

## User-driven Web Drive-by Attacks

Archived: 2026-05-03 02:09:34 UTC

Cobalt Strike makes several tools to setup web drive-by attacks available to you. To quickly start an attack, navigate to **Attacks** and choose one of the following option:

### Java Signed Applet Attack

This attack starts a web server hosting a self-signed Java applet. Visitors are asked to give the applet permission to run. When a visitor grants this permission, you gain access to their system.

The Java Signed Applet Attack uses Cobalt Strike's Java injector. On Windows, the Java injector will inject shellcode for a Windows listener directly into memory for you.

Navigate to **Attacks** -> **Signed Applet Attack**.

**figure 45** - Signed Applet Attack



**Local URL/Host/Path** - Set the Local URL Path, Host and Port to configure the webserver.

**Listener** - Press the ... button to select a Cobalt Strike listener you would like to output a payload for.

**SSL** - Check to serve this content over SSL. This option is available when you specify a [valid SSL certificate](#) in your Malleable C2 profile.

Press **Launch** to start the attack.

### Java Smart Applet Attack

Cobalt Strike's Smart Applet Attack combines several exploits to disable the Java security sandbox into one package. This attack starts a web server hosting a Java applet. Initially, this applet runs in Java's security sandbox and it does not require user approval to start.

The applet analyzes its environment and decides which Java exploit to use. If the Java version is vulnerable, the applet will disable the security sandbox, and execute a payload using Cobalt Strike's Java injector.

Navigate to **Attacks** -> **Smart Applet Attack**.

**figure 46** - Smart Applet Attack



**Local URL/Host/Path** - Set the Local URL Path, Host and Port to configure the webserver.

**Listener** - Press the ... button to select a Cobalt Strike listener you would like to output a payload for.

**SSL** - Check to serve this content over SSL. This option is available when you specify a [valid SSL certificate](#) in your Malleable C2 profile.

Press **Launch** to start the attack.

## Scripted Web Delivery (S)

This feature generates a stageless Beacon payload artifact, hosts it on Cobalt Strike's web server, and presents a one-liner to download and run the artifact.

Navigate to **Attacks** -> **Scripted Web Delivery (S)** from the menu.

**figure 47** - Scripted Web Delivery (S)



**Local URL/Host/Path** - Set the Local URL Path, Host and Port to configure the webserver. Make sure the **Host** field matches the CN field of your SSL certificate. This will avoid a situation where this feature fails because of a mismatch between these fields.

**Listener** - Press the ... button to select a Cobalt Strike listener you would like to output a payload for.

**Type** - Use the drop-down menu to select one of the following types:

**bitsadmin** : This option hosts an executable and uses bitsadmin to download it. The bitsadmin method runs the executable via cmd.exe.

**exe** : This option generates an executable and hosts it on Cobalt Strike's web server.

**powershell** This option hosts a PowerShell script and uses powershell.exe to download the script and evaluate it.

**powershell IEX** : This option hosts a PowerShell script and uses powershell.exe to download the script and evaluate it. Similar to prior **powershell** option, but it provides a shorter Invoke-Execution one-liner command.

**python** : This option hosts a Python script and uses python.exe to download the script and run it. Each of these options is a different way to run a Cobalt Strike listener.

**x64** - Check the box to generate an x64 stager for the selected listener.

**SSL** - Check to serve this content over SSL. This option is available when you specify a [valid SSL certificate](#) in your Malleable C2 profile.

Press **Launch** to start the attack.

---

Source: <https://www.cobaltstrike.com/help-scripted-web-delivery>