همان صورتی كه هستند يعنی به صورت فشرده سازيشده يا رمز گذاري شده حفظ نموده و فايل ها را در ديسكهاي NTFS پراكنده ميكند .همچنين ميتوان DisKeeper را زمانبندي كرد تا به طور پنهان و غير قابل رويت به صورت يک برنامه زمينها ي اجرا گردد يا به عنوان يک يكپارچهساز (defragmenterدستی، فايلها را دو باره مرتب كند و فضاي ديسك را خالي نمايد. اين رابط مرتب و كار با آن ساده ميباشد. مولفه هاي موجود اين امكان را فراهم ميسازند تا وجوه مختلف وضعيت ديسك خود را ببينند و در زمان اجراياDisKeeper آن ها را كنترل نمائيد و به ويژگي ها و ميان برهايي كه معمولاً استفاده ميشوند، دسترسي يابيد.

انتقال دادهها

ويژگي " Set it and Forget it " يكي از مفيدترين ويژگي هاي اين نرم افزار است .با اين ويژگي DisKeeper به طور خودكار با يك زمانبندي از پيش تعيين شده در زمينه اجرا ميگردد .همچنين ميتوانيد از گزينه SmartScheduling استفاده كنيد تا اين نرم افزار به طور خودكار بهترين زمانبندي يكپارچهسازي را براى ديسك هاي شما تعيين كند .شما ميتوانيد مطابق با نياز خود روشهاي مختلف يكپارچه سازي را انتخاب نمائيد. از جمله ويژگيهاي ديگر اين نرم افزار Boot-Time defragmentaionاست كه دايركتوريها را به يك محل منتقل ميكند. اين ويژگي اهميت خاصي دارد زيرا ويندوز دايركتوريها را در محلهاي اتفاقي در سراسر يك ديسك مينويسد و در حقيقت، فضاي خالي ديسك را تكه تكه مي كند. با گروه بندي تمام دايركتوريها در يك محل، امكان دسترسي به فضاهاي خالي بزرگترو پيوسته بيشتر ميگردد .بنابراين، فايلهاي جديد به طور پيوسته در ديسك نوشته ميشوند .اين كار همچنين موجب يكپارچه سازي Master File Table ميگردد كه بخش مهم و حساس پارتيشنهاي ديسكNTFS ويندوز است.

Registry Machanic 4.0

پاك كردن رجيستري موجب بهبود عملكرد و افزايش ثبات كامپيوتر مي گردد.

زمانيكه برنامههاي كاربردي زيادي را نصب ميكنيد، اين برنامهها u1608 ورودیهاي جديد زيادي

را به Registry شما ميافزايند :تنظيمات برنامه، پيوندهاي فايل، فونتها، ورودي Add/Remove Programsو بسياري ديگر.

البته اگر در صورت حذف برنامه كاربردي تمام اين موارد همگی حذف شوند بسيار خوب وعالی است .متاسفانه، چنين چيزي ندرتاً اتفاق ميافتد و نتيجه نهايي Registry ای است كه با استفاده از كامپيوتر بزرگ تر و كندتر ميگردد. نيازي نيست اين وضعيت را تحمل كنيد .با اجراي Registry Machanic ، رجيستري شما اسكن شده، خطاها برطرف و تمام ورودييهاي بدرد نخود حذف ميگردند. همچنين اين برنامه منوى Start شما را چك ميكند تا ميانبرهاي احتمالي به اين فايل را حذف نمايد.معمولاً وجود برنامههايي كه با رجيستري ما سرو كار دارند و آن را دست كاري ميكنند موجب رنجش ما ميگردد، اماRegistry

Mechanicدر اين رابطه داراي دو لايه محافظتي است .اولاً اين برنامه از تمامكليدهاي رجيستري كه تغيير داده ميشوند پشتيبانگيری ميكند، بنابراين ميتوانيد در صورت نياز دوباره آنها را برگردانيد .دوماً، كاربران ويندوز XP ميتوانند قبل از هرگونه اصلاح يا تغييری يک System Restore تنظيم كنند تا در صورت بروز مشكل آنها را بازيابي كنند.

فرآيند اسكن

برای آزمايش، از اين برنامه در كامپيوتر خود استفاده كرديم، اسكن كامل كامپيوتر حدود ۱۴ دقيقه

طول كشيد و بالاخره ۱۹۲ مشكل را گزارش كرد. اگر بخواهيد بررسيهاي كمتري صورت بگيرد،

اسكن سريع تر انجام ميشود .در مقايسه با اين برنامه،RegistryFirst Aid (www.rosecitysoftware.com) تقريباً در ۶ دقيقه ۱۲۲۵ مشكل را در ارتباط با رجيستري ما شناسايي كرد .بعلاوه، Registry TuneUp (www.acelogix.com) ظرف ۳ دقيقه و ۲۹ ثانيه در صورت بروز هر گونه اشتباهي، از پشتيبان هايRegistry Mechanicميتوان براي بازگرداندن رجيستري استفاده كرد. مدعي تشخيص ۱۳۲۵ مشكل رجيستري گرديد. Registry Machanic از نظر سرعت نسبت به دو برنامه ديگر پائين تر است، اما شمارش مشكلات نمايانگر بالا بودن كيفيت برنامه نيست.

Registry First Aid و Rgistry TuneUp با اين فرض كه كليدهاي خالي رجيستري خطا

هستند و ميبايد حذف شوند، مشكلات بيشتری را شمارش ميكنند .يك برنامه كاربردي ممكن است

با بررسي وجود يك كليد، اطلاعات مفيدي بدست بياورد .بنابراين روش Registry Mechanicكه كاری به كار اين ورود‌يها ندارد مطمئن تر است.

كار پر مخاطره

پس از اتمام كار اسكن،Registry Mechanic مشكلات را در گروههاي مختلف نشان ميدهد .سپس كاربر ممكن است بخواهد هر مشكل را به نوبت مرور كند و مشكل هر ورودي را حل و يا آن را به همان صورت باقي بگذارد .اگر برنامه صدها u1605 مشكل را بيابد،احتمالاً گزينه ساده تر را انتخاب خواهيد كرد، Repairرا كليك كنيد و Registry Mechanic را فعال نمائيد تا تمام مشكلات را حل كند. آيا روش خوبي است؟ احتمالاً خير . Registry Mechanicتنها پاك كنندهايي است كه يک ورودي برنامه (dumprep

(Startupرا نادرست شناسايي مي كند و آن را براي حذف كردن علامت گذاري مي نمايد. شايد علت آن اين است كه برنامهRegistry Mechanic به دنبال فايلي به نامdumprep است، در حاليكه نام واقعي dumperp.exe مي باشد؟

گرچه ويندوز اهميتي به اين موضوع نمي دهد : اين فايل يك فايل قانوني است كه براي گزارش فايل خطا به كار مي رود، با اين وجود Registry Mechanicدر زمان راه اندازي كامپيوتر اجراي آن را متوقف ميكند .البته اين مورد خيلي مهم نيست، اما اگر موارد مهم تری را بدون اطلاع شما حذف كند چه؟ بايد گفت كه مزاياي حذف اين ورودیهاي اضافي رجيستري بسيار مهمتر از مشكلاتي است كه ممكن است با يک حذف نادرست به وجود بيايد.

System Mechanic 5

كامپيوتر خود را برای اجرای راحتتر و روان تر، تنظيم كنيد

حتي سرعت عمل ما نيز با گذشت زمان و بالا رفتن سن، پائين ميآيد و ويندوزXP مايكروسافت نيز از اين قاعده استثناء نيست. دادههای ناخواستها ی كه پس از هربار استفاده از كامپيوتر در آن انباشته مي شوند، اگر دست نخورده باقی بمانند حقيقتاً ميتوانند مشكلاتي را به دنبال داشته باشند .بنابراين لازم است فرصتي به كامپيوتر داده شود تا بقاياي ديجيتالي را پاك كند و درايو سخت و حافظه كامپيوتر شما را به شكل اوليه خود بازگرداند. ده ها بلكه هم صدها برنامه برای انجام اين كار وجود دارند و ممكن است شما نيز يكي دو برنامه از اين دست در كامپيوتر خود نصب كرده باشيد .پس System Mechanic 5 بايد امكان خاصي را ارائه دهد تا آن را از ديگر برنامهها متمايز نمايد .اين برنامه كارهاي ارزشمندي همچون tweakكردن رجيستري، پاك كردن فايل هاي موقت و يكپارچه سازي

ديسك سخت را انجام مي دهد كه البته اين ويژگيها را ميتوان در برنامههاي ديگری نيز يافت . ويژگيهاي ديگري همچون ابزارهاي ضد جاسوس افزار، پاك كردن تاريخچه اينترنت و بلوكه كردن pop-up ها را نيزميتوان در Sevice Pack2 و بتاي برنامه ضد جاسوس افزار جديد مايكرسافت يافت.بهرحال، اين نسخه شامل ويژگي هاي جديدي است .يكپارچه ساز جديد زمان راه اندازي كه قبل از راه اندازي ويندوز فايل هاي اصلي سيستم را مرتب ميكند يك ويژگی عالي و ماهرانه است، و در صورتيكه با برنامه هاي كمكي ديگر همراه شود، موجب ارتقاء عملكرد سيستم شما مي گردد.

مهمترين ويژگي Service Mechanic 5 اين است كه تمام اين ويژگي ها را در يك رابط ساده ادغام ميكند .در اين صورت ديگر مشكل نصب برنامههاي مختلف و مجزا را نداريد . بعلاوه اين برنامه قابل اطمينان بوده و شامل تمام آن چيزهائي است كه شما نياز داريد و

اجرای آن مقرون به صرفه می باشد.اسکن کامل رجيستري حدود ۱۴ دقيقه طول مي كشد. براي آنكه كار مرورکردن ساده تر شود، مشكلات در گروه هاي مختلف گروه بندي مي شوند.

منابع:

www.persian blog.com
www.irandevelopers.com
www.zendagi.com
www.frontpageworld.com

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

با تشگر از دانلود این کتاب