




main		Go to file		<> Code
				808 Commits
📁	.github			
📁	.godana			
📁	data			
📁	docs			
📁	pkg			
📄	.gitattributes			
📄	.gitignore			
📄	.gitmodules			
📄	Dockerfile			
📄	LICENSE			
📄	Makefile			
📄	README.MD			
📄	go.mod			
📄	go.sum			
📄	main.go			

 README

 GPL-3.0 license



CodeQL

passing

go report

A+

License


GPL v3

release


v2.1.3

downloads

76k

 Follow

Merlin



Merlin is a cross-platform post-exploitation Command & Control server and agent written in Go.


Highlighted features:


About


Merlin is a cross-platform post-exploitation HTTP/2 Command & Control server and agent written in golang.


[agent](#) [golang](#) [http2](#) [post-exploitation](#)


[c2](#) [command-and-control](#)


 [Readme](#)

 [GPL-3.0 license](#)

 [Activity](#)


 [5.1k stars](#)

 [138 watching](#)

 [801 forks](#)

[Report repository](#)

Releases 29

 **v2.1.3** Latest

on Apr 23


+ 28 releases

Packages

No packages published

Contributors 15

Languages



A horizontal bar chart titled 'Languages' showing the distribution of languages. The chart has two categories: 'Go' and 'Other'. The 'Go' category is represented by a blue bar and accounts for 99.5% of the total. The 'Other' category is represented by a grey bar and accounts for 0.5% of the total.

Language	Percentage
Go	99.5%
Other	0.5%

- [merlin-cli](#) command line interface over gRPC to connect to the Merlin Server facilitating multi-user support
- Supported Agent C2 Protocols: http/1.1 clear-text, http/1.1 over TLS, HTTP/2, HTTP/2 clear-text (h2c), http/3 (http/2 over QUIC)
- Peer-to-peer (P2P) communication between Agents with bind or reverse for SMB, TCP, and UDP
- Configurable agent data encoding and encryption transforms: AES, Base64, gob, hex, JWE, RC4, and XOR
 - JWE transform use [PBES2_HS512_A256KW](#) PBES2 (RFC 2898) with HMAC SHA-512 as the PRF and AES Key Wrap (RFC 3394) using 256-bit keys for the encryption scheme
- Configurable agent authenticators:
 - None: No authentication
 - [OPAQUE](#): Asymmetric Password Authenticated Key Exchange (PAKE)
- Encrypted JWT for message authentication
- Configurable Agent message data [padding](#) to combat beaconing detections based on a fixed message size
- Execute .NET assemblies in-process with `invoke-assembly` or in a sacrificial process with `execute-assembly`
- Execute arbitrary Windows executables (PE) in a sacrificial process with `execute-pe`
- Various shellcode execution techniques: CreateThread, CreateRemoteThread, RtlCreateUserThread, QueueUserAPC
- Integrated [Donut](#), [sRDI](#), and [SharpGen](#) support
- Dynamically change the Agent's [JA3](#) hash
- [Mythic](#) support
- [Documentation & Wiki](#)

An introductory blog post can be found here:
<https://medium.com/@Ne0nd0g/introducing-merlin-645da3c635a>

Supporting Repositories:

- [Merlin Agent](#) - Agent source code
- [Merlin Agent DLL](#) - Agent DLL source code
- [Merlin CLI](#) - Command line interface for Merlin
- [Merlin Documentation](#) - Documentation source code
- [Merlin on Mythic](#) - Merlin agent for Mythic Framework
- [Merlin Docker](#) - Base Docker image for for Merlin images
- [Merlin Message](#) - A Go library for Merlin messages exchanged between a Merlin Server and Agent

Quick Start

- Download the latest version of Merlin Server from the [releases](#) section

The Server package contains compiled versions of the CLI and Agent for all the major operating systems in the `data/bin` directory

- Extract the files with 7zip using the `x` function **The password is:** `merlin`
- Start Merlin
- Start the CLI
- Configure a [listener](#)
- Deploy an agent. See [Agent Execution Quick Start Guide](#) for examples
- Pwn, Pivot, Profit

```
mkdir /opt/merlin;cd /opt/merlin
wget https://github.com/Ne0nd0g/merlin/releases/latest/download/merlinServer-Linux-x64.7z
7z x merlinServer-Linux-x64.7z
sudo ./merlinServer-Linux-x64
./data/bin/merlinCLI-Linux-x64
```



Mythic

Merlin can be integrated and used as an agent with the [Mythic](#) a collaborative, multi-platform, red teaming framework.

Visit the [Merlin on Mythic](#) repository in the MythicAgents organization to get started.

Misc.

- To compile Merlin from source, view the [Custom Build](#) page
- For a full list of available commands:
 - [Main Menu](#)
 - [Listener Menu](#)
 - [Agent Menu](#)
 - [Module Menu](#)
- View the [Frequently Asked Questions](#) page
- View the [Blog Posts](#) page for additional information

Slack

Join the `#merlin` channel in the [BloodHoundGang](#) Slack to ask questions, troubleshoot, or provide feedback.

JetBrains

Thanks to [JetBrains](#) for kindly sponsoring Merlin by providing a Goland IDE Open Source license

