


<div> <div></div> <div>its-a-feature</div> </div>	adding icon back so it appears in overview page	a73b750 · last year	🕒 17 Commits
📁 C2_Profiles	Updating default port in config.json to ...		last year
📁 Payload_Type	Updating to Mythic 3.0		last year
📁 agent_icons	adding icon back so it appears in overv...		last year
📁 documentation-c2	Updating to Mythic 3.0		last year
📁 documentation-payload	Updating to Mythic 3.0		last year
📁 documentation-wrapper	Initial Commit		3 years ago
📄 .gitignore	Initial Commit		3 years ago
📄 README.md	Updating to Mythic 3.0		last year
📄 config.json	Updating to Mythic 3.0		last year

📖

README



Typhon

Typhon is a macOS specific payload aimed at targetting Jamf managed devices. This payload can be used to manipulate macOS devices into communicating with a Mythic instance, which acts as a Jamf server with the ability to execute commands.

This version of Typhon is compatable with Mythic 3.0.

Please use an older version if on Mythic 2.x.

Talks & Publications

- Typhon was presented in the Black Hat USA 2021 talk [Come to the Dark Side, We Have Apples: Turning macOS Management Evil](#).
- Further information about detecting typhon can be found at [TheMacPack.io - Detecting Orthrus and Typhon](#)

Installation

About

Payload designed for targeting Jamf enrolled devices.

📖

Readme

📈

Activity

📋

Custom properties

★

35 stars

👁

6 watching

🔗

2 forks

Report repository

Releases

No releases published

Packages

No packages published

Contributors 3

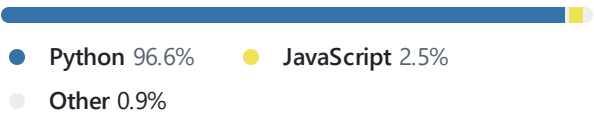
- 🌐

sclow
- 🔴

its-a-feature Cody Thomas
- 👤

calhall Calum Hall

Languages



To install typhon, you'll need Mythic installed on a remote computer. You can find installation instructions for Mythic at the [Mythic project page](#).

From the Mythic install root, run the command:

```
./mythic-cli install github https://github.com/MythicAgents/typhon.git
```

Once installed, restart Mythic to build a new agent.

Notable Features

The typhon agent utilises functionality provided by the Jamf binary. As such no additional code needs to be introduced to the compromised device for this agent to operate.

The client-side Jamf agent contains a variety of functionality that may be utilised by this Mythic payload/profile, however the main focus of the initial release is providing code execution through the agent itself. Any additional feature requests are welcomed.

Commands Manual Quick Reference

The agent currently employs three commands that imitate standard Jamf policy instructions.

Commands

Command	Syntax	Description
add_user	<code>add_user</code>	Add a standard or administrative user to the device.
delete_user	<code>delete_user</code>	Deletes a user account on the device.
execute_command	<code>execute_command</code>	Executes a bash command on the target device with root privileges.

