

دوره کاردانی حرفه ای
مربیگری پایه شطرنج

کاربرد فناوری اطلاعات

مدرّس: هامون هرنده
نیم سال اوّل سال تحصیلی ۹۳-۹۲

KASPERSKY



مقدّمه



- با فراغیر شدن استفاده از کامپیووترها و افزایش زمان مشغولیت افراد با این وسیله و در محیط های مجازی و غیر فیزیکی (از طریق شبکه ها)، تمایلات انحرافی نوع بشر نیز تغییر شکل یافته اند.
- شاید تمایل برای ایجاد خسارت به یک تلفن همگانی توسط یک «وندالیست» در محیط مجازی پاسخی نگیرد، ولی این تمایل از بین نرفته و یا سرکوب نمی شود. بلکه به نسبت تغییرات محیط، تغییر می کند و به اشکال دیگر خود را نشان می دهد.



ویروس کامپیوتری چیست؟!

■ ویروس کامپیوتری، برنامه‌ای است که خود به خود تکثیر می‌شود و از کامپیووتری به کامپیووتر دیگر راه می‌یابد. این نوع ویروس‌ها درست مانند ویروس‌های بیولوژیکی که موجودات زنده را آلوده نموده و سلامت آن‌ها را مختل می‌کنند و از فردی به فرد دیگر سرایت می‌نمایند، سبب می‌شوند در کار کامپیوتروها اختلال ایجاد شود. به این صورت که اطلاعات را از بین می‌برند و سبب کندی یا ناکارآمد شدن برنامه‌ها می‌شوند.

■ بعضی از ویروس‌ها فقط اختلالات کوچکی ایجاد می‌کنند؛ اما وجود برخی دیگر ممکن است به مشکلات بزرگ و جبران ناپذیری منجر شود. به طور مثال ویروس‌ها گاه ممکن است اطلاعات کامپیوتروها را به طور کامل پاک کنند یا آن‌ها را تغییر بدنهند، اطلاعات موجود در کامپیووتر را سرقت کنند، برنامه‌هایی را ناخواسته به اجرا درآورند یا حتی، کامپیووتر را به طور کامل از کار بیندازند.



ویروس ها چگونه کامپیوتر ما را آلوده می کنند؟!

- هر ویروس با چسباندن خود به یک فایل ناقل، وارد کامپیوتر میزبان می شود. این فایل ناقل در اکثر موارد هیچ نشان خاصی از آلودگی به همراه ندارد و می تواند از هر قالبی برخوردار باشد. ممکن است یک سند در یک واژه پرداز، یک عکس دیجیتال، یک برنامه کاربردی و یا اجرائی باشد.
- واضح است که فایل ناقل از یکی از درگاه های مجاز کامپیوتر میزبان و با اجازه کاربر وارد می شود. این اجازه ممکن است به صورت ارادی (اتصال فلش مموری آلوده و اجرای فایل ناقل) و یا به طور ناخواسته (یعنی عدم انجام تنظیمات صحیح و پیشگیرانه برای کامپیوتر شخصی) صادر شود.



ویروس ها چگونه کامپیوتر ما را آلوده می کنند؟!

- پس درگاه های ورودی اطلاعات به درون کامپیوتر باید کنترل شده و در بد و ورود هر گونه اطلاعات، از سلامت آن اطمینان حاصل شود.
- عمدۀ ترین مبادی ورودی فایل های ناقل عبارتند از:
 - CDها، DVDها، Blu-Rayها و از این قبیل؛
 - هارد دیسک های قابل حمل؛
 - فلاش مموری ها؛
 - درگاه شبکه های محلی؛
 - درگاه شبکه جهانی (اینترنت).



انواع ویروس های کامپیو تری

- شاید بتوان ویروس های کامپیو تری را بر مبنای نحوه انتقال به دو گروه تقسیم کرد:
 - ویروس سُتّی: ویروس سُتّی یک قطعه نرم افزار کوچک بوده که بر دوش یک برنامه حقیقی حمل می گردد. مثلاً یک ویروس می تواند خود را به برنامه ای نظیر واژه پرداز الحاق نماید. هر مرتبه که برنامه واژه پرداز اجرا می گردد، ویروس نیز اجرا شده و این فرصت یا شанс را پیدا خواهد کرد که نسخه ای از خود را مجدداً تولید کرده و یا یک خرابی عظیم را باعث گردد.
 - ویروس های مبتنی بر پست الکترونیکی: ویروس هائی از این نوع، از طریق پیام های پست الکترونیکی منتقل می گردند. این نوع ویروس ها به صورت خودکار برای افراد متعدد پست خواهند شد. گزینش افراد برای ارسال نامه الکترونیکی بر اساس دفترچه آدرس پست الکترونیکی، انجام می گیرد.



آیا فقط ویروس ها آلوده کننده هستند؟!

- علت این نام گذاری، شباهت بسیار زیاد توالی عملکرد این برنامه های کامپیوتروی با ویروس های بیولوژیکی از نظر انتقال و آلوده سازی است.
- ولی تنها ویروس ها نیستند که محیط های کامپیوتروی را آلوده می کنند. بسیاری از «بَدَافَرَهَا» وجود دارند که از نظر مکانیزم انتقال و آلوده سازی شباهتی به ویروس ها ندارند، ولی آلاینده های قوی محیط های مجازی هستند. شناخته شده ترین این آلاینده ها عبارتند از:
 - کرم ها (**Worms**):
 - اسب های تروا (**Trojan Horses**):
 - بمب ها (**Bombs**).

کِرم ها (Worms)



- یک «کِرم»، برنامه نرم افزاری کوچکی بوده که با استفاده از شبکه های کامپیوتری و حفره های امنیتی موجود، اقدام به تکثیر خود می نمایند.
- نسخه ای از «کِرم»، شبکه را پیمايش نموده تا کامپیوتر های دیگر موجود در شبکه را که دارای حفره های باز امنیتی می باشند، پیدا کرده و نسخه ای از خود را در آن تکثیر نمایند. کرم ها با عبور از حفره های امنیتی موجود، نسخه ای از خود را بر روی کامپیوتر های جدید تکثیر کرده که هر یک از این نسخه ها نیز توانایی پیمايش شبکه، برای یافتن حفره های باز امنیتی جدید را خواهند داشت.



اسب های تروا (Trojan Horses)

- یک اسب تروا، نوع خاصی از آلاینده های کامپیوتروی می باشند. این برنامه ها ادعا دارند که قادر به انجام یک عملیات خاص می باشند (مثلاً شکل آن ها می تواند شبیه یک بازی کامپیوتروی ساده باشد). چنین برنامه هایی برخلاف ادعای خود، نه تنها عملیات مشتبی را انجام نخواهند داد بلکه باعث بروز آسیب های جدی پس از فراهم نمودن شرایط اجراء، می باشند. مثلاً ممکن است اطلاعات موجود بر روی هارد دیسک را حذف نمایند.
- اسب های تراوا دارای روشی برای تکثیر خود نمی باشند. از این رو سازندگان مدام آن ها را تبلیغ می کنند!



بُمب ها (Bombs)

- نرم افزارهای کوچکی هستند که مانند یک بمب ساعتی در مقطع مشخصی از زمان فعال شده و عملیات تخریبی از پیش تعیین شده ای را اجرا می نمایند.
- از منظر انتقال شباهت زیادی به ویروس ها دارند، ولی چون تمایلی به تکثیر و انتقال نداشته اند، از گروه جدا می شوند.
- این گونه آلاینده ها در اکثر مواقع موفق به دستیابی به اهداف خود می شوند. چرا که تا رسیدن به زمان مقرر هیچ گونه رفتار مشکوکی نداشته و تشخیص وجودشان به عنوان یک آلاینده بسیار مشکل است.
- جالب است بدانید بسیاری از این تخریب گران از سال ها پیش تا کنون هنوز هم از بین نرفته و قربانیان خاص خود را دارند!



علائم وجود ویروس در کامپیو تر

- در صورتی که کامپیو تر تان ویروسی شده باشد، حداقل یکی از موارد زیر در سیستم شما دیده می شود:
- مرور گر اینترنت شما عوض می شود، بدون آن که خودتان آن را تغییر داده باشید.
- بدون اینکه شما خواسته باشید، یک **Toolbar** جدید برایتان ایجاد می شود.
- فایروال سیستم (اگر فایروال فعال داشته باشید) به شما هشدار می دهد که یک برنامه جدید در سیستم تلاش می کند به اینترنت متصل شود.
- **shortcut** های جدید روی **desktop** ظاهر می شوند، بدون اینکه شما آن ها را ایجاد کرده باشید.
- به منوی **Favorite** مرورگرتان یک لینک جدید اضافه می شود.
- سیستم بدون دلیل خاصی کُند می شود.
- عملکرد **CPU** به طور غیر طبیعی افزایش پیدا می کند.
- **Pop-Up** های تبلیغاتی به شکل پنجره های کوچکی باز می شوند و به هیچ وجه نمی توان آن ها را بست.
- هر زمان که در محیط اینترنت به جستجو می پردازید، علاوه بر صفحات مورد نظرتان، صفحات نا مربوط دیگر هم برایتان باز می شوند.
- در پاره ای از موارد، دسترسی شما به اینترنت قطع می شود.
- در قسمت **control panel** در **add/remove programs**، برنامه های ناخواسته ای نصب می شود.
- فعالیت فایر وال یا آنتی ویروس سیستم به طور ناگهانی مختل می شود.

چه کنیم؟!



- اگرچه برای از بین بردن گُدهای ویروسی از درون یک کامپیوتر، بدون کمک هیچ نرم افزاری هم می توان اقدام کرد، اما چنین اقدامی مستلزم داشتن اطلاعات نسبتاً جامعی در خصوص علم نرم افزار و البته سیستم عامل موجود بر روی کامپیوتر شماست. از این رو چنین راه کاری در اینجا به کسی پیشنهاد نمی شود!
- در مواجهه با علائمی نظیر آن چه بر شمرده شد، پیشنهاد می شود از یک نرم افزار ویروس کُش تجاری و البته معتبر استفاده نمایید.
- انجام کارهایی نظیر عوض کردن سیستم عامل و یا رفع نقص آن از طریق نصب مجدد، راه کار ریشه ای نخواهد بود.



نرم افزار ویروس کُش تجاری چیست؟!

- **ویروس کُش تجاری (آنتی ویروس = Anti Virus)**، نرم افزاریست شامل سلسله دستورالعمل ها و فرمان هایی که توسط عده ای از متخصصان «بد افزارهای کامپیوتری» از یک شرکت خاص (و ترجیحاً معتبر) که برای شناسایی، جلوگیری از ورود و پاک سازی محیط کامپیوتر از آلاینده های مخرب نوشته شده و همانند تمامی نرم افزارهای کاربردی، در ازای مبلغی مشخص به کاربران متقاضی عرضه می شود.
- این نرم افزارها بر خلاف منطق پیچیده و تخصصی خود، از طریق یک «رابط کاربری گرافیکی» (GUI) بسیار ساده، با کاربران خود ارتباط برقرار کرده و از محیط کامپیوتر در برابر نفوذ و خراب کاری احتمالی محافظت خواهند کرد.

شرکت های معتبر؟!



دانشگاه جامع علمی کاربردی





ویژگی های یک آنتی ویروس خوب!

- آنتی اِکس (Anti-X) باشد.
- قابلیت به روز رسانی به صورت آفلاین را نیز داشته باشد.
- سرعت واکاوی بالا و بار کاری کم برای سیستم.
- قابلیت واکاوی فایل های سیستم عامل در هنگام بارگذاری (بوت).
- خدمات و پشتیبانی مناسب.
- رابط کاربری مناسب و سهولت استفاده از آن.



دانشگاه جامع علمی کاربردی

KASPERSKY lab





معرفی نرم افزار

- آنتی ویروس کَسپرسکی از نرم افزارهای ضدویروس معروف است که توسط شرکت کَسپرسکی ساخته شده است.
- قابلیت ها:
 - حفاظت، کشف و نابودی هر گونه آلاینده کامپیوتري.
 - کشف و نابودی روتکیت های ناشناخته.
 - جلوگیری از هک در چت رومها.
 - اسکن همزمان اینترنت و پست الکترونیکی.
 - قطع بدافزارها به طور سریع و بدون اجازه گیری.
 - ابزارهایی جهت امنیت هارد دیسک.
 - پشتیبانی رایگان از مشکلات کاربران از طریق سایت اصلی شرکت.



معرفی شرکت سازنده

- کَسپِرسکی (/kæ'spɜːrski/) با نام کامل لابراتوار کَسپِرسکی (به روسی: Лаборатория Касперского) شرکتی روسی است که در زمینه امنیت فضاهای کامپیوتروی فعال است.
- این شرکت در سال ۱۹۹۷ توسط «ناتالیا» و «یوگنی کَسپِرسکی» به وجود آمد. دفتر اصلی آن در شهر مُسکو، در کشور روسیه است و در انگلستان، فرانسه، آلمان، هلند، لهستان، رومانی، ژاپن، چین، کره جنوبی و آمریکا نمایندگی دارد.
- در حال حاضر، بر اساس رده‌بندی سایت TopTenReviews، نرم‌افزار کاسپِرسکی یکی از ۳ آنتی ویروس برتر دنیاست. در آخرین تست - Av-comparatives با کسب ۹۹٪ از امتیازات، مقام اول را در protection rate بدست آورد.



فضای نرم افزار

Kaspersky Anti-Virus 6.0 for Windows Workstations

Kaspersky
Anti-Virus 6.0

Your computer is protected

Settings

Protection

Scan

Full Scan
Quick Scan

Update

License

Protection

Kaspersky Anti-Virus protects your computer against security threats like viruses, network attacks, spam, spyware and other malicious programs.

File Anti-Virus
Mail Anti-Virus
Web Anti-Virus
Anti-Spam
Proactive Defense
Application Activity Analyzer
Registry Guard

Anti-Spy
Anti-Banner
Anti-Dialer

Anti-Hacker
Firewall
Intrusion Detection

Access Control
Device Control

Total scanned 18290
Active threats 0
Quarantined objects 0
Backup objects 0
Attacks blocked 0

Rescue Disk

Help | Support

Detected

Reports

A screenshot of the Kaspersky Anti-Virus 6.0 software interface. The main window title is "Kaspersky Anti-Virus 6.0 for Windows Workstations". The top bar includes the product name, a green circular icon, and a "Settings" button. Below the title, the text "Your computer is protected" is displayed. On the left, there's a sidebar with icons for "Scan" (magnifying glass), "Update" (globe), and "License" (certificate). The main content area has two columns under the heading "Protection". The left column lists "File Anti-Virus", "Mail Anti-Virus", "Web Anti-Virus", and "Anti-Spam" with checkmarks. The right column lists "Anti-Spy", "Anti-Hacker", and "Access Control" with checkmarks. Below these are sub-options: "Proactive Defense" (with "Application Activity Analyzer" and "Registry Guard"), "Anti-Spy" (with "Anti-Banner" and "Anti-Dialer"), "Anti-Hacker" (with "Firewall" and "Intrusion Detection"), and "Access Control" (with "Device Control"). At the bottom, there's a summary of system statistics: "Total scanned" (18290), "Active threats" (0), "Quarantined objects" (0), "Backup objects" (0), and "Attacks blocked" (0). A "Rescue Disk" icon is also present. The bottom navigation bar includes "Help | Support", "Detected", and "Reports".



سطح حفاظت

The screenshot shows the Kaspersky Anti-Virus 6.0 interface. On the left, there's a sidebar with 'Protection', 'Scan' (Full Scan, Quick Scan), 'Update', and 'License'. The main area has a green banner saying 'Your computer is protected'. Below it, under 'Protection', there's a list of features: File Anti-Virus, Mail Anti-Virus, Web Anti-Virus, Anti-Spam, Proactive Defense (Application Activity Analyzer, Registry Guard), Anti-Spy (Anti-Banner, Anti-Dialer), Anti-Hacker (Firewall, Intrusion Detection), and Access Control (Device Control). A red box highlights the 'Protection' section. At the bottom, there's a summary of scanned files and threats, and a 'Rescue Disk' button.

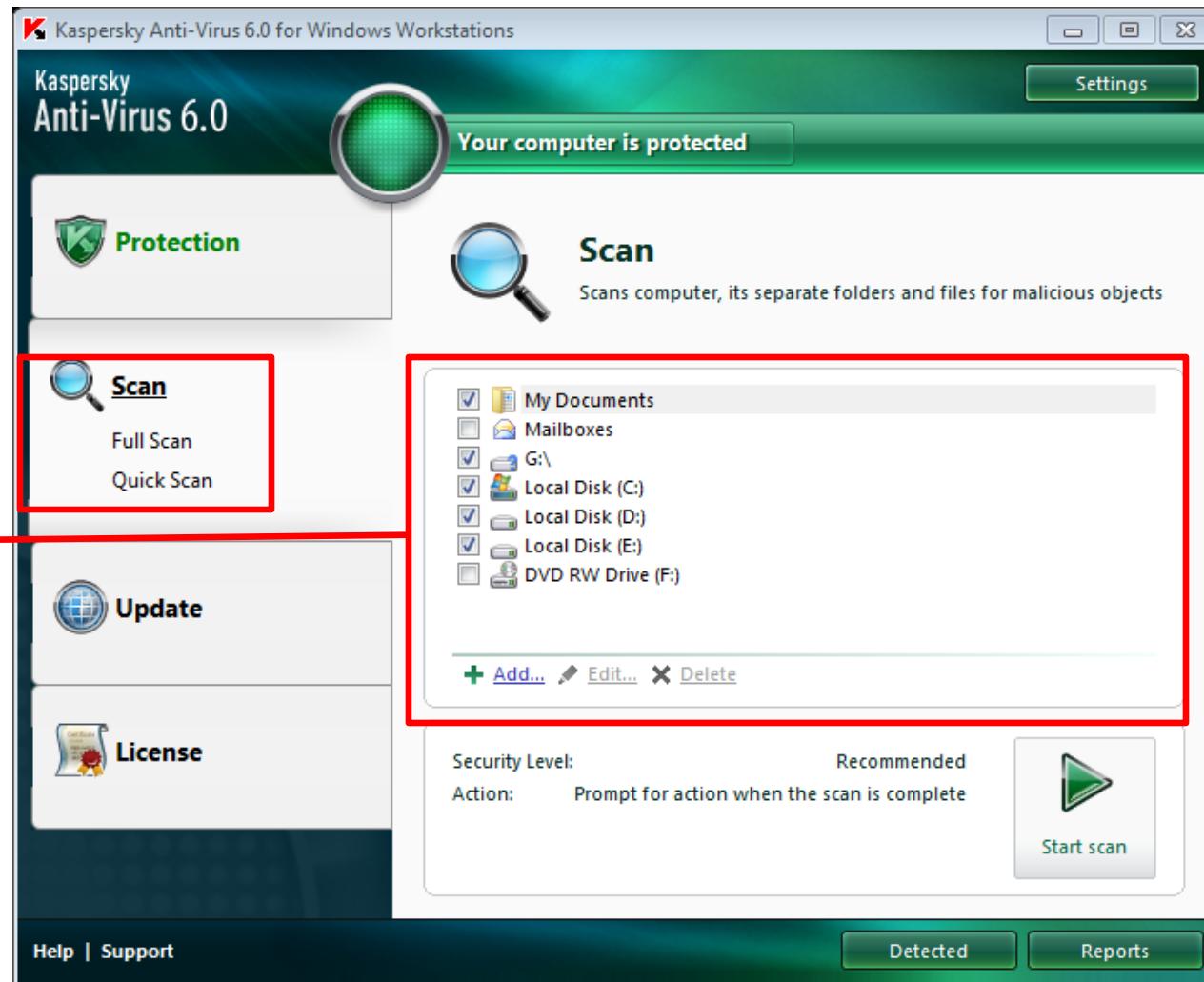
| | |
|---------------------|-------|
| Total scanned | 18290 |
| Active threats | 0 |
| Quarantined objects | 0 |
| Backup objects | 0 |
| Attacks blocked | 0 |

Help | Support Detected Reports

با فعال کردن هر گزینه، به سادگی می توان در مقابل تهدیدات احتمالی آماده بود.



واکاوی و بررسی



امكان «واکاوی
кампл» و
«واکاوی سریع»
برای درایوهای
انتخابی به
سادگی وجود
خواهد داشت.



به روز رسانی

Kaspersky Anti-Virus 6.0 for Windows Workstations

Kaspersky
Anti-Virus 6.0

Your computer is protected

Settings

Protection

Scan

Full Scan

Quick Scan

Update

Databases status: Up to date

Virus activity review

Threat types: Total: Databases release date:

| | | |
|-------------------|---------|------------------------|
| Malware | 7224955 | 1/4/2014 5:35:00 PM |
| Banners | 30623 | 12/27/2013 10:32:00 AM |
| Phishing sites | 459698 | 1/4/2014 5:17:00 PM |
| Spam | 104614 | 1/4/2014 5:57:00 PM |
| Malicious scripts | 30115 | 1/4/2014 9:22:00 AM |
| Network attacks | 1219 | 1/4/2014 7:31:00 AM |

Run mode: Every 2 hour(s)

Last update: 1/4/2014 6:39:06 PM

Roll back to the previous databases

Start update

Help | Support

Detected

Reports

با فشار یک دکمه،
پایگاه داده های
مربوط به
«بدافزارهای فعال در
سراسر فضای
مجازی» به روز
رسانی شده و از این
پس در کنکاش بسته
های اطلاعاتی
ورودی استفاده
خواهد شد.



عملیات به روز رسانی

Kaspersky Anti-Virus 6.0 for Windows Workstations

Kaspersky
Anti-Virus 6.0

Your computer is protected

Settings

Protection

Scan

Full Scan

Quick Scan

Update

Databases status: Up to date

Virus activity review

Threat types: Total: Databases release date:

| | | |
|-------------------|---------|------------------------|
| Malware | 7224955 | 1/4/2014 5:35:00 PM |
| Banners | 30623 | 12/27/2013 10:32:00 AM |
| Phishing sites | 459698 | 1/4/2014 5:17:00 PM |
| Spam | 104614 | 1/4/2014 5:57:00 PM |
| Malicious scripts | 30115 | 1/4/2014 9:22:00 AM |
| Network attacks | 1219 | 1/4/2014 7:31:00 AM |

Duration: 00:00:18

Downloaded: 20.9 KB

Average speed: 11.48 KB/s

Details... Stop update

License

Help | Support

Detected Reports



مجوز استفاده از خدمات

Kaspersky Anti-Virus 6.0 for Windows Workstations

Kaspersky
Anti-Virus 6.0

Your computer is protected

Settings

Protection

Scan
Full Scan
Quick Scan

Update

License

License grants you access to fully-functional version of Kaspersky Anti-Virus, allows you to update the application and consult technical support

License info
1714-000451-21261F80 [Commercial license for 450 computers](#)

License expires **8/5/2014 3:29:59 AM**
212 days remain.

Renew the license **Add/Delete** **View End User License Agreement**

Help | Support Detected Reports

A screenshot of the Kaspersky Anti-Virus 6.0 software interface. The main window has a green header bar with the title 'Kaspersky Anti-Virus 6.0 for Windows Workstations'. Below the header is a banner stating 'Your computer is protected'. On the left, there's a vertical menu with icons for Protection, Scan (with Full Scan and Quick Scan options), Update, and License. The 'License' section is highlighted with a circular callout. It shows a certificate icon and text explaining that it grants access to a fully-functional version, allows updates, and provides technical support. It displays license info (1714-000451-21261F80) and a link to a commercial license for 450 computers. It also shows the license expiration date (8/5/2014 3:29:59 AM) and remaining days (212). At the bottom, there are buttons for Renew the license, Add/Delete, and View End User License Agreement, along with links for Help | Support, Detected, and Reports.



خسته نباشید!

به امید دیدار...