GitHub - Ne0nd0g/merlin: Merlin is a cross-platform post-exploitation HTTP/2 Command & Control server and agent written in golang.

By Ne0nd0g

Archived: 2026-04-06 00:28:09 UTC

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

Highlighted features:

- 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

1. 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

2. Extract the files with 7zip using the `x` function **The password is:** `merlin`
3. Start Merlin
4. Start the CLI
5. Configure a listener
6. Deploy an agent. See Agent Execution Quick Start Guide for examples
7. 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

Source: https://github.com/Ne0nd0g/merlin