# GitHub - SecurityBlueTeam/Smartloader_Wireshark: Wireshark dissector for Smartloader malware

By blitztide-sbt

Archived: 2026-04-05 20:54:05 UTC

Skip to content

## Navigation Menu


- ◦ AI CODE CREATION
  - GitHub CopilotWrite better code with AI
  - GitHub SparkBuild and deploy intelligent apps
  - GitHub ModelsManage and compare prompts
  - MCP RegistryNewIntegrate external tools
  - ◦
  - ◦
  - ◦

  View all features
- 
- 
- 
- 
- Pricing

Sign up

- Notifications
- Fork 0
- Star 7


## Folders and files

| Name | Name | Last commit message | Last commit date |
|---|---|---|---|
| **Latest commit**<br><br>blitztide-sbt<br><br>Merge pull request #3 from SecurityBlueTeam/DEV<br><br>Feb 13, 2025<br><br>1169e78 · Feb 13, 2025<br><br>**History**<br><br>7 Commits | | | |
| LICENSE.md | LICENSE.md | Initial commit | Feb 11, 2025 |
| Readme.md | Readme.md | Initial commit | Feb 11, 2025 |
| Smartloader_Encryption.lua | Smartloader_Encryption.lua | Initial commit | Feb 11, 2025 |
| base64.lua | base64.lua | Initial commit | Feb 11, 2025 |
| json.lua | json.lua | Initial commit | Feb 11, 2025 |
| smartloader.lua | smartloader.lua | Further fixes to dump script | Feb 13, 2025 |

| Name | Name | Last commit message | Last commit date |
| --- | --- | --- | --- |
| smartloader_githubpayloaddump.lua | smartloader_githubpayloaddump.lua | Further fixes to dump script | Feb 13, 2025 |

- README
- GPL-3.0 license

## Smartloader Wireshark plugin

This plugin is designed and tested on Wireshark 4.4.3 and is intended to decode C2 traffic for the Smartloader malware variant.

## Installing

Windows users are to unzip the zip file in `%APPDATA%\Wireshark\plugins`. *nix users are to unzip the zip file in `~/.local/lib/wireshark/plugins`.

## Configuring

In Preferences>Protocols>Smartloader you are able to enable/disable the plugin, and change the encryption key used by the malware.

---