FORTRA™

DATASHEET (CYBERSECURITY)

COBALT STRIKE

Adversary Simulations and Red Team Operations

Cobalt Strike is a powerful threat emulation tool that provides a post-exploitation agent and covert channels ideal for Adversary Simulations and Red Team exercises, replicating the tactics and techniques of an advanced adversary in a network.

Simulate an Embedded Threat Actor

Beacon, Cobalt Strike's post-exploitation payload, can be quietly transmitted over HTTP, HTTPS, or DNS and uses asynchronous "low and slow" communication commonly utilized by embedded attackers who wish to remain undetected. With Malleable C2, Beacon's flexible Command and Control language, users can modify network indicators to blend in with normal traffic or cloak its activities by emulating different types of malware. Beacon can perform various post-exploitation activities, including PowerShell script execution, keystroke logging, capturing screenshots, downloading files, and spawning other payloads.

Gain a Foothold with Targeted Attacks

Begin by gathering intelligence using Cobalt Strike's system profiler, which maps out a target's client-side attack surface, providing a list of applications and plugins it discovers through the user's browser, as well as Internal IP address of users who are behind a proxy server. With this advanced reconnaissance, it's easier to determine the most successful attack path.

Design an attack using one of Cobalt Strike's numerous packages. For example, host a web drive-by attack using website clones. Alternately, you can transform an innocent file into a trojan horse using Microsoft Office Macros or Windows Executables.

You can also deliver an attack using Cobalt Strike's spear phishing tool. Assemble a list of targets and select one of the preconfigured templates or create your own.

PRODUCT SUMMARY

KEY FEATURES

- Client-side reconnaissance
- Post exploitation payload
- Covert communication
- Attack packages
- Browser pivoting
- Spear phishing
- Red team collaboration
- 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)

Tailor Scripts and Frameworks to Suit Specific Needs

Cobalt Strike is designed with flexibility in mind in order to meet all of your needs. Users are encouraged to extend Cobalt Strike's capabilities by making changes to built-in scripts or bringing their own weaponization. Additional modifications can be made to the Cobalt Strike client by writing scripts in its custom scripting language, Aggressor Script.

Alterations can also be made to kits downloaded from the Cobalt Strike arsenal. Modify the Artifact Kit, the is a source code framework used to generate executables and DLLs or redefine the script templates located in the Resource Kit, which Cobalt Strike uses in its workflows.

Finally, you can write your own Beacon Object File (BOF) and expand the Beacon agent with post-exploitation features. A BOF is a compiled C program, written to a convention that allows it to execute within a Beacon process and use internal Beacon APIs.

Collaborate for Efficient Red Teaming

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. They are also able to share hosts, captured data, and download files.

Reconstruct Engagements with Comprehensive Reports

Cobalt Strike can generate multiple reports to provide a complete picture of all the activities that took place during an engagement. 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

Reports are exported in MS Word or as a PDF, and can be tailored as needed. Custom logos may be added, and title, description, and hosts can be configured.

Streamline Efforts with Solution Interoperability

Outflank Security Tooling (OST) is an evasive red teaming toolkit that provides coverage for every step of an engagement, from initial breach to final exfiltration. Developed to work in tandem with Cobalt Strike, OST integrates directly with Cobalt Strike's flexible framework through BOFs and reflective DLL loading techniques. Those with both tools can extend the reach of their engagements, running advanced attack simulations designed to intelligently bypass defensive measures and detection tools.

Cobalt Strike can also be used with Core Impact, an automated pen testing tool ideal for exploitation and lateral movements. Those with both Core Impact and Cobalt Strike can take advantage of session passing and tunneling capabilities between the two tools. They can also share resources, such as .NET assembly tools or any executions that employ the execute-assembly command.

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.