Docs » Analytics » Modification of ld.so.preload

○ Edit on GitHub

Modification of ld.so.preload

Identifies modification of ld.so.preload for shared object injection. This technique is used by attackers to load arbitrary code into processes.

id:	fd9b987a-1101-4ed3-bda6-a70300eaf57e
categories:	detect
confidence:	medium
os:	linux
created:	05/17/2019
updated:	05/17/2019

MITRE ATT&CK™ Mapping

tactics:	Defense Evasion
techniques:	T1055 Process Injection

Query

```
file where file_path="/etc/ld.so.preload"
```

Detonation

Atomic Red Team: T1055

Contributors

- Tony Lambert

◀ Previous

Next ▶

© Copyright 2019, Endgame Revision 30243396.

Built with Sphinx using a theme provided by Read the Docs.