دانشکده مهندسی

گروه کامپیوتر-گرایش نرم‌افزار

ارائه کتبی درس شیوه پژوهش و ارائه

بدافزارها

استاد: دکتر سمانه شیبانی

نگارنده: زهرا میرزایی

بهار ۹۷

چکیده

بدافزار به یک برنامه مخرب گفته می‌شود که برای کاربران کامپیوتری مضر می‌باشد بدافزارها عملکردهای متفاوتی را مثل سرقت اطلاعات، تغییر یا حذف داده‌ها، کدگذاری ناخواسته روی داده‌ها و یا مانیتور کردن فعالیت‌های کاربر بدون مجوز او را انجام می‌دهند و انواع مختلفی دارند که هر کدام از آن‌ها دارای صفات و ویژگی‌های خاص خود می‌باشند که معروف‌ترین آنها ویروس‌ها هستند. نویسندگان بدافزار از روش‌های متفاوتی برای انتشار و تکثیر بدافزار خود در شبکه‌ها و یا دستگاه‌های رایانه‌ای استفاده می‌کنندکه رایج‌ترین راه انتشار اینترنت می‌باشد با توجه به نقش کاربردی سیستم‌های عامل در جوامع، شرکت‌های بزرگ و ادارات و... نگهداری اطلاعاتی درآن‌ها که حذف و یا انتشار آن‌ها موجب آسیب‌های جدی به این مجموعه‌ها میشود امنیت سیستم‌ها و اهمیت شناخت بدافزارها، راه‌های جلوگیری از نفوذ آن‌ها و در آخر راه‌های مقابله با آن‌ها مطرح میشود.

کلمات کلیدی

بدافزار، ویروس، امنیت، آنتی ویروس، تروجان، کرم‌اینترنتی

فهرست مطالب

مقدمه ۱

بدافزار و مقاصد آن ۲

انواع بدافزار و نحوه انتشار آن‌ها ۴

راه‌های پیشگیری از نفوذ بدافزارها ۱۴

معرفی بهترین آنتی‌ویروس‌ها ۱۷

جمع‌بندی ۲۲

مراجع ۲۳

مقدمه

به تازگی جنگ جدیدی بین موسسات و انجمن‌های امنیتی و توسعه‌دهندگان نرم‌افزارهای مخرب درگرفته است. متخصصین امنیتی از همه روش‌ها و تکنیک‌های ممکن برای حذف و متوقف کردن تهدیدات بهره می‌برند در حالی‌که توسعه‌دهندگان بدافزارها[۱] از روش‌های جدید برای دور زدن ویژگی‌های امنیتی استفاده می‌کنند. همه ساله تعداد بسیار زیادی از بدافزارها با قدرت انتشار و استراتژی‌های مختلف ساخته می‌شوند. برای این‌که بتوان در این جنگ به نتیجه مطلوب رسید و سازمان خود را از این آسیب‌ها و تهدیدات در امان نگه‌داشت باید اطلاعات کامل‌تری در خصوص بدافزارها، انواع آن‌ها و از همه مهم‌تر نحوه انتشار آن‌ها کسب نمود.

یکی از رایج‌ترین راه انتشار و انتقال بدافزارها، فرآیند دانلود آن از اینترنت است. در برخی موارد بدافزارها فقط اقدام به تخریب نمی‌کنند بلکه می‌توانند عملکرد سیستم را تحت تاثیر خود قرار دهند و بار اضافی به سیستم تحمیل کنند. در موارد جاسوسی بدافزارها خود را پنهان می‌کنند به طوریکه حتی آنتی‌ویروس‌ها[۲] نیز قادر به تشخیص آن‌ها نیستند و این بدافزارها اطلاعات ارزشمند و حیاتی از قربانی خود را به مبدا ارسال می‌کنند.

با توجه به چالش مهمی که امروزه گریبان‌گیر دولت‌ها، سازمان‌ها، شرکت‌ها و افراد شده‌است در این‌جا سعی شده است تا با نگاهی دقیق به مشکل بدفزارها و نحوه انتشار آن‌ها، راه‌های موثر مقابله با این تهدید ارائه گردد.

[۱] Malware(malicious software)
[۲] Antivirus

بدافزار و مقاصد آن

برنامه‌های رایانه‌ای هستند؛ به علت آن‌که معمولاً کاربر را آزار می‌دهند یا خسارتی بوجود می‌آورند، به این نام مشهورند. برخی از آنان فقط کاربر را می‌آزارند. مثلاً وی را مجبور به انجام کاری تکراری می‌کنند. اما برخی دیگر سیستم رایانه‌ای و داده‌های آن را هدف قرار می‌دهند که ممکن است خساراتی به بار آورند. در عین حال ممکن است هدف آن سخت‌افزار سیستم کاربر باشد.

یک نرم‌افزار بر پایه نیت سازنده آن به عنوان یک بدافزار شناخته می‌شود. در قانون گاه بدافزار را به عنوان یک آلودگی رایانه‌ای می‌نامند.دستاورد های مقدماتی که توسط سیمنتک[۳] در سال ۲۰۰۸ منتشر شد، بیان می‌کند که میزان کدهای آزاردهنده و دیگر برنامه‌های ناخواسته از شمار نرم‌افزارهای قانونی، ممکن است افزون باشد [۱]. همچنین گفته شده است: «تعداد بدافزارهای تولید شده در سال ۲۰۰۷ به اندازه مجموع ۲۰ سال قبل بوده است.» [۲] مهمترین پل ارتباطی بدافزار ها از تولید کنندگان انها به کاربران از طریق اینترنت است [۳].

در ۲۹ مارس ۲۰۱۰ شرکت سیمنتک شهر شاوشینگ چین را به عنوان پایتخت بدافزار در دنیا معرفی کرد. مایکروسافت در می ۲۰۱۱ گزارش داد که از هر ۱۴ دانلود در اینترنت یکی شامل بدافزار است. به ویژه شبکه های اجتماعی و فیسبوک در حال مشاهده ی افزایش تاکتیک های جدید برای ضربه زدن به رایانه‌ها هستند [۴].

بدافزار یا یک نرم افزار معیوب یعنی نرم افزاری قانونی ولی شامل اشکالات مضر، تفاوت دارد. گاه بدافزار به صورت یک نرم افزار سالم و صحیح طراحی میشود و حتی ممکن است از یک سایت رسمی بیاید؛ بنابراین برخی از برنامه های امنیتی مانند مک‌آفی [۴]ممکن است بدافزار را یک برنامه «به طور بالقوه ناخواسته» بنامد.

[۳] Symantec Corporation: بزرگترین شرکت تولیدکننده نرم‌افزارهای امنیتی

[۴] McAfee: یک شرکت در زمینه امنیت رایانه است

بسیاری از برنامه‌های آلوده‌کننده اولیه، از جمله اولین کرم اینترنتی[۵] و تعدادی از ویروس‌های[۶] سیستم عامل داس[۷]، به قصد آزمایش یا سرگرمی نوشته شدند. آن‌ها عموماً به مقاصد بی‌ضرر یا فقط به قصد آزار بودند، تا اینکه بخواهند خسارات جدی به سیستم‌های رایانه وارد کنند. در برخی موارد سازنده نمی‌توانست تشخیص دهد که چقدر کارش می‌تواند مضر باشد.

برنامه‌نویسان جوان وقتی درباره ویروس‌ها و ترفندهایش می‌آموختند، تنها به منظور تمرین یا به قصد اینکه ببینند چقد شیوع پیدا می‌کند، آن‌ها را می‌نوشتند. در سال۱۹۹۹ ویروس‌های شایعی مانند ویروس ملیسا[۸] و ویروس دیوید[۹] تنها به قصد سرگرمی نوشته شده بودند. اولین ویروس تلفن‌همراه در سال۲۰۰۴ با نام ویروس کابیر[۱۰] بر روی تلفن همراه منتشر شد.

با این حال مقاصد سوء به منظور خرابکاری را می‌توان در برنامه‌هایی یافت که برای ایجاد آسیب به سیستم رایانه‌ای یا از دست رفتن اطلاعات، طراحی شده‌اند. بسیاری از ویروس‌های سیستم عامل داس، با این هدف طراحی شدند تا فایل‌های موجود در یک دیسک سخت را نابود کنند یا فایل‌های سیستمی را با نوشتن اطلاعات نادرست بر روی آن‌ها دچار اختلال کنند.

از زمان گسترش دسترسی به اینترنت پر سرعت، بدافزارهایی به منظور ایجاد سود طراحی شده‌اند. به عنوان مثال از سال ۲۰۰۳، اغلب ویروس‌ها و کرم‌های رایانه‌ای، طراحی شدند تا کنترل رایانه‌های کاربران را به منظور بهره‌گیری در بازار سیاه به کار گیرند [۵].

---

[۵] Worm
[۶] Virus
[۷] DOS
[۸] Melissa
[۹] David
[۱۰] Cabir

انواع بدافزارها

با توجه به افزایش تهدیدات از سوی بدافزارها، آشنایی با انواع آن‌ها می‌تواند در شناخت و مقابله با آن‌ها بسیار موثر باشد. ویروس رایانه‌ای تنها نوعی بدافزار است که خود را باز تولید می‌کند، اما اغلب کاربران رایانه به اشتباه به همه بدافزارها ویروس گویند.

از انواع بدافزارها می‌توان به ویروس‌ها، کرم‌ها، اسب‌های تروآ[۱۱]، جاسوس‌افزارها[۱۲]، آگهی‌افزارها[۱۳]، روت‌کیت‌ها[۱۴]، و... اشاره کرد که در ادامه به تعریفی به همراه ویژگی‌های هرکدام از آنها می‌پردازیم:

ویروس رایانه‌ای

ویروس، یک نوع از بدافزار است که در اغلب مواقع بدون اطلاع کاربر اجرا شده و تلاش می‌کند خودش را در یک کد اجرایی دیگر کپی کند. وقتی موفق به انجام این کار شد، کد جدید، آلوده نامیده می‌شود. کد آلوده وقتی اجرا شود، به نوبه خود کد دیگری را می‌تواند آلوده کند. این عمل تولید مثل یا کپی‌سازی از خود بر روی یک کد اجرایی موجود، ویژگی کلیدی در تعریف یک ویروس است [۶].

معمولاً کاربران رایانه به ویژه آنهایی که اطلاعات تخصصی کمتری درباره رایانه دارند، ویروس‌ها را برنامه‌هایی هوشمند و خطرناک می‌دانند که خود به خود اجرا و تکثیر شده و اثرات تخریبی زیادی دارند که باعث از دست رفتن اطلاعات و گاه خراب شدن کامپیوتر می‌گردند در حالی‌که طبق آمار تنها پنج درصد ویروس‌ها دارای اثرات تخریبی بوده و بقیه صرفاً تکثیر می‌شوند؛ بنابراین ویروس‌های رایانه‌ای از جنس برنامه‌های معمولی هستند که توسط ویروس‌نویسان نوشته شده و سپس به طور ناگهانی توسط یک فایل اجرایی یا جا گرفتن در ناحیه سیستمی دیسک، فایل‌ها یا کامپیوترهای دیگر را آلوده می‌کنند. در این حال پس از اجرای فایل آلوده به ویروس یا دسترسی

[۱۱] Trojan horse
[۱۲] Spyware
[۱۳] Adware
[۱۴] Rootkit

به یک دیسک آلوده توسط کاربر دوم، ویروس به صورت مخفی نسخه‌ای از خودش را تولید کرده و به برنامه‌های دیگر می‌چسباند و به این ترتیب داستان زندگی ویروس آغاز می‌شود و هر یک از برنامه‌ها یا دیسک‌های حاوی ویروس، پس از انتقال به رایانه‌های دیگر باعث تکثیر نسخه‌هایی از ویروس و آلوده شدن دیگر فایل‌ها و دیسک‌ها می‌شوند؛ لذا پس از اندک زمانی در رایانه‌های موجود در یک کشور یا حتی در سراسر دنیا منتشر می‌شوند. از آنجا که ویروس‌ها به طور مخفیانه عمل می‌کنند، تا زمانی که کشف نشده و امکان پاکسازی آنها فراهم نگردیده باشد، برنامه‌های بسیاری را آلوده می‌کنند و از این رو یافتن سازنده یا منشأ اصلی ویروس مشکل است.

ویروس هم مانند هر برنامه رایانه‌ای نیاز به محلی برای ذخیره خود دارد؛ ولی این محل باید به گونه‌ای باشد که ویروس‌ها را به وصول اهداف خود نزدیک‌تر کند. اکثر ویروس‌ها به طور انگل‌وار به فایل‌های اجرایی می‌چسبند و آنها را آلوده می‌کنند. در ذیل فهرست پسوندهای رایج فایل‌های اجرایی ارائه شده‌است و اکثر نرم‌افزارهای ضد ویروس در حالت عادی (بدون تنظیمات خاص) این فایل‌ها را ویروس‌یابی می‌کنند (البته در برخی برنامه‌های ضد ویروس ممکن است برخی پسوندها حذف یا اضافه شوند) :

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

همانطور که گفتیم یکی از اصلی‌ترین میزبان‌های ویروس، فایل‌های اجرایی هستند. از طرف دیگر برخی ویروس‌ها نیز از سکتور راه‌انداز[۱۵] و جدول بخش‌بندی دیسک[۱۶] یا به عنوان میزبان استفاده می‌کنند. سکتور راه‌انداز واحد راه‌اندازی سیستم‌عامل است که در سکتور شماره صفر دیسکت فلاپی یا درایوهای منطقی یک دیسک سخت قرار دارد و جدول بخش‌بندی شامل اطلاعات تقسیم‌بندی دیسک سخت می‌باشد که آن نیز در سکتور شماره صفر دیسک سخت قرار دارد. اینگونه ویروس‌ها با قرار گرفتن در یکی از این دو محل، هنگام راه‌اندازی رایانه، اجرا شده

[۱۵] Boot Sector
[۱۶] Partition Table

و در حافظه سیستم مقیم می‌شوند و تا زمان خاموش کردن رایانه یا راه‌اندازی دوباره، همان‌جا مانده و فلاپی‌ها یا دیسک‌های سخت دیگر را آلوده می‌کنند.

همان‌طور که گفته شد تنها پنج درصد از ویروس‌ها دارای اثرات تخریبی هستند و بقیه صرفاً تکثیر می‌شوند. با توجه به این مطلب این پرسش مطرح است که چرا ویروس‌ها به عنوان یک معضل شناخته می‌شوند و باید با آنها مبارزه کرد؟ پاسخ به این پرسش در موارد زیر خلاصه گردیده‌است:

۱ - بسیاری از ویروس‌ها دارای اثراتی هستند که هرچند تخریبی نمی‌باشد ولی می‌تواند برای کاربر ایجاد مزاحمت کند. مثلاً ممکن است پیغامی نمایش دهد، باعث ریزش حروف صفحه نمایش به پایین شود یا اینکه یک آهنگ پخش نماید. علاوه بر این برخی از ویروس‌ها به علت اشکالات نرم‌افزاری که ناشی از عدم دقت ویروس‌نویس می‌باشد، ممکن است دارای اثراتی غیرقابل پیش‌بینی باشند که گاهی این اثرات می‌توانند تخریبی نیز باشند. از دیدگاه کاربر اهمیتی ندارد که خسارت ایجاد شده بوسیله یک ویروس، یک کار عمدی پیش‌بینی شده توسط نویسنده ویروس بوده باشد یا یک اشتباه برنامه‌نویسی.

۲ - برخی از ویروس‌ها در حافظه رایانه مقیم شده و از این طریق عملیات تکثیر خود را انجام می‌دهند. این عمل ممکن است به گونه‌ای باشد که جایی برای اجرای برنامه‌های دیگر نماند یا باعث ایجاد تأخیر یا وقفه در حین عملیات سیستم اعم از اجرای برنامه‌ها یا راه‌اندازی رایانه گردد.

۳ - ویروس‌ها و برنامه‌های مخرب زیادی وجود دارند که اقدام به سرقت اطلاعات و کلمات عبور کاربر می‌نمایند. بعضی از اینگونه برنامه‌ها با مقیم شدن در حافظه از عباراتی که توسط شما نوشته می‌شود گزارش گرفته و پس از اتصال رایانه شما به اینترنت این اطلاعات را برای مقصد خاصی ارسال می‌کنند. گیرنده این اطلاعات می‌تواند به راحتی از آنها سوء استفاده‌های مختلفی نماید.

علاوه بر همه اینها هیچ ویروسی کاملاً بی‌ضرر نیست و در خوشبینانه‌ترین حالت، آنها وقت شما، وقت پردازنده و فضای دیسک شما را تلف می‌کنند [۷].

کرم رایانه‌ای

کرم رایانه به برنامه‌ای گفته می‌شودکه توانایی بازتولید خود را داراست، و با استفاده از شبکه کپی‌های خود را به دیگر رایانه‌های موجود در شبکه می‌فرستد. برخلاف ویروس کرم‌ها خود را به برنامه‌های دیگر نمی‌چسباند. همچنین کرم‌ها عموماً با اشغال پهنای باند به شبکه آسیب می‌رسانند در حالی که ویروس‌ها در بیشتر اوقات باعث خرابی برنامه‌های موجود در کامپیوتر آلوده و از دست رفتن اطلاعات موجود در آن می‌شوند. هدف کرم‌ها معمولاً استفاده از منابع می‌باشد و می‌تواند در دسترسی شما به منابع تأخیر بیاندازد [۸].

کرم در برخی از خصوصیات با ویروس مشترک است. مهمترین ویژگی مشترک آن‌ها این است که کرم‌ها نیز خود-همانندساز هستند، اما تولید مثل آن‌ها از دو جهت متفاوت است. اول اینکه، کرم‌ها مستقل و متکی به خود هستند، و محتاج به کد اجرایی دیگری نیستند. دوم، کرم‌ها از طریق شبکه‌ها، از ماشینی به ماشین دیگر منتقل و توزیع می‌شوند [۹].

اسب‌های تروآ (تروجان)

تروجان، برنامه مخربی است که به صورت یک نرم افزار جالب به نظر می‌رسد .بر عکس ویروس‌ها، تروجان‌ها تکثیر نمی شوند؛ ولی به اندازهٔ ویروس ها مخرب هستند. یکی از انواع تروجان‌ها، برنامه‌ای است که ادعا می‌کند، رایانه شما را از شر ویروس‌ها نجات می‌دهد؛ اما در حقیقت ویروس‌ها را با سیستم شما آشنا و به آنها معرفی می‌کنند . لغت تروجان برگرفته از افسانهٔ یونانی جنگ تروجان است. در این داستان یونانی‌ها از طریق هدیه دادن اسب چوبی بزرگی به دشمنانشان، تعدادی سرباز به قلعهٔ آن‌ها فرستادند؛ سپس این سربازها از داخل اسب بیرون آمده و درب قلعه را باز کردند تا دیگر افراد به داخل قلعه بیایند و قلعه را فتح کنند. این مثال دقیقاً عملی است که تروجان با کامپیوتر شما انجام می‌دهد. تروجان ابتدا به قسمت های مختلف نفوذ می‌کند؛ سپس، راهی برای آسیب به آنها پیدا خواهد کرد [۱۰].

به بیان دیگر، یک اسب تروآ برنامه‌ای است که کاربر را ترغیب می‌کند تا اجرایش کند در حالی که قابلیت خرابکاریش را مخفی می‌کند. آثار منفی ممکن است بلافاصله آغاز شوند و حتی می‌توانند منجر به آثار نامطلوب فراوانی گردند. از جمله حذف کردن فایل‌های کاربر یا نصب نرم‌افزارهای خرابکار یا نامطلوب بیشتر. اسب‌های تروآ برای آغازسازی شیوع یک کرم استفاده می‌شوند.

تروجان‌ها ممکن است به وسیله دانلود نا خواسته یا نصب بازیهای آنلاین یا برنامه‌های تحت شبکه یا به رایانه هدف دسترسی داشته باشند. عملیات‌هایی که می‌تواند توسط یک هکر بر روی یک سیستم رایانه‌ی مورد هدف اجرا شود شامل:

- استفاده از دستگاه به عنوان بخشی از بات نت (به عنوان مثال برای اجرای خودکار اسپم یا حمله محروم سازی از سرویس)
- از کار افتادن رایانه
- صفحه آبی مرگ
- سرقت پول الکترونیکی
- سرقت اطلاعات (به عنوان مثال بازیابی کلمه عبور یا اطلاعات کارت اعتباری)
- نصب و راه‌اندازی نرم‌افزار، از جمله بدافزارهای شخص ثالث و باج افزار[۱۷]
- دانلود یا آپلود فایل‌ها بر روی کامپیوتر کاربر
- اصلاح یا حذف فایل
- کی لاگر[۱۸]
- تماشای صفحه نمایش کاربر

[۱۷] Ransomware
[۱۸] Keylogger

- مشاهده وب کم کاربر
- کنترل سیستم رایانه‌ای از راه دور
- رمزنگاری فایل
- انحراف اطلاعات
- تغییرات رجیستری
- CPUو GPU بیش از حد
- لینک کردن رایانه به بات نت
- با استفاده از رایانه آلوده به عنوان پروکسی برای فعالیت‌های غیرقانونی و حمله به رایانه‌های دیگر
- نصب خود به خود برنامه‌ها

شرکت امنیتی پاندا در گزارش تازه خود که به بررسی وضع امنیت سایبر در سال ۲۰۱۱ اختصاص دارد، تصویر کاملی از تحولات مرتبط با امنیت در فضای مجازی ارایه کرده است. نکته مهمی که در این گزارش به چشم می‌خورد، افزایش دامنه فعالیت تروجان‌های مخرب است، به گونه‌ای که از میان انواع بدافزارها شامل ویروس، کرم، تروجان و... این تروجان‌های نفوذگر هستند که بخش عمده تهدیدات سایبری را به خود اختصاص داده‌اند.

در بخشی از این گزارش که به بررسی آلودگی‌های بدافزاری اختصاص دارد، آمار مفصلی درباره دسته‌بندی تهدیدات سایبری ارایه شده است. بر همین اساس در حالی‌که در سال ۲۰۰۹، ۶۰ درصد از کل بدافزارها را تروجان‌ها تشکیل می‌دادند، این رقم در سال ۲۰۱۰ به ۵۶ درصد کاهش یافته، اما در سال ۲۰۱۱ با رشدی حیرت‌انگیز به ۷۳درصد رسیده است [۱۱].

روش های نفوذ تروجان‌ها عبارتند از:

۱. دانلود کردن نرم‌افزار: شما نرم‌افزاری را دانلود می‌کنید و تروجان در پس این نرم‌افزار پنهان شده و وارد سیستم شما می‌شود.

۲. سایت‌های مخرب: وقتی شما وارد سایتی می‌شوید سایت یک برنامه را روی سیستم شما اجرا می‌کند و تروجان را وارد سیستم شما می‌کند.

۳. ایمیل: احتمال دارد همراه با ایمیل فایلی باشد که اگر شما آن را باز کنید تروجان وارد سیستم شما می‌شود.

۴. استفاده از نقص نرم‌افزارها: تروجان از طریق نقص‌هایی که در نرم‌افزارهایی مثل مرورگر وجود دارد وارد سیستم شما می‌شود.

۵. از طریق دیسکت‌ها

هر عملی که بدون مداخله کاربر انجام شود، نشانه‌ای از حمله تروجان است، برخی از علائم تروجان عبارتند از:

- فایل‌هایی بصورت خودکار از پرینتر، پرینت گرفته می‌شوند.
- کلیدهای راست و چپ ماوس، بصورت معکوس کار می‌کنند.
- نشانگر ماوس، ناپدید یا جابجا می‌شود.
- شرکت ISP به کاربر اعتراض می‌کند که کامپیوترش عملیات IP Scanning انجام می‌دهد.
- رمزهای حساب‌های کاربری تغییر می‌کند یا اشخاص دیگری می‌توانند به حساب‌های کاربری دسترسی داشته‌باشند.
- مودم بصورت خود به خود به اینترنت متصل می‌شود.
- سرعت انتقال داده و پهناباند اینترنت شخص افت پیدا می‌کند [۱۲].

جاسوس افزار

جاسوس‌افزارها بدافزارهایی هستند که بر روی رایانه کاربر نصب می‌شوند و بدون اطلاع وی، اطلاعات مختلف در مورد او را جمع‌آوری می‌کنند. اکثر جاسوس‌افزارها از دید کاربرها مخفی می‌مانند و تشخیص و پیدا کردن آن‌ها در اغلب موارد مشکل است.

در یک تقسیم بندی کلی نرم‌افزارهای جاسوسی را می‌توان به دو دسته تقسیم کرد:

۱-نرم‌افزارهای جاسوسی خانگی: نرم‌افزاری که معمولاً توسط صاحبان رایانه‌ها به منظورآگاهی یافتن از تأثیرات اینترنت بر شبکه‌های رایانه‌ای خودشان خریداری و نصب می‌گردد. مدیران از این نرم‌افزار برای آگاهی از فعالیت‌های کارمندان استفاده می‌کنند. بعضی افراد هم برای اطلاع از فعالیت‌های سایر اعضای خانواده این روش را به کار می‌برند. مانند مشاهده محتویات اتاق‌های گفتگو توسط والدینی که فرزندانشان در آن‌ها شرکت می‌کنند. همچنین این نوع جاسوس افزار می‌تواند توسط یک شخص ثالث بدون آگاهی صاحب رایانه روی سیستم وی نصب شود و اطلاعات شخصی وی را جمع‌آوری کند.

۲-نرم‌افزارهای جاسوسی تجاری: نرم‌افزاری است که شرکت‌ها برای تعقیب فعالیت‌های کاربران در اینترنت استفاده می‌کنند. این شرکت‌ها که وظیفه نصب جاسوس افزار روی سیستم‌های رایانه‌ای را دارند اغلب اطلاعات حاصل را به بازاریابان می‌فروشند و آن‌ها کاربر را با تبلیغات خاص که با علائق وی مطابقت دارد و برایش جذاب است مورد هدف قرارمی دهند.

راه‌های نفوذ جاسوس افزارها:

- پنجره‌های پاپ آپ[۱۹]

[۱۹] Pop up

پنجره‌های کوچکی که به هنگام بازدید از سایت در برابر کاربر ظاهر می‌شوند و حاوی پیام‌های مختلفی برای فریب اشخاص می‌باشند. در این پنجره‌ها اغلب دکمه‌های مختلفی مانند قبول، لغو، بستن و... وجود دارد ولی هیچ‌کدام از آن‌ها کار اصلی خود را انجام نمی‌دهند و با فشردن هر کدام از این دکمه‌ها جاسوس افزار روی سیستم نصب می‌شود.

- نرم‌افزارهای ضد جاسوس افزار

بعضی نرم‌افزارهای ضدجاسوسی به جای از بین بردن جاسوس افزار آن را روی سیستم نصب می‌کنند. از برنامه‌های مطمئن و معروف برای بالا بردن امنیت سیستم خود استفاده کنید.

- برنامه‌های رایگان اینترنتی

امروزه بسیاری از کاربران اینترنت بنا بر نیاز خود برنامه‌هایی را که به صورت رایگان روی اینترنت قرار گرفته دانلود و نصب می‌کنند .اغلب صاحبان این برنامه‌ها در ازای دریافت مبلغی یا بااهداف تجاری دیگر کد جاسوس افزار را در برنامه خود قرار می‌دهند و به هنگام نصب آن نرم‌افزار جاسوس افزار نیز روی سیستم رایانه‌ای قرار گرفته و شروع به کار می‌کند

- سی دی‌ها و فلش‌ها

حافظه‌های جانبی قابل حمل مانند سی دی و فلش به این علت که بین سیستم‌های زیادی جا به جا می‌شوند حاوی برنامه‌های مخرب هستند .سوء استفاده از ضعف امنیتی اینترنت اکسپلورر بعضی از طراحان برنامه‌های مخرب که با ضعف‌های امنیتی اینترنت اکسپلورر آشنا باشند می‌توانند در کد صفحه وب خود دستورهایی قرار دهند که به هنگام باز کردن آن صفحه با اینترنت اکسپلورر جاسوس افزار روی رایانه نصب شود

- ویروس‌ها

برخی ویروس‌ها حاوی کدهایی برای نصب جاسوس افزارهستند.

تشخیص آلوده بودن یک کامپیوتر به جاسوس افزار کار سختی نیست. سیستم آلوده نشانه‌های ساده‌ای دارد از جمله:

- ظاهر شدن مداوم پنجره‌های پاپ آپ
- تغییر آدرس توسط مرورگر
- ایجاد آیکون‌های جدید روی صفحه نمایش
- عدم کارایی بعضی کلیدهای صفحه کلید
- عملکرد کند کامپیوتر [۱۳]

آگهی‌افزار

این بدافزار جهت اهداف تبلیغاتی و نشان دادن پیام‌ها و آگهی‌های تبلیغاتی در رایانه افراد طراحی‌شده است. این نوع نرم‌افزارها عموماً خطر خاصی برای رایانه ایجاد نمی‌کنند اما برخی از آن‌ها سرعت سیستم را کاهش داده و در کار نرم‌افزارهای امنیتی اختلال ایجاد می‌کنند.

نحوه کار آگهی‌افزارها بدین‌گونه است که در پوشش یک نرم‌افزار به ظاهر سالم با اجازه کاربر بر روی سیستم نصب می‌شوند سپس بدون آنکه کاربر متوجه شود در هنگام اتصال به اینترنت به سرورهای خاصی متصل شده و پیام‌های تبلیغاتی را به صورت بالاپر بر روی صفحه رایانه نمایش می‌دهند. برخی ازآگهی‌افزارها با استفاده از جاسوس‌افزارهایی که به همراه دارند اطلاعات و علاقمندی‌های کاربر را جمع‌آوری کرده و تبلیغات ارسالی بر روی سیستم آلوده را بر همان مبنا انتخاب و ارسال می‌کنند. کار دیگری که این نرم‌افزارها انجام می‌دهند بارگیری سایر آگهی‌افزارها و جاسوس‌افزارها بر روی سیستم آلوده می‌باشد که این عمل منجر به کاهش سرعت اینترنت می‌گردد [۱۴].

روت‌کیت

روت‌کیت بدافزارهایی هستند که اغلب، آن‌ها را به خودی خود نمی‌توان مخرب یا خطرناک دانست، بلکه قرار گرفتن آن‌ها در کنار ویروس‌ها یا کرم‌های اینترنتی یا نوع استفاده از آن‌هاست که به آنان ماهیتی خطرناک می‌بخشد. به عنوان یک تعریف می‌توان گفت که روت‌کیت ابزاری نرم‌افزاری است که بوسیله آن این امکان وجود دارد تا فایل، پروسه یا کلیدی خاص در رجیستری را پنهان نمود. روت‌کیت‌ها اغلب در سطح سیستم‌عامل فعالیت کرده و با تغییراتی که در سیستم‌عامل یا منابع آن انجام می‌دهند، به مقاصد خود دست پیدا می‌کنند. به علت قابلیت پنهان‌سازی قوی این‌گونه برنامه‌ها، شناسایی آن‌ها یا برنامه‌هایی که توسط آن‌ها پنهان گردیده اغلب مشکل بوده و این امر می‌تواند مشکلاتی را برای کاربران بوجود آورد. به عنوان مثال برخی از روت‌کیت‌ها پس از اجرا بر روی سیستم کاربر، کرمی را از دل خود بیرون آورده و بر روی سیستم کاربر اجرا می‌نمایند. سپس با قابلیت‌های خاص خود آن را از دید کاربر مخفی می‌کنند و کرم مزبور به راحتی به فعالیت‌های مخرب خود به دور از چشم کاربر ادامه می‌دهد.

راه‌های پیشگیری از نفوذ بدافزارها

بهترین راه که به کاربران کمک میکند از نفوذ بدافزارها جلوگیری کنند، شناخت راه‌های نفوذ بدافزارهاست که به هرکدام پرداختیم ،اما با رعایت نکات زیر میتوان تا حد زیادی از آلودگی به بدافزارها جلوگیری کرد:

- فقط صفحات مطمئن را باز کنید:

این توصیه آنقدرابتدایی است که گاهی به دلیل همین ویژگی نادیده گرفته می شود. اگر به لینک یا فایلی برای دانلود اطمینان ندارید پس باید از بازکردن یا بارگذاری آن جلوگیری کنید. اغلب بدافزارها در سایت هایی که محتوای غیرقانونی دارند بیشتر دیده می شوند. به عنوان مثال وقتی که به دنبال شماره سریال یک نرم افزار برای شکستن قفل آن هستید احتمال آلودگی در این سایت ها به شدت افزایش پیدا می کند. ضمن اینکه این آلودگی

فقط مخصوص سایت های خاص نیست پس اگر از سلامت یک پیوند اطمینان ندارید از آن صرف نظر کنید.برخی برنامه ها نیز می توانند در یافتن این سایت ها موثر باشند.

- HTML را خاموش کنید:

ایمیل ، یکی از موثرترین شیوه های انتشار انواع بدافزارها است. زمانی که یک ایمیل را باز می کنید اگر محتوای آن آلوده به بدافزارها باشد می تواند به صورت خودکار و بدون هیچ اطلاعی اقدام به اجرا و نصب اسکریپت های مخرب در سیستم شما کند. ایمیل ها معمولا به شکل یک متن ساده نمایش داده می شوند در این حالت خطری متوجه کاربر نیست. اما اگر اجرای فرمان های HTML در ایمیل فعال شده باشد آنگاه بدافزارها می توانند از طریق اسکریپت ها اجرا شوند. به همین دلیل است که سرویس دهنده های معتبر، عکس ها و محتوای چندرسانه ای را در حالت عادی نشان نمی دهند و قبل از نمایش آنها از کاربر اجازه می گیرند. البته می توانید فقط به فرستنده هایی که اطمینان دارید اجازه نمایش محتوای غیرمتنی را بدهید و مابقی را فیلتر کنید.

- پیوست ناشناس دانلود نکنید:

از زمانی که اجرای خودکار محتوای ایمیل ها روی اکثر سرویس دهنده ها غیرفعال شده، خرابکاران از ارسال فایل های ضمیمه بیشتر استفاده می کنند. به عنوان مثال ایمیلی را دریافت می کنید که ناشناس است اما شما را ترغیب می کند که برای اطلاعات بیشتر به پیوست و فایل ضمیمه ایمیل مراجعه کنید. این ضمیمه ها می توانند آلوده به بدافزارها باشند پس اگر فرستنده را نمی شناسید برای دستیابی به اطلاعات بیشتر تلاش نکنید.

- ویروس ها و آنتی ویروس ها:

در حال گشت و گذار در اینترنت هستید و یک صفحه اینترنتی به شما هشدار می دهد که سیستم شما آلوده است. یک سری اسم و عدد هم در آن آورده شده که مطمئن شوید وضعیت تا چه حد بحرانی و خطرناک است.

برای جلوگیری از آلودگی و پاکسازی رایانه، شما را به یک صفحه جدید راهنمایی می کنند و لینک دانلود یک آنتی ویروس را در اختیارتان قرار می دهند. با دانلود این آنتی ویروس در حقیقت گرفتار ویروس اصلی می شوید و آنچه تاکنون دیده اید تنها ظاهرسازی برای دانلود ویروس اصلی و فریب شما بوده است. این روش یکی از موثرترین شیوه های فریب کاربران است و برای پیشگیری از آلودگی کافی است که پنجره را ببندید.

- درایوهای بیرونی را کنترل کنید:

زمانی که یک بدافزار رایانه را آلوده می کند قبل از هر اقدامی به دنبال روشی برای تکثیر و انتشار خود است. به همین دلیل تمام خروجی ها که توانایی ذخیره اطلاعات را دارند می توانند به بدافزارها آلوده شوند. فرقی نمی کند که این خروجی درون شبکه است یا یک فلش دیسک که به سیستم متصل شده و حتی ممکن است این فایل ها روی دیسک هم ذخیره شوند. پس وقتی یک فلش دیسک را به کامپیوتر وصل می کنید قبل از بازکردن محتویات آن، از طریق آنتی ویروس آن را اسکن کنید. بهتر است برای دیسک ها نیز این روش را مورد استفاده قرار دهید. اغلب آنتی ویروس ها گزینه ای را به منوی امکانات سیستم اضافه می کنند که با انتخاب آن می توانید یک فایل، پوشه یا درایو را بررسی کنید. اگر روی سیستم خود آنتی ویروس دارید، تنها کاری که باید انجام دهید کلیک راست روی فایل یا پوشه مورد نظر و انتخاب گزینه اسکن است.

- برنامه های مطمئن را نصب کنید:

گاهی اوقات سازندگان برنامه های مخرب از پوشش یک نرم افزار کاربردی برای توسعه بدافزارها استفاده می کنند. در نتیجه وقتی یک نرم افزار را نصب می کنید ممکن است بدون اطلاع شما به همراه آن تعدادی از جاسوس ها و برنامه های مخرب هم نصب شوند. برای پیشگیری از این مشکل فقط به نرم افزارهای شناخته شده اجازه نصب دهید و برنامه هایی که تولیدکننده آن را نمی شناسید، نصب نکنید.

ممکن است افراد شناختی از شرکت های معتبر نرم افزاری نداشته باشند پس تنها راه باقی مانده دانلود نرم افزار از سایت های معتبر است. معمولا حجم و اندازه یک سایت و توانایی آن در معرفی و پیشنهاد برنامه می تواند به عنوان معیاری از دقت آن سنجیده شود با این حال با کمی جست وجو خواهید توانست سایت های ارایه دهنده نرم افزار را بهتر بشناسید.

یکی از روش هایی که اخیرا میان بدافزارها رایج شده است پیشنهاد نصب نوار ابزار روی مرورگر اینترنتی است تا از طریق آن بتوانید به برخی از امکانات سایت دسترسی داشته باشید و از آخرین تغییرات آن مطلع شوید که برای نصب این نوار ابزار ها نیز باید دقت کافی را داشته باشید [۱۵].

معرفی چند نمونه از بهترین انتی ویروس ها

بهترین آنتی‌ویروس برای سیستم‌عامل ویندوز

همه آنتی‌ویروس‌های آزمایش شده مخصوص ویندوز هستند و با ویندوزهای ۷، ۸ و ۱۰ سازگاری کامل دارند. این آنتی ویروس‌ها همچنین با ویندوزهای ویستا و XP هم کارمی‌کنند اما به دلیل آپدیت نشدن این ویندوزها از طرف مایکروسافت، شما قادر به دریافت پشتیبانی برای این سیستم‌عامل‌ها نخواهید بود.

چنانچه شما یکی از نسخه‌های ویندوز را استفاده می‌کنید، آنتی ویروس Bitdefender به دلیل شناسایی بیشترین تعداد بدافزارها، نسبت به بقیه آنتی ویروس‌ها، بهترین گزینه شماست. این نرم‌افزار از باز کردن فایل‌ها و لینک‌های خطرناک و آلوده توسط شما جلوگیری می‌کند و در مورد سایت‌های خطرناک در موتورهای جست‌وجوی اینترنتی به شما هشدار می‌دهد. این نرم‌افزار همچنین به یک امحاء کننده فایل[۲۰] و یک فیلتر اطلاعات شخصی

[۲۰] Shredder

مجهز است. Bitdefender بسیار سبک طراحی شده است و حتی در زمان اجرای بازی‌های سنگین هم کار خود را بدون کند کردن سیستم، به خوبی انجام می‌دهد.

بهترین آنتی‌ویروس برای تلفن‌های همراه

با استفاده روزافزون مردم از تلفن‌های هوشمند و تبلت‌ها برای دسترسی به اینترنت، هکرها و بدافزارها نیز روزبه‌روز بیشتر این دسته از کاربران را تهدید می‌کنند. امروزه بیشتر شرکت‌های تولیدکننده آنتی‌ویروس یک نسخه موبایل هم برای محافظت از این دستگاه‌ها ارائه می‌دهند.

البته شما برای این استفاده از این آنتی ویروس‌ها معمولاً باید یک لایسنس جداگانه خریداری کنید اما بعضی از شرکت‌ها نیز وجود دارند که نسخه موبایل و رومیزی را در یک بسته به شما عرضه می‌کنند.

برای مثال در صورت خرید آنتی‌ویروس Avast شما به نسخه موبایل آن هم به‌طور رایگان دسترسی خواهید داشت و می‌توانید با استفاده از آن، همه دستگاه‌های متصل به اینترنت خود را به آنتی‌ویروس مجهز کنید.نسخه موبایل آنتی ویروس Avast هم مانند نسخه ویندوزی آن می‌تواند بدافزارها، روتکیت‌ها و ایمیل‌های جعلی را شناسایی کند و جلوی دسترسی آنها به تلفن هوشمندتان را بگیرد؛ این بدان معنی است که شما بعد از نصب Avastمی‌توانید با خیال راحت و بدون نگرانی درباره بدافزارها، به گشت‌وگذار در شبکه‌های اجتماعی و مرور اینترنت بپردازید.

بهترین آنتی‌ویروس برای فعالیت‌های مالی آنلاین

آنتی ویروس‌های معتبر با تجهیز نرم‌افزار خود به ابزارهای مختلف، سعی در این دارند که خیال شما را از دسترسی نداشتن هکرها به اطلاعاتتان راحت کنند. کسپرسکی یکی از ابزارهای مهم در این عرصه است که به طور خاص برای حفاظت از اطلاعات حساس مالی شما در هنگام استفاده از کارت‌های بانکی و یا نرم‌افزارهای بانکداری اینترنتی،

طراحی شده است. اگر سیستم شما این آنتی ویروس را داشته باشد که به ابزارهای بانکداری اینترنتی مجهز باشد، هکرها به این آسانی‌ها نخواهند توانست به اطلاعات مالی شما دست پیدا کنند. استفاده از این ابزار، یکی از بهترین راه‌ها برای محافظت از هویت آنلاین و سیستم کامپیوتری شماست.

آنتی ویروس کسپرسکی علاوه بر قدرت بی‌نظیرش در زمینه مقابله با بدافزارها، به ابزارهایی مجهز است که امنیت شما را در زمان فعالیت‌های بانکی، تضمین می‌کنند.

برای مثال کسپرسکی یک صفحه کلید مجازی دارد که شما می‌توانید از آن برای وارد کردن نام کاربری و رمز عبور خود استفاده کنید. این کار باعث خواهد شد که هکرها نتوانند با استفاده از کی‌لاگرها (بدافزارهایی که قادرند هر چه را تایپ می‌کنید ذخیره و برای هکر ارسال کنند.) به اکانت شما دسترسی پیدا کنند. کسپرسکی همچنین ایمیل‌های جعلی را که مرتباً از شما درخواست وارد کردن اطلاعات بانکیتان را می‌کنند، شناسایی و مسدود می‌کند.

بهترین آنتی‌ویروس برای سیستم عاملMac

اکثر آنتی‌ویروس‌ها روی ویندوز ۱۰ آزمایش شده‌اند ولی بسیاری از آنها دارای نسخه مخصوص کامپیوترهای مک نیز هستند. معمولاً آنتی‌ویروس‌هایی که در دو نسخه ویندوزی و مک ارائه می‌شوند، روی هر دو سیستم‌عامل به خوبی کار می‌کنند اما بعضی از آنتی‌ویروس‌ها هم هستند که به طور خاص برای کامپیوترهای مک ساخته شده‌اند و به همین دلیل کارکرد آنها روی این سیستم‌ها، طبیعی‌تر و روان‌تر است. به‌علاوه، این شرکت‌ها به دلیل تسلط بهتری که روی سیستم‌عامل مک دارند، پشتیبانی بهتری هم به مشتری ارائه خواهند داد.

آنتی ویروس Intego یکی از ۱۰ آنتی‌ویروس برتر سیستم‌عامل مک است. این نرم‌افزار به صورت بی‌درنگ سیستم شما را اسکن می‌کند و پیش‌ازآن‌که بدافزارها فرصت آلوده کردن سیستم شما را پیدا کنند، آنها را از بین می‌برد. Integoعلاوه بر بدافزارهای سیستم‌عامل مک، بدافزارهای ویندوزی را هم شناسایی می‌کند و از این طریق مانع انتقال آنها از سیستم شما به کامپیوتر دوستان و اقوامتان خواهد شد.

بهترین آنتی‌ویروس رایگان

یک آنتی‌ویروس رایگان برای کسانی که بودجه محدودی در اختیار دارند، می‌تواند وسوسه‌کننده باشد. این آنتی‌ویروس‌ها بر خلاف انواع غیررایگان آن، معمولاً به طور اتوماتیک کامپیوتر شما را اسکن نمی‌کنند و به سیستم محافظت بی‌درنگ مجهز نیستند. آنها همچنین از شما در برابر وب‌سایتهای خطرناک و آلوده محافظت نمی‌کنند، زیرا فاقد افزونه‌های لازم برای نصب در مرورگر شما هستند. علاوه‌براین نسخه‌های رایگان همیشه در حال تبلیغ برای مجبور کردن شما به خرید نسخه پولی آنتی‌ویروس هستند. باوجودآن‌که این تبلیغ‌ها روی کارآیی نرم‌افزار تأثیری ندارند اما می‌توانند برای کاربر گیج‌کننده و عذاب‌آور باشند. البته شاید بدترین نکته در مورد آنتی‌ویروس‌های رایگان، که در مورد بهترین آنها هم صدق می‌کند، پشتیبانی نکردن شرکت سازنده از مشتری‌ها باشد.

به هر حال در بررسی‌ها مشخص شد که آنتی‌ویروس AVG بهترین آنتی‌ویروس رایگان است AVG .به ابزارهای محافظتی اضافه‌ای مجهز است که خیلی از آنتی‌ویروس‌های رایگان فاقد آنها هستند؛ برای مثال یک اسکنر فایل‌های قابل نصب روی درایوUSB، یک نرم‌افزار بهینه‌ساز سیستم و پشتیبانی از طریق ایمیل AVG .با دریافت امتیازهای بالایی در شناسایی و مسدود کردن ویروس‌ها از آزمایشگاه‌های تست آنتی‌ویروس معتبر، در این زمینه از کارآیی خوبی برخوردار است AVG .همچنین از مراحل نصب و رابط کاربری ساده‌ای برخوردار است.

باید اشاره کرد که آنتی‌وبروس رایگان AVG بر خلاف دیگر آنتی‌ویروس‌های رایگان، به شما امکان می‌دهد که اسکن‌ها را زمان‌بندی کنید و به جای یک بررسی ساده، کل سیستم شما را به طور کامل اسکن می‌کند [۱۶].

جمع‌بندی

در اینجا سعی شد تا انواع کدهای مخرب و بدافزارها معرفی شده و روش های انتشار و انتقال این کدها روی رایانه ها و شبکه ها بررسی گردد. نکته مهم پس از دانستن درباره بدافزارها، نحوه شناسایی و جلوگیری از انتشار آنها است. بدین منظور می بایست از تکنیک های مختلف و پیشرفته برای مقابله و شناسایی بدافزارها استفاده کرد چرا که توسعه دهندگان کدهای مخرب از روش های متنوع، جدید و پیچیده استفاده می کنند. آشنایی با انواع بدافزارها یکی از ابتدایی‌ترین مراحل بمنظور حفاظت از سیستم و اطلاعاتتان می‌باشد و قطعاً می‌بایست به هنگام انتخاب ضدویروس یا ابزارهای امنیتی نیز در مطالعه بررسی‌ها و انتخاب بهترین ابزار امنیتی کوشید.

مراجع

[۱] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_exec_summary_internet_security_threat_report_xiii_۰٤-۲۰۰۸.en-us.pdf Access On Jun.۱۰.۲۰۱۸

[۲] https://fa.wikipedia.org/wiki/بدافزار Access On Jun.۱۰.۲۰۱۸

[۳] F-Secure Quarterly Security Wrap-up for the first quarter of ۲۰۰۸». F-Secure. March ۳۱, ۲۰۰۸. Retrieved ۲۰۰۸-۰۴–۲۵ Access On Jun.۱۱.۲۰۱۸

[۴]https://www.wsj.com/articles/SB۱۰۰۰۱٤۲٤۰٥۲۷٤۸۷۰٤۹۰٤٦۰٤٥۷٦۳۳۲۸۱۲٥۹۲۳٤٦۷۱٤ Access On Jun.۱۰.۲۰۱۸

[۵] https://technet.microsoft.com/en-us/library/cc٥۱۲٥۹٦.aspx

Access On Jun.۱۰.۲۰۱۸

[۶]بشری راد، بابک، حبیبی لشکری، آرش، ویروس‌ها و بدافزارهای کامپیوتری، انتشارات ناقوس، ۱۳۹۱

[۷] https://fa.wikipedia.org/wiki/ویروس_رایانه%E۲٪۸۰٪۸Cای Access On Jun.۱۰.۲۰۱۸

[۸] http://www.hamshahrionline.ir/details/۱۱۹۲۴ Access On Jun.۱۰.۲۰۱۸

[۹] http://kharazmi.org/read/fargh_beyn_trojan_virus_va_kerm_chist Access On Jun.۱۰.۲۰۱۸

[۱۰] https://www.cyberpolice.ir/learning/۹۹۸۱ Access On Jun.۱۲.۲۰۱۸

[۱۱] http://www.khabaronline.ir/detail/۱۹۸۷۲۷ Access On Jun.۱۲.۲۰۱۸

[۱۲] https://fa.wikipedia.org/wiki/تروجان (رایانه) Access On Jun.۱۰.۲۰۱۸

[۱۳] https://en.wikipedia.org/wiki/Spyware Access On Jun.۱۰.۲۰۱۸

[۱۴] https://fa.wikipedia.org/wiki/افزار%E۲٪۸۰٪۸Cآگهی Access On Jun.۱۰.۲۰۱۸

[۱۵] https://www.sarzamindownload.com/contents/۹۱۳ Access On Jun.۱۳.۲۰۱۸

[۱۶] https://blog.faradars.org/compare-top-antivirus/ Access On Jun.۱۲.۲۰۱۸