حملة بمساعدة الذكاء الاصطناعي تخترق خوادم Check Point Security Management بحسب GreyNoise



تفيد GreyNoise بأن الجهة GT13 استخدمت أدوات هجومية مدعومة بالذكاء الاصطناعي ضد خوادم Check Point Security Management، وطال الأمر 22 جهة على الأقل. وترجّح أن الحملة مستمرة لاحتفاظ المهاجم بوصول دائم.

- تتتبع GreyNoise الجهة GT13 منذ أوائل أكتوبر، وقد استخدمت 99 عنوان IP مرتبطة بخروج عبر ExpressVPN أو بأجهزة Check Point مخترقة.
- استُهدفت 22 جهة على الأقل في قطاعات منها الطاقة والخدمات المالية والحكومة والتصنيع والتعدين والنقل، في دول عدة.
- ترى GreyNoise أن أنظمة وكيلة (agentic) أتمتت تحويل الثغرات إلى أدوات هجوم والمسح والاستغلال، مع تدخل يدوي مكمّل.
- كان للمهاجم وصول إلى خوادم Check Point قبل اختراق خادم HFS منفصل، ولم يُعرف كيف

حصل على الوصول الأول.

- رُصد النشاط بين 17 أكتوبر و2 نوفمبر، لكن الوصول الدائم يشير إلى احتمال استمرار الحملة.

وصفت شركة استخبارات التهديدات GreyNoise حملة تستهدف خوادم Check Point Security Management ينفذها فاعل تسميه GreyNoise Threat 13 (GT13). بدأت الشركة تتبعها في أوائل أكتوبر، وترجّح أنها لا تزال مستمرة.

ما الذي رُصد

نفّذ GT13 أنشطة مسح واستغلال وتحكم من 99 عنوان IP، جميعها إما نقاط خروج عبر ExpressVPN أو أجهزة Check Point مخترقة. وأحصت GreyNoise أكثر من 1,400 جلسة شبكية وأكثر من 800 أثر لأوامر سطر الأوامر وأكثر من 1,200 ملف جرى تنزيله أو رفعه أو إنشاؤه. واستُهدفت 22 جهة على الأقل.

في إحدى الحالات زوّر المهاجم ملف تعريف ارتباط (cookie) موقّعًا لجلسة مسؤول للحصول على صلاحيات إدارية على خادم HFS، ثم نال وصول SSH وفحص البيئة وسرّب بيانات. شملت الأدوات Nmap وChisel وImpacket وParamiko، واستُخدمت في الاستطلاع والحركة الجانبية ورفع الصلاحيات. واستُخدم خادم أحد الضحايا كنقطة وسيطة تحفظ بيانات مأخوذة من 24 خادم Check Point Security Management مخترقًا.

لماذا يهم ذلك

ترى GreyNoise أن أنظمة وكيلة (agentic) منفصلة تحوّل الثغرات إلى أدوات هجوم وتبحث عن الأصول المكشوفة وتستغلها آليًا، بينما يعمل المشغلون يدويًا بالتوازي. وكان للمهاجم وصول إلى خوادم Check Point قبل اختراق HFS، ولم تتمكن الشركة من تحديد وقته أو كيفيته. ولأن GT13 احتفظ بوصول دائم، فقد تستمر الحملة رغم توقف الرصد في 2 نوفمبر.

ويورد المصدر ثغرات عدة استُخدمت أو جرت محاولة استغلالها في بيئة أحد الضحايا، تشمل HFS Rejetto وCitrix NetScaler وIvanti Connect Secure وLinux وCheck Point SmartConsole وWindows NetLogon وMicrosoft Exchange وVMware vCenter. وبما أن خوادم الإدارة الأمنية تمنح تحكمًا إداريًا عالي القيمة، فعلى المؤسسات التي تشغّلها مراجعة تعرضها بهدوء ومنهجية.

ما يجب فعله الآن

1. تحقق من إمكانية الوصول إلى خوادم Check Point Security Management من الإنترنت، وقيّد الوصول الإداري بشبكات موثوقة.
2. راجع سجلات هذه الخوادم بحثًا عن مفاتيح SSH غير متوقعة ومهام إدارة شهادات جماعية ونقل ملفات صادر عبر scp.
3. ابحث عن الأدوات التي ذكرتها GreyNoise (Nmap وChisel وImpacket وParamiko) وعن سكربتات Python غير المتوقعة على خوادم الإدارة والخوادم المجاورة.
4. تأكد من تطبيق التحديثات الخاصة بالثغرات المذكورة في المصدر على HFS وCitrix وIvanti Connect Secure وCheck Point SmartConsole وWindows Exchange وvCenter.

5. عند وجود أي مؤشر اختراق، بدّل بيانات الاعتماد الإدارية وأسرار الجلسات ومفاتيح SSH، واتبع إجراءات الاستجابة للحوادث ومتطلبات الإبلاغ للهيئة الوطنية للأمن السيبراني.