

GitHub - LOLBAS-Project/LOLBAS: Living Off The Land Binaries And Scripts - (LOLBins and LOLScripts)

By wietze

Archived: 2026-04-05 18:25:18 UTC

build passing LOLBAS 232 Stars 8.4k

Living Off The Land Binaries and Scripts (and now also Libraries)



All the different files can be found behind a fancy frontend here: <https://lolbas-project.github.io> (thanks @ConsciousHacker for this bit of eyecandy and the team over at <https://gtfobins.github.io/>). This repo serves as a place where we maintain the YML files that are used by the fancy frontend.

Goal

The goal of the LOLBAS project is to document every binary, script, and library that can be used for Living Off The Land techniques.

Criteria

A LOLBin/Lib/Script must:

- Be a Microsoft-signed file, either native to the OS or downloaded from Microsoft.
- Have extra "unexpected" functionality. It is not interesting to document intended use cases.
 - Exceptions are application whitelisting bypasses
- Have functionality that would be useful to an APT or red team

Interesting functionality can include:

- Executing code
 - Arbitrary code execution
 - Pass-through execution of other programs (unsigned) or scripts (via a LOLBin)
- Compiling code
- File operations
 - Downloading
 - Upload
 - Copy
- Persistence
 - Pass-through persistence utilizing existing LOLBin
 - Persistence (e.g. hide data in ADS, execute at logon)
- UAC bypass
- Credential theft
- Dumping process memory
- Surveillance (e.g. keylogger, network trace)
- Log evasion/modification
- DLL side-loading/hijacking without being relocated elsewhere in the filesystem.

We do not approve binaries that allows for netntlm coercing, since most Windows binaries allows for that. Only exception is binaries that allows that on other than default ports (such as rpcping) or can allow direct credential theft.

Contributing

If you have found a new LOLBin or LOLScript that you would like to contribute, please review the contributing guidelines located here: <https://github.com/LOLBAS-Project/LOLBAS/blob/master/CONTRIBUTING.md>

A template for the required format has been provided here: <https://github.com/LOLBAS-Project/LOLBAS/blob/master/YML-Template.yml>

The History of the LOLBin

The phrase "Living off the land" was coined by Christopher Campbell (@obscuresec) & Matt Graeber (@mattifestation) at [DerbyCon 3](#).

The term LOLBins came from a Twitter discussion on what to call binaries that can be used by an attacker to perform actions beyond their original purpose. Philip Goh (@MathCasualty) [proposed LOLBins](#). A highly scientific internet poll ensued, and after a general consensus (69%) was reached, the name was [made official](#). Jimmy (@bohops) [followed up with LOLScripts](#). No poll was taken.

Common hashtags for these files are:

- #LOLBin
- #LOLBins
- #LOLScript
- #LOLScripts
- #LOLLib
- #LOLLibs

Our primary maintainer (@oddvarmoe) of this project did a talk at DerbyCon 2018 called: #Lolbins Nothing to LOL about! - <https://www.youtube.com/watch?v=NiYTdmZ8GR4> This talk goes over the history of this project.

Maintainers

The following folks help maintain the LOLBAS Project on their personal time:

- Oddvar Moe ([@oddvarmoe](#))
- Jimmy Bayne ([@bohops](#))
- Conor Richard ([@xenosCR](#))
- Chris 'Lopi' Spehn ([@ConsciousHacker](#))
- Liam ([@liamsomerville](#))
- Wietze ([@Wietze](#))
- Jose Hernandez ([@_josehelps](#))

Thanks

As with many open-source projects, this one is the product of a community and we would like to thank ours:

- The domain <http://lolbins.com> has been registered by an unknown individual and redirected it to the old version of this project.

- The domain <http://lolbas-project.com> has been registered by Jimmy (@bohops).
- The logos for the project were created by Adam Nadrowski (@_sup_mane). We #@&!!@#! love them.

Notice

- Please refer to NOTICE.md for license information

Source: <https://github.com/LOLBAS-Project/LOLBAS>