دانشگاه علوم پزشکی و خدمات بهداشتی درمانی سپرجند

حراست

آشنایی با ویروس

(قسمت هشتم – ضد ویروس)

تنظیم کننده :

حراست فناوری اطلاعات دانشگاه

روش‌های تشخیص ویروس در آنتی‌ویروس

نرم‌افزارهای آنتی‌ویروس عموماً از دو تکنیک برای تشخیص ویروسها استفاده می کنند:

۱. استفاده از فایل امضای ویروس : این تکنیک توانایی شناسایی ویروسهایی را دارد که شرکتهای آنتی‌ویروس تا کنون برای آنها امضا یا Signature تولید کرده اند. در این روش ضدویروس، متن فایلهای موجود در رایانه را هنگامی که سامانه‌ی عامل، آنها را بازمی‌کند ،می‌بندد یا ارسال میکند، امتحان کرده و آن را به فایل امضای ویروس، که نویسندگان آنتی ویروس تشخیص داده‌اند ارجاع می‌دهد.

فایل امضای ویروس، یک رشته بایت است که با استفاده از آن می‌توان، ویروس را به صورت یکتا مورد شناسایی قرار داد و از این جهت مشابه اثر انگشت انسانها می‌باشد.

اگر یک تکه کد در فایلی با ویروس موجود، در فایل امضای ویروس مطابقت داشت، نرم‌افزار ضدویروس یکی از کارهای زیر را انجام می دهد:

-سعی می کند تا فایل را توسط از بین بردن ویروس به تنهایی تعمیر کند.

-قرنطینه کردن فایل (فایل قابل دسترسی توسط برنامه‌های دیگر نباشد و ویروس، نمی‌تواند گسترش یابد.)

-فایل ویروسی و آلوده را پاک کند.

دراین تکنیک، فایل امضای ویروس یا همان پایگاه داده ویروسهای شناخته شده، باید به طور متناوب update شودتا آخرین اطلاعات را، راجع به آخرین ویروسها به دست آورد.

کاربران وقتی ویروسهای جدید (ناشناخته) را تشخیص دادند ، می‌توانند فایل‌های آلوده را به نویسندگان آنتی‌ویروس ارسال کنند.

۲. استفاده از الگوریتم اکتشافی

(Heuristic Analyzer):

وقتی تعداد کدهای مخرب به بیش از هزاران مورد رسید و کمپانیهای ضدویروس دیدند که نمی‌توانند برای هر ویروس، یک امضای جداگانه تهیه کنند، به فکر این روش افتادند. این تکنیک برای کشف ویروسهای ناشناخته که فایل امضای آنها وجود ندارد به کار می رود.

دراین تکنیک از روش زیر استفاده می شود:

Dynamic Heuristic analysis : شبیه سازی کد، به این معنی است که، فایل در یک محیط محافظت شده در داخل ماشین مجازی، شروع به اجرا می‌کند. سپس به برنامه آنتی‌ویروس اجازه می‌دهد تا رفتار یک فایل مشکوک را به هنگام اجرا شبیه سازی کند، در حالی که کد مشکوک اصلی ازماشین واقعی کاملاً مجزا شده است.وبعد بر فعالیتهای ویروسی مثل تکرار کد ، دوباره نویسی فایل و تلاش برای پنهان سازی فایلهای مشکوک، نظارت می‌کند.

هرگاه یک یا بیشتر از آن فعالیتهای شبه ویروس را پیدا کرد، فایل مشکوک علامت گذاری و به کاربر اطلاع داده می‌شود. مثلا اگر برنامه‌ای از رمز خود تصحیح کننده، استفاده کرده، ویروس به شمار می‌آید.

این تکنیک، حفاظت بیشتری را در مقابل ویروسهای جدید تجاری که هنوز وارد پایگاه داده‌ی نشانه‌های ویروسی نشدند، به وجود می آورد.

مشکلات روش های اکتشافی

***تشخیص مثبت اشتباه False Positive: این روش از ویژگیهای عمومی ویروس استفاده می کند، و بنابراین ممکن است برخی از نرم افزارهای قانونی و معتبر را در صورتی که خصوصیاتی شبیه بدافزار داشته باشند،نیز به اشتباه بدافزار شناسایی کند.**

***بررسی کندتر: پروسه جستجوی ویژگیها برای یک نرم افزار بسیار سخت تر از جستجوی الگوهای مشخص است.به همین دلیل جستجوی اکتشافی مدت زمان بیشتری نسبت به جستجوی امضاء جهت شناسایی بدافزارها نیاز دارد.**

***ندیدن ویژگیهای جدید: در صورتی که یک حمله بدافزاری جدید ویژگیهایی از خود به نمایش بگذارد، که پیش از شناسایی نشده اند،جستجوی اکتشافی نیز آن را شناسایی نمیکند مگر اینکه به روز رسانی شده و ویژگی مذکور به حافظه آن اضافه شود.**

بعضی از آنتی‌ویروسها از روشهای دیگر اکتشافی استفاده می‌کنند

Instruction Prevention System-ips: این روش متکی بر بستن آسیب‌پذیرهای یک سامانه است که در واقع قبل از آنکه یک کد مخرب حمله خودش را آغاز کند، راه ورود و تخریبش را می‌بندد.

یک فنّاوری خوب علیه هکرها و ویروسها و کرمهای bodiless .

برای دیگر کدهای مخرب مثل کرمهای ایمیل ، ویروسهای عادی و تروجان‌ها موثر نیست.

Behavior Blockers : محدود کننده رفتارها .تقریبا حدود ۱۳ سال پیش به وجود آمدند و مورد توجه قرار نگرفته‌اند!!

اما در سالهای اخیر با پخش شدن سریع کدهای مخرب، این روش هم رونق پیدا کرده است . این روش به رفتارهای مشخص و واضح کرمها و ویروسها توجه میکند ودر صورت کشف چنین رفتاری اجازه انجام شدن آن را نمی‌دهد.

Prehistoric behavior blockers : در واقع همان **behavior blocker** های قدیمی.کار این نوع که اولین نسل بودند خیلی ساده بود: رفتارهای اتفاقی را به کاربر هشدار می‌داد و به او اختیار انجام یا توقف آن را می‌داد.

behavior blockers for vba programs : این نوع سپر دفاعی هم از کاربر دستور می‌گرفت و همان کار را انجام می‌داد چون خودش نمی‌توانست بفهمد چه رفتاری مخرب و چه رفتاری مخرب نیست. ولی این بلوکرها قدرت تشخیص در مخرب بودن را نسبت به نوع اولیه بیشتر داشتند.

Second generation behavior blockers : در این روش که نسل بعدی بلوکرها است، به جای بلوک کردن تک تک رفتارها ؛ یک رشته از رفتار، آنالیز و بلوکه می‌شود و به این صورت اخطارهایی که به کاربر داده می‌شود به طور چشم گیری کاهش می‌یابد.

- نرخ شناسایی این روش زیاد است . (بیش از ٪۶۰).

- به روز آوری های منظم احتیاج ندارد.

- از منابع سامانه به میزان خیلی کم استفاده می‌کند.

- کاربر را در تصمیم گیری برای متوقف ساختن یک کد مخرب درگیر می‌کند.

Policy based security : این روش هم یکی از روشهای موثر در جلوگیری از اجرای کدهای مخرب، از طریق تعریف **Policy** برای منابع به شمار می‌رود. شرکت‌های زیادی از این راهبرد برای جلوگیری از طیف وسیعی از آلودگی‌ها استفاده می‌کنند. یک طراحی خوب می‌تواند از حمله‌های بسیاری از هکرها و کدهای مخرب جلوگیری کند.

Check Summing: ازمحاسبات ریاضی استفاده می‌کند تا وضعیت برنامه‌های اجرایی را قبل و بعد از آنکه آنها اجرا شوند مقایسه کند.اگر مجموع (**checksum**) تغییر نکند، بنابراین سامانه آلوده نشده است.این روش می‌تواند آلودگی را فقط بعد از زمانی که ویروس، سامانه را آلوده کرده کشف کند. از آنجا که این فنّاوری منسوخ و کهنه شده و

بعضی از ویروسها می‌توانند از آن فرار کنند، امروزه این روش به ندرت استفاده می‌شود.

*همیشه ترکیبی از چند روش یکی از راهکار های اساسی خواهد بود

نرم افزارهای ضدویروس چگونه ویروسهای جدید را به دست می‌آورند ؟

۱. رباتهای مخصوص این کار

۲. استخدام Virus Researcher ها و یافتن کدهای مخرب جدید به طور دستی.

۳. ارسال کدهای مخرب جدید، توسط کاربران از طریق ایمیل یا سامانه‌های تعبیه شده درون نرم‌افزار.

۴. رایانه هایی در سراسر اینترنت که وظیفه جمع آوری کدهای مخرب را دارند.این سامانه‌ها با ربات‌هایی که ترافیک را کنترل می‌کنند فرق دارند و همیشه در پایین ترین سطح امنیتی و بالا ترین شانس آسیب پذیری قرار دارند.

۵. اسکنرهایی که کاربران فایلهایشان را برای تشخیص آلودگی به آنها آپلود می‌کنند، مانند اسکنرهای jotti,virus total .

۶. تبادل فایلهای آلوده بین کمپانی‌های ضدویروس.