Compromise Infrastructure: Domains, Sub-technique T1584.001 - Enterprise

Archived: 2026-04-05 14:02:43 UTC

Adversaries may hijack domains and/or subdomains that can be used during targeting. Domain registration hijacking is the act of changing the registration of a domain name without the permission of the original registrant.[1] Adversaries may gain access to an email account for the person listed as the owner of the domain. The adversary can then claim that they forgot their password in order to make changes to the domain registration. Other possibilities include social engineering a domain registration help desk to gain access to an account, taking advantage of renewal process gaps, or compromising a cloud service that enables managing domains (e.g., AWS Route53).[2]

Subdomain hijacking can occur when organizations have DNS entries that point to non-existent or deprovisioned resources. In such cases, an adversary may take control of a subdomain to conduct operations with the benefit of the trust associated with that domain.[3]

Adversaries who compromise a domain may also engage in domain shadowing by creating malicious subdomains under their control while keeping any existing DNS records. As service will not be disrupted, the malicious subdomains may go unnoticed for long periods of time.[4]

Source: https://attack.mitre.org/techniques/T1584/001