

Open in app 

Sign up

Sign in

Medium

 Search

 Write



L0LBin — Execution via Diskshadow



Harjot Shah Singh · Follow

2 min read · Aug 30, 2023

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

```
diskshadow
```

For script mode, type the following, where script.txt is a script file containing Diskshadow commands:

```
diskshadow -s script.txt
```

Medium

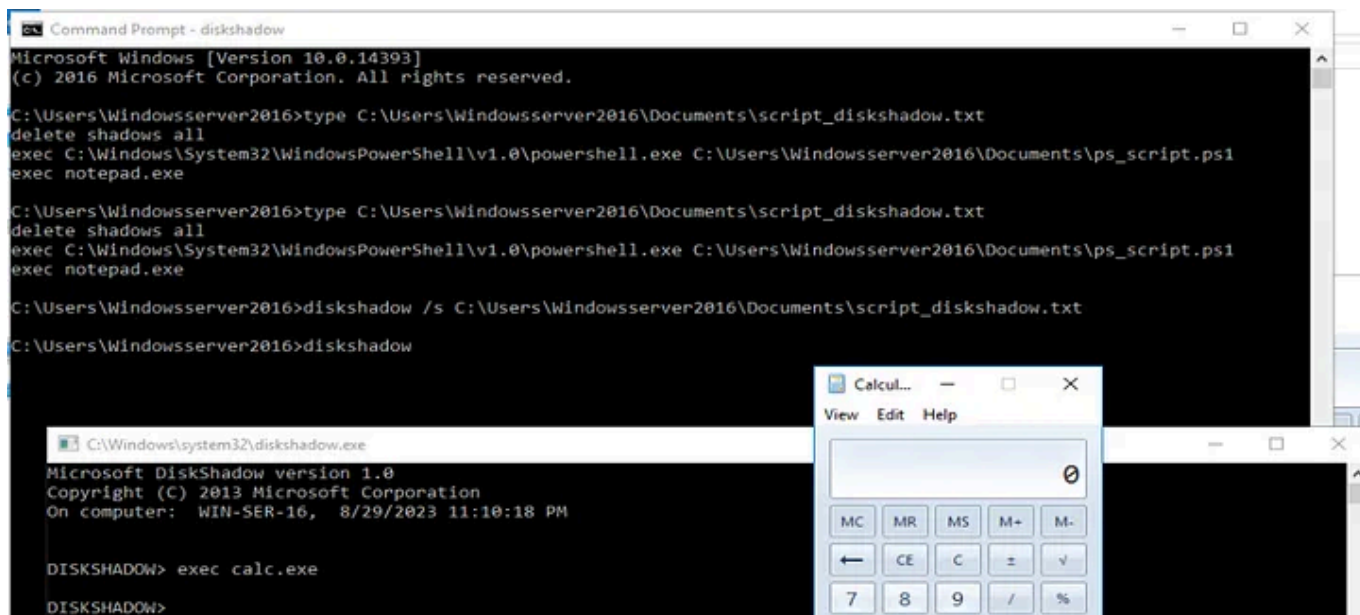
Sign up to discover human stories that deepen your understanding of the world.

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



Medium

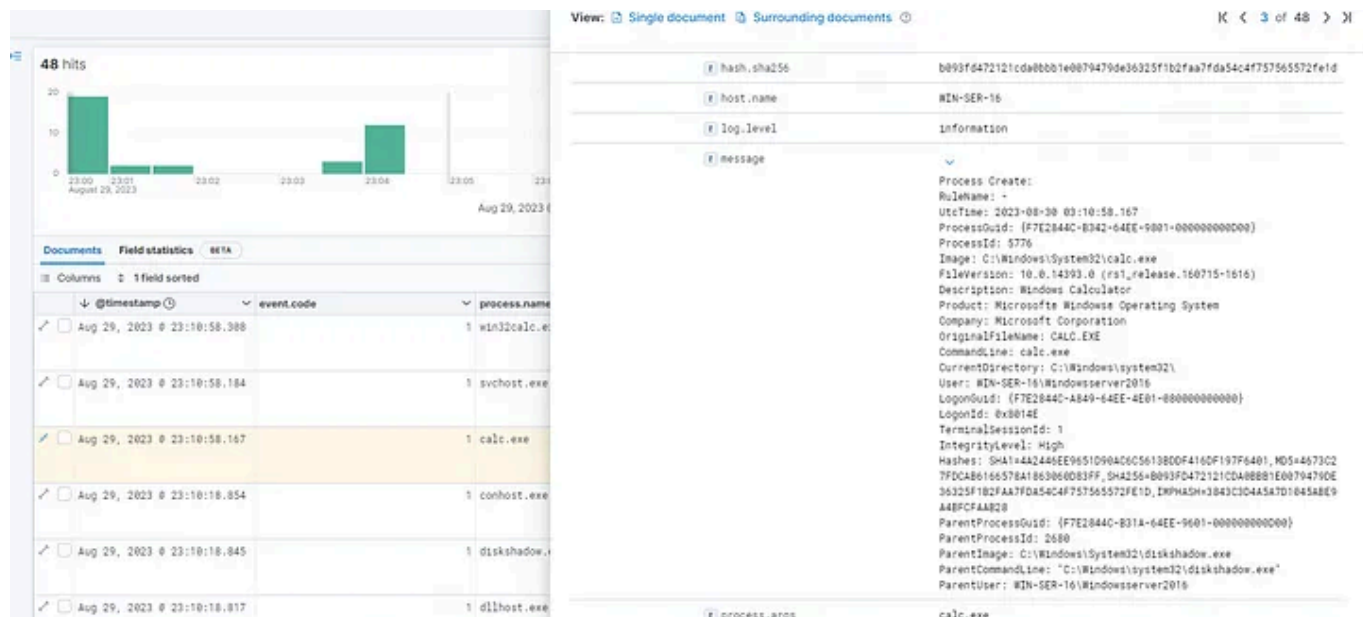
Sign up to discover human stories that deepen your understanding of the world.

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



Medium

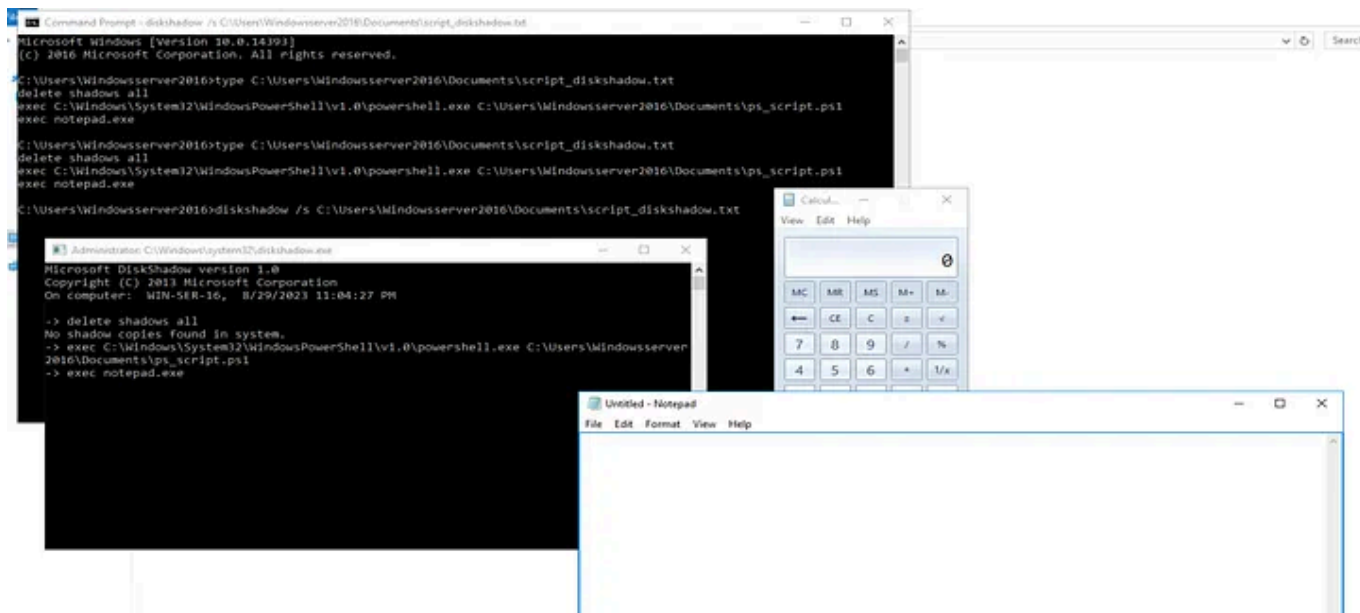
Sign up to discover human stories that deepen your understanding of the world.

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



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

Process creation ([DS0009](#)): We can monitor for the child processes of Diskshadow to suspicious binary execution

```
Kibana Query: event.code: 1 AND ParentImage: *\diskshadow.exe
```

Command Execution ([DS0017](#)): We can also monitor for command-line to check if the diskshadow is executed in scriptable mode

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

DiskShadow: The Return of VSS Evasion, Persistence, and Active Directory Database Extraction

Source: blog.microsoft.com] Introduction Not long ago, I blogged about Vshadow: Abusing the Volume Shadow Service for...

bohops.com

```
and decrypted: 3a46a38ab1f50f483fd0d7d7697844f9
Decrypting hashes from ntfs.dit
ad3b435b51404eead3b435b51404ee:7644c618486283b490c28c3c590492
435b51404eead3b435b51404ee:3106c7f6d16a931b73c56d76c089e0c
43b435b51404eead3b435b51404ee:8f03f0e135a55f1134146a07782a4
43b51404eead3b435b51404ee:c76b3d259452197c540f4ad62a11982a
3b435b51404eead3b435b51404ee:598323278b380536320757220921b
4435b51404eead3b435b51404ee:492865740f33553899c5513c307730b
43b435b51404eead3b435b51404ee:4c74bc8c85acab82c578c3661709bcf
3b435b51404eead3b435b51404ee:0f5246c376f7b0dc23c233c4c68f706a
3b435b51404eead3b435b51404ee:60895092f764bdc1895f3874558a6eb
3b435b51404eead3b435b51404ee:80b3bac3a94fba54f1188a755c38c4951
1aad3b435b51404eead3b435b51404ee:0896a6572668a3864790d7916c8
3211aad3b435b51404eead3b435b51404ee:35c4d986200ad3b4a7396c78
3b435b51404eead3b435b51404ee:080af700f0a753e781320c6e9a9f713
43b435b51404eead3b435b51404ee:2f6b48427b5a0c76e97f4a97874738
43b435b51404eead3b435b51404ee:b6477b447460bdf78608b032cfc1c8
ad3b435b51404eead3b435b51404ee:080372a7f61f3093009783706e0a97
43b435b51404eead3b435b51404ee:8a2b0c51f2aec18025a3226047cccb
43b435b51404eead3b435b51404ee:51398908e2960a32735ab813930532
3b435b51404eead3b435b51404ee:67f6d024271625272c30f640896648
3b435b51404eead3b435b51404ee:c5348015c7ede417e960b9420b484ac
ad3b435b51404eead3b435b51404ee:c29f62a4562c1089799220474
435b51404eead3b435b51404ee:784ade7ee050ee7fa5231169a82c4a91
3b435b51404eead3b435b51404ee:3733967cecd14e382f8624fba2af87e
3b435b51404eead3b435b51404ee:0532e959102382f5394065064e4c022
435b51404eead3b435b51404ee:7082831473b710846a2e7547283343171
```

Windows Diskshadow Proxy Execution

System Binary Proxy Execution

research.splunk.com

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 Harjot Shah Singh

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