به نام خدا

پدافند غیر عامل باید همچون شعله‌ای بلند شود.

مقام معظم رهبری

پدافند غیرعامل– ضد بدافزار

فهرست:

مقدمه

فضای IT همچون دنیایی که در آن زندگی می کنیم سرشار از ویروس های آلاینده، دزدان و جاسوسانی است که همواره در کمین هستند تا با استفاده از فرصت ها و ویژگی های خاص این فضا، کاربران ناآگاه، ناآماده و اهداف تعیین شده خود را آلوده کرده، اطلاعاتشان را نابود و یا به سرقت برند. زندگی و استفاده از این فضا که ویژگی ها و محسنات آن را نه می توان و نباید نادیده گرفت؛ می بایست با نگاه ویژه و اساسی به مقوله امنیت به عنوان عنصر کلیدی و نقطه عطف استفاده از فناوری اطلاعات همراه باشد؛ وگرنه همواره باید آلوده و غارت شده به دنبال سهم خود در این فضا بدویم.

کتابچه حاضر با توجه به اهمیت نرم افزارهای ضدبدافزار[۱] و نقش اساسی آن ها در تأمین امنیت سیستم ها و شبکه های رایانه ای در کنار دیگر ابزارهای امنیتی و در جهت آشنایی با انواع بدافزارها و نحوه عملکرد ضدبدافزارها، با رویکرد ایجاد و استفاده از ضدبدافزارهای بومی پرقدرت در جهت رسیدن به حداکثر امنیت، ایمنی و پایداری زیرساخت و فضای IT کشور در راستای اهداف پدافند غیرعامل کشور در این حوزه تهیه شده است.

---

[۱] Antivirus

فصل ۱ - آشنایی با بدافزارها

بدافزار، نرم افزاری است که با هدف نقض امنیت، ایمنی یا پایداری اطلاعات، ناخواسته یا ناآگاهانه وارد رایانه ها و شبکه های رایانه ای شده و در بیشتر موارد اقدام به تکثیر خود یا بدافزارهای دیگر می نماید.

بطور کلی بدافزارها به دو دسته زیر تقسیم می شوند:

- **بدافزارهای باغ وحش:** این نوع بدافزارها گسترش چندانی نیافته و در محدوده خاص باقی می مانند. بعنوان مثال بدافزاری که در یک آزمایشگاه بدافزارنویسی ایجاد شده است و هرگز به بیرون از آن آزمایشگاه ارسال نشده است، از این نوع بدافزار به حساب می آید.
- **بدافزارهای حیات وحش:** بدافزارهایی هستند که در گستره جغرافیایی معینی گسترش یافته اند و لیست این نوع بدافزارها توسط سازمان های مختلفی چون سازمان WildList.Org نگهداری و بروز می شود.

شایعترین نوع بدافزار ویروس نام دارد. ویروس نوعی بدافزار است که قادر به تکثیر نمونه های یکسان یا تغییر یافته خود می باشد. ویروس ها عموماً فایل های سیستم میزبان را آلوده کرده و یا

ارتباطات بین فایلهای موجود روی سیستم میزبان را تغییر جهت می دهند.

انواع ویروس ها عبارتند از: ویروس های رکورد راه انداز، ویروسهای فایل، ویروس های فایل سیستم و ویروس های رمزشده.

کرم ها نیز در واقع ویروسهایی هستند که هدفشان شبکه های رایانه ای می باشد. این نوع بدافزارها باتوجه به ضعف های امنیتی موجود در شبکه های رایانه ای که بعضاً ذاتی است، قادرند بدون اطلاع کاربران ایستگاه های کاری شبکه، وارد سیستم آنها شده و فعالیت کنند. کرم ها نوعاً برنامه اجرائی مستقل هستند و نیازی به واردشدن به فایل های کاربران ندارند. در واقع کرم ها ویروس هایی هستند که بستر اصلی گسترش و فعالیت آنها عموماً شبکه های رایانه ای می باشد.

بمب های منطقی به رفتارهای مخربی اطلاق می شود که خواسته یا ناخواسته از سوی نرم افزارهایی که با این هدف ساخته نشده اند، دیده می شود. بعنوان نمونه یک بمب منطقی ممکن است بمنظور محافظت از کپی غیرمجاز از یک نرم افزار، بعد از مدتی و در صورت وقوع شرایط خاصی برنامه اجرائی را از روی دیسک سخت حذف کند. این موارد عمدتاً در نرم افزارهایی رخ می دهد که قبل از توزیع مورد بازبینی دقیق قرار نگرفته باشند.

تروجان ها بی شک پیچیده ترین نوع بدافزارها می باشند. این نوع بدافزارها در ظاهر نرم افزارهای مفیدی هستند ولی در باطن اقدام به فعالیت های مخرب در سطح رایانه کاربر نموده و یا زمینه را برای فعالیت مخرب دیگر بدافزارها یا نفوذ هکرها فراهم می آورند. کاربرد عمده تروجان ها در عملیات نفوذ به شبکه ها و رایانه ها توسط هکرها می باشد. تروجان ها با ایجاد تغییر در کد منبع نرم افزارهای کاربردی دیگر، ایجاد شده و پس از آن به سختی قابل شناسایی و پاکسازی هستند. در حال حاضر سه نوع تروجان شناسایی شده است که عبارتند از: تروجان های نوع درپشتی[۱]، تروجان های نوع روت کیت و تروجان های نوع پسورد دزد[۲].

شبه بدافزارها نوع دیگری از نرم افزارهای آلاینده بحساب می آیند و بطور کلی برای تغییر رفتار رایانه و ایجاد نگرانی یا جاسوسی استفاده می شوند. انواع شبه بدافزارها بشرح ذیل می باشند:

جاسوس افزارها[۳] اقدام به جمع آوری اطلاعات کاربر می کنند. برخی از Spywareها اقدام به جمع آوری اطلاعات مالی افراد و

---

[۱] Backdoor

[۲] Password Stealer

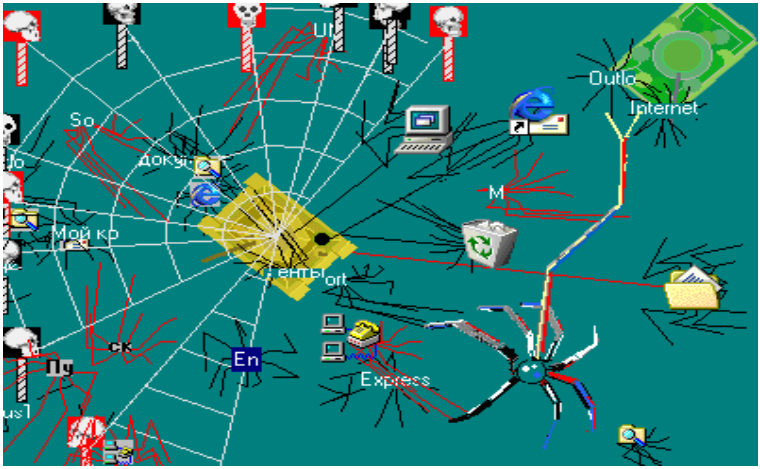
[۳] Spyware

حساب های بانکی اینترنتی آنها می کنند، بنحوی که با انتقال صفحات اصلی سایت های خرید و فروش معروف به صفحات دیگری در اینترنت اطلاعات بانکی آنها را به سرقت می برند.

برنامه های Joke با ایجاد تغییر در رفتار رایانه باعث ایجاد مزاحمت و نگرانی کاربران می شوند.

برنامه های Hoax معمولاً کاربر را در جهت مقاصد خود وادار می کنند تا این شبه بدافزار را به کاربران دیگر ارسال کند. بعنوان مثال نامه ای در مورد یک کودک فقیر که در انتهای آن یک شماره حساب برای کمک به وی آمده است از نمونه های رایج Hoax می باشد.

برنامه های Adware بدون اطلاع کاربر وارد رایانه می شوند. برنامه های Adware صفحات تبلیغاتی را مرتباً در رایانه کاربر بارگذاری می کنند.



در ادامه به شرح انواع خاصی از مفاهیم مرتبط با بدافزارها می پردازیم :

- Germ: اولین نسخه یک بدافزار قبل از اینکه وارد یک فایل آلوده شده باشد، Germ نامیده می شود. آن ها قدرت فعالیت و تکثیر ندارند. Germ بعنوان نسل اول یک بدافزار بوده و برای اجرا باید وارد یک فایل اجرائی شود.
- Exploit: براساس نقاط نفوذ[۱] ایجاد می شوند و از نوع برنامه اجرائی هستند که نتیجه اجرای آنها سوءاستفاده از نقاط نفوذ موجود روی سیستم عامل می باشد. البته هکرهای کلاه سفید معمولاً فایل های Exploit را برای اهداف آزمون نفوذ و رفع ضعف های موجود روی سیستم ها ایجاد و منتشر می کنند.
- Downloader: این نوع بدافزارها مجموعه دیگری از بدافزارها را از اینترنت دریافت کرده و وارد سیستم کاربر می کنند. آن ها معمولاً از طریق نامه الکترونیکی ارسال شده و بعد از ورود به سیستم کاربر بدافزارهای معینی را از اینترنت دانلود می کنند.

---

[۱] Vulnerability

- Dialer: هدف این نوع بدافزارها شبکه های اینترنت DialUp و سیستم های BBS[۱] می باشد. این بدافزارها در صورت فعال شدن اقدام به شماره گیری از طریق رایانه کاربر کرده و با اهداف مالی به نفع نویسندگان آنها شروع به فعالیت می کنند.
- Dropper: این نوع بدافزارها برای بستر سازی فعالیت دیگر انواع بدافزارها استفاده می شوند. یکی از مهمترین کاربردهای این نوع بدافزارها وارد نمودن فایل ویروس های سکتور راه انداز در سیستم می باشد.
- Injector: این نوع بدافزارها قادر به وارد کردن دیگر بدافزارها در برنامه های درحال اجرا روی RAM سیستم هستند. بعنوان مثال Injector ها می توانند کد ویروس مورد نظر را در برنامه های فعال مربوط به دیسک وارد کنند.
- Auto-Rooter: این بدافزارها توسط هکرها و بمنظور ورود به سیستم های کاربران از راه دور استفاده می شوند. این بدافزارها با اجرای مجموعه ای از Exploitها روی سیستم کاربر با هدف دسترسی به root سیستم (بالاترین

[۱] Bulletin Board System

سطح دسترسی) شرایط را برای فعالیت هکرها روی رایانه هدف فراهم می آورند.

- Kit ها (Virus Generator): بدافزارنویسان با توسعه Kit ها تحت عنوان لابراتوارهای توسعه بدافزارنویسی، سطح دانشی لازم برای تولید بدافزار را کاهش می دهند؛ با استفاده از آنها حتی برنامه نویسان مبتدی kit نیز می توانند اقدام به تولید بدافزار و توزیع آن کنند.
- Spammer: این نوع بدافزارها پیام های تبلیغی خاصی را از طریق گروههای پیام رسانی یا گروههای خبری یا انواع نامه های الکترونیکی و یا SMS ارسال می کنند.
- Flooder: این نوع بدافزارها توسط هکرها و برای شکل گیری حملات DoS استفاده می شود.
- Keylogger: این بدافزارها قادر به تشخیص و ضبط کلیدهای فشارداده شده توسط کاربر می باشند. از این نوع بدافزارها برای مقاصد مختلفی از جمله سرقت اطلاعات شخصی افراد و ورود غیرمجاز به سیستم ها استفاده می شود.

فصل ۲ - نحوه عملکرد ضد بدافزار ها

بطور کلی ضدبدافزارها سه عمل اصلی انجام می دهند:

- **ردیابی**

در این مرحله کد داخل فایلهای اجرائی بررسی و آلوده بودن آن تعیین می شود. البته ردیابی بدافزارها توسط یک ضدبدافزار، نسبی است و بستگی به بروزرسانی آن دارد. حتی اگر یک بدافزار قابلیت فعال شدن نداشته باشد باید توسط یک ضدبدافزار ردیابی و حذف شود تا باعث آلودگی دیگر سیستم ها نگردد. روشهای ردیابی را می توان به دو نوع ایستا و پویا تقسیم نمود. روش های ردیابی ایستا بدون نیاز به اجرای کد بدافزار قابلیت ردیابی آن را دارند ولی در روش پویا باید کد بدافزار اجرا و رفتار آن مورد بررسی قرار گیرد؛ البته این اجرا معمولاً در یک محیط شبیه سازی شده انجام می گیرد.

روش های ایستا

- روش بکارگیری پویشگر:

این روش جزو اولین و رایجترین روشهای بکاررفته در ضدبدافزارها برای شناسایی بدافزارها می باشد بطوریکه ضدبدافزارها عموما با عنوان اسکنر شناخته می شوند. فرآیند جستجوی الگوی بدافزار در داخل یک فایل، توسط ابزاری بنام پویشگر انجام می شود. بطور کلی جستجو برای یافتن الگوی دودویی بدافزار در یک بلوک دودویی برحسب واحد بایت انجام می شود. بلوک دودویی مورد جستجو می تواند سکتور راه انداز دیسک، کل یک فایل یا بسته اطلاعاتی شبکه باشد.

با توجه به اینکه صدها هزار الگو برای بدافزار باید در داخل هر فایل جستجو شود؛ پیمایش هر فایل به تعداد الگوی بدافزارها و برای هر بدافزار بصورت ترتیبی امکانپذیر نبوده و باید تمهیداتی در این خصوص اندیشیده شود. الگوریتمهای بکاررفته در پویشگرها از نوع الگوریتم های جستجوی همزمان چندالگویی[۱] می باشد.

[۱] Multi pattern search algorithm

- روش مکاشفه ای یا هوشمندانه

در روشهای هوشمندانه بجای جستجوی الگوی بدافزارها در داخل تمامی فایلها، فایلهای اجرائی حاوی کدهای مشکوک به وجود بدافزار مورد بررسی قرار می گیرد. این روش در دو مرحله اصلی انجام می شود، در مرحله اول داده های مهم از فایلها جمع آوری می شود. در این مرحله علائم مشخصه احتمال آلودگی فایل که اصطلاحاً بوستر[۱] نامیده می شوند، جستجو و جمع آوری می شود. وجود هر بوستر میزان احتمال آلودگی را افزایش می دهد. در مرحله دوم داده های حاصل از مرحله اول مورد تحلیل قرار می گیرد واگر حاصل نهایی از یک مقدار معین بالاتر باشد، فایل به عنوان یک فایل آلوده گزارش می شود.

- روش بررسی جامعیت

با آلوده شدن یک فایل، بطور حتم کد CRC[۲] مربوط به آن تغییر خواهد کرد زیرا محتوای فایل تغییر یافته است. در این روش در یک سیستم عاری از هر نوع بدافزار جامعیت مربوط به تمامی فایل ها محاسبه و ثبت می شود. سپس در

[۱] Booster

[۲] Cyclic Redundancy Check

ادامه با دسترسی به هر فایل، کد جامعیت جدید محاسبه و با کد پایه مقایسه می گردد؛ اگر این کد تغییر یافته باشد، تغییری در این فایل ایجاد شده است که باید مورد توجه قرار گیرد. این روش به تنهایی نمی تواند پاسخگوی مناسبی برای مقابله با بدافزارها باشد.

روش های پویا

- روش بکارگیری ناظرو بلوکه کننده رفتاری

در این روش، ضدبدافزار رفتار برنامه در حال اجرا را تحت نظر گرفته و رفتارهای مشکوک را مورد توجه قرار می دهد. سوالاتی که در مورد نحوه اجرای این روش مطرح است عبارتند از:

۱. ترکیب مختلف رفتارهای مشکوک و عادی ممکن است وجود داشته باشد؛ ضدبدافزار به چه روشی سلسله رفتارهای مشکوک را تشخیص می دهد؟
۲. تا چه مدتی باید رفتار یک برنامه در حال اجرا تحت نظر قرار گیرد؟

در پاسخ به سؤال اول، متخصصین تحلیل بدافزار معمولا طول ثابتی برای مشخصه پویای بدافزارها در نظر می گیرند.

اگر عملیات مشکوک به تعداد مشخص شده و پشت سرهم رخ دهد، این مجموعه عملیات با جدول مشخصه پویای بدافزارها مقایسه و مورد بررسی قرار می گیرد.

در پاسخ به سوال دوم، بدیهی است که این زمان نمی تواند مدت زیادی باشد؛ زیرا باعث کاهش کارآیی رایانه در اجرای برنامه ها خواهد گردید. با توجه به اینکه اغلب بدافزارها در ابتدای اجرای یک برنامه اقدام به تکثیر و فعالیت می کنند، معمولاً تحت نظر گرفتن یک برنامه در ابتدای اجرا کافی به نظر می رسد. البته این فرض همیشه درست نیست و به همین دلیل می بایست مرتباً در دوره های تصادفی، ضدبدافزار اقدام به بررسی مجدد رفتار برنامه در حال اجرا نماید.

- روش بکارگیری شبیه ساز

در روش بکارگیری ناظر رفتاری به برنامه ای که احتمال آلودگی آن می رود، مجوز اجرای مستقیم روی رایانه کاربر داده می شود که می تواند بسیار خطرناک باشد. در مقابل در روش بکارگیری شبیه ساز، کد برنامه مورد بررسی ابتدا در یک محیط شبیه سازی شده اجرا و رفتار آن بررسی می شود و سپس در صورت عدم رویت آلودگی در آن، مجوز اجرای

مستقیم روی رایانه کاربر صادر می شود. هر شبیه ساز باید شامل پنج قابلیت اصلی باشد:

۱. قابلیت شبیه سازی پردازنده
۲. قابلیت شبیه سازی حافظه اصلی
۳. قابلیت شبیه سازی سخت افزار و سیستم عامل
۴. قابلیت کنترل شبیه ساز
۵. قابلیت تحلیل رفتار

❖ **شناسایی**

پس از تشخیص اینکه یک فایل اجرائی آلوده است نوبت به شناخت نوع آلودگی آن و شناسایی بدافزاری است که فایل اجرائی بدان آلوده شده است. مرحله شناسایی می تواند با مرحله ردیابی یکپارچه شود و یا مستقل مطرح شود.

❖ **پاکسازی**

- در روش پاکسازی استاندارد، کد ویروس از داخل برنامه اجرائی حذف می شود و برنامه اجرائی به نحوی اصلاح می شود تا قادر به ادامه کار باشد.

- اضافه کردن موانع رفتاری به فایل آلوده جهت جلوگیری از رفتارهای بدافزاری ضمن اینکه فعالیت عادی آنها متوقف نگردد؛ از دیگر تکنیک های مطرح می باشد.
- پاکسازی می تواند با تکیه بر حفظ جامعیت فایل که براساس یک وضعیت اولیه محاسبه و اعمال می شود؛ صورت پذیرد.
- روش sand-boxing، در این روش کدی به برنامه اضافه می شود تا برنامه آلوده در یک محیط مجازی که کپی اطلاعات واقعی در دسترس وی است اجرا شود و هیچگاه به برنامه مجوز اجرا در محیط واقعی داده نمی شود.

«به طور کلی ضدبدافزاری کامل است که در صورت وجود یک بدافزار حتماً آن را شناسایی کند و در صورتی که فایلی آلوده نیست بعنوان آلوده تشخیص ندهد. »

جدول مقایسه نقاط قوت وضعف روش های شناسایی ضد بدافزار ها

روش	قوت	ضعف
روش بکارگیری پویشگر	شناسایی دقیق	نیاز به پایگاه بروز بدافزارها، حفره نفوذ بدافزار در فاصله زمان تحلیل بدافزار توسط آزمایشگاه بدافزار
روش هوشمندانه	شناسایی بدافزارهای شناس و ناشناس	امکان تشخیص غلط آلودگی، عدم شناسایی بدافزار مورد نظر، عدم قابلیت پاکسازی بجز با استفاده از روشهای هوشمندانه و پیچیده
روش بررسی جامعیت	سرعت بالای شناسایی، شناسایی بدافزارهای شناس و ناشناس	شناسایی تنها پس از آلودگی فایلهای کاربر، عدم قابلیت شناسایی آلودگی فایلهای جدید ایجاد شده یا به صورت قانونی تغییر یافته، اخذ تأیید کاربر برای هر تغییر در فایل، عدم شناسایی بدافزار مورد نظر
روش بکارگیری ناظر و بلوکه کننده	شناسایی بدافزارهای شناس و ناشناس	عدم قابلیت شناسایی و پاکسازی فایلهای آلوده قبل از اجرا، سربار زمان اجرای برنامه ها، امکان تشخیص غلط آلودگی اجرای فایل آلوده در محیط واقعی
روش بکارگیری شبیه ساز	اجرای فایل آلوده در محیط غیرواقعی، شناسایی بدافزارهای شناس و ناشناس	کندی اجرای برنامه ها در محیط شبیه سازی شده، عدم امکان شبیه سازی دقیق برای تشخیص رفتار بدافزارها، عدم قابلیت شناسایی و پاکسازی فایلهای آلوده قبل از اجرا

فصل ۳ - روش های ارزیابی ضدبدافزارها

ارزیابی بمنظور انتخاب یک ضدبدافزار جهت استفاده در سازمان های بزرگ دولتی و خصوصی می باشد و مستلزم آشنایی با معیارهای خاصی است که متفاوت از معیارهایی است که برای تست ضدبدافزار به کار می رود. تست ضدبدافزار به منظور رده بندی و مقایسه آن با ضدبدافزارهای دیگر انجام می شود و نیازمند ایجاد آزمایشگاه تست نرم افزار با طراحی خاص نرم افزارهای ضدبدافزار است.

به علت تغییرات سریعی که در حوزه امنیت و به ویژه در فناوری ضدبدافزار بوجود می آید هرگز نباید انتظار داشت که یک چک لیست، تهیه شده و براساس آن یک یا چند ضدبدافزار انتخاب شود و دیگر تغییری در این چک لیست و نیز نتایج رده بندی آن ایجاد نشود. از طرفی چک لیستی که برای ارزیابی ضدبدافزار استفاده می شود؛ برای هر سازمان و نوع اطلاعات و شبکه های رایانه ای موجود متفاوت از دیگر سازمان ها می باشد و روال ارزیابی جهت تصمیم گیری برای انتخاب یک ضدبدافزار و استفاده از آن در یک سازمان باید حداقل در یک دوره زمانی ۲ الی ۳ ساله مورد بازبینی قرار گیرد.

در ادامه به معیارهای مهمی که برای ارزیابی یک ضدبدافزار و انتخاب یا عدم انتخاب آن برای بکارگیری در سازمانها باید در نظر گرفته شود اشاره شده است؛ هر یک از این معیارها به سه شکل توسط سازمان ها قابل ارزیابی می باشد:

۱. مقایسه ارزیابی های انجام شده در منابع غیرتخصصی با یکدیگر
۲. بررسی نتایج ارزیابی منابع معتبر تخصصی همچون Virus Bulletin یا مجلات تخصصی.
۳. ارزیابی معیارهای مورد نظر توسط خود سازمان.

❖ معیارهای ارزیابی ضدبدافزارها

قابلیت پیکربندی[۱]

قابلیت پیکربندی ضدبدافزار ارتباط مستقیم با کارکرد آن داشته و می تواند یکی از معیارهای مهم در انتخاب یک ضدبدافزار به شمار رود.

[۱] Configurability

قیمت[۱]

قیمت یک ضدبدافزار تنها قیمت ثبت شده روی آن نیست بلکه هزینه های جانبی نصب و بکارگیری آن در سطح شبکه و آموزش کاربران نیز باید مد نظر قرار گیرد. بعنوان مثال آموزش یک ضدبدافزار خارجی برای کاربران ایرانی ممکن است چندین برابر قیمت خود آن برای یک سازمان هزینه داشته باشد. ضمن اینکه میزان هزینه ای که توسط هر سازمان برای امنیت در نظر گرفته می شود متفاوت از سازمانهای دیگر است و در یک کلاس هزینه باید انتخاب بین چند نمونه محدود صورت پذیرد.

سادگی استفاده[۲]

سادگی استفاده از یک ضدبدافزار معیار مهم دیگری است که باید در انتخاب یک ضدبدافزار مد نظر قرار گیرد. همزبانی کاربران با محیط برنامه یکی از بارزترین نمونه هایی است که میتواند سادگی استفاده از ضدبدافزار را ارتقاء بخشد. طراحی واسط کاربری برنامه نیز می تواند تاثیر زیادی روی سهولت

---

[۱] Cost

[۲] Ease of Use

بکارگیری ضدبدافزار و دسترسی سریع به تمام قابلیتهای آن داشته باشد.

کارکرد[۱]

کارکرد یک ضدبدافزار به معنی میزان کامل بودن آن از نظر شناسایی انواع بدافزارها و پاکسازی رایانه های آلوده و نیز قابلیت جلوگیری از ورود و تکثیر بدافزارها می باشد. ارزیابی این معیار کمی مشکل بوده و در این موارد باید نتایج ارزیابی های مراجع رسمی و معتبر با نتایج ارزیابی انجام شده توسط کارشناسان سازمان ترکیب و استفاده شود.

کارآیی[۲]

کارآیی یک ضدبدافزار به معنی کفایت و قابلیت ضدبدافزار از نظر شناسایی انواع بدافزارها بخصوص بدافزارهای حیات وحش می باشد. سرعت شناسایی و پاکسازی بدافزارها معیار مهمی است که می تواند در کارآیی یک ضدبدافزار مد نظر قرار گیرد. قابلیت شناسایی و پاکسازی

---

[۱] Functionality

[۲] Performance

در ضدبدافزارها به دو روش در صورت نیاز[۱] و بیدرنگ[۲] بوده و کارآیی ضدبدافزار در هر دو مورد باید مد نظر قرارگیرد.

- پشتیبانی[۳]

معیاری که بعنوان پشتیبانی برای یک ضدبدافزار مطرح می شود به معنی میزان پاسخگویی و همکاری پرسنل شرکت ارائه دهنده ضدبدافزار می باشد. بطور کلی در دو حوزه زیر نیاز به پشتیبانی توسط شرکت ارائه دهنده ضدبدافزار می باشد:

۱. دانش بکارگیری ضدبدافزار از نظر بایدها، نبایدها و معنی و تفسیر خطاها و رفع مشکلات احتمالی بکارگیری خود نرم افزار
۲. دانش بدافزارها از نظر سؤالات مربوط به رفتار بدافزارها و نتایج حاصل از فعالیت یک بدافزار و گام های تکمیلی لازم برای مقابله با بدافزارها

❖ تست ضد بدافزار

تست ضدبدافزار به منظور بررسی قدرت شناسایی و پاکسازی ضدبدافزار براساس معیارهای استاندارد و مدون انجام می شود.

---

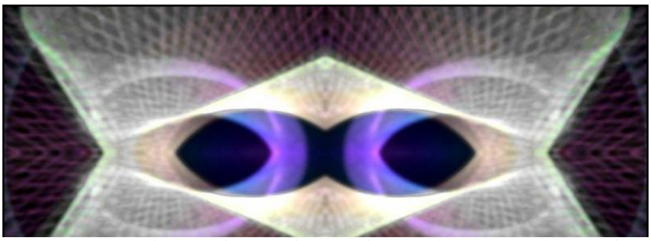
[۱] On Demand

[۲] Realtime

[۳] Support

برای اینکه روال تست ضدبدافزار سندیت داشته باشد، باید قابل تکرار مجدد، با قابلیت بررسی صحت مراحل مختلف و براساس یک متدولوژی معین باشد.

یکی از معروف ترین تستهای ضدبدافزار تست میزان شناسایی بدافزارهای حیات وحش توسط آن است. تست دیگری که در مورد ضدبدافزار انجام می شود فرکانس بروزرسانی آن می باشد؛ در این تست، فاصله بین بروزرسانی های ضدبدافزار با توجه به گسترش بدافزارها و براساس معیارهای زمانی استاندارد سنجیده می شود و ضدبدافزارهای موجود در یک لیست رده بندی قرار می گیرند. تست دیگر میزان هوشمندی یک ضدبدافزار در شناسایی انواع تغییریافته و جدید یک بدافزار شناسایی شده قبلی می باشد؛ در این نوع تست برخلاف تست قبلی از بروزرسانی ضدبدافزار در یک بازه زمانی معین جلوگیری می شود تا میزان توانایی ضدبدافزار در شناسایی بدافزارها بدون بروزرسانی سنجیده شود.



❖ **مراجع استاندارد مقایسه ضدبدافزارها**

یک نرم افزار ضد بدافزار برجسته باید به سادگی قابل نصب و بهره برداری باشد، به طور مؤثر به دنبال ویروس ها بگردد، رفتار آن ها را تشخیص دهد و قادر باشد به خوبی ویروس ها را از بین ببرد؛ همچنین گزارشات قابل فهمی برای هر جستجو ارائه دهد، حمایت ها و پشتیبانی های زیادی برای کمک در دسترس باشد تا براحتی بتوان از قابلیت ها و امکانات آن استفاده نمود.

یک روش مناسب برای انتخاب ضدبدافزار، مراجعه به سازمان ها، مجلات، مقالات و مراجع رسمی که به مقایسه نرم افزارهای ضدبدافزار می پردازند، می باشد. این مراجع بر اساس معیارهایی ضدبدافزارها را رتبه بندی می کنند.

مراجع رسمی اغلب بر اساس دو دسته عمده اطلاعات آماری مانند میزان فروش، رضایت مشتریان، میزان شناسایی ویروس ها و اطلاعات تکنولوژیکی مانند روشهای جستجوی مکاشفه ای، هوشمندی نرم افزارهای ضدویروس، نحوه بروز رسانی،

ضدبدافزارها را رتبه بندی می کنند. در ادامه به برخی از مراجع رسمی مقایسه ضدبدافزار ها در جهان اشاره می شود:

هنگامیکه توسط مرجع رسمی اینترنتی ICSA یک مدرک به محصولی اعطا می شود، نشان دهنده این موضوع می باشد که این محصول موارد زیر را ارائه می دهد:

- کشف ۱۰۰ % ویروسهای لیست شده در حیات وحش
- کشف ۱۰۰ % ویروسهای موجود در لیست متداول برای انجام دنباله تستهای مربوط به ICSA
- کشف ۱۰۰ % از دنباله تست چند ریختی ICSA
- کشف ۹۰ % ویروسهای ماکرو از مجموعه ویروس های ICSA
- کشف ۹۰ % از مجموعه ویروسهای ICSA
- عدم اعلان هشدار نادرست

ملاک دیگر برای ارزیابی ضدبدافزارها، که حتی به طور دقیقتر و سخت تری نسبت به ICSA می باشد، VB۱۰۰ است که برای کسب آن، باید یک محصول ضدبدافزار، در یافتن حتی یک ویروس از ویروسهای موجود در لیست با شکست مواجه نگردد. به عبارت دیگر همه ویروسهای موجود در این لیست را شناسایی و کشف نماید.

هنگام مطالعه نتایج موجود در سایت www.virusbtn.com، باید به ویژگیهای محصولات، بسیار توجه نمود. ممکن است بعضی از محصولاتی که در گذشته عملکرد خوبی را ارائه می داده اند، اخیراً به خوبی گذشته عمل نکرده باشند.

از مرجع رسمی اینترنتی AV-Test.org نیز می توان جهت بررسی و ارزیابی ضدویروسها با مطالعه نتایج حاصل از تستهای انجام شده، استفاده نمود. نتایج تستهای این مرجع نیز قابل دریافت و رؤیت به صورت زنده می باشد. هرچند نتایج ارائه شده این مرجع بسیار جامع و کامل است، ولی ممکن است دنبال کردن این گزارشات به دلیل ساختار پیچیده آن کمی مشکل باشد.

در مرجع رسمی اینترنتی Av-comparative.org نیز مقایسه هایی از نرم افزارهای ضد ویروس وجود دارد. همه محصولاتی که در این سایت قراردارند، بخشی از موتورهای بسیار خوب ضدبدافزار می باشند. به منظور این که محصولی توسط این مرجع تست شود، سازندگان نرم افزارهای ضد ویروس باید شرایط مختلفی داشته باشند. نتایج مقایسه ها نیز برای همه قابل استفاده است.

فصل ٤ - انواع ضدبدافزار

بطور کلی دو نوع ضدبدافزار وجود دارد که عبارتند از:

- ضدبدافزار ایستگاه کاری[۱] (تک کاربره)
- ضدبدافزار شبکه (کارگزار[۲] و دروازه شبکه[۳])

ضدبدافزار ایستگاه کاری صرفاً روی یک رایانه نصب شده و کلیه فعالیت های ردیابی، شناسایی و پاکسازی بصورت مستقل توسط همین ضدبدافزار انجام می شود. این نوع ضدبدافزارها به دو روش Pull و Push قابل بروزرسانی هستند که روش Push بصورت غیر برخط[٤] و روش Pull بصورت خودکار و برخط و از طریق اتصال به اینترنت می باشد ضدبدافزار تک کاربره به نوبه خود می تواند حاوی کارکردهای عمده زیر باشد:

---

[۱] Client

[۲] Server

[۳] Gateway

[٤] Offline

- ضدویروس[۱] : اصلی ترین بخش هر ضدبدافزار بوده و باید شامل یک موتور ردیابی /شناسایی با قابلیت پاکسازی و نیز یک سرویس مقابله با ورود بدافزار به رایانه باشد . این بخش برخلاف نام آن نه تنها با انواع ویروس بلکه با انواع بدافزار و از جمله انواع ویروس، کرم مقابله کرده و معمولاً براساس فناوری های مختلف و پیشرفته، شناسایی و پاکسازی آنها را انجام می دهد .
- ضدجاسوس افزار[۲] : جاسوس افزار با قرارگیری در رایانه کاربر اقدام به جمع آوری اطلاعات مالی و خصوصی وی نموده و باعث ایجاد مشکلاتی برای کاربر می شود . این بخش در برخی از ضدبدافزارها موجود بوده و عموماً مبتنی بر الگوهای شناخته شده انواع جاسوس افزار می باشد . با شناسایی و حذف جاسوس افزارها ضمن رفع خطرات احتمالی سرعت محاسباتی رایانه و کارایی سیستم عامل افزایش می یابد .

---

[۱] Antivirus

[۲] AntiSpyware

- دیواره آتش میزبان[۱] : دیواره آتش میزبان با پوشش مناسب ضعف های موجود در پروتکلهای شبکه، راه های نفوذ هکرها به رایانه کاربر را مسدود نموده و براساس سیاست امنیتی تعریف شده تمامی اطلاعات ارسالی و دریافتی به / از شبکه را تحت کنترل می گیرد . امروزه با توجه به اینکه اکثر آلودگیهای بدافزاری رایانه ها از ناحیه کرم ها بوده و گسترش کرم ها بعلت وجود نقصهای امنیتی در ارتباطات شبکه رایانه ها می باشد، لزوم وجود دیواره آتش میزبان به صورت یکپارچه با ضدبدافزار، بیش از پیش نمایان می گردد .
- سیستم جلوگیری از نفوذ به میزبان: نرم افزار HIPS[۲]، نرم افزاری مبتنی بر رفتارشناسی فعالیت های تحت شبکه در دو مسیر ورودی و خروجی رایانه واقع در شبکه و اینترنت بوده و عامل مهمی برای مقابله با تهدیدات موجود از ناحیه هکرها براساس بسترهای ایجادشده با فعالیت بدافزارها در رایانه کاربر می باشد . از آنجا که با وجود اعمال تمامی کنترلهای امنیتی احتمال آن می رود که یک

---

[۱] Personal Firewall

[۲] Host Intrusion Prevention System

بدافزار وارد رایانه کاربر شده و بستر نفوذ را برای یک هکر فراهم آورد، در چنین مواقعی با بهره گیری از سیستم HIPS عرصه برای نفوذ هکرها تنگ و در بسیاری از موارد غیر ممکن می گردد .

- کنترل کننده دسترسی به شبکه[۱]: این بخش از آخرین فناوری های مطرح در ضدبدافزارها بوده و کاربرد اصلی آن در اعمال سیاست های امنیتی سازمانی[۲] روی رایانه کاربران و قطع ارتباط رایانه های آلوده به بدافزارها با شبکه برای جلوگیری از وقوع حملاتDoS یا DDoS و کندی حاصله در شبکه های رایانه ای می باشد . در چنین مواقعی رایانه های آلوده سریعاً شناسایی و بدینوسیله از گسترش دامنه فعالیت بدافزار در سطح شبکه جلوگیری می گردد .

ضدبدافزار شبکه برخلاف نوع ایستگاه کاری روی تمامی رایانه های شبکه نصب شده و معمولاً یک رایانه بعنوان کارگزار ضدبدافزار و سامانه کنترل مرکزی ضدبدافزار تعیین می شود. این نوع ضدبدافزارها در شبکه های رایانه ای با توجه به اینکه دامنه

---

[۱] Network Access Control

[۲] Security Enforcement

فعالیت آنها کل شبکه را در بر می گیرد، از قدرت بیشتری برای مقابله با حملات بدافزارها برخوردار می باشند.

ضدبدافزار شبکه، خود حاوی بخشهای زیر می باشد:

- بخش های حفاظت بدافزاری شروع بکار[۱]، بلادرنگ[۲]، زمان نیاز[۳] و اینترنت[۴]: این ۴ بخش وظیفه ردیابی، شناسایی و پاکسازی بدافزارها را در زمان راه اندازی سیستم، لحظه ورود بدافزار به رایانه، بنا به درخواست کاربر، و یا به هنگام کار در اینترنت را بر عهده دارند .
- بخش مدیریت مرکزی[۵]: این بخش معمولاً روی کارگزار ضدبدافزار نصب شده و وظیفه پیکربندی ، گزارشگیری و نظارت بر بروزرسانی و آلودگی رایانه های شبکه را برعهده دارد . این بخش در ضدبدافزار شبکه اصلی ترین بخش محسوب می شود و وظیفه اصلی آن ایجاد هماهنگی بین رایانه های شبکه برای مقابله با بدافزارها می باشد .

---

[۱] Start-up Protection

[۲] Realtime Protection

[۳] On-Demand Protection

[۴] Internet Protection

[۵] Centralized Management

- بخش بروزرسانی تحت شبکه و نصب در شبکه: این بخش با مدیریت کارگزار شبکه قابلیت نصب ضدبدافزار روی رایانه های کاربران و بروزرسانی آنها را از راه دور و از طریق کارگزار شبکه فراهم می آورد .