

مقایسه و تفاوت بین آنتی‌ویروس‌های کرک شده و نسخه اصلی



چرا آنتی‌ویروس اصلی بخریم؟

در کشور ما ایران، قانونی به اسم کپی رایت (Copyright) وجود ندارد؛ لذا استفاده از محصولات نرم‌افزاری کرک شده و قفل شکسته مانعی ندارد ولی با وجود این شرایط، بسیاری از شرکت‌ها و کاربران حرفه‌ای و یا حتی آماتور از سیستم عامل‌ها و آنتی‌ویروس‌های اصلی استفاده می‌کنند. در این میان، استفاده از آنتی‌ویروس‌های اصلی بسیار بیشتر از سایر نرم‌افزارها به چشم می‌خورد؛ این مورد در شرایطی است که کرک‌های بسیاری برای هر کدام از این محصولات وجود دارد؛ پس چرا بسیاری از افراد از محصولات اصلی استفاده می‌کنند؟

چندین پاسخ به این سؤال وجود دارد که در اینجا به چند مورد از آنها می‌پردازیم:

۱- در ابتدا باید به این موضوع توجه داشت که آنتی‌ویروس یک محصول امنیتی محسوب می‌شود و امنیت زمانی معنا می‌یابد که پایدار و قدرتمند باشد. از آنجا که کرک‌ها و سریال‌های غیر اصلی قابل اطمینان نیستند ممکن است در یک بازه زمانی آنتی‌ویروس شما از کار بیفتد در این صورت حتی اگر آنتی‌ویروس شما بسیار هم قدرتمند باشد تاثیر بسزایی در امنیت سیستم شما نخواهد داشت. این زمان بهترین فرصت برای فعالیت بدافزارها و هکرها می‌باشد.

۲- هکرها شناخت خوبی از فضای کامپیوتر و رفتار کاربران کامپیوتر دارند و دقیقاً می‌دانند که چگونه باید آنها را فریب دهند به همین دلیل چون می‌دانند که کاربران نیاز به امنیت در فضای سایبر دارند تمرکز خود را بر روی شکستن قفل محصولات امنیتی از جمله آنتی‌ویروس‌ها می‌گذارند و هنگامی که کاربر اقدام به شکستن قفل آنتی‌ویروس کامپیوتر خود طبق راهکار آن هکر می‌کند در واقع احساس می‌کند که آنتی‌ویروس خود را فعال ساخته است؛ بدون آنکه هزینه‌ای پرداخت کند و احتمالاً از این بابت احساس غرور هم می‌کند؛ ولی در واقع کاری کرده که

آن هکر بدافزار خود را توسط خود کاربر به آسانی بر روی سیستم او تعبیه کند و در صورت تمایل از آن سوء استفاده نماید. به همین سادگی او توانسته است کاربر را فریب دهد!

۳- به عنوان سومین مورد باید به این موضوع توجه داشت که برخی از فروشندگان معتبر آنتی ویروس های اصلی (در ایران) یک سرور آنتی ویروس برای خود راه اندازی می کنند و سپس آنتی ویروس هایی که می فروشند را طوری تنظیم می کنند که آپدیت های خود را از سرور فروشنده بگیرند نه از سرور تولید کننده آنتی ویروس. بنابراین علاوه بر اینکه آن فروشنده سود کلانی از راه کلاهبرداری بدست می آورد آپدیت ها نیز همواره با یک وقفه طولانی به دست کاربران می رسد و چه بسا که این آپدیت ها کارایی مناسب خود را نیز نداشته باشند. این مورد در اکثر مواقع در مورد آنتی ویروس های معروفی که تحریم شده اند اتفاق افتاده است. بنابراین همواره باید توجه داشته باشید که از نمایندگی های معتبر در ایران خریداری کنید. (نماینده معتبر کسی است که در وب سایت شرکت سازنده آنتی ویروس «به عنوان مثال: شرکت Kaspersky» به عنوان نماینده نامش ذکر شده باشد).

اکنون که متوجه شده اید که چرا باید آنتی ویروس اصلی تهیه کنید به چند فاکتور مهم جهت مقایسه آنتی ویروس ها می پردازیم:

ابتدا توجه داشته باشید که ما در شرایط تحریم به سر می بریم و بسیاری از شرکت های تولید کننده آنتی ویروس هیچ نمایندگی ای برای محصولات خود در ایران نمی پذیرند و حتی اگر کسی موفق به تهیه لایسنس آن محصول شود آن را غیر قانونی شناخته و غیر فعال می سازد. البته راهکارهایی برای این مورد وجود دارد که به یکی از آنها در مورد بالا اشاره کردیم که چندان هم عاقلانه نیست. بنابراین این مهم پیش می آید که تحت هر شرایطی از محصولات اصلی دارای نمایندگی در ایران استفاده نماییم. همچنین سازمان هایی در نقاط مختلف دنیا وجود دارند که از راه های مختلف به مقایسه آنتی ویروس ها می پردازند که از معروف ترین آنها می توان به AV-Comparatives.org، Virus Bulletin، AV-Test، OPSWAT و... اشاره کرد. گزارش های این سازمان ها کاملاً معتبر بوده و مورد تأیید کلیه تولید کنندگان آنتی ویروس می باشد.

مقایسه بین آنتی ویروس های کرک شده و نسخه اصلی

بدانید که اگر آنتی ویروس را دانلود کنید (بصورت رسمی از سایت های سازندگان آنتی ویروس) معمولاً این نرم افزارها بصورت نسخه های Trial می باشند نه Demo، یعنی همه امکانات یک آنتی ویروس رجیستر شده را دارند بجز محدودیت زمانی (مثلاً اجازه می دهند بین ۲۰ تا ۳۰ روز بصورت رایگان آپدیت شوند) بعد از این مدت شما دیگر قادر به استفاده از امکانات نرم افزار نمی باشید. از جمله مهم ترین ویژگی که همه آنتی ویروس ها آن را از کار می اندازند امکان بروزرسانی لیست ویروس ها و گارد یا جستجوی آنلاین ویروس ها است و برای ادامه استفاده از یک آنتی ویروس شما نیاز دارید که آن را رجیستر و لایسنس آن را خریداری کنید.

چرا شرکتهای امنیتی سازنده آنتی ویروس ها اجازه آپدیت نرم افزارهای کرک شده را می دهند؟

شاید شما فکر کنید که راحتی و با داندود فایل های کرک توانسته باشید این شرکتهای بزرگ را گول زده باشید و این شرکت ها که کارشان امنیت است نتوانسته اند مشکل کرک را حل کرده باشند! اگر این چنین فکر می کنید کاملاً در اشتباهید! همه شرکت ها به راحتی می توانند بفهمند که چه کسانی و با چه IP یی و از چه کشوری و از چه نسخه ای و با چه شماره سریالی به سرور آنها وصل شده و اقدام به آپدیت آنتی ویروس خود می کنند. بنابراین شرکتهای بزرگی همچون بیت دیفندر، کسپراسکی، نود ۳۲، مکافی و غیره به راحتی می توانند مانع آپدیت برنامه های کرک شده شوند. حتماً می پرسید اگر این شرکت ها می توانند؛ چرا مانع کپی غیر قانونی نرم افزارهایشان نمی شوند؟

دلایل متعددی برای این کار وجود دارد:

از نظری تجاری کارشناسان شرکتهای آنتی ویروسی معتقدند که برای اینکه بتوانند بر سر زبانها بیفتند و افرادی که توانایی خریدن را ندارند و یا نیازی ندارند بتوانند از این آنتی ویروس ها استفاده کنند. در واقع این شرکت ها اجازه استفاده ۲۰٪ بصورت غیرقانونی را برای اهداف تجاری و تبلیغاتی می دهند.

افرادی که از برنامه های کرک شده استفاده می کنند حتماً احتیاجی به ساپورت و پشتیبانی ندارند و اطلاعات روی سیستمشان آنقدر برایشان مهم نیست که در صورت ویروسی شدن و یا مورد حمله قرار گرفتن (اطلاعات خصوصی)، چیزی را از دست نمی دهند و می توانند با یکبار فرصت و نصب دوباره سیستم عاملشان (مثل ویندوز) دوباره همه چیز را از اول آغاز کنند.

بنابراین شرکتهای امنیتی از آپدیت برنامه های کرک شده مطلع هستند.

تفاوت بین آنتی ویروس های Crack شده و اصلی چیست؟

آپدیت برنامه های کرک شده از سرور اصلی آپدیت صورت نمی گیرد بلکه از سرور مخصوص آپدیت برنامه های کرک شده انجام می گیرد.

بعلت وجود کرک های مختلف که بدست افراد خرابکار بوجود می آید امکان دزدی و کپی اطلاعات شخصی کامپیوتر شما مثل پسوردها و اطلاعات ایمیل ها و اطلاعات بانکی و فایل های شخصی و غیره و همچنین ایجاد خرابکاری در کامپیوتر شما وجود دارد. در واقع در ۹۹ درصد مواقع خود این کرک ها حاوی نرم افزارهای مخرب و جاسوسی هستند. کرک ها که عاشق چشم و ابروی شما نیستند!

سرورهای شرکت‌های آنتی‌ویروس ابتدا اقدام به آپدیت نرم‌افزارهای اصلی یا Genuine و یا لایسنس دار می‌کنند و برنامه‌های کرک شده با سرعت بسیار پایین و تنها لیست برخی از ویروس‌ها را بروز می‌کنند و البته آن‌هم از سرورهای مخصوص برنامه‌های کرک.

سپورت‌ها و پشتیبانی امروزه در همه محصولات حرف اول را می‌زند. خصوصاً در یک آنتی‌ویروس که روزانه تعداد بی‌شماری برنامه‌های مخرب بوجود می‌آیند و امکان شناختن ویروس یا مخرب‌ها وجود دارد، بسیار مهم است. یکی از مهم‌ترین مزایای نرم‌افزارهای اورجینال امکان استفاده از خدمات پشتیبانی است.



چگونه یک آنتی‌ویروس خوب انتخاب کنیم؟

شاید یکی از مهم‌ترین و بهترین راه جلوگیری از ویروسی و هک شدن کامپیوتر در اینترنت، داشتن یک آنتی‌ویروس قوی و به روز باشد. با توجه به پیشرفت روز به روز علم کامپیوتر و دانش اینترنت، تعداد آنتی‌ویروس‌ها رو به رشد می‌باشد. ولی آیا هر آنتی‌ویروسی قابلیت شناسایی ویروس‌ها و تروجان‌های جدید را دارد؟ خیر. معمولاً آنتی‌ویروس‌ها طوری تقسیم و طبقه‌بندی می‌شوند که هر نرم‌افزاری که بتواند ویروس‌های بیشتر و جدیدتری را شناسایی نماید، در رتبه بالاتری قرار بگیرد.

اولین گام: تعریفی از ویروس

ویروس به نرم‌افزارها و تکه‌های اطلاعاتی گفته می‌شوند که توسط افراد باهوش و با تجربه نوشته می‌شود و با دو هدف تخریب و یا جاسوسی در سطح شبکه و کامپیوترهای شخصی توزیع می‌شود.

چگونگی پخش ویروس

در اصل، پخش ویروس به دو صورت جهنده و راکد است. پخش جهنده بدین صورت است که خود ویروس با بهره‌گیری از ابراز انتقال اعم از سی دی، فلاپی دیسک، کول دیسک و ... خودبخود توزیع می‌شود. ویروس‌های

راکد ویروس‌هایی هستند که در اصل می‌بایست نسخه‌ای از آن در سیستم جدید کپی شود وگرنه خود جابجا نمی‌شود. چگونگی ویروس‌ها در این خصوص باتوجه به طراحی آن ویروس است.

عملکرد ویروس‌ها

تخریبی: در ابتدا با همین هدف ویروس‌ها نوشته و توزیع می‌شد که به کل یا قسمتی از اطلاعات آسیب جزیی یا جدی برساند و در مواردی نادر، کل اطلاعات را از بین ببرد. فرض کنید یک فرد ناآرام ویروسی را در شبکه پلیس شهر پخش می‌نماید تا کلیه پرونده‌ها را نابود سازد. هدف وی از این کار، تخریب اطلاعات است ولی چرا تخریب؛ از خودش سؤال کنید!

جاسوسی: به مرور این نوع ویروس‌ها هم شیوع پیدا نمود که به شبکه‌ها و اطلاعات ارزشمند و یا غیر ارزشمند دسترسی پیدا نمایند. همان فرد مثال ما، به شبکه بانک شهر ویروس ارسال می‌کند. این بار می‌خواهد که اطلاعات حساب‌ها بانکی را دریافت نموده و بعد آن را به نوع اول تخریب و دستکاری کند!

کسب و کار: کشور لهستان بالاترین رقم درآمد از ویروس نویسی را داراست. ساده است فردی ویروسی را آماده می‌کند، کمی هم در شبکه‌ها توزیع می‌نماید و به شرکتهای دیگر برای جاسوسی یا خراب کردن شرکت رقیب می‌فروشد. البته در برخی موارد ویروس نویس به صورت مستقیم با قربانی معامله می‌کند. مثلاً «جان» شبکه ناسا را هدف قرار می‌دهد و با مقامات ذیربط تماس می‌گیرد که راه حل رفع آن را در ازاء مبلغی به آنها بفروشد. البته در بعضی از کشورهای دنیا، نگارش ویروس، پخش و هرگونه دخالت در پدید آمدن آن جرم محسوب می‌شود.

هدف اصلی چیست؟

نمی‌توان هدف مشخصی را تدوین نمود. در اصل و در نگاه نویسنده ویروس، شاید دو عامل تخریبی و جاسوسی مهم باشد ولی در مواردی هم درآمدزایی در اولویت است. در مجموع پس از طراح ویروس، بیشتر کاربران بدون هدف و بدون آنکه آگاه باشند، ویروس را منتشر می‌کنند.



ویروس‌های ایرانی

ویروس‌های ایرانی به جز چند ویروس، مشهور و معروف نشدند و کمتر مورد توجه قرار گرفتند به خصوص ویروس‌هایی که کل اطلاعات را نابود می‌نمودند و مورد تنفر قرار گرفتند. در دهه گذشته، اخبار انتشار ویروس‌های ایرانی شنیده می‌شد اما اینک متخصصین آی تی بیشتر به سمت هک سایت‌ها تمایل نشان می‌دهند.

نسل جدید ویروس‌ها

اگر اخبار آی تی را دنبال کنید؛ هر هفته تعدادی ویروس جدید منتشر و منطقه‌ای را آلوده می‌سازند. برخی از کاربران واژه‌های تروجان و اسب تراوا و کرم‌ها را ویروس می‌دانند ولی این دوستان! نرم‌افزارهای جاسوسی اینترنتی بوده گرچه از نوادگان ویروس هستند اما نمی‌توان در تعاریف ویروس آنها را ذکر نمود.

راه حل مواجهه با ویروس‌ها

ساده است: آنتی‌ویروس‌ها و برنامه‌های امنیتی شبکه! البته اگر شما کامپیوتر شخصی دارید، نصب آنتی‌ویروس و در نهایت دیوار آتش کافی است. دیوار آتش (فایروال) یک برنامه امنیتی است که از نفوذ انواع نرم‌افزارهای مزاحم جلوگیری می‌نماید. البته از ویندوز XP به بعد یک دیوار آتش خفیف! در خود سیستم عامل موجود است.

نکات مهم در انتخاب آنتی‌ویروس‌ها

همیشه برای انتخاب یک آنتی‌ویروس برای خود سعی کنید نکاتی را مد نظر قرار دهید:

- آنتی‌ویروسی معروف و مطمئن انتخاب نمایید.

- حتماً نسخه اصلی آن را خریداری نمایید که در داخل کشور دارای پشتیبانی باشد.

- آنتی‌ویروسی را انتخاب کنید که بروزرسانی آن بدون مشکل انجام شود (بعضی از شرکت‌ها به علت تحریم اجازه بروزرسانی مستقیم را به کاربرهای ایرانی نمی‌دهند).

- سعی کنید تا آنجا که امکان دارد نسخه‌ای را تهیه کنید که دارای دیوار آتش (فایروال) هم باشد.

- بسیاری از شرکت‌های معتبر هستند که آنتی‌ویروس را به صورت نسخه اصل (اورجینال) ولی رایگان ارائه می‌دهند. شما می‌توانید با استفاده از این آنتی‌ویروس‌ها علاوه بر اینکه از نرم‌افزار کرک نشده استفاده می‌کنید؛ از آپدیت‌های قانونی از سرور اصلی آنها بهره‌مند شوید.

در زیر لیستی از شرکت‌های معتبر و معروف ارائه آنتی‌ویروس‌های رایگان را برای استفاده شما دوستان ذکر می‌کنیم به این امید که این طرز فکر (به دنبال کرک بودن برای آنتی‌ویروس) رخت از اذهان همه بر بندد!

Avast (آنتی‌ویروس رایگان به دلیل عملکرد سریع و رابط کاربری ساده و آسان و ویروس‌یابی قوی و پیشرفته)

Avira (آنتی‌ویروس رایگان با قابلیت ویروس‌یابی قوی)

AVG (آنتی‌ویروس رایگان و قدرتمند با آمار دانلود بسیار بالا)

Microsoft Security Essential (ساخت شرکت مایکروسافت، شرکت سازنده ویندوز)

ZoneAlarm (فایروال رایگان با قابلیت جلوگیری از حملات هکرها و site Phishing)

Comodo (این شرکت آنتی‌ویروس، **internet Security** و همچنین **Firewall** رایگان ارائه می‌دهد)

نکات ایمنی در کار با ویروس‌کش‌ها

خرید یک آنتی‌ویروس و نصب آن به معنای دستیابی به امنیت دائمی نیست. در استفاده از این نرم‌افزارها همیشه به نکات زیر توجه داشته باشید:

- سعی کنید هر روز یا حداقل هر هفته آنتی‌ویروس را بروز رسانی کنید.

- هر هفته کل درایوها مخصوصاً درایو ویندوز را اسکن نمایید.

- اجازه کانکت شدن هر برنامه اجرایی که توسط فایروال شناسایی می‌شود را ندهید. فقط نرم‌افزارهای مورد نیاز مثل مسنجرها را مجاز مشخص کنید.

حالا که شما یک آنتی‌ویروس مناسب برای کامپیوتر خود انتخاب کرده‌اید و آن را به روز رسانی کرده و بقیه کارهای جزئی را انجام داده‌اید؛ می‌توان گفت تا حد خیلی زیادی از هک و ویروسی شدن کامپیوترتان جلوگیری کرده‌اید.



چرا بر بروز رسانی تأکید داریم؟

بسیار ساده است: در هفته نزدیک به ۲۰۰ ویروس جدید منتشر می‌شود که آنتی‌ویروس‌ها برای شناسایی آنها نیاز به بروز رسانی دارند. از طرف دیگر بعضی از ویروس‌ها در تاریخ خاصی فعال می‌شوند که برای شناسایی آنها باید سیستم را هر هفته یکبار اسکن کرد.

در پایان به خاطر داشته باشید خرید یک آنتی‌ویروس مطمئن، ارزش حفاظت از اطلاعات شخصی، عکس‌های خانوادگی، اکانت شبکه‌های اجتماعی، رمز کارت‌های اعتباری و ده‌ها مورد دیگر که این روزها جزء جدایی ناپذیر روزمرگی ما هستند را دارد.

