Stage Capabilities: Link Target, Sub-technique T1608.005 - Enterprise

Archived: 2026-04-05 17:31:46 UTC

Adversaries may put in place resources that are referenced by a link that can be used during targeting. An adversary may rely upon a user clicking a malicious link in order to divulge information (including credentials) or to gain execution, as in Malicious Link. Links can be used for spearphishing, such as sending an email accompanied by social engineering text to coax the user to actively click or copy and paste a URL into a browser. Prior to a phish for information (as in Spearphishing Link) or a phish to gain initial access to a system (as in Spearphishing Link), an adversary must set up the resources for a link target for the spearphishing link.

Typically, the resources for a link target will be an HTML page that may include some client-side script such as JavaScript to decide what content to serve to the user. Adversaries may clone legitimate sites to serve as the link target, this can include cloning of login pages of legitimate web services or organization login pages in an effort to harvest credentials during Spearphishing Link.[1][2] Adversaries may also Upload Malware and have the link target point to malware for download/execution by the user.

Adversaries may purchase domains similar to legitimate domains (ex: homoglyphs, typosquatting, different top-level domain, etc.) during acquisition of infrastructure (Domains) to help facilitate Malicious Link.

Links can be written by adversaries to mask the true destination in order to deceive victims by abusing the URL schema and increasing the effectiveness of phishing.[3][4]

Adversaries may also use free or paid accounts on link shortening services and Platform-as-a-Service providers to host link targets while taking advantage of the widely trusted domains of those providers to avoid being blocked while redirecting victims to malicious pages.[5][6][7][8] In addition, adversaries may serve a variety of malicious links through uniquely generated URIs/URLs (including one-time, single use links).[9][10][11][12] Finally, adversaries may take advantage of the decentralized nature of the InterPlanetary File System (IPFS) to host link targets that are difficult to remove.[13]

Source: https://attack.mitre.org/techniques/T1608/005