Hide Infrastructure, Technique T1665 - Enterprise

Archived: 2026-04-05 17:19:27 UTC

Adversaries may manipulate network traffic in order to hide and evade detection of their C2 infrastructure. This can be accomplished by identifying and filtering traffic from defensive tools,[1] masking malicious domains to obfuscate the true destination from both automated scanning tools and security researchers,[2][3][4] and otherwise hiding malicious artifacts to delay discovery and prolong the effectiveness of adversary infrastructure that could otherwise be identified, blocked, or taken down entirely.

C2 networks may include the use of Proxy or VPNs to disguise IP addresses, which can allow adversaries to blend in with normal network traffic and bypass conditional access policies or anti-abuse protections. For example, an adversary may use a virtual private cloud to spoof their IP address to closer align with a victim's IP address ranges. This may also bypass security measures relying on geolocation of the source IP address.[5][6]

Adversaries may also attempt to filter network traffic in order to evade defensive tools in numerous ways, including blocking/redirecting common incident responder or security appliance user agents.[7][8] Filtering traffic based on IP and geo-fencing may also avoid automated sandboxing or researcher activity (i.e., Virtualization/Sandbox Evasion).[1][7]

Hiding C2 infrastructure may also be supported by Resource Development activities such as Acquire Infrastructure and Compromise Infrastructure. For example, using widely trusted hosting services or domains such as prominent URL shortening providers or marketing services for C2 networks may enable adversaries to present benign content that later redirects victims to malicious web pages or infrastructure once specific conditions are met.[9][10]

Source: https://attack.mitre.org/techniques/T1665