

ویروس و برنامه‌های ضدویروس

پس از آموزش این فصل، هنرجو می‌تواند:

- انواع برنامه‌های مخرب را توضیح دهد.
- مشخصات کلی برنامه‌های ضدویروس را توضیح دهد.
- روش کار با انواع برنامه‌های ضدویروس را توضیح دهد.
- با برنامه ضدویروس متداول کار کند.

با توجه به پیشرفت فناوری اطلاعات و رایانه‌ای شدن انجام کارها در زندگی روزمره حجم داده‌های ذخیره شده رو به افزایش است. و این مسئله وابستگی زیادی را بین انسان و رایانه بوجود آورده به طوری که قطع این وابستگی در برخی موارد غیرممکن می‌نماید. به‌عنوان مثال فرض کنید که کلیه سوابق تحصیلی یک دانش‌آموز یا سوابق پرسنلی یک کارمند که در رایانه ذخیره شده است ناگهان از بین برود. یا دستیابی به آن غیرممکن شود. در چنین مواردی جبران خسارت تقریباً غیرممکن است. لذا برای حفظ داده‌ها باید راه کارهای خاصی را در نظر گرفت که ضمن کاهش احتمال از دست دادن آنها امکان بازیابی وجود داشته باشد.

امروزه در حوزه رایانه برنامه‌های مخرب (مانند ویروس‌های رایانه‌ای) خطر بزرگی برای داده‌ها و برنامه‌ها هستند که می‌توانند به‌طور ناخواسته اطلاعات را تخریب کنند و عملکرد رایانه را تحت تأثیر خود قرار دهند. در برخی از موارد حتی اگر رایانه ما مجهز به آخرین تکنولوژی ضدویروس باشد باز هم ممکن است که در برابر حمله یک برنامه مخرب جدید نتواند از خود حفاظت کند. به‌عنوان مثال برنامه مخرب Blaster در زمان بسیار کوتاهی روی تمامی رایانه‌ها و سرویس‌دهنده‌های اینترنت سراسر دنیا تکثیر شد به طوری که در لحظات اولیه حمله حتی سازمان‌های امنیتی بزرگ در کشورهای توسعه یافته هم نتوانستند در برابر آن

۷-۱- برنامه‌های مخرب

برنامه‌های مخرب برنامه‌هایی هستند که موجب مختل شدن عملکرد رایانه، کاهش کارایی و حتی از بین رفتن برنامه‌ها یا داده‌ها می‌شوند هم‌چنین دست‌یابی یا سوءاستفاده از رایانه یا داده‌ها را برای افراد غیر مجاز فراهم می‌کنند.

برنامه‌های مخرب با توجه به چگونگی اجرا، تکثیر و عملی که روی رایانه انجام می‌دهند به دسته‌های مختلفی تقسیم می‌شوند. برخی از برنامه‌های مخرب عبارت‌اند از ویروس، اسب تروا، هرزنامه، کرم

۷-۱-۱- ویروس‌های رایانه‌ای (Virus): ویروس برنامه‌ی کوچکی است که می‌تواند با تکثیر خود، از یک رایانه به رایانه دیگر منتقل شود. ویروس‌ها عملکرد رایانه را مختل کرده و مانع از اجرای درست سایر نرم‌افزارهای رایانه‌ای می‌شوند. هم‌چنین ویروس‌ها می‌توانند باعث خرابی اطلاعات یک پرونده شوند یا حتی یک پرونده را به‌طور کامل از بین ببرند. برخی از ویروس‌ها با اتصال به یک برنامه اجرایی و آلوده کردن آن با هر بار اجرای برنامه توسط کاربر فعال شده و شروع به تکثیر و تخریب کنند. امروزه فناوری ساخت برنامه‌های مخرب به گونه‌ای پیشرفت کرده که آن‌ها را قادر می‌سازد حتی پرونده‌های صوتی و تصویری یا متنی را نیز آلوده کنند.

برخی از ویروس‌ها ممکن است برای مدتی بدون انجام فعالیت‌های مخرب، خود را از دید کاربر پنهان کنند و تا مدت‌ها روی رایانه باقی بماند سپس در تاریخ مشخصی یا با انجام عملی خاص توسط کاربر یا سیستم، فعال شوند. نمونه‌ای از این ویروس‌ها Autorun.inf است. که در شرایط عادی هیچ عملکردی از خود ندارد اما هر بار که اقدام به کپی اطلاعات روی دیسک نوری کنید. این ویروس ناخواسته به دیسک نوری کپی می‌شود و در صورت استفاده از آن دیسک، ویروس به رایانه منتقل شده و از طریق برنامه ویندوز اکسپلور در رایانه قربانی اجرا شده، عملکرد تخریبی خود را شروع می‌کنند. بعضی از برنامه‌های مخرب به نام ویروس‌های چندریختی^۱ برای آن که شناخته نشوند به صورت دوره‌ای یا تصادفی خودشان را تغییر می‌دهند. مانند Sality.AM که پرونده‌های با پسوند exe و scr را مورد حمله قرار می‌دهند.

۷-۱-۲- اسب تروا (Trojan Horse): اسب تروا برنامه‌ای است که ناخواسته هنگام

۱- Polymorphism

دریافت اطلاعات از اینترنت به وسیله کاربران یا از طریق حافظه‌های جانبی نظیر دیسک‌ها روی رایانه منتقل می‌شود و معمولاً پس از نصب، عملکرد مخرب خود را نشان می‌دهد. برخلاف ویروس‌های رایانه‌ای که خودشان منتشر می‌شوند اسب‌های تروا چنین قابلیت‌هایی ندارند.

به‌طور کلی اسب تروا شامل دو بخش است. بخش سرویس‌گیرنده که روی رایانه شما نصب می‌شود و دیگری بخش سرویس‌دهنده که در رایانه حمله‌کننده قرار دارد. بخش سرویس‌گیرنده ممکن است خود را به شکل یک نرم‌افزار مهم در شبکه یا سایت‌های غیررسمی قرار داده باشد و توسط کاربران دریافت شود. زمانی که این بخش در سیستم قربانی اجرا شود، حمله‌کننده که در این‌جا دسترسی بالایی روی این سیستم دارد می‌تواند بسته به نیت و هدف خود حمله کند و تأثیرات مخربی را روی آن بگذارد.

اسب‌های تروا بر اساس عملکردشان به چند دسته تقسیم می‌شوند که برخی از آن‌ها عبارتند

از :

- تروای دسترسی از راه دور (Remote Access Trojans)
- تروای ارسال داده و گذر واژه (Data And Password Sending Trojans)
- تروای ثبت رویدادهای صفحه کلید (Key logger)
- تروای مخرب داده (Destructive Trojans)
- تروای پروکسی (Proxy Trojans)
- تروای اف تی پی (FTP Trojans)
- تروای غیرفعال‌کننده برنامه‌های امنیتی (security software disabler Trojans)
- تروای رد سرویس (denial-of-service attack (DoS) Trojans)

قالب اکثر پرونده‌های حاوی اسب تروا، «.exe»، «.vbs»، «.com»، «.bat» است گاهی ممکن است که یک پرونده با قالب .jpg. به صورت پست الکترونیکی دریافت شود و پس از اجرا عکسی مشاهده نشود، در واقع قالب اصلی این پرونده .exe است که با نام *.jpg.exe ارسال شده است اما چون ویندوز به‌طور پیش فرض پسوند پرونده‌هایی را که می‌شناسد نشان نمی‌دهد، و در این حالت پسوند EXE بوسیله ویندوز شناسایی می‌شود نشان داده نشده و دریافت‌کننده پرونده، آن را نوعی پرونده تصویری شناسایی می‌کند و از ماهیت اصلی آن پرونده که اجرایی و مخرب است بی‌اطلاع می‌ماند. پس گاهی ممکن است که یک پرونده حاوی اسب تروا به‌ظاهر بیش از یک پسوند داشته باشد.

پژوهش

در مورد انواع تروا و عملکرد آن‌ها بررسی و نتیجه را در کلاس ارائه کنید.

برخی از اقدامات برای جلوگیری از آلوده شدن سیستم به اسب تروا

■ از اشخاصی که به آن‌ها اعتماد ندارید یا محل‌های اینترنتی غیرمعتبر پرونده‌ای دریافت نکنید.

■ پرونده‌هایی که از طریق پست الکترونیکی از طرف دوستانتان دریافت می‌کنید ممکن است آلوده باشد. مخصوصاً اگر پرونده‌های مذکور با عنوان و پیوست غیر مرتبط همراه باشد. زیرا برخی از اسب‌های تروا این قابلیت را دارند که خود را از طریق پست الکترونیکی منتشر کنند و بدون این که فرستنده‌ای که نام آن به عنوان فرستنده اعلام شده، اطلاع داشته باشد، پرونده‌های حاوی تروا از طرف آن‌ها برای شما ارسال شده است.

■ بهتر است سیستم عامل ویندوز را طوری تنظیم کنید که پسوند همه پرونده‌ها را نشان دهد.

■ از نرم افزارهایی که بطور خودکار محتویات پرونده‌ها را باز می‌کنند استفاده نکنید. بعنوان مثال در برنامه Outlook امکانی وجود دارد (Preview Mode) که تمامی پرونده‌های پیوست نامه را اجرا کند بهتر است این حالت همیشه غیر فعال باشد.

■ برخی از کدها اگر در مرورگرها اجرا شوند ممکن است مخرب باشند. لذا کدها و دستوراتی که دیگران در اینترنت به شما می‌دهند را نباید به صورت ناآگاهانه اجرا کنید به عنوان مثال فرد ناشناسی از شما می‌خواهد کدی را در نوار آدرس مرورگر خود وارد و اجرا کنید، که نباید به آن خواسته توجه کنید؛ زیرا ممکن است این کد مخرب و خطرناک باشد. یکی از این خطرات ارسال نام کاربری و گذرواژه شما برای او است.

نکته

وجود ضدویروس نمی‌تواند مانع از آلوده شدن سیستم به تروا شود. در واقع ضدویروس‌ها در نقطه جلویی امنیت رایانه قرار ندارند. بلکه آن‌ها به عنوان یک پشتوانه امنیتی در برابر حرکات پنهانی بعضی از نرم افزارهای مخرب عمل می‌کند.

برای پاک کردن اسب تروا از سیستم می‌توان از برنامه‌های Anti Trojan استفاده کرد در صورت موفقیت‌آمیز نبودن روش اول باید مجدداً سیستم عامل و نرم افزارهای مورد نیاز را نصب کنید. اگرچه این کار بسیار وقت‌گیر و دشوار است اما قالب بندی دیسک سخت و نصب مجدد سیستم عامل و برنامه‌های کاربردی یکی از بهترین راه حل‌ها، برای رهایی از تروا است.

۳-۱-۷- جاسوس‌ها (Spyware): برنامه‌هایی هستند که بدون اطلاع کاربر، اطلاعاتی را از سیستم جمع کرده و آن‌ها را به آدرس‌های مشخصی ارسال می‌کنند. با توجه به آن که معمولاً این ویروس‌ها به رمز درآمده‌اند، نرم‌افزارهای ویروس یاب نمی‌توانند به صورت مستقیم آن‌ها را شناسایی کنند، اما می‌توانند با شناسایی بخش رمزگشا، نسبت به شناسایی این ویروس اقدام کنند.

۴-۱-۷- کرم‌ها (Worm): برنامه‌هایی که با استفاده از شبکه، کپی‌هایی از خودشان روی دیگر رایانه‌ها می‌فرستند ممکن است بدون اطلاع کاربر باشد و برخلاف ویروس‌ها به برنامه‌های اجرایی دیگر متصل نمی‌شوند. کرم‌ها تقریباً همیشه با پترافیک کردن شبکه باعث صدمه زدن به آن می‌شوند. این نوع از برنامه‌های مخرب ممکن است اطلاعات رایانه میزبان را تخریب یا امکان سوءاستفاده از آن‌ها را برای افراد سودجو فراهم کنند.

کنجکاوی

عملکرد کرم‌های زیر را بررسی و نتیجه را در کلاس ارایه کنید.

نام کرم	تاریخ انتشار
Win32/Sasser	January 2005 (V 1.0)
Win32/Busky	July 2007 (V 1.31)
Win32/Virut.A	August 2007 (V 1.32)
Win32/Virut.B	August 2007 (V 1.32)
Win32/Ldpinch	February 2008 (V 1.38)
Win32/Virtumonde	March 2008 (V 1.39)
Win32/Vundo	March 2008 (V 1.39)

۵-۱-۷- هرزنامه (Spam): هرزنامه‌ها، نامه‌های الکترونیکی ناخواسته‌ای هستند که از طرف اشخاص ناشناس دریافت می‌شود. این نامه‌ها از لحاظ محتوا و موضوع معمولاً جنبه تبلیغاتی تجاری دارد و برای گروه زیادی از کاربران ارسال می‌شود. اشخاص با ارسال این نامه‌ها، قصد هدف قرار دادن رایانه و کاربر را دارند و حتی در برخی از موارد امکان دسترسی کامل رایانه از طریق شبکه به فرستنده نامه داده می‌شود.

در حال حاضر سرویس‌دهنده‌گان سرویس پست الکترونیک مجهز به سیستم Anti Spam هستند و قادرند از ورود هرزنامه‌ها به پست الکترونیک ممانعت به عمل آورند. اما باز هم امکان دارد که بتوانند تمامی هرزنامه‌ها را شناسایی کنند. در چنین مواقعی استفاده از برنامه Anti Spam روی رایانه ضروری است.

۲-۷- روش‌های انتقال برنامه‌های مخرب

معمولاً انتقال برنامه‌های مخرب از دو راه امکان‌پذیر است: حافظه‌ی جانبی و شبکه. انتقال ویروس از طریق حافظه‌ی جانبی زمانی رخ می‌دهد که بخشی از اطلاعات را روی دیسک نوری یا حافظه فلش یا هر نوع حافظه جانبی دیگری کپی و آن‌را به رایانه دیگری منتقل کنیم. در این صورت با اجرای پرونده‌های آلوده به برنامه مخرب سایر اطلاعات رایانه نیز آلوده می‌شوند.

امروزه با توجه به گسترش استفاده از شبکه‌های رایانه‌ای، معمولاً ارسال و دریافت اطلاعات از طریق شبکه انجام می‌شود. امروزه شبکه اینترنت بستر مناسبی برای ایجادکنندگان برنامه‌های مخرب شده است و بیشتر حملات خود را به رایانه‌ها از این طریق انجام می‌دهند.

۳-۷- نفوذگر (Hacker)

نوع دیگری از تخریب اطلاعات که ممکن است همیشه رایانه‌های متصل به شبکه را تهدید کند، برنامه‌های نفوذگر هستند. افراد می‌توانند با استفاده از برنامه‌های نفوذگر از طریق شبکه وارد رایانه‌ها شوند. امروزه افرادی را که با استفاده از امکانات شبکه و برنامه‌های مخرب وارد رایانه می‌شوند را تحت‌عنوان هکر می‌شناسیم. وقتی رایانه شما به شبکه اینترنت متصل می‌شود، می‌توانیم با هر رایانه دیگری که به شبکه متصل است ارتباط برقرار کنیم، اما این ارتباط به این معنی نیست که ما مجاز

باشیم که از تمام اطلاعاتی که در دیگر رایانه‌هاست، استفاده کنیم. چرا که اگر واقعاً چنین بود، در این صورت هیچ امنیتی وجود نداشت. و همه به راحتی می‌توانستند به اطلاعات مربوط به حساب‌های بانکی رایانه‌های بانک‌های بزرگ جهانی دسترسی پیدا کنند و با تغییر اطلاعات، از آن‌ها پول برداشت کنند. یا این‌که هر کسی می‌توانست به اطلاعات شخصی و محرمانه‌ای که در رایانه‌تان ذخیره کرده‌اید، دست یابد.

کسانی که به قصد نفوذ وارد رایانه‌ها می‌شوند. به ۳ گروه هکر، واکر و کراکر تقسیم‌بندی می‌شوند. هکرها و White Hat ها اشخاصی هستند که فقط به داخل رایانه‌ها نفوذ می‌کنند بدون این‌که به کار خاصی پردازند و بیشتر هدف‌شان این است که به شما اعلام کنند سیستم امنیتی شما چه قدر در مقابل آن‌ها ضعیف است. اما واکرها وارد رایانه شما شده و از اطلاعات موجود در آن استفاده می‌کنند.

گروه سوم، یعنی کراکرها و Black Hat ها خطرناک‌ترند، چون وقتی به رایانه شما نفوذ کنند اطلاعات موجود در آن را تخریب می‌کنند.

برای این‌که بتوانیم از ورود نفوذگران به داخل رایانه جلوگیری کنیم. باید بتوانیم کلیه درگاه‌های ورودی و خروجی رایانه را کنترل کنیم و سعی کنیم آن‌هایی را که نیاز نداریم ببندیم و یا آن‌ها را همواره تحت کنترل خود درآوریم. برای رسیدن به این هدف همیشه باید از دیوار آتش امنیتی استفاده کنیم که مانند فیلتر میان درگاه‌های رایانه و شبکه قرار گیرد. به این دیوار آتش امنیتی فایروال Firewall گفته می‌شود. فایروال‌ها معمولاً دو نوع نرم‌افزاری و سخت‌افزاری هستند. فایروال‌ها قابلیت برنامه‌ریزی و کنترل دارند و با توجه به تنظیمات انجام شده می‌توانند از ورود و دسترسی‌های غیر مجاز جلوگیری کنند.

نکته

فایروال‌ها دارای توانایی حفاظتی نسبت به نفوذگران، ویروس‌های پست الکترونیکی، اسب‌های تروا هستند. و هیچ موقع نمی‌توان از آن‌ها به‌عنوان برنامه ضدویروس استفاده نمود.

۴-۷- برنامه‌های ضدویروس

امروزه با وجود تنوع زیاد برنامه‌های مخرب الزاماً باید برای مقابله با اثرات برنامه‌های مخرب

مخصوصاً ویروس‌ها از برنامه‌هایی که برای این منظور تولید می‌شوند استفاده کرد.

۱-۴-۷- مشخصات کلی یک برنامه ضدویروس : شناسایی یک برنامه ضدویروس باید

بر مبنای مشخصات و توانمندی‌های آن‌ها و متناسب با مشکلاتی که با آن روبه‌رو می‌شویم انجام شود. برخی از مشخصات کلی یک برنامه ضدویروس عبارتند از :

- **ثبت پرونده آلوده یا Submit :** در یکی از مهم‌ترین عواملی که باید در هنگام تهیه یک برنامه ضدویروس به آن توجه داشت، شرکت تولید کننده برنامه ضدویروس می‌باشد. به دلیل این که ارزش یک برنامه ضدویروس به پشتیبانی درست و به موقع آن می‌باشد. به عنوان مثال امکان دارد که روی رایانه یک پرونده آلوده به ویروس وجود داشته باشد که برنامه ضدویروس قادر به پاک‌سازی آن نباشد. برنامه ضدویروس باید امکان Submit پرونده آلوده را به سرور اصلی شرکت تولید کننده داشته باشد. تا در کوتاه‌ترین زمان بتواند پرونده آلوده را پاک‌سازی کند. و نتیجه آن را برای رایانه ارسال کند.

- **به روز رسانی خودکار :** برنامه ضدویروس باید بتواند مطابق با زمان‌بندی خاصی که روی آن تعریف می‌شود به شبکه وصل شود و بانک اطلاعات خود را به روز کند. بهتر است که حجم اطلاعات به روز رسانی کم باشد. تا کاربرانی که با خط تلفن به شبکه وصل می‌شوند نیز بتوانند اطلاعات را دریافت کنند. در حال حاضر بعضی از برنامه‌های ضدویروس در هنگام به روز رسانی فقط آخرین تغییرات را دریافت می‌کنند اما برخی دیگر کل بانک اطلاعات ویروس را دریافت می‌کنند که این کار به راحتی انجام نمی‌شود. و نیاز به خطوط اینترنت پر سرعت دارد. یکی از بهترین امکاناتی که برخی از برنامه‌های ضدویروس از آن پشتیبانی می‌کنند. قابلیت Intelligent Update می‌باشد. در بخش‌های بعدی آن را توضیح می‌دهیم.

- **مصرف کم منابع رایانه :** عملکرد رایانه را تحت تأثیر خود قرار ندهد. برخی از برنامه‌های ضدویروس سرعت سیستم عامل را بیش از اندازه کند می‌کنند و کاربر به راحتی نمی‌تواند برنامه‌های خود را اجرا کند.

- **هوشمندی Smart :** معمولاً برنامه‌های ضدویروس از روی بانک اطلاعاتی که به همراه دارند ویروس‌ها را شناسایی می‌کنند و از بین می‌برند. خوب مسلم است اگر برنامه ضدویروس به پرونده آلوده‌ای برخورد کند و در بانک اطلاعات خود آن ویروس را نداشته باشد. نمی‌تواند آن را از بین ببرد. اما اگر برنامه ضدویروس بتواند از روی رفتار و عملکرد پرونده‌های در حال اجرا آن‌ها را شناسایی کند. (با توجه به الگوریتم‌های از پیش تعیین شده) بهتر می‌تواند برنامه‌های مخرب را

شناسایی و از بین برد.

۲-۴-۷- مقایسه چند ضدویروس متداول: به طور کلی نمی توان گفت که کدام یک

از برنامه های ضدویروس بهتر یا قوی تر است، چرا که فناوری تمامی این برنامه ها روز به روز در حال پیشرفت است و شرکت های تولیدکننده هر روز روش های جدیدتری را برای مقابله با ویروس ها پیدا می کنند. به عنوان مثال ضدویروس AVG امکان دارد از لحاظ قدرت نسبت به سایر انواع خود پایین تر باشد. اما به لحاظ رایگان بودن، نسخه خانگی آن محبوبیت بیشتری را نسبت به سایر انواع ضدویروس دارد.

جدول ۱-۷- مقایسه چند برنامه ضدویروس

ضدویروس ها							ویژگی ها
Bit defender	Kasper sky	ESET Nod32	MacAfee	One Care	Norton	AVG Antivirus	
هر ساعت	هر ساعت	در صورت لزوم	روزانه	هر ساعت	هفتگی	روزانه	به روز رسانی ویروس های جدید
20 Min	8 Min	24 Min	1 hours	30 Min	35 Min	24 Min	مدت زمان پوش یا دیسک سخت 80 GB
دارد	دارد	دارد	دارد	دارد	دارد	دارد	محافظت در برابر Instant message
دارد	دارد	ندارد	ندارد	دارد	ندارد	ندارد	محافظت در برابر File Sharing
ندارد	دارد	ندارد	ندارد	دارد	ندارد	ندارد	محافظت از Web Mail
دارد	دارد	دارد	دارد	دارد	دارد	دارد	بانک اطلاعات ویروس ها
دارد	دارد	دارد	ندارد	دارد	ندارد	ندارد	ویروس یابی برخط
دارد	دارد	ندارد	ندارد	دارد	ندارد	ندارد	تشخیص مدت زمان پوش

گزارش از ویروس‌های شناسایی شده	دارد	دارد	دارد	دارد	دارد	دارد	دارد
حجم پرونده به هنگام‌سازی	کم حجم	کم حجم	کم حجم	کم حجم	زیاد	کم حجم	کم حجم
شناسایی هرزمانه به صورت بلادرنگ	ندارد	* ندارد	دارد	* ندارد	دارد	ندارد	دارد

* البته این دو برنامه فقط در زمانی که در حالت بویس کامل باشند، توانایی شناسایی هرزمانه را دارند. ولی در شرایط عادی اگر هرزمانه وارد رایانه شود قادر به شناسایی نیستند.

۵-۷- انواع ضدویروس

الف- ضدویروس‌های قابل حمل (Portable): برخی از ویروس‌ها در صورتی که سیستم را آلوده کنند، از فعالیت ضدویروس جلوگیری می‌کنند. حتی مانع از نصب برنامه‌های ضدویروس می‌شود. گاهی ممکن است که بخواهید با توجه به داشتن یک ضدویروس باز هم از ضدویروس‌های دیگر استفاده کنید در شرایط عادی دو ضدویروس روی یک سیستم عامل نصب نمی‌شوند و اگر هم نصب شوند عملکرد درستی ندارند.

در این حالت از نرم افزارهایی که نیاز به نصب ندارند و می‌توانند مستقیماً از دیسک نوری یا حافظه جانبی دیگر اجرا شوند استفاده می‌شود شرکت‌های معروف معمولاً چنین برنامه‌هایی را تولید و در اختیار قرار می‌دهند.

از بین بردن برنامه‌های مخرب به وسیله **Microsoft Windows Malicious Software** : این نرم افزار برای از بین بردن برنامه‌های مخرب در سیستم عامل ویندوز استفاده می‌شود و به جای ضدویروس قابل استفاده نیست. زیرا برنامه‌های ضدویروس جلوی ورود برنامه‌های مخرب به سیستم عامل را می‌گیرند اما این نرم افزار زمانی استفاده می‌شود که سیستم عامل مورد حمله قرار گرفته باشد و ضدویروس‌های نصب شده نتوانند مشکل را حل کنند. این برنامه فقط قادر به شناسایی ترواها و کرم‌ها است و برای شناسایی جاسوس‌ها بهتر است از برنامه‌های دیگر (Windows Defender) استفاده کنید.

نکته

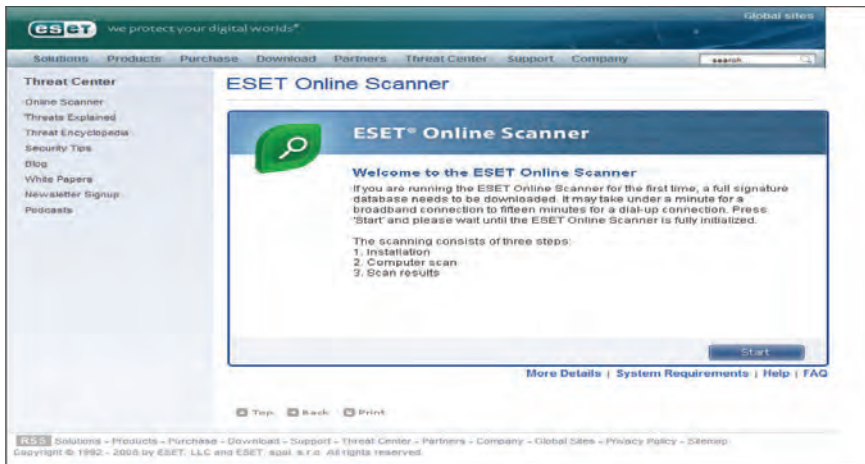
این برنامه فقط برنامه‌های مخربی که در سیستم عامل ویندوز در حال اجرا هستند را شناسایی می‌کند.

برای تهیه این برنامه می‌توانید به آدرس <http://support.microsoft.com/?kbid=890830> مراجعه کنید پس از تهیه برنامه باید آن را اجرا کنید چرا که این برنامه قابل نصب نیست و در طول اجرا پرونده‌های موجود را بررسی نموده و در صورت یافتن پرونده مخرب آن را از بین می‌برد. زمانی که سیستم عامل ویندوز در حال به هنگام‌سازی محصولات خود است با شناسایی این برنامه روی رایانه کلیه بانک‌های اطلاعاتی جدید خود را نیز منتقل می‌کند. به این ترتیب این برنامه به روزرسانی می‌شود.

ب - ضد ویروس‌های برخط (Online): این ضد ویروس‌ها بدون نیاز به نصب روی سیستم، بخشی از پایگاه اطلاعات خود را برای شناسایی ویروس‌ها، روی سیستم کپی می‌کنند. سپس اطلاعات را پویش نموده، در صورت یافتن ویروس آن را از بین می‌برند. یکی از مزایای ضد ویروس‌های برخط، سبک بودن آن‌ها در زمان اجرا می‌باشد. به طوری که حجم استفاده از حافظه RAM و CPU در شرایطی که اطلاعات دیسک سخت در حال بررسی است بسیار ناچیز و کمتر از برنامه‌های دیگر می‌باشد.

استفاده از ضد ویروس برخط NOD32: ابتدا وارد سایت <http://www.eset.com/> onlinescan/scanner.php شوید. گزینه Start را مطابق با شکل ۱-۷ انتخاب کنید، تا بانک اطلاعات ویروس‌ها روی سیستم عامل کپی شود. لازم به ذکر است که انجام این عملیات کپی خیلی زمان‌گیر نیست و در صورتی که اتصال از طریق اینترنت کم سرعت باشد، این عملیات نصب چیزی حدود ۱۵ دقیقه زمان می‌برد.

طبق شکل ۲-۷ نوع عملکرد ضد ویروس در برابر ویروس‌ها سؤال می‌شود. با انتخاب گزینه‌ی اول کلیه پرونده‌های مشکوک که امکان دارد سیستم را مورد تهدید قرار دهند از سیستم عامل پاک می‌شوند و اگر گزینه‌ی دوم را انتخاب کنید، برنامه‌ها و نرم‌افزارهای کاربردی که به طور ناخواسته روی رایانه نصب شده‌اند را شناسایی می‌کند.

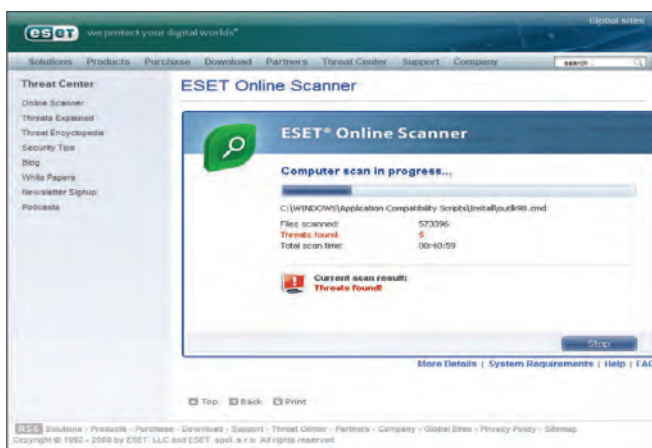


شکل ۷-۱



شکل ۷-۲

پس از انتخاب گزینه موردنظر و کلیک روی دکمه Scan شروع به بررسی کل اطلاعات دیسک سخت نموده و پرونده‌های مشکوک را از بین می‌برد (شکل ۷-۳).



شکل ۳-۷

ج — ضد ویروس های قابل نصب (Installed) : در این روش یک برنامه ضد ویروس مناسب را در سیستم نصب می کنند در صورتی که دو برنامه ضد ویروس همزمان نصب شود تداخل عملکرد پیش می آید و ممکن است کل سیستم از نظر نرم افزاری از کار بیافتد. برخی از برنامه های ویروس یاب در سیستم نصب می شود که مانع از ورود ویروس یا جلوگیری از عملکرد مخرب ویروس شود و برخی از آن ها پس از ورود ویروس و آلوده شدن سیستم به برنامه های مخرب برای پاک کردن سیستم مورد استفاده قرار می گیرند.

۶-۷ — محافظت از رایانه با برنامه ESET Smart Security

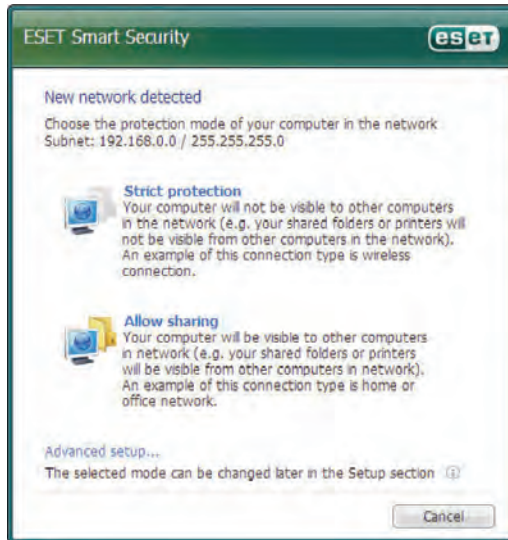
وقتی برای اولین بار برنامه ESET Smart Security را اجرا کنید پنجره ای مطابق با شکل ۴-۷ ظاهر می شود که حالت حفاظت را سؤال می کند. این حفاظت می تواند به یکی از دو صورت زیر انجام شود :

۱ — **Strict protection** : در این حالت سایر کاربران شبکه نمی توانند به رایانه شما دسترسی داشته باشند و آن را مشاهده کنند. یعنی اگر روی رایانه شما پوشه یا چابگری به صورت اشتراکی وجود داشته باشد، این منابع از دید سایر کاربران در شبکه غیر قابل رؤیت است. این ویژگی برای رایانه هایی مفید است که کارت شبکه بی سیم دارند و در محیطی غیر قابل اطمینان قرار دارند و ممکن است از طریق شبکه به آن ها نفوذ شود.

نکته

از ویژگی‌های مهم در برنامه‌های ضدویروس خصوصیت Stealth یا پنهان می‌باشد. این ویژگی سبب می‌شود که رایانه در سراسر شبکه اعم از شبکه داخلی یا اینترنت از دید سایرین پنهان باشد و نفوذگرها و برنامه‌های مخرب نتوانند آن را مورد حمله قرار دهند.

۲- Allow sharing : در این حالت، رایانه در تمام شبکه قابل دسترس است و همه کاربران می‌توانند از منابع به اشتراک گذاشته شده آن مانند پوشه و چاپگر استفاده کنند.



شکل ۷-۴

پس از اجرای برنامه، کادرمحاوره‌ای مطابق شکل ۷-۵ ظاهر می‌شود که شامل بخش‌های زیر است :

۱- وضعیت حفاظت Protection Status

۲- پوش رایانه Computer Scan

۳- به هنگام‌سازی Update

۴- تنظیم ها Setup

۵- ابزار Tools

۶- راهنمایی و پشتیبانی Help & Support



شکل ۵-۷

نکته

برای استفاده از این برنامه ضدویروس حتماً آن را در حالت Advanced یا پیشرفته قرار دهید تا بتوانید از تمامی امکانات آن استفاده کنید.

۱-۶-۷- وضعیت حفاظت : وظیفه اصلی این بخش، آگاهی دادن از وضعیت امنیت و سطح حفاظت سیستم به کاربر است. در این بخش هم چنین تعداد دسترسی های مسدود شده (Block) به سیستم و شماره آخرین نسخه بانک اطلاعات ویروس که به هنگام سازی شده است به کاربر اعلام می شود.

وضعیت حفاظت دارای سه حالت است که با رنگ های سبز و نارنجی و قرمز نشان داده می شود.

• **حالت سبز** : در این حالت برنامه ESET در حداکثر وضعیت محافظت از سیستم است و می توان به عملکرد برنامه ضدویروس اطمینان کامل داشت. رنگ نشانه ی نوار وظیفه برنامه ضدویروس در بخش اعلان در این حالت سبز خواهد بود.

• **حالت نارنجی:** در این حالت امکان دارد بعضی از اجزای برنامه ضدویروس غیرفعال باشد مانند وضعیت محافظت از صندوق پست الکترونیکی، محافظت از دسترسی به وب. هم چنین ممکن است، برنامه دیواره آتش تمامی ترافیک شبکه را مسدود کرده باشد. (Block Network Traffic) رنگ نشانه‌ی نوار وظیفه برنامه ضدویروس در این حالت نارنجی خواهد بود.

• **حالت قرمز:** فقط در شرایط بحرانی امکان تغییر حالت به رنگ قرمز وجود دارد. این شرایط بحرانی می‌تواند به دلیل بروز تهدید یا حمله به رایانه باشد یا ممکن است به دلیل غیرفعال شدن سیستم حفاظتی بلادرنگ یا دیواره آتش باشد. رنگ نشانه نوار وظیفه برنامه ضدویروس در این حالت قرمز خواهد بود.

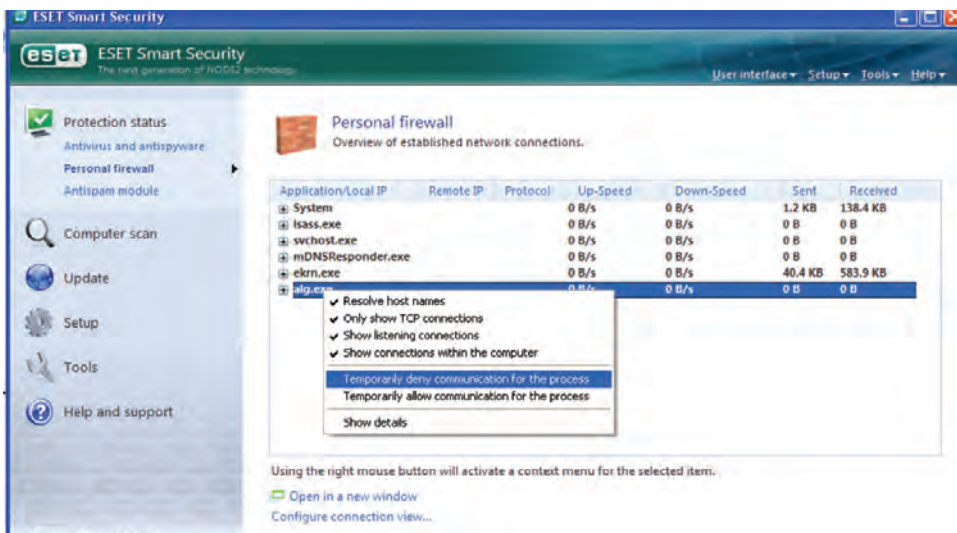
الف – بخش ضدویروس و ضدجاسوس (Anti Virus & Anti Spyware): این بخش اطلاعات آماری دقیقی از تعداد نفوذها و تعداد حملات ویروسی که به سیستم شده است را ارائه می‌دهد. این اطلاعات شامل تعداد پرونده‌ها و پوشه‌های پویش شده، آلوده و پاک‌سازی شده و پرونده‌هایی که ممکن است در صورت ویروسی بودن حذف شده یا قرنطینه شده باشند، است (شکل ۶-۷).



شکل ۶-۷

ب – دیواره آتش شخصی (Personal Firewall): در این بخش لیستی از ارتباطات فعال و ارتباطاتی که به صورت معوق یا حالت انتظار قرار دارند مشاهده می‌شود. با این لیست می‌توان برنامه‌های کاربردی که در حال برقراری ارتباط با محیط خارج از شبکه هستند را بررسی کرد. در شکل ۷-۷ نام برنامه به همراه حجم و سرعت تبادل ارتباط با محیط بیرون به صورت بلادرنگ نشان داده می‌شود. با کلیک راست روی نام هر برنامه می‌توانید آن را موقتاً غیرفعال کنید تا دیگر با محیط خارج از شبکه ارتباط نداشته باشد. هم‌چنین می‌توانید جزئیات ارتباط برنامه را در این قسمت مشاهده کنید.

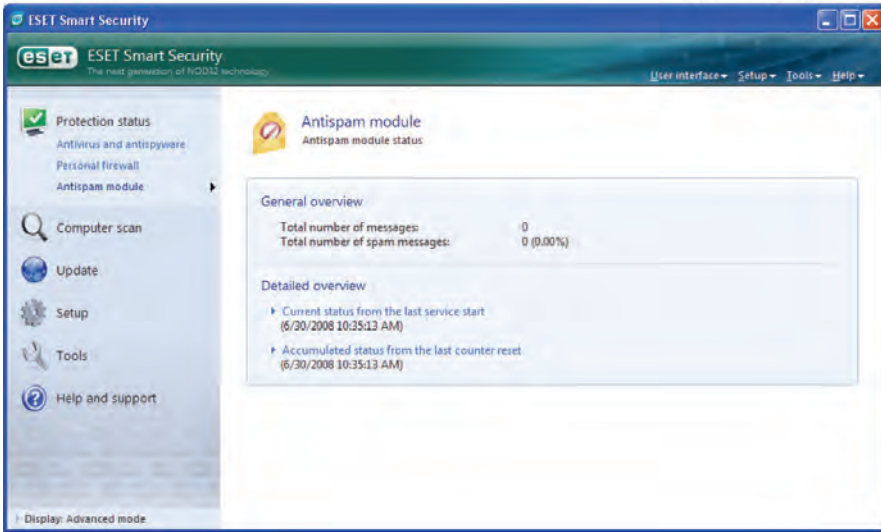
توضیحات تکمیلی در این بخش به درس شبکه‌های رایانه‌ای مربوط می‌شود.



شکل ۷-۷

ج – مازول ضد جاسوس (AntiSpam Module): تعداد کل پیام‌های دریافت شده از طریق شبکه به همراه پیام‌هایی که حاوی هرزنامه می‌باشند در این قسمت مشاهده می‌شوند (شکل ۷-۸).

۲-۶-۷- پویش اطلاعات رایانه (Computer Scan): پویش کردن اطلاعات در رایانه یکی از مهم‌ترین بخش‌های یک برنامه ضد ویروس است چرا که طی این عمل تمامی پوشه‌ها و پرونده‌ها روی رایانه بررسی می‌شود. توصیه برنامه ضد ویروس بر این است که پویش به صورت دقیق و



شکل ۸-۷

عمیق انجام شود تا سیستم از لحاظ امنیتی، کامل بررسی شود.

حالت Standard Scan روشی است که ضدویروس سیستم را خیلی سریع پوشش می‌کند تا پرونده‌های آلوده را شناسایی کرده و از بین ببرد. در این حالت نیازی به مداخله کاربر برای انجام عملیات پاک‌سازی اطلاعات نیست. مزیت این روش آسان بودن بررسی سیستم بدون دانستن جزئیات پیکربندی برنامه ضدویروس است. لازم به ذکر است که پوشش استاندارد به هیچ وجه نامه‌های الکترونیکی و پرونده‌های فشرده را بازبینی نمی‌کند و در صورت پیدا شدن پرونده یا پوشه آلوده، ضدویروس بدون اینکه از کاربر سؤالی بپرسد، به سرعت ویروس آن را از بین می‌برد.

حالت Custom Scan در این حالت می‌توانید برای پوشش رایانه، تنظیم‌های خاصی تعیین کنید مثلاً محتویات پوشه خاصی را در درایو مورد نظر با استفاده از روشی بررسی کنید. مزیت این روش این است که کاربر را قادر می‌سازد تا عملیات پوشش را با دقت بیشتر و در زمان کمتر انجام دهد.

برای پاک‌سازی یک پرونده آلوده سه حالت وجود دارد:

• **Do Not Clean**: در این حالت پرونده‌های آلوده به طور خودکار پاک نمی‌شوند. بلکه

برنامه ضد ویروس یک پنجره اعلان خطر ظاهر می‌کند و اجازه می‌دهد که خود کاربر نوع عملیات پاک‌سازی پرونده را تعیین کند.

• **Default level** : در این حالت ضد ویروس تلاش می‌کند تا پرونده‌های آلوده به طور خودکار پاک‌سازی شوند و در صورتی که موفق به پاک‌سازی نشود برای انجام عملیات بعدی مجوز لازم را از کاربر می‌گیرد.

• **Strict cleaning** : در این حالت ضد ویروس در صورت مشاهده پرونده آلوده بلافاصله آن را پاک‌سازی یا حذف می‌کند البته در مورد پرونده‌های سیستمی این کار را انجام نمی‌دهد و امکانات دیگری را در اختیار کاربر قرار می‌دهد.

نکته مهم

اگر یک پرونده از پوشه فشرده یا آرشیو شده آلوده به ویروس باشد، در برنامه ضد ویروس دو انتخاب برای رفتار با چنین پرونده‌هایی وجود خواهد داشت. در حالت Standard mode فقط پرونده‌ها و پوشه‌های آلوده حذف خواهد شد و پوشه‌ها و پرونده‌های فشرده پاک‌سازی نمی‌شوند. اما در حالت strict cleaning mode کل پرونده یا پوشه فشرده حذف می‌شود.

عملیات روی پرونده‌های آلوده

• **Copy to Quarantine** : در این حالت یک کپی از پرونده آلوده به محلی مطمئن به وسیله‌ی برنامه ضد ویروس منتقل و در آن جا قرنطینه می‌شود.

• **Submit for analysis** : این حالت زمانی اتفاق می‌افتد که برنامه ضد ویروس قادر به شناسایی نوع ویروس نباشد یا این که ویروس جدید باشد و در بانک اطلاعات ویروس ثبت نشده باشد. در این حالت یک نسخه از پرونده آلوده به همراه ویروس آن به آزمایشگاه شرکت سازنده برنامه ضد ویروس ارسال می‌شود تا پس از آنالیز آن نتیجه به همراه بانک اطلاعات جدید ضد ویروس به کاربر ارسال شود.

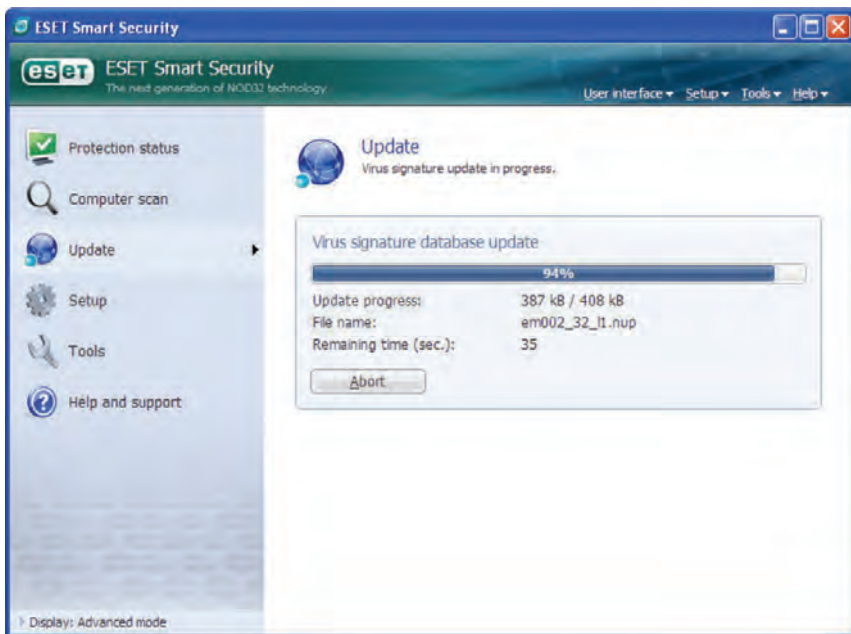
• **Clean** : این عملیات زمانی فعال می‌شود که پرونده آلوده قابل پاک‌سازی شدن باشد. پس از انجام این عملیات ویروس از پرونده آلوده پاک می‌شود.

• **Delete**: این بخش برای حذف کردن پرونده استفاده می‌شود. البته اگر پرونده قابل پاک‌سازی باشد. این بخش غیرفعال خواهد بود.

• **Leave**: با انتخاب این بخش پنجره هشدار برنامه ضدویروس بسته شده و هیچ عملیاتی روی پرونده آلوده انجام نمی‌شود.

۳-۶-۷- به هنگام سازی برنامه ضدویروس (Update): همان‌طور که گفته شد از ویژگی‌های مهم برنامه‌های ضدویروس خاصیت به هنگام سازی آن است. چرا که باید یک سرویس دهنده برنامه ضدویروس بتواند به‌طور روزانه یا هر زمان که کاربر به پرونده مشکوک برخورد کند، آن را برای سرویس دهنده خود ارسال یا Submit کند و سرویس دهنده در اولین فرصت برنامه ضدویروس را به هنگام سازی کرده و مورد مشکوک را از بین ببرد. در واقع سرویس به هنگام سازی یکی از بالاترین سطوح امنیتی در برابر تهدیدات شبکه است.

برای به هنگام سازی برنامه ضدویروس Eset با کلیک روی گزینه Update می‌توان برنامه را به هنگام سازی کرد (شکل ۹-۷).



شکل ۹-۷

روش‌های به هنگام‌سازی برنامه ضدویروس

الف – خودکار^۱: در این روش می‌توان از طریق خود برنامه ضدویروس اقدام به این کار نمود و برنامه ضدویروس با برقراری ارتباط با سرویس‌دهنده خود، بانک اطلاعات و اجزای خود را به هنگام‌سازی می‌کند. از ویژگی‌های برنامه Eset Smart Security این است که حجم فایل به هنگام‌سازی شده بعد از نصب آخرین نسخه برنامه، معمولاً کمتر از 400 KB می‌باشد و این برای کاربرانی که با اینترنت کم سرعت، این پرونده‌ها را دریافت می‌کنند، مزیت مهمی به‌شمار می‌رود.

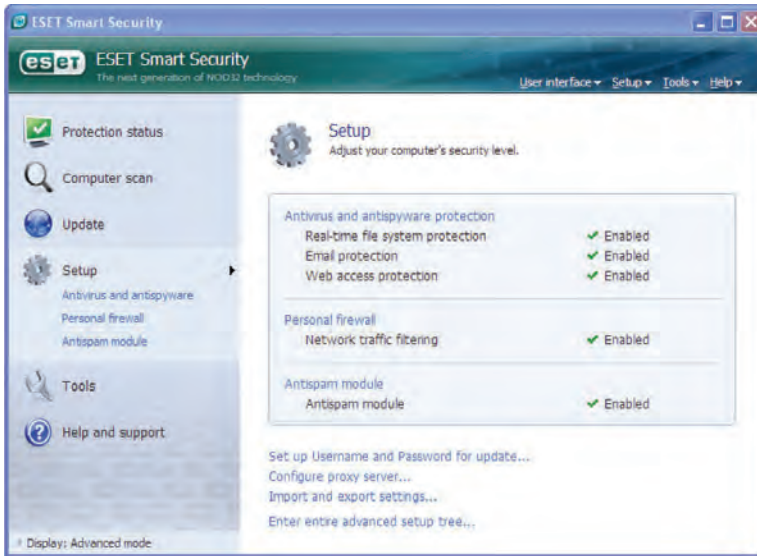
معمولاً پرونده‌های به هنگام‌سازی دریافت شده از اینترنت در مسیر All user/Application Data/ eset/ smart security کپی می‌شوند. پسوند آن‌ها Dat. است.

ب – هوشمند (intelligent): در این روش می‌توان بدون استفاده از برنامه ضدویروس، با رجوع به سایت سرویس‌دهنده، پرونده‌های به هنگام‌سازی شده را از روی تاریخ آن‌ها دریافت کرد و سپس آن‌ها را روی رایانه به‌صورت یک فایل اجرایی نصب کرد. در حال حاضر برنامه ضدویروس Eset این روش را پشتیبانی نمی‌کند. اما می‌توانیم پرونده‌های Dat. را از روی یک رایانه به هنگام‌سازی شده روی رایانه موردنظر کپی و برنامه ضدویروس آن‌را به هنگام‌سازی کرد.

کنجکاوی

کدام یک از دو روش فوق برای به هنگام‌سازی بهتر است؟ چرا؟
کدام یک از برنامه‌های ضدویروس رایج، روش دوم را برای به هنگام‌سازی پشتیبانی می‌کند؟

۴-۶-۷ – تنظیم‌ها (Setup): در این بخش از برنامه می‌توان سطح امنیتی رایانه و شبکه را تنظیم کرد. این سطح امنیتی شامل دیواره آتش، ضدویروس، ضدهرزنامه و ضدجاسوس می‌باشد (شکل ۱-۷).



شکل ۱۰-۷

هم چنین در این قسمت می توان نام کاربری و کلمه عبور برنامه را برای به هنگام سازی تغییر داد. این گذر واژه معمولاً در هنگام خرید برنامه ضدویروس برای کاربر ارسال می شود.

تنظیم های مربوط به Antivirus and antispymware protection: توصیه کلیه

برنامه های ضدویروس برای رسیدن به حداکثر امنیت در رایانه این است که همه اجزای این بخش همیشه فعال باشد. هم چنین کاربر می تواند بعضی از این قسمت ها را غیرفعال کند. در چنین شرایطی اگر کاربر فراموش کند که آن را مجدداً فعال کند بعد از راه اندازی مجدد رایانه کلیه بخش های غیرفعال دوباره فعال می شوند.

تغییر پیکربندی پوش های درخواستی از دیگر تنظیم های این بخش می باشد که در آن می توان مشخص نمود که در هنگام پوش رایانه کدام بخش مورد بازبینی قرارگیرد و این بازبینی شامل چه پوشه ها و پرونده هایی باشد. لیست این پیکربندی ها به شرح زیر است:

• **Real-time protection:** محافظت هم زمان - در هر لحظه که رایانه مورد تهدید قرار

بگیرد برنامه ضدویروس فعال بوده و از رایانه در برابر تهدید محافظت می کند.

• **Threat Sense engine:** موتور تشخیص تهدید (این بخش از روی عملکرد و رفتار

پرونده ها تشخیص می دهد که آلوده هستند یا خیر)

• **Media Scan:** شامل دیسک سخت، حافظه فلش و اطلاعات روی شبکه است.

• **Scan On**: شامل پوشش کردن پرونده‌های باز، پرونده‌های در حال ایجاد، پرونده‌های اجرایی، پرونده‌های روی دیسکت یا پرونده‌هایی که در فرآیند خاموش شدن رایانه در حال اجرا هستند، می‌باشد.

• **Email protection**: در این بخش کلیه نامه‌های الکترونیکی در هنگام ارسال و دریافت بررسی می‌شود و در صورت داشتن ویروس با تنظیم این بخش می‌توان نام ویروس را به نامه پیوست یا در موضوع نامه اضافه کرد.

• **Web access protection**: هنگامی که به صفحات وب دسترسی دارید، با فعال کردن این بخش برنامه ضدویروس به طور خودکار کلیه صفحات و محتوای آن‌ها را بررسی می‌کند.

تنظیم‌های دیوار آتش شخصی Personal firewall setup: این تنظیم‌ها مربوط به رفتار رایانه با محیط بیرون از شبکه می‌باشد. به عنوان مثال اگر رایانه در محیط شبکه‌ای ناشناسی قرار گرفته باشد در این حالت می‌توان تمامی ترافیک ارتباطی با رایانه را مسدود کرد، تا هیچ رایانه‌ای نتواند با آن رایانه در تماس باشد و آن را مورد حمله قرار دهد.

• **Block all network traffic**: با انتخاب این گزینه می‌توان همه اطلاعات ورودی^۱ و خروجی^۲ رایانه را مسدود کرد. این گزینه ارتباط رایانه را از شبکه قطع می‌کند و کلیه ارتباطات به سمت رایانه را غیرفعال می‌کند.

• **Filtering mode**: زمانی که رایانه به شبکه متصل است امکان دارد بعضی از برنامه‌ها به طور ناخواسته بخواهند با آن ارتباط برقرار کنند یا این که یکی از برنامه‌های داخل رایانه بخواهد با شبکه بیرون ارتباط برقرار کند. در چنین شرایطی اگر حالت فیلترینگ به صورت خودکار (Automatic) باشد، با توجه به نوع رفتار آن برنامه، ضدویروس تصمیم می‌گیرد که ارتباط برقرار یا مسدود شود. اما در حالت تبادلی (Interactive) برای برقراری ارتباط، از کاربر سؤال می‌شود و کاربر تصمیم می‌گیرد که ارتباط برقرار یا مسدود شود.

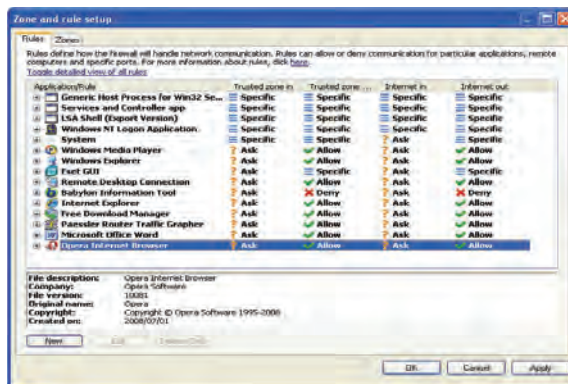
به عنوان مثال با اجرای برنامه Opera چون این برنامه به عنوان یک مرورگر می‌خواهد با بیرون شبکه یعنی اینترنت ارتباط برقرار کند (Outbound traffic) پنجره‌ای مطابق با شکل (۱۱-۷) باز می‌شود و از کاربر برای اجرای برنامه سؤال می‌کند.



شکل ۷-۱۱

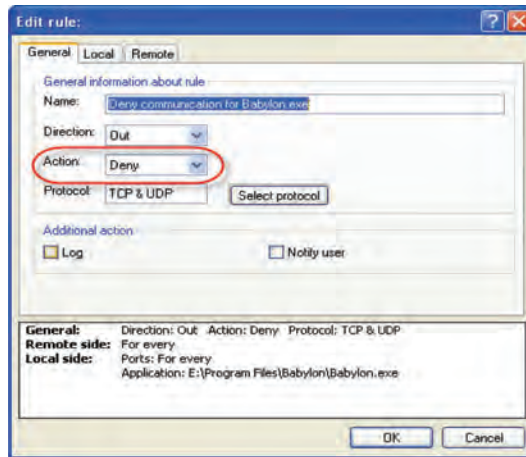
برای تأیید و اجرای برنامه می‌توان روی دکمه Allow و برای ممانعت از اجرای آن روی کلید Deny کلیک کرد. با انتخاب گزینه‌ی Remember Action در برنامه ضد ویروس یک قانون برای این برنامه (Opera) ایجاد می‌شود که دیگر این کادر محاوره‌ای ظاهر نشود. اما اگر بخواهید که برنامه فقط یک بار آن‌هم به صورت موقت اجرا شود و برای آن هیچ قانونی در برنامه ضد ویروس ایجاد نشود، گزینه Temporarily remember action for the process را انتخاب کنید.

با انتخاب گزینه Configure trust and zone مطابق با شکل ۷-۱۲ می‌توان لیستی از برنامه‌هایی که در Rule list تعریف شده است را مشاهده کرد و در صورت لزوم برنامه جدیدی اضافه یا حذف نمود و وضعیت آن‌را مسدود و یا باز کرد.



شکل ۷-۱۲

به عنوان مثال اگر بخواهیم که برنامه Babylon به هنگام سازی نشود و با سرویس دهنده خود ارتباط نداشته باشد. باید وضعیت آن را به صورت Deny در آوریم. برای انجام این کار باید با زدن دکمه Edit به محیط ویرایش وارد شویم و مانند شکل ۷-۱۳ تغییرات لازم را در اجرای این برنامه به وجود آوریم:



شکل ۷-۱۳



شکل ۷-۱۴

• **Antispam module**: تنظیم های این قسمت مربوط می شود به هرزنامه هایی که از طریق پست الکترونیک برای کاربران رایانه ها ارسال می شود. در این بخش می توان تعداد هرزنامه هایی که توسط برنامه ضدویروس شناسایی شده است را مشاهده و شمارش گر آن را صفر کرد.

دو بخش مهم برنامه ضد هرزنامه لیست سیاه Black List و لیست سفید White List است. در این لیست‌ها می‌توان با وارد کردن پست الکترونیک اشخاصی که اقدام به فرستادن هرزنامه می‌کنند، از وارد شدن آن به پست الکترونیک شخصی جلوگیری کرد. برای انجام این کار باید آدرس پست الکترونیک شخص مورد نظر را در قسمت لیست سیاه وارد نمود. آدرس پست الکترونیک اشخاصی را که نامه‌های آن‌ها فاقد برنامه‌های مخرب بوده و مطمئن هستند در قسمت لیست سفید وارد می‌شود.

۵-۶-۷ Tools: بخش ابزارهای سیستمی، شامل مازول‌های مکملی است که به کاربران پیشرفته برای بررسی ساده وضعیت برنامه ضدویروس کمک می‌کند. این ابزارها فقط در حالت پیشرفته (Advance mode) قابل استفاده است.

Log: در این بخش می‌توانید گزارش کاملی از عملکرد برنامه ضدویروس به شرح زیر داشته باشید:

• **Detected threats**: حملات ویروس‌هایی که قصد آلوده کردن رایانه را داشته‌اند، به همراه تاریخ، ساعت، نام و همچنین نتیجه عملکرد برنامه ضدویروس در برابر این برنامه‌های مخرب را نشان می‌دهد.

• **Events (رویدادها)**: شامل ثبت تمامی رویدادها و اشکالات در برنامه ضدویروس است.

• **On-demand computer scan**: در این بخش تعداد دفعاتی که رایانه پویش شده است ثبت می‌شود. معمولاً تعداد پرونده‌های پویش شده به همراه تعداد ویروس‌های شناسایی و پاک‌سازی شده ثبت می‌شود.

• **ESET personal firewall log**: در این گزارش تمامی حملاتی که از سمت بیرون شبکه به رایانه شده است، ثبت می‌شود. معمولاً در این قسمت نام و آدرس شبکه (IP Address) رایانه حمله‌کننده به همراه تاریخ و ساعت ثبت می‌شود.

Quarantine: معمولاً پرونده‌های آلوده که امکان پاک‌سازی آن‌ها وجود ندارد به صورت قرنطینه در رایانه ثبت و محافظت می‌شوند. در این قسمت اگر خود کاربر به مورد مشکوکی برخورد کند می‌تواند به‌طور دستی آن پرونده را قرنطینه کند.

Scheduler and Planner: در تمامی برنامه‌های ضدویروس می‌توان با این امکان، طرح‌هایی را به صورت زمان‌بندی اجرا کرد. معمولاً این طرح‌ها شامل به‌هنگام‌سازی بانک اطلاعات ویروس‌ها،

پوش کردن اطلاعات، آزمایش پرونده‌هایی که در لحظه شروع به کار سیستم عامل اجرا می‌شوند و ایجاد گزارش‌هایی که برای نگهداری برنامه ضدویروس مفید است.

۷-۷- توصیه‌های ایمنی برای پیش‌گیری از ورود برنامه‌های مخرب

- روی رایانه‌تان یک ویروس‌یاب به همراه دیوار آتش نصب کنید و بخش ویروس‌یابی خودکار آن را فعال کنید. قبل از استفاده از هر دیسکت، یا حافظه جانبی دیگری آن را ویروس‌یابی کنید و برنامه ضدویروس به محض یافتن برنامه مخرب روی رایانه، شما را از آن مطلع می‌کند.
- اطلاعات ویروس‌یاب دستگاه خود را هر چند وقت یک بار به روز کنید.
- از برنامه‌های مهم و اساسی خود یک پشتیبان تهیه کنید تا در صورت از بین رفتن آن‌ها بتوانید از نسخه‌ی کپی آن استفاده نمایید.
- قبل از انجام کپی اطلاعات روی سی‌دی حتماً از آلوده نبودن اطلاعات اطمینان داشته باشید. چرا که بعد از ذخیره اطلاعات روی سی‌دی دیگر پرونده‌های آلوده قابل پاک‌سازی نمی‌باشد.
- نامه‌ها و برنامه‌های ناشناخته در اینترنت را باز نکنید.
- روی پرونده‌های ضمیمه به Email‌هایی که دریافت می‌کنید دوبار کلیک نکنید.
- اطمینان پیدا کنید که در تمام نرم‌افزارهای میکروسافت، Macro Virus Protection فعال است. هم‌چنین اگر پیامی برای باز کردن ماکروی جدید روی صفحه آمد، تا زمانی که نمی‌دانید چیست هرگز آن را اجرا نکنید.

خلاصه‌ی فصل

داده‌ها، برنامه‌ها و سخت‌افزار رایانه در معرض همیشگی خرابکاری قرار دارند و از این طریق هزینه‌های زیادی به کاربران و شرکت‌ها وارد می‌شود. خرابکاری‌ها در بیشتر مواقع به صورت نرم‌افزاری و بدون آگاهی قبلی کاربران انجام می‌شود.

ویروس، اسب تراوا، کرم رخنه‌گرها برخی از برنامه‌های مخربی هستند که روزانه میلیون‌ها رایانه را آلوده می‌کنند و از این طریق مشکلاتی را ایجاد می‌نمایند.

برنامه‌هایی مانند ضدویروس وجود دارند که با استفاده از آن‌ها می‌توان مانع از آلوده شدن رایانه‌ها به برنامه‌های مخرب شد یا سیستم‌های آلوده به برنامه‌های مخرب را پاک کرد. برنامه‌هایی که برای این منظور استفاده می‌شوند ممکن است به صورت نصب شده یا بدون نیاز به نصب روی سیستم مورد استفاده قرار گیرند.

برنامه‌های ضدویروس با توجه به ویژگی‌هایی مانند حجم پرونده به هنگام‌سازی، شناسایی هرزنامه به صورت بلادرنگ، تشخیص مدت زمان پویش و میزان استفاده از منابع سیستم انتخاب می‌شوند.

خودآزمایی

- ۱- برخی از تهدیدها در مورد داده‌ها و برنامه‌ها را بیان کنید.
- ۲- انواع مهم برنامه‌های مخرب را به طور خلاصه شرح دهید.
- ۳- انواع نفوذگرها را نام ببرید. عملکرد هر کدام را توضیح دهید.
- ۴- بررسی کنید کدام یک از برنامه‌های ضدویروس رایج خاصیت Smart , Intelligent update را دارند.
- ۵- برنامه Eset را به گونه‌ای تنظیم کنید که در صورت یافتن برنامه مخرب بدون دادن هشدار آن را از بین ببرد.
- ۶- آیا می‌توان ضدویروس برخط را جایگزین سایر ضدویروس‌ها کرد؟
- ۷- چگونه می‌توان لیست برنامه‌هایی را که از اینترنت استفاده می‌کنند مشاهده کرد؟