Shimcache Flush!

BlueteamOps · Follow
1 min read · May 27, 2020

```
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 occurence). Endpoint Detection & Response agent telemetry OR command

Written by BlueteamOps

81 Followers

Janantha Marasinghe's Research

Follow