پیشگیری از تهدید

بهره‌برداری جامع، تروجان و حفظ فرمان و کنترل برای شبکه شما

سازمان‌ها با حملات مکرر تهدیدکننده در سراسر جهان روبرو هستند. امروزه مهاجمان به دارایی‌های خوبی مجهز شده‌اند. آنها از روش‌های گریز برای موفقیت در بدست آوردن جای ثابت در شبکه استفاده می کنند، حجم بالا و حملات پیچیده در حالی انجام می‌شوند که در دفاع سنتی سازمان قابل مشاهده نیستند، بسته‌های پیچیده، نرم‌افزارهای مخرب چندگانه و رمزنگاری برای محوله‌های چندمرحله‌ای و سرعت انتشار DNS استفاده می کنند.

هدف از ایجاد پلتفرم امنیتی نسل جدید Palo Alto Networks®، ارائه خدمات پیشگیری تهدیدهای شبکه‌ها است که از فازهای مختلف حمله محافظت می‌کنند:

- کلیه ترافیک‌ها را در متن کامل برنامه‌ها و کاربران اسکن می‌کند.
- در هر مرحله از چرخه زندگی سایبری از تهدیدها جلوگیری می کنند.
- معماری اسکن یکپارچه اجازه می‌دهد تا بدون به خطر انداختن امنیت، کارایی افزایش یابد.
- برای کشف تهدید تازه به طور خودکار و روزانه به‌روزرسانی می‌شود، از طریق پیشگیری‌های موجود در ۳۰۰ ثانیه برای بدافزار جدید و بهره برداری از طریق سرویس WildFire™ به عنوان سرویس تحلیل تهدید مبتنی بر ابر استفاده می کنند.
- امضای فرمان و انقلاب کنترل خودکار که در مقیاس و سرعت دستگاه ارائه می‌شود.

آدرس: یوسف آباد- میدان جهاد- خیابان بیستون- خیابان فتحی شقاقی- پلاک ۹۳- طبقه دوم - واحد ۵
تلفن:۱-۸۸۳۵۳۴۰۰-۰۲۱
فکس: ۸۹۷۸۴۲۷۱

با بدتر شدن شرایط، محصولات امنیتی شبکه از همان استراتژی‌های دفاعی استفاده می‌کنند که پیش از چشم انداز تهدید استفاده می‌کردند. ترافیک تنها در درگاه‌های خاص بررسی می‌شوند، در حالی که افزودن دستگاه‌های تک عملکردی به پشته دفاعی باید به حل مشکل خاص کمک کند، منجر به عملکرد ضعیف می‌شود. این وضعیت خطرناکی را پشت سر گذاشته است، حفره‌های شکاف در مقابل دفاع از شبکه وجود دارند، زیرا پاسخ‌های امنیتی شکست خورده‌اند و مدیریت آن مشکل است، در حالی که مهاجمان به طور فزاینده‌ای در آن نفوذ می‌کنند.

فعال کردن برنامه، پیشگیری از تهدید

برنامه‌های کاربردی بخش جدایی ناپذیر نحوه فعالیت شرکت‌ها هستند و به همین علت با وارد کردن شبکه‌ها با استفاده از کانال‌های رمزنگاری از طریق درگاه‌های غیراستاندارد و پرش از درگاه باز برای باز کردن درگاه برای تضمین دسترسی همیشگی کاربران به طور فزاینده‌ای در دسترس کاربران قرار می‌گیرند.

ما با ارائه لایه‌های مختلف پیشگیری از شبکه شما در مواجه با تهدیدات در هر مرحله از حمله محافظت می‌کنیم. علاوه بر قابلیت‌های پیشگیری نفوذ سنتی، به جای امضاهای مبتنی بر مجموعه محدودی از درگاه‌های از پیش تعریف شده، توانایی منحصر به فردی را برای تشخیص و توقف تهدیدات در کلیه درگاه‌ها ارائه می‌دهیم. با اعمال فناوری شناسایی کاربر User-ID™ و فناوری تشخیص برنامه کاربردی App-ID™ در دیوار آتش نسل بعدی که متن را برای کلیه ترافیک‌ها در درگاه‌ها شناسایی و اضافه می‌کند، موتور پیشگیری تهدید صرف نظر از روش فرار هرگز از نظر تهدید شکست نمی‌خورد.

اشتراک تهدید ما شامل پیشگیری از نفوذ، شبکه ضد تروجان و حفاظت از فرمان و کنترل است.

از بین بردن تهدید در هر فاز

تقریباً در هر یک از شکست‌های اخیر؛ سازمان مورد هدف ابزار دفاعی تک- عملکردی داشت که جایگزین آن شده بود.

- تحلیل مبتنی بر اکتشاف، بسته‌های غیرعادی و الگوهای ترافیکی مانند مرور درگاه، جابجایی میزبان و حملات شناور DdoS را شناسایی می‌کند.
- سایر قابلیت‌های محافظت در مقابل حمله، مانند مسدود کردن بسته های نامعتبر و ناقص، نابودی IP ، و تلفیق مجدد TCP، برای حفاظت در برابر روش‌های گریز و سوء استفاده مهاجمان مورد استفاده قرار می‌گیرد.
- آسان برای پیکربندی، امضاهای آسیب‌پذیر سفارشی به شما اجازه می‌دهد تا قابلیت‌های پیشگیری نفوذ را به نیازهای منحصر به فرد شبکه تخصیص دهید.

شبکه‌های Palo Alto، فناوری‌های دفاعی محلی را به کار می‌گیرند تا اطمینان حاصل شود که وقتی تهدیدی جلوی فناوری را می‌گیرد، دیگری آن را بدست می‌آورد. کلید حفاظت مؤثر آن است که از ویژگی‌های امنیتی به طور هدفمند برای به اشتراک‌گذاری اطلاعات استفاده شود و در زمینه بررسی حول هر ترافیک و شناسایی و مسدود کردن تهدید از آن استفاده می‌شود.

پیشگیری از نفوذ (IPS)

حفاظت‌های مبتنی بر تهدید، روش‌های سوءاستفاده و روش‌های انحرافی در هر دو شبکه و لایه کاربردی از جمله مرور درگاه، بافر اضافی، اجرای کد از راه دور، تکه تکه شدن پروتکل و سوءاستفاده را شناسایی و مسدود می‌کنند. حفاظت‌ها بر اساس تطابق امضا و تشخیص ناهنجاری است که رمزنگاری و تحلیل پروتکل‌ها را انجام می‌دهد و از اطلاعات یاد شده برای ارسال هشدارها استفاده می‌کنند و الگوهای ترافیک مخرب را مسدود می‌کنند. تطبیق ماشین‌های الگوی مقررات بر اساس بسته‌های مختلف با توجه به سفارش و ترتیب ورود و اطمینان از عملکرد خوب ترافیک‌های مجاز و از بین رفتن روش‌های گریز شناسایی می‌شوند.

- تحلیل پروتکل مبتنی بر رمزگشایی پروتکل است و بنابراین امضا را به طور هوشمندانه برای شناسایی سوءاستفاده از شبکه و برنامه کاربردی استفاده می‌کند.
- از آنجا که راه‌های زیادی برای بهره‌برداری از آسیب‌پذیری وجود دارد، امضاهای پیشگیری ما بر پایه نفوذ آسیب‌پذیری‌شان ساخته می‌شوند، و حفاظت کامل‌تری در برابر انواع مختلف سوء استفاده‌ها ایجاد می‌شود. امضا تنها می‌تواند برخی از تلاش‌های سوءاستفاده را در آسیب‌پذیری سیستم یا برنامه شناخته شده متوقف کند.
- حفاظت پروتکل مبتنی بر ناهنجاری که کاربرد پروتکل ناسازگار با RFC را تشخیص می‌دهد، مانند URI اضافی یا ورودی FTP.
- آسان برای پیکربندی، امضاهای آسیب‌پذیر سفارشی به شما اجازه می‌دهد تا قابلیت‌های پیشگیری نفود را به نیازهای منحصر به فرد شبکه تخصیص دهید.

حفاظت تروجان

حفاظت درون خطی، بدافزارها را پیش از رسیدن به میزبان هدف از طریق امضاها بر اساس اطلاعات بارگذاری شده و غیر Hash بلوک می‌کند. حفاظت‌های تروجان شبکه‌های Palo Alto، بدافزار شناخته شده و انواع تروجان‌های آینده از جمله مواردی که هنوز مشاهده نشده اند را شامل می‌شوند. موتور مبتنی بر جریان ما از شبکه محافظت می‌کند بدون آن که تأخیر قابل توجهی را نشان دهد که نشان دهنده نقص جدی آنتی‌ویروس‌های شبکه است و بر موتورهای اسکن مبتنی بر پروکسی متکی است. مرور تروجان مبتنی بر جریان به محض دریافت بسته‌های اولیه فایل، ترافیک را بررسی کرده و تهدیدات و همچنین مسائل مربوط به کارایی مرتبط با راه‌حل‌های سنتی و مستقل را از بین می‌برد. قابلیت‌های کلیدی ضد تروجان عبارتند از :

- تشخیص و پیشگیری درون خطی نرم‌افزارهای مخرب در فایل‌های فشرده و محتوای پنهان وب.

- حفاظت در برابر بارهای بارگذاری شده در انواع فایل‌های معمولی مانند اسناد Microsoft® Office و PDF.
- به روزرسانی دیوار آتش، اطمینان از حفاظت در برابر بدافزار جدید.

امضا برای انواع نرم‌افزارهای مخرب به طور مستقیم از طریق میلیاردها نمونه جمع‌آوری شده توسط شبکه‌های Palo Alto، شامل بدافزارهای ناشناخته از قبل ارسال شده به دیوار آتش، توسط گروه تحقیق تهدید واحد ۲۴ و سایر شرکای تحقیقاتی شخص ثالث و الگوهای فناوری در سراسر جهان انجام شده است.

امضاهای مبتنی بر بار مفید و Hash

امضاهای مبتنی بر بار مفید، الگوهایی را در ساختار فایل شناسایی می‌کنند که می‌توان برای شناسایی تغییرات فایل در آینده به کار برد، حتی اگر محتوا کمی اصلاح شده باشد. این به ما اجازه می‌دهد تا نرم‌افزارهای مخرب را بلافاصله شناسایی کرده و مسدود کنیم، در غیر این صورت به عنوان فایل ناشناخته جدید مورد استفاده قرار می‌گیرند.

امضاهای مبتنی بر Hash در رمزگذاری ثابت برای هر فایل منحصر به فرد مورد استفاده قرار می‌گیرد. از آنجا که فایل Hash به راحتی تغییر می‌کند، امضاهای مبتنی بر Hash در تشخیص نرم‌افزارهای مخرب و یا انواع فایل‌های مشابه مؤثر نیستند.

حفاظت فرمان و کنترل (نرم‌افزار جاسوسی)

می‌دانیم که هیچ مانعی برای جلوگیری از ورود هر گونه تهدید به شبکه وجود ندارد. پس از ابتلا به آلودگی، مهاجمان از طریق کانال فرمان و کنترل (CnC) با دستگاه میزبان ارتباط برقرار می‌کنند تا از تروجان اضافی جلوگیری کنند، دستورات بیشتری صادر کرده و اطلاعات را سرقت کنند. حفاظت از فرمان و کنترل در کانال‌های ارتباطی غیرمجاز پیچیده شده است و با مسدود کردن درخواست‌های خروجی به دامنه‌های مخرب و ابزار شناخته شده توسط کانال فرمان و کنترل که بر دستگاه آلوده وصل شده قطع می‌شوند. شبکه‌های Palo Alto مبتنی بر URLها و دامنه‌ها فراتر از استانداردسازی امضاهای فرمان و کنترل

هستند. به طور خودکار امضا فرمان و کنترل مبتنی بر الگویی را تضمین می‌کنیم که دارای درجه دقیقی از سرعت و مقیاس ماشین است.

مرور کلیه تهدیدات در یک گذر

موتور پیشگیری تهدیدات شبکه‌های Palo Alto صنعتی را ارائه می‌دهد که ابتدا با بررسی و طبقه‌بندی ترافیک و شناسایی و مسدود کردن بدافزار و آسیب‌پذیری‌ها در گذرگاه مجاز ارائه می‌شود. فناوری‌های پیشگیری تهدید سنتی به دو یا چند موتور مروری نیاز دارد، زمان قابل ملاحظه‌ای افزوده شده و عملکرد را به طرز چشمگیری کاهش می‌دهد. از فرمت امضای واحد برای کلیه تهدیدات استفاده می‌کنیم تا پردازش سریع را با انجام کلیه تحلیل‌ها در مرور یکپارچه انجام دهیم، فرایندهای انحصاری مشترک را برای پاسخ‌هایی که از موتورهای مروری چندگانه استفاده می‌کنند، حذف می‌کنیم.

جستجوی فناوری پیشگیری از تهدید از طریق هر بسته همانند عبور از طریق پلت‌فرم به دنبال نزدیک شدن در توالی‌های بایت در بخش بالایی بسته و بار اضافی انجام می‌شود. این تحلیل ما را قادر می‌سازد تا جزئیات مهم این بسته از جمله برنامه کاربردی مورد استفاده، منبع و مقصد آن، بررسی سازگار پروتکل با RFC و بررسی کد استثنا یا مخرب را شناسایی کنیم. فراتر از بسته‌های منحصر به فرد، زمینه ارائه شده توسط ورودی سفارشی و دنباله چندین بسته را برای جلوگیری از روش‌های حذف تحلیل می‌کنیم. کلیه تحلیل‌ها و تطابق امضا در یک مرور اتفاق می‌افتند، بنابراین ترافیک شبکه شما در همان سرعت مورد نیاز باقی می‌ماند.

ادغام اشتراک پیشگیرانه تهدید با دیوار آتش

سازمان‌ها می‌توانند حفاظت در مقابل بدافزارهای جدید را گسترش دهند و از سرویس دیوار آتش استفاده کنند. دیوار آتش پیشرفته‌ترین موتور جستجوی پیشرفته برای بدافزارها و ابزارهای سوءاستفاده جدید است. سرویس مبتنی بر ابر رویکرد چند

روشی منحصر به فردی را به کار می‌گیرد که ترکیبی از تحلیل پویا و استاتیک، روش های یادگیری ماشین نوآورانه و محیط تحلیل متداول خیره‌کننده برای شناسایی و جلوگیری از تهدیدات فرار است.

کاهش سطح حمله

رمزگشایی SSL

تقریباً ۴۰ درصد ترافیک شبکه شرکت با SSL رمزگذاری شده است که در صورت عدم اسکن رمزگشایی و تهدید در مقابل آن، حفره‌هایی در دفاع شبکه به وجود می‌آید. پلت‌فرم ما در رمزگشایی SSL ساخته شده است که می‌توان به طور انتخابی برای رمزگشایی ترافیک ورودی و خروجی SSL به کار برد. پس از آن که ترافیک رمزگشایی شد و امنیت آن تأیید شد، دوباره رمزگذاری شده و کل مسیر آن مجاز است.

مسدود کردن فایل

حدود ۹۰ درصد فایل‌های مخرب مورد استفاده در حملات سرقت اطلاعات قابل اجرا هستند. یعنی، حقیقت آن است که تقریباً ۶۰ درصد حوادث امنیتی نتیجه غفلت کارکنان است، این بدین معنی است که کاربران ممکن است ندانند چه چیزی امن است و چه چیزی امن نیست. احتمال بروز ویروس مخرب از طریق جلوگیری از انواع فایل‌های خطرناک شناخته شده برای پنهان کردن بدافزارهایی مانند سرقت اطلاعات از طریق ورود به شبکه شما کاهش می‌یابد. قابلیت مسدود کردن فایل را می توان با ID- کاربر ترکیب کرد تا فایل‌های غیرضروری بر اساس نقش کاربری کارکنان مسدود شوند، اطمینان حاصل شود که همه کاربران به فایل‌های مورد نیاز دسترسی دارند و شما روش دانه‌ای را برای کاهش در معرض خطر گرفتن را ارائه می‌دهید به نحوی که باعث می‌شود تا احساس نیازهای متنوع سازمان‌تان را درک کنید. شما می‌توانید تعداد فرصت‌های حمله را با ارسال کلیه فایل‌های مجاز به دیوار آتش برای تحلیل به منظور تعیین این که آیا آنها شامل بدافزارهای مخرب جدید هستند یا خیر، کاهش دهید.

تحریک- با استفاده از حفاظت دانلود

کاربران قربانی سهواً بدافزارهای مخرب را با مراجعه به صفحه وب مورد علاقه‌شان دانلود می‌کنند. اغلب کاربران و یا حتی مالک وب‌سایت ممکن است ندانند که سایت آسیب دیده است. فناوری پیشگیری از تهدید ما خطرات دریافتی بالقوه را شناسایی کرده و به کاربران هشدار می‌دهد تا از دانلود در نظر گرفته شده مطمئن شوند و مورد تأییدشان باشد. با مرتبط کردن این ویژگی به فیلترهای URL و سیاست‌های مسدود کردن فایل، از حملات دامنه‌های جدید و به سرعت در حال تغییر جلوگیری می‌شود.

کاهش آسان و دقیق تله DNS

حفاظت از کنترل و فرمان ما قابلیت‌های تله را برای درخواست‌های خروجی برای ورودی های مخرب DNS، جلوگیری از نفوذ و شناسایی دقیق قربانی ارائه می‌دهد. پیکربندی تله به گونه‌ای است که هر درخواست خروجی به جای آن‌که به یکی از آدرس‌های IP داخلی شبکه شما هدایت شود، به یک دامنه مخرب یا آدرس IP هدایت می‌شود. این به طور مؤثر ارتباط کنترل و فرمان را مسدود می‌کند، و از این درخواست‌ها جلوگیری می‌کند تا از شبکه خارج شود. گزارش میزبان‌ها در شبکه شما، این درخواست‌ها را جمع‌آوری می‌کند، حتی اگر میزبان‌ها پشت سرور DNS قرار گرفته باشند. تیم‌های واکنش حادثه، لیست روزانه دستگاه‌های به خطر افتاده را بدون تأکید اضافی در زمان بحرانی ارائه می‌دهند زیرا ارتباطات با مهاجمان قبلاً قطع شده است.

اشیا همبستگی خودکار

فناوری پیشگیری از تهدید ما شامل توانایی شناسایی وجود تهدیدات پیشرفته از طریق نظارت و همبستگی ترافیک شبکه و گزارش‌های تهدید است، بنابراین به سرعت می‌توان کاربران آلوده را شناسایی و الگوهای رفتاری عجیب را تحلیل کرد. تحقیقات تهدید ابزار اشیا همبستگی واحد ۲۴ و تهدیدات مجهول از طریق دیوار آتش و ID- کاربر برای ارتباط ناهنجاری‌های ترافیکی و

شاخص‌های سازش تحلیل می‌شوند، بنابراین آنچه که ممکن است دستگاه‌های شما را آلوده کند با سرعت و دقت شناسایی می‌شود.

اهرم سراسری تهدید اطلاعات برای جلوگیری از حملات

گزارش‌های دقیق کلیه تهدیدات صرفاً در درون رابطه مدیریتی قرار نگرفته‌اند، بلکه در میان کلیه مکانیزم‌های پیشگیرانه برای ایجاد محتوا به اشتراک گذاشته شده‌اند. ما با استفاده از اهرم تهدید اطلاعات سراسری از طریق دیوار آتش خودکار، بدافزارهای ناشناخته را شناسایی کرده و حفاظت از کلیه مشتریان خود را ارائه داده و به طور مستمر از آنها در برابر تهدیدات پیشرفته محافظت می‌کنیم. حفاظت از سازمان شما شامل حفاظت در برابر شبکه‌های بدافزار و وب‌سایت‌های مخرب با استفاده از تحلیل مبتنی بر DNS شبکه‌های Palo Alto انجام می‌شود. از طریق شبکه هوشمند گسترده از مزایای استفاده از نظارت DNS استفاده می‌شود که به پایگاه اطلاعاتی ما در حوزه‌های مخرب کمک می‌کند تا حفاظت سراسری پایگاه مشتریان‌مان ایجاد شود.

شبکه DNS منفعل

Model	Threat Throughput
PA-200	50 Mbps
PA-500	100 Mbps
PA-2020	200 Mbps
PA-2050	500 Mbps
PA-3020	1 Gbps
PA-3050	2 Gbps
PA-3060	2 Gbps
PA-5020	2 Gbps
PA-5050	5 Gbps
PA-5060	10 Gbps
PA-7050	100 Gbps*
PA-7080	160 Gbps*

*DSRI-enabled

تحقیق تهدید واحد ۲۴

گروه تحقیق تهدید شبکه‌های Palo Alto، واحد ۲۴، اطلاعات انسانی را برای شناسایی آسیب پذیری در مقابل بحران‌های جدید در Microsoft®، Adobe®، Apple®، Android™ و سایر اکوسیستم‌ها به کار می‌برد. با شناسایی فعالانه این آسیب‌پذیری‌ها، ایجاد حفاظت برای مشتریان و به اشتراک‌گذاری اطلاعات با جامعه امنیتی، سلاح های مورد استفاده توسط مهاجمان را برای تهدید کاربرن و سازش با شبکه‌های سازمانی، دولتی و خدماتی از بین می‌بریم