Boma Network Managers
مدیران شبکه برنا

خبرنامه برنا

اخبار حوزه امنیت و شبکه (مهر 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
(رایگان، تخصصی، به‌روز)

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

پایان پشتیبانی مایکروسافت از Windows 10
زمان مهاجرت به Windows 11 فرا رسیده است.
مایکروسافت رسماً اعلام کرده است که در تاریخ ۱۴ اکتبر ۲۰۲۵ (۲۲ مهر ۱۴۰۴) چرخه پشتیبانی از Windows 10 پایان می‌رسد. این تاریخ پایان ارائه به‌روزرسانی های امنیتی، Bug Fix، و پشتیبانی رسمی برای تمامی نسخه‌های Windows 10 است.
نسخه22H2 آخرین به‌روزرسانی اصلی این سیستم عامل محسوب می‌شود.
پیامدهای فنی برای سازمان‌ها
افزایش ریسک امنیتی:
پس از پایان پشتیبانی، هیچ به‌روزرسانی امنیتی منتشر نمی‌شود. این یعنی هر آسیب‌پذیری جدید می‌تواند مستقیماً امنیت شبکه سازمان را تهدید کند.
کاهش پایداری و سازگاری:
نرم‌افزارها و درایورهای جدید احتمالاً دیگر از Windows 10 پشتیبانی نخواهند کرد. در نتیجه، یکپارچگی زیرساخت IT ممکن است مختل شود.
هزینه‌های پنهان نگهداری:
باقی‌ماندن بر روی Windows 10 پس از پایان پشتیبانی، هزینه‌های امنیتی و مدیریتی سازمان را به مرور افزایش می‌دهد .

گزینه‌های پیش روی سازمان‌ها
ارتقا به Windows 11
توصیه اصلی مایکروسافت، ارتقاء تدریجی سیستم‌ها به Windows 11 است. پیش از ارتقاء، باید سازگاری سخت‌افزاری TPM 2.0، Secure Boot و CPU بررسی شود.
دریافت Extended Security Updates (ESU)
برای سازمان‌هایی که به‌طور موقت نمی‌توانند به Windows 11 ارتقا یابند، مایکروسافت برنامه ESU را ارائه داده است. این طرح به‌صورت اشتراک سالانه، بروزرسانی‌های امنیتی حیاتی را تا سه سال پس از پایان پشتیبانی ارائه می دهد.
پیشنهادات عملی برای تیم‌های IT
• تهیه لیست کامل دارایی‌ها (Asset Inventory) از تمامی سیستم‌های مبتنی بر Windows 10
• بررسی سازگاری سخت‌افزاری و نرم‌افزاری جهت مهاجرت به Windows 11.
• برنامه‌ریزی آزمایشی و مرحله‌ای (Phased Roll-out) برای مهاجرت کاربران
• در صورت نیاز، برآورد بودجه و زمان‌بندی برای دریافت مجوزESU
• تقویت سیاست‌های امنیتی برای سیستم‌هایی که تا زمان ارتقا همچنان از Windows 10 استفاده می‌کنند مانند فایروال، EDR و محدودیت دسترسی به اینترنت.
جمع‌بندی
پایان پشتیبانی Windows 10 یک هشدار جدی برای تمام سازمان‌هاست تا برنامه ارتقا خود را در نیمه دوم سال ۲۰۲۵ تکمیل کنند. برنامه‌ریزی پیش‌دستانه، آزمایش نسخه‌های جدید و مدیریت مرحله‌ای ارتقا، کلید حفظ امنیت و پایداری در زیرساخت‌های IT خواهد بود.

کارشناسان Fortinet حملات فیشینگ جدیدی را شناسایی کرده‌اند که با جعل هویت نهادهای دولتی اوکراین، بدافزار Count Loader را توزیع می‌کند. این حملات از فایل‌های SVG مخرب استفاده می‌کنند که با باز شدن، یک فایل ZIP رمزدار حاوی CHM را دانلود می‌کنند. اجرای CHM زنجیره‌ای از اقدامات را فعال می‌کند که به نصب CountLoader منجر می شود.

در این سناریو، CountLoader به عنوان واسطه انتشار Amatera Stealer (نسخه‌ای از ACRStealer برای سرقت اطلاعات) و PureMiner (.NET کریپتوماینر مخفی) عمل می‌کند. این ابزارها بخشی از مجموعه بدافزارهای توسعه‌یافته توسط گروه PureCoder هستند که شامل PureHVNC RAT، PureRAT (Re-solverRAT)، PureLogs، BlueLoader و PureClipper نیز می‌شود. ترکیب این ابزارها مهاجمان را قادر می سازد تا سیستم‌های قربانی را کنترل، داده‌ها را استخراج، و منابع پردازشی را برای استخراج ارز دیجیتال سوءاستفاده کنند.

کارزار تازه COLDRIVER با بدافزارهای جدید BAITSWITCH و SIMPLEFIX

گروه APT روسی COLDRIVER (با نام‌های دیگر Cal-listo، Star Blizzard، UNC4057) کارزار پیشرفته‌ای را آغاز کرده که از تاکتیک ClickFix در چند مرحله استفاده می‌کند. این گروه که از سال ۲۰۱۹ فعال است، به فریب قربانیان در بخش‌های دولتی، تحقیقاتی و زیرساختی شهرت دارد.

روش حمله

فیشینگ و وب‌سایت جعلی: قربانی از طریق لینک های فیشینگ وارد صفحات نامعتبر می‌شود که ظاهر آنها مشابه صفحات رسمی یا CAPTCHA واقعی طراحی شده‌است.

اجرا کردن دستی کد مخرب: کاربر با فریب، دستور اجرای DLL یا فرمان PowerShell را خود در Windows Run یا ترمینال وارد می‌کند.

BAITSWITCH Downloader: این ماژول کوچک پس از اجرا، payload اصلی یعنی SIMPLEFIX را بارگذاری می‌کند.

SIMPLEFIX PowerShell Backdoor: نفوذگران با این backdoor امکان اجرای دستورات، دانلود ابزار اضافی، و جمع‌آوری داده‌ها از سیستم آلوده را پیدا می‌کنند.

ابزارهای پیشین و تکامل زرادخانه

COLDRIVER پیش‌تر در کارزارهای مختلف از ابزارهای اختصاصی نظیر:

SPICA: ابزار جاسوسی پیشرفته.

LOSTKEYS: اسکریپت Visual Basic تخصیص یافته برای نفوذ از طریق ClickFix.

نقاط قوت تاکتیک ClickFix

هرچند از نظر فنی پیچیده نیست، اما:

تکیه بر تعامل قربانی باعث می‌شود بسیاری از سامانه‌های امنیتی که به شناسایی خودکار متکی هستند، آن را نادیده بگیرند.

قابلیت تطبیق با محیط‌های مختلف Windows و ترکیب آسان با ابزارهای جدید.

امکان اجرای مستقیم کد بدون نیاز به اکسپلویت کلاسیک.

این تکامل زرادخانه نشان‌دهنده تمرکز COLDRIVER بر بهره‌برداری از خطای انسانی و استفاده از بدافزارهای سبک‌وزن برای عبور از خطوط دفاعی است.

حمله Battering RAM که توسط محققان KU Leuven و University of Birmingham معرفی شده، یک حمله فیزیکی سطح سخت‌افزار علیه مکانیزم‌های محرمانگی داده در پردازنده‌های ابری Intel SGX و AMD SEV-SNP است. این حمله با استفاده از یک DDR4 interposer (مدار واسط حافظه) با هزینه کمتر از ۵۰ دلار، سیگنال‌های باس بین CPU و DRAM را در سطح آنالوگ دستکاری می‌کند.

مهاجم با فعال‌سازی سوئیچ‌های آنالوگ، آدرس‌های فیزیکی محافظت‌شده را به نواحی حافظه تحت کنترل خود alias کرده و از این طریق:

بر روی پلتفرم‌های Intel، امکان دسترسی خواندن آزاد به plaintext یا نوشتن مستقیم در داخل enclave را پیدا می‌کند.

بر روی پلتفرم‌های AMD، دور زدن محافظت‌های firm-ware جدید علیه BadRAM و تزریق backdoor به VM ممکن می‌شود.

دلیل اصلی موفقیت این حمله حذف freshness check از طرح‌های رمزگذاری حافظه در راستای افزایش ظرفیت رمزگذاری‌شده است؛ در نتیجه aliasهای حافظه می‌توانند در زمان اجرا ایجاد شوند و حتی مکانیزم‌های attestation در بوت را بی‌اثر سازند.

برای مقابله، لازم است طراحی رمزگذاری حافظه با بررسی و تأیید یکپارچگی زمان‌اجرا (runtime freshness validation) بازطراحی شود، که در حال حاضر خارج از محدوده امنیتی تعریف‌شده توسط Intel و AMD محسوب می‌شود.

https://thehackernews.com/2025/10/50-battering-ram-attack-breaks-intel.html

گروه APT تازه‌نامگذاری‌شده Phantom Taurus که بر اساس شواهد به دولت چین وابسته است، از اواخر ۲۰۲۲ تا کنون علیه وزارت‌خانه‌های امور خارجه، سفارت‌ها، زیرساخت‌های مخابراتی و نهادهای نظامی در آفریقا، خاورمیانه و آسیا عملیات جاسوسی سایبری انجام داده است. این گروه پیش‌تر تحت شناسه‌های CL-STA-0043 و TGR-STA-0043 توسط واحد Unit 42 شرکت Palo Alto Networks ردیابی می شد و فعالیت‌های آن بخشی از کارزار Operation Diplomatic Specter بوده است.

رویکرد این تهدید پیشرفته (APT) بر دستیابی پایدار (Persistence)، عملیات مخفیانه (Stealth) و تطبیق سریع تاکتیک‌ها و تکنیک‌ها (TTPs) متمرکز است. تاکتیک‌ها شامل:

اهداف دیپلماتیک و ارتباطات محرمانه برای جمع آوری اطلاعات حساس مرتبط با سیاست خارجی.

استفاده از بدافزارهای پنهان‌کار (Stealth Malware) با قابلیت تغییر مسیر داده‌ها، رمزگذاری ارتباطات C2، و دور زدن آنتی‌ویروس/EDR.

تثبیت حضور بلندمدت در شبکه قربانی از طریق بهره‌گیری از ضعف‌های پیکربندی و زنجیره تأمین نرم‌افزار.

بهره‌برداری از زیرساخت‌های مخابراتی و سرویس دهنده‌های اینترنت محلی برای پوشش هویت و مسیر حمله.

هدف نهایی: جمع‌آوری مداوم اطلاعات محرمانه برای استفاده در تصمیم‌گیری‌های ژئوپولیتیک و اقتصادی دولت چین.

برای مقابله، نیاز به مانیتورینگ رفتار شبکه (Network Behavior Analysis)، تحلیل مداوم ترافیک رمزگذاری‌شده، و به‌روزرسانی‌های مستمر سامانه های تشخیص پیشرفته وجود دارد؛ چرا که این گروه از Low-and-Slow Attacks استفاده می‌کند که شناسایی آنها توسط ابزارهای سنتی دشوار است.

https://thehackernews.com/2025/09/phantom-taurus-new-china-linked-hacker.html

Range یک محیط آزمایشی امنیتی شبیه‌سازی‌شده است که به تیم‌های SOC، Blue Team و Red Team اجازه می‌دهد حملات سایبری را با استفاده از زیرساخت‌ها و داده‌های واقعی اما در شرایط ایزوله، بازسازی کنند. هدف، ارزیابی کارایی ابزارهای دفاعی، توسعه واکنش‌های Incident Response و تست سناریوهای پیشرفته تهدید است.

در این محیط، با استفاده از ترکیبی از فناوری‌ها و پیکربندی‌های نزدیک به Production، کاملاً چرخه چک‌لیست MITRE ATT&CK شبیه‌سازی می‌شود:

اجرای TTPهای واقعی مهاجمان (مانند Lateral Movement، Privilege Escalation، و Data Exfiltration)

تست کارکرد IDS/IPS، SIEM، EDR و هماهنگی آن‌ها تحت شرایط حمله

تولید لاگ‌های معتبر برای تحلیل رفتار و بهینه‌سازی Detection Rules

بررسی نقاط ضعف در Incident Handling Playbooks و ارتقای آن‌ها

استفاده از Threat Range باعث می‌شود تیم‌ها قبل

- رخداد واقعی، عملکرد خود را در برابر حملات
- ته ارزیابی کنند و شکاف‌های امنیتی را با
- طرف کنند. این رویکرد در چارچوب Se-
- Purple Teaming اهمیت ویژه‌ای

یک آسیب‌پذیری بحرانی با امتیاز CVSS 10.0 در ماژول License Servlet نرم‌افزار Fortra GoAny-where MFT شناسایی و از ۱۱ سپتامبر ۲۰۲۵ توسط گروه باج‌افزار Medusa به‌طور فعال بهره‌برداری شده است.

این نقص از نوع Deserialization بوده و امکان Remote Code Execution بدون نیاز به احراز هویت را فراهم می‌کند، به مهاجم اجازه می دهد با جعل امضای پاسخ لایسنس، کنترل کامل سیستم را به دست گیرد.

تحقیقات watchTowr Labs نشان می‌دهد مهاجمان پس از نفوذ، حساب مدیریتی مخفی ایجاد کرده، با استفاده از ابزارهای RMM مانند SimpleHelp و MeshAgent پایداری ایجاد کرده، حرکت جانبی انجام داده و نهایتاً با بهره‌گیری از ابزارهایی نظیر Rclone و تونل‌های Cloudflare داده‌ها را استخراج و Medusa را اجرا کرده‌اند.

با توجه به تأیید بهره‌برداری فعال توسط تیم امنیتی مایکروسافت و افزوده شدن این نقص به فهرست KEV سازمان CISA، تمامی سازمان‌ها باید فوراً به نسخه‌های 7.8.4 یا SR 7.6.3 به روزرسانی کرده و بررسی کامل رخداد امنیتی انجام دهند.

مدل جدید Gemini 2.5 Computer Use از Google DeepMind به‌صورت پیش‌نمایش از طریق Gemini API عرضه شده و برای ساخت عامل‌های هوش مصنوعی طراحی شده که می‌توانند با رابط‌های کاربری وب و موبایل تعامل مستقیم داشته باشند. این مدل بر پایه توانایی‌های Visual Understanding و Reasoning نسخه Pro توسعه یافته و در بنچمارک های کنترل رابط کاربری از رقبا عملکرد دقیق‌تر و با تأخیر کمتر ارائه می‌دهد.

قابلیت‌های کلیدی شامل:

- اجرای وظایفی مانند پر کردن فرم‌ها، انتخاب گزینه‌ها، مدیریت عناصر تعاملی و ورود به سامانه ها.
- استفاده از ورودی‌های شامل اسکرین‌شات محیط، تاریخچه اقدامات و درخواست کاربر برای تولید اقدامات مانند کلیک یا تایپ.
- فرآیند حلقه‌ای برای تحلیل وضعیت بعد از هر اقدام تا انجام کامل وظیفه.
-

بهینه‌سازی برای مرورگر وب و پشتیبانی نویدبخش از کنترل رابط کاربری موبایل (هنوز بهینه‌سازی کامل برای کنترل سیستم‌عامل دسکتاپ انجام نشده).

همچنین مکانیزم‌های ایمنی در مدل تعبیه شده تا ریسک‌هایی مانند سوءاستفاده عمدی، رفتار غیرمنتظره مدل و حملات Prompt Injection به حداقل برسد.

این مدل اکنون در Google AI Studio و Vertex AI در دسترس توسعه‌دهندگان قرار دارد.