DATASHEET (Outflank-OST)

OST - Outflank Security Tooling

OST is a curated set of offensive security tools created by expert red teamers. Ideal for advanced security teams testing even mature and sensitive target environments, this toolkit covers every significant step in the attacker kill chain, from difficult stages such as initial access to final exfiltration.

Prioritizing Stealth and Evasion

One of the key challenges that red teams face today is staying undetected. OST tools specialize in staying under the radar and are explicitly developed to assist in bypass defensive measures and detection tools. For example, tools like **Sharpfuscator** utilize obfuscation to compile C# repositories, while **Payload Generator** deploys anti-forensic features to help evade antivirus and EDR solutions. Ongoing research and development of evasive measures give OST users access to capabilities not yet published or weaponized by any other solutions or services.

A Multi-Phase Approach

With OST, security teams will have multiple tools for every stage of an engagement. For instance, initial access can be accomplished with the **Office Intrusion Pack**, which uses high quality offensive macros for phishing with MS Office documents or can hide payloads in pictures using steganography with **Stego Loader**.

Once a successful breach has been achieved, teams can deploy a stealthy C2 implant with **Stage 1 C2** to make an informed decision before increasing their footprint and start full C2 frameworks such as Cobalt Strike. They can move laterally using non-public techniques within the environment using tools like the **Lateral Pack**, extract credentials with Credential Pack, or escalate privileges with **DLL Hijack Library**. Post-exploitation actions can be performed with tools like **HiddenDesktop**, which grants interaction on a target desktop including client applications, active cookies of the target user and connected hardware tokens, all without leaving any indicators of a red teamer's presence. OST also features tools that can provide support throughout the engagement, like **BlueCheck**, which monitors and sends alerts of Blue Team activities.

PRODUCT SUMMARY

KEY FEATURES

- A broad set of tools for red teams
- Focus on antivirus and EDR evasion
- Integrations with other red teaming solutions
- Tools for every phase of the attack chain
- Full documentation within application portal
- Access to the private OST Slack community

Technical Specifications

- Cloud delivered platform
- Web browser interface
- Locally downloaded payloads

Building a More Resilient IT Environment

OST allows you to increase efficiency without adding to your headcount. By leveraging an external toolkit developed and verified by red teaming experts, even small teams can safely run top to bottom engagements with ease.

Our seasoned team of security professionals constantly research the current cybersecurity landscape to continuously enhance OST with the latest offensive techniques. With regular updates and extensive documentation, security teams can stay up-to-date and one step ahead of attackers. Additionally, users have access to a private Slack community monitored by OST developers for support and knowledge sharing with other users.

Integrations With Other Fortra Solutions

OST was developed to work in tandem to work with Fortra's advanced adversary simulation tool, Cobalt Strike. Those with both Cobalt Strike and OST can take advantage of features that extend the reach of these two tools to further enhance testing efforts. For example, users can integrate directly with Cobalt Strike's framework through Beacon Object Files (BOFs) and reflective DLL loading techniques. Additionally, Cobalt Strike users can enrich the evasiveness of their payloads using **Payload Generator's** obfuscation methods.

OST is also compatible with Fortra's automated penetration testing solution, Core Impact. Just as with Cobalt Strike, Core Impact users can take advantage of OST's **Payload Generator** to increase the evasiveness of their payloads. Additionally, OST's **Fake Ransom** complements Core Impact's ransomware simulator, enhancing its authenticity to better test incident response.

An Evolving Toolkit

OST regularly adds new tools to provide the most effective solution possible. A sample of the current tooling includes:

- **KerberosAsk** - Perform Kerberos actions from a Beacon Object File (BOF) using a custom ASN.1 decoding implementation
- **Payload Generator** - Create advanced payloads that enhance antivirus evasion and detection strategies using anti-forensic features
- **SharpFuscator** - Custom .Net obfuscator to make use of the many public red teaming tools written in .Net
- **Hidden Desktop** - Covertly interact with a target's desktop including fat client applications without impacting their user experience
- **Fake Ransom** - Simulate an authentic ransomware attack with a ransom notice that takes over the screen, displaying file listings on the target machine
- **Stage 1** - OPSEC focused C2 framework that allows for basic task and safe recon to determine strategy prior to deploying other C2 frameworks
- **Office Intrusion Pack** - Create powerful VBA macro's for your MS Office phishing documents
- **Lateral Pack** - Move laterally with specialized techniques intended for staying under the radar
- **Stego Loader** - Deploy steganography to deftly conceal payloads in images
- **Language Panda** - Change language forensics within a document to make it appear as if it was created using an Office installation from another country

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.