# TTP Detail – T1070.007

## TTP Information

Name: Clear Network Connection History and Configurations

Description: Adversaries may clear or remove evidence of malicious network connections in order to clean up traces of their operations. Configuration settings as well as various artifacts that highlight connection history may be created on a system and/or in application logs from behaviors that require network connections, such as [Remote Services](https://attack.mitre.org/techniques/T1021) or [External Remote Services](https://attack.mitre.org/techniques/T1133). Defenders may use these artifacts to monitor or otherwise analyze network connections created by adversaries.

Network connection history may be stored in various locations. For example, RDP connection history may be stored in Windows Registry values under (Citation: Microsoft RDP Removal):

\* <code>HKEY\_CURRENT\_USER\Software\Microsoft\Terminal Server Client\Default</code>
\* <code>HKEY\_CURRENT\_USER\Software\Microsoft\Terminal Server Client\Servers</code>

Windows may also store information about recent RDP connections in files such as <code>C:\Users\\%username%\Documents\Default.rdp</code> and `C:\Users\%username%\AppData\Local\Microsoft\Terminal
Server Client\Cache\`.(Citation: Moran RDPieces) Similarly, macOS and Linux hosts may store information highlighting connection history in system logs (such as those stored in `/Library/Logs` and/or `/var/log/`).(Citation: Apple Culprit Access)(Citation: FreeDesktop Journal)(Citation: Apple Unified Log Analysis Remote Login and Screen Sharing)

Malicious network connections may also require changes to third-party applications or network configuration settings, such as [Disable or Modify System Firewall](https://attack.mitre.org/techniques/T1562/004) or tampering to enable [Proxy](https://attack.mitre.org/techniques/T1090). Adversaries may delete or modify this data to conceal indicators and/or impede defensive analysis.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* SUNBURST

## APTs (Intrusion Sets)

* Volt Typhoon