# TTP Detail – T1078

## TTP Information

Name: Valid Accounts

Description: Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Compromised credentials may be used to bypass access controls placed on various resources on systems within the network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access, network devices, and remote desktop.(Citation: volexity\_0day\_sophos\_FW) Compromised credentials may also grant an adversary increased privilege to specific systems or access to restricted areas of the network. Adversaries may choose not to use malware or tools in conjunction with the legitimate access those credentials provide to make it harder to detect their presence.

In some cases, adversaries may abuse inactive accounts: for example, those belonging to individuals who are no longer part of an organization. Using these accounts may allow the adversary to evade detection, as the original account user will not be present to identify any anomalous activity taking place on their account.(Citation: CISA MFA PrintNightmare)

The overlap of permissions for local, domain, and cloud accounts across a network of systems is of concern because the adversary may be able to pivot across accounts and systems to reach a high level of access (i.e., domain or enterprise administrator) to bypass access controls set within the enterprise.(Citation: TechNet Credential Theft)

## Threat-Mapped Scoring

Score: 3.25

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: defense-evasion

**•** mitre-attack: persistence

**•** mitre-attack: privilege-escalation

**•** mitre-attack: initial-access

## Malware

* Dtrack
* Duqu
* Industroyer
* Kinsing
* Linux Rabbit
* SeaDuke

## APTs (Intrusion Sets)

* APT18
* APT28
* APT29
* APT33
* APT39
* APT41
* Akira
* Axiom
* BlackByte
* Carbanak
* Chimera
* Cinnamon Tempest
* Dragonfly
* FIN10
* FIN4
* FIN5
* FIN6
* FIN7
* FIN8
* Fox Kitten
* GALLIUM
* INC Ransom
* Indrik Spider
* Ke3chang
* LAPSUS$
* Lazarus Group
* Leviathan
* OilRig
* POLONIUM
* PittyTiger
* Play
* Sandworm Team
* Sea Turtle
* Silence
* Silent Librarian
* Star Blizzard
* Suckfly
* Threat Group-3390
* Volt Typhoon
* Wizard Spider
* menuPass