# TTP Detail – T1583.001

## TTP Information

Name: Domains

Description: Adversaries may acquire domains that can be used during targeting. Domain names are the human readable names used to represent one or more IP addresses. They can be purchased or, in some cases, acquired for free.

Adversaries may use acquired domains for a variety of purposes, including for [Phishing](https://attack.mitre.org/techniques/T1566), [Drive-by Compromise](https://attack.mitre.org/techniques/T1189), and Command and Control.(Citation: CISA MSS Sep 2020) Adversaries may choose domains that are similar to legitimate domains, including through use of homoglyphs or use of a different top-level domain (TLD).(Citation: FireEye APT28)(Citation: PaypalScam) Typosquatting may be used to aid in delivery of payloads via [Drive-by Compromise](https://attack.mitre.org/techniques/T1189). Adversaries may also use internationalized domain names (IDNs) and different character sets (e.g. Cyrillic, Greek, etc.) to execute "IDN homograph attacks," creating visually similar lookalike domains used to deliver malware to victim machines.(Citation: CISA IDN ST05-016)(Citation: tt\_httrack\_fake\_domains)(Citation: tt\_obliqueRAT)(Citation: httrack\_unhcr)(Citation: lazgroup\_idn\_phishing)

Different URIs/URLs may also be dynamically generated to uniquely serve malicious content to victims (including one-time, single use domain names).(Citation: iOS URL Scheme)(Citation: URI)(Citation: URI Use)(Citation: URI Unique)

Adversaries may also acquire and repurpose expired domains, which may be potentially already allowlisted/trusted by defenders based on an existing reputation/history.(Citation: Categorisation\_not\_boundary)(Citation: Domain\_Steal\_CC)(Citation: Redirectors\_Domain\_Fronting)(Citation: bypass\_webproxy\_filtering)

Domain registrars each maintain a publicly viewable database that displays contact information for every registered domain. Private WHOIS services display alternative information, such as their own company data, rather than the owner of the domain. Adversaries may use such private WHOIS services to obscure information about who owns a purchased domain. Adversaries may further interrupt efforts to track their infrastructure by using varied registration information and purchasing domains with different domain registrars.(Citation: Mandiant APT1)

In addition to legitimately purchasing a domain, an adversary may register a new domain in a compromised environment. For example, in AWS environments, adversaries may leverage the Route53 domain service to register a domain and create hosted zones pointing to resources of the threat actor’s choosing.(Citation: Invictus IR DangerDev 2024)

## Threat-Mapped Scoring

Score: 2.65

Priority: P3 - Important (Medium)

## Kill Chain Phases

**•** mitre-attack: resource-development

## Malware

* DarkGate
* Raspberry Robin
* XLoader

## APTs (Intrusion Sets)

* APT1
* APT28
* APT32
* APT38
* APT42
* BITTER
* CURIUM
* Dragonfly
* EXOTIC LILY
* Earth Lusca
* FIN7
* Ferocious Kitten
* Gamaredon Group
* HEXANE
* IndigoZebra
* Kimsuky
* Lazarus Group
* LazyScripter
* Leviathan
* Magic Hound
* Moonstone Sleet
* Mustang Panda
* OilRig
* RedEcho
* Sandworm Team
* Sea Turtle
* Silent Librarian
* Star Blizzard
* Storm-1811
* TA2541
* TA505
* TeamTNT
* Threat Group-3390
* Transparent Tribe
* Winnti Group
* Winter Vivern
* ZIRCONIUM
* menuPass