حملة منسوبة إلى APT29 تستغل سكربت تحليلات ويب لاستهداف مستخدمي iOS وAndroid



تفيد التقارير بأن حملة «ووترينغ هول» منسوبة إلى APT29 تستهدف مستخدمي iOS وAndroid عبر مواقع مخترقة ونطاقات مزيفة وهجوم على سلسلة التوريد في خدمة Plerdy SEO Tracker.

- تُنسب الحملة إلى APT29، وهي جهة تهديد مرتبطة بروسيا.
- تجمع الحملة بين مواقع مخترقة ونطاقات مزيفة وهجوم على سلسلة التوريد.
- يتعلق جانب سلسلة التوريد بخدمة Plerdy SEO Tracker، وهي خدمة تحليلات ويب أوكرانية.
- يذكر باحثو Sekoia أن كود JavaScript المحقون يجمع خصائص المتصفح والجهاز.
- تستهدف الحملة مستخدمي iOS وAndroid على حد سواء.

ما الذي ورد في التقرير

تفيد التقارير بأن جهة التهديد المرتبطة بروسيا والمعروفة باسم APT29 تقف وراء حملة واسعة من نوع «ووترينغ هول» تستهدف مستخدمي iOS وAndroid. ووفق المصدر، تعتمد العملية على مواقع مخترقة ونطاقات مزيفة وهجوم على سلسلة التوريد يخص خدمة تحليلات الويب الأوكرانية Plerdy SEO Tracker.

ويذكر باحثو Sekoia أن كود JavaScript المحقون يجمع خصائص المتصفح والجهاز. ويشير عنوان المصدر إلى أن الهدف النهائي هو إيصال ثغرات استغلال لنظامي iOS وAndroid إلى الزوار.

أهمية الموضوع

تعمل السكربتات الخارجية، مثل أكواد التحليلات، بثقة الموقع الذي يحمّلها. وعند العبث بأحدها، قد يتحول كل موقع يضمّنه إلى نقطة توصيل، حتى المواقع التي تعدّها المؤسسة محكمة الضبط. ويقع الموظفون الذين يتصفحون عبر الأجهزة المحمولة ضمن نطاق هذه الحملة.

ولا يقدّم مقتطف المصدر مؤشرات فنية ولا تفاصيل عن الثغرات المستغلة أو الضحايا، لذا ينبغي عدم افتراض التعرض أو السلامة قبل مراجعة المؤسسة لاستخدامها لهذه الخدمة.

الخطوات العملية

تتمثل الاستجابة في معرفة أماكن تحميل السكربتات الخارجية، والتحقق من استخدام الخدمة المذكورة، والتأكد من تحديث الأجهزة المحمولة ومراقبتها، ومتابعة أبحاث Sekoia للحصول على مؤشرات الاختراق عند نشرها.

ما يجب فعله الآن

1. حصر السكربتات الخارجية، ومنها أكواد التحليلات، المحمّلة في مواقعكم العامة وتطبيقات الويب الداخلية.
2. التحقق من استخدام Plerdy SEO Tracker في أي من أصولكم الرقمية ومراجعته في ضوء نتائج Sekoia.
3. تطبيق أحدث تحديثات iOS وAndroid على الأجهزة المؤسسية والشخصية المستخدمة في العمل عبر إدارة الأجهزة المحمولة.
4. مراجعة سجلات الوكيل وDNS بحثاً عن اتصالات بنطاقات مشبوهة أو منتحلة فور نشر المؤشرات.
5. النظر في تطبيق سياسة أمان المحتوى (CSP) وسلامة الموارد الفرعية (SRI) للحد من أثر السكربتات الخارجية المعبث بها.
6. إدراج اختراق السكربتات الخارجية ضمن مراجعات مخاطر الأطراف الثالثة وخطط الاستجابة للحوادث.