



گردآورنده: شیرین شغلی
شماره دانشجویی: ۹۶۲۵۵۱۲۱۲۳
استاد راهنما: استاد روزگار

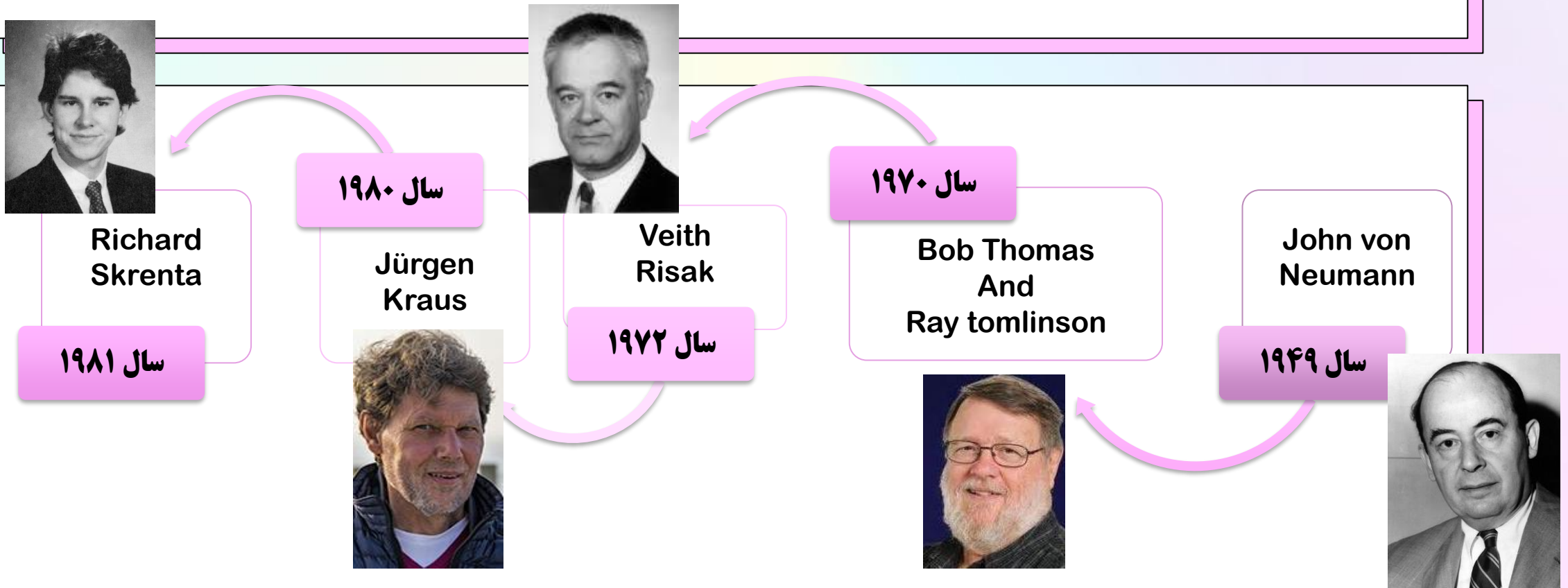
بررسی ویروس های کامپیوتری

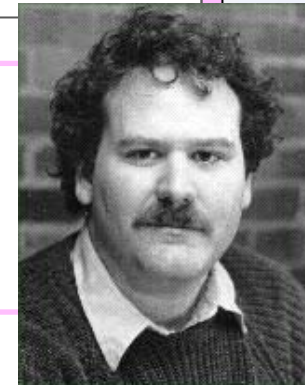
- تاریخچه ویروس ها
- چند مثال از ویروس ها
- ویروس چیست؟
- ویروس I LOVE YOU!
- متمایز کردن ویروس از نظر خصوصیات آن
- انواع ویروس ها
- راههای مقابله
- تعدادی از آنتی ویروس های قوی
- اگر کامپیوتر به ویروس مبتلا شد باید چه کارهایی انجام دهیم
- منابع

فهرست



تاریخچه ویروس ها





Fred Cohen

سال ۱۹۸۳ "فرد کوهن" دانشجوی دوره کارشناسی ارشد دانشگاه کالیفرنیا جنوبی در یک سمینار امنیت در دانشگاه پنسیلوانیا یک کد مفهومی را به خط فرمان یونیکس بر روی سیستم رایانه تایپ کرد و بعد از ۵ دقیقه کنترل تمامی رایانه‌های آن دانشگاه را در دست گرفت.

در آن زمان او موفق شد تمام سیستم‌های امنیتی رایانه‌ها را دور زده و آنها را غیرفعال کند. فرد کوهن نام این کد مخرب را **ویروس** گذاشت و بدین ترتیب اولین ویروس رایانه‌ای پا به عرصه گذاشت و کوهن توانست با ویروسش، کارشناسان فناوری را در فکر تغییرات اساسی در امنیت رایانه‌ها بیاندازد.

دکتر فرد کوهن در پروژه دکترای خود اثبات کرد که نمی توان یک برنامه جامع نوشت که با نگاه به یک فایل و یا یک دیسکت با احتمال ۱۰۰ درصد بتواند تشخیص دهد که ویروسی در آن وجود دارد یا خیر؟ به عبارت دیگر ، هیچ ضد ویروسی نمی توان نوشت که صد درصد بتواند همه ویروسها را پیدا کند . او همچنین خود یک ویروس نوشت و سرعت انتشار آن را شبیه سازی کرد و نشان داد یک ویروس چقدر سریع می تواند رشد کند و انتشار یابد .

چند مثال از ویروس ها

در سال ۱۹۸۸ اولین ویروس کشهای تجاری به بازار آمدند



command.com

:Jerusalem

در سیزدهم هرماه
اگر روز جمعه بود به
تمام فایل های com
و exe حمله می کرد
و آنها را پاک می
کرد.

:Lehigh

پس از ۴ بار اجرا
شدن به میزبان حمله
می کرد و فایل
command.com
را آلوده میکرد.

شروع ویروس های رمزگذاری شده

نکته بیزینسی

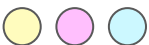
همزمان با ورود ویروس کشا به بازار تعدادی **ویروس تبلیغاتی** هم نوشته شد که کار خاصی نمی کرد ، فقط بر روی صفحه می نوشت که این فایل ویروسی است و بزودی تمام فایلها را آلوده خواهد کرد . این برای این کار انجام می شد که مردم ویروس را باور کنند و برای خرید ویروس کش پول خرج کنند .

در سال ۱۹۸۹ ویروسهای جدیدی نوشته شد حالا دیگر متخصصین برای همدیگر بصورت پی در پی ویروس می فرستادند تا روی آن کار کنند و ضد ویروس بنویسند . در همین سال بلغارها و روسها نیز شروع به ویروس نویسی کردند . در سپتامبر ۱۹۸۹ شرکت IBM ویروس کش خود را به همراه توضیحات کاملی برای تمام مشتریان فرستاد و تعداد زیادی کامپیوتر برای اولین بار scan شد .

در سال ۱۹۹۰ ویروسهای رمز شده زیادی نوشته شد که به سختی پاک می شد . همچنین ویروس کشا به اشتباه ممکن بود فایلهای سالم را ویروسی اعلام کنند . همین روزها یک فرد بلغاری که هیچ وقت نامش کشف نشد ویروسی نوشت که به سرعت انتشار می یافت .

همچنین فایلهای پشتیبانی که برای روز مبادا کپی می شد را نیز ویروسی میکرد و به همراه ویروس ، برنامه ویروس را هم می فرستاد تا مردم و برنامه نویسهای عادی نیز ویروس نویسی را یاد بگیرند و با کمی تغییرات از روی آن ویروس جدیدی بسازند .

در سال ۱۹۹۰ و زمانی که مرکز تحقیقات ضد ویروس اروپا در هامبورگ افتتاح شد ۱۵۰ ویروس و کارخانه ویروس سازی بلغارستان در حال کار بود . مقدار ویروسها به سرعت در حال افزایش بود . به عنوان مثال در دسامبر ۹۱ تعداد ویروسها ۱۰۰۰ تا و در فوریه سال بعد یعنی فقط در فاصله دو ماه ۱۳۰۰ تا بود .



بزرگترین مشکل در این سالها این بود که تعداد کسانی که بتوانند یک ویروس را در عرض چند ساعت تحلیل کنند بسیار کم بود و زمان یادگیری نیز برای تبدیل یک برنامه نویس معمولی به یک متخصص ویروسی بسیار طولانی بود. مشکل بعدی در اگوست همان سال به وجود آمد که یک سری نرم افزار بسیار شیک که کار کردن با آن نسبتا ساده بود، بیرون آمد که به کاربران معمولی اجازه می داد ویروس بنویسند در عرض یک سال صدها ویروس با استفاده از این نرم افزار ساخته شد.



در سالهای بین ۹۰ تا ۹۵ هر سال تعداد ویروسها ۲ برابر شد. هر چند این روند در سالهای بعدی ادامه نیافت ولی در هر صورت تعداد ویروسها در هر سال زیادتر می شود. در حال حاضر **ده ها هزار ویروس** وجود دارند.

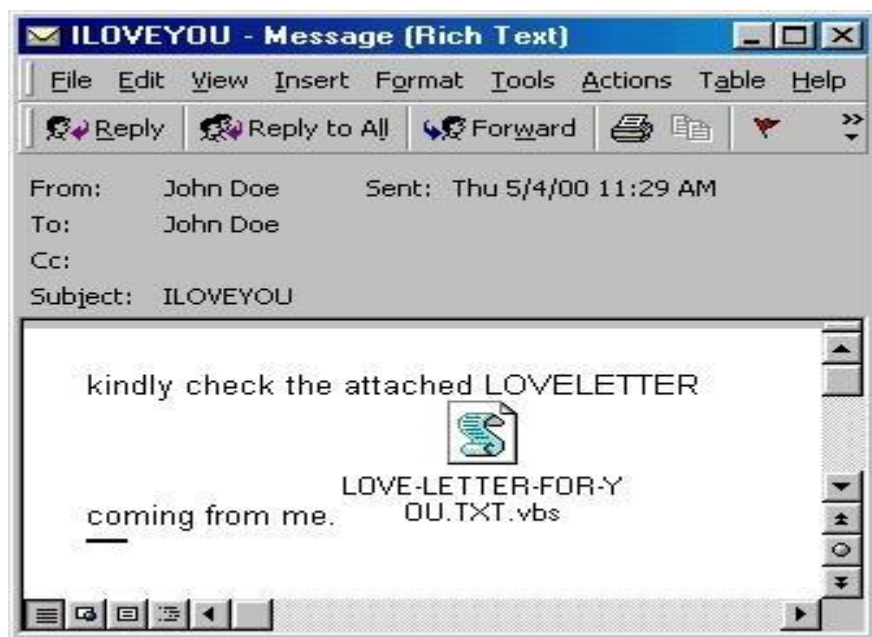
ویروس چیست؟

ویروس های کامپیوتری برنامه هایی هستند که مشابه ویروس های بیولوژیک گسترش یافته و پس از وارد شدن به کامپیوتر اقدامات غیرمنتظره ای را انجام می دهند. با وجودی که همه ویروس ها خطرناک نیستند، ولی بسیاری از آنها با هدف تخریب انواع مشخصی از فایل ها، برنامه های کاربردی و یا سیستم های عامل نوشته شده اند.

ویروس ها هم مشابه همه برنامه های دیگر از منابع سیستم مانند حافظه و فضای دیسک سخت، توان پردازنده مرکزی و سایر منابع بهره می گیرند و می توانند اعمال خطرناکی را انجام دهند به عنوان مثال فایل های روی دیسک را پاک کرده و یا کل دیسک سخت را فرمت کنند. همچنین یک ویروس می تواند مجوز دسترسی به دستگاه را از طریق شبکه و بدون احراز هویت فراهم آورد.



ویروس I LOVE YOU!



- این ویروس وحشتناک، ضمیمه ایمیل عاشقانه میشد و به محض باز کردن فایلی که در ظاهر یک فایل txt. بود، به تمام افراد موجود در لیست مخاطبین فرد ارسال میشد.
- این ویروس در سال ۲۰۰۰ شناسایی شد.
- نزدیک به ۱۰ درصد از کامپیوترهای متصل به اینترنت رو آلوده کرده بود (۴۵ میلیون کامپیوتر).
- ۱۰ میلیارد دلار ضرر مالی.
- خیلی از دولت ها و کمپانی های بزرگ سیستم ایمیل های خود را آف کرده بودند تا آلوده نشوند.
- گسترش از طریق ایمیل.

کارش چی بود؟
یک دانشجوی ۲۴ ساله فیلیپینی این ویروس را طراحی کرده بود که پسوردهای کاربران را بدست آورد و وارد حساب های اینترنتی افراد شود. او معتقد بود اینترنت حق همه است و این کار دزدی نیست.

متمایز کردن ویروس از نظر خصوصیات آن



انواع ویروس ها

Boot Sector یا سکتور بوت همانطور که از نامش نیز مشخص است قسمتی (سکتور) فیزیکی بر روی هارد دیسک است که شامل اطلاعاتی مانند چگونگی شروع بوت شدن سیستم عامل میباشد.



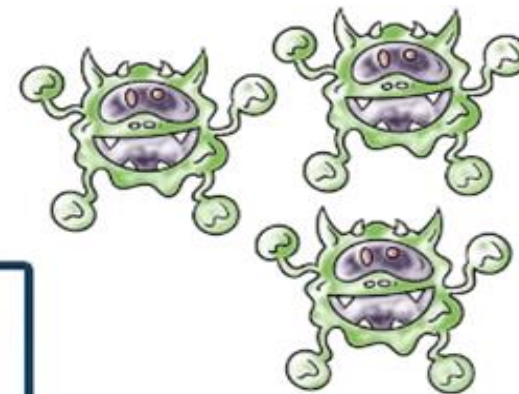
ویروس های کامپیوتری بوت سکتور (Boot Sector Virus)

این نوع از ویروس های کامپیوتری ، از خطرناک ترین ویروس ها به حساب می آیند زیرا با آلوده کردن بوت اصلی سیستم عامل، پاکسازی را تقریباً غیرممکن می سازند. قربانی این ویروس ها معمولاً مجبور خواهد بود سیستم خود را **format** کند. علاوه بر تخریب، **رمزگذاری فایل های بوت** نیز از دیگر روش های عملکرد این ویروس ها است. این ویروس ها از سال ۱۹۹۰ تاکنون عمدتاً از طریق ابزارهایی همچون فلاپی دیسک و فلش مموری به سیستم قربانیان خود نفوذ کرده اند.

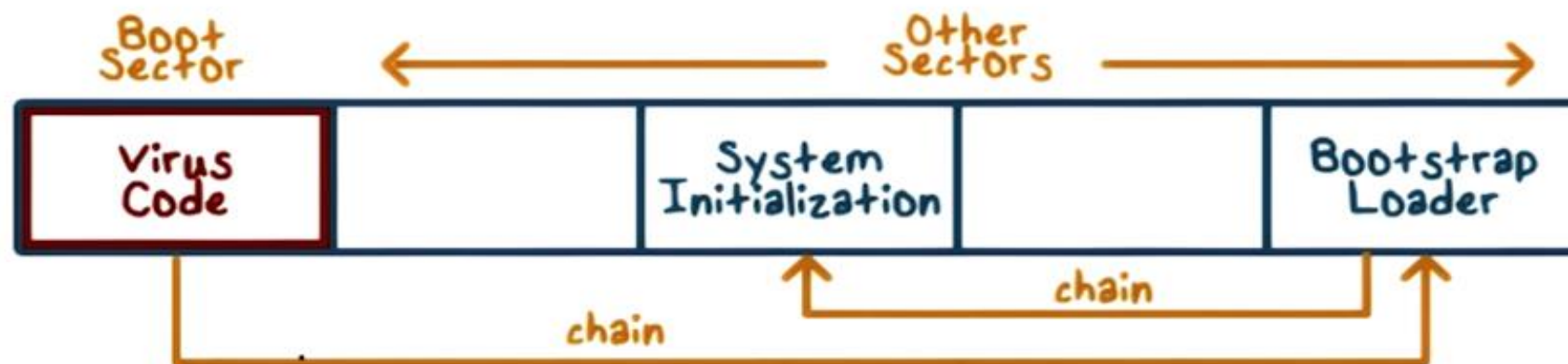
ویروس های کامپیوتری عملکرد مستقیم (Direct Action Virus)

این ویروس ها تا زمانی که کاربر ناخواسته فرمان اجرای آنها را صادر نکند، اجرای نمی شوند و معمولاً از طریق فایل هایی با فرمت های **exe** و **com** منتقل می شوند. این ویروس ها معمولاً بعد از فعال سازی اقدام به تکثیر خود می کنند. تأثیر این نوع از ویروس ها معمولاً به شکل غیرفعال سازی برخی از فایل ها دیده می شود و معمولاً **تخریب بی بازگشتی را در سیستم ایجاد نمی کنند**. فایل های آلوده شده نیز پس از اجرای آنتی ویروس ها پاکسازی و مجدداً قابل استفاده خواهند بود.

Boot Sector Virus



(a) Before infection



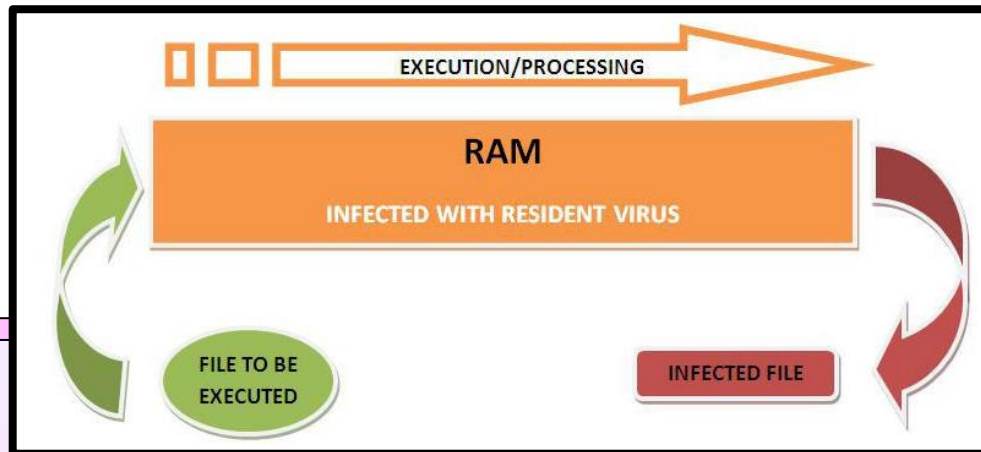
(b) After infection

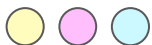
ویروس‌های رزیدنت (Resident Virus)

این نوع از ویروس‌ها، برخلاف ویروس‌های عملکرد مستقیم، برای نصب و انتشار خود نیازی به اقدام قربانی ندارند. آنها بلافاصله بعد از ورود به سیستم دست به کار می‌شوند و به طور اتوماتیک اقدام به نصب و انتشار خود در سیستم می‌کنند.

این ویروس‌ها گاهی با سرعت بالا شروع به تکثیر می‌کنند که این امر گاهی به شناسایی آنها توسط نرم‌افزارهای امنیتی کمک می‌کند اما در مواردی هم اقدام به انتشار تدریجی می‌کنند که این مسئله شناسایی آنها را به شدت دشوار می‌کند. در نسخه‌های پیشرفته و خطرناک، ویروس حتی می‌تواند خود را به نرم‌افزار آنتی‌ویروس متصل کند و همزمان با اسکن فایل‌ها، آنها را آلوده سازد.

نکته حائز اهمیت در مورد این ویروس‌ها این است که گاهی حتی با شناسایی و پاکسازی منشأ آلودگی، ویروس همچنان به حیات خود ادامه می‌دهد و حذف آن در پاره‌ای از موارد با استفاده از نرم‌افزارهای امنیتی ممکن نیست. استفاده از پچ‌های امنیتی سیستم‌عامل‌ها و یا بهره‌گیری از آنتی‌ویروس‌های لایو که از سیستم‌عامل دیگری استفاده می‌کنند، آخرین راه‌های ترمیم سیستم به حساب می‌آید.





ویروس‌های چندوجهی (Multipartite Virus)

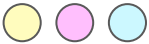
این ویروس‌ها به طور معمول از چندین روش توزیع بهره می‌گیرند. همچنین می‌توانند ضمن آلوده‌سازی فایل‌ها، در بخشی بوت سیستم نیز نفوذ کنند. آنچه به دشواری مقابله با این نوع ویروس‌ها می‌افزاید، **امکان مخفی‌سازی آنها در قسمت بوت سیستم** است. این ویروس‌ها **حتی پس از پاک‌سازی**، با راه‌اندازی مجدد سیستم عامل مجدداً اجرا و شروع به تکثیر خود می‌کنند.

استفاده از آنتی‌ویروس‌هایی که قابلیت اسکن در محیط بوت را دارند، از جمله راهکارهایی است که برای مقابله با این نوع ویروس کارایی خواهد داشت.

ویروس‌های پلی مورفیک (Polymorphic Virus)

شناسایی این ویروس‌ها از آن جهت دشوار است که ویروس می‌تواند **به طور پیوسته و مستمر تغییر شکل داده** و امضاء و ردپای خود را تغییر دهد. از آنجا که عملکرد آنتی‌ویروس‌ها بر مبنای روش تخریب و یا تکثیر ویروس‌ها و امضای آنهاست، تغییر در امضا آنها را دچار سردرگمی خواهد کرد.

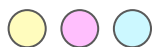
شناسایی این نوع ویروس، معمولاً برای شرکت‌های امنیتی و سازندگان آنتی‌ویروس‌ها هم پروسه‌ای بسیار زمان‌بر است.



ویروس‌های حفره (Spacefiller Virus)

این ویروس‌ها پیچیده‌ترین و در عین حال دشوارترین نوع ویروس‌ها برای هکرها هستند. دشواری در نوشتن این ویروس‌ها، باعث شده تا تعداد بسیار کمی از آنها در فضای سایبری وجود داشته باشد. این نوع ویروس‌ها برخلاف سایر ویروس‌ها که معمولاً به انتهای برنامه‌ها می‌چسبند خود را در **فضاهای خالی** درون برنامه‌ها جای می‌دهند. این نوع ویروس‌ها هیچ نشانه قابل مشاهده‌ای از خود بروز نمی‌دهند و حتی هیچ نشانه‌ای از افزایش حجم و کاهش سرعت در برنامه حمل‌کننده آنها دیده نمی‌شود.

این ویروس‌ها می‌توانند در درون یک برنامه معتبر و کاربردی جای بگیرند و بدون ایجاد اختلال در عملکرد برنامه میزبان، به راحتی به حیات خود ادامه دهند.



راههای مقابله:

1. اولین توصیه داشتن یک **ویروس کش قوی** و به روز روی کامپیوتر خودتان میباشد
2. کمی دقت در باز کردن ایمیل های رسیده هرگز ایمیلی که **فرستنده آن را نمیشناسید** باز نکنید.
3. استفاده از یک سرویس دهنده ایمیل مطمئن
4. در دانهادهای خود کمی دقت کنیم (هرگز اگر به یک نرم افزار نیاز دارید متوسل به سایتهای نامربوط نشوید. برای مثال اگر به نرم افزاری گرافیکی نیاز داریم هرگز دنباله این نرم افزار در سایت آموزش هک نگردیم چون در سورت موجود کمی مشکوک است نیست؟)
5. هرگز در چت از کسی که نمیشناسید و آشنایی کامل ندارید فایلی نگیرید و تا جایی که امکان دارد از شون بخواهید برایتان ایمیل کنند. (که اگر **ویروس کش ایمیل شناسایی** کند)
6. هرگز سی دی و فلاپی که به آن مطمئن نیستید را بر روی کامپیوترتان اجرا نکنید.
7. هرگز روی لینکهای پیشنهادی مشکوک کلیک نکنید.


تعدادی از آنتی ویروس های قوی



ولی حال اگر کامپیوتر به ویروس مبتلا شد باید چه کارهایی انجام دهیم:

1. نصب ویروس کش و به روز کردن آن و اسکن کردن (بازبینی) کل هارد توسط ویروس کش
2. اگر فایل یا پوشه ای دارید که برایتان خیلی مهم است سعی کنید یک Backup تهیه نمایید و Backup را روی سی دی نگه داری کنید.
3. اگر برایتان امکان دارد ویندوز خود را عوض کنید و درایو ویندوز قبلی را نیز فرمت نمایید





ممنون از توجه شما

ارتباط با من:

shirinshoqli@gmail.com

RESOURCES

- **Éric Filiol, Computer viruses: from theory to applications, Volume 1 ,2017**
- **Mishra Umakant Detecting Boot Sector Viruses- Applying TRIZ to Improve Anti-Virus Programs ,2012**
- **Avoine Gildas, Computer System Security: Basic Concepts and Solved Exercises ,2007**
- **favataradis.com**
- **us.norton.com**