# TTP Detail – T1110.004

## TTP Information

Name: Credential Stuffing

Description: Adversaries may use credentials obtained from breach dumps of unrelated accounts to gain access to target accounts through credential overlap. Occasionally, large numbers of username and password pairs are dumped online when a website or service is compromised and the user account credentials accessed. The information may be useful to an adversary attempting to compromise accounts by taking advantage of the tendency for users to use the same passwords across personal and business accounts.

Credential stuffing is a risky option because it could cause numerous authentication failures and account lockouts, depending on the organization's login failure policies.

Typically, management services over commonly used ports are used when stuffing credentials. 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)

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: credential-access

## Malware

* TrickBot

## APTs (Intrusion Sets)

* Chimera