# TTP Detail – T1027.011

## TTP Information

Name: Fileless Storage

Description: Adversaries may store data in "fileless" formats to conceal malicious activity from defenses. Fileless storage can be broadly defined as any format other than a file. Common examples of non-volatile fileless storage in Windows systems include the Windows Registry, event logs, or WMI repository.(Citation: Microsoft Fileless)(Citation: SecureList Fileless) In Linux systems, shared memory directories such as `/dev/shm`, `/run/shm`, `/var/run`, and `/var/lock` may also be considered fileless storage, as files written to these directories are mapped directly to RAM and not stored on the disk.(Citation: Elastic Binary Executed from Shared Memory Directory)(Citation: Akami Frog4Shell 2024)(Citation: Aquasec Muhstik Malware 2024)

Similar to fileless in-memory behaviors such as [Reflective Code Loading](https://attack.mitre.org/techniques/T1620) and [Process Injection](https://attack.mitre.org/techniques/T1055), fileless data storage may remain undetected by anti-virus and other endpoint security tools that can only access specific file formats from disk storage. Leveraging fileless storage may also allow adversaries to bypass the protections offered by read-only file systems in Linux.(Citation: Sysdig Fileless Malware 23022)

Adversaries may use fileless storage to conceal various types of stored data, including payloads/shellcode (potentially being used as part of [Persistence](https://attack.mitre.org/tactics/TA0003)) and collected data not yet exfiltrated from the victim (e.g., [Local Data Staging](https://attack.mitre.org/techniques/T1074/001)). Adversaries also often encrypt, encode, splice, or otherwise obfuscate this fileless data when stored.

Some forms of fileless storage activity may indirectly create artifacts in the file system, but in central and otherwise difficult to inspect formats such as the WMI (e.g., `%SystemRoot%\System32\Wbem\Repository`) or Registry (e.g., `%SystemRoot%\System32\Config`) physical files.(Citation: Microsoft Fileless)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* CHOPSTICK
* Chaes
* ComRAT
* DarkWatchman
* Exaramel for Windows
* Gelsemium
* Grandoreiro
* Mosquito
* NETWIRE
* Pikabot
* Pillowmint
* PipeMon
* PolyglotDuke
* QUADAGENT
* QakBot
* RCSession
* REvil
* RegDuke
* ShadowPad
* Sibot
* SysUpdate
* TYPEFRAME
* ThreatNeedle
* TinyTurla
* Uroburos
* Valak
* Volgmer

## APTs (Intrusion Sets)

* APT32
* Turla