# TTP Detail – T1110.003

## TTP Information

Name: Password Spraying

Description: Adversaries may use a single or small list of commonly used passwords against many different accounts to attempt to acquire valid account credentials. Password spraying uses one password (e.g. 'Password01'), or a small list of commonly used passwords, that may match the complexity policy of the domain. Logins are attempted with that password against many different accounts on a network to avoid account lockouts that would normally occur when brute forcing a single account with many passwords. (Citation: BlackHillsInfosec Password Spraying)

Typically, management services over commonly used ports are used when password spraying. Commonly targeted services include the following:

\* SSH (22/TCP)
\* Telnet (23/TCP)
\* FTP (21/TCP)
\* NetBIOS / SMB / Samba (139/TCP & 445/TCP)
\* LDAP (389/TCP)
\* Kerberos (88/TCP)
\* RDP / Terminal Services (3389/TCP)
\* HTTP/HTTP Management Services (80/TCP & 443/TCP)
\* MSSQL (1433/TCP)
\* Oracle (1521/TCP)
\* MySQL (3306/TCP)
\* VNC (5900/TCP)

In addition to management services, adversaries may "target single sign-on (SSO) and cloud-based applications utilizing federated authentication protocols," as well as externally facing email applications, such as Office 365.(Citation: US-CERT TA18-068A 2018)

In default environments, LDAP and Kerberos connection attempts are less likely to trigger events over SMB, which creates Windows "logon failure" event ID 4625.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: credential-access

## Malware

* Bad Rabbit
* Linux Rabbit

## Tools

* CrackMapExec
* MailSniper

## APTs (Intrusion Sets)

* APT28
* APT29
* APT33
* Agrius
* Chimera
* Ember Bear
* HAFNIUM
* HEXANE
* Lazarus Group
* Leafminer
* Silent Librarian