Amazon blocks APT29 campaign targeting Microsoft device code authenti

Data: 2025-08-31 11:44:37

Autor: Inteligência Against Invaders

Amazon blocks APT29 campaign targeting Microsoft device code authentication

Amazon stopped a Russia-linked APT29 watering hole attack that hijacked Microsoft device code authentication via compromised sites.

Amazon announced that it had disrupted an opportunistic watering hole campaign orchestrated by the Russia-linked cyber espionage group APT29 (akaSVR group,Cozy Bear,Nobelium,BlueBravo, Midnight Blizzard, andThe Dukes).

Amazon experts labeled the attacks as an opportunistic watering hole campaign using compromised websites to redirect visitors to malicious infrastructure. The bogus websites that are employed in the attack are designed to trick visitors into authorizing attacker-controlled devices through Microsoft's device code authentication flow.

"Amazon's threat intelligence team has identified and disrupted a watering hole campaign conducted by APT29" reads the report published by Amazon. £This opportunistic approach illustrates APT29's continued evolution in scaling their operations to cast a wider net in their intelligence collection efforts."

APT29 continues evolving its credential-harvesting tactics. After past AWS and Google disruptions, its latest watering hole campaign shows refined tradecraft: injecting obfuscated JavaScript, shifting to server-side redirects, and quickly adapting infrastructure. The campaign targeted academics and Russia critics to gather intelligence.

Amazon uncovered the watering hole campaign via custom analytics, finding actor domains like findcloudflare[.]com mimicking Cloudflare pages. Threat actors injected a malicious JavaScript into legitimate sites, redirecting ~10% of visitors to capture Microsoft device code authentication.

Tactics included randomization, base64 encoding, cookies, and rapid infrastructure pivots. Amazon, working with Cloudflare and Microsoft, disrupted operations, isolated the affectedEC2 instances, and blocked malicious domains.

"Despite the actor's attempts to migrate to new infrastructure, including a move off AWS to another cloud provider, our team continued tracking and disrupting their operations." concludes the report that includes recommendations for users and administrators. "After our intervention, we observed the actor register additional domains such as cloudflare[.]redirectpartners[.]com, which again attempted to lure victims into Microsoft device code authentication workflows."

Follow me on Twitter:@securityaffairsandFacebookandMastodon

PierluigiPaganini

(SecurityAffairs–hacking,Russia)