روش های شناسایی ویروس های کامپیوتری

فاطمه سادات هل اتائی*[۱]، مرجان کرامتی[۲]

۱- هیات علمی دانشکده علوم ریاضی، آمار و کامپیوتر، دانشگاه سمنان **halataei@semnan.ac.ir**

۲- هیات علمی دانشکده علوم ریاضی، آمار و کامپیوتر، دانشگاه سمنان **keramati_marjan@semnan.ac.ir**

چکیده

امروزه ویروس های کامپیوتری تهدید بزرگی برای دنیای کامپیوتر هستند. محققانی که در این زمینه کار می کنند برای طبقه بندی ویروس‌ها و روش های شناسایی آنها کارها و تلاش های مختلفی انجام داده اند. ویروس های کامپیوتری مانند ویروس های پلی مورف و دگرگون شده از روش های پیچیده تری برای تکامل خود استفاده می کنند. بنابراین، لازم است از مدل های قوی تری برای درک تکامل و سپس تشخیص اعمال برای حذف آنها استفاده شود. در این مقاله برآنیم تا دیدگاهی کلی از ویروس ها و روش های شناسایی ویروس ها ارائه دهیم.

کلمات کلیدی: ویروس، بدافزار، آنتی ویروس، ویروس پلی مورف، شناسایی ویروس، ماشین بردار پشتیبان، منطق فازی

۱. مقدمه

در سال ۱۹۴۹ مقاله جان فون نیومن* با نام "تئوری اتوماتای خود تکثیر " منتشر شد ،که آغازی برای ساخت ویروس‌ها بود.

سال ۱۹۷۱ یک برنامه آزمایشی "The Creeper " که توسط باب توماس† در تکنولوژی BB، نوشته شده بود.

در سال ۱۹۷۴ ویروس "Wabbit " که چندین نسخه از خود را بر روی کامپیوتر می‌ساخت، نوشته شد. در سال ۱۹۷۵ ویروس "ANIMAL" توسط جان والکر‡ ساخته شده بود.

ویروس " Elk Cloner" نوشته شده توسط ریچ اسکرنتا§ در سال ۱۹۸۲ در گردش بود و ویروس‌های تولید شده توسط جو دلینگر

نیز بین سال‌های ۱۹۸۱ تا ۱۹۸۳ ساخته شده بودند؛ که همه‌ی آن‌ها برای پلتفرم‌های Apple II بودند.

در سال ۱۹۸۳ فردریک کوهن** دانشجوی دوره کارشناسی ارشد دانشگاه کالیفرنیای جنوبی در یک سمینار امنیت به نام "حفاظت دیسک"

در دانشگاه پنسیلوانیا یک کد مفهومی را به خط فرمان یونیکس بر روی سیستم رایانه تایپ کرد و بعد از۵ دقیقه کنترل تمامی رایانه‌های آن دانشگاه را دردست گرفت. افراد شرکت کننده درسمینار مدعی بودند که اطلاعات درون دیسک‌ها اگر بطور عادی حذف نشوند وآسیب فیزیکی نبینند، در دیسک دارای عمرطولا نی هستند. ولی فرد کوهن این را قبول نداشت.

* John Von Neuman
† Bob Thomas
‡ John Walker
§ Richard Skrenta
** Frederick Cohen

وقتی سمینار تمام شد کوهن نظر خود را با استادش "آدلمن" در میان گذاشت وآدلمن بلافاصله به شباهت نظر کوهن با ویروس‌های بیولوژیکی اشاره کرد. در آن زمان او موفق شد تمام سیستم‌های امنیتی رایانه‌ها را غیرفعال کند. فرد کوهن نام این کد مخرب را ویروس گذاشت و بدین ترتیب اولین ویروس رایانه‌ای پا به عرضه گذاشت و کوهن توانست با ویروسش، کارشناسان فناوری را درفکر تغییرات اساسی در امنیت رایانه‌ها بیاندازد. از نظر وی برنامه‌هایی که قادر بودند سایر برنامه‌ها را به گونه‌ای دستکاری کنند که سبب تغییر و تحول خودکار در آن‌ها شوند، ویروس خوانده می‌شوند.

در نتیجه کوهن برنامه کوچک چند بایتی نوشت که پس از چند بار اجرا باعث می‌شد به طول برنامه مقداری اضافه شود و این عمل موجب می‌شد که بعد از چند بار اجرا دیگر برنامه آلوده شده، اجرا نشود و در واقع آسیب ببیند. به این ترتیب فرد کوهن از دانشگاه کالیفرنیای آمریکا اولین ویروس کامپیوتری را نوشت. ولی هدف کوهن تخریب و صدمه زدن نبود، بلکه او می خواست ثابت کند که اطلاعات روی دیسک‌ها صدمه پذیر هستند. اما اولین ویروس کامپیوتری غیرآزمایشی در ژانویه ۱۹۸۶ کشف شد و در سال ۱۹۸۷ نام ویروس های کامپیوتری بر سر زبان‌ها افتاد. کوهن به تدریج به عنوان "پدر ویروس‌های کامپیوتری "شناخته شد و کتاب وی با نام "تئوری وآزمایشات ویروس‌های کامپیوتر" مورد توجه فراوان قرار گرفت. اما واقعاً ویروس‌هایی بودند که قبل از شروع تحقیقات او تولید شده بودند،که قبلا به آنها پرداختیم.

در این مقاله تعریفی از ویروس و بدافزار ارائه می گردد و پس از آن در بخش ۳ دسته بندی از ویروس ها ارائه می شود. سپس روش ماشین بردار پشتیبان و منطق فازی در شناسایی ویروس ها بررسی می شوند.

۲. ویروس چیست؟

بدافزار، به هر برنامه ای اطلاق می‌شود که عمدا برای انجام اعمال غیرمجاز و گاها مضر، ایجاد شده است. می توان ویروس‌ها، بک دور*، کی‌لاگر†، و تروجان را به عنوان نمونه ای از بدافزار ها نام برد. یک ویروس، برنامه کامپیوتری است که راندمان سیستم را کاهش داده یا اطلاعات را از بین می برد. در واقع یک ویروس های کامپیوتری یک برنامه مخرب یا یک کد (اسکریپت) بسیار کوچک و قابل اجرا هستند که بر دوش سایر برنامه ها و یا مستندات قرار گرفته تا در زمان لازم، شرایط اجرای آنها فراهم گردد. به محض اجرای برنامه اصلی خود را وارد سیستم رایانه ای شخص قربانی کرده و به هنگام اجرای برنامه به طور خودکار اجرا شده و شروع به تخریب می کنند. این در حالی است که کاربر از وجود ویروس و اعمال آن کاملا بی اطلاع است و هنگامی متوجه می شود که ویروس در عملکرد کامپیوتر اخلال ایجاد کرده است.

ویروس ها ویژگی هایی دارند که این ویژگی ها آنها را از یکدیگر متمایز می کند. در ادامه برخی از ویژگی‌های ویروس‌ها را شرح می‌دهیم:

۱. حجم: حجم ویروس باید بسیار کوچک بوده و دارای کد کمی باشد. دلایل مختلفی برای این ویژگی وجود دارد که مهم‌ترین آنها انتقال آسان، عدم شناسایی و عدم تاثیر چشمگیر برحجم برنامه آلوده شده توسط ویروس است.
۲. تطبیق پذیری: یک ویروس باید توانایی حمله به طیف وسیعی از برنامه‌های متنوع را داشته باشد.
۳. اثر بخشی: یک ویروس باید آثار مخرب بر روی برنامه‌ها و اطلاعات سیستم قربانی به صورت موثر داشته باشد.
۴. عملکرد: ویروس‌ها دارای عملکرد مختلفی هستند. برخی از آنها بدون پاک کردن اطلاعات یا تخریب برنامه‌ها خود را به آنها اضافه می‌کنند. اما برخی دیگر با تخریب برنامه خود را به آن اضافه می‌کنند.

* BACKDOOR
† KEY LOGGER

۵. ماندگاری: ویروس با انجام هر چه بیشتر تکثیر و آلوده کردن برنامه‌های مختلف باعث افزایش ماندگاری خود می‌شود.

۶. وابستگی: از عوامل تاثیرگذار در گسترش ویروس میزان وابستگی آن به محیط اجرایی است. ویروسی می‌تواند تخریب بیشتری داشته باشد که عمومی‌تر، منحصر و مخصوص یک محیط خاص نبوده و وابستگی کمتری به محیط و شرایط داشته باشد.

۷. روش آلوده سازی و انتشار: خصوصیت مهم دیگر ویروس انتشار و آلوده‌سازی است. یک ویروس باید بتواند برای ادامه حیات خود منتشر و برنامه‌های بیشتری را آلوده کند. ویروس باید قادر باشد پس از آلوده کردن یک برنامه سایر برنامه‌ها را نیز آلوده کند. یک ویروس می‌تواند با روش‌های متفاوتی برنامه میزبان را آلوده کند. در زیر سه روش که بیشتر مورد استفاده است شرح داده می‌شود:

a) بازنویسی کردن*: زمانی که یک ویروس با این روش برنامه‌ای را آلوده می‌کند، بسادگی یک کپی از کد خود را در بالای کد برنامه میزبان می‌نویسد این روش خیلی ساده بوده و در ویروس‌های اولیه بکار گرفته می‌شد.

b) الصاق کردن: این روش کمی پیچیده‌تر است. ویروس خود را به انتهای فایل میزبان الصاق می‌کند و سرخط برنامه را اصلاح می‌کند در هنگام اجرای برنامه، برنامه ابتدا به قسمتی که کد ویروس قرار دارد رفته، دستورات ویروس را اجرا می‌کند و بعد برمی‌گردد و به اجرای برنامه میزبان می‌پردازد. در نظر کاربر برنامه به صورت نرمال اجرا می‌شود اما ایراد این روش این است که حجم فایل افزایش می‌یابد.

c) آلوده کننده‌های دیسک: ویروس‌های دیگر رکورد بوت (بوت سکتور) دیسک یا جدول پارتیشن را آلوده می‌کنند. این رکورد قسمتی از دیسک است که هنگام راه‌اندازی سیستم بصورت اتوماتیک خوانده می‌شود این یعنی بعد از راه‌اندازی سیستم ویروس در حافظه قرار می‌گیرد.

۳. طبقه بندی ویروس ها

ویروس ها اغلب با تکثیر خود و الحاق کپی از خودشان به بخشی از فایل برنامه، انتشار می یابند. می توان طبقه بندی زیر را برای ویروس ها نام برد:

۱. ویروس های ساده: این ویروس ها به سادگی کشف می شوند و به ندرت خود را تکثیر می کنند. اگر برنامه آلوده به ویروس اجرا شود، ویروس کنترل کامپیوتر را در دست گرفته و کپی از خودش به فایل برنامه دیگری الحاق می کند. پس از آن که انتشار یافت کنترل را به برنامه اولیه بازگردانده تا کار خود را به صورت عادی ادامه دهد. برای شناسایی این ویروس ها، کافیست آنتی ویروس جستجو یا اسکنی برای یافتن امضای آن داشته باشد. امضای ویروس†، دنباله ای از بایت هاست که شناسه آن محسوب میشوند.

۲. ویروس رمز گذاری شده‡: ایده‌ی این ویروس ها پنهان سازی امضای ثابت آنها بود. این کار با در هم آمیختن ویروس انجام میشد که سبب عدم شناسایی آنها هنگام اسکن ویروس میگردد. یک ویروس رمزگذاری شده از دو بخش تشکیل شده است: روال رمز گشایی و بدنه ی ویروس رمزگذاری شده. اگر برنامه آلوده اجرا شود،

* Overwrite
† Virus signature
‡ Encrypted virus

ابتدا روال رمزگشایی کنترل کامپیوتر را در اختیار می گیرد و پس از آن بدنه ویروس را رمز گشایی میکند. پس از آن روال رمزگشایی کنترل کامپیوتر را به ویروس رمزگشایی شده منتقل میکند.
یک ویروس رمزگذاری شده همچون ویروس های ساده، برنامه ها و فایل ها را آلوده می کند. هر بار که یک برنامه جدید آلوده شود، ویروس یک کپی از هر دو بخش بدنه ویروس رمزگشایی شده، و روال رمزگشایی مربوط به آن تهیه کرده، کپی را رمزگذاری کرده و هر دو را به فایل هدف الحاق می کند.
به منظور رمزگذاری کپی جدید بدنه ویروس، پیش بینی شده که کلید رمز گذاری جدیدی در هر انتقال تولید شود. با تغییر این کلید، بدنه ویروس تغییر کرده و این موضوع سبب می شود ویروس در هر برنامه آلوده شده ای متفاوت از قبل ظاهر شود. به همین سبب شناسایی این ویروس ها توسط آنتی ویروس به علت جستجو برای امضا استخراج شده از بدنه ویروس بسیار دشوار است. البته نقطه ضعف این ویروس ها ثابت ماندن روال رمزگشایی در این مرحله است که منجر میشود آنتی ویروس ها موفق به شناسایی آنها بشوند.

۳. ویروس‌های پلی مورفیک* : این نوع ویروس‌ها به صورت رمزنگاری شده وجود دارند و برای مقابله در برابر شناخته شدن توسط آنتی‌ویروس‌ها کدهای خود را مرتبا رمزنگاری و مخفی می‌کنند و پس از گذشتن آنتی‌ویروس از روی آنها مجددا کد خود را رمزگشایی کرده و شروع به توسعه و رشد خود در سیستم هدف می‌کنند و به این روش خود را از دیده شدن توسط آنتی‌ویروس حفظ می‌کنند. آنها از الگوهای متفاوت در کدگذاری استفاده می‌کنند. این حرکت هوشمندانه این ویروس‌ها عرصه را بر آنتی‌ویروس ها تنگ نموده و نمی‌گذارند آنتی‌ویروس آنها را به راحتی توسط جستجوی، امضاء یا سرنخ (String) پیدا کنند. (چرا که آنها در هر کدگذاری به طور کامل تغییر می‌کنند) نکته جالب در مودی این گونه ویروس‌ها این است که به محض این که توسط آنتی‌ویروسی شناخته شوند یا فایلی را آلوده کنند که آنتی‌ویروس متوجه شود بلافاصله الگوریتم رمزنگاری خود را تغییر می‌دهند و این به این معناست که با هر بار شناسایی این نوع ویروس نوع جدیدی الگوریتم بوجود می‌آید و شناسایی ویروس را برای نرم‌افزار آنتی‌ویروس فوق‌العاده دشوار می‌کند.

۴. آنتی ویروس ها

در دنیای شبکه ای امروز، وجود یک نرم افزار آنتی ویروس قدرتمند به منظور صیانت کامپیوترها از ویروس ها، کرم ها، بمب های منطقی و به طور کلی کدهای مخرب، ضروری است. در واقع آنتی ویروس ها مسئول مقابله با انواع بدافزارها هستند. یک نرم افزار آنتی ویروس مناسب باید دارای ویژگی های زیر باشد:

۱. تست Demand : باید بتواند هنگامی که می‌خواهید به یک فایل یا صفحه اینترنتی یا یک mail دسترسی داشته باشید، آن را کنترل کند.
۲. تست Update : به این معنی که آنتی ویروس باید بتواند در بازه‌های زمانی مشخص بانک اطلاعاتی خود را بروز کند که این بانک شامل الگوهای ویروس‌ها یا امضای آنهاست.
۳. تست Respond : تستی است که نرم‌افزار ضد ویروس بتواند تمامی رفتارهای منطقی در برخورد با یک ویروس را از خود نشان دهد. فایل کثیف را دوباره سازی و تمیز کند و یا آن را حذف نماید.

* Polymorphic

۴. تست Check : باید بتواند تمام فایل‌ها از نوع مختلف را که می‌توانند محلی برای پنهان شدن ویروس باشند را کنترل کند.

۵. تست Heuristics : به این معنی که نرم‌افزار ضد ویروس شما باید با وجود نداشتن الگوی همه ویروس‌ها، بتواند تشخیص خطر دهد و به شما هشدار دهد که "با وجود آن که مطمئن نیستم اما احتمالاً مسئله مشکوکی در کامپیوتر شما وجود دارد." این کنترل نیاز به آن دارد که نرم‌افزار ضد ویروس از هوش بالایی برخوردار باشد.

۶. تکنیک تله گذاری (Mata Hari) : یک تکنیک جالب استفاده شده در آنتی ویروس‌ها فرستادن یک برنامه درون کامپیوتر و جلب کردن توجه ویروس‌ها می‌باشد این برنامه شرایط نفوذ را در خود فراهم کرده و با بررسی مداوم برنامه از لحاظ افزایش حجم و .... به نفوذ برنامه ویروس پی می‌برد.

۵. روش های شناسایی ویروس ها

روش های شناسایی ویروس ها برحسب لزوم اجرای فایل یا عدم لزوم آن در هنگام بررسی به دو دسته تقسیم می شوند: شناسایی ایستا، و شناسایی پویا.

۵,۱ روش‌های ایستا

به روشی که در آن شناسایی بدافزار بدون اجرای فایل مورد نظر انجام گیرد، شناسایی ایستا می‌گوییم. از مزایای این روش می‌توان به آلوده نشدن سیستم در حال اجرای ویروس و سرعت بالای شناسایی اشاره کرد. از روش‌های موجود در این حوزه می‌توان به موارد زیر اشاره کرد:

۵,۱,۱ شناسایی براساس امضا

هر بدافزاری برای اینکه بتواند شناسایی شود نیازمند یک شناسه یکتا می‌باشد. این شناسه می‌تواند قسمت‌های مشخصی از باینری مربوط به فایل باشد یا اینکه می‌تواند یک مجموعه رفتار یکتا از بدافزار باشد که اصطلاحا به آن امضای بدافزار گفته می‌شود، امضا باید به گونه‌ای باشد که بتواند حجم زیادی از آن خانواده توسط آن امضا گرفته شود، با این کار حجم زیادی از ویروس‌ها فقط توسط یک امضا شناسایی می‌شود.

نرم‌افزارهای آنتی ویروس که به این روش کار می‌کنند دارای یک بانک اطلاعاتی هستند. این بانک اطلاعاتی شامل امضای ویروس هاست و به محض این‌که کدی را ملاحظه کرد که معادل یکی از رکوردها باشد آن را به عنوان ویروس شناسایی می‌کند. به نظر می‌رسد که موثرترین راه برای کشف ویروس‌ها همین باشد. روش فوق ذاتا به‌گونه‌ای است که اول ویروس را شناسایی می‌کند و بعد متناظر با آن یک رکورد به بانک اطلاعاتی اضافه می‌کند و حالا اگر ویروسی پیدا کند، در صورتی‌که متناظر با این ویروس، رکوردی در بانک اطلاعاتی باشد قادر به شناسایی آن خواهد بود. در زمان پویش فایل، محتوای فایل‌ها با این امضاها بررسی می‌شود و در صورت تطابق فایل مورد جستجو به عنوان یک ویروس شناخته می‌شود و همین امر ایجاب می‌کند شرکت‌هایی که از این فناوری در نرم‌افزار خود استفاده می‌کنند مدام آن را بروز نگه دارند. به هر حال این یک نقطه ضعف می‌باشد و برای فائق آمدن بر آن دو روش دیگر در نرم‌افزارهای ضدویروس معرفی شده است. استفاده از الگوریتم‌های پویش فایل که در سرعت و حافظه مصرفی مناسب باشند یکی از مهم‌ترین موارد شناسایی بر اساس امضا هستند.

۵,۱,۲ شناسایی بر اساس اکتشاف

فلسفه Heuristic این است که بتوانیم ویروس‌هایی را شناسایی کنیم که هنوز امضای ویروس در بانک اطلاعاتی موجود نمی‌باشد،

این کار با استفاده از یک بانک اطلاعاتی که رکوردهای آن حاوی Virus behavior signature می‌باشد قابل انجام است. یک فایل حاوی بدافزار ممکن است که دارای مشخصه‌های باشد که یک فایل سالم معمولا آن ویژگی‌ها و مشخصه‌ها را ندارد، مثلا این‌که هر کجا تشخیص بدهند کدی قصد پاک کردن Boot Sector را دارد از آن جلوگیری می‌کنند. برخلاف روش قبل که بیشتر در یک خانواده به دنبال یک مشخصه خاص برای اعلام ویروسی بودن آن فایل می‌نمود، در این روش به دنبال مشخصه‌های عامی هستیم که بتوانیم بوسیله آنها و با استفاده از الگوریتم‌های بر پایه هوش مصنوعی به شناسایی بدافزارهایی که از آنها امضایی وجود ندارد و ناشناخته هستند بپردازیم. در این روش‌ها معمولا یکسری از هیورستیک‌ها که می‌توانند خاصیت بدافزاری بودن فایل را بالا ببرند بررسی می‌شوند و در نهایت ترکیبی از این‌ها به عنوان یک احتمال جهت ویروسی بودن معرفی می شود. هیورسیتیک‌های همچون حلقه‌های رمزگشا، فراخوانی توابع ، API های مشکوک، رشته‌ها و کلید واژه‌های که ایجاد خاصیت بدافزاری می‌کنند و ... . همچنین ممکن است از هیورستیک‌های استفاده شود که احتمال بدافزار بودن فایل را کمتر کند، مانند اینکه بدافزار از واسط کاربری گرافیکی یا پنجره‌های Pop-up استفاده کند. یکی از مهم‌ترین مزایای این روش این است که بسیاری از بدافزارها هستند که ممکن است هنوز ناشناخته مانده باشند و امضای برای آنها تاکنون ایجاد نشده باشد، با استفاده از این روش می‌توان با توجه به ویژگی‌ها و خصیصه‌های که آن بدافزار دارد احتمالی را به آن اختصاص دهد که باعث کشف بدافزار شود. نگرانی که در استفاده از این روش وجود دارد، وجود خطاهای مثبت کاذب می باشد، که آنتی ویروس های مختلف با استفاده از روش‌های مختلف سعی بر این دارند که این خطای مثبت کاذب را به پایین‌ترین حد ممکن برسانند.

الگوریتم‌های Heuristic به دو صورت پیاده‌سازی می‌شوند:

اگر تکنولوژی Heuristic کد هر برنامه را با Virus behavior Signature مقایسه کند و مورد آنالیز قرار دهد آن را روش static heuristic می‌نامیم.

در بعضی مواقع این تکنولوژی قطعه کد را در یک ماشین مجازی اجرا می‌کند تا نتایج رفتاری آن را ببینند به این روش dynamic heuristic می‌گوییم. این روش ممکن است نتایج غلطی نیز تولید کند. که در قسمت شناسایی پویا به آن می‌پردازیم.

۵,۲ شناسایی پویا

به روشی که در آن شناسایی بدافزار با اجرای فایل مورد نظر انجام گیرد، شناسایی پویا می‌گوییم. در این روش سعی بر این است که بدافزار در یک محیط مجازی اجرا شود و تمامی رفتارهای آن مورد بررسی قرار گیرد و در صورت مشکوک بودن رفتارهای فایل اجرا شده، ویروسی بودن آن اعلام شود. بسیاری از بدافزارها هستند که در حالت ایستا قابل شناسایی نیستند، زیرا فایل مرتبط با آن بدافزار به صورت رمزشده می‌باشد، و از این رو نمی‌توان اطلاعات لازم برای شناسایی بدافزار همچون وجود امضا ویروس یا ویژگی‌های که باعث شناسایی بدافزار از طریق روش‌های هیورستیک است را استخراج نمود و برای شناسایی این نوع بدافزارها باید به گونه ای بدافزار را رمزگشایی کرد، در شناسایی پویا با اجرا کردن بدافزار سعی در گذر از این موانع داریم.

اما از معایب این روش می توان به بدافزارهایی اشاره کرد که فعال شدن آنها نیازمند برآورده شدن شرایطی خاص باشد، و ممکن است زمانی که بدافزار در حال اجرا است شرایط لازم برای آن مهیا نشود، در صورتی که با استفاده از روش‌های ایستا امکان داشت که بتوان ویژگی‌هایی را استخراج کنیم که بدافزار به راحتی قابل شناسایی باشد. در مجموع جهت شناسایی بدافزار بهتر است از ترکیبی از هر دو روش استفاده شود تا بتوان دقت شناسایی را بدین ترتیب بالاتر برد. از جمله از روش‌های شناسایی پویا ،می‌توان به جامعیت سر جمع اشاره نمود.

۵,۲,۱ جامعیت سرجمع

در این روش، فرض براین است که ویروس قصد اعمال تغییراتی در فایل دارد. مثلا یک ویروس می‌خواهد که روی یک فایل چیزی بنویسد یا این‌که خودش را به آخر فایلی اضافه کند. در این روش نرم‌افزار checksum فایل غیر ویروسی و یا درایورهای تمیز را ذخیره می‌کند و هرگاه که تغییری در این checksum مشاهده شود متوجه می‌شود که احتمال دارد ویروسی این کار را انجام داده باشد. در این روش نیز احتمال تولید نتایج غلط وجود دارد. این روش در مقابله با ویروس‌های ماکرویی یا ویروس‌های مانند Red Code که بدون این‌که در هیچ فایلی ذخیره شوند در حافظه بارگذاری و اجرا می‌شوند، کارایی چندانی ندارد.

اگر یک کد مزاحم از تمام الگوریتم‌های یک ضدویروس که تاکنون نام بردیم بگذرد، در گام آخر توسط فناوری دیگری به نام Activity Blocker از فعالیت آن جلوگیری می‌شود. این تکنولوژی از تمام فعالیت‌هایی که ممکن است توسط یک کد مخرب صورت بپذیرد جلوگیری می‌کند مثلا اگر تشخیص دهد که هارد دیسک در حال فرمت شدن است از آن جلوگیری می‌کند.

۶. استفاده از **SVM** و منطق فازی در شناسایی بدافزارها

در زمان ظهور اولین ویروس های کامپیوتری در سال 1986 تا کنون تعداد قابل توجهی از ویروس های جدید هر ساله منتشر می‌شوند. تلاش های سنتی برای مبارزه با این حجم بالا از ویروس ها نتیجه چندان رضایت بخشی را به همراه نمی آورد. از طرف دیگر دیدگاه سنتی شناسایی ویروس ها که صبر می کرد تا چند رایانه آلوده شود، سپس ویروس را تشخیص میداد و بعد از آن شروع به مبارزه با ویروس می‌کرد یک راه حل پر هزینه است. همچنین این راه حل برای شناسایی برخی از ویروس ها چندان کاربردی نیست. پس نیاز به طراحی یک سیستم هوشمند به عنوان یک راه حل دقیق و قابل اعتماد برای شناسایی ویروس ها یا کمک به کارشناسان در پیدا کردن انواع ویروس‌های جدید احساس می شود.

۶,۱ ماشین بردار پشتیبان*

در بسیاری از کاربردها برای تحلیل و بررسی یک سیستم، ابتدا رفتار آن سیستم را بر اساس اطلاعاتی که از سیستم داریم، مدل می‌کنیم و سپس از آن مدل برای تشخیص رفتارهای آتی آن سیستم استفاده خواهیم کرد. در اینجا تمرکز بر روی ویروس است. هدف این است که رفتارهای یک ویروس را مدل کنیم و سپس از این مدل برای تحلیل رفتارهای ناشناخته آن ویروس استفاده کنیم. برای مدلسازی رفتار یک ویروس می‌توانیم از روش‌های مختلفی مانند زنجیره های مارکوف، گراف‌ها و تئوری گراف‌ها، روش‌های خوشه‌بندی و روش‌های طبقه‌بندی استفاده کنیم. یکی از روش های مدل سازی رفتار ویروس مبتنی بر روش طبقه بندی، استفاده از تکنیک ماشین های بردار پشتیبان است. ماشین‌های بردار پشتیبان، الگوریتم های بسیار قدرتمندی در دسته بندی و تفکیک داده ها هستند بخصوص زمانی که با سایر روشهای یادگیری ماشین تلفیق شوند. این روش برای جاهایی که با دقت بسیار بالا نیاز به ماشینی داده ها است، به شرط اینکه توابع نگاشت به درستی انتخاب شوند، بسیار خوب عمل می کند.

در مقاله[۲] یک روش جدید برای شناسایی ویروس های کامپیوتری از طریق SVM پیشنهاد شده است. در [۲] گفته شده آزمایش سیستم طبقه بندی ویروس ها اولین بار از روش های مبتنی بر SVM ایجاد شده است که برای شناسایی ویروس های کامپیوتری ناشناخته استفاده می‌شود. بنابراین طبق آزمایش انجام شده ماشین بردار پشتیبان نتیجه بهتری از سایر الگوریتم های شناسایی داشته است.

* Support Vector Machine

۶,۲ منطق فازی

منطق فازی عبارت است از استدلال با مجموعه فازی. مجموعه فازی توسط لطفی زاده ارائه گردید. در [۵] با ترکیب منطق فازی و استفاده از فایل n-gram در دسته بندی فایل ها، ویروس ها شناسایی میشوند. در روش ذکر شده در این مرجع، فایل ها را به سه دسته تقسیم می کند که فایل های آلوده به ویروس، فایل های سالم، و فایل هایی که ویروس نبوده و رفتاری مشابه ویروس ها دارند که اصطلاحا به آنها شبه ویروس گفته می شود. این روش کد باینری یک فایل را معیاری برای ارزیابی قرار داده و برای طبقه بندی و تطبیق آن با پایگاه داده ویروس ها از n-gram فایل استفاده می کند. برای اینکه مشخص شود فایلی درکدامیک از سه دسته نامبرده قرار میگیرد کافیست n-gram آن محاسبه شده و درصد تطبیق آن با هر یک از اعضای پایگاه داده معلوم گردد.

شبکه های عصبی، سیستم های ایمنی مصنوعی*، ویا مدل پنهان مارکوف† روش هایی هستند که تاکنون جهت شناسایی بدافزارها استفاده شده است[۳].

۷. مراجع

1.Duc Nguyen Trung, Jason J. Jung. (2013),“Semantic Analysis based on Fuzzy propagation in Online Social Networks: a case study on TweetScope,” Journal of computer science and information systems, pp 215–228.

2.Bo-yun Zhang, Jain-ping Yinl and and co-author. (2006),“Using support Vector Machine to detect Unknown Computer Viruses*”,ISSN 0973-1873 Vol. 2,No. 1,pp. 100-104.*

3.Mai Trong Khang, Vu Thanh Nguyen, Tuan Dinh Le,(2015) “Acombination of Artificial Immune System for Virus Detection”, REV Journal on Electronics and Communication, Vol. 5, pp. 52-57

4.Anita Thengade, Aishwarya Khaire, and Co-author,(2014), “Identification of Metamorphic Viruses,” International advanced computing conference (IACC)

۵. شمسی ف، میرعمادی م، هل اتائی ف. (۱۳۹۶) ، "شناسایی ویروس ها با منطق فازی بر مبنای n-gram فایل،" دومین کنفرانس بین المللی ترکیبیات رمزنگاری و ترکیبیات .

* Artificial Immune System
† Hidden Markov Model