

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.

۹-۱- لزوم حفاظت از اطلاعات

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 به وجود آورده به طوری که قطع این وابستگی در برخی موارد غیرممکن می‌نماید. به عنوان مثال فرض کنید که کلیه سوابق تحصیلی یک دانش آموز یا سوابق پرسنلی یک کارمند که در رایانه ذخیره شده است ناگهان از بین برود، یا دست یابی 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 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. به عنوان مثال برنامه مخرب Blaster در زمان بسیار کوتاهی روی تمامی رایانه‌ها و سرویس دهنده‌های 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 مقاومت کنند.

۹-۲- 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، جاسوس، هرزنامه، کرم.

الف) ویروس‌های رایانه‌ای (Virus): ویروس برنامه 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 می‌کنند.

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 اکسپلورر در رایانه قربانی اجرا شده، عملکرد تخریبی خود را شروع می‌کنند.

ب) اسب تروا (Trojan Horse): اسب تروا برنامه‌ای است که ناخواسته هنگام دریافت اطلاعات از اینترنت به‌وسیله کاربر 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 قابلیتی ندارند.

به‌طور کلی اسب تروا شامل دو بخش است. بخش سرویس‌گیرنده که روی رایانه

شما نصب می‌شود و دیگری بخش سرویس دهنده که در رایانه حمله کننده قرار دارد. بخش سرویس گیرنده ممکن است خود را به شکل یک نرم افزار مهم در شبکه یا سایت های غیر رسمی قرار داده باشد و توسط کاربران دریافت شود. زمانی که این بخش در سیستم قربانی اجرا شود، حمله کننده که در این جا دسترسی بالایی روی این سیستم دارد می تواند بسته به نیت و هدف خود حمله کند و تأثیرات مخربی را روی آن بگذارد.

بیشتر بدانید

اسب های تروا بر اساس عملکردشان به چند دسته تقسیم می شوند که برخی از آن ها عبارتند از:

- **تروای دسترسی از راه دور (Remote Access Trojan)**
- **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 غیرفعال کننده برنامه های امنیتی (security software disabler Trojans)**
- **تروای رد سرویس (denial-of-service attack (DOS) Trojans)**

قالب اکثر پرونده های حاوی اسب تروا، «bat»، «com»، «vbs»، «exe» 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 به طور پیش فرض پسوند پرونده هایی را که می شناسد نشان نمی دهد، و در این حالت پسوند exe به وسیله ویندوز شناسایی می شود نشان داده نشده و دریافت کننده پرونده، آن را نوعی پرونده تصویری شناسایی می کند و از ماهیت اصلی آن پرونده که اجرایی و مخرب است بی اطلاع می ماند. بنابراین ممکن است که یک پرونده حاوی اسب تروا به ظاهر 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.
- بهتر است سیستم عامل ویندوز را طوری تنظیم کنید که پسوند همه پرونده‌ها را نشان دهد.
- از نرم‌افزارهایی که به طور خودکار محتویات پرونده‌ها را باز می‌کنند استفاده نکنید.

نکته

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

برای پاک کردن اسب تروا از سیستم می‌توان از برنامه‌های Anti Trojan استفاده کرد در صورت موفقیت آمیز نبودن روش اول باید مجدداً سیستم عامل و نرم‌افزارهای مورد نیاز را نصب کنید. اگرچه این کار بسیار وقت گیر و دشوار است اما قالب‌بندی دیسک سخت و نصب مجدد سیستم عامل و برنامه‌های کاربردی یکی از بهترین راه‌حل‌ها، برای رهایی از تروا است.

ج) 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 آن‌که معمولاً این ویروس‌ها به رمز درآمده‌اند، نرم‌افزارهای ویروس‌یاب نمی‌توانند به صورت مستقیم آن‌ها را شناسایی کنند، اما می‌توانند با شناسایی بخش رمزگشا، نسبت به شناسایی این ویروس اقدام کنند.

د) 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

اجرای دیگر متصل نمی شوند. کرم‌ها تقریباً همیشه با پرتراфик کردن شبکه باعث صدمه زدن به آن می شوند. این نوع از برنامه‌های مخرب ممکن است اطلاعات رایانه میزبان را تخریب یا امکان سوءاستفاده از آن‌ها را برای افراد سودجو فراهم کنند.

ه) 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 سرویس دهندگان 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 نتوانند تمامی هرزنامه‌ها را شناسایی کنند. در چنین مواقعی استفاده از برنامه Anti Spam روی رایانه ضروری است.

۳-۹- روش‌های انتقال برنامه‌های مخرب

معمولاً انتقال برنامه‌های مخرب از دو راه امکان‌پذیر است: **حافظه جانبی و شبکه.**

انتقال ویروس از طریق حافظه جانبی زمانی رخ می‌دهد که بخشی از اطلاعات را روی دیسک نوری یا حافظه فلش یا هر نوع حافظه جانبی دیگری کپی و آن را 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 ایجاد کنندگان برنامه‌های مخرب شده است و بیشتر حملات خود را به رایانه‌ها از این طریق انجام می‌دهند.

۴-۹- برنامه‌های ضدویروس

امروزه با وجود تنوع زیاد برنامه‌های مخرب الزاماً باید برای مقابله با آن‌ها، مخصوصاً ویروس‌ها از برنامه‌های ضدویروس استفاده می‌شود. وظیفه اصلی یک برنامه ضدویروس **شناسایی، حذف و مقابله با خرابکاری** برنامه‌های مخرب است. امروزه برنامه‌های ضدویروس متنوعی موجود می‌باشد.

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:** یکی از عوامل مهمی که باید در هنگام تهیه یک برنامه ضدویروس به آن توجه داشت، شرکت تولیدکننده 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 تولیدکننده داشته باشد، تا در کوتاه‌ترین زمان بتواند پرونده آلوده را پاک‌سازی کند و نتیجه آن را برای رایانه ارسال کند.

- **به روزرسانی 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 روزرسانی کم باشد. تا کاربرانی که با خط تلفن به شبکه وصل می‌شوند نیز بتوانند اطلاعات را دریافت کنند.

- **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. 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. بهتر می‌تواند برنامه‌های مخرب را شناسایی و از بین ببرد.

۹-۵- مقایسه چند ضدویروس متداول

به‌طور کلی نمی‌توان گفت که کدام یک از برنامه‌های ضدویروس بهتر یا قوی‌تر است، چرا که فناوری تمامی این برنامه‌ها روزبه‌روز در حال پیشرفت است و شرکت‌های 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. در جدول ۹-۱ ویژگی های تکراری از برنامه های ضدویروس بیان شده و با یکدیگر مقایسه شده اند.

جدول ۹-۱- مقایسه چند برنامه ضدویروس^۱

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 با دیسک سخت 80 GB
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
دارد	دارد	دارد	دارد	دارد	دارد	دارد	گزارش از ویروس های شناسایی شده

۱- این اطلاعات مربوط به مشخصات برنامه های ضدویروس در سال ۲۰۱۰ میلادی می باشد.

کم حجم	کم حجم	کم حجم	کم حجم	کم حجم	زیاد	کم حجم	حجم پرونده بهنگام سازی
دارد	دارد	دارد	ندارد*	دارد	ندارد*	ندارد	شناسایی هرزمانه به صورت بلادرنگ

۹-۶- انواع ضد ویروس

الف) ضد ویروس های قابل حمل (Portable): برخی از ویروس ها در صورتی که سیستم را آلوده کنند، از فعالیت ضد ویروس جلوگیری می کنند. حتی مانع از نصب برنامه های ضد ویروس می شود. گاهی ممکن است که بخواهید با توجه به داشتن یک ضد ویروس باز هم از ضد ویروس های دیگر استفاده کنید در شرایط عادی دو ضد ویروس روی یک سیستم عامل نصب نمی شوند و اگر هم نصب شوند عملکرد درستی ندارند.

در این حالت از نرم افزار هایی که نیاز به نصب ندارند و می توانند مستقیماً از دیسک نوری یا حافظه جانبی دیگر اجرا شوند استفاده می شود شرکت های معروف معمولاً چنین برنامه هایی را تولید و در اختیار قرار می دهند.

از بین بردن برنامه های مخرب به وسیله Microsoft Windows Malicious Software:

این نرم افزار برای از بین بردن برنامه های مخرب در سیستم عامل ویندوز استفاده می شود و به جای ضد ویروس قابل استفاده نیست. زیرا برنامه های ضد ویروس جلوی ورود برنامه های مخرب به سیستم عامل را می گیرند اما این نرم افزار زمانی استفاده می شود که سیستم عامل مورد حمله قرار گرفته باشد و ضد ویروس های نصب شده نتوانند مشکل را حل کنند. این برنامه فقط قادر به شناسایی ترواها و کرم ها است و برای شناسایی جاسوس ها بهتر است از برنامه های دیگر (Windows Defender) استفاده کنید.

نکته

ضد ویروس Microsoft Windows Malicious Software فقط برنامه های مخربی که در سیستم عامل ویندوز در حال اجرا هستند را شناسایی می کند.

برای تهیه این برنامه می‌توانید به نشانی <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 بهنگام‌سازی 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) ضدویروس‌های برخط (Online): این ضدویروس‌ها بدون نیاز به نصب روی سیستم، بخشی از پایگاه اطلاعات خود را برای شناسایی ویروس‌ها، روی سیستم کپی می‌کنند. سپس اطلاعات را پوشش نموده، در صورت یافتن ویروس آن را از بین می‌برند. یکی از مزایای ضدویروس‌های برخط، سبک بودن آن‌ها در زمان اجرا می‌باشد.

استفاده از ضدویروس برخط NOD32: ابتدا وارد سایت <http://www.eset.com/> و [online/scan/online.php](http://www.eset.com/online/scan/online.php) شوید. گزینه Start را مطابق شکل ۹-۱ 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.



شکل ۹-۱

طبق شکل ۹-۲ نوع عملکرد ضدویروس در برابر ویروس‌ها سؤال می‌شود. با انتخاب گزینه اول کلیه پرونده‌های مشکوک که امکان دارد سیستم را مورد تهدید قرار دهند از سیستم عامل پاک می‌شوند و اگر گزینه دوم را انتخاب کنید، برنامه‌ها و نرم‌افزارهای کاربردی که

به طور ناخواسته روی رایانه نصب شده‌اند را شناسایی می‌کند.



شکل ۹-۲

پس از انتخاب گزینه مورد نظر و کلیک روی دکمه Scan شروع به بررسی کل اطلاعات دیسک سخت نموده و پرونده‌های مشکوک را از بین می‌برد (شکل ۹-۳).



شکل ۹-۳

ج) **ضدویروس‌های قابل نصب (Installed):** در این روش یک برنامه ضدویروس مناسب را در سیستم نصب می‌کنند در صورتی که دو برنامه ضدویروس همزمان نصب شود تداخل عملکرد پیش می‌آید و ممکن است کل سیستم از نظر نرم افزاری از کار بیفتد. برخی از برنامه‌های ویروس یاب در سیستم نصب می‌شود که مانع از ورود ویروس یا جلوگیری از عملکرد

مخرب ویروس شود و برخی از آن‌ها پس از ورود ویروس و آلوده شدن سیستم به برنامه‌های مخرب برای پاک کردن سیستم مورد استفاده قرار می‌گیرند.

۹-۷- محافظت از رایانه با برنامه ESET Smart Security

وقتی برای اولین بار برنامه ESET Smart Security را اجرا کنید پنجره‌ای مطابق با شکل ۹-۴ ظاهر می‌شود که حالت حفاظت را سؤال می‌کند. این حفاظت می‌تواند به یکی از دو صورت زیر انجام شود:

۱- **Strict protection**: در این حالت سایر کاربران شبکه نمی‌توانند به رایانه شما دسترسی داشته باشند و آن را مشاهده کنند. یعنی اگر روی رایانه شما پوشه یا چاپگری به صورت اشتراکی وجود داشته باشد، این منابع از دید سایر کاربران در شبکه غیرقابل رؤیت است. این ویژگی برای رایانه‌هایی مفید است که کارت شبکه بی‌سیم دارند و در محیطی غیرقابل اطمینان قرار دارند و ممکن است از طریق شبکه به آن‌ها نفوذ شود.



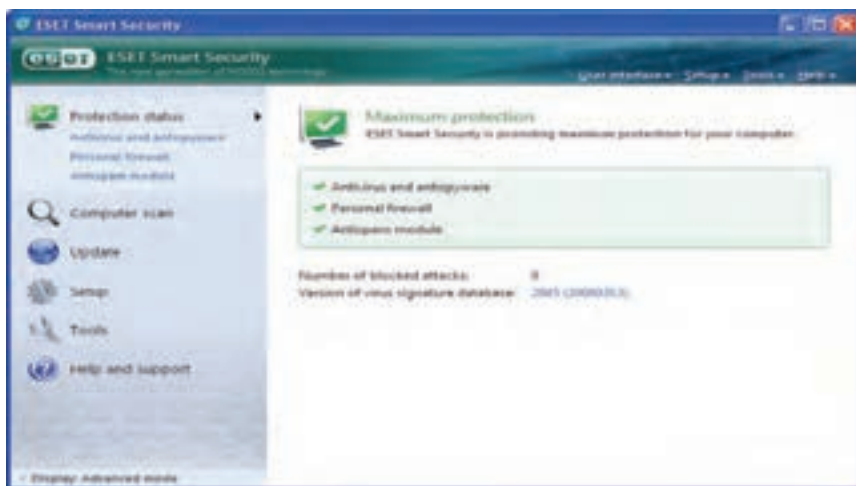
شکل ۹-۴

نکته

از ویژگی‌های مهم در برنامه‌های ضد ویروس 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 می توانند از منابع به اشتراک گذاشته شده آن مانند پوشه و چاپگر استفاده کنند. پس از اجرای برنامه، کادر محاوره‌ای مطابق شکل ۹-۵ ظاهر می شود که شامل بخش های زیر است:

- ۱- وضعیت حفاظت (Protection Status)
- ۲- پویش رایانه (Computer Scan)
- ۳- بهنگام سازی (Update)
- ۴- تنظیم ها (Setup)
- ۵- ابزار (Tools)
- ۶- راهنمایی و پشتیبانی (Help & Support)



شکل ۹-۵

نکته

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

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 و ویروس که بهنگام 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 ضد ویروس اطمینان کامل داشت. رنگ نشانه نوار وظیفه برنامه ضد ویروس در بخش اعلان در این حالت سبز خواهد بود.

• **حالت نارنجی:** در این حالت امکان دارد بعضی از اجزای برنامه ضد ویروس 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 نشانه نوار وظیفه برنامه ضد ویروس در این حالت نارنجی خواهد بود.

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

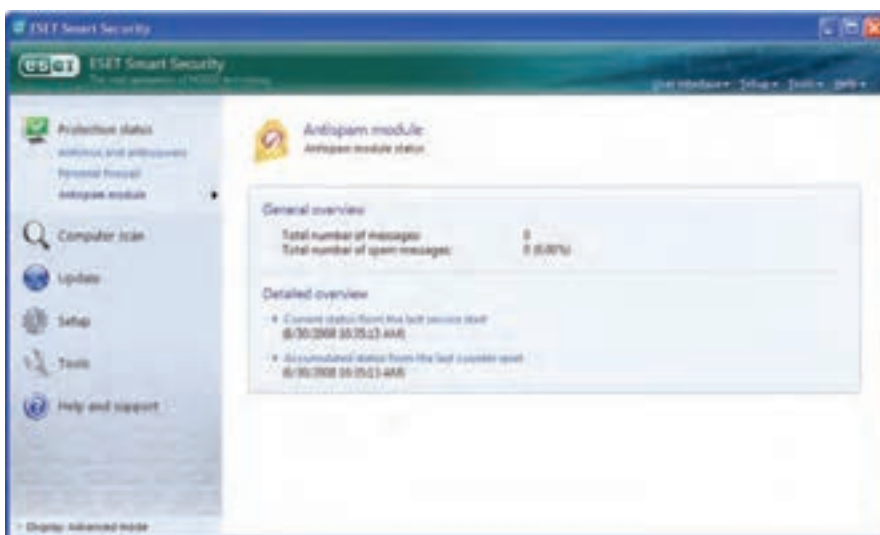
الف) بخش ضد ویروس و ضد جاسوس (Anti Virus & Anti Spyware): این بخش

اطلاعات آماری دقیقی از تعداد نفوذها و تعداد حملات ویروسی که به سیستم شده است را ارائه می دهد. این اطلاعات شامل تعداد پرونده ها و پوشه های پویس شده، آلوده و پاک سازی شده و پرونده هایی که ممکن است در صورت ویروسی بودن حذف شده یا قرنطینه شده باشند است (شکل ۹-۶).



شکل ۹-۶

ب) ماژول 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 ۹-۷).



شکل ۹-۷

پویش اطلاعات رایانه (Computer Scan)

پویش کردن اطلاعات در رایانه یکی از مهم ترین بخش های یک برنامه ی ضد ویروس است چرا که طی این عمل تمامی پوشه ها و پرونده ها روی رایانه بررسی می شود. توصیه برنامه ضد ویروس بر این است که پویش به صورت دقیق و عمیق انجام شود تا سیستم از لحاظ امنیتی، کامل بررسی شود.

● **Standard Scan:** روشی است که ضد ویروس سیستم را خیلی سریع پویش می کند تا پرونده های آلوده را شناسایی کرده و از بین ببرد. در این حالت نیازی به مداخله کاربر برای انجام عملیات پاک سازی اطلاعات نیست. مزیت این روش آسان بودن بررسی سیستم بدون دانستن جزئیات پیکربندی برنامه ضد ویروس است. لازم به ذکر است که پویش استاندارد به هیچ وجه نامه های الکترونیکی و پرونده های فشرده را بازبینی نمی کند و در صورت پیداشدن پرونده یا پوشه آلوده، ضد ویروس بدون این که از کاربر سؤالی پرسد، به سرعت ویروس آن را از بین می برد.

● **Custom Scan:** در این حالت می توانید برای پویش رایانه، تنظیم های 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 می سازد تا عملیات پویش را با دقت بیشتر و در زمان کمتر انجام دهد.

برای پاک سازی یک پرونده آلوده سه حالت وجود دارد:

● **Do Not Clean:** در این حالت پرونده های آلوده به طور خود کار پاک نمی شوند. بلکه برنامه ضد ویروس یک پنجره اعلان خطر ظاهر می کند و اجازه می دهد که خود کاربر نوع عملیات پاک سازی پرونده را تعیین کند.

● **Default level:** در این حالت ضد ویروس تلاش می کند تا پرونده های آلوده به طور خود کار پاک سازی شوند و در صورتی که موفق به پاک سازی نشود برای انجام عملیات بعدی مجوز لازم را از کاربر می گیرد.

● **Strict cleaning:** در این حالت ضد ویروس در صورت مشاهده پرونده آلوده بلافاصله آن را پاک سازی یا حذف می کند البته در مورد پرونده های سیستمی این کار را انجام نمی دهد و امکانات دیگری را در اختیار کاربر قرار می دهد.

نکته مهم

اگر یک پرونده از پوشه فشرده یا آرشیو شده آلوده به ویروس باشد، در برنامه ضدویروس 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

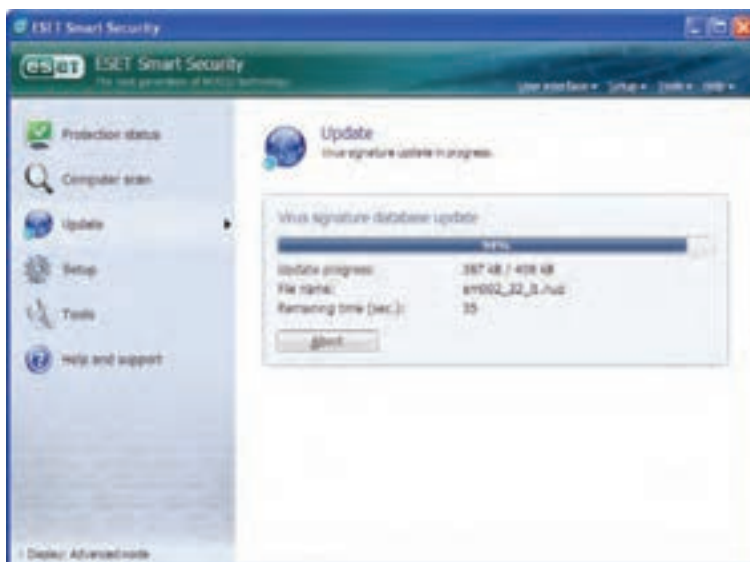
- **Copy to Quarantine**: در این حالت یک کپی از پرونده آلوده به محلی مطمئن به وسیله برنامه ضدویروس منتقل و در آن جا قرنطینه می‌شود.
- **Submit for analysis**: این حالت زمانی اتفاق می‌افتد که برنامه ضدویروس قادر به شناسایی نوع ویروس نباشد یا این که ویروس جدید باشد و در بانک اطلاعات ویروس ثبت نشده باشد. در این حالت یک نسخه از پرونده آلوده به همراه ویروس آن به آزمایشگاه شرکت سازنده برنامه ضدویروس ارسال می‌شود تا پس از آنالیز آن نتیجه به همراه بانک اطلاعات جدید ضدویروس 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.

بهنگام‌سازی برنامه ضدویروس (Update)

همان‌طور که گفته شد از ویژگی‌های مهم برنامه‌های ضدویروس خاصیت بهنگام‌سازی آن است. چرا که باید یک سرویس‌دهنده برنامه ضدویروس بتواند به‌طور روزانه یا هر زمان که کاربر به پرونده مشکوک برخورد کند، آن را برای سرویس‌دهنده خود ارسال یا Submit کند و سرویس‌دهنده در اولین فرصت برنامه ضدویروس را بهنگام‌سازی کرده و مورد مشکوک را از

بین ببرد. در واقع سرویس بهنگام سازی یکی از بالاترین سطوح امنیتی در برابر تهدیدات شبکه است.

برای بهنگام سازی برنامه ضد ویروس Eset با کلیک روی گزینه Update می توان برنامه را بهنگام سازی کرد (شکل ۹-۸).



شکل ۹-۸

بهنگام سازی برنامه ضد ویروس به صورت خود کار^۱

در بهنگام سازی خود کار می توان برنامه ضد ویروس اقدام به این کار نمود و برنامه ضد ویروس با برقراری ارتباط با سرویس دهنده خود، بانک اطلاعات و اجزای خود را بهنگام سازی می کند. از ویژگی های برنامه Eset Smart Security این است که حجم فایل بهنگام سازی شده بعد از نصب آخرین نسخه برنامه، معمولاً کمتر از 400 KB می باشد و این برای کاربرانی که با اینترنت کم سرعت، این پرونده ها را دریافت می کنند، مزیت مهمی به شمار می رود.

تنظیم ها (Setup)

در این بخش از برنامه می توان سطح امنیتی رایانه و شبکه را تنظیم کرد. این سطح امنیتی شامل دیواره آتش، ضد ویروس، ضد هرزنامه و ضد جاسوس می باشد (شکل ۹-۹).

۱- به روز رسانی Automatic



شکل ۹-۹

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

تنظیم های مربوط به Antivirus and antispyware 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 پویس های درخواستی از دیگر تنظیم های این بخش می باشد که در آن می توان مشخص نمود که در هنگام پویس رایانه کدام بخش مورد بازبینی قرار گیرد 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 پویش کردن پرونده‌های باز، پرونده‌های در حال ایجاد، پرونده‌های اجرایی، پرونده‌های روی دیسکت یا پرونده‌هایی که در فرایند 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.

Tools

بخش ابزارهای سیستمی، شامل ماژول‌های 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.

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

۸-۹- 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 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 برنامه‌ها و پرونده‌های یک پشتیبان تهیه کنید تا در صورت از بین رفتن آن‌ها بتوانید از نسخه 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 مایکروسافت، 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.

خلاصه 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، کرم‌های رخنه‌گر 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 بهنگام‌سازی، 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؟