


# Learn Pipe Fitting for all of your Offense Projects

---

 [blog.cobaltstrike.com/2021/02/09/learn-pipe-fitting-for-all-of-your-offense-projects/](https://blog.cobaltstrike.com/2021/02/09/learn-pipe-fitting-for-all-of-your-offense-projects/)

Raphael Mudge

February 9, 2021



Named pipes are a method of inter-process communication in Windows. They're used primarily for local processes to communicate with each other. They can also facilitate communication between two processes on separate hosts. This traffic is encapsulated in the Microsoft SMB Protocol. If you ever hear someone refer to a named pipe transport as an SMB channel, this is why.

Cobalt Strike uses named pipes in several of its features. In this post, I'll walk you through where Cobalt Strike uses named pipes, what the default pipename is, and how to change it. I'll also share some tips to avoid named pipes in your Cobalt Strike attack chain too.

## Where does Cobalt Strike use named pipes?

---

Cobalt Strike's default Artifact Kit EXEs and DLLs use named pipes to launder shellcode in a way that defeats antivirus binary emulation circa 2014. It's still the default. When you see `\\.\pipe\MSSE-###-server` that's likely the default Cobalt Strike Artifact Kit binaries. You can change this via the Artifact Kit. Look at `src-common/bypass-pipe.c` in the Artifact Kit to see the implementation.

Cobalt Strike also uses named pipes for its payload staging in the jump `psexec_psh` module for lateral movement. This pipename is `\\.\pipe\status_##`. You can change the pipe via Malleable C2 (set `pipename_stager`).

Cobalt Strike uses named pipes in its SMB Beacon communication. The product has had this feature since 2013. It's pretty cool. You can change the pipename via your profile and when you configure an SMB Beacon payload. I'm also aware of a few detections that target the content of the SMB Beacon feature too. The SMB Beacon uses a `[length][data]` pattern and

these IOCs target predictable [length] values at the beginning of the traffic. The [smb\\_frame\\_header](#) Malleable C2 option pushes back on this. The default pipe is `\\[target]\pipe\msagent_##`.

Cobalt Strike uses named pipes for its [SSH sessions](#) to chain to a parent Beacon. The SSH client in Cobalt Strike is essentially an SMB Beacon as far as Cobalt Strike is concerned. You can change the pipename (as of 4.2) by setting `ssh_pipename` in your profile. The default name of this pipe (CS 4.2 and later) is `\\.pipe\postex_ssh_####`.

Cobalt Strike uses named pipes for most of its [post-exploitation jobs](#). We use named pipes for post-ex tools that inject into an explicit process (screenshot, keylog). Our fork&run tools largely use named pipes to communicate results back to Beacon too. F-Secure's [Detecting Cobalt Strike Default Modules via Named Pipe Analysis](#) discusses this aspect of Cobalt Strike's named pipes. We introduced the ability to change these pipenames in Cobalt Strike 4.2. Set `post-ex -> pipename` in your [Malleable C2 profile](#). The default name for these pipes is `\\.pipe\postex_####` in Cobalt Strike 4.2 and later. Prior to 4.2, the default name was random-ish.

## Pipe Fitting with Cobalt Strike

---

With the above, you're now armed with knowledge of where Cobalt Strike uses named pipes. You're also empowered to change their default names too. If you're looking for a candidate pipename, use `ls \.pipe` from Beacon to quickly see a list of named pipes on a lived-in Windows system. This will give you plenty to choose from. Also, when you set your plausible pipe names, be aware that each `#` character is replaced with a random character (0-9a-f) as well. And, one last tip: you can specify a comma-separated list of candidate pipe names in your `ssh_pipename` and `post-ex -> pipename` profile values. Cobalt Strike will pick from this list, at random, when one of these values is needed.

## Simplify your Offense Plumbing

---

Cobalt Strike uses named pipes in several parts of its offense chain. These are largely optional though and you can avoid them with some care. For example, the default Artifact Kit uses named pipes; but this is not a requirement of the Artifact Kit. Our other Artifact Kit templates do not use named pipes. For lateral movement and [peer-to-peer chaining](#) of Beacons, the [TCP Beacon](#) is an option. To avoid named pipes from our SSH sessions, tunnel an external SSH client via a [SOCKS proxy pivot](#). And, while a lot of our fork&run post-exploitation DLLs use named pipes for results, [Beacon Object Files](#) are another way to [build and run post-exploitation tools](#) on top of Beacon. The Beacon Object Files mechanism does not use named pipes.

## Closing Thoughts

---

This post focused on named pipe names, but the concepts here apply to the rest of Cobalt Strike as well. In offense, knowing your IOCs and how to change or avoid them is key to success. Our goal with Cobalt Strike isn't amazing and ever-changing default pipe names or IOCs. Our goal is flexibility. Our current and future work is to give you more control over your attack chain over time. To know today's options, read [Kits, Profiles, and Scripts... Oh my!](#) This blog post summarizes ways to customize Cobalt Strike. Our late-2019 [Red Team Operations with Cobalt Strike](#) mixes these ideas into each lecture as well.

---

## **Interested in Trying Cobalt Strike?**

---

**[REQUEST A QUOTE](#)**

---