

Schritt 0: Ausgangszustand des Hauptspeichers.

Header	Header	Belegt	Frei	Frei	Frei	Belegt	Frei
--------	--------	--------	------	------	------	--------	------

Schritt 1: Pool-Grooming führt zu Headerblöcken im Hauptspeicher.

Header Header	Belegt	Hole-Connection	Frei	Belegt	Frei
---------------	--------	-----------------	------	--------	------

Schritt 2: Die Hole-Connection belegt einen Bereich im Hauptspeicher.

Header Header Belegt	Hole-Connection	Header	Belegt	Header
----------------------	-----------------	--------	--------	--------

Schritt 3: Zweites Pool-Grooming erstellt zusätzliche Headerblöcke.

Header Header	Belegt F	Frei Frei	Header	Belegt	Header
---------------	----------	-----------	--------	--------	--------

Schritt 4: Abbruch der Hole-Connection führt zu freiem Speicherplatz.

Header F	Header Belegt	Datenpaket	Header	Belegt	Header
----------	---------------	------------	--------	--------	--------

Schritt 5: Ein Umgewandeltes Datenpaket wird im erzeugten freien Speicher abgelegt. Es folgt ein Buffer-Overflow in den anliegenden Header.