به‌نام خداوند جان و خرد

بدافزارها و راه‌کارهای مقابله

(Virus, Worm, Trojan horse, Spyware, ….)

انتشارات پندار پارس

تألیف: مهندس مجید داوری دولت آبادی

عضو گروه امنیت GrayHat Hackers

Security Information Assets

شابک : 978-600-6529-68-4: ۱۸۰۰۰۰ ریال
شماره کتابشناسی ملی : ۳۷۰۰۲۲۴
عنوان و نام پدیدآور : بدافزارها و راه‌کارهای مقابله (Worm, Trojan, Spyware, Virus, ...)/ تالیف مجید داوری دولت‌آبادی.
مشخصات نشر : تهران : پندار پارس ، ۱۳۹۳.
مشخصات ظاهری : ۲۵۲ ص.: مصور.
موضوع : ویروس‌های کامپیوتر
موضوع : جرایم کامپیوتری
رده بندی دیویی : ۰۰۵/۸۴
رده بندی کنگره : QA۷۶/۷۶ ۱۳۹۳ ۲د۹و/
سرشناسه : داوری دولت‌آبادی، مجید، ۱۳۵۹ -
وضعیت فهرست نویسی : فیپا

انتشارات پندارپارس

دفتر فروش: انقلاب، ابتدای کارگرجنوبی، کوی رشتچی، شماره ۱٤، واحد ۱٦ **www.pendarepars.com**

تلفن: ٦٦٥٧٢٣٣٥ - تلفکس: ٦٦٩٢٦٥٧٨ همراه: ۰۹۲۱٤۳۷۱۹٦٤ **info@pendarepars.com**

نام کتاب : بدافزارها و راه‌کارهای مقابله

ناشر : انتشارات پندار پارس

ترجمه و تالیف : مجید داوری دولت آبادی

چاپ نخست : دی‌ماه ۹۳

شمارگان : ۵۰۰ نسخه

طرح جلد : رامین شکرالهی

چاپ و صحافی : روز

قیمت : ۱۸۰۰۰ تومان **شابک : ٤-٦٨-٦٥٢٩-٦٠٠-٩٧٨**

هدیه به روح پاکش

تقدیم به

سید پویامر تضویان

فهرست

سخنی با خوانندگان

امروزه در دنیای فناوری‌اطلاعات و کامپیوتر، حفظ و نگهداری اطلاعات به‌صورت سالم و مقوله امنیت اطلاعات از جایگاه ویژه‌ای برخوردار است که باید همواره در پایداری و استحکام آن کوشید. هم‌اینک وجود کدهای مُخرب و در اصطلاح بدافزارها تهدیدی جدی برای اطلاعات سازمان‌ها و کاربران به‌شمار می‌آیند که هر دم ممکن است صدمات جبران‌ناپذیری به منابع مالی و اطلاعاتی سازمان و یا کاربران وارد کنند. از بین رفتن اطلاعات و فایل‌های معتبر یک سازمان در واقع با درهم شکسته شدن آن سازمان در دنیای رقابت و کار برابری می‌کند که این امر در بیشتر مواقع توسط کدهای مُخرب و بدافزارهای تولید و منتشر شده در سطح اینترنت و شبکه‌های کامپیوتری صورت می‌گیرد. این روزها، محیط شبکه‌های کامپیوتری و اینترنت بستر مناسب و خوبی برای فعالیت و جولان بدافزارهای گوناگون به‌شمار می‌رود که باید هر متخصص و کارشناس فناوری اطلاعات با انواع آنها و روال‌ها و ساختارهای آنها و همچنین روش مقابله با آنها آشنایی کامل داشته باشد.

هدف از تألیف این کتاب آشنایی بیشتر کارشناسان و متخصصان با نحوه عملکرد و نوشتن نرم‌افزارها و کدهای مُخرب می‌باشد. با کمک این کتاب می‌توان آشنایی بیشتری در مورد ساختار انواع کدهای مُخرب به‌دست آورد. این آشنایی می‌تواند تا نوشتن یک کدمُخرب ادامه داشته باشد. الگوهای کدهای مُخرب در این کتاب به‌طور کامل بررسی خواهد شد. یک کارشناس و متخصص امنیت بایستی با ساختار و الگوهای مخصوص کدهای مُخرب آشنایی بیشتری داشته باشد تا در زمان انتشار یک کد مُخرب در سطح شبکه، اولا بتواند نوع و ساختار را شناسایی و تشریح کند و در ادامه بتواند برای برخورد با آن راه‌کارهایی ارائه نماید. محافظت از انواع کدهای مُخرب نیز باید در تمامی شبکه‌ها و سیستم‌ها مدنظر قرار گیرد. نحوه انجام این‌کار در این کتاب ارائه شده است. این کتاب تلاش می‌کند مخاطب را ابتدا با الگوهای انواع کدهای مُخرب آشنا کند و سپس به ارائه راه‌کارهایی برای محافظت از سیستم‌ها و شبکه‌ها درمقابل این‌گونه کدها بپردازد. کتاب تلاش دارد تا حد امکان تکنولوژی‌های نوین را در مورد انواع کدهای مُخرب معرفی نماید.

اینجانب به‌عنوان عضو کوچکی از خانواده بزرگ امنیت و شبکه درصدد گردآوری و تألیف کتابی مرجع به‌منظور افزایش آگاهی متخصصان، دانشجویان و مدیران شبکه در زمینه ساختار و عملکرد بدافزارها و نرم‌افزارهای ضدویروس بودم تا آنها را با اصول فنی کدهای مُخرب آشنا و آگاه سازم تا بتوان از آن در طراحی و پیاده‌سازی بدافزارها و نرم‌افزارهای ضدویروس استفاده نمود (گرچه مدیران و متخصصان امنیت شبکه حُکم اساتید اینجانب را دارند، اما به حُکم وظیفه برخود لازم دانستم که این آگاه‌سازی را انجام دهم.)

شیرازه اصلی کتاب حاضر برگرفته از کتاب‌ها و منابع معتبر و استاندارد شاخه امنیت داده، بدافزارها، کدنویسی بدافزارها و نرم‌افزارهای ضدویروس و بررسی انواع کدهای مُخرب می‌باشد که با تجربیات اینجانب در این خصوص آمیخته شده است، که به‌فرم کاملا آزاد از مطالب و تجربیات گردآوری، و دخل و تصرفی نیز با آن همراه بوده است. پیشاپیش تمام کاستی‌های آن را می‌پذیرم و ضمن پوزش از اساتید، متخصصان، دانشجویان و مدیران عزیز، انتقادات و راهنمایی‌های دلسوزانه آنها را به دیده منت پذیرا هستم.

(m_Davari@TOP-co.ir)
(m_Davary@Parshack.zzn.com)

پس از سپاس و ستایش به درگاه پروردگار از تمام دوستان و اساتید عزیزی که مهربانانه دست مرا در انجام اینکار ناچیز فشردند، سپاسگزاری می‌کنم. برخود لازم می دانم از زحمات بی‌دریغ سرکار خانم مهندس سیده پونهٔ مرتضویان تشکر و قدردانی نمایم. زحمات خاضعانهٔ ایشان سهم بزرگی در تهیه و تدوین این کتاب داشته است.

در پایان از مدیریت فرزانه انتشارات پندار پارس جناب آقای مهندس یعسوبی و تمامی همکارانشان که زحمت چاپ کتاب را متقبل شده‌اند، صمیمانه قدردانی می‌نمایم.

یا رب چو به وحدتت یقین می‌دارم

ایمان به تو عالم آفرین می‌دارم

دارم لب خشک و دیده‌ی‌تر بپذیر

کز خشک و تر جهان همین می‌دارم

(مجید داوری دولت آبادی –پاییز ۱۳۹۳)

فصل نخست

معرفی انواع بدافزارها

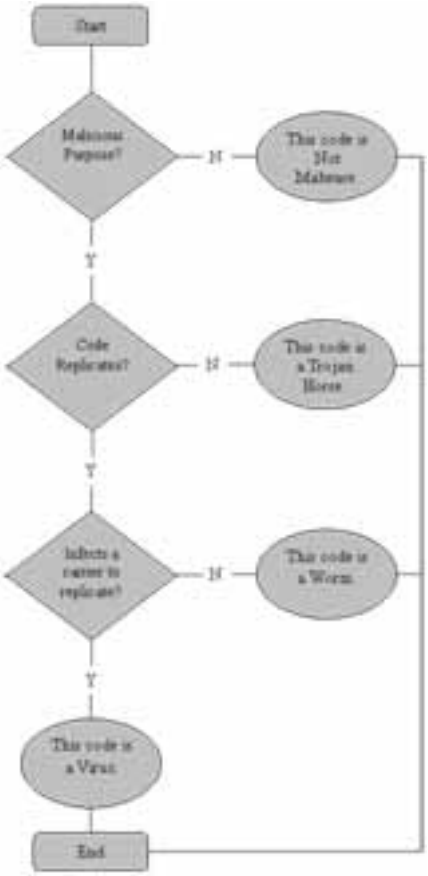
بیشتر نرم‌افزارهای مُخرب برپایهٔ و برعلیه سیستم‌عامل ویندوز طراحی و نوشته می‌شوند و دلیل آن هم وجود آسیب‌پذیری‌ها و ضعف‌های بی‌شمار در این نوع سیستم‌عامل می‌باشد که از دیرباز مورد توجه و حمله نفوذگران و انواع نرم‌افزارهای مُخرب بوده است و هم اکنون نیز این حملات از جوانب گوناگون علیه این نوع سیستم‌های‌عامل وجود دارند. معمولا کاربران معمولی، تمامی این نرم‌افزارهای مُخرب را با نام ویروس می‌شناسند و تفاوتی بین آنها از نظر عملکرد قائل نمی‌شوند، درصورتی‌که انواع مختلفی از نرم‌افزارهای مُخرب در دنیای کامپیوتر موجود می‌باشند و هر کدام عملکردی متفاوت با دیگری دارند. اینک در این فصل قصد داریم به بررسی هریک از این نرم‌افزارها بپردازیم که در ادامه به آنها در اصطلاح بدافزار می‌گوییم. نرم‌افزارهای مُخرب کامپیوتری از جمله موارد اسرارآمیز و مرموز در دنیای کامپیوتر بوده که توجه بیشتر کاربران، برنامه‌نویسان و مشاوران امنیتی شبکه‌های کامپیوتری و حتی افراد عادی را که از کامپیوتر برای کارهای معمولی خود استفاده می‌کنند، به خود جلب کرده‌اند. سالانه هزینه هنگفتی برای جلوگیری از انتشار و بالا بردن امنیت شبکه‌ها و کامپیوترها در مقابل ویروس‌ها صرف می‌شود.

درحقیقت نرم‌افزارهای مُخرب که معروف‌ترین آنها، ویروس‌ها نام دارند را می‌توان نخستین تخریب‌گران دنیای کامپیوتر به‌شمار آورد. قِدمت ویروس‌ها به زمان ابداع نخستین نرم‌افزارها می‌رسد؛ زمانی‌که مفهومی به نام شبکه وجود نداشت و کسی حتی در رویا هم نمی‌توانست ساختاری شبیه اینترنت را تصور کند. کاربران قدیمی کامپیوتر به یاد دارند حتی درهمان روزهای خوب و پر خاطره، کار با سیستم‌عامل سیاه و دوست داشتنی DOS نیز هزاران ویروس وجود داشت و در اوایل، تنها یک شوالیه قدرتمند به نام ابزار Toolkit (دکتر سالومون) وجود داشت که یک تنه تمامی این ویروس‌ها را نابود می‌کرد. در آن روزها نیازی به حضور یک گارد ویروس در حافظه نبود و پویش دوره‌ای سیستم توسط ضدویروس‌ها یا کنترل دیسکت‌های ورودی می‌توانست برای مبارزه با آنها کافی باشد. دلیل اینکه ویروس‌ها با این نام شناخته می‌شوند این است که همانند ویروس‌های دنیای جانداران عمل می‌کنند. بیشتر کسانی‌که با اینترنت سر و کار دارند با نام‌هایی چون ویروس، اسب‌های‌تروا (تروجان)، کرم‌ها و غیره آشنا هستند. تقریبا نیمی از صاحبان مشاغل در سراسر جهان به‌دلیل بی‌توجهی به افزایش ضریب امنیت سیستم‌های خود، به انواع کرم‌ها و ویروس‌های اینترنتی آلوده می‌شوند. هکرها و ویروس‌نویسان نیز با آگاهی از

کم توجهی کاربران، بدافزارهای خود را به‌گونه‌ای طراحی می‌کنند که به‌راحتی قادر به بُروز آسیب‌های کاملاً غیرقابل پیش‌بینی در سیستم کامپیوتری اشخاص شوند. آشنایی با انواع بدافزارها و روش‌های تکثیرشان در مقابله با آنها حائز اهمیت است. در ادامه به بررسی مفاهیم پایه‌ای در مورد بدافزارها و انواع آنها می‌پردازیم.

۱-۱ مفهوم بدافزار

واژه بدافزار معادل Malware انگلیسی است که یک خلاصه برای واژگان Malicious Software یا نرم‌افزار بدخواه می‌باشد. واژه بدافزار به ویروس، کرم، تروجان و هر برنامه دیگری که با نیت اعمال خرابکارانه ایجاد شود، گفته می‌شود، اما تفاوت ویروس و کرم در چیست؟ این دو چه تفاوتی با تروجان دارند؟ آیا برنامه‌های‌کاربردی ضدویروس برعلیه کرم‌ها و تروجان‌ها نیز اقدام می‌کنند یا تنها به جنگ با ویروس‌ها می‌روند؟ تمامی این پرسش‌ها از یک منبع سرچشمه می‌گیرند و آن هم دنیای پیچیده و گیج‌کننده کدهای بدخواه است. تعداد بی‌شمار و تنوع زیاد در کدهای بدخواه موجود، طبقه‌بندی دقیق آنها را مشکل می‌سازد. در مورد تمامی این موارد در ادامه فصل توضیح کامل داده خواهد شد. این تعاریف برای طبقه‌بندی‌های مختلف بدافزار، ما را قادر می‌سازد تا تفاوت‌های بین آنها را در یک فلوچارت ساده نشان دهیم. نمودار شکل (۱-۱) آیتم‌هایی را نشان می‌دهد که به ما کمک می‌کنند تشخیص دهیم یک اسکریپت در کدام طبقه می‌گنجد.



شکل (۱-۱) تشخیص نوع بدافزار

شکل (۱-۱) به کاربر کمک می‌کند تا تفاوت بین هر کدام از کدهای خرابکار معمول را تشخیص داده و طبقه‌بندی آن‌را شناسایی کند. البته طبقه‌بندی‌های متفاوت دیگری در مورد بدافزارها وجود دارد که در ادامه فصل به تشریح آنها خواهیم پرداخت. به هر روی، باید در نظر داشته باشیم که ممکن است در یک حمله به کدی برخورد کنیم که در بیش از یکی از این طبقه‌بندی‌ها بگنجد. به این حملات در اصطلاح تهدید ترکیبی[1] گفته می‌شود که شامل بیش از یک نوع بدافزار شده و از بردارهای حمله چندگانه استفاده می‌کنند. حملاتی از این دست می‌توانند با سرعت بیشتری گسترش پیدا کنند. یک بردار حمله مسیری است که بدافزار می‌تواند از آن برای پیش بردن حمله استفاده کند. به‌همین دلیل مقابله با حملات ترکیبی کار مشکلی است.

[1] _Blended Threats

درحالت کلی می‌توان گفت، بدافزارها ابزارهای بد نیتی هستند که به‌صورت مخفیانه وارد سیستم کاربر می‌شوند و اعمال خاص خود را روی داده‌های قربانی انجام می‌دهند که ممکن است خساراتی به بار آورند و به علت آنکه معمولا کاربر را آزار می‌دهند یا خسارتی به‌وجود می‌آورند، به این نام مشهورند. در واقع Malware، واژه‌ای عمومی برای معرفی انواع ویروس‌ها، کرم‌ها، ابزارهای جاسوسی، اسب‌های‌تروا و غیره است که هر کدام به نوعی برای صدمه زدن به سیستم‌های کامپیوتری یا سرقت اطلاعات کاربران طراحی شده‌اند. یک برنامه بر اساس نیت خالق آن به‌عنوان یک بدافزار شناخته می‌شود. البته اشکالات برنامه‌نویسی نرم‌افزارها که ممکن است به کامپیوتر آسیب برسانند، جزو این دسته‌بندی قرار نمی‌گیرند. درحالت کلی بدافزارها را می‌توان به دو دسته عمده تقسیم کرد:

- بدافزارهای مستقل که بدون نیاز به برنامه دیگری توسط سیستم‌عامل اجرا می‌شوند، مانند اسب‌های‌تروا (تروجان‌ها)
- بدافزارهای نیازمند میزبان که به تنهایی نمی‌توانند فعال شوند همانند ویروس‌ها

با توجه به پیشرفت تکنولوژی، بدافزارها نیز شدیدا رو به رشد هستند. آشنایی با انواع بدافزارها و روش‌های تکثیر و نوع کارکرد آنها حائز اهمیت است که در این فصل به انواع آن اشاره می‌گردد.

۲-۱ چرخه حیات بدافزار

ویروس‌ها و بدافزارهای کامپیوتری نیز مانند ویروس‌های بیولوژیکی دارای یک ظهور و یک افول هستند. منظور از چرخه حیات بدافزار حد فاصل بین ظهور و افول آن است. یک بدافزار زمانی متولد می‌شود که یک نویسنده بدافزار آن را ایجاد می‌کند و زمانی می‌میرد که کاملا از روی کامپیوترهای قربانی و شبکه‌های آلوده، پاک و ریشه کن شود. مراحل حیات یک بدافزار درحالت کلی شامل موارد زیر می‌باشند:

۱. ایده بدافزار جدید: خلق بدافزارها معمولا زمانی روی می‌دهد که یک روش و ایده جدید حمله یا سوءاستفاده، کشف و پیشنهاد شده و سپس در جوامع هکرها انتشار پیدا کند. این روش‌ها غالبا به بحث گذاشته شده و توسعه پیدا می‌کنند تا جایی‌که بتوانند تبدیل به حملاتی فعال و واقعی شوند.
۲. پیاده‌سازی: زمانی ایجاد یک ویروس یا بدافزار نیازمند داشتن دانش حرفه‌ای در زمینه برنامه‌نویسی کامپیوتر، به‌ویژه زبان ماشین و همچنین دانش دقیق در زمینه نحوه عملکرد سیستم مورد حمله بود؛ اما امروزه با پیشرفت‌هایی که در ابزارهای ایجاد بدافزار انجام شده و همچنین به مدد اتاق‌های گفتگو، هر کسی با استفاده از ابزارهای موجود و داشتن دانش برنامه‌نویسی اولیه می‌تواند یک بدافزار ایجاد کند.
۳. تکرار: پس از اینکه بدافزار جدید پیاده‌سازی شده و منتشر می‌شود، پیش از انجام عملیات اصلی و خرابکارنه، نیازمند تکرار برای پیدا کردن میزبان‌های جدید و بالقوه است.
۴. عملیات خرابکارانه: پس از اینکه بدافزار توانست به‌صورت موفقیت‌آمیز یک میزبان را آلوده سازد، به احتمال زیاد دست به عملیات خرابکارانه می‌زند. گاهی کد خرابکار دارای یک شرط برای تحریک شدن است و زمانی‌که این شرط روی دهد عملیات خرابکارانه آغاز خواهد شد. برای نمونه، برخی از بدافزارها زمانی

عملیات خرابکارانه را اجرا می‌کنند که کاربر کار خاصی را بر روی سیستم انجام دهد و یا تاریخ کامپیوتر میزبان به تاریخ یا ساعت خاصی برسد. گاهی نیز به محض آلودگی، عملیات خرابکارانه آغاز می‌شود مانند مواردی که بدافزار برای ثبت تبادل داده طراحی شده است. در این مورد بدافزار به سادگی به جمع‌آوری و ثبت داده‌های لازم می‌پردازد.

۵. شناسایی: در این مرحله بدافزار توسط جوامع ضدویروس شناسایی می‌شود. در بیشتر موارد، این مرحله پیش از مرحله چهار و حتی گاهی پیش از مرحله سه اتفاق می‌افتد.

۶. روش تشخیص: پس از شناسایی تهدید، لازم است توسعه‌دهندگان نرم‌افزارهای ضدویروس، کد بدافزار را تحلیل کنند تا یک روش تشخیص قابل اعتماد را نهایی سازند. پس از تعیین روش مورد نظر، فایل‌های حاوی امضای ویروس‌ها به‌روز رسانی می‌شود تا ضدویروس‌های موجود نیز قادر به تشخیص بدافزار جدید باشند. مدت زمانی‌که برای این مرحله صرف می‌شود، در مهار حمله بسیار مؤثر و حیاتی است.

۷. پاکسازی: زمانی‌که به‌روز رسانی ضدویروس‌ها در اختیار عموم قرار می‌گیرد، به‌کارگیری این به‌روز رسانی در کمترین زمان برای محافظت از سیستم در برابر حمله و یا پاکسازی سیستم در صورت آلوده شدن، بر عهده کاربران ضدویروس‌ها می‌باشد. انجام ندادن به موقع به‌روز رسانی توسط کاربران بسیار خطرناک است، زیرا در حقیقت با کاربرانی روبرو هستیم که فرض می‌شود محافظت شده و در امان هستند، در حالی که در واقع در معرض تمام حملات جدید قرار دارند. با افزایش تعداد کاربرانی که ضدویروس‌هایشان را به‌روز رسانی می‌کنند، خطر بدافزار کم و کمتر می‌شود. بعید است که این فرایند منجر به پاکسازی کامل بدافزار از دنیای کامپیوترها شود، زیرا همواره تعدادی کامپیوتر با محافظت ضعیف یا حتی بدون هیچ‌گونه محافظت ضدویروس به اینترنت متصل می‌شوند و طبیعتا مورد هجوم بدافزارها قرار می‌گیرند، اما با این وجود در این مرحله، خطر کلی بدافزار کاهش پیدا کرده است.

با وجودی‌که این چرخه حیات برای هر حمله بدافزاری جدید تکرار می‌شود، اما برای تمامی بدافزارها و حملات یکسان نیست. بسیاری از حملات به سادگی نسخه تغییر یافته قسمتی از کد یک بدافزار اصلی هستند، بنابراین زیربنای کد و شیوه حمله جدید، با بدافزار پیشین یکسان است، اما تغییرات کوچکی برای جلوگیری از شناسایی و حذف بدافزار توسط ضدویروس‌ها، ایجاد می‌شود. معمولا در حملات بدافزاری موفق، نسخه‌های جدیدی از بدافزار در هفته‌ها و ماه‌های اولیه انتشار پیدا می‌کنند. این وضعیت به نوعی "مسابقه تسلیحاتی" تبدیل می‌شود که از طرفی ویروس‌نویسان تلاش می‌کنند تا برای رسیدن به اهدافشان که می‌تواند اهداف مالی، شهرت یا کنجکاوی باشد، از خطر تشخیص توسط ضدویروس‌ها در امان بمانند. از سوی دیگر شیوه‌های دفاعی ضدویروس‌ها نیز به‌روز رسانی و اصلاح می‌شود و یا به شیوه‌ای تغییر می‌یابد تا خطرات تهدیدهای جدید را کاهش دهد.

اکنون در ادامه فصل به بررسی و تشریح هریک از بدافزارها در شاخه‌های گوناگون می‌پردازیم تا درک کاملی در مورد هر یک از آنها و تفاوت‌های موجود در این نوع نرم‌افزارها ایجاد شود.

۳-۱ ویروس چیست؟

ویروس‌های کامپیوتری برنامه‌هایی هستند که مشابه ویروس‌های بیولوژیک گسترش یافته و پس از وارد شدن به کامپیوتر اقدامات غیرمنتظره‌ای را انجام می‌دهند. ویروس‌های کامپیوتری بدین دلیل ویروس نامیده شده‌اند، زیرا دارای برخی وجوه مشترک با ویروس‌های زیست‌شناسی می‌باشند. ویروس‌ها دسته‌ای از کدهای مُخرب هستند که مشخصه اصلی آنها خود همتاسازی هنگام اجرا به همراه برنامه میزبان می‌باشند. با این تعریف می‌توان نتیجه گرفت برنامه ویروس دارای خاصیت انگلی است و همواره افزون بر آسیب به سیستم، نسخه یا نسخه‌هایی از خود را تولید می‌کند. یک ویروس کامپیوتری، از کامپیوتری به کامپیوتر دیگر منتقل می‌شود، دقیقا همانند ویروس‌های زیست‌شناسی که از شخصی به شخص دیگر منتقل می‌گردند. ویروس زیست‌شناسی یک موجود زنده نیست. ویروس بخشی از DNA می‌باشد و داخل یک روکش حفاظتی قرار می‌گیرد. ویروس برخلاف سلول، قادر به انجام عملیات و یا تکثیر مجدد خود نمی‌باشد (ویروس زنده و در قید حیات نمی‌باشد). یک ویروس زیست‌شناسی باید DNA خود را به یک سلول تزریق نماید. DNA ویروسی در ادامه با استفاده از دستگاه موجود سلول، قادر به تکثیر خود می‌گردد. در برخی حالات، سلول با ذرات ویروسی جدید آلوده می‌شود و تا زمانی‌که سلول مذکور فعال و باعث رهاسازی ویروس نشود، آلوده می‌ماند. در حالات دیگر، ذرات ویروس جدید باعث عدم رشد سلول در هر لحظه شده و سلول همچنان زنده باقی خواهد ماند.

ویروس‌های کامپیوتری دارای همین وجوه مشترک می‌باشند. یک ویروس کامپیوتری باید بر دوش دیگر برنامه‌ها یا مستندات قرار گرفته تا در زمان لازم شرایط اجرای آن فراهم گردد. پس از اجرای یک ویروس، زمینه آلوده کردن دیگر برنامه‌ها یا مستندات نیز فراهم می‌گردد.

به برنامه‌ای که کد ویروس به آن افزوده شده باشد برنامه آلوده می‌گویند. ویروس‌ها عمل انتشار خود را بر روی یک کامپیوتر و یا از طریق Floppy Disk، USB(Flash Memory)، CD-ROM و DVD-ROM بر روی سیستم‌های دیگر انجام می‌دهند. باید توجه داشت که ویروس‌ها قابلیت انتشار از طریق شبکه را ندارند. این قابلیت در دسته‌ای دیگر از کدهای مُخرب به‌نام کرم وجود دارد. به نخستین نسل از ویروس‌ها جرم گفته می‌شود. درحقیقت جرم، نخستین نسخه برنامه ویروس است که توسط برنامه‌نویس نوشته شده و پس از نخستین اجرا و قرار گرفتن در نخستین برنامه میزبان، ویروس شروع به تولید کدهای همانند خود خواهد کرد. می‌توان گفت نخستین نسل ویروس با نسل‌های دیگر متفاوت خواهد بود، ویروسی که قادر به ایجاد نسخه‌های همانند خود نباشد، بالقوه گفته می‌شود. این امر می‌تواند به دلایلی مانند بُروز خطا در کد ویروس و یا رویارویی با نسخه‌هایی از سیستم‌عامل که توسط نویسنده در نظر گرفته نشده‌اند، صورت گیرد.

پس درحقیقت ویروس، بدافزاری است که هیچ فعالیتی ندارد و هنگامی‌که در یک سیستم نرم‌افزاری دیگر قرار می‌گیرد با استفاده از اجزای آن خود را تکثیر می‌کند و به تخریب می‌پردازد که این‌کار معمولا بدون آگاهی کاربر صورت می‌گیرد. با وجودی‌که تمامی ویروس‌ها خطرناک نیستند، اما بسیاری از آنها با هدف تخریب انواع مشخصی از فایل‌ها، برنامه‌های‌کاربردی و یا سیستم‌های‌عامل نوشته شده‌اند. ویروس‌ها هم همانند تمامی

برنامه‌های دیگر از منابع سیستم مانند حافظه و فضای دیسک‌سخت، توان پردازنده مرکزی و دیگر منابع بهره می‌گیرند و می‌توانند اعمال خطرناکی را انجام دهند. برای نمونه، فایل‌های روی دیسک را پاک کرده یا کل دیسک‌سخت را فرمت می‌کنند. همچنین یک ویروس می‌تواند مجوز دسترسی به دستگاه را از طریق شبکه و بدون احرازهویت فراهم آورد.

تولد ویروس‌ها به روزهایی مربوط می‌شود که کامپیوتر شخصی وجود نداشت و کامپیوترها سیستم‌هایی حجیم و پر هزینه بودند و تنها در اختیار نهادهایی قرار داشتند که به استفاده از آنها نیاز داشتند. در واقع نخستین نویسندگان ویروس‌ها متخصصان علوم کامپیوتر در زمان خود بودند و انگیزه‌های متفاوتی برای این‌کار داشتند. در کل به غیر از ویروس‌هایی که تنها با انگیزه مردم آزاری نوشته می‌شوند، ویروس‌های فراوانی هم هستند که با انگیزه‌های سیاسی یا مالی به وجود می‌آیند. برای نمونه، ویروس‌هایی هستند که در روز خاصی از هر سال حملات خود را به یک نهاد دولتی یا نظامی معطوف می‌کنند و یا ویروس‌هایی که با نمایش دادن پیام‌هایی به انتقاد از وضعیت سیاسی یا اقتصادی کشور خاصی می‌پردازند.

معمولا ویروس‌ها به‌منظور آلوده کردن شمار زیادی کامپیوتر طراحی می‌شوند و هدف منفردی ندارند. اگرچه هدف نهایی آنها می‌تواند یک شبکه یا ارگان خاص باشد. به این ترتیب که یک ویروس خاص ممکن است با هدف نهایی از کار انداختن یک شبکه طراحی شود، اما به این طریق عمل می‌نماید که در ابتدا خود را تکثیر می‌کند و پس از آلوده کردن هزاران کامپیوتر، در تاریخ معینی از طریق تمامی آن کامپیوترها به حمله می‌پردازد. تاریخ کامپیوتر مواردی این چنینی را بسیار به خاطر دارد. ویروس‌هایی بوده‌اند که شبکه‌های دولتی را از کار انداخته‌اند و یا فعالیتشان را دچار اِشکال کرده‌اند.

در سال‌های گذشته موردی از حمله به مایکروسافت نیز وجود داشت که مسئولان مایکروسافت ناچار شدند چند ساعت پیش از شروع حمله ویروس، آدرس IP سایت وب خود را تغییر دهند تا در اثر حمله از کار نیفتد. برخی از ویروس‌ها هم اطلاعات موجود روی دیسک‌سخت را کد و هم غیرقابل خواندن می‌کنند. همچنین شایعاتی نیز وجود داشت که برخی از شرکت‌های ضدویروس برای داشتن درآمد بیشتر، ویروس‌هایی را طراحی و منتشر می‌کردند و پس از اینکه فعالیت ویروس‌ها به مرحله خطرناکی می‌رسید، خودشان ضدویروس آن‌را روانه بازار می‌ساختند. تعجب می‌کنید اگر بدانید که تمامی ویروس‌ها، مُخرب نبوده‌اند. ویروس‌های خوبی نیز ساخته شده‌اند که با تکثیر روی سیستم‌ها، برای نمونه، نقطه ضعف سیستم‌های‌عامل را در رویارویی با یک ویروس دیگر برطرف کرده‌اند و یا ویروس مُخربی را از روی آنها حذف نموده‌اند.

البته موردی که نمی‌توان نادیده گرفت این است که هر ویروسی به دلیل مصرف منابع سیستم و تلاش در تکثیر، حداقل اثری که دارد این است که سرعت سیستم را کاهش می‌دهد و اجرای وظایف عادی آن‌را با خطا مواجه می‌سازد.

نرم‌افزارهای ضدویروس توانایی شناسایی و از بین بردن ویروس‌ها را دارند، اما برای مقابله با ویروس‌هایی که هر روز وارد دنیای کامپیوتر می‌شوند همواره باید این نرم‌افزارها را از طریق ارتقاء، به‌روز نگاه داشت. بیشتر ویروس‌ها تنها تکثیر می‌شوند و همان‌طور که گفته شد برخلاف تصور بیشتر مردم تنها پنج درصد آنها اثرات تخریبی دارند. برنامه‌ای که تنها خاصیت تخریبی داشته باشد و نتواند تکثیر شود ویروس نامیده نمی‌شود. ویروس‌ها پس از تکثیر در یک کامپیوتر می‌توانند در مدت زمان نه‌چندان طولانی یک منطقه ویا حتی جهان را آلوده کنند.

از آنجاکه ویروس‌ها به‌طور مخفیانه عمل می‌کنند، تا زمانی‌که کشف نشده و امکان پاکسازی آنها فراهم نگردیده باشد، برنامه‌های بسیاری را آلوده می‌کنند و از این‌رو یافتن سازنده ویا منشاء اصلی ویروس مشکل است. ویروس‌ها نیاز به مکانی برای ذخیره خود دارند و محلی که ویروس‌ها را به اهدافشان نزدیک‌تر می‌کند، فایل‌های اجرایی هستند و کمتر ویروسی یافت می‌شود که در یک فایل غیراجرایی قرار بگیرد. در ادامه، فهرست پسوندهای رایج فایل‌هایی که به نوعی هر کدام در نقش فایل‌های اجرایی ارائه می‌شوند، آورده شده است و بیشتر نرم‌افزارهای ضدویروس در حالت عادی (بدون تنظیمات خاص) این فایل‌ها را ویروس‌یابی می‌کنند:

.com, .exe, .dll, .ovl, .bin, .sys, .dot, .doc, .vbe, .vbs, .hta, .htm, .scr, .ocx, .hlp, .eml

بنابراین یکی از اصلی‌ترین میزبان‌های ویروس، فایل‌های اجرایی هستند. از سویی دیگر، برخی ویروس‌ها نیز از سکتور راه‌انداز[1] و جدول بخش‌بندی دیسک[2] یا MBR[3] به‌عنوان میزبان استفاده می‌کنند. این نوع از ویروس‌ها را در ادامه فصل بررسی خواهیم کرد. همان‌طور که می‌دانید سکتور راه‌انداز، واحد راه‌اندازی سیستم‌عامل است که در سکتور شماره صفر دیسکت فلاپی ویا درایوهای منطقی یک دیسک‌سخت قرار دارد و جدول بخش‌بندی شامل اطلاعات تقسیم‌بندی دیسک‌سخت می‌باشد که آن نیز در سکتور شماره صفر دیسک‌سخت قرار دارد. این‌گونه ویروس‌ها با قرارگرفتن در یکی از این دو محل، هنگام راه‌اندازی کامپیوتر، اجرا شده و در حافظه سیستم مقیم می‌شوند و تا زمان خاموش کردن کامپیوتر ویا راه‌اندازی دوباره، همان‌جا مانده و فلاپی‌ها ویا دیسک‌های‌سخت دیگر را آلوده می‌کنند. اکنون این پرسش پیش می‌آید که اگر تنها پنج درصد از ویروس‌ها خاصیت تخریبی دارند و مابقی تنها تکثیر می‌شوند، چرا ویروس‌ها به‌عنوان یک معضل شناخته می‌شوند و ضرورت مبارزه با آنها چیست؟ پاسخ این پرسش در موارد زیر خلاصه گردیده است:

- بسیاری از ویروس‌ها کار تخریبی انجام نمی‌دهند، اما با نمایش پیغام ویا ایجاد مشکلاتی همانند ریزش حروف صفحه نمایش یا راه‌اندازی مجدد خودکار سیستم در هنگام کار با سیستم برای کاربر ایجاد مزاحمت می‌کنند.

---

[1] _Boot Sector
[2] _Partition Table
[3] _Master Boot Record

- برخی از ویروس‌ها با تکثیر خود به مرور زمان حافظه سیستم را پُر می‌کنند و باعث بُروز اختلال در روند کار سیستم می‌شوند.
- وجود ویروس در سیستم شما و انتقال آن از طریق شما به دوستانتان باعث سلب اعتماد آنها نسبت به شما می‌شود.
- برخی از ویروس‌ها می‌توانند از واژه‌های تایپ شده بر روی سیستم شما گزارش‌گیری به عمل آورند و پس از اتصال به اینترنت، آنها را برای مقصد مورد نظر ارسال کنند. تمامی این ویروس‌ها به‌صورت مخفیانه کار خود را انجام می‌دهند.

این نکته را نیز لازم است بدانید که ویروس‌ها ممکن است بی‌درنگ پس از منتقل شدن به سیستم شروع به کار کنند یا در تاریخ مشخصی ویا در اثر اجرای برنامه خاصی فعالیت خود را آغاز نمایند. ویروس‌ها هیچ‌گاه بی‌ضرر نیستند و در خوشبینانه‌ترین حالت، زمان شما و وقت پردازنده و فضای حافظه سیستم را از بین می‌برند. اثرات تخریبی ویروس‌ها می‌تواند شامل موارد زیر باشد:

- فرمت‌کردن دیسک
- کدکردن اطلاعات و برنامه‌ها
- تخریب اطلاعات حافظه فلش

ویروس‌ها را می‌توان به روش‌های گوناگون دسته‌بندی کرد که در اینجا به برخی از این روش‌ها اشاره می‌کنیم. ویروس‌ها ممکن است در یک یا چند دسته از دسته‌های زیر قرار گیرند. حالت‌های کامل‌تری از این دسته‌ها در ادامه فصل ارائه می‌گردد:

- ویروس‌های مستقر در حافظه[1]: این نوع ویروس‌ها با مقیم شدن در حافظه فایل‌های دیگر را آلوده می‌کنند.
- ویروس‌های پنهان‌کار[2]: این‌گونه ویروس‌ها با استفاده از روش‌های متفاوت، اثرات بجامانده از خود را پاک می‌کنند، به‌گونه‌ای که کاربر متوجه آلوده بودن آن فایل نخواهد شد. ویروس‌های دیگر برای مثال تغییراتی بر روی حجم ویا تاریخ ایجاد فایل به‌وجود می‌آورند.
- ویروس‌های کدشده[3]: این دسته از ویروس‌ها پس از هربار آلوده‌سازی به شیوه خودرمزی، شکل ظاهری خود را تغییر می‌دهند و با شکلی متفاوت آشکار می‌شوند.
- ویروس‌های چندشکلی[4]: این ویروس‌ها به‌وسیله الگوریتم‌های خاص، ساختار و شکل ظاهری خود را تغییر می‌دهند.

---

[1]_Memory Resident Viruses
[2]_Stealth Viruses
[3]_Encrypting Viruses
[4]_Polymorphic Viruses

- ویروس‌های فعال‌شونده بر اساس رویداد خاص[1]: این ویروس‌ها بخشی از فعالیت خود را در تاریخ و زمان مشخصی انجام می‌دهند. البته تکثیر و آلوده‌سازی فایل‌ها در تمام اوقات فعال‌بودن ویروس انجام می‌شود.

۱-۴ انواع گوناگون ویروس‌ها

انواع ویروس‌های رایج را می‌توان به دسته‌های زیر تقسیم‌بندی نمود:

- **سِکتور بوت (Boot Sector)**

سِکتور بوت نخستین سِکتور روی فلاپی و یا دیسک‌سخت کامپیوتر است. در این قطاع کدهای اجرایی ذخیره شده‌اند که فعالیت کامپیوتر با استفاده از آنها انجام می‌شود. با توجه به اینکه در هر بار روشن شدن و بارگذاری، سِکتور بوت مورد ارجاع قرار می‌گیرد و با هر بار تغییر پیکربندی کامپیوتر محتوای سِکتور بوت هم دوباره نوشته می‌شود، لذا این قطاع مکانی بسیار آسیب‌پذیر در برابر حملات ویروس‌ها می‌باشد. ویروس‌های سکتور بوت، نخستین نوع ویروس‌هایی بودند که مشاهده شدند. این نوع ویروس‌ها از طریق فلاپی‌هایی که قطاع بوت آلوده دارند، انتشار می‌یابند. درصورت آلوده شدن سِکتور بوت دیسک‌سخت کامپیوتر توسط ویروس، هر بار که کامپیوتر روشن می‌شود، ویروس خود را در حافظه بار کرده و منتظر فرصتی برای آلوده کردن فلاپی‌ها می‌ماند تا بتواند خود را منتشر کرده و دستگاه‌های دیگری را نیز آلوده نماید. این‌گونه ویروس‌ها می‌توانند به‌گونه‌ای عمل کنند که تا زمانی‌که دستگاه آلوده است امکان بوت کردن کامپیوتر از روی دیسک‌سخت وجود نداشته باشد. این ویروس‌ها پس از نوشتن روی متن اصلی بوت تلاش می‌کنند کد اصلی را به قطاعی دیگر روی دیسک منتقل کرده و آن قطاع را به‌عنوان یک قطاع خراب[2] علامت‌گذاری کنند. هنگامی‌که کاربر در مرتبه بعدی دستگاه را روشن می‌کند، سکتور بوت آلوده شده، مورد استفاده سخت‌افزار قرار خواهد گرفت و بنابراین ویروس فعال خواهد شد. پس درصورتی‌که کاربر دستگاه را به‌وسیله یک دیسکت آلوده، (معمولا دیسک‌های نرمی که سِکتور بوت آلوده دارند) راه‌اندازی کند، درنهایت دستگاه آلوده به ویروس خواهد شد. بسیاری از ویروس‌های سِکتور بوت، هم‌اینک دیگر جزء ویروس‌های کهنه و قدیمی محسوب می‌شوند. آنهایی‌که برای دستگاه‌های تحت سیستم‌عامل DOS نوشته شده بودند، معمولا نمی‌توانند از طریق سیستم‌های‌عامل ویندوز گسترش یابند، گرچه ممکن است گاهی این سیستم‌های‌عامل را از راه‌اندازی صحیح متوقف کنند.

- **ویروس‌های ماکرو (کلان دستور)**

ویروس‌های ماکرو که از مزایای برنامه‌نویسی ماکرو سود می‌برند، کدهایی هستند که در دستورات داخل فایل‌ها ادغام شده و به‌صورت خودکار اجرا می‌شوند. این نوع ویروس‌ها مستقیما برنامه‌ها را آلوده نمی‌کنند. هدف این دسته از ویروس‌ها فایل‌های تولید شده توسط برنامه‌هایی است که از زبان‌های برنامه‌نویسی ماکرویی مانند مستندات Excel یا Word استفاده می‌کنند. درحقیقت ویروس‌های ماکرو، یک برنامه ماکرو است که می‌تواند از

---

[1] _Triggered Event Viruses
[2] _Bad Sector

خود کپی ساخته و از فایلی به فایل دیگر گسترش پیدا کند. این ویروس‌ها از راه دیسک‌ها، شبکه و یا فایل‌های پیوست شده با نامه‌های‌الکترونیکی قابل گسترش می‌باشند. چنانچه شما فایلی را باز کنید که حامل ویروسی از نوع ماکرو است، ویروس خود را در فایل‌های آغازین اجرای آن برنامه کپی کرده و این زمان آغاز آلوده شدن آن کامپیوتر می‌باشد. زمانی‌که کاربر در مرحله بعد، فایلی را باز می‌کند که از همان برنامه استفاده می‌نماید، ویروس، آن فایل را نیز آلوده خواهد کرد. چنانچه کامپیوتر وی در یک شبکه باشد، این آلودگی به سرعت گسترش پیدا خواهد کرد و دلیل آن نیز این است که، هنگامی‌که کاربر فایلی آلوده را برای فرد دیگری می‌فرستد، او هم با باز کردن فایل، آلوده خواهد شد. یک ماکروی مُخرب همچنین می‌تواند باعث به وجود آمدن تغییرات در اسناد و تنظیمات شما شود.

ویروس‌های ماکرو می‌توانند فایل‌هایی که در بیشتر ادارات مورد استفاده قرار می‌گیرند را آلوده کنند و همچنین برخی از آنها می‌توانند چندین نوع متفاوت از فایل‌ها مانند فایل‌های برنامه‌های بسته نرم‌افزاری Office را تحت تأثیر قرار دهند. همچنین آنها می‌توانند به تمام فایل‌هایی که توسط برنامه میزبان آنها اجرا می‌شود، گسترش پیدا کنند. درنتیجه یکی از پُر انتشارترین ویروس‌ها نیز به‌شمار می‌روند؛ چراکه اسناد به‌طور پی‌درپی در نامه‌های الکترونیکی و سایت‌های وب در حال تبادل هستند. انتقال این فایل‌ها به کامپیوترهای دیگر یا اشتراک فایل بین دستگاه‌های گوناگون باعث گسترش آلودگی به این ویروس‌ها می‌شود.

برنامه‌های‌کاربردی شرکت مایکروسافت دارای یک ویژگی خاص با نام "حفاظت ماکروها در مقابل ویروس" بوده که از فایل‌ها و مستندات مربوطه، در مقابل ویروس حفاظت می‌نماید. زمانی‌که این ویژگی فعال شود، امکان "اجرای خودکار"، غیرفعال می‌گردد. در چنین حالتی اگر یک سند تلاش در اجرای خودکار کدهای ویروسی نماید، یک پیام هشدار دهنده روی نمایشگر آشکار می‌گردد.

متأسفانه، بیشتر کاربران دارای شناخت لازم و مناسب از ماکروها و ماکروهای ویروسی نبوده و به‌محض مشاهده پیام هشدار دهنده، از آن چشم‌پوشی می‌کنند. درچنین مواردی، ویروس با خیالی آسوده اجرا خواهد شد. برخی دیگر از کاربران، این امکان حفاظتی را غیرفعال می‌کنند و ناآگاهانه در توزیع و گسترش ویروس‌های کامپیوتری نظیر مِلیزا، سهیم می‌گردند.

▪ ویروس‌های انگلی[1]

ویروس‌های انگلی که با نام ویروس‌های فایل هم شناخته می‌شوند، خود را به برنامه‌ها یا همان فایل‌های قابل اجرا (فایل‌های با پسوند exe. و com.) پیوند می‌زنند و آنها را آلوده نموده و هم‌زمان با اجرای این برنامه‌ها خود را در حافظه دستگاه بار کرده و شروع به گسترش خود و آلوده کردن دیگر فایل‌های اجرایی سیستم می‌نمایند. در واقع این نوع ویروس‌ها، تکه کدهایی هستند که خود را به فایل‌های اجرایی، فایل‌های درایور یا فایل‌های فشرده متصل می‌کنند و زمانی‌که برنامه میزبان اجرا می‌گردد، فعال می‌شوند. پس از فعال شدن، ویروس با چسباندن خود

[1] _File infecting viruses

به برنامه‌های موجود دیگر در سیستم گسترش می‌یابد و پخش می‌شود و همچنین کارهای بدخواهانه‌ای را انجام می‌دهد که برای آن برنامه‌ریزی شده است. هنگامی‌که کاربر اجرای برنامه آلوده شده توسط ویروسی را آغاز می‌کند، در ابتدا ویروس اجرا خواهد شد. ویروس برای مخفی نگاه داشتن حضور خود، برنامه اصلی را اجرا می‌کند. سیستم‌عامل دستگاه که ویروس را بخشی از برنامه اجرا شده توسط کاربر می‌داند، به آن مجوزهای اجرا را می‌دهد. این مجوزها به ویروس اجازه می‌دهند تا از خود کپی بسازد، خود را در حافظه کامپیوتر قرار داده و بدنه خود را آزاد کنند. برخی از نمونه‌های این ویروس‌ها متن مورد نظر خود را به‌جای متن فایل اجرایی قرار می‌دهند.

ویروس‌های انگلی در تاریخچه ویروس‌ها از نخستین انواع آنها می‌باشند، اما هم‌اینک نیز از تهدیدهای واقعی به‌شمار می‌روند. شبکه اینترنت که گسترش برنامه‌ها را ساده‌تر کرده، به ویروس‌ها نیز فرصتی جدید برای گسترش داده است. بیشتر ویروس‌های فایل با بارگذاری خود در حافظه سیستم و جست‌وجوی برنامه‌های دیگر موجود در دیسک‌سخت، گسترش می‌یابند. اگر برنامه‌ای را بیابند، کد برنامه را به‌گونه‌ای تغییر می‌دهند که در صورت اجرای دوباره‌ی آن برنامه، ویروس فعال شود. این‌کار بارها و بارها تکرار می‌شود تا جایی‌که ویروس‌ها در سراسر سیستم و احتمالا در سیستم‌های دیگری که در ارتباط با این برنامه آلوده هستند، منتشر شوند.

- **ویروس‌های چندریخت**[1]

این ویروس‌ها در هر فایل آلوده به شکلی متفاوت آشکار می‌شوند. با توجه به اینکه از الگوریتم‌های کدگذاری استفاده کرده و ردپای خود را پاک می‌کنند، آشکارسازی و تشخیص این‌گونه ویروس‌ها دشوار است.

- **ویروس‌های مخفی**

این ویروس‌ها تلاش می‌کنند خود را از سیستم‌عامل و نرم‌افزارهای ضدویروس مخفی نگه دارند. برای این‌کار ویروس در حافظه مقیم شده و حائل دسترسی به سیستم‌عامل می‌شود. در این‌صورت ویروس همه‌ی درخواست‌هایی که نرم‌افزار ضدویروس به سیستم‌عامل می‌دهد، را دریافت می‌کند. به این ترتیب نرم‌افزارهای ضدویروس هم فریب خورده و این تصور به‌وجود می‌آید که هیچ ویروسی در کامپیوتر وجود ندارد. این ویروس‌ها کاربر را هم فریب داده و استفاده از حافظه را به‌صورت مخفیانه انجام می‌دهند.

- **ویروس‌های چندبخشی یا چندوجهی**

رایج‌ترین انواع این ویروس‌ها ترکیبی از ویروس‌های سِکتور بوت و ویروس‌های انگلی می‌باشند. ترکیب انواع دیگر ویروس‌ها نیز امکان‌پذیر است. این‌گونه ویروس‌ها به‌صورت هم‌زمان سکتور بوت و فایل‌های اجرایی را مورد حمله و آلودگی قرار می‌دهند. ترکیب انواع دیگر ویروس‌ها نیز امکان‌پذیر است.

---

[1] _Polymorphic

▪ ویروس‌های مبتنی بر پست‌الکترونیکی

ویروس‌هایی از این نوع از طریق پیام‌های پست‌الکترونیکی منتقل می‌شوند. این نوع ویروس‌ها به‌صورت خودکار برای افراد فراوانی پست می‌شود. گزینش افراد برای ارسال نامه‌الکترونیکی براساس دفترچه آدرس پست‌الکترونیکی انجام می‌گیرد. درحقیقت آخرین اطلاعات موجود در رابطه با ویروس‌های کامپیوتری به "ویروس‌های پست‌الکترونیکی" اشاره دارد و هم‌اینک پست‌الکترونیک بزرگترین منشأ ویروس‌ها است. علت آنکه این ویروس‌ها به چنین عمومیتی دست یافته و در تیترهای خبری جای گرفته‌اند، آن است که آنها توانسته‌اند از طریق پست‌الکترونیک در سرتاسر جهان انتشار پیدا کنند. تا زمانی‌که ویروس‌ها به‌وسیله دیسکت انتقال پیدا می‌کردند، انتشارشان بسیار کُند بود. شرکت‌ها می‌توانستند استفاده از دیسکت‌ها را ممنوع کرده یا کاربران را مجبور به بررسی دیسکت‌ها برای اطمینان از عدم وجود ویروس نمایند، اما پست‌الکترونیک همه چیز را تغییر داده است. اکنون می‌توانید فایل‌هایتان را با سرعت بسیار بیشتری مبادله کنید و در عوض، دستگاه شما نیز به راحتی یک کلیک روی یک آیکن و شاید هم ساده‌تر از آن آلوده می‌شود. ویروس‌های معمولی این امکان را دارند که بسیار سریع‌تر از گذشته منتشر شده و انواع جدیدتر ویروس هم می‌توانند کارکرد برنامه‌های پست‌الکترونیک را مورد سوء استفاده خود قرار دهند.

برخی از کاربران فکر می‌کنند تا زمانی‌که به فایل پیوندی نامه‌ها کاری نداشته باشند، بازکردن و خواندن نامه‌ها اشکالی ندارد و آنها از امنیت کافی برخوردار خواهند بود. هم‌اینک چنین تفکری دیگر ارزشی ندارد. نرم‌افزارهای مُخربی مانند Kakworm و Bubbleboy می‌توانند کاربران را در هنگامی‌که تنها نامه‌هایشان را می‌خوانند، آلوده کنند. آنها شبیه دیگر نامه‌ها هستند با این تفاوت که شامل یک کد اسکریپت مخفی نیز می‌باشند. این کد اسکریپت مخفی به محض باز کردن نامه یا مشاهده آن در صفحه پیش‌نمایش[1] اجرا خواهد شد. کد اسکریپت مورد نظر می‌تواند تنظیمات سیستم را تغییر داده و ویروس را از راه پست‌الکترونیک برای دیگر کاربران ارسال نماید.

▪ ویروس‌های کُند (Slow Virus)

از آنجایی‌که این‌گونه ویروس‌ها صرفا هنگامی فایل‌ها را آلوده می‌کنند که در حال کپی شدن یا انتقال آن ویا در حال اِعمال تغییرات بر روی آنها هستند، شناسایی آنها برای ضدویروس دشوار است، بنابراین فایل اصلی آلوده نخواهد شد. بهترین روش برای شناسایی و عدم آلودگی توسط این‌گونه ویروس‌ها، استفاده از نرم‌افزارهای بررسی صحت فایل می‌باشد.

---

[1] _ درصورتی‌که شما از برنامه Outlook به‌همراه نسخه منطبقی از Internet Explorer استفاده می‌کنید، این صفحه مورد استفاده قرار می‌گیرد.

- **ویروس‌های پس‌رو (Retro Virus)**

این نوع از ویروس‌ها به ضدویروسی که قرار است آنها را حذف کند، حمله می‌کنند. این‌گونه ویروس‌ها با حمله به پایگاه‌داده ضدویروس که شامل اطلاعات شناسایی ویروس‌ها است و با از بین بردن یا دستکاری آنها باعث از بین رفتن قابلیت شناسایی ویروس‌ها توسط ضدویروس می‌شوند و عملا کار ضدویروس را مختل می‌کنند. در دیگر موارد نیز سعی بر دستکاری ضدویروس و ایجاد مزاحمت برای شناسایی ویروس‌ها می‌کند.

- **ویروس های مسلح (Armored Virus)**

این‌گونه ویروس‌ها برای اینکه خود را از دید ضدویروس پنهان نگه دارند به ضدویروس این‌طور القا می‌کنند که در جایی دیگر از حافظه قرار دارند، بنابراین شناسایی و تجزیه این‌گونه ویروس‌ها بسیار دشوار می‌باشد.

- **ویروس‌های همنشین (Companion Virus)**

این‌گونه ویروس‌ها فایلی هم‌نام یا نزدیک به نام فایل اصلی تولید کرده و به هنگام فراخوانی فایل اصلی، ویروس نیز فراخوانی می‌شود، برای نمونه، فایل Scandisk.exe در سیستم وجود دارد و توسط یکی از این نوع ویروس‌ها آلوده شده است و در کنار آن فایل Scandisk.com و Scandisk.bat ایجاد شده است که با فراخوانی Scandisk.exe هر دو فایل آلوده فراخوانی خواهند شد.

- **ویروس‌های خورنده (Phage Virus)**

این نوع ویروس‌ها، یکی از خطرناک‌ترین نوع ویروس می‌باشند. به این دلیل که افزون بر اینکه فایل را آلوده می‌کند و خود را به آن متصل می‌نماید، کدمُخرب خود را جایگزین کدهای موجود در روی فایل اجرایی سیستم می‌کند و بنابراین هرگاه این نوع ویروس، فایلی از یک برنامه را آلوده کند، به‌طور حتم قصد تخریب کامل آن نرم‌افزار را دارد.

- **ویروس‌های بازدیدکننده (Revisiting Virus)**

این نوع ویروس در حقیقت ماهیتی شبیه کرم[1] دارد و به‌وسیله استفاده از پروتکل TCP/IP و قراردادن خود در حافظه سیستم‌ها ترویج پیدا می‌کند.

- **ویروس‌های اسکریپتی (Script Viruses)**

این ویروس‌ها که اسکریپت‌های نوشته شده به زبان‌های ویژوال بیسیک یا جاوا می‌باشند، تنها در کامپیوترهایی اجرا می‌شوند که بر روی آنها مرورگر وب Internet Explorer یا هر مرورگر وب دیگری با توانایی اجرای اسکریپت‌ها، نصب شده باشد و فایل‌هایی با پسوند html.، htm.، vbs.، js.، htt. یا asp. را آلوده می‌کنند.

---

[1] _Worm

- **ویروس‌های دوزیست**

این‌گونه ویروس‌ها، ویروس‌هایی هستند که در دو محیط گوناگون از نظر نوع سیستم‌عامل قادر به زیست و آلوده‌سازی می‌باشند. این نوع از ویروس‌ها در سیستم‌های‌عامل معروفی چون ویندوز و خانواده لینوکس بیشتر دیده شده‌اند و به‌راحتی قادر به مهاجرت از سیستم‌عامل ویندوز به لینوکس و عکس آن می‌باشند. نگارندگان ویروس‌های کامپیوتری تاکنون نمونه‌های مختلفی از این کدهای مُخرب را که می‌تواند هر دو سیستم‌عامل "ویندوز" و "لینوکس" را مبتلا سازند، به‌صورت محدود و کنترل شده منتشر کرده‌اند. نمونه‌ای از این نوع ویروس‌ها VIRUS.LINUX.BIA.A و VIRUS.WIN32.BI.A نام دارند. ویروس‌های نام‌برده شده به زبان برنامه‌نویسی " اسمبلی" نوشته شده‌اند و قادرند فایل‌های دارای فرمت‌های مورد استفاده در هر دو سیستم‌عامل "ویندوز" و همچنین "لینوکس" را آلوده کند. کارشناسان عقیده دارند ویروس Bia.a اثبات این مدعا است که می‌توان کدهای مُخربی با قابلیت حمله به سیستم‌های‌عامل متفاوت ایجاد کرد و احتمالا در آینده شاهد انتشار ویروس‌های واقعی با قابلیت مبتلا کردن سیستم‌های‌عامل گوناگون خواهیم بود. احتمالا هم‌اکنون نفوذگران و نگارندگان ویروس‌های کامپیوتری در حال مطالعه روی ویروس‌هایی با قابلیت جهش از یک سیستم‌عامل به سیستم‌عامل دیگر هستند و در آینده ظهور این ویروس‌ها می‌تواند مشکلات امنیتی چشم‌گیری ایجاد کند. این دو ویروس تنها به پوشه‌های فعال سیستم صدمه وارد می‌کند، اما صدمات وارده زیاد جدی نیست و تکثیر نمی‌شوند. نحوه عمل ویروس‌های یاد شده برای لینوکس محدودتر است، چراکه باید توسط کاربران گشوده شود و نمی‌تواند خود به خود عمل کند. از آنجاکه بیشتر کاربران لینوکس از طریق سرور کار می‌کنند، کمتر به این ویروس‌ها آلوده می‌شوند.

- **ویروس‌های شبیه‌سازی خطا**

یک نوع دیگر از ویروس‌ها کاربر را به این سو هدایت می‌کنند که تصور کند سیستم و یا یک نرم‌افزار خاص، دارای خطا است. شرکت‌های نرم‌افزاری برای مدتی از این "خطاهای دروغین"، برای فاش شدن کپی‌های غیرمجاز نرم‌افزارهایشان استفاده کرده‌اند. مثالی از خطایی از این نوع به‌فرم زیر است:

International error number:084 876 at posititon PC 586 please notify the manufacturer

طبیعی است که چنین خطایی وجود ندارد. این پیغام خطا درصورت تلاش در شکستن حفاظت در برابر کپی ایجاد شده و حاوی هیچ‌چیز جز شماره سری برنامه نیست، که شرکت نرم‌افزاری با استفاده از آن می‌تواند دریابد که این نسخه از کجا آمده است. می‌توان انتظار داشت که برنامه‌نویسان ویروس‌ها نیز از چنین روش‌هایی استفاده کنند. مثالی بی‌ضرر از ویروس‌های شبیه‌سازی کننده‌ی خطا، برنامه‌ی ویروس Rush Hour نوشته شده توسط بی.فیکس است که خرابی صفحه‌کلید را شبیه‌سازی می‌کند و هر بار که کلیدی فشار داده می‌شود، صدایی را از بلندگوی سیستم تولید می‌کند. ویروس این‌کار را پس از مدت معینی انجام می‌دهد تا کاربر تصور کند که یک اِشکال حرارتی در مورد صفحه‌کلید وجود دارد.