Merlin

github.com/Ne0nd0g/merlin

Ne0nd0g

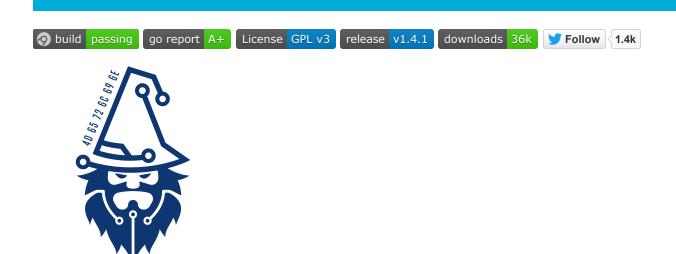
Ne0nd0g/merlin



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







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

Highlighted features:

- Supported 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)
- Server and Agent: Windows, Linux, macOS (Darwin), MIPS, ARM or anything Go can natively build

Windows DLL Agent

- Domain Fronting
- 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
- OPAQUE Asymmetric Password Authenticated Key Exchange (PAKE)
- Encrypted JWT for authentication
- Agent traffic is an encrypted JWE using PBES2 (RFC 2898) with HMAC SHA-512 as the PRF and AES Key Wrap (RFC 3394) using 256-bit keys for the encryption scheme. (PBES2 HS512 A256KW)
- Integrated <u>Donut</u>, <u>sRDI</u>, and <u>SharpGen</u> support
- C2 traffic message <u>padding</u> to combat beaconing detections based on a fixed message size
- Dynamically change the Agent's <u>JA3</u> hash
- Mythic support
- Documentation & Wiki

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

Quick Start

1. Download the latest compiled version of Merlin Server from the releases section

The Server package contains a compiled 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. Configure a <u>listener</u>
- 5. Deploy an agent. See Agent Execution Quick Start Guide for examples
- 6. Pwn, Pivot, Profit

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

Agents

The Merlin Agent is kept in its own repository so that it can easily be retrieved and compiled:

go get github.com/NeOndOg/merlin-agent

The <u>Windows DLL Agent</u> is also kept in a separate repository. See the <u>DLL Agent</u> documentation for building instructions.

Mythic

The Merlin server is a self-contained command line program that requires no installation. You just simply download it and run it. The command-line interface only works great if it will be used by a single operator at a time. The Merlin agent can be controlled through <u>Mythic</u>, which features a web-based user interface that enables multiplayer support, and a slew of other features inherent to the project.

Visit the Merlin repository in the MythicAgents organization to get started.

Misc.

- The latest development build of Merlin can be downloaded from AppVeyor
- To compile Merlin from source, view the <u>Custom Build</u> page
- For a full list of available commands:
- View the <u>Frequently Asked Questions</u> page
- View the <u>Blog Posts</u> page for additional information

Slack

Join the #merlin channel in the <u>BloodHoundGang</u> Slack to ask questions, troubleshoot, or provide feedback.

JetBrains

Thanks to <u>JetBrains</u> for kindly sponsoring Merlin by providing a Goland IDE Open Source license

