خبرنامه برنا

Borna Network Managers
مدیران شبکه برنا

اخبار حوزه امنیت و شبکه (شهریور ۱۴۰۴)

خبرنامه تخصصی «مدیران شبکه برنا»؛ نگاهی حرفه‌ای به دنیای امنیت شبکه هر ماه با ما همراه باشید تا در جریان جدیدترین تهدیدات سایبری، تحلیل رویدادها، به‌روزرسانی محصولات و راهکارهای نوین امنیت اطلاعات قرار بگیرید.

ویژه مدیران و کارشناسان شبکه و امنیت
(رایگان، تخصصی، به‌روز)

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

۱. آسیب‌پذیری بحرانی در Docker Desktop (CVE-2025-9074)

یک آسیب‌پذیری با شدت بحرانی (CVSS 9.3) در Docker Desktop برای ویندوز و macOS کشف و رفع شده است. این ضعف امکان فرار از کانتینر (Container Escape) را می‌دهد؛ مهاجم بدون احراز هویت می‌تواند از طریق API داخلی Docker به Docker Engine متصل شود، فایل‌سیستم میزبان را مونت کند، داده‌های حساس را بخواند یا بنویسد و در ویندوز حتی DLLهای سیستمی را جایگزین کند.

🔒 **اقدامات ضروری:**

- ارتقا به نسخه‌ی ۴/۴۴/۳ یا بالاتر؛
- محدود کردن دسترسی به API داخلی Docker؛
- اعمال سیاست‌های least privilege برای کانتینرها و میزبان.

۲. بزرگ‌ترین حمله تاریخ به اکوسیستم NPM

حمله‌ای فیشینگ منجر به تزریق کد مخرب در بسته‌های محبوب NPM شده است؛ بسته‌هایی که مجموع دانلود هفتگی‌شان بیش از دو میلیارد بار است. کتابخانه‌هایی مثل chalk, debug, sup-ports-color, ansi-regex و غیره تحت تأثیر قرار گرفته‌اند.

🔒 **اقدام فوری:**

- بررسی کامل وابستگی‌ها و به‌روزرسانی به نسخه‌های امن؛
- استفاده از lock file‌ها (مثلاً package-lock.json)؛
- انجام ممیزی امنیتی برای زنجیره بسته‌ها.

۳. ظهور بدافزار مبتنی بر هوش مصنوعی: PromptLock

ESET بدافزاری به نام PromptLock را شناسایی کرده است که نمونه تحقیقاتی آن با استفاده از هوش مصنوعی (مدل gpt-oss:20b همراه رابط Ollama) ساخته شده است. بدافزار اسکریپت Lua تولید می کند، فایل‌های محلی را کاوش می‌کند، داده‌ها را استخراج کرده و در نهایت آن‌ها را رمزگذاری می نماید. قابلیت تغییر در هر اجرا دارد تا تشخیص آن دشوار شود.

🔒 **اقدام پیشنهادی:**

- تقویت شناسایی رفتاری (behavioral detection)؛
- استفاده از تحلیل استاتیک و دینامیک با محیط کنترل شده؛
- رصد شاخص‌های IoC منتشر شده؛

۴. افشای عظیم داده‌ها مرتبط با «دیوار آتش بزرگ چین» (Great Firewall)

نشت داده‌ای تقریباً ۶۰۰ گیگابایتی که به پروژه های مرتبط با دیوار آتش بزرگ چین (GFW) مربوط است توسط گروه هکتیویست منتشر شده است. محتوای نشت شامل کد منبع، اسناد فنی، گزارش‌های داخلی، لاگ‌ها، ارتباطات کارکنان، نرم افزارهای مورد استفاده برای پایش و سانسور ترافیک است. برخی سرویس‌ها و شرکت‌های تحقیقاتی مرتبط در این پروژه شناسایی شده‌اند.

🔒 **اقدامات پیشنهادی:**

- تحلیل داده‌ها در محیط ایزوله (VM یا air-gapped)؛
- احتیاط در مواجهه با فایل‌های ممکن است مخرب؛
- مستندسازی دقیق قطعات نشت‌شده برای درک کامل ساختار.

۵. ابزار AI-Powered جدید "Villager" برای Pen-Testing و نگرانی از سوءاستفاده

ابزار جدیدی به نام Villager که توسط کمپانی مطرح Cyberspike در چین ساخته شده است، با کمک هوش مصنوعی و ادغام ابزارهای Kali Linux و مدل‌های DeepSeek، برای خودکارسازی عملیات Pen-Testing عرضه شده است. این ابزار از PyPI قابل دریافت است و از زمان انتشار در جولای ۲۰۲۵ تا کنون بیش از ۱۱,۰۰۰ بار دانلود شده است.

ویژگی‌های قابل توجه شامل تولید دستورات بر پایه ی دستورات زبان طبیعی (natural language)، استفاده از promptهای از پیش تعریف شده (بیش از ۴,۲۰۰ prompt)، راه‌اندازی کانتینرهای Kali Linux جداگانه برای اسکن و تست نفوذ که پس از مدت کوتاهی تخریب می‌شوند، و همچنین کنترل و فرمان‌دهی (C2) از طریق FastAPI است.

🔒 ریسک‌ها و اقدام پیشنهادی:

• این نوع ابزارها مرز بین استفاده قانونی و سوءاستفاده را کمرنگ می‌کنند؛ امکان استفاده توسط بازیگران مخرب وجود دارد.

• لازم است سازمان‌ها مراقب بسته‌های نرم افزاری از منابع عمومی مثل PyPI باشند؛ کنترل منشأ بسته (package provenance)، اعمال سیاست allow-list در نصب بسته‌ها، و پایش رفتار نصب و عملکرد ابزارها الزامی است.

• تیم‌های امنیتی داخلی باید تست‌های نفوذ و red-team exercises را با سناریوهایی که شامل ابزارهای AI-محور باشند انجام دهند تا آماده باشند پاسخ به تهدیدات سریع و خودکار باشند.