# TTP Detail – T1552.004

## TTP Information

Name: Private Keys

Description: Adversaries may search for private key certificate files on compromised systems for insecurely stored credentials. Private cryptographic keys and certificates are used for authentication, encryption/decryption, and digital signatures.(Citation: Wikipedia Public Key Crypto) Common key and certificate file extensions include: .key, .pgp, .gpg, .ppk., .p12, .pem, .pfx, .cer, .p7b, .asc.   
  
Adversaries may also look in common key directories, such as <code>~/.ssh</code> for SSH keys on \* nix-based systems or <code>C:&#92;Users&#92;(username)&#92;.ssh&#92;</code> on Windows. Adversary tools may also search compromised systems for file extensions relating to cryptographic keys and certificates.(Citation: Kaspersky Careto)(Citation: Palo Alto Prince of Persia)  
  
When a device is registered to Entra ID, a device key and a transport key are generated and used to verify the device’s identity.(Citation: Microsoft Primary Refresh Token) An adversary with access to the device may be able to export the keys in order to impersonate the device.(Citation: AADInternals Azure AD Device Identities)  
  
On network devices, private keys may be exported via [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as `crypto pki export`.(Citation: cisco\_deploy\_rsa\_keys)   
  
Some private keys require a password or passphrase for operation, so an adversary may also use [Input Capture](https://attack.mitre.org/techniques/T1056) for keylogging or attempt to [Brute Force](https://attack.mitre.org/techniques/T1110) the passphrase off-line. These private keys can be used to authenticate to [Remote Services](https://attack.mitre.org/techniques/T1021) like SSH or for use in decrypting other collected files such as email.

## Threat-Mapped Scoring

Score: 3.25

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: credential-access

## Malware

* Ebury
* FoggyWeb
* Hildegard
* Kinsing
* Machete
* Mafalda
* Troll Stealer
* jRAT

## Tools

* AADInternals
* Empire
* Mimikatz

## APTs (Intrusion Sets)

* Rocke
* Scattered Spider
* TeamTNT
* Volt Typhoon