User-driven Web Drive-by Attacks

Archived: 2026-04-06 01:20:03 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

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

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 - Scrpted Web Delivery (S)

Press **Launch** to start the attack.
