خبرنامه برنا

Borna Network Managers
مدیران شبکه برنا

اخبار حوزه امنیت و شبکه (آبان ۱۴۰۴)

خبر نامه تخصصی « مدیران شبکه برنا » نگاهی حرفه ای به دنیای امنیت شبکه هرماه با ما همراه باشید تا در جریان جدید ترین تهدیدات سایبری ؛ تحلیل رویداد ها ؛ به روز رسانی محصولات و راهکار های نوین امنیت اطلاعات قرار بگیرید.

ویژه مدیران و کارشناسان شبکه و امنیت

www.bornanetwork.co
info@bornanetwork.co
۰۲۱-۷۴۰۲۸

تهدید اصلی ناشی از دسترسی غیرمجاز مدیران سیستم

طبق گزارش‌های امنیتی Verizon Data Breach Investigations Report (DBIR 2024) و IBM Cost of a Data Breach Report 2024، بیش از ۳۵% از رخدادهای نشت داده ناشی از دسترسی بیش از حد یا Excessive Privileges و حتی مدیریت ضعیف حساب های دارای امتیاز بالا Privileged Accounts می‌باشد.

در استانداردهای بین‌المللی امنیت اطلاعات مانند ISO/IEC 27001 و چارچوب NIST SP 800-53، کنترل دسترسی و نظارت بر فعالیت مدیران سیستم، یکی از کلیدی‌ترین الزامات به شمار می‌رود. نادیده گرفتن این کنترل‌ها می‌تواند پیامدهای جبران ناپذیری برای شبکه به ارمغان آورد که در ادامه به برخی از آنها اشاره شده است:

افشای داده‌های حساس سازمانی

مدیران سیستم معمولاً به پایگاه‌های داده، فایل سرورها و ایمیل‌ها دسترسی مستقیم دارند. هرگونه سوءاستفاده یا نفوذ به حساب آن‌ها، معادل دستیابی کامل مهاجم به داده‌های حیاتی است.

تغییر یا تخریب پیکربندی‌های حیاتی (Configuration Tampering)

تغییرات ناخواسته در تنظیمات امنیتی یا حذف سیاست‌های دسترسی، می‌تواند مسیر نفوذ بعدی را هموار کند.

ایجاد درب پشتی (Backdoor) یا بدافزار داخلی

در نبود کنترل‌های نظارتی، مدیر سیستم می تواند بدون ثبت در لاگ‌ها، حساب‌های پنهان ایجاد کند یا اسکریپت‌های مختلف در سطح سیستم‌عامل اجرا نماید.

پاک‌سازی لاگ‌ها و آثار رویداد (Log Manipulation)

یکی از خطرناک‌ترین تهدیدها حذف یا تغییر لاگ های امنیتی است، زیرا کشف رخداد را تقریباً ناممکن می‌کند.

آسیب به اعتماد سازمان و اعتبار برند

نشت داده از سطح مدیریت، از دید مشتریان و شرکای تجاری، به‌معنای ضعف بنیادی در حاکمیت امنیتی سازمان است.

راهکارهای پیشنهادی بر اساس Best Practices

• اجرای مدیریت دسترسی مبتنی بر نقش (RBAC) و اصل حداقل دسترسی لازم (Least Privilege)
• فعال‌سازی ثبت و تحلیل مداوم لاگ‌ها (Audit Logging & SIEM Integration)
• بازبینی دوره‌ای مجوزهای کاربران دارای دسترسی بالا
• استفاده از راهکارهای DLP (Data Loss Prevention) برای کنترل، پایش و جلوگیری از خروج داده‌های حساس از نقاط انتهایی

در این میان، شرکت مدیران شبکه برنا با بیش از ده سال سابقه در حوزه امنیت سایبری و همچنین ارائه راهکارهای امنیتی به سازمان‌های خصوصی و دولتی، استفاده از محصول DLP Safetica را در این زمینه پیشنهاد می‌نماید. Safetica با ترکیب کنترل دسترسی، پایش فعالیت کاربر، و حفاظت از داده‌ها در سطح Endpoint، به سازمان‌ها کمک می‌کند تا دسترسی‌های غیرمجاز مدیران سیستم و ریسک‌های ناشی از آن را شناسایی و مدیریت کنند.

جهت ارائه مشاوره امنیتی در حوزه جلوگیری از نشت داده‌های حساس سازمانی و همچنین استفاده از راهکارهای امنیتی اورجینال و معتبر در این حوزه با ما در ارتباط باشید.

مدیریت نشت داده در سازمان: از کنترل USB تا استقرار چارچوب DLP و DRM

چکیده

با رشد روزافزون جریان داده در محیط‌های سازمانی و افزایش وابستگی به سرویس‌های ابری و ابزارهای قابل‌حمل، احتمال خروج غیرمجاز اطلاعات به یکی از چالش‌های اصلی امنیت سایبری تبدیل شده است. تهدید نشت داده امروز تنها از سوی نفوذگران خارجی شکل نمی‌گیرد؛ بلکه رفتار کاربران داخلی، انتقال فیزیکی اطلاعات و همگام‌سازی ابری (Cloud Sync) نیز مسیرهای بالقوه محسوب می‌شوند. این مقاله سه لایه‌ی دفاعی مؤثر در برابر Data Leakage را بررسی کرده و در پایان، چارچوب تلفیقی DRM + DLP را به‌عنوان مدل پایدار امنیت داده معرفی می‌کند.

۱. لایه اول: کنترل ابزارهای انتقال داده (Device Control)

در سطح کاربر (Endpoint)، کنترل پورت‌ها و رسانه‌های قابل حمل اولین مانع در برابر نشت فیزیکی اطلاعات است. سیاست‌هایی مانند مسدود یا Read Only کردن درایوهای USB، تهیه‌ی Whitelist براساس شماره‌سریال دستگاه و ثبت لاگ Device Control در کنسول مرکزی (ESET PROTECT) راه‌حلی پایه‌ای اما ضروری به‌شمار می‌رود.

لایه دوم: پایش و تحلیل داده (DLP)

راهکارهای Data Loss Prevention (مانند Safetica ONE، Microsoft Purview DLP، یا Symantec DLP) بر مبنای تحلیل محتوایی و رفتاری عمل می‌کنند.

این سامانه‌ها قادرند داده‌های طبقه‌بندی‌شده را به‌صورت خودکار تشخیص دهند، از ارسال ایمیل یا آپلود غیرمجاز در مرورگر جلوگیری کنند و به صورت بلادرنگ گزارش کامل از الگوهای حرکت داده ارائه دهند.

در واقع، DLP عملکردی چون «سنسور داده» دارد؛ محتوای در حال انتقال را پایش می‌کند، به رفتار کاربران آگاهی دارد و داده‌ها را براساس سطح ریسک علامت‌گذاری می‌کند.

. لایه سوم: حفاظت پایدار از داده (Digital Rights Management – DRM)

در مواردی که به دلایل قانونی یا تجاری، داده باید با شرکای خارجی به اشتراک گذاشته شود، پشتیبانی صرف DLP کافی نیست. اینجاست که DRM به کار می‌آید و با رمزنگاری سطح فایل و تعریف حقوق دسترسی (Digital Rights)، امنیت را فراتر از مرز شبکه گسترش می‌دهد.

این فناوری اطمینان می‌دهد که فایل تنها توسط کاربران مجاز قابل مشاهده است، کلیه اقدامات (پرینت، Screenshot، Copy) ثبت می‌شوند و در صورت لغو مجوز، فایل از راه دور بی‌اثر می‌گردد. به این ترتیب، DRM آخرین خط دفاعی در چرخه عمر داده است.

مدل تحلیلی برنا برای معماری امنیت داده

تجربه تحلیلگران بُرنا نشان می‌دهد افزودن پوشش رفتاری (DLP) روی کنترل‌های سخت افزاری (Device Control) و تکمیل آن با DRM، نه تنها ریسک نشت را کاهش می‌دهد، بلکه تحلیل داده‌محور در واحد SOC را ارتقا می‌دهد.

در این مدل سه‌مرحله‌ای:

۱-کنترل درگاه‌ها با ESET PROTECT به‌عنوان لایه فیزیکی اجرا می‌شود.

۲-پایش رفتار و تحلیل محتوا از طریق Safetica ONE در سطح داده صورت می‌گیرد.

۳-حفاظت حقوقی و رمزنگاری داده با DRM (نظیر Microsoft AIP یا Seclore) امنیت چند مرحله‌ای را تکمیل می‌نماید.

این چیدمان در انطباق با الزامات استانداردهای ISO 27001 و NIST SP 800 171 است و به‌ویژه برای سازمان‌های Data Centric با سطح طبقه بندی بالا مؤثر است.

۵. جمع‌بندی و تحلیل راهبردی

نشت داده در سازمان‌ها بیش از هر زمانی به رفتار انسانی و خطاهای فرآیندی وابسته است. در چنین شرایطی، مدل‌های سنتی امنیت (مبتنی بر USB Block یا Firewall) کافی نیستند. برای دستیابی به امنیت واقعاً داده‌محور، سازمان‌ها باید به ترکیب سامانه‌های DLP و DRM روی آورند؛ DLP حرکت داده را رصد می‌کند و DRM مالکیت آن را صیانت می‌کند.

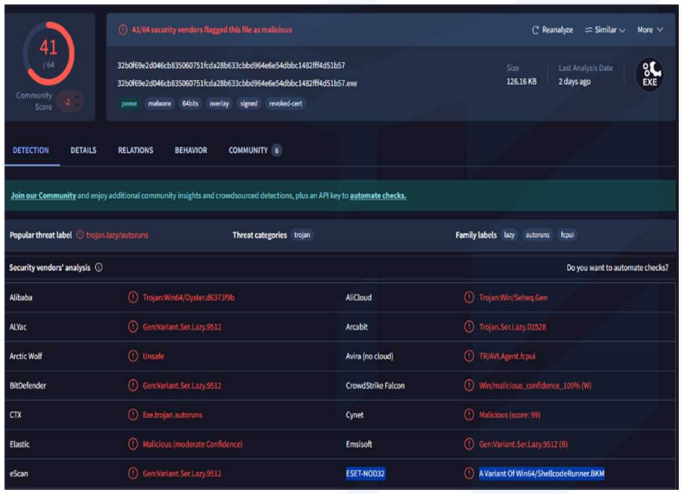
۶. یادداشت تحلیلی تهدیدات و نتایج اجرایی

مشاهدات واحد «امنیت داده و تهدیدات درون سازمانی» در بُرنا نشان می‌دهد که به‌کارگیری هوشمند Safetica ONE DLP در کنار سیاست‌های Device Control در کنسول ESET PROTECT، می تواند زنجیره کامل کنترل حرکت داده تا تحلیل رفتار کاربر را در درون سازمان تکمیل کند.

این ترکیب در چارچوب فنی Borna Data Protection Framework به شکل عملیاتی در زیرساخت‌های مالی و دولتی پیاده‌سازی شده و کاهش چشمگیری در موارد ثبت شده Leak Eventها در کنسول SIEM به دنبال داشته است. به عبارتی، Safetica به‌عنوان هسته هوشمند تحلیل رفتار کاربر و ESET به‌عنوان لایه کنترل سخت‌افزاری، الگوی موفق امنیت چندلایه در محیط‌های داده‌محور را شکل می دهند، بی‌آنکه هیچ ارجاع مستقیم تبلیغاتی در متن اصلی ارائه شود.

بدافزار Oyster

بدافزار Oyster که در برخی منابع با نام‌های Broomstick و CleanUpLoader نیز شناخته می‌شود، از اواسط سال ۲۰۲۵ در کمپین‌های باج‌افزاری فعال بوده است. این بدافزار پس از نفوذ به سیستم قربانی، با ایجاد ارتباط با سرور فرمان و کنترل (C2)، امکان اجرای دستورات از راه دور، دانلود ابزارهای اضافی و در نهایت اجرای Rhysida را فراهم می‌کند.



شاخص‌های فنی

دامنه‌های مخرب شناسایی شده:

- teams-download.buzz
- teams-install.run

فایل مشکوک:

- MSTeamsSetup.exe

هش شناسایی‌شده (SHA256):

32b0f69e2d046cb835060751fcda28b633cbbd964
e6e54dbbc1482fff4d51b57

نام‌های شناسایی در موتورهای ضدبدافزار:

براساس بررسی تیم فنی و پشتیبانی شرکت مدیران شبکه برنا، راهکار ESET این فایل را با نام زیر شناسایی می‌نماید.

- A Variant Of Win64/ShellcodeRunner.BKM

گواهی‌های جعلی مرتبط با:

- DigiCert
- GlobalSign
- SSL.com
- Trusted Signing

تأثیر و واکنش مایکروسافت

به گزارش مایکروسافت، این اقدام باعث شد بدافزارهای امضاشده توسط Vanilla Tempest به راحتی قابل شناسایی و مسدودسازی شوند. با این حال کارشناسان هشدار داده‌اند که مهاجمان احتمالاً با گواهی‌های جدید و تاکتیک‌های متفاوتی به فعالیت خود ادامه خواهند داد

توصیه‌های امنیتی برای سازمان‌ها

• نرم‌افزارهای کاربردی را تنها از وبسایت مایکروسافت و یا وبسایت‌های معتبر دریافت نمایید.
• دامنه های اعلام شده و مشکوک را در سطح شبکه مسدود نمایید.
• Hash فایل‌های اجرایی را پیش از اجرا بواسطه راهکارهای امنیتی موجود در شبکه اسکن نمایید. (جهت اطلاع از چگونگی انجام این کار با تیم فنی و پشتیبانی شرکت مدیران شبکه برنا در ارتباط باشید.)
• همواره گواهینامه‌های سیستم‌عامل را بررسی و بروزرسانی نمایید.
• آموزش کاربران شبکه مبنی بر آگاهی رسانی امنیتی و همچنین محدودسازی دسترسی کاربران در جهت استفاده از وب و نصب نرم‌افزار را در دستور کار سازمان قرار دهید.

جمع‌بندی

این گزارش نشان داد که حتی گواهی‌های دیجیتال معتبر نیز می‌توانند به ابزاری برای فریب کاربران و عبور از سیستم‌های امنیتی تبدیل شوند. اقدام اخیر مایکروسافت در لغو گواهی‌های جعلی، یک گام مهم در مقابله با زنجیره‌ی توزیع باج‌افزار Rhysida محسوب می‌شود، اما کارشناسان هشدار می‌دهند موج بعدی حملات با روش‌های جدید و گواهی‌های تازه امضا شده در راه است.

پیشنهاد شرکت مدیران شبکه برنا جهت امن سازی شبکه در سطح ایستگاه‌های کاری استفاده از راهکارهای نوین Eset Inspect جهت تحلیل داده های سازمانی در جهت دفع حملات هدفمند و مدیریت داده‌های حساس سازمانی بواسطه ابزارهای پیشرفته DLP Safetica می‌باشد. شما می‌توانید با استفاده از ابزارهای امنیتی معتبر و نوین در زمینه امنیت سایبری، ریسک‌های امنیتی در سطح شبکه را به حداقل برسانید. فراموش نکنیم تنها خرید محصولات امنیتی ملاک نبوده و همواره محصولات امنیتی را از نمایندگی های رسمی محصولات خریداری نمایید.

با ما امن بمانید.

حمله‌ی تایپ‌اسکواتینگ در عمل

در نگاه اول، این ایمیل ظاهراً از طرف مایکروسافت ارسال شده است:

اما با بررسی دقیق‌تر مشخص می‌شود که دامنه‌ی واقعی فرستنده، rnicrosoft Com است ،جایی که حروف "r" و "n" کنار هم قرار گرفته‌اند تا شبیه حرف "m" به نظر برسند.این تکنیک که با نام TypoSquatting یا Homograph Spoofing شناخته می‌شود، یکی از رایج‌ترین روش‌های فیشینگ در سال‌های اخیر است و به سرعت در کمپین‌های هدفمند برای سرقت اطلاعات کاربری و دسترسی به حساب‌های حساس سازمان‌ها گسترش یافته است.

تحلیل فنی

سوءاستفاده از ثبت دامنه‌ها

مهاجمان دامنه‌هایی ثبت می‌کنند که از نظر ظاهری بسیار شبیه دامنه‌های معتبر سازمانی هستند. روش های رایج شامل:

- ترکیب کاراکترهای ASCII: مثال rn ▯ m
- استفاده از نویسه‌های Unicode مشابه حروف لاتین (حروف سیریلیک یا نمادهای شبیه به حروف انگلیسی)
- ثبت دامنه‌های با غلط‌های املایی رایج یا فاصله های اضافی در دامنه

هدف از این کار، ایجاد حس اعتماد اولیه و گول زدن کاربر است.

دور زدن احراز هویت ایمیل

برای افزایش موفقیت، این دامنه‌ها اغلب با رکوردهای SPF و DKIM معتبر پیکربندی می‌شوند تا از فیلترهای امنیتی عبور کنند

به این ترتیب، حتی کاربرانی که نسبت به ایمیل های ناشناس محتاط هستند، ممکن است به اشتباه این پیام‌ها را معتبر فرض کنند.

تحویل Payload

محتوای ایمیل معمولاً شبیه اعلان‌های بازنشانی رمز عبور، پیام‌های MFA یا اطلاعیه‌های امنیتی رسمی است.

قربانی با کلیک روی لینک به صفحه ورود جعلی هدایت می‌شود.

این صفحات معمولاً از HTTPS و گواهی SSL معتبر استفاده می‌کنند تا حس واقعی بودن سایت را منتقل کنند و اطلاعات کاربری یا کوکی های نشست را جمع‌آوری کنند.

توصیه‌های دفاعی

اجرای سیاست DMARC:

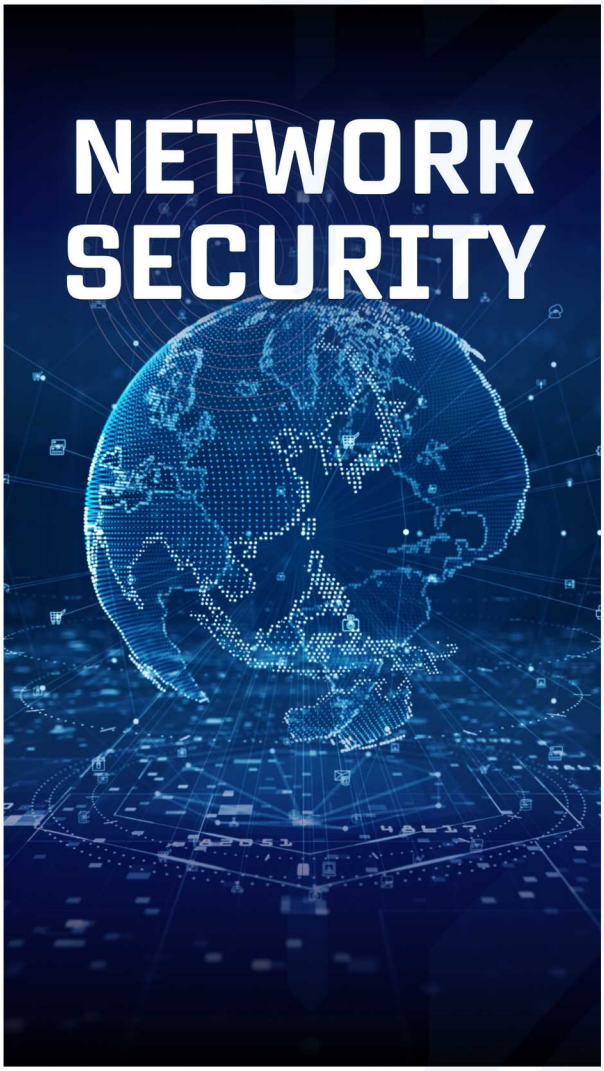
ایمیل‌هایی که با سیاست DMARC همخوانی ندارند، رد یا قرنطینه شوند. این کار از جعل دامنه و حملات فیشینگ جلوگیری می‌کند.

پایش مداوم برند و شناسایی دامنه های مشابه:

با استفاده از ابزارهای تخصصی، دامنه‌های جعلی یا شبیه به دامنه برند را رصد کنید تا پیش از سوءاستفاده، شناسایی و مسدود شوند. در این حوزه استفاده از راهکارهای امنیتی پیشرفته همچون Security for Mail Server راهکار ESET پیشنهاد می‌گردد.

استفاده از سامانه‌های امنیتی پیشرفته ایمیل:

فناوری‌های مبتنی بر هوش مصنوعی و الگوریتم‌های یادگیری ماشین می‌توانند شباهت‌های ظاهری و ناهنجاری‌های نام‌های نمایشی را تشخیص دهند و از رسیدن ایمیل‌های خطرناک به کاربران جلوگیری کنند. این قابلیت نیز یکی از ویژگی‌های موجود در راهکار Security for Mail محصولات ESET می‌باشد.



آموزش کاربران نهایی:

به کاربران آموزش دهید که همیشه دامنه‌ها را دقیق بررسی کنند. حتی یک تفاوت کوچک مانند "rn" به جای "m" می‌تواند نشانه‌ی یک حمله فیشینگ باشد. تمرین‌های دوره‌ای و شبیه‌سازی حملات می‌تواند اثرگذاری آموزش را افزایش دهد.

اهمیت موضوع

طبق گزارش‌های اخیر، بیش از ۳۰٪ از دامنه‌های فیشینگ در سال ۲۰۲۴ نسخه‌های فریبنده و شبیه به ارائه‌دهندگان بزرگ سازمانی بوده‌اند.
این آمار نشان می‌دهد که حتی شرکت‌های بزرگ نیز همواره هدف حملات تایپ‌اسکواتینگ و Homograph Spoofing هستند.

سخن پایانی

شرکت « مدیران شبکه برنا » با پشتوانه ای از تجربه و دانش تخصصی و تمرکز بر ارائه راهکارهای نوین امنیت شبکه همواره تلاش کرده است تا نیازهای امنیتی سازمان ها و شرکت ها را در بالاترین سطح پوشش دهد . ما با بهره گیری از محصولات و فناوری های برتر جهانی در حوزه های چون , DLP EDR , XDR فایروال ؛ انتی ویروس DRM و NDR سعی کرده ایم فضای سایبری امن و پایدار برای مشتریان خود فراهم کنیم.
ماموریت ما فراتر از ارائه محصول است . ما به دنبال ارائه راهکارهایی هستیم که نه تنها امنیت شبکه و داده های سازمان ها را تضمین می کنند بلکه امکان مدیریت هوشمند تهدیدات ؛ انطباق پذیری با الزامات قانونی و افزایش بهره وری فناوری اطلاعات را نیز به همراه دارند . در این مسیر ؛ تیم فنی متخصص ؛ پشتیبانی سریع و ارائه مشاوره دقیق ؛ از ارزش های محوری شرکت ما به شمار می آیند.
ما باور داریم که امنیت سایبری صرفا یک محصول نیست ؛ بلکه یک تعهد دائمی و یک رویکرد حرفه ای برای حفظ سرمایه های اطلاعاتی سازمان هاست.شرکت مدیران شبکه برنا همواره همراهی قابل اعتماد برای سازمان ها و مدیران فناوری اطلاعات بوده و خواهد بود.

در پایان ؛ امیدواریم این رزومه بتواند نمایی شفاف از توانمندی ها ؛ حوزه های تخصصی و خدمات ما ارائه دهد و زمینه ساز همکاری های حرفه ای و مؤثر با سازمان شما باشد . آماده ایم تا در کنار شما ؛ گامی مطمئن در مسیر توسعه و امنیت برداریم.

www.bornanetwork.co info@bornanetwork.co ۰۲۱-۷۴۰۲۸