

 [Product](#) [Solutions](#) [Resources](#) [Open Source](#) [Enterprise](#) [Pricing](#) [Sign in](#) [Sign up](#)

 [logangoins](#) / [Krueger](#) Public

[Notifications](#) [Fork 38](#) [Star 343](#)

[Code](#) [Issues](#) [Pull requests](#) [Actions](#) [Projects](#) [Security](#) [Insights](#)

main     Code

 <b>HullaBrian</b> Update yara_rule.yar to reduce false positives 8a89a11 · 2 months ago  <b>52 Commits</b>
 Detections Update yara_rule.yar to reduce false po... 2 months ago
 Krueger Code cleanup 3 months ago
 .gitignore Initial project structure 4 months ago
 Krueger.sln Added initial solution 4 months ago
 LICENSE Initial commit 4 months ago
 README.md Update README.md 3 months ago

## Description

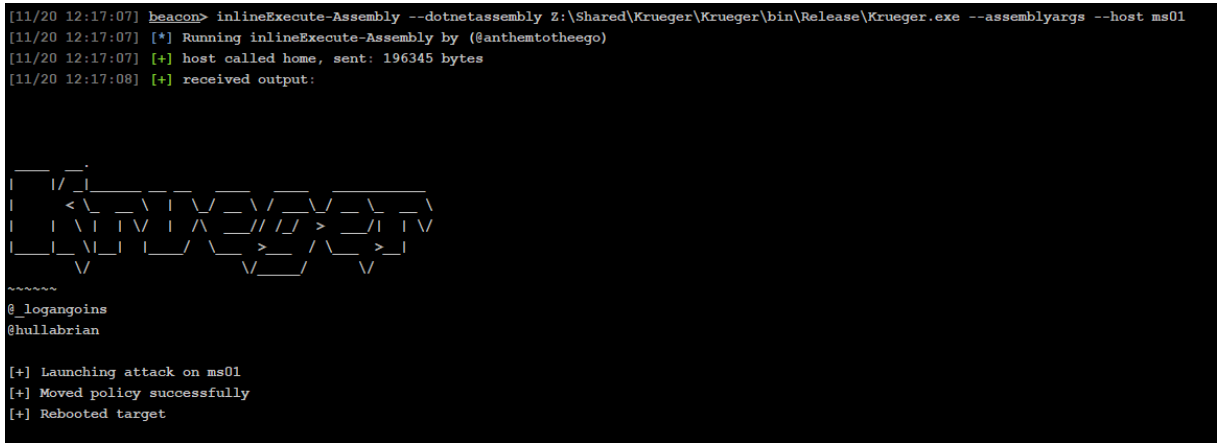
Krueger is a Proof of Concept (PoC) .NET post-exploitation tool for remotely killing Endpoint Detection and Response (EDR) as apart of lateral movement procedures. Krueger accomplishes this task by utilizing Windows Defender Application Control (WDAC), which is a built in Microsoft created application control utility that has the

-  [README](#)    [GPL-3.0 license](#)

a WDAC policy to disk and perform a remote reboot, preventing the EDR service from starting on boot.

Krueger can also be run from memory using tools such as `execute-assembly` and `inlineExecute-Assembly` ([@anthemtotheego](#)). Additionally, to prevent the need to load a WDAC policy from disk while executing Krueger from memory, Krueger includes an embedded WDAC policy inside of the .NET assembly inserted at compile time which can be read from memory and written to a target at runtime.

More information about this technique can be found on our blog at:  
<https://beierle.win/2024-12-19-Weaponizing-WDAC-Killing-the-Dreams-of-EDR/>



## About

## Proof of Concept (PoC) .NET tool for remotely killing EDR with WDAC

-  Readme
-  GPL-3.0 license
-  Activity
-  343 stars
-  3 watching
-  38 forks

## Report repository

## Releases

No releases published

## Packages

No packages published

## Contributors 2

-  **logangoins** Logan Goins

 **HullaBrian** Jonathan Beierle

## Languages



