Borna Network Managers
مدیران شبکه برنا

ماهنامه برنا

اخبار حوزه امنیت و شبکه (خرداد ۱۴۰۵)

در این شماره به بررسی تازه‌ترین تهدیدات امنیت سایبری در جهان می‌پردازیم؛ از عملیات جاسوسی گروه‌های پیشرفته تا کمپین‌های باج افزاری و نشت داده‌های سازمانی. گزارش‌هایی از فعالیت گروه‌های UNC۶۵۰۸ و FishMonger، باج‌افزار Gentlemen و ماجرای نشت اطلاعات Kodak را مرور کرده‌ایم.همچنین چالش‌های امنیتی دوران اختلال اینترنت، مدیریت آسیب‌پذیری‌ها و راهکارهای افزایش تاب آوری سازمان‌ها در برابر تهدیدات پیشرفته تحلیل شده است.

ویژه مدیران و کارشناسان شبکه و امنیت

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

خبرنامه امنیت سایبری - خرداد ماه ۱۴۰۵

شکارچیان سایبری در کمین زیرساخت‌های استراتژیک؛ تحلیل کمپین جاسوسی گروه UNC6508

گزارش اخیر «گروه اطلاعات تهدید گوگل» (GTI)، از فعالیت‌های هدفمند گروه جاسوسی سایبری «UNC6508» پرده برداشته است؛ گروهی که با انتساب به چین، سازمان‌های کلیدی در حوزه‌های سلامت، صنایع دفاعی، زیرساخت‌های نظامی و پژوهش‌های پیشرفته هوش مصنوعی در آمریکای شمالی را نشانه رفته است. برخلاف حملات سایبری متداول، استراتژی این مهاجمان تنها به نفوذ اولیه محدود نمی‌شود؛ آن ها با بهره‌گیری از زیرساخت‌های چندمرحله‌ای و پیچیده، به دنبال دستیابی به دسترسی‌های طولانی مدت، حفظ ماندگاری در شبکه قربانیان و حرکت‌های جانبی برای سرقت داده‌های حساس و اطلاعات راهبردی هستند.

این کمپین از منظر اطلاعات تهدید (Threat Intelligence)، اهمیت فوق‌العاده‌ای دارد. انتخاب هم زمان بخش‌های درمانی و نظامی نشان می‌دهد که هدف مهاجمان، نه فقط خرابکاری، بلکه کسب برتری ژئوپلیتیکی و جمع‌آوری داده‌هایی با ارزش اطلاعاتی بالاست. برای تیم‌های مرکز عملیات امنیت (SOC) و پاسخ به حوادث (IR)، شناسایی این نوع تهدیدات نیازمند فراتر رفتن از تحلیل ساده شاخص‌های آلودگی (IOC) است. سازمان‌ها باید الگوهای رفتاری (TTPs) و ساخت‌های پنهان مهاجمان را با دقت تحلیل کنند.

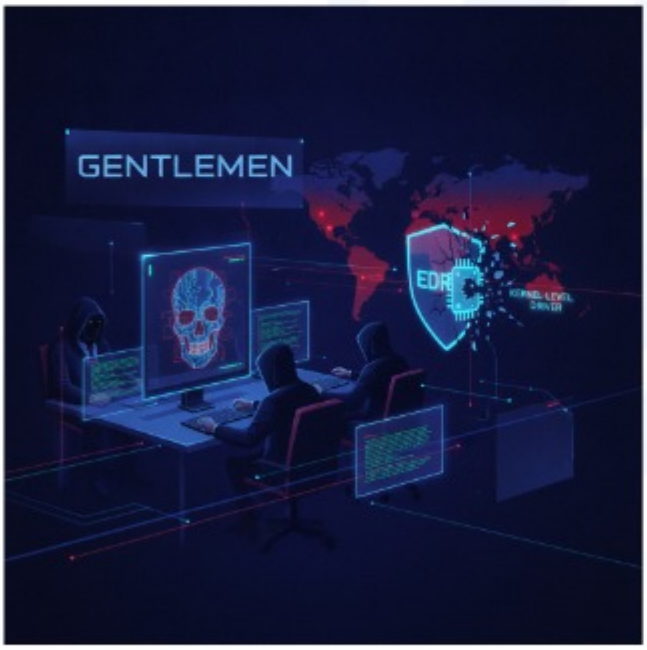
آدر مواجهه با بازیگران پیشرفته (APT)، دفاع‌های واکنشی دیگر کارآمد نیستند. سازمان‌ها نیازمند راهکارهای اطلاعات تهدید عملیاتی هستند تا بتوانند داده‌ها را به‌درستی همبسته‌سازی، اولویت‌بندی و در فرآیندهای امنیتی ادغام کنند. تنها با داشتن دیدگاهی جامع نسبت به تهدیدات صنعت‌محور و دارایی‌های در معرض ریسک، می‌توان فاصله میان «آگاهی از خطر» و «اقدام بازدارنده» را به حداقل رساند. در عصر حاضر، پیش‌دستی در شناسایی این کمپین‌های جاسوسی، کلید اصلی بقای زیرساخت‌های حیاتی است.

Gentlemen؛ باج‌افزاری که ابتدا EDR را می‌کشد

در سال‌های اخیر باج‌افزارها به یکی از جدی‌ترین تهدیدهای امنیت سایبری برای سازمان‌ها تبدیل شده اند. در میان بازیگران جدید این حوزه، گروه Gentlemen به‌سرعت توجه پژوهشگران امنیتی را جلب کرده است. این گروه که با مدل Ransomware-as-a-Service (RaaS) فعالیت می‌کند، از اواخر سال ۲۰۲۵ وارد صحنه شد و در مدت کوتاهی توانست جایگاه قابل توجهی در اکوسیستم باج‌افزار به دست آورد. بررسی‌های شرکت امنیتی ESET نشان می دهد که این گروه علاوه بر اجرای حملات متعدد، تمرکز ویژه‌ای بر توسعه ابزارهای پیشرفته برای دور زدن سامانه های دفاعی سازمان‌ها دارد.

یکی از مهم‌ترین ویژگی‌های Gentlemen، سرمایه‌گذاری جدی بر ابزارهای موسوم به EDR Killer است؛ ابزارهایی که برای غیرفعال کردن راهکارهای Endpoint Detection and Response طراحی شده‌اند. این سامانه‌ها معمولاً آخرین لایه دفاعی در برابر حملات پیشرفته محسوب می‌شوند، بنابراین مهاجمان تلاش می‌کنند پیش از اجرای باج‌افزار، آن‌ها را از کار بیندازند. چارچوب اصلی مورد استفاده این گروه که توسط پژوهشگران GentleKiller نام‌گذاری شده، با سوءاستفاده از درایورهای آسیب‌پذیر و تکنیک BYOVD امکان دسترسی در سطح کرنل سیستم را فراهم می‌کند و به مهاجمان اجازه می‌دهد فرایندهای امنیتی را متوقف کنند.

علاوه بر این، گروه Gentlemen از ابزارهای شخص ثالث مانند HexKiller و HavocKiller نیز استفاده می‌کند و برای سرقت داده‌ها ابزاری به نام OxideHarvest را به کار می‌گیرد. مدل تجاری این گروه نیز جذاب است؛ به‌طوری‌که حدود ۹۰ درصد درآمد حملات به همکاران اختصاص داده می‌شود. این ساختار باعث گسترش سریع شبکه مهاجمان و افزایش دامنه حملات در مناطق مختلف جهان شده است.



تاب‌آوری دیجیتال در دوران پساجنگ؛ وقتی اینترنت دیگر قابل اتکا نیست

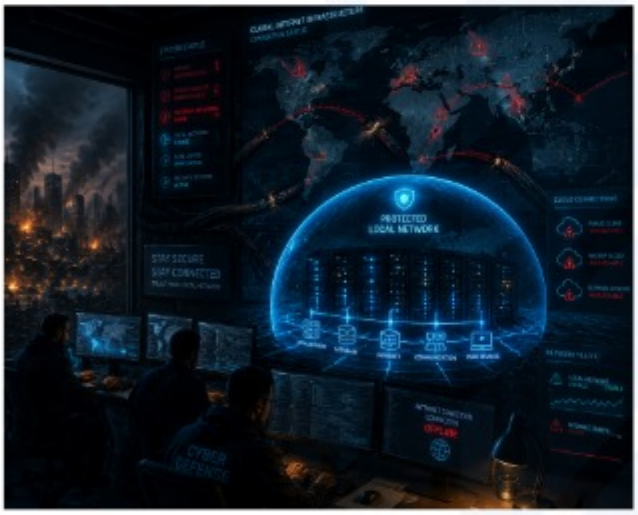
با فروکش‌کردن تنش‌های نظامی، توجه عمومی معمولاً از بحران فاصله می‌گیرد، اما برای تیم‌های فناوری اطلاعات و امنیت، دوران پساجنگ آغاز مرحله‌ای تازه از چالش‌هاست. تجربه ماه‌های اخیر نشان داد که تهدیدات سایبری تنها به حملات مستقیم محدود نمی شوند و اختلال گسترده یا قطع طولانی‌مدت اینترنت می‌تواند به بحرانی جدی برای عملیات سازمان‌ها تبدیل شود. در چنین شرایطی، بسیاری از سازمان‌ها با توقف یا اختلال در سرویس‌های حیاتی، کاهش دید امنیتی و از کار افتادن بخشی از ابزارهای مدیریتی و ارتباطی مواجه شدند. این تجربه نشان می‌دهد که دسترسی پایدار به اینترنت دیگر یک پیش‌فرض قطعی برای تداوم کسب‌وکار نیست.

نخستین گام برای مواجهه با این واقعیت، بازبینی وابستگی سازمان‌ها به اینترنت و سرویس‌های خارجی است. بسیاری از ابزارهای ابری، سرویس‌های SaaS، سامانه‌های احراز هویت و حتی برخی ابزارهای امنیتی در زمان اختلال اینترنت دچار مشکل می‌شوند. به همین دلیل، سازمان‌ها باید برای سرویس‌های حیاتی خود مسیرهای جایگزین و نسخه‌های محلی در نظر بگیرند.

در کنار این موضوع، طراحی سناریوهای تداوم کسب وکار در شرایط قطع ارتباط اهمیت زیادی دارد.

نگهداری نسخه‌های محلی داده‌های حیاتی، استقرار سرویس‌های ارتباطی داخلی و تعریف روش‌های جایگزین برای احراز هویت از جمله اقداماتی است که می‌تواند تاب‌آوری سازمان را افزایش دهد.

در نهایت، تجربه اختلال‌های اخیر نشان می‌دهد که امنیت سایبری تنها به مقابله با مهاجمان محدود نمی‌شود. سازمان‌هایی موفق‌تر خواهند بود که امنیت را در قالب «تاب‌آوری دیجیتال» تعریف کنند؛ یعنی توان ادامه فعالیت حتی در شرایط قطع ارتباط، محدودسازی شبکه و بی ثباتی زیرساخت‌های ارتباطی.



تنشت داده در Kodak؛
ادعای سرقت ۲.۲ میلیون رکورد توسط ShinyHunters

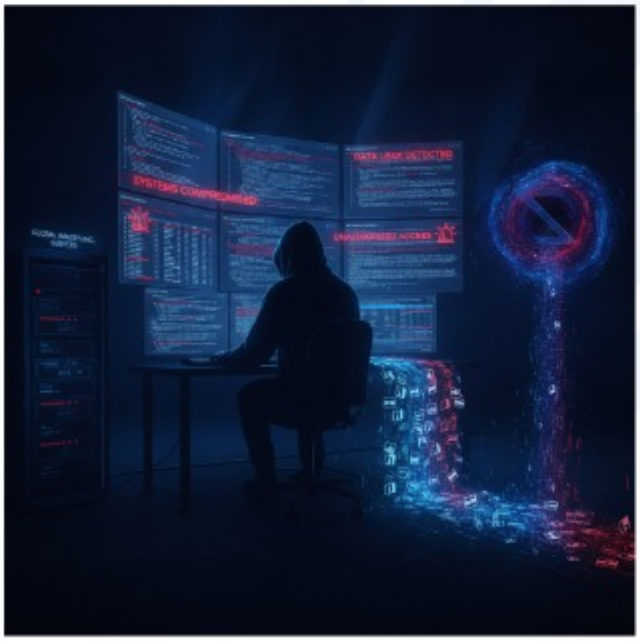
شرکت Kodak به‌تازگی وقوع یک رخداد امنیتی و نشت اطلاعات را تأیید کرده است؛ حادثه‌ای که پس از ادعای گروه اخاذی سایبری ShinyHunters درباره سرقت بیش از ۲.۲ میلیون رکورد داده از این شرکت رسانه‌ای شد. بر اساس گزارش‌های منتشرشده، نام Kodak در وب‌سایت افشای داده این گروه قرار گرفته و مهاجمان مدعی شده‌اند که علاوه بر اطلاعات مشتریان، به بخشی از داده‌های داخلی سازمان نیز دسترسی پیدا کرده‌اند. این ادعا نگرانی‌های قابل توجهی درباره میزان داده‌های در معرض افشا ایجاد کرده است.

Kodak در بیانیه‌ای اعلام کرده که با همکاری کارشناسان امنیتی خارجی در حال بررسی ابعاد این حادثه است. طبق اطلاعات اولیه، یک شخص ثالث غیرمجاز برای مدت محدودی به بخشی از داده‌های شرکت دسترسی داشته است. با این حال، گروه ShinyHunters مدعی است حجم اطلاعات سرقت‌شده بسیار فراتر از مواردی است که تاکنون به‌صورت رسمی تأیید شده و شامل میلیون‌ها رکورد مرتبط با داده‌های مشتریان و اطلاعات سازمانی می‌شود.
این رخداد نمونه‌ای از روند رو به گسترش حملات مبتنی بر سرقت داده و اخاذی است. در این مدل، مهاجمان ابتدا اطلاعات ارزشمند سازمان را استخراج کرده و سپس با تهدید به انتشار عمومی آن‌ها، قربانی را برای پرداخت باج تحت فشار قرار می‌دهند.

چنین حملاتی علاوه بر اختلال فنی، می‌تواند پیامدهای اعتباری، حقوقی و مالی گسترده‌ای برای سازمان‌ها به همراه داشته باشد.

به همین دلیل، سازمان‌ها باید در کنار کنترل های امنیتی سنتی، بر راهکارهایی مانند طبقه بندی داده، سامانه‌های DLP، پایش رفتار کاربران و شناسایی انتقال غیرعادی اطلاعات سرمایه‌گذاری کنند تا از تبدیل یک نفوذ محدود به بحران افشای داده جلوگیری شود.

اگر دوست داشته باشی، می‌توانم یک الگوی ثابت ۲۲۷ کلمه‌ای مخصوص ماهنامه‌ات هم طراحی کنم تا همه مقاله‌ها از نظر طول، ریتم و ساختار یکدست شوند.



خبرنامه امنیت سایبری - خرداد ماه ۱۴۰۵

SprySOCKS ویندوزی؛
گسترش ابزار جاسوسی گروه FishMonger

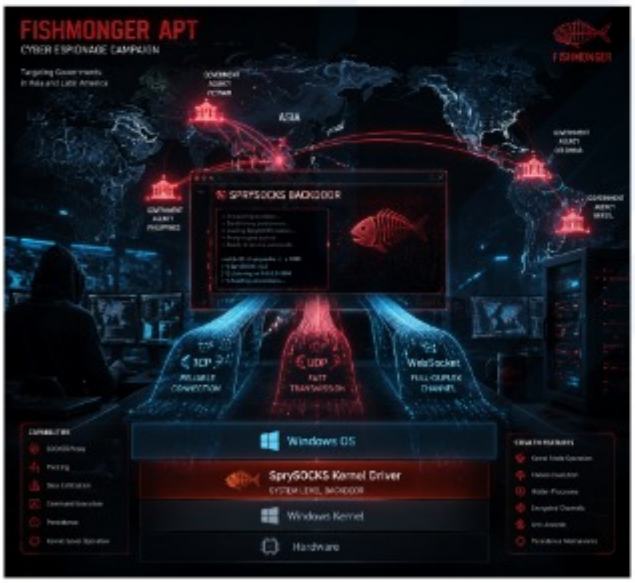
در سال‌های اخیر فعالیت گروه‌های جاسوسی سایبری وابسته به دولت‌ها به‌طور چشمگیری افزایش یافته است و بسیاری از این گروه‌ها با توسعه ابزارهای پیچیده به دنبال نفوذ بلندمدت به شبکه‌های حساس هستند. یکی از این بازیگران، گروه FishMonger است که بر اساس گزارش پژوهشی ESET Research در ژوئن ۲۰۲۶ بار دیگر مورد توجه تحلیلگران امنیتی قرار گرفته است. این گروه که به چین نسبت داده می‌شود، با به‌روزرسانی مجموعه ابزارهای خود حملاتی را علیه سازمان‌های دولتی در چندین کشور انجام داده است.

پژوهشگران در این گزارش دو نسخه جدید و پیش‌تر مستندسازی‌نشده از درب پشتی SprySOCKS برای سیستم‌عامل ویندوز را شناسایی کرده‌اند. این بدافزار که پیش‌تر تنها در محیط لینوکس مشاهده شده بود، اکنون با نمونه‌های WIN_DRV و WIN_PLUS در حملات واقعی بین سال‌های ۲۰۲۳ تا ۲۰۲۴ مورد استفاده قرار گرفته است. داده‌های تله‌متری نشان می‌دهد اهداف اصلی این کمپین‌ها سازمان‌های دولتی در کشورهایی مانند تایوان، تایلند، پاکستان و هندوراس بوده‌اند.

نسخه ویندوزی SprySOCKS قابلیت‌های گسترده‌ای برای کنترل سیستم آلوده در اختیار مهاجمان قرار می دهد.

برای مثال، نسخه WIN_DRV بیش از ۳۰ دستور مختلف برای ارتباط با سرور فرماندهی و کنترل پشتیبانی می‌کند و امکان جمع‌آوری اطلاعات سیستم، مدیریت فایل‌ها و کنترل فرایندهای در حال اجرا را فراهم می‌سازد. همچنین این بدافزار می‌تواند از پروتکل‌های TCP، UDP و WebSocket برای ارتباط با سرورهای مهاجم استفاده کند.

از مهم‌ترین ویژگی‌های این نسخه، استفاده از درایورهای سطح کرنل برای پنهان‌سازی فعالیت بدافزار است. این درایورها می‌توانند اتصالات شبکه، فرایندها و فایل‌های مرتبط با بدافزار را از دید ابزارهای امنیتی مخفی کرده و شناسایی آن را برای سامانه‌های دفاعی دشوارتر کنند.



ریسک پنهان پس از بحران؛ انباشت آسیب‌پذیری‌های وصله‌نشده

در دوره‌های طولانی اختلال یا محدودیت اینترنت، بسیاری از سازمان‌ها تمرکز خود را بر حفظ دسترسی و تداوم سرویس‌ها قرار می‌دهند. با این حال، کارشناسان امنیت سایبری هشدار می‌دهند که یکی از پیامدهای مهم چنین شرایطی، انباشت آسیب‌پذیری های وصله‌نشده در زیرساخت‌های فناوری اطلاعات است. محدودیت در دریافت به‌روزرسانی‌ها، Patchهای امنیتی و ارتباط با سرویس‌های پشتیبانی خارجی می تواند باعث شود تعداد زیادی از ضعف‌های امنیتی برای مدت طولانی بدون اصلاح باقی بمانند.

در بسیاری از سازمان‌ها، فرآیند Patch Management به طور مستقیم به دسترسی پایدار اینترنت وابسته است. زمانی که امکان دریافت به‌روزرسانی‌های سیستم عامل، تجهیزات شبکه، فایروال‌ها، سامانه‌های مجازی سازی یا نرم‌افزارهای سازمانی محدود شود، ده‌ها آسیب‌پذیری شناخته‌شده ممکن است هفته‌ها یا حتی ماه‌ها اصلاح نشوند. این شرایط زمانی خطرناک تر می‌شود که مهاجمان معمولاً پس از پایان بحران، شبکه‌ها را برای یافتن سامانه‌های وصله‌نشده به‌طور گسترده اسکن می‌کنند.

با بازگشت تدریجی ارتباطات، احتمال افزایش اسکن های اینترنتی و تلاش برای سوءاستفاده از این آسیب پذیری‌ها وجود دارد. سرویس‌های اینترنتی، VPNها، تجهیزات Edge، سامانه‌های دسترسی از راه دور و ایمیل ورها از جمله دارایی‌هایی هستند که بیش از سایر در معرض خطر قرار دارند.

بسیاری از حملات موفق نیز از سوءاستفاده از همین آسیب‌پذیری‌های شناخته‌شده آغاز می شوند.

به همین دلیل، متخصصان توصیه می‌کنند سازمان‌ها پس از بازگشت شرایط عادی، یک برنامه فشرده برای ارزیابی آسیب‌پذیری و مدیریت وصله‌ها اجرا کنند. اولویت‌بندی آسیب پذیری‌های بحرانی، بررسی سرویس‌های در معرض اینترنت و مقایسه وضعیت فعلی با Baseline امنیتی پیش از بحران می‌تواند به جبران «بدهی امنیتی» ایجادشده در این دوره کمک کند.

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 XDR , EDR 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.