APT29-linked campaign abuses a web analytics script to target iOS and Android users



A watering hole campaign linked to Russia-associated APT29 reportedly targets iOS and Android users through compromised sites, fake domains and a supply chain compromise of the Plerdy SEO Tracker analytics service.

- The campaign is attributed to APT29, a Russia-linked threat actor.
- It combines compromised websites, fake domains and a supply chain attack.
- The supply chain element involves Plerdy SEO Tracker, a Ukrainian web analytics service.
- Researchers at Sekoia report that the injected JavaScript collects browser and device attributes.
- Both iOS and Android users are targeted.

What was reported

The Russia-linked threat actor known as APT29 is said to be running a large-scale watering hole campaign aimed at iOS and Android users. According to the source, the operation relies on compromised websites, fake domains and a supply chain attack involving a Ukrainian web analytics service, Plerdy SEO Tracker.

Researchers at Sekoia report that the injected JavaScript code gathers browser and device attributes. The source headline indicates the end goal is delivery of iOS and Android exploits to visitors.

Why it matters

Third-party scripts such as analytics tags run with the trust of the site that loads them. When such a script is tampered with, every site embedding it can become a delivery point, including sites the organisation considers well controlled. Staff browsing on mobile devices are within the scope of this campaign.

The source excerpt does not provide technical indicators, affected vulnerabilities or details of victims, so organisations should avoid assuming exposure or safety until they review their own use of the service.

What to do next

The practical response is to understand where third-party scripts are loaded, check whether the named service is in use, and make sure mobile devices are patched and monitored. Follow Sekoia's published research for indicators as they become available.

What to do now

1. Inventory third-party scripts, including analytics tags, loaded on your public websites and internal web applications.
2. Check whether Plerdy SEO Tracker is used in any of your web properties and review it against Sekoia's findings.
3. Apply the latest iOS and Android updates to corporate and BYOD devices through mobile device management.
4. Review proxy and DNS logs for connections to suspicious or look-alike domains once indicators are published.
5. Consider content security policy and subresource integrity controls to limit the impact of tampered third-party scripts.
6. Include third-party script compromise in third-party risk reviews and incident playbooks.