FORTRA™

DATASHEET (OFFENSIVE SECURITY)

Red Team Bundle – Cobalt Strike and Outflank Security Tooling (OST)

Cobalt Strike and Outflank Security Tooling (OST) are two elite red teaming solutions ideal for assessing the security posture of an organization by deploying sophisticated adversary simulations.

Cobalt Strike is a threat emulation tool that provides a post-exploitation agent and covert channels, replicating the tactics and techniques of an advanced adversary in a network. OST is a curated set of offensive security tools that covers every step in the attacker kill chain. Though both solutions work well independently, OST was developed to work in tandem with Cobalt Strike, extending its reach and empowering red team operators for increased efficiency.

Cobalt Strike and OST can be bundled together for a reduced price, enabling organizations to benefit from red teaming tools that seamlessly integrate with one another. This overview provides details on the key functionalities of each of these solutions and how they can be used together to amplify your red teaming efforts.

Cobalt Strike

Cobalt Strike enables security professionals to simulate the tactics and techniques of a stealthy long-term embedded attacker in an IT environment. Red teams can launch targeted attacks using Beacon, Cobalt Strike's post-exploitation payload, which can execute PowerShell scripts, log keystrokes, take screenshots, download files, and spawn other payloads.

Additionally, Cobalt Strike has a malleable command and control framework that can be modified with custom scripts, adjustable attack kits, and the Community Kit with user-created extensions. For example, new post-exploitation features can be added through the creation of a Beacon Object File (BOF), a compiled C program that can be executed within a Beacon process and use internal Beacon APIs.

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. OST's toolkit has coverage for every aspect of an engagement, with tools for initial breach, lateral movements, privilege escalation, achieving persistence, and final exfiltration.

OST tools specialize in evasion, helping red teamers stay under the radar. For example, tools like Payload Generator deploy anti-forensic features to help evade antivirus and EDR solutions. OST tools also utilize techniques that have not yet been published or weaponized by solutions or services.

Cobalt Strike and OST

Cobalt Strike was built to be a highly flexible command and control framework that could be easily extended, tailoring it to meet the needs of any engagement. OST was created with Cobalt Strike's adaptability in mind, with end-to-end tools which can be used within Cobalt Strike out of the box. OST integrates directly with Cobalt Strike's framework through BOFs and reflective DLL loading techniques. With a mature C2 framework and expertly developed and tested tools, the Red Team Bundle is an OPSEC safe way to efficiently perform highly technical and difficult post-exploitation tasks.

Having multiple tools from Fortra's large portfolio of cybersecurity solutions matures risk management without increasing headcount. 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 portfolio.

Evasive Red Teaming: 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. Outflank's expert red teamers regularly develop new tooling for OST to ensure it is keeping up with attack methodology being seen in the wild.

The following use cases provide how users can take advantage of the Red Team Bundle:

- **Payload Generator** – Payload generator is used for creating stealthy payloads equipped with anti-forensics and other obfuscation methods for tasks like phishing, privilege escalation, or lateral movements. Users with the Red Team Bundle can generate Cobalt Strike payloads with Payload Generator of a multitude of output formats such as exe, cpl, xll, that are enriched with strong evasive techniques, anti-forensics, and make use of strong process migration techniques, custom Sleep Masks and anti-forensics.
- **Stage 1** – Stage 1 is a lightweight C2 framework focused on OPSEC safety and is ideal for performing reconnaissance and gaining an initial foothold while staying under the radar of antivirus and EDR software. Session passing capabilities enable users to begin an engagement in Stage 1 and quietly transition to Cobalt Strike for post-exploitation activities.
- **Lateral Pack: ShovelNG** – ShovelNG is a lateral movement toolkit for remote code execution that incorporates specialized techniques for moving undetected throughout the targeted environment. Implemented through BOFs, this tool is easily integrated into Cobalt Strike.
- **Hidden Desktop** – Hidden Desktop enables a full, non-intrusive take over the desktop of a target user, including use of applications and hardware tokens. This custom implementation of "Hidden VNC" can be deployed through Cobalt Strike, all without the user knowing what is happening.
- **Beacon Object File Collection** – OST offers multiple BOF capabilities for extending Cobalt Strike, including Kerberos interaction, novel coercion techniques, O365 token extraction, and more.

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.