

ماژول 3

محافظت از سیستم توسط آنتی ویروس



Certified Secure Computer User

Honors & Awards

- ❑ **MCSA2003-MCSA2003Security**
- ❑ **MCSE2003-MCSE2003Security**
- ❑ **Windows Server 2008 Network Infrastructure Configuration**
- ❑ **Windows Server 2008 Application Infrastructure Configuration**

- ❑ **Windows Server 2008 Active Directory Configuration**
- ❑ **MCITP Server Administrator**
- ❑ **MCITP Enterprise Administrator**
- ❑ **Microsoft Certified Information Technology Professional**
- ❑ **Installing and Configuring Windows Server 2012**
- ❑ **Administering Windows Server 2012**
- ❑ **Configuring Advanced Windows Server 2012 Services**
- ❑ **Microsoft Certified Solutions Associate 2008, 2012**
- ❑ **Microsoft Certified Solutions Expert 2012 - Server Infrastructure**
- ❑ **IT professional - Cyber Security Org – SANS – Cloud Security Org – Network Security Org**
- ❑ **Compitia A+ - Comptia Network + - Comptia Security + - Comptia Master Level Security (CASP)**
- ❑ **Mcp V1, 2- MCTS**
- ❑ **Microsoft Certified Solutions Expert 2012 - Cloud & Security**
- ❑ **Microsoft Certified Solutions Expert 2012 – MSG**
- ❑ **BA-IT , MS-MBA E.Commerce**

Best Regards,

Alireza Ghahrood

Pm: Security Products Manager

(Security Solution Provider : Cyber Space | BigData | Cloud | Virtualization

Sarv Co

Email: Ghahrood.A@Sarvrayaneh.com

Tel : +98 (21) 88027364 Ext.136 | Cell :+98 (912) 1964383 |



مشاور انفورماتيك شما . قابل اعتماد . قابل اتکا



نگاهی به ویروس‌های خطرناک و مشهور سالهای قبل

طی سال های گذشته، کامپیوترهای فراوانی توسط ویروس های کامپیوتری آلوده شدند و در اقتصاد دنیا تأثیر بسزایی داشتند.

۱۰ تا از مخربترین ویروس ها در زمان های مختلف و مطابق با تکنولوژی های متعدد در آن زمان ها در زیر لیست شده است:

CIH (1998)

خسارت وارده: ۲۰ تا ۸۰ میلیون دلار، نابودی مقادیر بیشماری از اطلاعات کامپیوتر، انتشار یافته از تایوان

Melissa (1999)

خسارت وارده: ۳۰۰ تا ۶۰۰ میلیون دلار

ILOVEYOU (2000)

خسارت وارده: ۱۰ تا ۱۵ میلیارد دلار

Code Red (2001)

خسارت وارده: ۲ میلیارد دلار

SQL Slammer (2003)

بدلیل اینکه این ویروس روز شنبه (تعطیل) انتشار یافت، خسارت مالی زیادی وارد نکرد. تعداد ۵۰۰ هزار سرور را در سراسر جهان صدمه وارد کرد. سرورهای آنلاین کره جنوبی را به مدت ۱۲ ساعت خاموش کرد.

Blaster ((2003

خسارت وارده: ۲ تا ۱۰ میلیارد دلار، ۱۰۰ ها هزار کامپیوتر آلوده شدند

Sobig.F ((2003

خسارت وارده: ۵ تا ۱۰ میلیارد دلار، ۱ میلیون کامپیوتر آلوده شدند

Bagle ((2004

خسارت وارده: ۱۰ ها میلیون دلار

MyDoom ((2004

در اوج خود، ۱۰ تا ۵۰ درصد باعث کندی اینترنت جهانی شد

Sasser ((2004

خسارت وارده: ۱۰ ها میلیون دلار

آنتی ویروس چیست؟



آنتی ویروس چگونه کار می کند؟

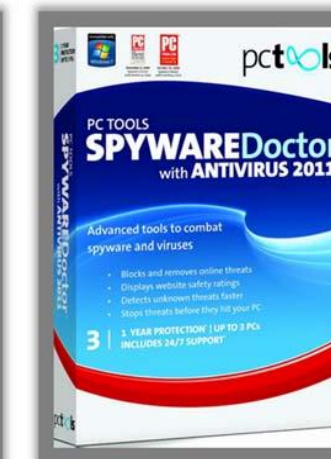
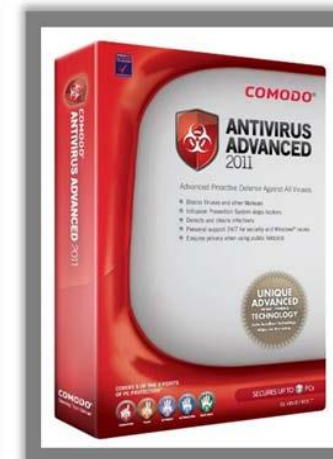
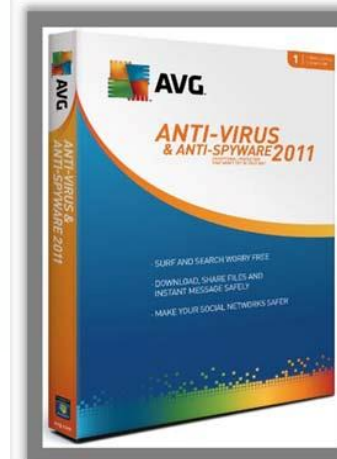
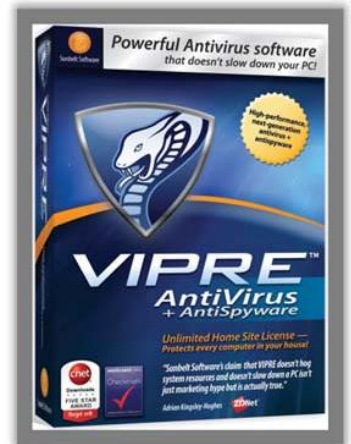
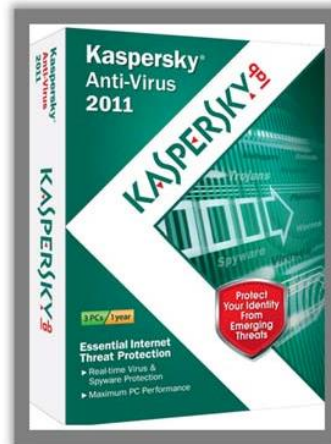
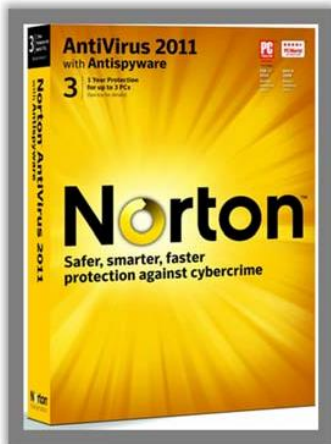
بیشتر آنتی ویروس های تجاری، از دو روش عمده برای شناسایی تهدید استفاده می کنند:

موقع بررسی فایل، از دیکشنری ویروس های شناخته شده برای بررسی استفاده می کنند

رفتارهای مشکوک برنامه های کامپیوتری را شناسایی می کنند



برخی آنتی ویروس ها



<http://www.eccouncil.org>

Antivirus avast مجموعه ای از آخرین تکنولوژی های حفاظتی هست برای تحقق تنها یک هدف و آن چیزی نیست جز دست یابی به بالاترین سطح حفاظتی در مقابل انواع ویروس های کامپیوتری. avast نرم افزار ایده الی برای کلیه ایستگاه های کاری تحت سیستم عامل ویندوز می باشد. avast! همچنین با دارا بود گواهینامه ICسا آنتی ویروس مناسبی برای شرکت ها خواهد بود. avast! به خوبی انواع ویروس ها، کرم های اینترنتی و تروجان ها را پیدا کرده و آنها را از بین می برد. همچنین قادر به کنترل موردی (On Demand) و کنترل دائمی (On Access) می باشد. قابلیت های کلیدی نرم افزار:

- دارای موتور ویروس یابی با قابلیت های برجسته جستجو برای پیدا کردن انواع ویروس ها، تروجان ها و ...
- دارای محیطی ساده، شروع سریع جسجوی موردی (جستجوی قسمت های مشخص شده توسط کاربر)، تغییر سریع و راحت تنظیمات و ...
- ویژگی Resident protection. این ویژگی یکی از مهم ترین ویژگی های آنتی ویروس های امروزی می باشد و برای از بین بردن ویروس ها قبل از فعالیت و آلوده کردن سیستم (مانند ویروس های مقیم در حافظه) کاربرد دارد
- محافظت از Email ها. این آنتی ویروس دارای دو ماژول مستقل برای محافظت از Email ها می باشد
- جستجو کننده ای جامع که بر روی پروتکل های SMTP/POP3/IMAP4 کار می کند و قابلیت محافظت از تمام ایمیل کلاینت هایی را دارد که از این پروتکل ها استفاده می کنند
- پلاگینی برای محافظت از Microsoft Outlook
- قابلیت محافظت از سیستم در برابر انواع ویروس ها، کرم های اینترنتی و ... جدید و ناشناخته
- دارای Script Blocker برای محافظت و بلوکه کردن اسکریپت های آلوده ای که در کامپیوتر و یا مرورگر ها اجرا می شوند.
- قابلیت آپدیت خودکار و همیشگی آنتی ویروس
- دارای Virus Chest برای جداسازی ویروس ها از سیستم عامل ویندوز و قرنطینه آن ها در محیطی امن و جلوگیری از فعالیت مجدد آن ها
- یکپارچگی و هماهنگی کامل با سیستم عامل به گونه ای که در محیط ویندوز با راست کلیک بر روی هر فایل یا پوشه ای می توانید آن ها را اسکن کنید
- جستجو به وسیله خط فرمان با قابلیت های پیشرفته و مناسب برای کاربران حرفه ای



چک لیست امنیتی آنتی ویروس

هرگز از چندین آنتی ویروس بطور همزمان استفاده نکنید



آنتی ویروس را همیشه بروز رسانی کنید



معمولا وب سایت سازنده آنتی ویروسی که استفاده می کنید را برای دانلود وصله های جدید بازدید کنید



اسکن بلا درنگ را فعال کنید



همیشه لینک ها و پیوست ایمیل را اسکن کنید



فایروال آنتی ویروس را فعال کنید



یک برنامه زمانی برای اسکن داشته باشید

