

Forum:[Hack Forums](#)

Thread: [Amazon Disrupts APT29 Watering Hole Campaign Abusing Microsoft Device Code Authentic](#)

Stanley - September 9, 2025, 11:35 am

Amazon Disrupts APT29 Watering Hole Campaign Abusing Microsoft Device Code Authentic

Amazon on Friday said it flagged and disrupted what it described as an opportunistic watering hole campaign orchestrated by the Russia-linked APT29 actors as part of their intelligence gathering efforts.

The campaign used "compromised websites to redirect visitors to malicious infrastructure designed to trick users into authorizing attacker-controlled devices through Microsoft's device code

<https://thehackernews.com/2025/08/amazon-disrupts-apt29-watering-hole.html>

Rsynced - September 9, 2025, 12:35 pm

Sounds like fun! ??

W1NK1LL3RX - September 9, 2025, 3:41 pm

APT29 never quits, now they're abusing Microsoft's device code auth. Good catch by Amazon shutting that down before it spread further.

plops - September 9, 2025, 6:39 pm

Good ol russia. Amazon gives ope sometimes.

sharn - September 14, 2025, 8:20 am

Fake Cloudflare verification is sneaky.

Users click because it feels routine.

The Pact - September 28, 2025, 5:01 am

Just like predators in the wild wait near watering holes to ambush prey, attackers lie in wait on trusted websites, hoping their targets will come to them.

Attackers identify websites popular with their intended victims like they might target government workers or journalists or even diplomats! Their goal might be to steal login credentials, install spyware, or gain access to systems.

Victims often trust the compromised site. That's what we all have to watch out for. :-(