ریاست جمهوری

سازمان مدیریت و برنامه ریزی

مرکز آموزش و پژوهش

امنیت کاربری فناوری اطلاعات (اکفا)

مدرس: مهدی هدایت فر

جلسه اول

مفاهیم امنیت سایبری

جلسه دوم

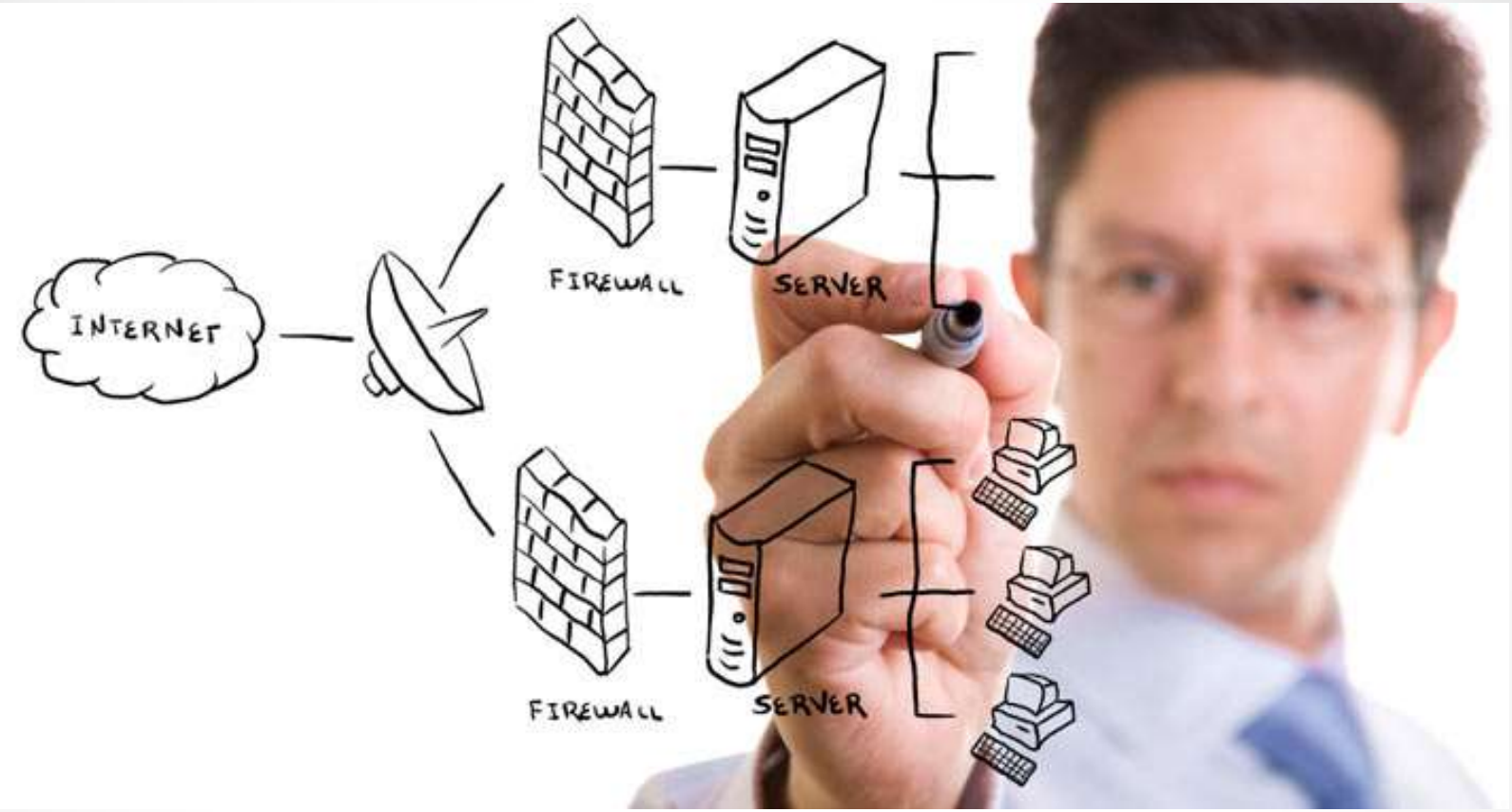
بهداشت سایبری و مفاهیم حقوقی

جلسه سوم

روشهای کنترل و مقابله

جلسه چهارم

نهادهای متولی و کار عملی

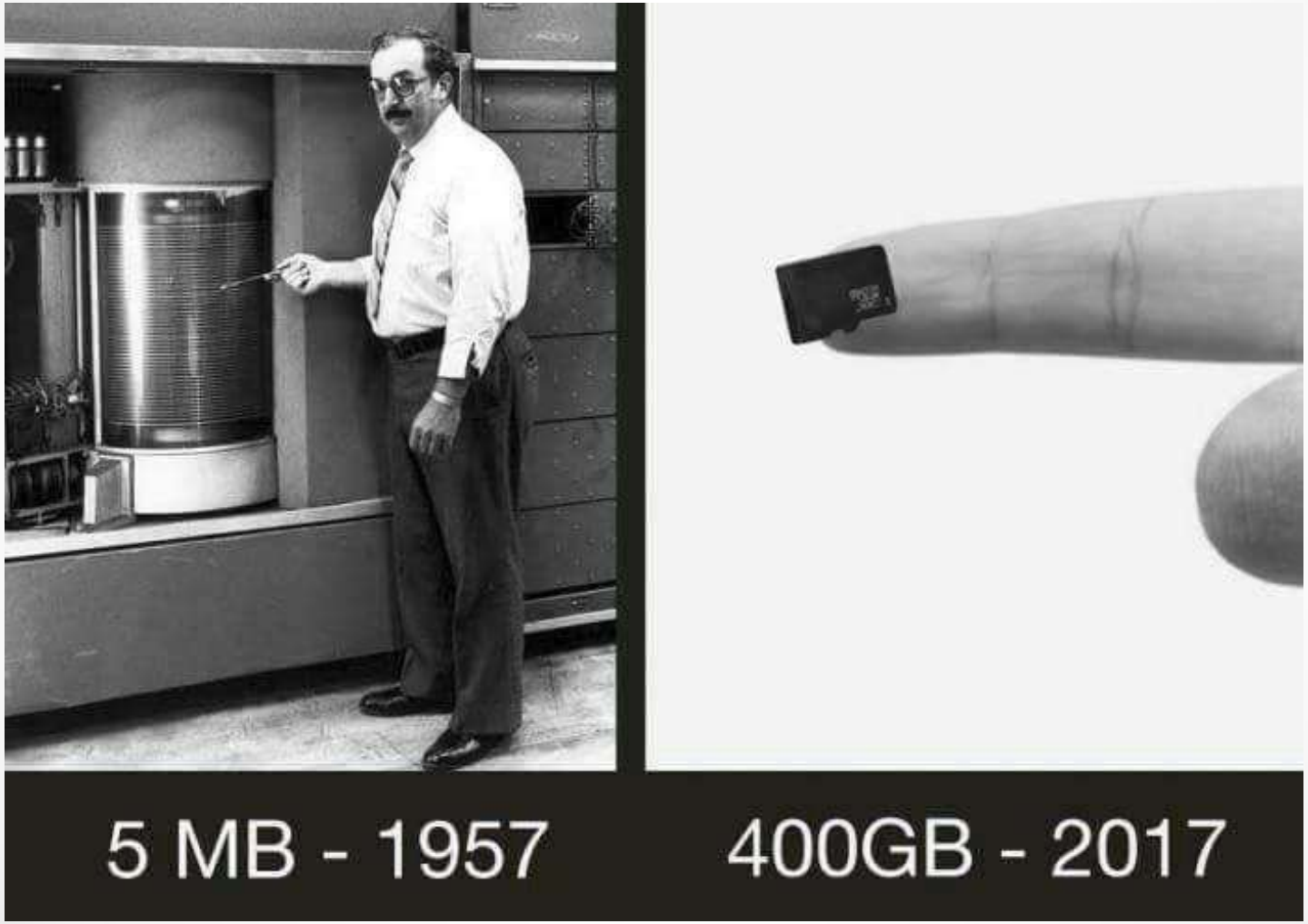


وضعیت کنونی دنیای فناوری

مقدمه: سرعت پیشرفت و نفوذ پارادایم‌ها

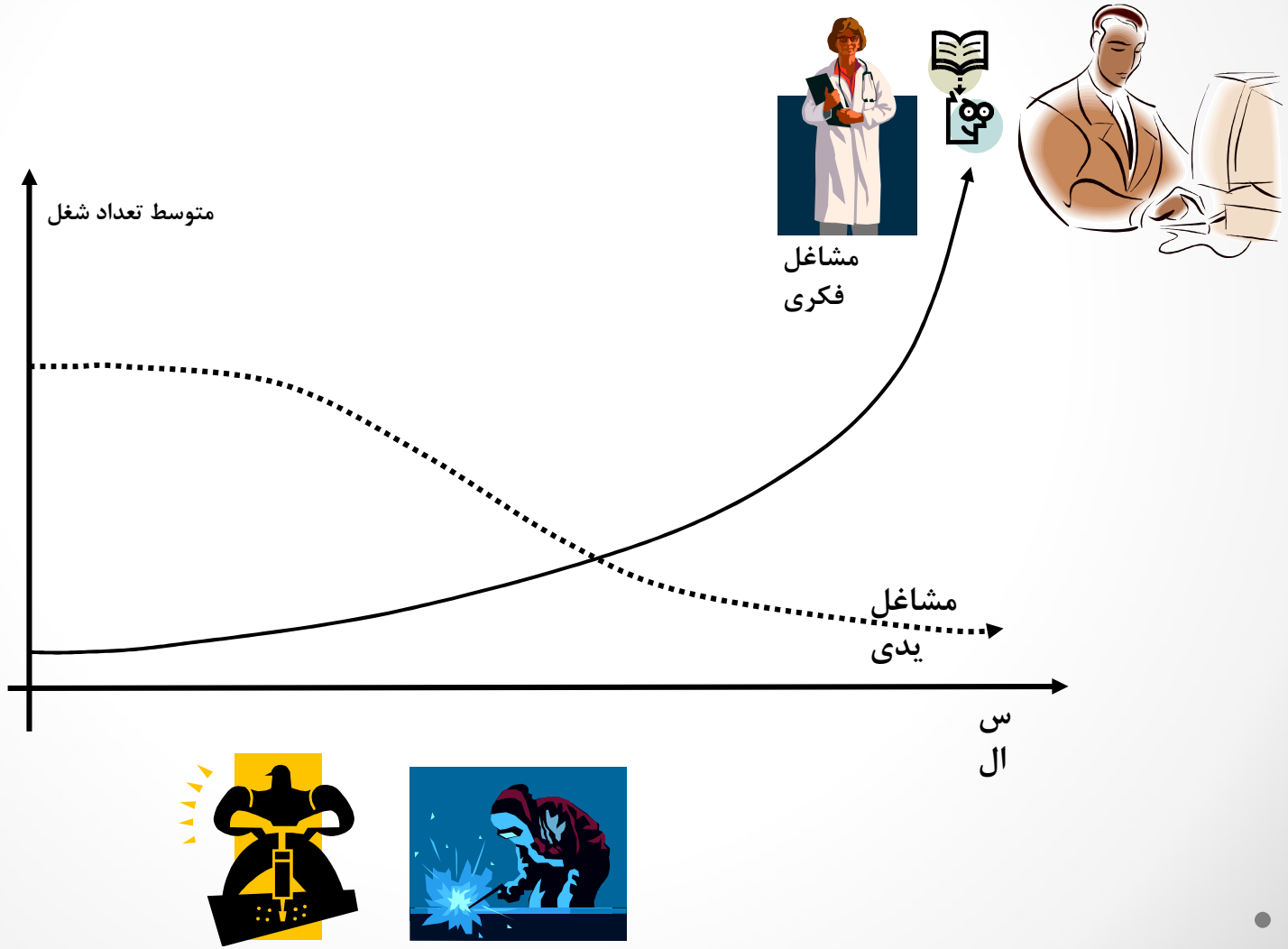
سرعت رسیدن به ۲۵٪ حجم بازار

رشد زیر ساخت ذخیره سازی فناوری اطلاعات در گذر زمان

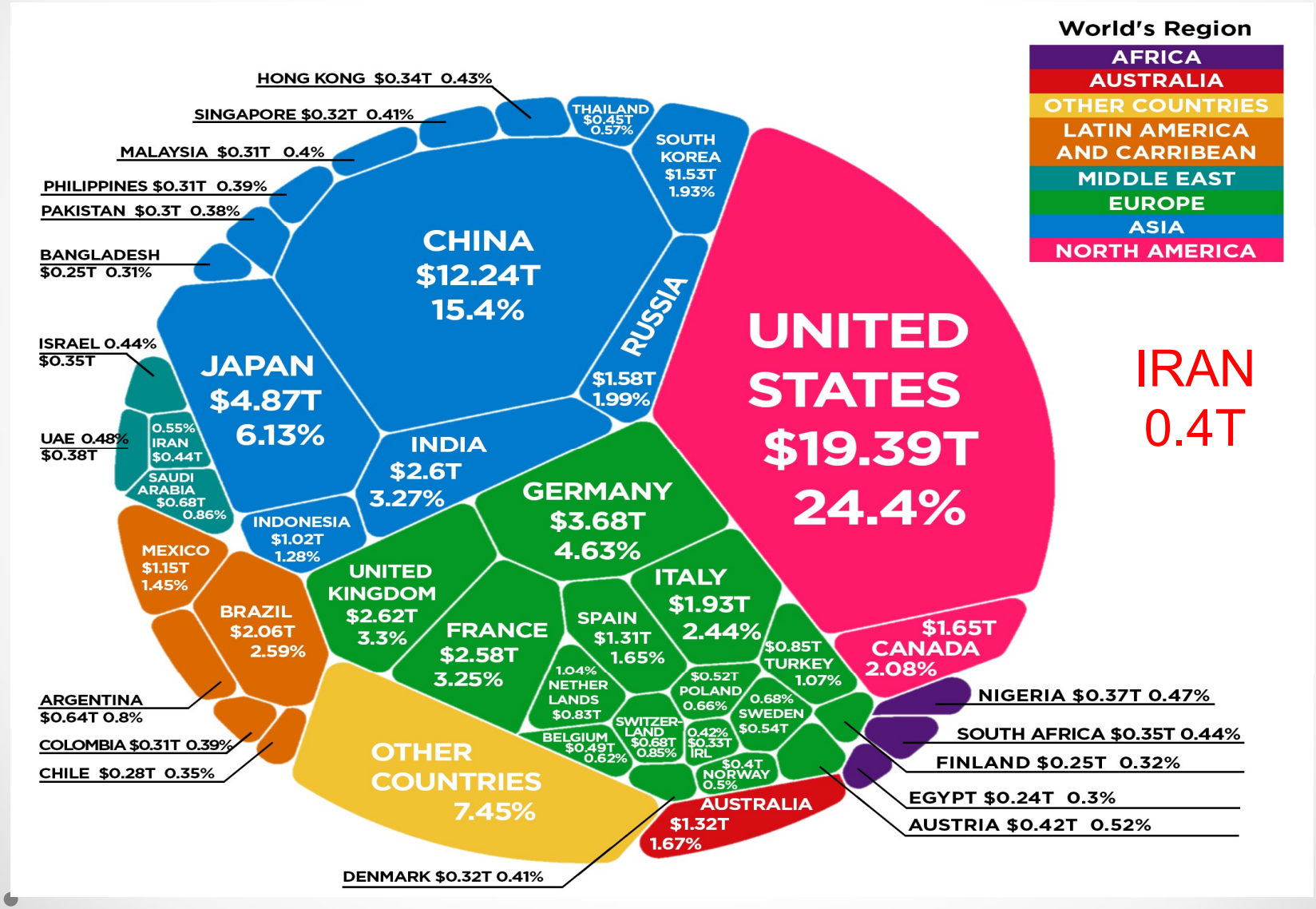


اتفاقاتی که در هر یک دقیقه در سال ۲۰۱۸ در فضای مجازی رخ می دهد

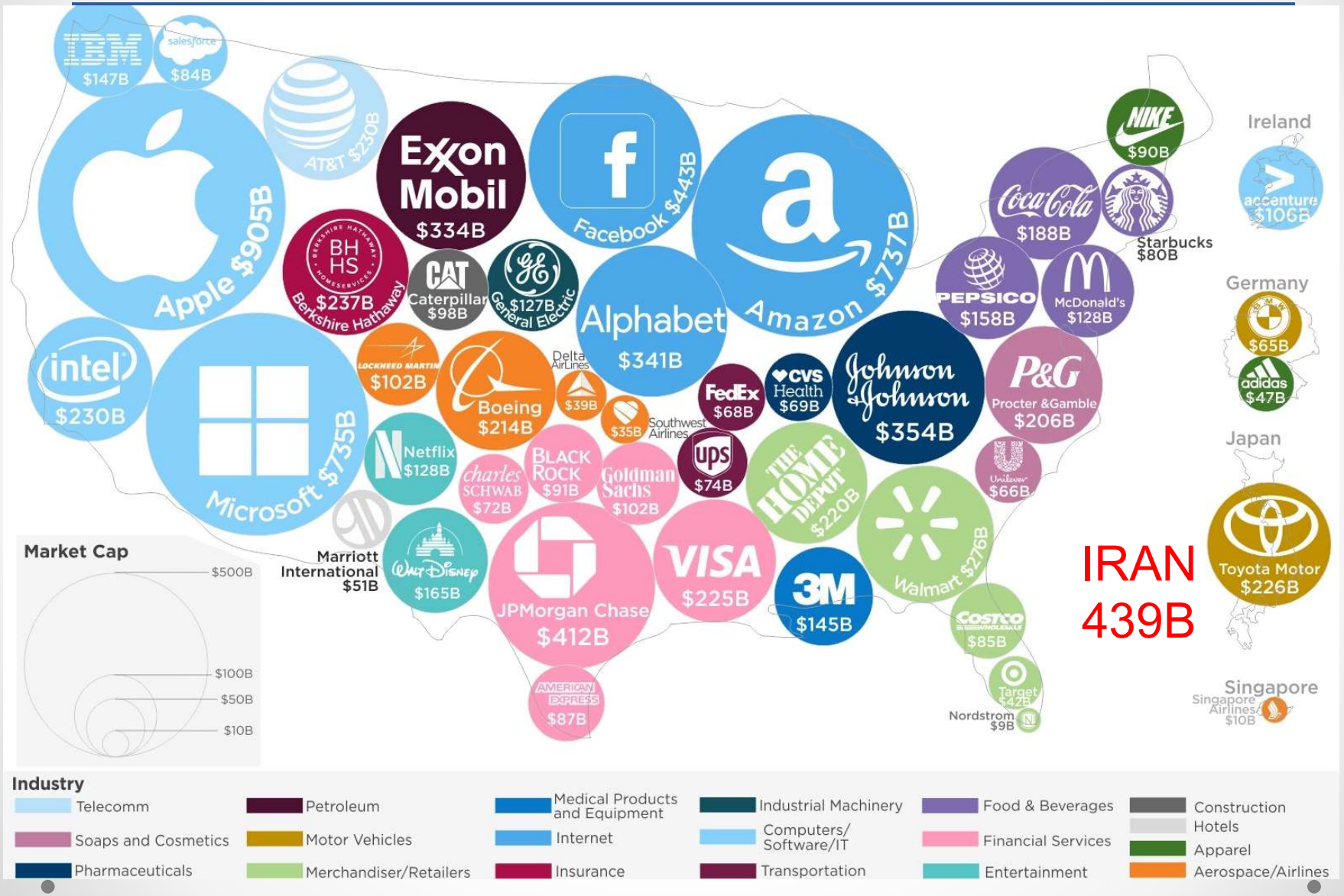
روند تحولات مشاغل



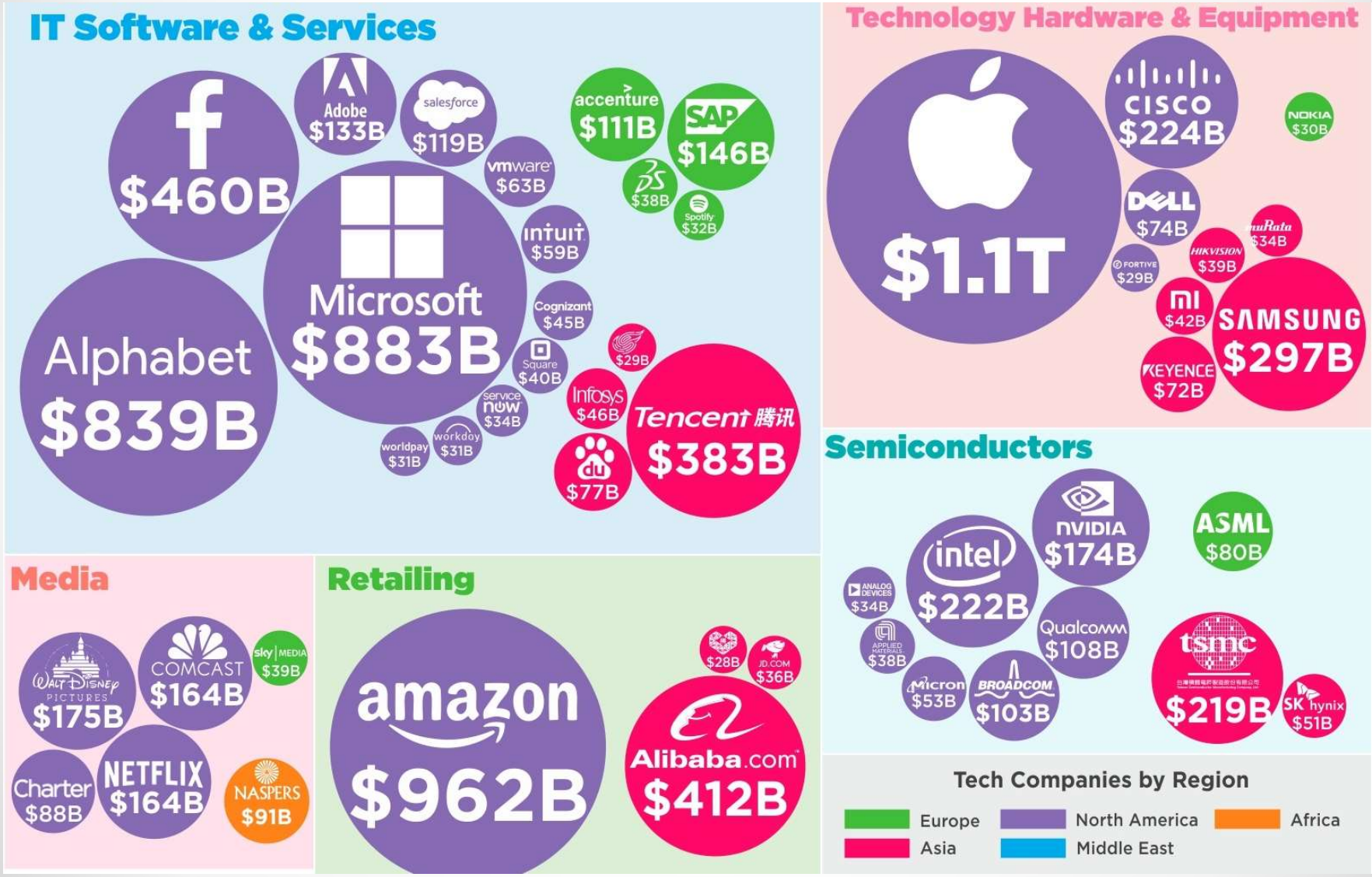
وضعیت GDP سال 2017 بر اساس کشورها



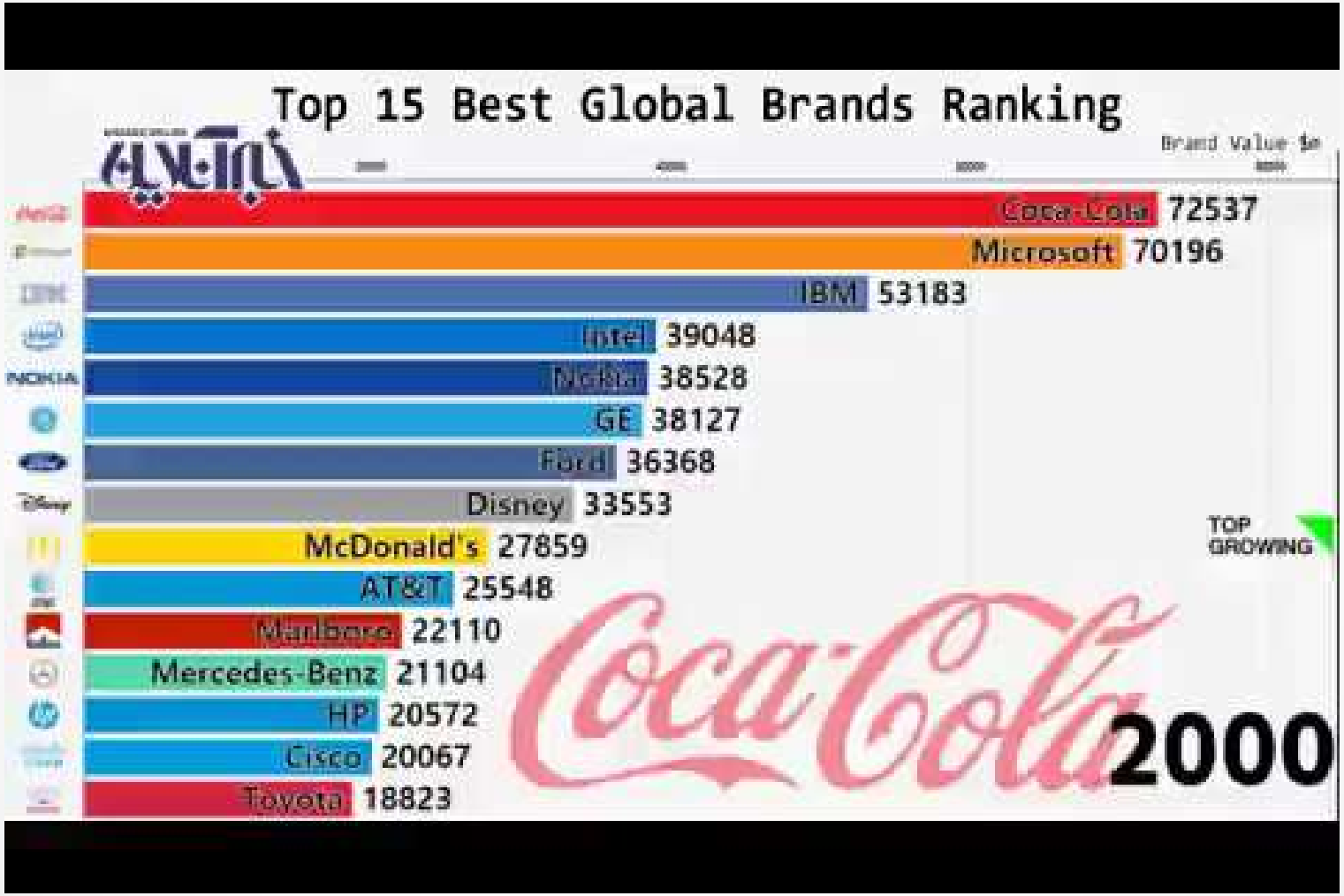
شرکت های برتر سال 2018

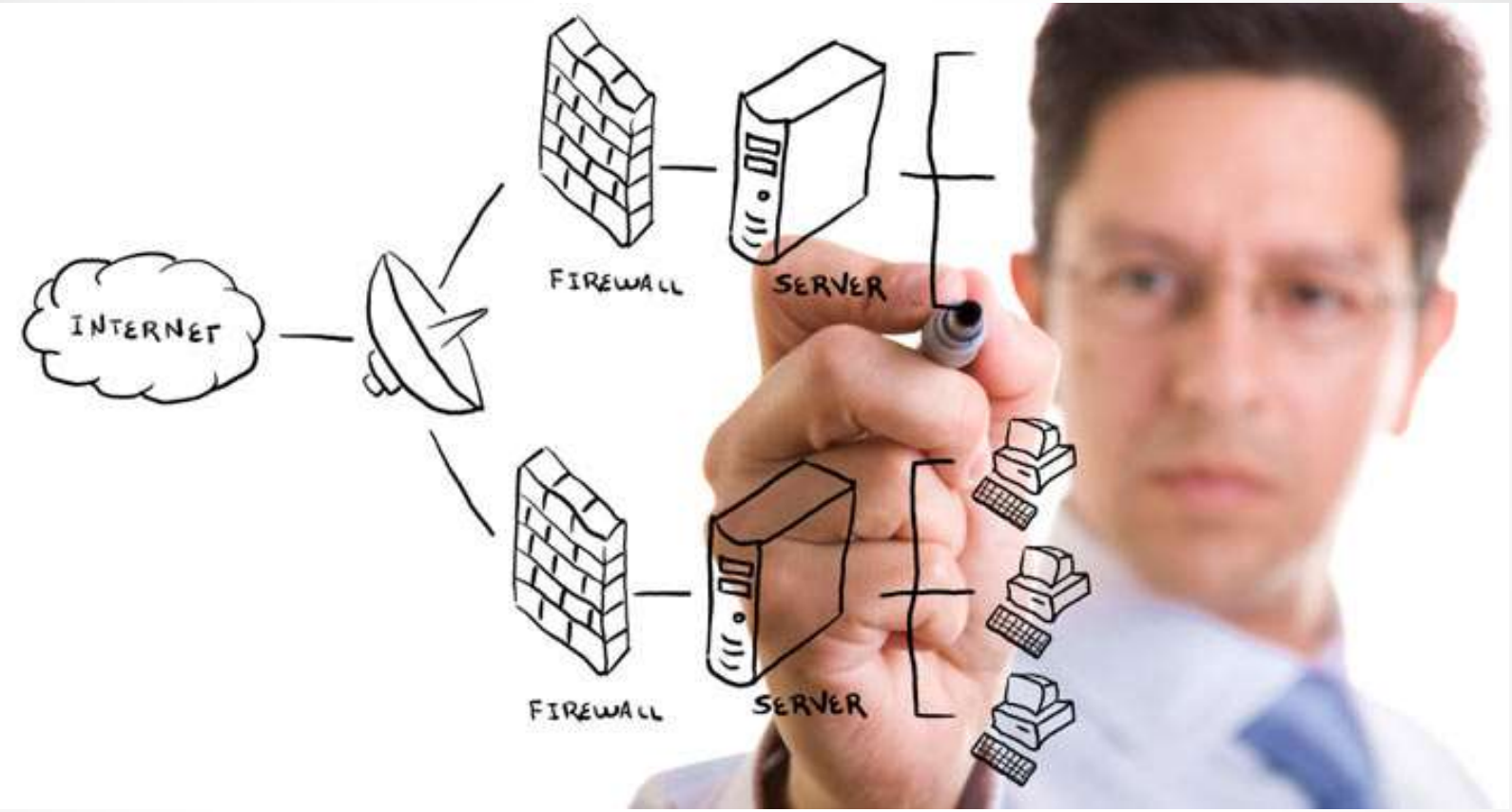


غولهای جهانی فناوری در سال 2018



روند رشد 15 برند برتر دنیا از سال 2000



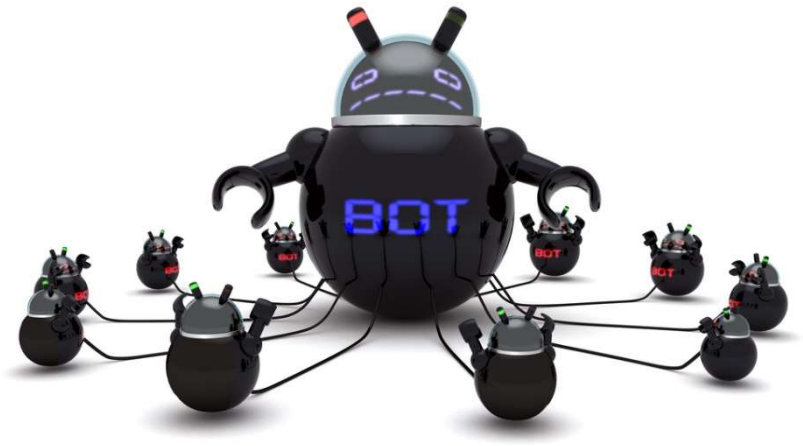


تهدیدات امنیت اطلاعات

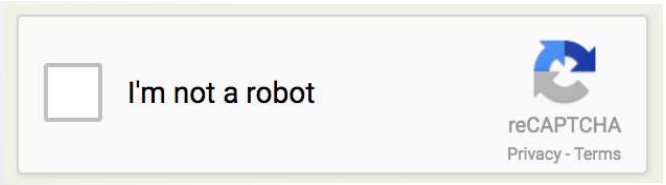
آگهی افزار

- به‌طور خودکار تبلیغات را ارائه‌می‌دهد.
- تبلیغات بالاپر pop-upبر روی وبسایت ها
- تبلیغات نمایش‌داده‌شده توسط نرم‌افزارها.
- اغلب اوقات نرم‌افزارها و برنامه‌های کاربردی که نسخه‌های رایگان عرضه‌می‌نمایند، همراه با آگهی‌افزارها می‌باشند.
- به عنوان ابزار تولید درآمد، توسط تبلیغات‌کننده‌ها، حمایت و یا نوشته‌می‌شوند.
- بسیاری از آن‌ها همراه با جاسوس افزارها برای ردیابی فعالیت‌های کاربران و سرقت اطلاعات همراه می‌شوند

رباتها



- برای انجام عملیات خاص به طور خودکار، ایجادشده‌اند
- برخی از ربات‌ها برای مقاصد بی‌ضرر ساخته‌شده‌اند (بازی‌های ویدئویی، مسابقات برخط، حراج‌های اینترنتی و...)
- می‌توان از ربات‌ها در باتنت‌ها (مجموعه‌ای از رایانه‌های متصل به‌هم که توسط شخص ثالث کنترل می‌شوند) برای حملات محروم‌سازی از خدمات (DDOS) استفاده نمود،
- به عنوان هرزنامه‌ها در ارائه‌ی تبلیغات در وب‌گاه‌ها، عنکبوت‌های وب که به داده‌های کارگزار آسیب‌می‌رسانند،
- برای توزیع بدافزارها که به عنوان اقلام جستجوی محبوب در وب‌گاه‌های بارگیری، تغییر چهره می‌دهند.
- وب‌گاه‌ها می‌توانند در برابر ربات‌ها، با استفاده از آزمون‌های کپچا (CAPTCHA)، در تأیید کاربران به عنوان انسان، از خود محافظت نمایند



اشکالات-BUGS

- نقصی است که منجر به تولید نتیجه‌ی نامطلوب می‌شود
- ناشی از خطاهای انسانی است و در کدمنبع و یا در برنامه‌ی مترجم وجود دارد
- اشکالات جزئی تنها بر روی رفتار یک برنامه اثر می‌گذارد و نمایش نتیجه‌ی برنامه را برای مدت زمان طولانی به تعویق می‌اندازد
- اشکالات مهم‌تر می‌توانند منجر به توقف عملیات و یا مکث برنامه (انجماد) گردند
- اشکالات امنیتی که شدیدترین نوع اشکالات می‌باشند، می‌توانند به نفوذگران اجازه دهند تا بدون احراز هویت و یا نادیده گرفتن امتیازهای دسترسی وارد سامانه شده و به سرقت اطلاعات بپردازند
- این اشکالات را می‌توان توسط توسعه‌دهندگان آموزش، کنترل کیفیت و ابزارهای تجزیه و تحلیل کد متوقف ساخت.

باج افزار-RANSOM

- در اصل دسترسی به یک سامانه را محدود ساخته
- برای برداشتن این محدودیت، درخواست باج می‌نمایند
- از طریق رمزگذاری فایلها بر روی دیسک‌سخت
- معمولاً مانند یک کرم رایانه‌ای و از طریق یک فایل بارگیری‌شده و یا وجود یک آسیب‌پذیری در خدمات شبکه، خود را بر روی رایانه‌ها گسترش می‌دهند.

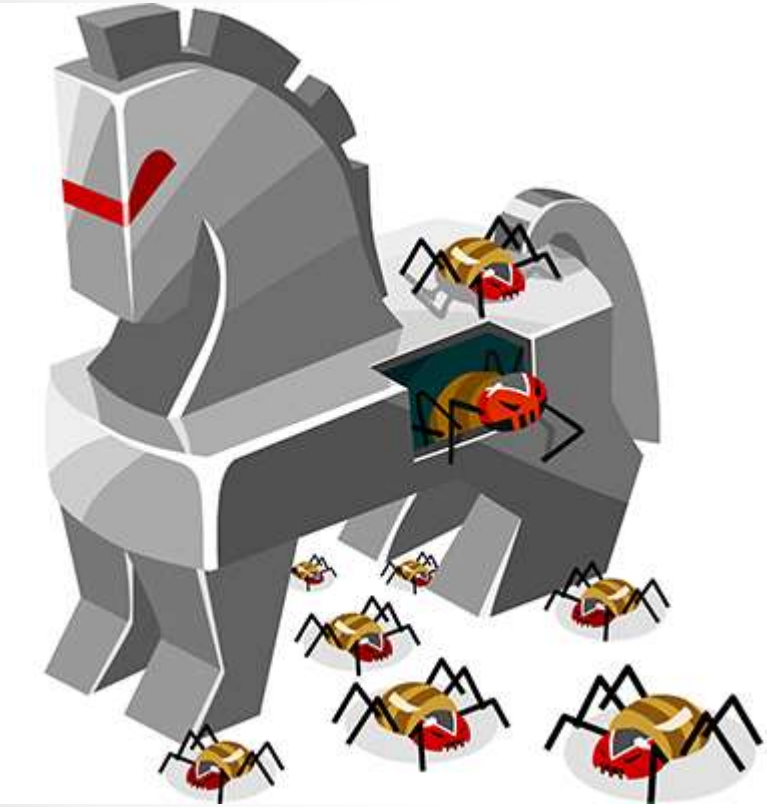
روت کیت-ROOTKIT

- برای دسترسی از راه دور و یا کنترل یک رایانه بدون تشخیص کاربر یا برنامه‌های امنیتی طراحی شده است
- امکان اجرای پرونده‌ها از راه دور، دسترسی و یا سرقت اطلاعات، تغییر تنظیمات پیکربندی سامانه، جایگزینی نرم‌افزارها (به‌ویژه نرم‌افزارهای امنیتی که قادر به تشخیص روت‌کیت می‌باشند)،
- نصب بدافزارهای پنهان، و یا کنترل رایانه به عنوان بخشی از یک بات‌نت
- پیشگیری، تشخیص و حذف روت‌کیت‌ها به دلیل عملیات پنهانیِ آن‌ها، کاری دشوار می‌باشد.
- محصولات امنیتی در تشخیص و حذف روت‌کیت‌ها مؤثر نمی‌باشند؛چرا که روت‌کیت‌ها به طور مستمر حضور خود را پنهان می‌سازند.
- سازمان‌ها و کاربران می‌توانند خود را در برابر روت‌کیت‌ها با استفاده از وصله‌های آسیب‌پذیری در نرم‌افزارها، برنامه‌های کاربردی، سامانه‌های عامل و به‌روز رسانی تشخیص بدافزار، اجتناب از بارگیری‌های مشکوک، و انجام پویش ایستای تجزیه و تحلیل، ایمن نگه‌دارند.

جاسوس افزار-SPYWARE

•بر روی فعالیت‌های کاربر، بدون آگاهیِ وی، جاسوسی می‌نماید.
•این قابلیت جاسوسی شامل نظارت فعالیت‌ها، جمع‌آوری ضربه‌های کلید، برداشت داده‌ها (اطلاعات حساب‌کاربری، ورود و داده‌های مالی) و موارد بیشتر می‌شود.
•اغلب دارای قابلیت‌های اضافی از جمله تغییر تنظیمات امنیتیِ نرم‌افزار یا مرورگر برای ایجاد تداخل با اتصالاتِ شبکه، نیز می‌باشند.
•با استفاده از بهره‌برداری از آسیب‌پذیری‌های نرم‌افزاری، مجموع‌ساختن خود همراه با نرم‌افزارهای قانونی و یا تروجان‌ها، خود را گسترش می‌دهند.

اسب تراوا-TROJAN



•خود را در قالب یک پرونده و یا برنامه‌ی معمولی، کاربر را برای بارگیری و نصب بدافزار فریب‌می‌دهند.

•امکان دسترسی از راه دور به رایانه‌ی آلوده را برای گروه مخرب فراهم‌می‌سازد

•زمانی که یک نفوذگر به رایانه‌ی آلوده دسترسی پیدا کرد، می‌تواند به سرقت اطلاعات (داده‌های مالی، داده‌های ورود، حتی پول الکترونیکی)، نصب بدافزارهای بیشتر، ویرایش پرونده‌ها، نظارت بر فعالیت‌های کاربر (تماشای صفحه‌نمایش، ثبت داده‌های واردشده از طریق صفحه‌کلید و ...)، به‌کارگیری رایانه در بات‌نت‌ها و فعالیت‌های اینترنتی ناشناس بپردازد.

ویروس کامپیوتری

توانایی کپی‌کردن خود و گسترش به رایانه‌های دیگر را دارا می‌باشد

اغلب از طریق اتصال خود به برنامه‌های مختلف و اجرای کد در زمان راه‌اندازی یکی از برنامه‌های آلوده، منتشر می‌شوند

همچنین می‌توانند از طریق پرونده‌های اسکریپت، اسناد، آسیب‌پذیری حملات تزریق کد در برنامه‌های تحت وب منتشرگردند

می‌توانند به منظور سرقت اطلاعات، آسیب‌رساندن به رایانه‌ی میزبان و شبکه، ایجاد بات‌نت‌ها، سرقت پول، نمایش تبلیغات، و... مورد استفاده قرارگیرند.

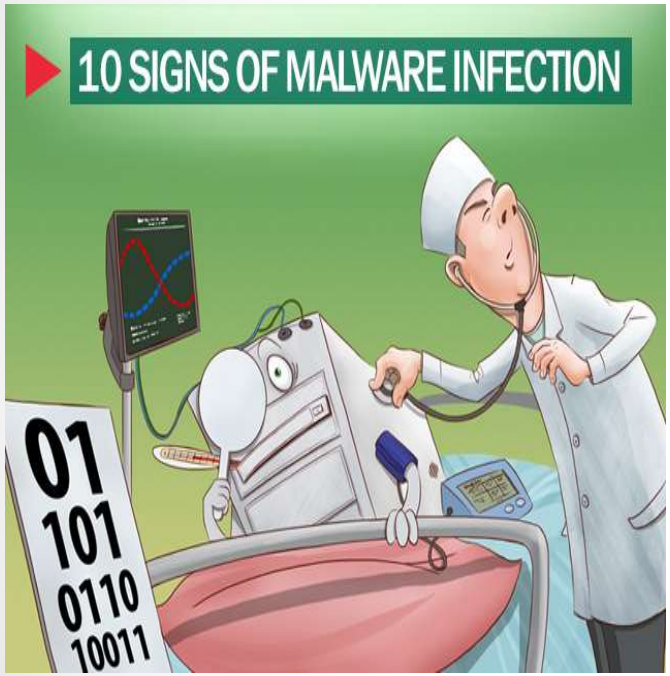
کرم رایانه ای-WORM

- برخلاف ویروس کرم‌ها خود را به برنامه‌های دیگر نمی‌چسباند.
- عموماً با اشغال پهنای باند به شبکه آسیب می‌رسانند
- که ویروس‌ها در بیشتر اوقات باعث خرابی برنامه‌های موجود در کامپیوتر آلوده و از دست رفتن اطلاعات موجود در آن می‌شوند.
- هدف کرم‌ها معمولاً استفاده از منابع می‌باشد و می‌تواند در دسترسی شما به منابع تأخیر بیاندازد.
- کرم در برخی از خصوصیات با ویروس مشترک است.
- مهمترین ویژگی مشترک آن‌ها این است که کرم‌ها نیز خود-همانندساز هستند،
- تولید مثل آن‌ها از دو جهت متفاوت است. اول اینکه، کرم‌ها مستقل و متکی به خود هستند، و محتاج به کد اجرایی دیگری نیستند.
- دوم، کرم‌ها از طریق شبکه‌ها، از ماشینی به ماشین دیگر منتقل و توزیع می‌شوند

هرزنامه-SPAM

- ارسال الکترونیکیِ پیام‌های ناخواسته می‌باشند
- رایج‌ترین رسانه برای هرزنامه‌ها، رایانامه می‌باشد
- غیرمعمول نیست که از پیام‌های فوری، نوشته‌ها، وب‌نوشت‌ها، انجمن‌های تحت وب، موتورهای جستجو و رسانه‌های اجتماعی برای ارسال هرزنامه استفاده نمایند.
- درست است که هرزنامه‌ها درواقع نوعی بدافزار نمی‌باشند، اما یکی از رایج‌ترین روش‌ها برای گسترش بدافزارها می‌باشند
- و این موضوع زمانی اتفاق می‌افتد که رایانه‌هایی که با ویروس‌ها، کرم‌های رایانه‌ای یا انواع دیگر بدافزار، آلوده شده‌اند، برای توزیع پیام‌های هرزنامه شامل بدافزارهای بیشتر، مورد استفاده قرارگیرند.
- کاربران می‌توانند با اجتناب از بازکردن رایانامه‌های ناشناس و خصوصی نگه‌داشتن آدرس رایانامه، خود را در برابر هرزنامه‌ها ایمن نگه‌دارند.

علائم بدافزار



1.اشکالات غیر-منتظره Unexpected Crashes

2.کاهش سرعت-Slow System

3.فعالیت بیش از حد هارد درایو-Excessive Hard Drive Activity

4.پنجره های ناشناس-Strange Windows

5.پیامهای عجیب و غریب-Peculiar Messages

6.فعالیت های بد برنامه-Bad Program Activity

7.فعالیت شبکه بصورت تصادفی-Random Network Activity

8.ایمیل ناخواسته-Erratic Email

9.آدرس های آی درون لیست سیاه-Blacklisted IP Address

10.غیرفعالی غیر منتظره آنتی ویروس-Unexpected Antivirus Disabling