به نام خداوند یکتا

مستند

سامانه‌ی پیشگیری از نفوذ مبتنی بر میزبان

آنتی‌ویروس eScan

(HIPS)

تاریخ انتشار: خردادماه ۱۳۹۵

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

فهـرسـت

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

۱- مقدمه

اگر به سال‌های گذشته بازگردیم، راهکارهای نسبتاً آسان‌تری به منظور شناسایی و رمزگشایی برنامه‌های مخرب با استفاده از الگوهای از پیش تعریف شده‌ی شناسایی انواع بدافزار شامل ویروس، کرم، تروجان و ... وجود داشت؛ اما امروزه روند تهدیدهای مبتنی بر بدافزار تغییر فراوانی یافته و تولیدکنندگان بدافزارها از فناوری‌های پیشرفته به منظور فریب دادن راه‌های سنتی پیشگیری از تهدیدهای مخرب مانند آنتی‌ویروس، دیواره‌آتش و ... استفاده می‌نمایند.

همان‌گونه که بیان شد، در گذشته روال شناسایی تولیدکنندگان آنتی‌ویروس بر مبنای تشخیص مبتنی بر الگوهای شناسایی بدافزار انجام می‌پذیرفت؛ این روش گرچه قابل اعتماد تلقی می‌گردید، اما روند آن به طور کامل به امضاهای ویروس وابسته بود. وجود این ضعف، راهکاری برای موفقیت تولیدکنندگان بدافزار در دور زدن حفاظت مبتنی بر امضاهای ویروس ایجاد نمود که بر این اساس اکثر تولیدکنندگان آنتی‌ویروس تلاش‌های خود را مبنی بر ایجاد و توسعه‌ی تکنیک‌هایی که منجر به کاهش این نوع حمله‌ها شود، آغاز نمودند. تولیدکنندگان آنتی‌ویروس الزام به نوآوری و سازگاری با تغییر فناوری را به منظور پیشگیری از آخرین تهدیدهای موجود و پیش‌تر بودن حداقل یک گام از تولیدکنندگان بدافزار در اولویت نقشه راه خود قرار دادند؛ بدین منظور برای مقابله با این نوع تهدیدها، فناوری HIPS یا سامانه‌ی پیشگیری از نفوذ مبتنی بر میزبان توسعه یافت.

راهکار امنیتی eScan در این زمینه، وجود قابلیت‌های سامانه‌ی پیشگیری از نفوذ مبتنی بر میزبان یا HIPS در محصولات eScan نسخه‌ی تحت شبکه و سازمانی است. این ویژگی‌ها به منظور شناسایی و مسدودسازی بلادرنگ برنامه‌های مخرب و ناخواسته، طراحی شده است.

۲- تعریف HIPS

روشی است که در آن از نرم‌افزارهای امنیتی به منظور حفاظت سامانه‌های حساس در مقابل حمله‌های مبتنی بر بدافزار استفاده می‌شود. سامانه‌ی پیشگیری از نفوذ مبتنی بر میزبان با شروع از لایه‌ی شبکه تا لایه‌ی برنامه‌های کاربردی، حفاظت چندلایه‌ای را در برابر بدافزارها، اجرایی می‌نماید. HIPS، مشخصه‌های ماشین میزبان و تمام رخدادهای مختلف به وقوع پیوسته‌ی آن را تجزیه و تحلیل نموده و فعالیت‌های مشکوک را شناسایی می‌نماید.

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

۳- علت برتری HIPS در مقایسه با IDS/IPS/AV/Anti-Spyware

همان‌گونه که می‌دانید سامانه‌ی تشخیص نفوذ (IDS) و سامانه‌ی پیشگیری از نفوذ در شبکه (IPS) تنها این قابلیت را دارند که بیان نمایند دقیقاً چه اتفاقی در شبکه رخ داده است. نقص عمده‌ی آن‌ها در این است که نمی‌توانند از وقوع حمله جلوگیری نمایند؛ به عبارت دیگر IDS و IPS برای اهداف بازیابی پس از وقوع حمله و اعلام هشدار نفوذ مناسب بوده و توانایی پیشگیری از وقوع حمله را ندارند.

تولیدکنندگان آنتی‌ویروس و ضدجاسوس‌افزار نیز، به دستاوردهای شگرفی در حوزه‌ی پویش و شناسایی انواع بدافزارها نائل شده‌اند که هنوز روال این کار به طور گسترده‌ای مبتنی بر الگوهای شناسایی بدافزار (امضاهای ویروس) انجام می‌شود که نقص قابل توجهی برای محافظت در مقابل آخرین تهدیدها محسوب می‌شود؛ به این دلیل که در صورت عدم به‌روزرسانی بلادرنگ امضاهای ویروس، شناسایی طیف عمده‌ای از بدافزارهای جدید امکان‌پذیر نمی‌باشد. در واقع، آنتی‌ویروس و ضدجاسوس‌افزار تنها قابلیت پویش و توقف انتشار بدافزارهای شناخته شده را دارند و عدم توانایی شناسایی تهدیدهای روز صفرم توسط آن‌ها، جزو نقاط آسیب‌پذیریشان تلقی می‌گردد.

HIPS از راه‌های متفاوت با موارد ذکر شده‌ی فوق، به محافظت از میزبان اقدام می‌نماید. منظور ما این نیست که IDS، IPS، آنتی‌ویروس و ضدجاسوس‌افزار، مورد نیاز نیستند؛ بلکه باید با اجرای محافظت چندلایه، امنیتی جامع را ایجاد نمود؛ بدین‌گونه که در صورت بروز رخداد امنیتی در یک لایه، لایه‌های دیگر قابلیت پیشگیری از نفوذ را فراهم نمایند.

۴- HIPS در نسخه eScan 11

در نسخه‌ی eScan 11، HIPS در لایه‌های شبکه، انتقال و برنامه‌های کاربردی پیاده‌سازی می‌شود. پیاده‌سازی در لایه‌های شبکه و انتقال به صورت پویا و در لایه‌ی برنامه‌های کاربردی به صورت ایستا انجام می‌شود. درایورهای دیواره‌ی آتش eScan با توجه به قابلیت‌های تجزیه و تحلیل شبکه پیاده‌سازی شده‌ی در آن، HIPS را در لایه‌ی شبکه فراهم می‌نماید. فناوری MWL موجود در eScan یا Microworld Winsock Layer که نوعی فناوری ابداع شده توسط شرکت MicroWorld است، راه تشخیص ویروس‌ها و تروجان‌ها را تغییر داده است، به این شکل که برخلاف دیگر آنتی‌ویروس‌های موجود، این آنتی‌ویروس، تروجان‌ها و حمله‌های ویروسی را در لایه‌ی Winsock

تشخیص می‌دهد و از تأثیرگذاری ویروس و تروجان بر روی برنامه‌ها و رسیدن آن‌ها به لایه Application ممانعت به عمل می‌آورد. این فناوری، علاوه بر بررسی و آنالیز مداوم ترافیک ارسالی و دریافتی از مرورگرها، کلاینت‌های رایانامه و...، HIPS را در سطح لایه انتقال فراهم می‌نماید. هم‌چنین در لایه کاربرد، پویش فعال هوشمند که به طور ایستا فایل‌های اجرایی را از نظر آلودگی بررسی می‌کند، به نوعی عملکرد HIPS را ارائه می‌نماید.

۵- HIPS در نسخه eScan 14

HIPS در نسخه‌ی eScan 14، مشابه نسخه‌ی eScan 11 می‌باشد با این تفاوت که برخی لایه‌های امنیتی به آن افزوده شده است. به عنوان نمونه، دیواره‌ی آتش eScan وظیفه‌ی پایش ارتباطات همزمان از هر نوع میزبان و مسدودسازی پویش درگاه را انجام می‌دهد؛ این موضوع قسمتی از وظایف و قابلیت‌های HIPS می‌باشد که به طور قابل توجهی در مقابله با حمله‌های گسترده در شبکه الزامی تلقی می‌گردد. از طرف دیگر در لایه کاربرد، هر ۲ مقوله‌ی پایش پویا و ایستای فایل‌های اجرایی، پیاده‌سازی می‌شود که در این فرآیند، شناسایی و مسدودسازی ۹۰%از بدافزارهای ناشناخته و تهدیدهای روز صفرم، بر اساس آنالیز رفتار الگوهای برنامه‌ها توسط eScan تضمین می‌شود. هر فایل اجرایی که بر روی ماشین میزبان اجرا می‌گردد، به طور مداوم در سطح هسته‌ی سیستم عامل و برخی اوقات نیز در سطح کاربر پایش می‌شود. این بدین معنی است که در هر فراخوانی فایل اجرایی، فرمت دودویی فایل‌های اجرایی قابل حمل (Portable Executable) ایجاد و پس از آنالیز، رتبه‌بندی می‌شوند. فراخوانی‌های عمومی که توسط برنامه‌های کاربردی انجام می‌شود، منجر به رتبه‌بندی نمی‌گردد؛ اما هر نوع فراخوانی که در ماهیت مشکوک و آلوده تشخیص داده شود، در رتبه‌ی بالاتری قرار می‌گیرد، موارد زیر جزو معیارهای آنالیز می‌باشند:

- شناسایی محیط‌های ماشین مجازی (مجازی‌سازی)
- تغییر کلیدهای رجیستری حساس
- شناسایی محیط اشکال‌زدایی
- فراخوانی به منظور تغییر مجوزها و یا سطح دسترسی‌ها
- ارتباط با یک عامل ناشناخته‌ی بیرونی

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

- تغییرات فایل‌های سیستمی (کتابخانه‌ای، پایگاه داده سیستمی و ...)
- تغییرات در سطح حافظه
- ایجاد نخ پردازشی در کد دودویی از راه دور و ...

هنگامی که تجزیه و تحلیل ترکیبی از نتایج بدست آمده به میزان آستانه مشخصی برسد، فرمت دودویی به عنوان فرآیند مشکوک تعیین و اجرای فایل متناظر، به حالت تعلیق در می‌آید. در همین لحظه نیز، پایگاه داده مرتبط که تغییرات مجموعه فایل‌های اجرایی را ثبت می‌کند، به‌روز می‌گردد. به‌روزرسانی‌های eScan به طور معمول جهت تهیه و تکمیل لیست‌های پذیرش (Whitelist) فایل‌های اجرایی امن و فعالیت‌های شناخته شده‌ی آن‌ها ارائه می‌شود. لیست پذیرش اجرای فایل‌های قانونی و بدون آلودگی را تضمین می‌نماید. HIPS پویای نسخه‌ی eScan 14، در سطح برنامه‌های کاربردی، ۹۰% بدافزارهای ناشناخته را شناسایی و مسدود می‌نماید.

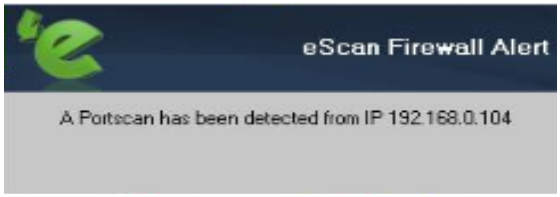
۶- نحوه‌ی پیکربندی HIPS در محصولات eScan

تیم eScan مناسب‌ترین تنظیمات پیکربندی را برای فناوری HIPS عملیاتی نموده است. به طور پیش فرض، HIPS در محصولات eScan فعال می‌باشد. در واقع این تنظیمات، تجمیعی از دیواره آتش eScan و فناوری پایش رفتار فعال هوشمند به همراه امنیت نقطه نهایی است. تنظیمات HIPS در حالت تعاملی قرار دارند، به این معنی که هرگاه تهدید ناشناخته‌ای شناسایی شد، پیغام هشداری برای کاربر نمایش داده می‌شود. هم‌چنین با استفاده از روش‌های خاص، دقت و صحت شناسایی فعالیت‌های مشکوک افزایش و در راستای آن، تشخیص نادرست (False Positive) کمینه شده است. در صورت شناسایی فعالیت مشکوک توسط HIPS، محصولات eScan هشداری مشابه شکل زیر نمایش می‌دهند:

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

همان‌گونه که در تصویر ارائه شده مشاهده می‌شود، HISP از تغییرات در رجیستری توسط یک برنامه کاربردی مشکوک جلوگیری می‌کند. در شکل زیر نیز، قابلیت دیگر HIPS در مسدودسازی فرمت‌های دودویی فایل‌های اجرایی نمایش داده شده است:

همچنین، در شکل زیر قابلیت مسدودسازی پویش درگاه توسط دیواره آتش eScan ارائه شده است:



لذا، فناوری HIPS موجود در eScan، با تجمیع تمهیدات امنیتی، راهکاری جامع را برای محیط رایانشی امن فراهم می‌نماید.

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