به نام خداوند یکتا

مستند

اعتبارسنجی فایل: رویکرد فعال مؤثر

آنتی‌ویروس eScan

(File Reputation)

تاریخ انتشار: خردادماه ۱۳۹۵

شماره تماس: ۴۴۹۵۵۵۶۷ (۰۲۱) - ۳۶۲۸۱۱۱۲ (۰۳۵)
ایمیل: info@kaipod.ir

فهـرسـت

۱- مقدمه

در این مستند، در مورد عوامل تأثیرگذار بر روی سیستم اعتبار امنیت دیجیتال مباحثی ارائه خواهد شد. سیستم اعتبار امنیت چه کاربردی دارد؟ چگونه از نظر رویکرد سنتی، اثربخشی بیش‌تری دارد؟ مزایای آن چیست؟

از نخستین روزهای پیدایش جوامع برخط، اعتبار مهم‌ترین عامل در انجام کسب و کار برخط محسوب شده است، ویکی‌پدیا اعتبار را به این صورت بیان نموده که "اعتبار یک نهاد اجتماعی"(یک فرد، یک گروه از افراد، یک سازمان) عقیده موجود در مورد آن نهاد می‌باشد که به طور معمول نتیجه‌ی ارزیابی اجتماعی مجموعه‌ای از معیارها است به‌طوری که در امورآموزش، کسب و کار و جوامع برخط حائز اهمیت می‌باشد.

هنگامی که در مورد اعتبار صحبت می‌کنیم، باید به این نکته توجه شود که ماهیت اعتبار پویا و موقت است. این ماهیت اغلب به محض تغییرات محتوا در حال دگرگونی است. سیستم اعتبار در مقایسه با روش سنتی فعال‌تر می‌باشد. امروزه اعتبار برای امنیت سایبری بسیار مهم‌تر از گذشته می‌باشد، چنان‌که کاربران بیشتری به اینترنت برای دسترسی به رایانامه‌ها، فایل‌ها و URLها متصل می‌شوند.

افراد بداندیش در حوزه‌ی فناوری اطلاعات (نفوذگران و مجرمان سایبری) متوجه این امر می‌باشند که رویکرد سنتی انفعالی است و توان مقابله با حجم بسیار بالایی از تهدیدها را ندارد، این موضوع باعث می‌شود تا فرصتی برای حمله به سیستم، دسترسی غیرمجاز به آن و انجام هر فرآیند مخربی امکان‌پذیر باشد و تا زمانی که امضاهای ویروس دانلود شوند، نفوذگران و مجرمان سایبری، ضربه خودشان را به امنیت وارد نموده‌اند. ضعف عمده‌ی رویکرد سنتی حجم بالای امضاهای ویروس است، فراوانی آن‌ها افزایش یافته و شرکت‌ها در حال رقابت برای یافتن راه‌هایی برای توزیع سریع‌تر و مؤثرتر امضاهای ویروسی می‌باشند، با توجه به گستره‌ی فراوانی الگوهای شناسایی بدافزار، بررسی آن‌ها در محیط‌های رایانشی وسیع بسیار خسته‌کننده و وقت‌گیر می‌باشد. تعداد تهدیدهای موجود نیز، به‌طور هشدار دهنده‌ای در حال رشد است.

کارشناسان eScan سال‌ها مشغول تحلیل و پایش انواع تهدیدهای موجود می‌باشند و نرخ یافتن تهدیدهای جدید و ناشناخته در این موضوع بسیار قابل توجه است. اگر از هم اکنون به فکر ۵ سال

شماره تماس: ۴۴۹۵۵۵۶۷ (۰۲۱) - ۳۶۲۸۱۱۱۲ (۰۳۵)
ایمیل: info@kaipod.ir

آینده باشید، استفاده از روش سنتی به تنهایی کافی نخواهد بود؛ بنا به مقتضیات زمان، نیاز به فرآیند شناسایی است که سریع و دقیق باشد؛ وقتی می‌گوییم سریع، به این معنی است که باید تهدیدهای جدید به طورآنی شناسایی و بلافاصله پاک‌سازی و حذف شوند. دقت و صحت تشخیص عاملی مهم در اجتناب از تشخیص False Positive است. eScan رویکرد فعال هوشمند را نسبت به روش سنتی توسعه داده است و این فناوری به عنوان اعتبارسنجی فایل نامیده می‌شود. در این مستند در مورد رویکرد اعتبارسنجی فایل مباحثی ارائه می‌شود.

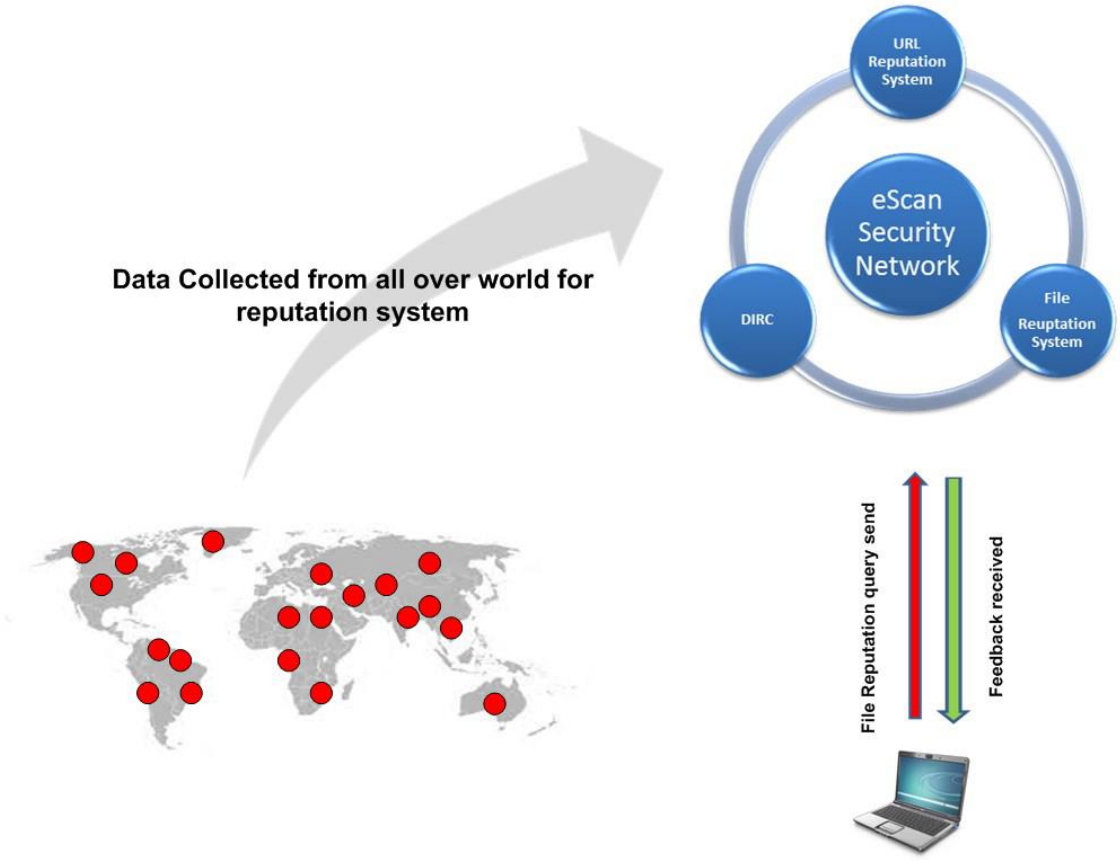
اعتبارسنجی، نه تنها یک عامل مهم امنیت سیستم بلکه بسیار ضروری تلقی می‌شود. اگر تعهدی برای محافظت از سیستم‌های کاربران به محض انتشار تهدیدهای جدید وجود دارد، لذا روش سنتی کافی نخواهد بود؛ پس چگونه eScan کاربران خود را در برابر تهدیدهای برخط در حال ظهور محافظت می‌نماید؟ پاسخ ساده است، eScan با استفاده از سیستم اعتبار فایل، فایل‌ها را به‌صورت برخط تجزیه و تحلیل، بررسی و شناسایی می‌کند که آیا فایل بدون آلودگی است و یا مشکوک؟. واقعیت این است که فرآیند اعتبارسنجی پویا است به طوری که ممکن است به سرعت تغییر یابد. از سوی دیگر افراد بداندیش جهت جلوگیری از سهولت تشخیص حمله‌ها، تهدیدها را به طور پراکنده انتشار می‌نمایند تا باعث حداکثر آسیب‌رسانی و دستیابی به اهداف بیش‌تری شوند. برای مقابله با این نوع از تهدیدها، کارشناسان eScan فناوری پیشرفته‌ای با عنوان خدمات اعتبارسنجی فایل را توسعه داده‌اند که در eScan، به عنوان شبکه امنیتی eScan و پایش فعال هوشمند رفتار فایل شناخته می‌شود، ترکیبی از دو روش که با تجمیع یک‌دیگر، در محدوده‌ی تمامل محصولات از SOHO تا سطح سازمانی قابل دسترس می‌باشد. اعتبارسنجی فایل eScan یک هوش تجمعی در مورد تشخیص بدافزار تلقی می‌شود، eScan بر اساس اعتبارسنجی برخط فایل، آن‌را برچسب‌گذاری کرده و سپس برای اقدام مناسب بر اساس اعتبار آن تصمیم‌گیری می‌نماید. (لطفاً برای اطلاعات بیش‌تر در مورد پایش فعال هوشمند رفتار فایل، به مستند HIPS مراجعه نمایید.)

۲- نحوه‌ی انجام فرآیند اعتبارسنجی

لابراتوار eScan از تمام محیط‌های رایانشی در سراسر جهان بازخورد دریافت می‌کند که در آن محصولات eScan بر اساس این بازخوردها سیستم اعتبارسنجی مبتنی بر ابر را پرس و جو کرده، داده‌ها بر روی سیستم اعتبارسنجی eScan تولید و سپس تجزیه و تحلیل شده، آن‌گاه بر اساس

شماره تماس: ۴۴۹۵۵۵۶۷ (۰۲۱) - ۳۶۲۸۱۱۱۲ (۰۳۵)
ایمیل: info@kaipod.ir

این تجزیه و تحلیل، پایگاه داده اعتبارسنجی بر روی ابر به‌رو رسانی می‌شود، که برای تمامی کاربران eScan قابل دسترسی خواهد بود.



پرس و جوها و پاسخ آن‌ها رویدادهای مهمی برای سیستم اعتبارسنجی می‌باشند. سیستم اعتبار قوی شامل میلیون‌ها نفر از کسانی که محصولات eScan را در سراسر جهان استفاده می‌کنند، به سیستم اعتبارسنجی درخواست ارسال می‌نماید و این گونه تجمیع داده‌ها بر روی سیستم اعتبارسنجی عملیاتی می‌شود که برای تمامی کاربران eScan طی مدت چند ثانیه در دسترس قرار خواهد گرفت. این رویکرد فعال در شناسایی تهدیدهای آنی ثابت شده است. یک سیستم اعتبارسنجی مؤثر می‌بایست اطلاعات را به طور کاملی جمع آوری و به سرعت آن را توزیع نماید. شبکه امنیتی eScan به صورت روزانه میلیون‌ها پرس و جوی اعتبارسنجی فایل را دریافت می‌کند و eScan بر اساس هوش تجمعی به آن‌ها پاسخ می‌دهد. در ادامه، مزایای سیستم اعتبارسنجی فایل به شرح زیر بیان می‌شود:

۱ – افزایش سرعت پویش فایل‌ها

شماره تماس: ۴۴۹۵۵۵۶۷ (۰۲۱) – ۳۶۲۸۱۱۱۲ (۰۳۵)
ایمیل: info@kaipod.ir

۲- کاهش تشخیص نادرست (False Positive)

۳- افزایش دقت و صحت شناسایی

۴- مستقل بودن از الگوهای شناسایی بدافزار سنتی

۵- مسدودسازی تهدیدهای روز صفرم (ناشناخته)

۶- استفاده‌ی کم‌تر از منابع سیستمی

موارد فوق، تعدادی از مزایای سیستم اعتبارسنجی فایل ابری بودند. eScan با جدیت می‌کوشد تا حفاظت بلادرنگ را با پیچیدگی کم‌تر ارائه نماید.

شماره تماس: ۴۴۹۵۵۵۶۷ (۰۲۱) - ۳۶۲۸۱۱۱۲ (۰۳۵)
ایمیل: info@kaipod.ir