# TTP Detail – T1482

## TTP Information

Name: Domain Trust Discovery

Description: Adversaries may attempt to gather information on domain trust relationships that may be used to identify lateral movement opportunities in Windows multi-domain/forest environments. Domain trusts provide a mechanism for a domain to allow access to resources based on the authentication procedures of another domain.(Citation: Microsoft Trusts) Domain trusts allow the users of the trusted domain to access resources in the trusting domain. The information discovered may help the adversary conduct [SID-History Injection](https://attack.mitre.org/techniques/T1134/005), [Pass the Ticket](https://attack.mitre.org/techniques/T1550/003), and [Kerberoasting](https://attack.mitre.org/techniques/T1558/003).(Citation: AdSecurity Forging Trust Tickets)(Citation: Harmj0y Domain Trusts) Domain trusts can be enumerated using the `DSEnumerateDomainTrusts()` Win32 API call, .NET methods, and LDAP.(Citation: Harmj0y Domain Trusts) The Windows utility [Nltest](https://attack.mitre.org/software/S0359) is known to be used by adversaries to enumerate domain trusts.(Citation: Microsoft Operation Wilysupply)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: discovery

## Malware

* BADHATCH
* Bazar
* DUSTTRAP
* IcedID
* Latrodectus
* MgBot
* Pikabot
* QakBot
* SocGholish
* TrickBot

## Tools

* AdFind
* BloodHound
* Brute Ratel C4
* Empire
* Nltest
* PoshC2
* PowerSploit
* Rubeus
* dsquery

## APTs (Intrusion Sets)

* Akira
* BlackByte
* Chimera
* Earth Lusca
* FIN8
* Lotus Blossom
* Magic Hound
* Storm-1811