

Open in app ↗

Sign up Sign in

Medium Search

Write 

Shimcache Flush!



BlueteamOps · Follow
1 min read · May 27, 2020



Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

Rundll32.exe apphelp.dll,ShimFlushCache - Works with Windows Vista onwards for endpoints and Windows Server 2008 onwards for servers.

Rundll32.exe kernel32.dll,BaseFlushAppcompatCache - Works with Windows XP onwards for endpoints and Windows Server 2003 onwards for servers.

How to detect this?

These command executions should not occur during BAU operations (I've only seen the 2nd command in use during IT troubleshooting, but it is a rare occurrence). Endpoint Detection & Response agent telemetry OR command

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app



Written by **BlueteamOps**

81 Followers

Janantha Marasinghe's Research

Follow

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app