دانشگاه علوم پزشکی و خدمات بهداشتی درمانی سیرجند

حراست

آشنایی با ویروس

(قسمت آخر – انتخاب یک ضد ویروس کارا و مناسب)

تنظیم کننده :

حراست فناوری اطلاعات دانشگاه

توجه: ویژگیهای ذکر شده در پایین بعنوان ویزگیهای عمومی برای تمام آنتی‌ویروس‌های مطرح در بازار بوده که لزوما باید داشته باشند و اختصاص به آنتی‌ویروس خاصی ندارد.

شما کاربرگرامی نیز می‌بایست بر اساس تحقیقات خودتان و با توجه به نیازتان برند خاصی را بعنوان آنتی ویروس انتخاب کنید و فقط توجه داشته باشید که برای بالا بردن امنیت خود در فضای مجازی از نسخه های اصلی و معتبر ضدویروس استفاده کرده و به هیچ عنوان از نسخه های جعلی و کرک شده استفاده نکنید.

چالشهای مقایسه آنتی‌ویروسها

چالش ۱: کاربران آنتی‌ویروس اغلب به دنبال حل مشکلات ویروس خود بوده و فرصت تحقیق و مطالعه و مقایسه آنتی‌ویروسها را ندارند. به هنگام تصمیم گیری درانتخاب یک آنتی‌ویروس مناسب، متاسفانه اغلب کاربران به جای اتخاذ یک روش علمی و تحقیق و مطالعه در کیفیات آنتی‌ویروسها، دست به دامان شنیده‌ها و توصیه‌ها و تبلیغات فروشندگان می شوند. مشخص است که این روش علمی نیست.

چالش ۲: در حال حاضر سازمانها و شرکتهای مختلفی اقدام به مقایسه محصولات امنیتی کرده و نتایج آزمونهای خود را در قالب نشانه‌ای خاص ارائه می‌کنند. این نشانه‌ها، به عنوان ابزار برتری محصولات از سوی تولیدکنندگان و یا سایر افراد ذینفع مورد استناد قرار می‌گیرد. کثرت این منابع و ادعای کلیه تولید کنندگان محصولات امنیتی مبنی بر بهترین بودن،کاربران را با ابهاماتی مواجه کرده است. حتی در مواردی ، با استناد به یک مرجع و منبع واحد، سازندگان زیادی ادعای برتری می‌کنند که این مورد ابهامات را دوچندان می کند.

راه حل:

۱-عدم اعتماد به ادعاهای فروشندگان، سازندگان و یا نمایندگان آنتی‌ویروسها و اتخاذ یک روش علمی

۲-تحقیق در مورد اعتبار و استقلال مرجع آزمون گیرنده

کدام ضدویروس بهترین است؟ شاید اگر از اشخاص گوناگون بپرسیم پاسخ های متفاوتی دریافت نماییم. اما اگر از همان اشخاص بخواهیم دلایل و مدارکی برای انتخاب خود بیاورند، به احتمال بسیار زیاد جواب قانع کننده‌ای دریافت نکنیم. دلیل این موضوع بسیار واضح است، اغلب ما از زاویه‌ای جانبدارانه به این قضیه می‌نگریم، شاید تنها معیار ما برای انتخاب بهترین ضدویروس تجربه چندین ساله از داشتن آن محصول خاص باشد.و شاید هم زحمت مطالعه و تحقیق را بر خود روا نداشته و اساس انتخاب خود را بر شنیده‌ها معطوف می‌داریم. از اینرو اینگونه قضاوت‌ها اساساً پایه علمی و تحقیقاتی نداشته و نمی‌توان به صحت و درستی آن اعتماد داشت.

اما شاید این پرسش برایتان مطرح شود که پس راه حل چیست؟ به راستی چگونه می توان بدون قضاوتی جانبدارانه بهترین (و یا حداقل یکی از بهترین محصولات آنتی‌ویروس) را انتخاب کرد. در جواب باید بگوییم اینکار نیاز به تحقیق و بررسی نتایج آزمایش‌های گوناگون که طی چندساله برگزار شده است دارد. آنچه مسلم است این است که تجربیات شخصی ما، به تنهایی نمی‌تواند برای بررسی تمامی ویژگیهای یک آنتی‌ویروس کافی باشد. برای بررسی آنتی‌ویروسها به صورت جامع، نیاز به آزمایشگاههای مجهز و مهمتر اینکه نیاز به دانش اختصاصی آن می باشد . خوشبختانه چند سازمان در سطح جهان وجود دارد که کار آن اختصاصا مقایسه آنتی‌ویروسها است.البته براساس نتایج این سازمانها، نیز نمی توان اعتماد صد در صد کرد چراکه یک برند در آزمون یک سازمان رتبه ممتاز کسب می کند ولی در آزمون سازمان دیگر در همان مقطع زمانی نمره متوسط کسب می کند لذا باید نتایج چندین سازمان را گرد آوری و باهم مقایسه کرد و آنتی ویروسی که در عمده نتایج همزمان این سازمان ها رتبه خوبی کسب نموده اند را انتخاب نمود، چرا که آن هنگام می توان ادعا کرد محصول انتخابی ما واقعاً ضدویروس خوب و قابل اطمینان است.

پارامترهای مهم در ارزیابی آنتی‌ویروسها

ویژگیهای مهم آنتی‌ویروسها را می توان به دو دسته فنی و غیر فنی دسته بندی کرد. از دید فنی، یک آنتی ویروس در درجه اول باید بتواند ویروسها را به خوبی تشخیص دهد. ثانیا، یک نرم افزار آنتی‌ویروس باید سبک بوده و کمترین منابع سیستمی را اشغال کند.

یک ویژگی بسیار مهم دیگر، هوش مصنوعی آنتی‌ویروس است. همه کاربران این مطلب معروف" ویروسها همیشه یک گام از ضدویروسها جلوتر هستند" را به دفعات شنیده‌اند. اما این مطلب بیشتر در مورد ضدویروسهای سنتی که شناسایی آنها بر پایه الگو می‌باشد صادق است.

با توجه به رشد صعودی ویروسها و با درنظر گرفتن اینکه، یک ویروس در مدت زمانی که سازنده ضد ویروس در حال شناسایی آن می‌باشد چه صدماتی را وارد می کند، این روش سنتی جوابگو نبوده و نیاز به یک ضدویروس هوشمند بیش از پیش ضروری به نظر می‌رسد.**استفاده از هوش مصنوعی،**

مزایایی مانند سبک بودن و سرعت اسکن بالا را به همراه دارد. زیرا در روش سنتی ، اطلاعات ویروسها در بانک اطلاعاتی ضدویروس ذخیره می شود. با توجه به اینکه در حال حاضر بیش از شش میلیون نوع ویروس در دنیا شناسایی شده، ذخیره این حجم بالای ویروسها تبعاتی مانند افت شدید کارایی سیستم (سنگین بودن) و عدم شناسایی ویروسهایی جدید را به همراه دارد در حالیکه، این مشکل با هوش مصنوعی قابل حل بوده

ویژگیهای مهم یک ضد ویروس که سازمانهای جهانی(VirusBulletin و Comparatives و ....) آنها را مورد ارزیابی قرار می دهند

به ترتیب اهمیت عبارتند از:

۱. قدرت شناسایی بالا(قدرتمند بودن)

۲. هوش مصنوعی مطمئن در جهت شناسایی ویروسهای ناشناخته جدید(هوشمند بودن)

۳. کمترین تاثیر بر کارایی سیستم (سبک بودن)

۴. سرعت اسکن: از دید غیر فنی قدرت تعمیر فایلهای آلوده است ، مسایلی همچون نداشتن بکدور ارسال فایلها و اطلاعات از سیستم کاربر به شرکت سازنده آنتی ویروس می باشد

۵.آنتی‌ویروسهای چند موتوره-سنگین ترین آنتی‌ویروسهای جهان

ویژگی‌های انتخاب یک ضدویروس کارآ و مناسب

۱- مشخصات عمومی :

* داشتن لایسنس معتبر و اصلی
* سهولت در نصب نسخه های مختلف حتی نسخه سازمانی تحت شبکه
* سهولت در استفاده
* عملکرد یا کارآیی
* زمان پاسخ به ویروس‌های جدید اعلام شده از طرف مشتری
* پشتیبانی ویروس‌های منطقه‌ای
* عدم تخریب فایلهای اصلی سیستم و اطلاعات ایجاد شده توسط کاربر
* وابگویی فایلهای تخریب شده توسط ضدویروس
* پاکسازی کامل فایل
* بازیابی اطلاعات کدشده توسط ویروس
* گزارش گیری مدیریتی جهت پیدا نمودن منبع آلودگی و کنترل کاربران
* وجود امنیت در طراحی نرم‌افزار
* عدم وجود Backdoor و Blackbox در برنامه ضدویروس
* پاکسازی سریعتر
* قابلیت سفارشی نمودن نرم‌افزار
* وجود مرکزی بومی برای تحقیقات روی ویروس‌های رایانه‌ای
*در دسترس بودن کارشناسان ضدویروس و تیم تحقیقاتی

* ارائه پشتیبانی مناسب

* ارائه کمترین پیام به کاربر بخصوص در زمان بازی

* داشتن امکانات اضافی مانند داشتن کنترل والدین و ....

* داشتن فایروال قوی یا بهینه سازی فایروال سیستم عامل

۲- قابلیت‌های اسکن (پویش یا کنترل):

* پویش بلادرنگ (آنی)

* پویش بر اساس جدول زمانی

* پویش مکاشفه‌ای

* پویش دستی

* تخمین زمان پویش

* پویش در زمان بیکاری سیستم

* گزارش گیری و ثبت تاریخچه آن

۳- به روز رسانی :

* اشتراک سالانه

* بروز رسانی اطلاعات ویروسها به صورت خودکار

* بروز رسانی رابط کاربری و موتور جستجو به صورت خودکار

* بروز رسانی اطلاعات ویروسها به صورت دستی

* بروز رسانی رابط کاربری و موتور جستجو به صورت دستی

* کلیه انواع بروز رسانی ها وقتی انجام می گیرد عملکرد سیستم را تحت تأثیر قرار نداده و بتوان سایر امورات را براحتی حین بروز رسانی انجام داد.

۴- گواهینامه (Certification)

۵- پشتیبانی فنی، همیشگی و موثر

* راهنما/پاسخ به سوالات متداول/ دانش‌مان یا پایگاه دانش (Knowledge Base)

* پشتیبانی تلفنی

* دوره‌های آموزشی برای نسخه های سازمانی

* پشتیبانی از طریق ایمیل

۶- پشتیبانی شده برای سیستم عامل‌های رایج

۷- دیگر ویژگی ها:

* هشدار در مورد تهدیدات فراگیر

* سازگاری سخت‌افزاری و نرم‌افزاری سیستم با ضدویروس انتخاب شده .

* توانای شناسائی الگوریتم‌های (Heuristic) .

* توانایی شناسائی انواع فایل‌ها با فرمت‌های مختلف .

* توانایی شناسائی اسب‌های تراوا، جاوا اپلت‌های مخرب، اکتیوایکس‌های مزاحم و اسکریپت‌های مخرب.

* توانایی پویش ضمیمه (Email) .

* قابلیت بررسی فایل‌های فشرده .