# TTP Detail – T1552.003

## TTP Information

Name: Bash History

Description: Adversaries may search the bash command history on compromised systems for insecurely stored credentials. Bash keeps track of the commands users type on the command-line with the "history" utility. Once a user logs out, the history is flushed to the user’s <code>.bash\_history</code> file. For each user, this file resides at the same location: <code>~/.bash\_history</code>. Typically, this file keeps track of the user’s last 500 commands. Users often type usernames and passwords on the command-line as parameters to programs, which then get saved to this file when they log out. Adversaries can abuse this by looking through the file for potential credentials. (Citation: External to DA, the OS X Way)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: credential-access

## Malware

* Kinsing