FORTRA

DATASHEET (INFRASTRUCTURE PROTECTION)

# COBALT STRIKE

## Adversary Simulations and Red Team Operations

Cobalt Strike is a standard-setting adversary simulation tool, recognized globally for facilitating red team operations with its signature payload and extensible C2 framework to accurately replicate the tactics of today's advanced threat actors.

### Beacon: The Customizable Post-Exploitation Payload

Beacon, Cobalt Strike's signature payload, models the behavior of advanced adversaries to perform post-exploitation activities. Beacon offers multiple avenues of communication, including:

- **Asynchronous** – Quietly transmit Beacon using "low and slow" communication to retain stealth
- **Interactive** – Rapidly transmit Beacon for tasks that require immediate action and control
- **Malleable C2 profiles** – Modify and save network indicators to blend in with normal traffic or cloak activities by emulating different types of malware

### A Highly Flexible Framework for Tailored Red Team Engagements

Cobalt Strike was engineered for flexibility and continues to prioritize versatility, enabling operators to tailor it to suit their precise needs.

#### Arsenal Kit

- **Sleep Mask Kit** - Obfuscate Beacon in memory while it's inactive, using a customizable algorithm to encrypt data and strings
- **Mutator Kit** – Create alternate versions of the sleep mask using Low Level Virtual Machine (LLVM) to evade detection by breaking in-memory YARA scanning
- **User-Defined Reflective Loaders (UDRLs)** – Modify default behaviors and bring personalized tradecraft to increase the evasiveness of Beacon

#### Community Kit

Cobalt Strike thrives on user community engagement. The Community Kit is a curated repository of tools written by Cobalt Strike users and submitted to be shared with other operators. Currently, there are over 100 tools in the Community Kit, with more tools added regularly.

### PRODUCT SUMMARY

#### KEY FEATURES

- Malleable C2 framework
- Post-exploitation payload
- Customizable tools
- Covert communication
- Payload generation
- Community built extensions
- Red team collaboration
- Browser pivoting
- Spear phishing
- Reporting and logging

#### SYSTEM REQUIREMENTS

- 2 GHz+ processor
- 2 GB RAM
- 500MB+ available disk space
- Java
  - Oracle Java 1.8
  - Oracle Java 11
  - OpenJDK 11

#### SUPPORTED OPERATING SYSTEMS

Cobalt Strike Team Server:

- Debian
- Ubuntu
- Kali Linux

Cobalt Strike Clients:

- Windows 7 and above
- MacOS X 10.13 and above
- GUI based Linux, such as: Debian, Ubuntu and Kali Linux (other versions may work but have not been tested)

### Beacon Object Files (BOFs)

Extend Beacon's capabilities using a compiled C program, written to a convention that allows it to execute within a Beacon process and use internal Beacon APIs. BOFs and lightweight and can be rapidly developed and executed. Possible uses include:

- New commands
- Methods for gathering target information
- Data management
- Post-exploitations techniques
- Process optimizations
- And more

### Malleable C2

Tailor C2 communication to suit specific environments and objectives by creating a Malleable C2 profile that specifies how to transform and store data.

## Layered Operations with OffSec Interoperability

Cobalt Strike's extendibility enables interoperability with other security assessment tools, allowing red teams to expand the reach of their engagements. Create a holistic testing methodology and consolidate vendors by incorporating other tools in Fortra's offensive security portfolio:

### Outflank Security Tooling

This evasive red teaming toolkit integrates directly with Cobalt Strike's flexible framework through BOFs and reflective DLL loading techniques, creating advanced attack simulations designed to intelligently bypass defensive measures and detection tools.

### Core Impact

Combine this automated penetration solution with Cobalt Strike and leverage session passing and tunneling capabilities. These tools can also share resources, such as .NET assembly tools or any executions that employ the execute-assembly command.

## Use Cases for Cobalt Strike

### Gain Initial Access and Move Laterally

Cobalt Strike provides targeted phishing emails for network infiltration, with options for email templates, custom messages, and social engineering package attachments. From there, operators can move laterally through multiple techniques, including browser pivoting to hijack authenticated web sessions from compromised users.

### Post-Exploitation and Persistence

After gaining access to systems, Cobalt Strike provides robust post-exploitation capabilities. Once deployed, Beacon can gather information, execute arbitrary commands, deploy additional payloads, and more. Further post-exploitation features can be added using Beacon Object Files to establish persistence through various methods. Additionally, the Arsenal Kit can be used to create customized post-exploitation workflows tailored to specific engagement requirements.

### Efficiently Collaborate and Generate Reports

Cobalt Strike is designed for team operations, allowing multiple operators to work together seamlessly. Multiple people can log on to the team server for Red Team efforts. Once connected, team members can use the same sessions and communicate in real time through a shared event log. Team members can share access to compromised systems, coordinate actions, and generate detailed reports of their activities. Report types include:

- Timeline of activities
- Summary of data on a per-host basis
- Indicators of compromise
- Full account of activity for all sessions
- Social engineering
- Tactics, techniques, and procedures

FORTRA

Fortra.com

**About Fortra**

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.