# TTP Detail – T1654

## TTP Information

Name: Log Enumeration

Description: Adversaries may enumerate system and service logs to find useful data. These logs may highlight various types of valuable insights for an adversary, such as user authentication records ([Account Discovery](https://attack.mitre.org/techniques/T1087)), security or vulnerable software ([Software Discovery](https://attack.mitre.org/techniques/T1518)), or hosts within a compromised network ([Remote System Discovery](https://attack.mitre.org/techniques/T1018)).

Host binaries may be leveraged to collect system logs. Examples include using `wevtutil.exe` or [PowerShell](https://attack.mitre.org/techniques/T1059/001) on Windows to access and/or export security event information.(Citation: WithSecure Lazarus-NoPineapple Threat Intel Report 2023)(Citation: Cadet Blizzard emerges as novel threat actor) In cloud environments, adversaries may leverage utilities such as the Azure VM Agent’s `CollectGuestLogs.exe` to collect security logs from cloud hosted infrastructure.(Citation: SIM Swapping and Abuse of the Microsoft Azure Serial Console)

Adversaries may also target centralized logging infrastructure such as SIEMs. Logs may also be bulk exported and sent to adversary-controlled infrastructure for offline analysis.

In addition to gaining a better understanding of the environment, adversaries may also monitor logs in real time to track incident response procedures. This may allow them to adjust their techniques in order to maintain persistence or evade defenses.(Citation: Permiso GUI-Vil 2023)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: discovery

## Malware

* Akira \_v2
* DUSTTRAP
* Megazord

## Tools

* Pacu

## APTs (Intrusion Sets)

* APT5
* Aquatic Panda
* Ember Bear
* Volt Typhoon