Cobalt Strike 3.8 – Who's Your Daddy?

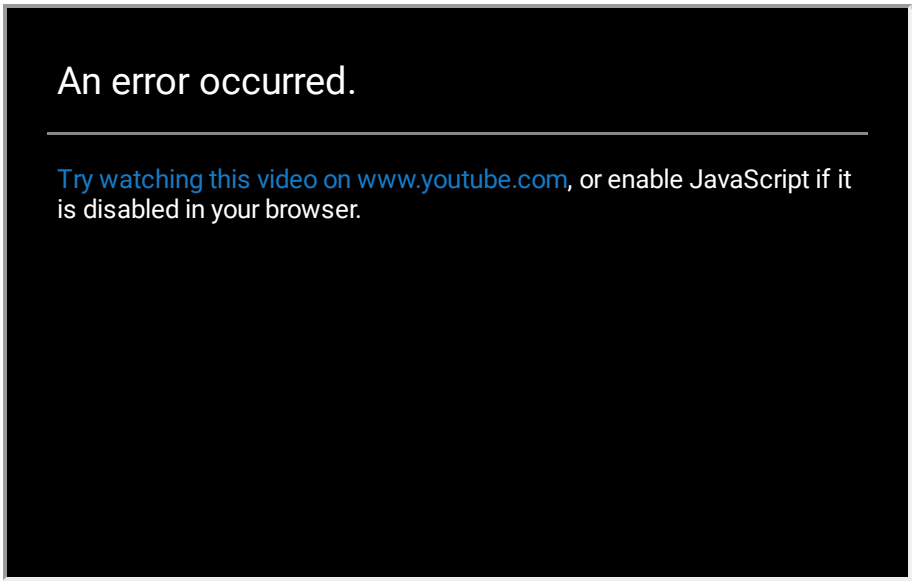
Published: 2017-05-23 · Archived: 2026-04-29 02:10:06 UTC

Cobalt Strike 3.8 is now available. This release adds features to spawn processes with an alternate parent process. This release also gives the operator control over the script templates Cobalt Strike uses in its attacks and workflows.

Processes with Alternate Parents

A favorite hunt technique is to instrument a host to report all new processes, their arguments, and the parent process. Hunt operators (and automated solutions) separate the noise from the interesting by looking for odd parent/child process relationships.

This release of Cobalt Strike pushes back on this technique with the **ppid** command. The PPID command tasks Beacon to launch cmd.exe, powershell.exe, and other processes with an alternate parent. This feature takes advantage of an API, introduced with Windows Vista, to enable consent.exe to launch elevated processes with the non-elevated requester as the parent.



This opens a lot of possibilities. For example, if I'm in a user context, I might set explorer.exe as my parent with something plausible (e.g, iexplore.exe) for my temporary processes. If I'm in a SYSTEM context, I might use services.exe as my parent process and ask Beacon to use svchost.exe for its temporary processes.

To benefit from the ppid command, your session must have rights to access the parent process. I also recommend that you specify a parent process that exists in the same desktop session. If you don't, random commands and workflows may fail.

Another way to hop Desktop Sessions

It's possible, with a few extra steps, to run commands under a parent that lives in another desktop session. Programs run this way will take on the rights and identity of their parent.

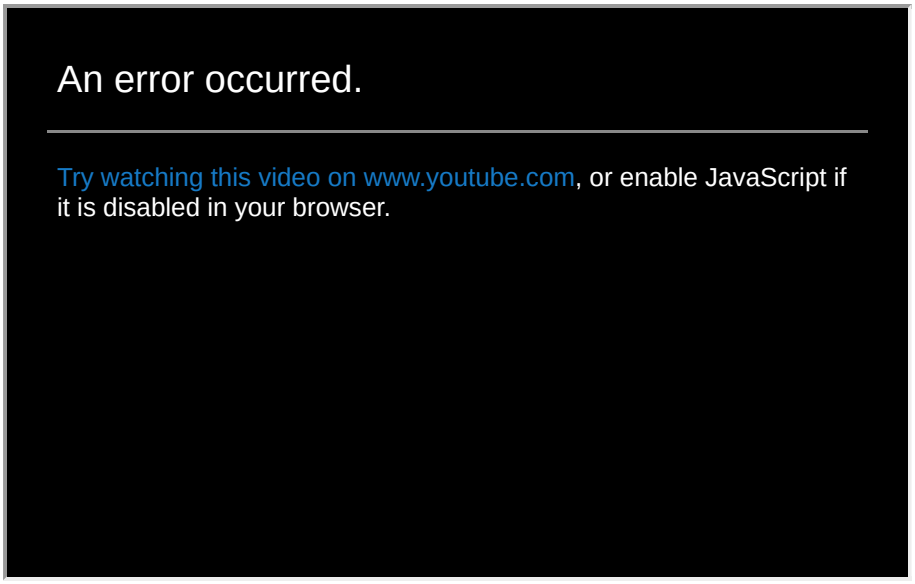
Beacon's **runu** command runs an arbitrary command as a child of another parent. This command takes the necessary extra steps to do this across session boundaries.
The **spawnu** command builds on this primitive to spawn a session with powershell.exe.

These commands offer means to spawn a payload, in another desktop session, without remote process injection. As detection of remote process injection becomes more common, it's important to have other ways to achieve our goals without this offensive technique.

The Resource Kit

Cobalt Strike 3.8's Resource Kit finally gives you a way to change Cobalt Strike's built-in script templates! The Resource Kit is a collection of Cobalt Strike's default script templates and a sample Aggressor Script to bring these into Cobalt Strike. Go to **Help** -> **Arsenal** from a licensed copy of Cobalt Strike to download the Resource Kit.

The Resource Kit benefits from new Aggressor Script hooks to provide the PowerShell, Python, and VBA script templates Cobalt Strike uses in its workflows.



Check out the release notes to see a full list of what's new in Cobalt Strike 3.8. Licensed users may use the update program to get the latest. A 21-day Cobalt Strike trial is also available.
