چالش‌های فـنـاوری‌هـای استفاده شده در

محصولات ضدبدافزار

شبکه گستر
شرکت مهندسی شـبکه گسـتر

عنوان سند: چالش‌های فناوری‌های استفاده شده در محصولات ضدبدافزار
شناسه سند: SPT-A-0139-00
تهیه‌کننده: گروه تحقیق و توسعه، شرکت مهندسی شبکه گستر
آخرین بازنگری: ۱۳ تیر ۱۳۹۶

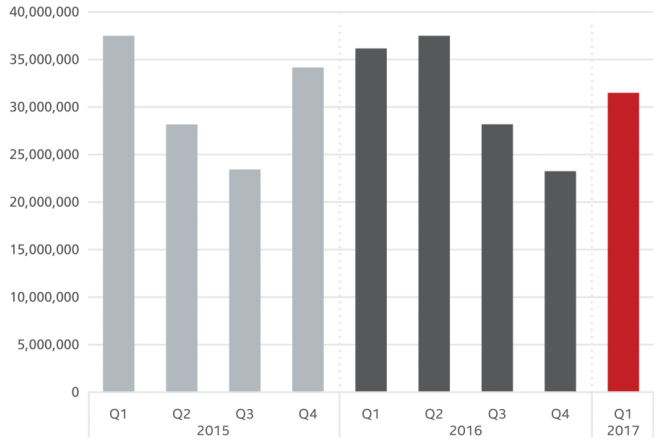
خلاصه مدیریتی

کمال در محصولات ضدبدافزار ارائه نمودن راهکاری است که با سربار اجرایی کم و با حداقل تأثیر بر روی عملکرد کاربر، بهترین محافظت را از دستگاه در برابر بدافزارها فراهم کند.

بر کسی پوشیده نیست که حفاظت از نقاط پایانی در برابر بدافزارهای پیشرفته و مخرب امروزی نه تنها آسان نیست بلکه در بسیاری از سازمان‌ها یکی از اصلی‌ترین دغدغه‌های مدیران ارشد امنیت محسوب می‌شود. سالهاست که متخصصان در جهت یافتن تعادل میان پوشش مناسب تهدیدات و کاهش تأثیر منفی بر عملکرد کاربر در محصولات ضدبدافزار در تلاش هستند.

شناسایی مبتنی بر امضاء[۱] یکی از فناوری‌های شناخته شده در مقابله بدافزارهاست که در آن از تطبیق دادن الگوها جهت شناسایی فایل‌های مخرب استفاده می‌شود. این بدان معناست که در ابتدا باید نمونه‌ای از بدافزار به دست سازنده ضدبدافزار برسد تا پس از انجام بررسی، امضای آن را تولید کرده و به دستگاه‌های حفاظت شده توسط آن محصول ارسال کند. مشخص است که در این روش نویسنده بدافزار یک گام جلوتر از محصول ضدبدافزار است.

بر اساس آمار ارائه شده توسط شرکت McAfee، در سه ماهه نخست سال ۲۰۱۷ میلادی به طور میانگین در هر یک ثانیه، بیش از چهار بدافزار منحصربفرد جدید در سطح جهان منتشر شده است.



شکل ۱: تعداد بدافزارهای منحصر بفرد جدید

واضح است که با این حجم عظیم از بدافزارها نمی‌توان صرفاً با بکارگیری فناوری شناسایی بر اساس امضاء مقابله کرد.

ظهور و پیشرفت فناوری‌های محافظت از نقاط پایانی در ۵ سال گذشته مزایای متعددی را به همراه داشته است. از جمله این پیشرفت‌ها می‌توان به کاهش اندازه فایل‌های به‌روزرسانی و بهبود محافظت در دسته‌های خاصی از بدافزارها اشاره کرد.

از جمله فناوری‌های شناسایی جدید نیز می‌توان به موارد زیر اشاره کرد:

- **یادگیری ماشین**[۲] – در این روش با استفاده از مدل‌های ریاضی میزان مخرب بودن پروسه ناشناخته مورد بررسی قرار می‌گیرد.
- **کنترل برنامه**[۳] – که در آن اجرای هر گونه برنامه و پروسه غیرمجاز بر روی نقطه پایانی محدود می‌شود.
- **محدودسازی یا مهار برنامه**[۴] – در این روش، فایل‌های ناشناخته توسط محصول ضدبدافزار و در نتیجه بالقوه مخرب در بستری قرنطینه و جدا از سایر پروسه‌های سیستم اجرا می‌گردد تا در صورت تشخیص مخرب بودن آن، محصول نسبت به متوقف نمودن آن اقدام کند.

---

[۱] Signature
[۲] Machine Learning
[۳] Application Control
[۴] Application Isolation

- **تجزیه و تحلیل رفتار**[۵] – این روش نوعی نظارت مبتنی بر قاعده را فراهم می‌کند. رفتار برنامه‌ها و پروسه‌ها مطابق با شاخص‌هایی رصد شده و در صورت لزوم مسدود یا حذف می‌شوند.
- **ضدبهره‌جو**[۶] – که با حفاظت از حافظه از سوءاستفاده از ضعف‌های امنیتی سیستم عامل و نرم‌افزارهای نصب شده بر روی دستگاه جلوگیری می‌کند. این فناوری نقطه پایانی را در برابر حملات سر ریز حافظه[۷] و حملاتی که از آسیب‌پذیری‌های نرم‌افزارها سوءاستفاده می‌کنند، محافظت می‌کند.

مدیران امنیت سازمان باید راهکارهای جدید محافظت در مقابل بدافزارها را با در نظر گرفتن وجه تمایز روش‌ها و اینکه راهکارهای مختلف چگونه می‌توانند به یک برنامه پیشگیری از بدافزار تبدیل شوند، ارزیابی کنند.

در جدول ۱ فناوری‌های ضدبدافزاری اشاره شده و تأثیر آنها بر اکثر سازمان‌ها نمایش داده شده است.

فناوری	پوشش تهدیدات	نیاز به راهبر	تأثیر بر عملکرد کاربر
امضاء	کم	کم	کم
یادگیری ماشین	متوسط	کم	کم
کنترل برنامه	بالا	بالا	بالا
محدودسازی برنامه	متوسط	بالا	بالا
تجزیه و تحلیل رفتاری	بالا	متوسط	کم
ضدبهره‌جو	متوسط	کم	کم

جدول ۱: میزان تأثیر فناوری‌های شناسایی بدافزار بر سازمان‌ها

فناوری‌های فوق هر کدام دارای قابلیت‌هایی متفاوت و البته محدودیت‌هایی هستند. عملکرد برخی از آنها ممکن است یکسان به نظر برسد که با توضیحات ارائه شده در این مقاله تفاوت آنها آشکار می‌شود.

بسیاری از سازندگان محصولات ضدبدافزار اغلب این فناوری‌ها را به عنوان راهکاری بی‌عیب و نقص برای پیشگیری از آلوده شدن به بدافزارها معرفی می‌کنند. هر چند که در عمل هم، ترکیب فناوری‌های اشاره شده با یکدیگر موجب حفاظت گسترده‌ای در برابر بدافزارها می‌شود.

شایان ذکر است حتی در صورت بهره‌گیری از تمامی فناوری‌های شناسایی همچنان باید به آموزش کاربران به عنوان یکی از عوامل بسیار مؤثر در مقابله با بدافزارها توجه شود. برنامه‌های آگاهی‌رسانی امنیتی نقش مهمی در افزایش دانش کاربران و محدود شدن فعالیت‌ها و رفتارهای آسیب‌پذیر آنها دارند.

---

۵ Behavioral Analysis

۶ Anti-exploit

۷ Buffer Overflow

فناوری امضاء

اکثر محصولات ضدبدافزار و همینطور بسیاری از محصولات امنیت وب[۸]، امنیت ایمیل و تجهیزات موسوم به مدیریت یکپارچه تهدید[۹] از فناوری امضاء به‌منظور شناسایی تهدیدات استفاده می‌کنند. این فناوری بخشی اساسی در حفاظت از نقطه پایانی محسوب می‌شود.

هر چند که در اوایل ظهور محصولات ضدویروس، فناوری مذکور راهکاری قابل قبول محسوب می‌شد اما اکنون سالهاست که مشخص شده روش شناسایی صرفاً مبتنی بر امضاء نرخ موفقیت پایینی در شناسایی بدافزارهای پیچیده و جدید امروزی دارد. چرا که بر طبق ماهیت آن، فقط می‌تواند با بدافزارهای شناخته شده و گونه‌های ساده آنها مقابله کند.

دور زدن این فناوری توسط نویسندگان بدافزار کار چندان دشواری نیست. توسعه امضاء توسط سازنده ضدبدافزار نیز خود زمانبر است. ضمن اینکه این فناوری نیاز به به‌روزرسانی مداوم نقطه پایانی دارد. در برخی محصولات، از ابر[۱۰] برای دریافت آخرین اطلاعات مربوط به اعتبار فایل‌های ناشناخته استفاده می‌شود. اما دسترسی به ابر فقط از طریق اینترنت امکان‌پذیر بوده و در صورت عدم اتصال نقطه پایانی به اینترنت در مقابل بدافزارها آسیب‌پذیر خواهد بود.

اما روش شناسایی مبتنی بر امضاء و اکتشاف[۱۱] مزایایی نیز دارد:

- **حفاظت پیشگیرانه در مقابل بدافزارهای شناسایی شده** – پویش فایل‌ها پیش از اجرا شدن، از آلوده شدن نقطه پایانی به بدافزار جلوگیری می‌کند (البته با فرض وجود امضای شناسایی تهدید). ضمن اینکه نیازی به استفاده فراوان از منابع سیستم یا فناوری‌های ردیابی پیچیده برای مقابله با بدافزارهای شناخته شده نیز ندارد.
- **نرخ شناسایی نادرست[۱۲] بسیار پایین** – منظور از شناسایی نادرست برخورد محصول ضدبدافزار با فایلی پاک و غیرآلوده به عنوان یک فایل مخرب است. نرخ پایین شناسایی نادرست برای راهکارهای امنیتی که به‌صورت خودکار از نقاط پایانی حفاظت می‌کنند بسیار حائز اهمیت است. بسیاری از محصولات ضدبدافزار حداقل یک بار حذف اشتباه یکی از فایل‌های کلیدی Windows و از کار انداختن سیستم‌ها را در کارنامه خود دارند.
- **جلوگیری از شناسایی نادرست در روش‌های سختگیرانه** – استفاده از امضاء می‌تواند به کاهش شناسایی نادرست در روش‌های سختگیرانه کمک کند. زمانی که از این روش برای محافظت از فایل‌های سالم استفاده شود، شناسایی مبتنی بر امضاء می‌تواند به عنوان یک افزونه قوی به راهکار امنیتی اضافه شود.

> **علیرغم وجود مزایایی در روش شناسایی بر اساس امضاء، محافظت از نقاط پایانی تنها با این فناوری توصیه نمی‌شود.**

فناوری یادگیری ماشین

واقعیت آن است که فناوری یادگیری ماشین پتانسیل آن را دارد که نقش مهمتری در صنعت محافظت از نقاط پایانی ایفا کند. برخی از سازندگان محصولات ضدبدافزار از موتورهای یادگیری ماشین تحت نظارت برای پردازش تعداد زیادی از فایل‌های مخرب استفاده می‌کنند. الگوریتم‌های این فناوری‌ها می‌توانند به‌صورت محلی بر روی نقاط پایانی و یا در ابر اجرا شده و فایل‌ها را از لحاظ سالم و یا مخرب بودن مورد ارزیابی قرار دهند.

---

[۸] Secure Web Gateways (SWG)
[۹] Unified Threat Management (UTM)
[۱۰] Cloud
[۱۱] Heuristics
[۱۲] False Positive

مزایای این نوع شناسایی عبارتند از:

- **عدم نیاز به امضاء** – در این فناوری بجای پایگاه داده سنتی امضاء از مدل‌های ریاضی استفاده می‌شود. موضوعی که سبب حذف نیاز به فضای ذخیره‌سازی و حافظه زیاد و همچنین چالش‌های به‌روزرسانی محصولات ضدبدافزار می‌شود.
- **شناسایی بدافزارهای جدید با استفاده از مدل‌های موجود** – مدل‌های پیش‌بینی شده می‌توانند از نتایج آماری برای شناسایی بدافزارهایی که هنوز بررسی نشده‌اند، استفاده کنند.
- **عدم وابستگی به اینترنت** – در بسیاری از محصولات مجهز به این فناوری، این امکان وجود دارد که تمامی پویش‌ها به‌صورت محلی و بر روی دستگاه انجام شود و مستلزم جستجوی مبتنی بر ابر نباشد.

اما مدیران ارشد امنیت باید نسبت به محدودیت‌ها و ضعف‌های فعلی یادگیری ماشین به عنوان یک منبع ضدبدافزار مستقل آگاه باشند.

استفاده از روش‌های بسته‌بندی[۱۳] و رمزنگاری[۱۴] کد، توسط نویسنده بدافزار، توانایی بررسی با این فناوری را محدود می‌کند. راهکارهایی که صرفاً از مدل‌های پیش‌بینی شده یادگیری ماشین بر روی نقاط پایانی استفاده می‌کنند، می‌توانند خطراتی را به سیستم تحمیل کرده و در نتیجه آنها نویسندگان بدافزار را قادر به اجرای امور زیر کنند:

۱. مدل رفتار شناسایی را ارزیابی کنند،
۲. کدهای مخرب خود را سازگار کنند.

هر چند که انتظار می‌رود میزان شناسایی نادرست در فناوری‌های محصولات ضدبدافزار حداقل باشد اما این امر نیز اجتناب‌ناپذیر است که فایل‌هایی وجود داشته باشند که خیلی نزدیک به فایل‌های سالم یا مخرب بوده و در نتیجه باعث بروز خطای شناسایی نادرست در محصول ضدبدافزار شوند. محصولات ضدبدافزاری که صرفاً بر روی شناسایی از طریق یادگیری ماشین تمرکز کرده‌اند نرخ شناسایی نادرست بالایی دارند. معمولاً محصولات ضدبدافزار برای رفع شناسایی نادرست از روش‌های زیر استفاده می‌کنند:

- قرار دادن فایل‌های سالم در فهرست استثنا[۱۵]
- جستجو در پایگاه داده ابر در خصوص فایل‌های مشکوک

برای سازمان‌ها ممکن است ایجاد یک فهرست استثناء در شرایطی که مدل‌های ریاضی یادگیری ماشین به ندرت به‌روز می‌شوند، مشکل و دشوار باشد.

توصیه‌ها

- نادیده گرفتن ادعاهای برخی از فروشندگان محصولات ضدبدافزار درباره بی‌فایده بودن استفاده از امضاء
- ارتقاء به آخرین نسخه محصول امنیت نقاط پایانی؛ نسخه‌های جدید، کمتر مبتنی بر امضاء بوده و از فناوری‌های اضافه دیگری بهره می‌برند.
- اطمینان از اینکه سازنده، یک گردش کاری جامع برای عدم شناسایی و شناسایی نادرست در اختیار داشته باشد. (راهکارهایی که قابلیت اضافه و کم کردن فایل‌ها به فهرست استثناء و فهرست سیاه را به‌صورت دستی داشته باشند.)

---

[۱۳] Packing
[۱۴] Encryption
[۱۵] Whitelist

فناوری کنترل برنامه / مستثنی کردن

در فناوری کنترل برنامه، تمامی برنامه‌ها یا پروسه‌های مستثنی نشده، غیرقابل اطمینان بوده و از اجرای آنها جلوگیری می‌شود. در این رویکرد، پروسه‌های غیر قابل اطمینان به صورت کامل مسدود شده و یا در محصولاتی که تصمیم‌گیری پویا نیز فراهم می‌کنند، تحت حفاظت یا نظارت بیشتری اجرا می‌شوند.

به عنوان یکی از فناوری‌های ضدبدافزار، کنترل برنامه نیز دارای نقاط قوتی است:

- **محافظت قوی** – اگر قواعد سختگیرانه‌ای استفاده شود، کنترل برنامه، محافظتی قوی را در برابر بدافزارها فراهم می‌کند. به خصوص اگر در کنار فناوری‌هایی که مانع از آلوده شدن پروسه‌های سالم می‌شوند اجرا شود.
- **کاهش سربار سیستم** – راهکارهای کنترل برنامه تأثیر ناچیزی بر روی منابع نقاط پایانی دارند.
- **پشتیبانی گسترده از بسترهای از رده خارج** – فناوری کنترل برنامه می‌تواند برای محافظت از سیستم‌های عامل پشتیبانی نشده یا بدون اصلاحیه مورد استفاده قرار گیرد. برای مثال دستگاه‌های قدیمی با یکی از نسخه‌های 2003 یا XP سیستم عامل Windows می‌توانند با این فناوری – ترجیحاً در کنار یک راهکار محافظت از حافظه – مورد حفاظت قرار گیرند.
- **بدون نیاز به امضای فایل و به‌روزرسانی** – کنترل برنامه نیازی به امضای فایل‌ها یا به‌روزرسانی‌های مداوم ندارد. با این وجود در موارد پیشرفته‌تر می‌توان در محیط‌های پویا از اعتبار فایل‌ها استفاده کرد که البته این روش مستلزم دسترسی به پایگاه داده اعتبار فایل‌هاست که اغلب نیاز به اینترنت دارد.
- **مؤثر در برابر تمامی برنامه‌های ناخواسته** – کنترل برنامه می‌تواند از اجرای آن دسته از برنامه‌هایی که به لحاظ فنی مخرب نیستند ولی ممکن است امنیت را به خطر بیندازند، جلوگیری کند. این دسته‌بندی شامل برنامه‌های دسترسی از راه دور[۱۶]، همگام‌سازی فایل[۱۷] و سفیرهای اشتراکی[۱۸] می‌شود.

ملاحظات متعددی وجود دارد که مدیران امنیت و ریسک سازمان باید در هنگام استقرار گسترده نهایی کنترل برنامه در نظر بگیرند. این رویکرد تأثیرات قابل توجهی بر عملکرد کاربران و نقاط پایانی دارد.

کنترل برنامه می‌تواند برای دستگاه‌هایی با عملکرد ثابت مانند سرورها که نرم‌افزارها و گردش‌های کاری[۱۹] آنها قابل پیش‌بینی است، بسیار موفق باشد. سیستم‌های کاربرانی با سبک کاری تعریف شده (برای مثال کارمندان مرکز تماس) نیز برای استفاده از این روش مناسب هستند. برای انواع دیگر کاربران مانند کارکنان سیار یا برنامه‌نویسان، ممکن است روش پیش‌فرض جلوگیری از اجرا مناسب نباشد، مگر آنکه گردش‌های کاری بتوانند تاخیر تایید نرم‌افزارهای شناخته نشده یا غیرقابل اطمینان را به حداقل برسانند. از لحاظ عملیاتی، مدیریت استثنائات منابع غیرقابل اطمینان، می‌تواند سربار قابل ملاحظه‌ای را تحمیل کند. سازمان‌ها باید برای چنین سربارهایی برنامه‌ریزی کرده و ابزارهای مورد نیاز را در اختیار راهبران شبکه قرار دهند. چنین ابزارهایی به راهبران شبکه امکان می‌دهند تا فرآیند مدیریت استثنائات را ساده‌تر انجام داده و تصمیماتی صحیح را در حداقل زمان بگیرند. اجازه دادن به منابع مورد اطمینان جهت ایجاد تغییرات، تعداد استثنائات لازم را کاهش می‌دهد.

مدیریت دقیق قواعد کنترل برنامه در محیط‌های پویا از لحاظ عملیاتی پیچیده است. راهکارهای پیشرو با اجازه دادن به ناشران قابل اعتماد، مکان‌ها، نصاب‌ها و کاربران جهت نصب نرم‌افزار و به‌روزرسانی خودکار قواعد کنترل نرم‌افزار، این مسئله را حل کرده‌اند اما این قواعد ممکن است موجب به خطر افتادن امنیت شوند.

قدرت کنترل نرم‌افزار به عنوان یک فناوری حفاظت در برابر بدافزارها، به قاعده و فناوری‌های اضافی نصب شده بر روی نقطه پایانی بستگی دارد. نویسندگان بدافزارها می‌توانند بدافزارهای خود را با استفاده از گواهی[۲۰] سرقت شده، امضای دیجیتالی کنند و یا از برنامه‌های مشروع در حافظه بهره‌جویی کنند و بدافزارهای بدون فایل را اجرا کنند. در نتیجه قابلیت کنترل برنامه در برابر حملات پیچیده کاهش می‌یابد.

---

[۱۶] Remote Access
[۱۷] File Sync
[۱۸] Share Agent
[۱۹] Workflows
[۲۰] Certificate

مدیران امنیت باید به دقت به ادعاهای فروشندگان درباره ویژگی‌های کنترل برنامه توجه کنند. تنها وجود امکانی برای قرار دادن برنامه‌ها با نام و مسیر آنها در فهرست سیاه یک قابلیت کنترل برنامه قوی محسوب نمی‌شود.

فناوری محدودسازی برنامه

در فناوری محدودسازی برنامه، پروسه‌ها و محتوای بالقوه خطرناک با محدودسازی آنها از مابقی سیستم اجرا می‌شوند.

مدیران امنیت می‌بایست نقاط قوت محدودسازی برنامه را مد نظر قرار داده و از دسترسی بدون محدودیت کاربران پرهیز کنند. مهار برنامه از دسترسی کاربران به سایت‌های آلوده، دریافت فایل‌های مخرب و یا پردازش محتوای مضر جلوگیری نمی‌کند. در سختگیرانه‌ترین حالت مهار برنامه، فایل‌های مشکوک در یک محیط قرنطینه امن اجرا می‌شوند.

برخی از راهکارها محیط محدودسازی شده را از بین می‌برند و یا به طور منظم سیستم را به وضعیت سالم باز می‌گردانند. برخی دیگر هنگامی که رفتار مخرب در محیط محدودسازی شده شناسایی شد، این کار را انجام می‌دهند و سیستم را به وضعیت سالم باز می‌گردانند.

محدودسازی به عنوان یک روش ارزشمند در جهت مقابله با عدم شناسایی بدافزارها می‌باشد. کد مشکوک در یک محیط در ظرف[۲۱] اجرا می‌گردد. بنابراین علیرغم اجرای کد، به دلیل در قرنطینه بودن آن احتمال آسیب رساندن به سیستم کاهش می‌یابد. سازمان‌هایی که به استقرار محدودسازی برنامه‌ها علاقمند هستند باید موارد زیر را در نظر بگیرند:

- **تأثیر بر کاربر** – فناوری‌های مهار نرم‌افزار تعامل بین محیط‌های محدودسازی شده و نشده را محدود می‌کند که این امر ممکن است بر عملکرد کاربر تأثیر منفی بگذارد.
- **تأثیر عملیاتی** – راهبران شبکه باید سایت‌های مورد اطمینان، برنامه‌ها، مکان فایل‌ها و قواعد را برای انتقال فایل‌ها بین بخش‌های مختلف با سطوح اطمینان متفاوت مدیریت کنند.
- **عدم پشتیبانی از نرم‌افزار** – محیط محدودسازی شده ممکن است از تمامی نرم‌افزارها و نگارش‌های مختلف پشتیبانی نکند.
- **نیاز به سخت‌افزارهای خاص** – برخی از راهکارهای محدودسازی نرم‌افزار برای پیاده‌سازی موفقیت‌آمیز به نوع خاصی از پردازنده یا مقدار حافظه بیشتری نیاز دارند.
- **تفاوت‌های زیاد در پیاده‌سازی** – راهکارها از لحاظ گزینه‌های کنترل قواعد بسیار متفاوت هستند. کنترل قواعد می‌تواند شامل مواردی مانند فناوری‌هایی که برای محدودسازی استفاده می‌شود، پشتیبانی از چندین ناحیه، پشتیبانی از نرم‌افزارها، مدیریت و گزارش‌گیری و تجزیه و تحلیل رفتار بدافزار در قرنطینه امن شود.
- **محافظت محدود** – نرم‌افزارهایی که در محیط خارج از ظرف اجرا می‌شوند توسط راهکار مهار نرم‌افزار محافظت نمی‌شوند. برخی از فروشندگان راه‌حل‌های خود را با ارائه فناوری "شناسایی و پاسخ نقطه پایانی[۲۲]" در داخل و خارج محیط آغاز کرده‌اند.

توصیه‌ها

- آمادگی بخش فناوری اطلاعات به افزایش درخواست‌ها به خصوص در ابتدای پیاده‌سازی این فناوری در شبکه. برای استثنائات از یک گردش کاری مناسب و مستند استفاده شود. در صورت استفاده از قواعد پیش‌فرض جلوگیری از اجرا، سربار اجرایی اجتناب‌ناپذیری به وجود خواهد آمد.

---

[۲۱] Contained

[۲۲] Endpoint Detection and Response (EDR)

- قاعده پیش‌فرض جلوگیری از اجرا فقط به گروهی از سیستم‌هایی که گردش‌های کاری قابل پیش‌بینی دارند اعمال شود. وضعیت سایر کاربران مانند برنامه‌نویسان که الزامات سختگیرانه کمتری برای آنها وجود دارد در حالت رصد[۲۳] قرار گیرد تا رفتارهای مشکوک شناسایی شوند.
- نیازمندی‌های سخت‌افزاری مورد نیاز سنجیده و بررسی شده و اطمینان حاصل شود که محصول انتخابی از تمامی نرم‌افزارهای کلیدی مورد استفاده در محیط، پشتیبانی کامل می‌کند.
- پیاده‌سازی فناوری محدودسازی نرم‌افزار برای گروهی از کاربران که بیشتر در معرض خطر هستند، برنامه‌ریزی شود و از استقرار آن بر روی همه کاربران پرهیز شود.

تجزیه و تحلیل رفتاری

تجزیه و تحلیل رفتاری در محافظت از نقطه پایانی چندین نقطه قوت دارد؛ حتی اگر به عنوان یک فناوری محدودسازی مورد استفاده قرار گیرد. چنین تجزیه و تحلیلی می‌تواند در مقابل فعالیت‌های حمله، محافظت در لحظه‌ای را فراهم کند. این فناوری، علاوه بر فراهم نمودن شناسایی در لحظه می‌تواند برای درک بهتر رفتار نرم‌افزار، تمام رفتار یا پروسه‌های مشکوک آن را رصد کنند.

برای مثال، بر روی دستگاه کاربری که اطلاعات را از طریق ایمیل دریافت می‌کند طبیعی است که یک پروسه Outlook.exe و یک پروسه از Word.exe اجرا شود. اما هنگامی که Word.exe با اینترنت ارتباط برقرار کند یا پروسه‌های دیگر را ایجاد کند، رفتار آن بیشتر و بیشتر مشکوک می‌شود.

راهکارهای امنیت نقاط پایانی با استفاده از تجزیه و تحلیل رفتاری می‌توانند شناسایی و مسدود کردن نرم‌افزارهای مخرب ناشناخته را بدون نیاز به پویش و بررسی پرهزینه و در نتیجه اشغال بخش زیادی از منابع سیستم انجام دهند. این نوع شناسایی، کد بدافزار را بررسی نمی‌کند بلکه رفتار آن را مورد ارزیابی قرار می‌دهد. این بدین معنی است که سازندگان محصول با توجه به این نوع تشخیص، به پایگاه داده‌ای از امضاء یا پویش فایل نیاز ندارند. تجزیه و تحلیل رفتاری می‌تواند چندین مرحله از زنجیره حمله به سازمان نظیر انتقال فایل‌های نصبی، توزیع در بستر شبکه و اجرای برخی از بهره‌جوها را شناسایی و آنها را خنثی کند.

برخی ملاحظاتی که در رابطه با پیاده‌سازی تجزیه و تحلیل رفتار به عنوان یک فناوری محافظت در مقابل بدافزارها باید به آنها توجه داشت عبارتند از:

- **پتانسیل نرخ بالای شناسایی نادرست** – بین رفتارهای مخرب و سالم رابطه نزدیکی وجود دارد بنابراین احتمال شناسایی نادرست در هر فناوری مبتنی بر رفتار وجود دارد. هر رفتار در ظاهر مشکوک لزوماً به معنای مخرب بودن پروسه اجرا کننده آن نیست. تغییر هسته سیستم‌های عامل و فراخوانی برخی توابع که به نظر مخرب می‌رسند لزوماً به معنای غیرمجاز بودن پروسه اجرا کننده نیست.
- **شناسایی در حین اجرا بجای جلوگیری قبل از اجرا** – بدافزار پیچیده موجب آن می‌شود که قواعد پاکسازی به آن اعمال نشده و در بهترین حالت بجای جلوگیری از اجرای آن بدافزار، شناسایی در زمان اجرا شدن آن انجام شود.
- **نیاز به تنظیم، تخصص و به‌روزرسانی** – محافظت مبتنی بر رفتار در سازمان‌ها نیازمند آن است که قواعد به درستی انتخاب شوند، اقدامات پس از شناسایی مشخص شوند و برنامه‌ها و گواهی‌نامه‌های مورد اطمینان در فهرست استثنائات قرار گیرند.
- **احتمال تأثیر بر عملکرد کاربران** – به علت اینکه تجزیه و تحلیل رفتاری به صورت مداوم تمام فعالیت‌های اجرا شده بر روی نقطه پایانی را رصد می‌کند، ممکن است سبب کاهش کارایی نقطه پایانی شود.

[۲۳] Monitoring Mode

فناوری ضدبهره‌جو

هدف این فناوری متوقف کردن اجرای کد آلوده در حافظه است؛ به نحوی که سبب دشوارتر شدن بهره‌جویی از آسیب‌پذیری‌های موجود در نقطه پایانی توسط مهاجمان شود. این امر با حفاظت از حافظه اختصاص یافته به یک پروسه یا نرم‌افزار انجام می‌شود. این روش لزوماً از قرار دادن کد مخرب مهاجم در حافظه جلوگیری نمی‌کند بلکه از روش‌هایی، برای جلوگیری از اجرای آن کد مخرب استفاده می‌کند. فناوری ضدبهره‌جو، مکانیزم‌هایی را به کار می‌گیرد که در حال حاضر توسط سیستم‌های عامل، پشتیبانی شده و در عمل قابلیت‌هایی فراتر از حفاظت اولیه را فراهم می‌سازد.

راهبران مدیریت امنیت و خطر می‌توانند چندین مزیت از جمله سربار مدیریتی کم را با استفاده از این روش برای سازمان‌ها انتظار داشته باشند. تعداد کمی روش مقابله با بهره‌جویی وجود دارد و بسیاری از آنها به امضاء یا به‌روزرسانی متکی نیستند. این راهکارها به طور کلی هزینه سربار کارایی را کاهش داده و برای کاربر به صورت شفاف عمل می‌کنند. به عنوان مثال مایکروسافت یک مجموعه ابزار پیشرفته[۲۴] رایگان برای مقابله با بهره‌جویی ارائه کرده که تا اواسط ۲۰۱۸ توسط مایکروسافت پشتیبانی می‌شود.

توصیه‌ها

- از بررسی‌های انجام شده توسط مؤسسات ارزیابی‌کننده معتبر و بی‌طرف جهت بررسی ادعاهای فروشندگان استفاده شود. مقایسه‌هایی که توسط فروشندگان یا کمیسیون‌ها انجام می‌شود، می تواند اطلاعات مفیدی را فراهم کنند اما ارزش آزمایش‌های بی‌طرفانه بیشتر خواهد بود.
- لزوم وجود ابزار پاسخگویی به رخداد مانند تجزیه‌وتحلیل‌های رفتاری با توجه به پس از اجرا بودن فناوری شناسایی

باید در نظر داشت تا زمانی که یک جریان ثابت از بردارهای حمله[۲۵] و آسیب‌پذیرهای جدید وجود داشته باشد، نتایج نیز تقریبا یکسان است. مورد باج‌افزار را در نظر بگیرید که هدف آن رمزنگاری داده‌هاست. اگر فناوری‌ها بتوانند قصد رفتاری بدافزار را شناسایی کنند، روش مقابله با آن اهمیت کمتری پیدا می کند. کاهش آسیب‌پذیری‌های شناخته شده باید در اولویت‌های اصلی یک سازمان باشد.

نتیجه‌گیری

سازمان‌ها در انتخاب محصولات ضدبدافزار خود با چالش‌های زیر روبرو هستند:

- رواج گسترده بازاریابی‌هایی که حول "ضدبدافزارهای نسل بعدی" صورت گرفته و در آنها از "یادگیری ماشین" به عنوان راهکاری انقلابی و سپری غیر قابل شکست در برابر بدافزارها و تهدیدات سایبری یاد می‌شود. موضوعی که موجب سردرگمی درباره ارزش واقعی این فناوری‌ها در صنعت ضدبدافزار شده است.
- ظهور اصطلاحات کلی و نسبتاً نامفهموم همچون "کنترل برنامه" که هر یک می‌توانند شامل طیف وسیعی از قابلیت‌های متعارف باشند.
- در هم آمیخته شدن فناوری‌های سازندگان مختلف با یکدیگر که خطر و ریسک ناسازگاری نرم‌افزاری را افزایش داده و در نتیجه موجب افزایش احتمال غیرفعال شدن ویژگی‌های امنیتی و کاهش کارایی مطلوب می‌شود.
- عدم اشاره به اتکای بسیاری از بدافزارها به کم‌توجهی و بی‌دقتی کاربران برای رخنه به سیستم‌ها در تبلیغات سازندگان محصولات ضدبدافزار و در نتیجه در نظر گرفته نشدن اهمیت بالای آموزش و آگاهی‌رسانی امنیت توسط راهبران شبکه‌ای که از محصولات این سازندگان استفاده می‌کنند.

---

[۲۴] Enhanced Mitigation Experience Toolkit (EMET)

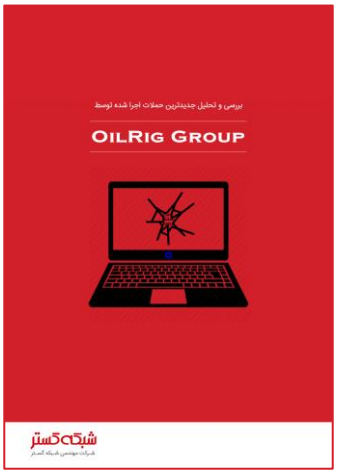
[۲۵] Attack Vectors

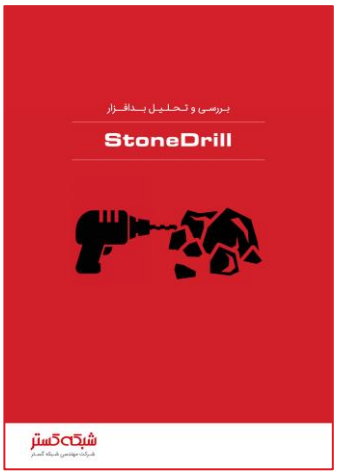
مدیران ارشد امنیت و ریسک سازمان‌ها می‌بایست همواره موارد زیر را مد نظر قرار دهند:

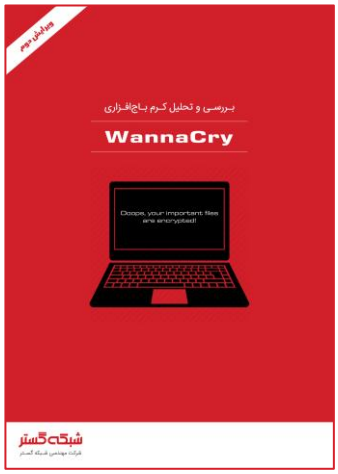
- یک استراتژی محافظت از نقاط پایانی متشکل از امنیت خوب، محافظت لایه‌ای، فناوری‌های شناسایی و آموزش کاربر نهایی طراحی شود.
- از تکرار قابلیت‌های امنیتی در محصولات مختلف اجتناب گردد. در عوض، در ابتدا یک محصول مناسب انتخاب شده و پس از پیاده‌سازی کامل آن نسبت به شناسایی بخش‌های خاصی که نیازمند تقویت و تکمیل هستند، اقدام شود.
- پرهیز از واکنش‌های ناگهانی و در عوض به تاخیر انداختن خریدهای جدید با مطالعه و بررسی اجرای یک برنامه مفید به‌منظور حصول اطمینان از متناسب بودن آن با گردش کاری موجود یا حتی بهبود آن
- مورد استناد قرار دادن بررسی‌های داخلی و آزمون‌های انجام شده توسط مؤسسات معتبر بی‌طرف و نه صرفاً پذیرفتن ادعاهای سازندگان محصولات ضدبدافزار؛ البته مقایسه‌های صورت پذیرفته توسط سازندگان نیز می‌تواند حاوی اطلاعات مفیدی باشد که به فرآیند بررسی داخلی سرعت ببخشد.
- کاهش آسیب‌پذیری‌های شناخته شده باید در اولویت‌های اصلی یک سازمان باشد.

منابع

- https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-jun-2017.pdf
- https://newsroom.shabakeh.net/9462
- https://www.gartner.com/doc/reprints?id=1-3Z764HA&ct=170501&st=sb&aliId=35510997&mkt_tok=eyJpIjoiTldZek1UZzNZekZoTWpJeCIsInQiOiJKK2ZscnBhZmU1MXdqTGhJdXFCMW9mcU14WForY05pTm9WTVFSXC8rckFUODZTTlYrWVJOditqXC90c3BcL2ZRXC9NaU1BdWFnOVFXMFVLRXhSU01Md05TTTc4ZjRjWDNzZWJZUmtHXC91dGl6aWFUM21BeFplalJVRlhzMTlcL2VzaW9MKyJ9







شبکه گستر

شرکت مهندسی شبکه گستر در سال ۱۳۷۰ تأسیس گردید و اولین شرکت ایرانی است که در زمینه نرم‌افزارهای ضدویروس فعالیت تخصصی و متمرکزی را آغاز کرده است. در ابتدا، همکاری مشترکی بین شرکت مهندسی شبکه گستر و شرکت انگلیسی S & S International (تولیدکننده ضدویروس مشهور Toolkit) آغاز گردید. در مدت کوتاهی، با فعالیت شبکه گستر به‌عنوان نماینده رسمی و انحصاری S & S International در ایران، به تدریج ضدویروس Dr Solomon's Toolkit به محبوب‌ترین ضدویروس در ایران تبدیل شد.

پس از خرید شرکت S & S International توسط شرکت McAfee در سال ۱۳۷۷، شرکت شبکه گستر نیز مانند دیگر نمایندگان بین‌المللی فعالیت خود را بر روی نرم‌افزارهای ضدویروس McAfee ادامه داد. در حال حاضر نیز شرکت شبکه گستر به‌عنوان فروشنده مجاز (Authorized Reseller) در منطقه خاورمیانه، به ارائه محصولات و خدمات درایران اقدام می‌نماید.

در سال ۱۳۸۴ شرکت مهندسی شبکه گستر موفق به کسب نمایندگی رسمی و انحصاری شرکت آلمانی Astaro، سازنده محصولات "مدیریت یکپارچه تهدیدات" (Unified Threat Management) گردید. به دنبال رشد چشمگیر و موفقیت جهانی محصولات امنیتی شرکت Astaro، در سال ۱۳۹۰ شرکت Sophos انگلیس، اقدام به خرید این شرکت آلمانی نمود. به دنبال این نقل و انتقال، شرکت مهندسی شبکه گستر به‌عنوان نماینده شرکت Sophos ادامه فعالیت داده و اکنون محصولات Astaro سابق را تحت نام جدید Sophos و دیگر محصولات امنیت شبکه این شرکت را در ایران عرضه می‌نماید.

از سال ۱۳۹۱ نیز، شرکت مهندسی شبکه گستر عرضه محصولات ضدویروس Bitdefender را به‌عنوان نماینده و توزیع‌کننده (Distributor) رسمی در ایران، آغاز کرد. عرضه محصولات ضدویروس Bitdefender در کنار محصولات امنیتی McAfee، پاسخی به شرایط و نیازهای متفاوت کاربران و مدیران شبکه است. ضد ویروس چابک‌تر، مدیریت آسان‌تر و محصولی مقرون به صرفه‌تر، انتظاراتی بودند که برخی کاربران و مدیران شبکه‌های کوچک و متوسط داشتند و با عرضه محصولات ضدویروس Bitdefender، شبکه گستر به نیازهای این بخش از بازار پاسخ داد.

شرکت مهندسی شبکه گستر افتخار دارد که مجری برخی از بزرگترین پروژه‌های طراحی، نصب، راه‌اندازی و طولانی مدت‌ترین خدمات نگهداری و پشتیبانی محصولات نرم‌افزاری ضدویروس و سخت‌افزاری فایروال در کشور بوده است.

این شرکت علاوه بر خدمات‌دهی به هزاران شرکت و سازمان که صدها هزار کاربر را در کشور شامل می‌شوند، دارای شبکه نمایندگی فروش و پشتیبانی در سراسر کشور نیز می‌باشد.

CSQ
ISO 9001:2008
Cert No 9150.C528

شبکه گستر

شـرکت مهندسی شبکه گستر

تهران ۱۹۶۸۶، خیابان شهید دستگردی، شماره ۲۷۳

تلفن / دورنگار ۰۲۱-۴۲۰۵۲

تارنمای شرکت www.shabakeh.net

سامانه پشتیبانی help.shabakeh.net

خدمات پس از فروش my.shabakeh.net

مرکز آموزش events.shabakeh.net

اتاق خبر newsroom.shabakeh.net