

BGP hijack infecting networks caused by a comedy of errors that's not funny at all

Hackers carried out a supply chain attack that installed malware on networks using an unusual technique: hijacking a chunk of Internet space where cloud management software used by hosting providers, data centers, and other large infrastructure companies is updated.

In a well-coordinated operation, the unknown attackers exploited weaknesses in the routing security setup of hosting provider Hetzner Online and the process for attaining valid TLS certificates. The lapses allowed the attackers to successfully perform a BGP (Border Gateway Protocol) hijacking to obtain control over IP addresses assigned to Softaculous. The company, based in the United Arab Emirates, is the maker of a platform for installing and managing Web software and is the developer of Virtualizor, a management platform for virtualized environments.

Softaculous used the IPs to issue updates and host a client and billing site. With control over the hijacked space, the attacker was now using the addresses to push malware masquerading as updates to unsuspecting users.

[Read full article](#)

Comments

<https://arstechnica.com/security/2026/09/well-executed-bgp-attack-uses-hijacked-ips-to-infect-real-networks/>