# TTP Detail – T1133

## TTP Information

Name: External Remote Services

Description: Adversaries may leverage external-facing remote services to initially access and/or persist within a network. Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential authentication for these services. Services such as [Windows Remote Management](https://attack.mitre.org/techniques/T1021/006) and [VNC](https://attack.mitre.org/techniques/T1021/005) can also be used externally.(Citation: MacOS VNC software for Remote Desktop)

Access to [Valid Accounts](https://attack.mitre.org/techniques/T1078) to use the service is often a requirement, which could be obtained through credential pharming or by obtaining the credentials from users after compromising the enterprise network.(Citation: Volexity Virtual Private Keylogging) Access to remote services may be used as a redundant or persistent access mechanism during an operation.

Access may also be gained through an exposed service that doesn’t require authentication. In containerized environments, this may include an exposed Docker API, Kubernetes API server, kubelet, or web application such as the Kubernetes dashboard.(Citation: Trend Micro Exposed Docker Server)(Citation: Unit 42 Hildegard Malware)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: persistence

**•** mitre-attack: initial-access

## Malware

* Doki
* Hildegard
* Kinsing
* Linux Rabbit
* Mafalda

## APTs (Intrusion Sets)

* APT18
* APT28
* APT29
* APT41
* Akira
* Chimera
* Dragonfly
* Ember Bear
* FIN13
* FIN5
* GALLIUM
* GOLD SOUTHFIELD
* Ke3chang
* Kimsuky
* LAPSUS$
* Leviathan
* OilRig
* Play
* Sandworm Team
* Scattered Spider
* Sea Turtle
* TeamTNT
* Threat Group-3390
* Velvet Ant
* Volt Typhoon
* Wizard Spider