FORTRA®

DATASHEET (OFFENSIVE SECURITY)

Cobalt Strike and Outflank Security Tooling (OST)

Cobalt Strike and Outflank Security Tooling (OST) are two red teaming solutions that enable operators to execute the diverse and varied tasks that each engagement requires. Cobalt Strike provides post-exploitation capabilities through its Beacon payload and malleable C2 framework, while OST is a curated set of offensive security tools that covers the full attack chain with emphasis on evasion techniques.

While both platforms operate as sophisticated standalone solutions, OST was developed to work in tandem with Cobalt Strike, extending the reach of both tools and enabling enhanced capabilities during operations.

Coordinating Red Teaming Tools for Advanced Engagements

Cobalt Strike's highly flexible command and control directly integrates with OST's end-to-end toolset through Beacon Object Files (BOFs) and reflective DLL loading techniques, adding functionality like:

- **Session Management:** Operators can leverage session passing between platforms, enabling seamless transitions between OST's initial access tools and Cobalt Strike's post-exploitation framework.
- **Centralized Testing Environment:** The combined architecture enables advanced post-exploitation tasks while maintaining operational security through tested and validated tool interactions.
- **Cohesive Portfolio:** Organizations improve efficiency not only with solution interoperability and centralization, but also by having a single point of contact for support of their offensive security strategy.

Evasive Red Teaming: Technical Use Cases

Combining OST and Cobalt Strike enables red teams to run advanced attack simulations designed to bypass defensive measures and detection tools with ease.

- **Advanced Payload Operations:** OST's Payload Generator enhances Cobalt Strike's capabilities with additional anti-forensic features and evasion techniques for improved OPSEC during operations.
- **Covert Initial Access:** Outflank C2, staying under the radar of antivirus and EDR software during the initial access phase, enables operators to use session passing to quietly transition to Cobalt Strike for post-exploitation activities.
- **Enhanced Movement:** ShovelNG, a lateral movement toolkit for remote code execution, incorporates specialized techniques for moving undetected throughout the targeted environment and is easily integrated into Cobalt Strike using BOFs.
- **Full System Access:** Hidden Desktop, which enables a full, non-intrusive take over the desktop of a target user (including use of applications and hardware tokens), can be covertly deployed through Cobalt Strike with a custom implementation of "Hidden VNC."
- **Extended Capabilities:** OST 's collection of BOF capabilities for extending Cobalt Strike includes Kerberos interaction, novel coercion techniques, O365 token extraction, and more.

ADDITIONAL PRODUCT FEATURES

Empowering Operators with Cobalt Strike

Cobalt Strike enables security professionals to simulate the tactics and techniques of a long-term embedded attacker in an IT environment. Features include:

- **Versatile Post-Exploitation:** Beacon, Cobalt Strike's signature payload, can be deployed to quickly expand access and maintain persistence by completing tasks like gathering information, executing commands, and deploying additional payloads.
- **Flexible Framework:** The malleable C2 framework allows operators to tailor engagements to suit each unique environment through C2 profiles, UDRLs, sleep mask kit, mutator kit, and more.
- **Community-Driven Extensions:** The Community Kit provides a curated repository of over 100 user-developed extensions, including custom BOFs, aggressor scripts, and post-exploitation modules.

Prioritizing Stealth with OST

OST is a toolkit for red teamers by red teamers, built for performing in mature and sensitive target environments to efficiently simulate techniques currently used by APTs and other cyber attackers.

- **Attack Chain Coverage:** Innovative research and a rapid development pace ensures operators are using cutting edge techniques, with over 30 purpose-built tools for initial access, lateral movement, privilege escalation, and exfiltration phases.
- **Unique Evasion Tactics:** OST tools prioritize advanced anti-forensic techniques and EDR bypass capabilities, including unpublished techniques to avoid detection.
- **Advanced Tradecraft Education:** Exclusive technical deep dives cover OFFSEC topics including EDR evasion methodologies, Windows Kernel Driver manipulation, Azure AD attack vectors through ROADtools, and Office Security.

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.