Cross-Platform Evasion

Offensive Tooling for Windows, macOS and Linux

Copyright © Fortra, LLC and its group of companies. Fortra®, the Fortra® logos, and other identified marks are proprietary trademarks of Fortra, LLC.

FORTRA

Solutions

INFRASTRUCTURE PROTECTION & DATA SECURITY

VULNERABILITY MANAGEMENT

- Vulnerability Management
- Web Application Scanning
- Application Security Testing
- Integrity Monitoring

OFFENSIVE SECURITY

- Automated Pen Testing
- Adversary Simulations
- Red Team Operations

EMAIL SECURITY & ANTI-PHISHING

- Brand Protection
- Business Email Compromise (BEC)
- Secure Email Gateway
- Security Awareness & Phishing Simulations

DATA PROTECTION

- Data Loss Prevention (DLP)
- Data Classification
- Rights Management

DIGITAL RISK PROTECTION

- Account Takeover Protection
- Social Media Protection

SECURE FILE TRANSFER

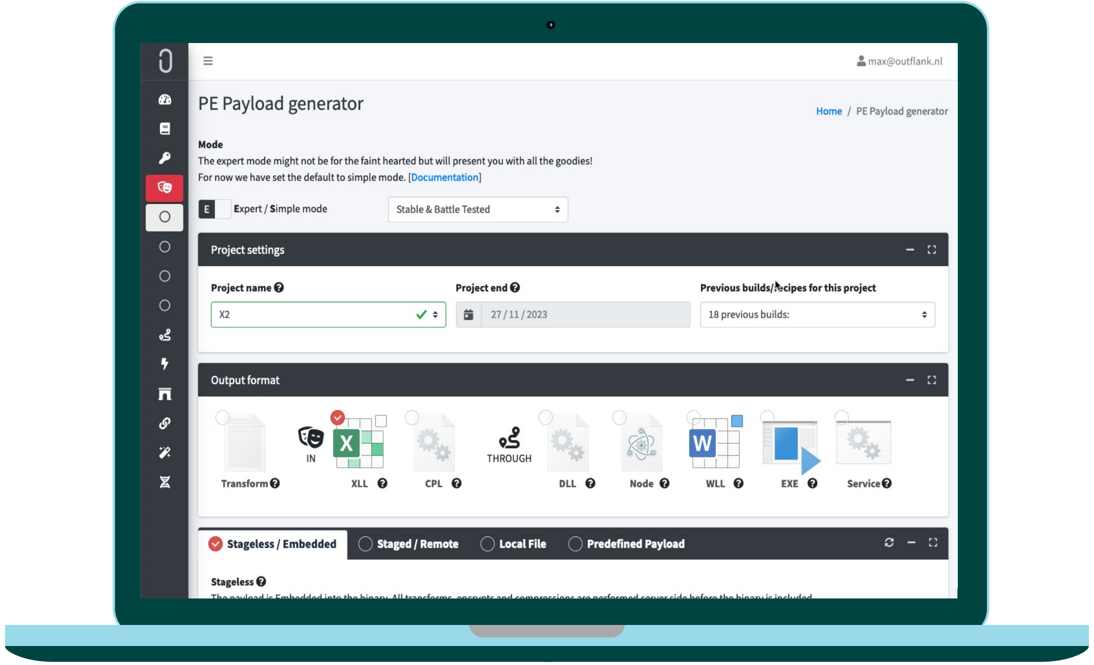
- Managed File Transfer
- Secure Email & Collaboration
- File Acceleration

Outflank Security Tooling (OST)

Tools

Knowledge

Community



PE Payload generator

Mode

The expert mode might not be for the faint hearted but will present you with all the goodies!
For now we have set the default to simple mode. [Documentation]

E Expert / Simple mode: Stable & Battle Tested

Project settings

Project name: X2

Project end: 27 / 11 / 2023

Previous builds/recipes for this project: 18 previous builds:

Output format

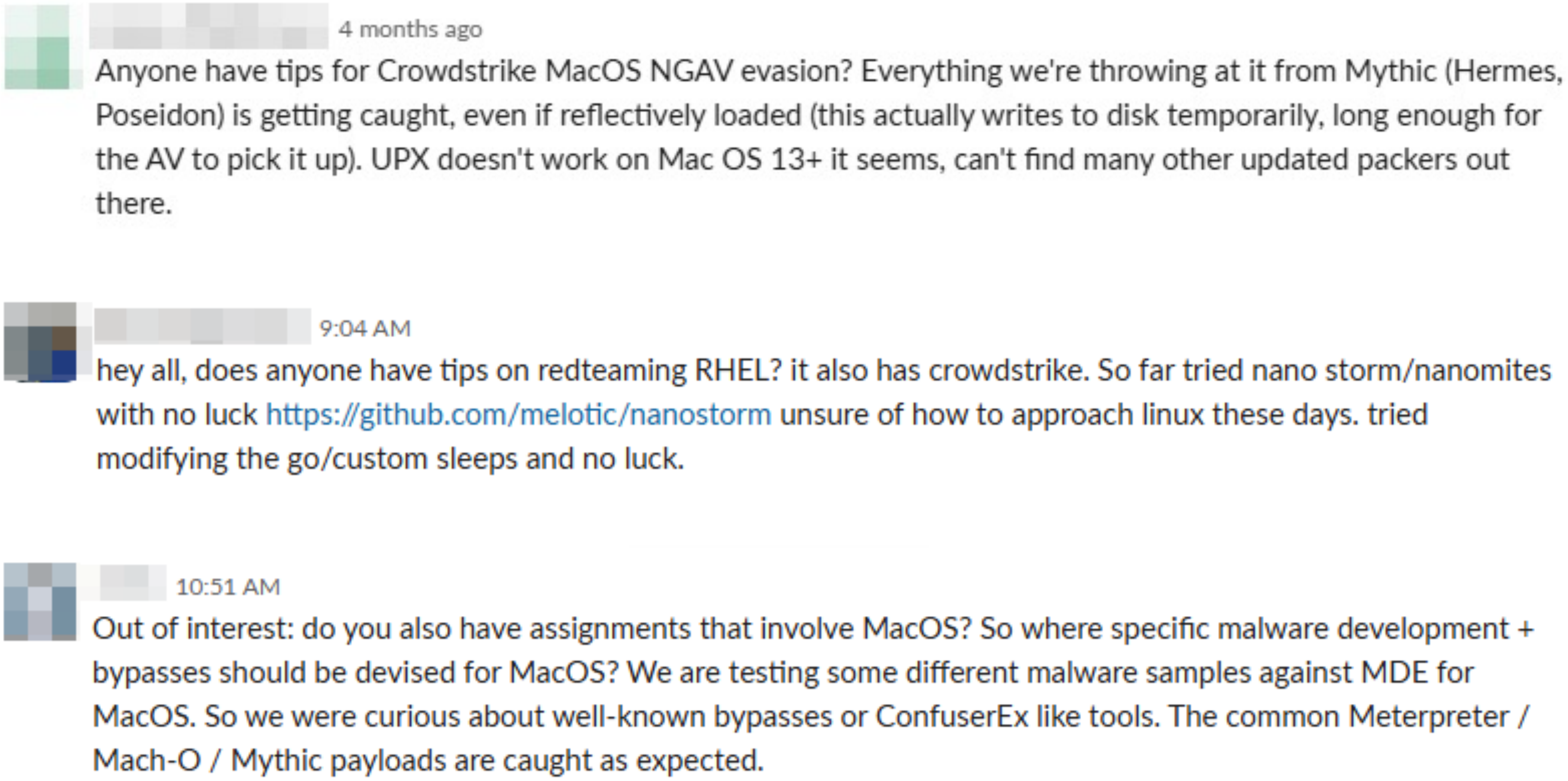
● Stageless / Embedded ○ Staged / Remote ○ Local File ○ Predefined Payload

Stageless

The payload is Embedded into the binary. All transforms, encrypts and compressions are performed server side before the binary is included

FORTRA

Why macOS and Linux?



[redacted] 4 months ago

Anyone have tips for Crowdstrike MacOS NGAV evasion? Everything we're throwing at it from Mythic (Hermes, Poseidon) is getting caught, even if reflectively loaded (this actually writes to disk temporarily, long enough for the AV to pick it up). UPX doesn't work on Mac OS 13+ it seems, can't find many other updated packers out there.

[redacted] 9:04 AM

hey all, does anyone have tips on redteaming RHEL? it also has crowdstrike. So far tried nano storm/nanomites with no luck https://github.com/melotic/nanostorm unsure of how to approach linux these days. tried modifying the go/custom sleeps and no luck.

[redacted] 10:51 AM

Out of interest: do you also have assignments that involve MacOS? So where specific malware development + bypasses should be devised for MacOS? We are testing some different malware samples against MDE for MacOS. So we were curious about well-known bypasses or ConfuserEx like tools. The common Meterpreter / Mach-O / Mythic payloads are caught as expected.

Observed malware effective on Linux:

31%

Up from 15% the previous year

Google Cloud Security / Mandiant
M-Trends 2024

Latest Additions to OST

Outflank C2 – New Implants for macOS and Linux

Native Implants

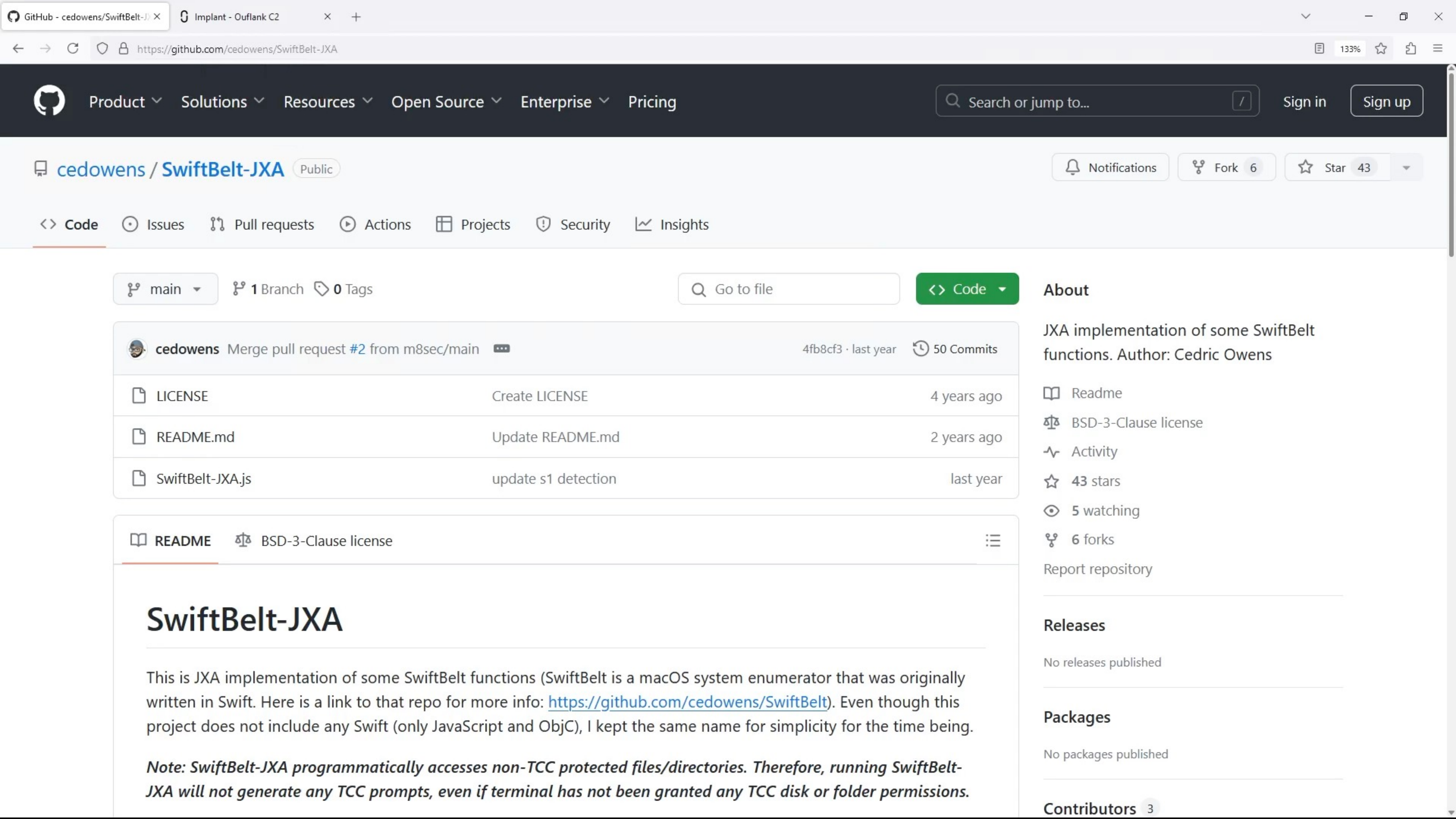
Written in C/C++/ASM, tailored to each OS (x86_64 or ARM64)

Dynamic Execution

Execute industry-standard post-exploitation tools

Network Tunneling

Proxy tools in with SOCKS, or exfiltrate data with P2P C2



cedowens / SwiftBelt-JXA Public

cedowens Merge pull request #2 from m8sec/main 4fb8cf3 · last year 50 Commits

LICENSE	Create LICENSE	4 years ago
README.md	Update README.md	2 years ago
SwiftBelt-JXA.js	update s1 detection	last year

README BSD-3-Clause license

SwiftBelt-JXA

This is JXA implementation of some SwiftBelt functions (SwiftBelt is a macOS system enumerator that was originally written in Swift. Here is a link to that repo for more info: https://github.com/cedowens/SwiftBelt). Even though this project does not include any Swift (only JavaScript and ObjC), I kept the same name for simplicity for the time being.

Note: SwiftBelt-JXA programmatically accesses non-TCC protected files/directories. Therefore, running SwiftBelt-JXA will not generate any TCC prompts, even if terminal has not been granted any TCC disk or folder permissions.

About

JXA implementation of some SwiftBelt functions. Author: Cedric Owens

Readme
BSD-3-Clause license
Activity
43 stars
5 watching
6 forks
Report repository

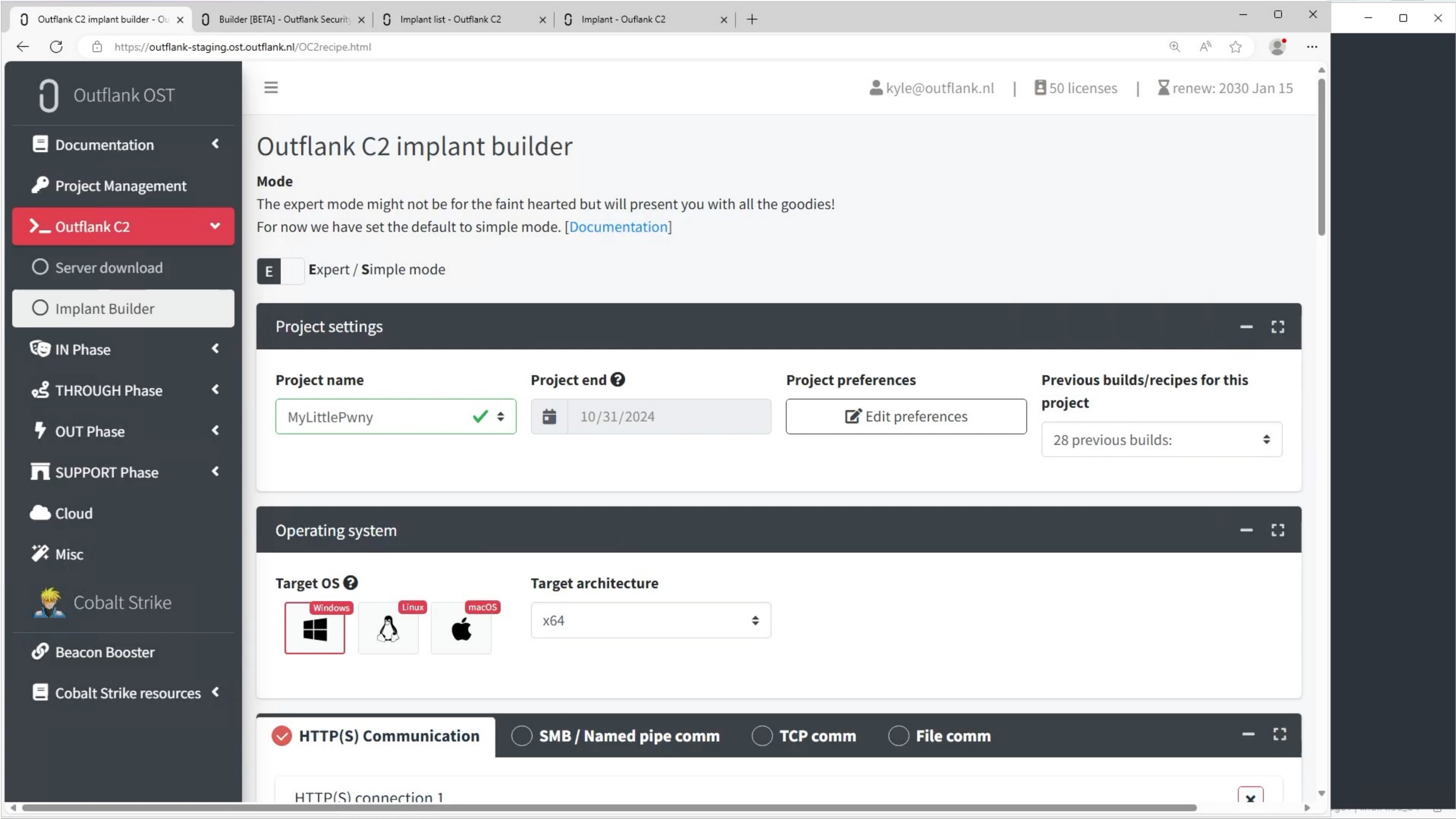
Releases

No releases published

Packages

No packages published

Contributors 3



Outflank C2 implant builder

Mode

The expert mode might not be for the faint hearted but will present you with all the goodies!
For now we have set the default to simple mode. [Documentation]

E **E**xpert / **S**imple mode

Project settings

Project name: MyLittlePwny ✓

Project end: 10/31/2024

Project preferences: Edit preferences

Previous builds/recipes for this project: 28 previous builds:

Operating system

Target OS: ☑ Windows ☐ Linux ☐ macOS

Target architecture: x64

● HTTP(S) Communication ○ SMB / Named pipe comm ○ TCP comm ○ File comm

HTTP(S) connection 1

In-Phase Builder – New macOS and Linux Payloads

Static Executable

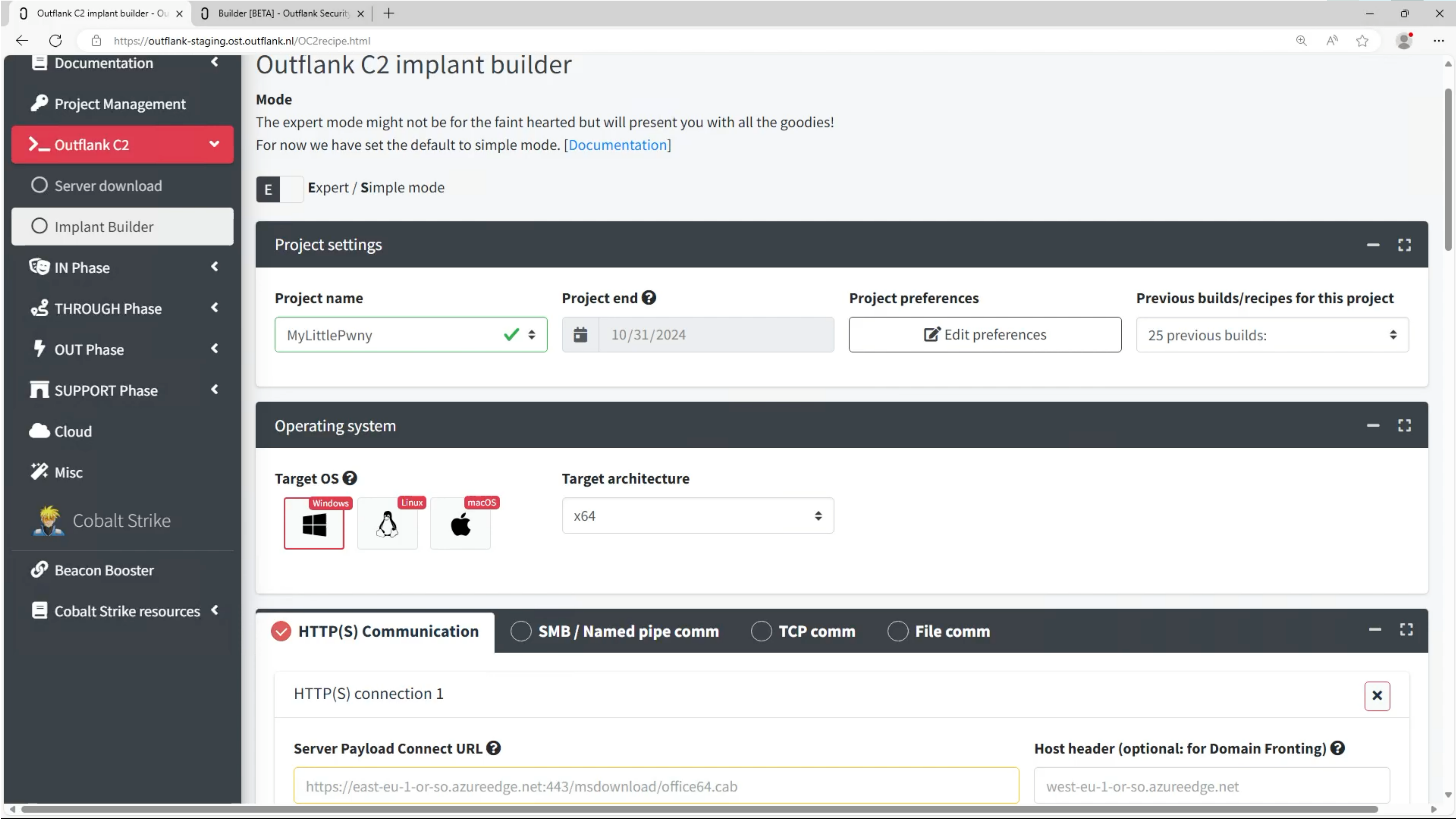
Simple payload for getting started on macOS or Linux

Excel VBA Macro

Initial access phishing payload for macOS

Shared Library

Flexible payload for sideloading on macOS or Linux



Outflank C2 implant builder

Mode

The expert mode might not be for the faint hearted but will present you with all the goodies!
For now we have set the default to simple mode. [Documentation]

E **E**xpert / **S**imple mode

Project settings

Project name: MyLittlePwny ✓

Project end: 10/31/2024

Project preferences: Edit preferences

Previous builds/recipes for this project: 25 previous builds:

Operating system

Target OS: Windows | Linux | macOS

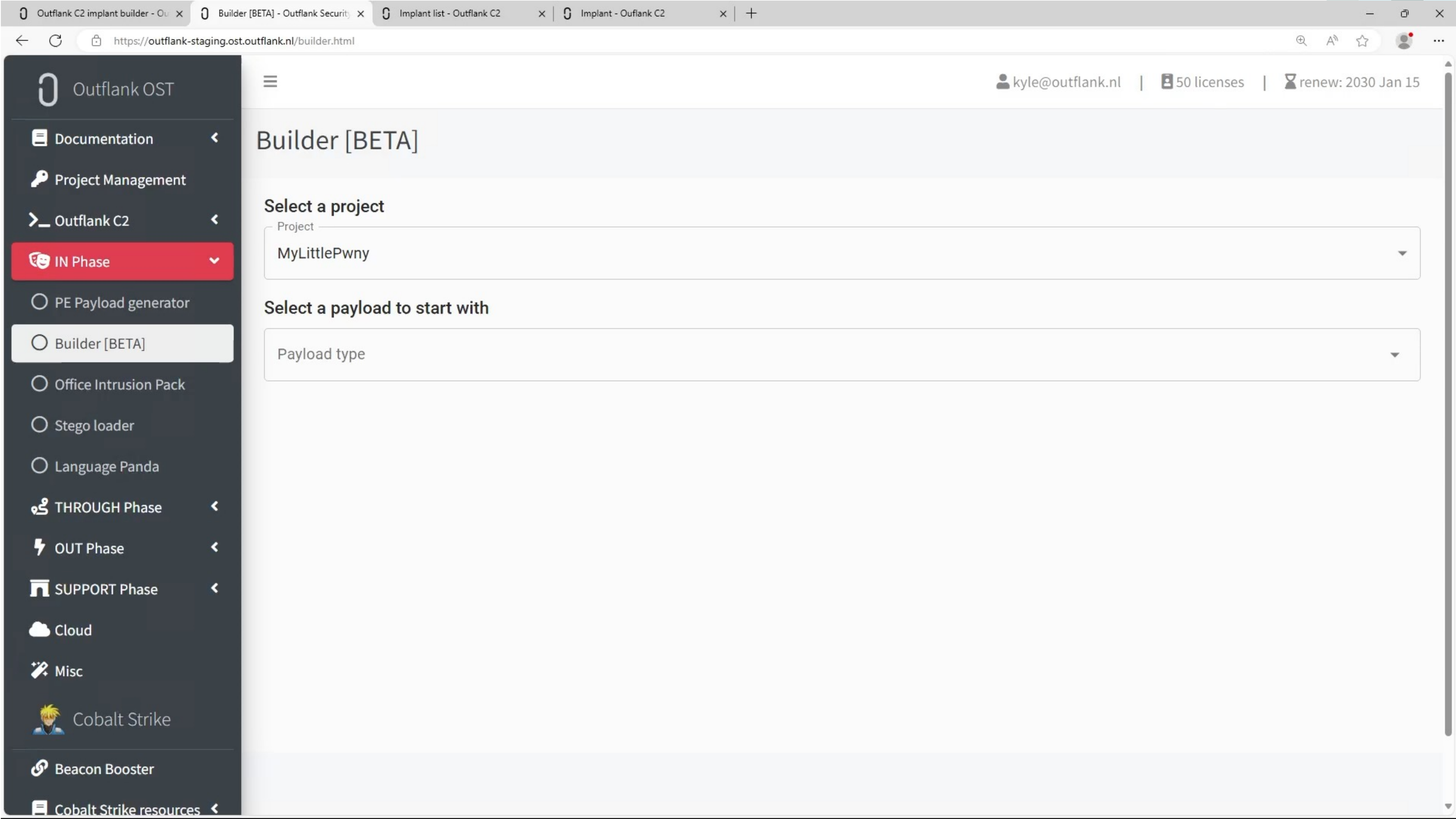
Target architecture: x64

● HTTP(S) Communication ○ SMB / Named pipe comm ○ TCP comm ○ File comm

HTTP(S) connection 1

Server Payload Connect URL: https://east-eu-1-or-so.azureedge.net:443/msdownload/office64.cab

Host header (optional: for Domain Fronting): west-eu-1-or-so.azureedge.net



Builder [BETA]

Select a project

Project: MyLittlePwny

Select a payload to start with

Payload type

Latest Additions to OST

Outflank C2 Implants

Two new implants for

macOS and Linux

In-Phase Builder Payloads

Three new loaders for

macOS and Linux

FORTRA

VISIT THE FORTRA BOOTH

Stop by booth **#305** to learn how Fortra can be your cybersecurity ally.

GET A DEMO

Receive a live demonstration of Outflank Security Tooling.

VISIT OUR WEBSITE

www.outflank.nl