ماهنامه برنا

Borna Network Managers
مدیران شبکه برنا

اخبار حوزه امنیت و شبکه (فروردین ۱۴۰۵)

بهره‌برداری فعال از آسیب‌پذیری بحرانی FortiClient EMS زنگ خطر تازه‌ای برای امنیت زیرساخت‌های سازمانی به‌صدا درآورده است. هم زمان، یک کمپین پنهان با دستکاری DNS روترها از سال ۲۰۲۲ کاربران را در سکوت کامل هدف قرار داده است. در حوزه تهدیدات مالی، موج تازه‌ای از فیشینگ بانکی با سوءاستفاده از اختلالات خدمات، کاربران را به صفحات جعلی هدایت می‌کند. از سوی دیگر، ردیابی انبوه دستگاه های موبایل از طریق داده‌های تبلیغاتی و نیز افشای اطلاعات عملیاتی از طریق سنسورهای ساده، چهره جدیدی از مخاطرات حریم خصوصی و OPSEC را نمایان ساخته است.

ویژه مدیران و کارشناسان شبکه و امنیت

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

خبرنامه امنیت سایبری - فروردین ماه ۱۴۰۵

زنگ خطر در قلب مدیریت امنیت: بهره‌برداری فعال از آسیب‌پذیری FortiClient EMS

افشای آسیب‌پذیری بحرانی CVE-2026-35616 در سامانه FortiClient EMS بار دیگر نشان داد که حتی سامانه‌های مدیریتی که برای تقویت امنیت طراحی شده‌اند، می‌توانند به نقطه ورود مهاجمان تبدیل شوند. این نقص که گزارش‌های متعدد از بهره‌برداری فعال آن منتشر شده، سطح تهدید را از یک هشدار فنی ساده فراتر برده و آن را به یک بحران بالقوه برای سازمان‌ها تبدیل کرده است. FortiClient EMS به‌عنوان محور مدیریت متمرکز تنظیمات امنیتی و سلامت دستگاه‌ها عمل می‌کند و هرگونه ضعف در آن می‌تواند پیامدهایی بسیار گسترده داشته باشد.

ماهیت این آسیب‌پذیری به کنترل دسترسی نادرست بازمی‌گردد؛ ضعفی که به مهاجم اجازه می‌دهد بدون نیاز به هرگونه اعتبارنامه، از راه دور درخواست‌های خاص ارسال کرده و دستورات غیرمجاز اجرا کند. در چنین شرایطی، مهاجم قادر است تنظیمات امنیتی Endpointها را تغییر دهد، مکانیزم‌های دفاعی را غیرفعال کند یا حتی بدافزار را به‌صورت متمرکز در شبکه توزیع نماید. از آنجا که EMS یک نقطه مرکزی مدیریت است، دامنه تأثیرگذاری این نفوذ بسیار گسترده خواهد بود.

گزارش بهره‌برداری فعال نشان می‌دهد زمان واکنش سازمان‌ها محدود است و تأخیر در نصب اصلاحیه منتشرشده، احتمال نفوذ را به‌شدت افزایش می‌دهد. نصب فوری به‌روزرسانی، بررسی نسخه همه سرورهای EMS، پایش دقیق لاگ‌ها و در صورت نیاز، محدودسازی دسترسی شبکه‌ای از جمله اقدامات ضروری است. این رخداد بار دیگر اهمیت معماری مبتنی بر حداقل دسترسی، پایش مستمر و نگاه پیشگیرانه به امنیت سایبری را یادآوری می‌کند.

خبرنامه امنیت سایبری - فروردین ماه ۱۴۰۵

نفوذ بی‌صدا به دروازه اینترنت؛ کمپین پنهان دستکاری DNS در روترها

در حالی که بسیاری از سازمان‌ها تمرکز خود را بر امنیت سرورها و سرویس‌های حیاتی گذاشته‌اند، یک کمپین پنهان از سال ۲۰۲۲ با هدف قرار دادن روترهای خانگی و اداری نشان داده است که تهدیدات امروزی می‌توانند از ساده‌ترین نقاط ورود آغاز شوند. بررسی های امنیتی نشان می‌دهد مهاجمان با نفوذ به پنل مدیریتی این تجهیزات، تنظیمات DNS را تغییر داده و بخشی از ترافیک اینترنت کاربران را به مسیرهای تحت کنترل خود هدایت می‌کنند؛ فرآیندی که بدون ایجاد نشانه‌های آشکار، برای مدت طولانی پنهان باقی می ماند.

جذابیت این هدف در آن است که روترها نقطه عبور تمام ترافیک شبکه هستند و بسیاری از کاربران، به روزرسانی امنیتی یا تغییر رمز عبور پیش‌فرض آن‌ها را جدی نمی‌گیرند. مهاجمان پس از دسترسی، آدرس‌های DNS را به سرورهای جعلی تغییر داده و از طریق زیرساختی پیچیده، پاسخ‌ها را به‌صورت انتخابی دستکاری می‌کنند. این روش، زمینه اجرای حملات adversary-in-the-middle را فراهم می‌سازد؛ جایی که کاربر تصور می‌کند ارتباطش عادی است، اما عملاً داده ها از مسیر واسط عبور می‌کند.

پیامد چنین حمله‌ای می‌تواند هدایت کاربران به صفحات فیشینگ، تزریق بدافزار یا رهگیری ترافیک باشد. برای مقابله، بررسی دوره‌ای تنظیمات DNS، تغییر رمز عبور، محدودسازی دسترسی مدیریتی و به‌روزرسانی Firmware ضروری است. این رخداد یادآور آن است که امنیت شبکه زمانی مؤثر است که حتی کوچک ترین تجهیزات، بخشی جدی از زنجیره دفاعی تلقی شوند.

فیشینگ در سایه اختلال؛ مهندسی اجتماعی علیه حساب های بانکی

گسترش خدمات بانکداری دیجیتال، در کنار مزایای گسترده، زمینه‌ای تازه برای سوءاستفاده مهاجمان فراهم کرده است. در موج اخیر حملات، پیام‌هایی با عنوان «اختلال در سامانه بانکی» منتشر شده که کاربران را به لینک‌هایی هدایت می‌کند که ظاهری مشابه اطلاعیه های رسمی دارند، اما در واقع صفحات فیشینگ هستند. این سناریو زمانی بیشترین اثر را دارد که هم زمان اختلالی واقعی در خدمات رخ داده باشد و کاربر در انتظار دریافت اخبار فوری باشد.

در این حملات، قربانی پس از ورود به صفحه جعلی، اطلاعات حساس نظیر نام کاربری، رمز عبور یا رمز پویا را وارد می‌کند و عملاً دسترسی حساب خود را در اختیار مهاجم قرار می‌دهد. در برخی موارد نیز فایل‌های آلوده برای نصب بدافزار ارائه می‌شود که می‌تواند زمینه نفوذ عمیق‌تر به دستگاه یا حتی شبکه سازمانی را فراهم کند.

مقابله با چنین تهدیداتی نیازمند رویکردی چندلایه است. در سطح شبکه، فایروال‌های نسل جدید، سامانه‌های تشخیص نفوذ و ابزارهای تحلیل رفتار می‌توانند ارتباط با دامنه‌های مشکوک را شناسایی و مسدود کنند. با این حال، عنصر انسانی همچنان حلقه حساس این زنجیره است. آموزش کاربران برای تشخیص لینک‌های جعلی و استفاده انحصاری از درگاه‌های رسمی بانکی، نقشی تعیین‌کننده در کاهش موفقیت حملات فیشینگ دارد.

خبرنامه امنیت سایبری - فروردین ماه ۱۴۰۵

ردیابی پنهان در اقتصاد تبلیغات؛ چگونه داده‌های موبایل به ابزار نظارت تبدیل می‌شوند؟

در سال‌های اخیر داده‌های رفتاری کاربران به یکی از ارزشمندترین منابع اقتصاد دیجیتال تبدیل شده‌اند. بسیاری از اپلیکیشن‌های موبایلی برای نمایش تبلیغات هدفمند، اطلاعاتی مانند شناسه تبلیغاتی دستگاه (AdID)، موقعیت مکانی تقریبی و الگوی استفاده از برنامه‌ها را جمع‌آوری می‌کنند. هرچند هدف اعلام‌شده این داده‌ها بهبود تجربه تبلیغات است، اما گزارش‌های تازه نشان می‌دهد همین اطلاعات می‌توانند در مقیاسی گسترده برای ردیابی جغرافیایی دستگاه‌ها مورد استفاده قرار گیرد.

در این روش، داده‌های جمع‌آوری‌شده از طریق کیت‌های تبلیغاتی در اپلیکیشن‌ها تجمیع شده و با تحلیل کلان داده، الگوهای حرکت کاربران استخراج می‌شود. ترکیب اطلاعاتی مانند مختصات مکانی، زمان اتصال و آدرس های IP ژئولکال‌شده می‌تواند تصویری نسبتاً دقیق از رفت‌وآمد روزانه یک دستگاه ارائه دهد. در مقیاس بزرگ، چنین داده‌هایی امکان پایش صدها میلیون دستگاه را فراهم می‌کند؛ آن هم بدون نیاز به نفوذ مستقیم به گوشی یا نصب بدافزار.

از منظر امنیت سایبری، چنین زیرساختی چالش های مهمی ایجاد می‌کند. پایگاه‌های داده حاوی اطلاعات مکانی به هدفی جذاب برای مهاجمان تبدیل می‌شوند و در صورت افشا می‌توانند الگوهای رفتاری کاربران یا حتی کارکنان سازمان های حساس را آشکار کنند. به همین دلیل، رمزنگاری ارتباطات، کنترل دقیق دسترسی به داده ها و استفاده از محصولات امنیت شبکه پیشرفته برای محافظت از این زیرساخت‌ها ضروری است.

این روند نشان می‌دهد تهدیدات جدید لزوماً از طریق حملات مستقیم شکل نمی‌گیرند؛ گاهی داده‌هایی که برای اهداف تجاری جمع‌آوری شده اند، خود به ابزاری قدرتمند برای نظارت و ردیابی تبدیل می‌شوند.

خبرنامه امنیت سایبری - فروردین ماه ۱۴۰۵

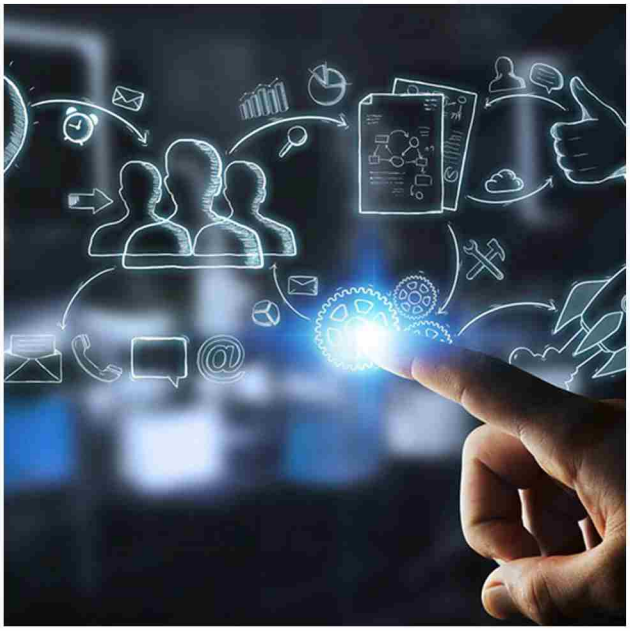
OPSEC در عصر سنسورها؛ وقتی یک کارت‌پستال کوچک می تواند یک ناو را لو دهد

امنیت عملیاتی یا OPSEC سال‌ها بر پایه جلوگیری از افشای ناخواسته اطلاعات حساس تعریف شده بود، اما در سال‌های اخیر ماهیت تهدیدها دگرگون شده است. اکنون دیگر برای افشای موقعیت یک شناور نظامی یا مسیر لجستیکی یک پایگاه، نیازی به بدافزارهای پیچیده یا نفوذ شبکه‌ای وجود ندارد؛ گاهی یک ردیاب ارزان‌قیمت بلوتوثی، پنهان‌شده در یک کارت‌پستال معمولی، می‌تواند همان کاری را انجام دهد که سابقاً تنها از عهده عملیات جاسوسی پیشرفته برمی‌آمد.

در سناریوی اخیر، پژوهشگران امنیتی نشان دادند که یک کارت‌پستال حاوی ردیاب، هنگام انتقال از مسیر پست نظامی، همراه با جریان عادی عملیات لجستیک حرکت می‌کند. هیچ‌یک از لایه‌های امنیت سایبری کلاسیک—فایروال، سیستم تشخیص نفوذ یا نظارت شبکه—قادر به شناسایی چنین انتقال فیزیکی نیستند. با این حال، دستگاه کوچک می‌تواند موقعیت و مسیر حرکت را به‌صورت مستمر ثبت کند و این اطلاعات، در دست یک تحلیلگر OSINT، تصویر دقیقی از تحرکات یک یگان نظامی ارائه می‌دهد.

این مسئله مشابه رخداد مشهور Strava است؛ جایی که داده‌های عمومی ورزش کاربران، به‌دلیل تجمیع و تحلیل، موقعیت پایگاه‌های نظامی را آشکار کرد. در هر دو مورد مشکل، «داده محرمانه» نبود، بلکه کنار هم قرار گرفتن داده‌های بی اهمیت بود.

این تحول نشان می‌دهد OPSEC امروز نیازمند نگاهی تازه است: شناخت اشیای متصل به عنوان سنسور بالقوه، کنترل دقیق زنجیره‌های لجستیکی و آموزش عملیاتی مبتنی بر تحلیل رفتار داده. چنین رویکردی است که می‌تواند در برابر تهدیدات فیزیکال–دیجیتال جدید ایجاد تاب آوری کند.



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

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.