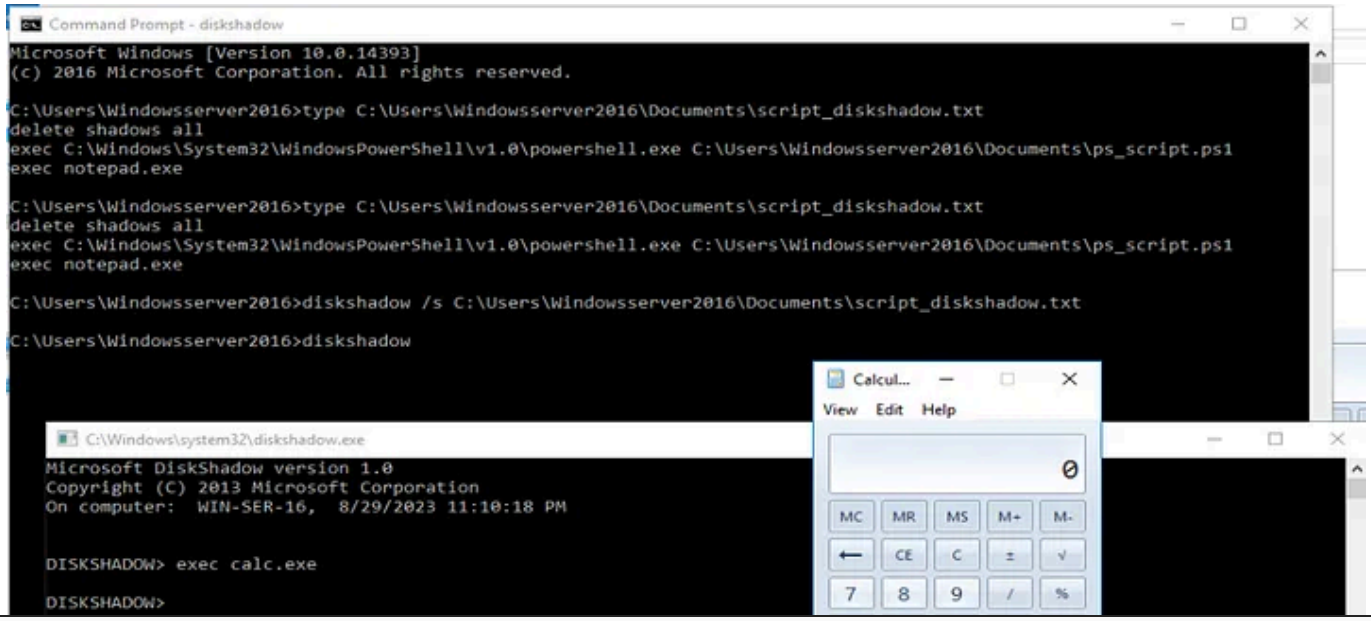
LOLBin — Execution via Diskshadow

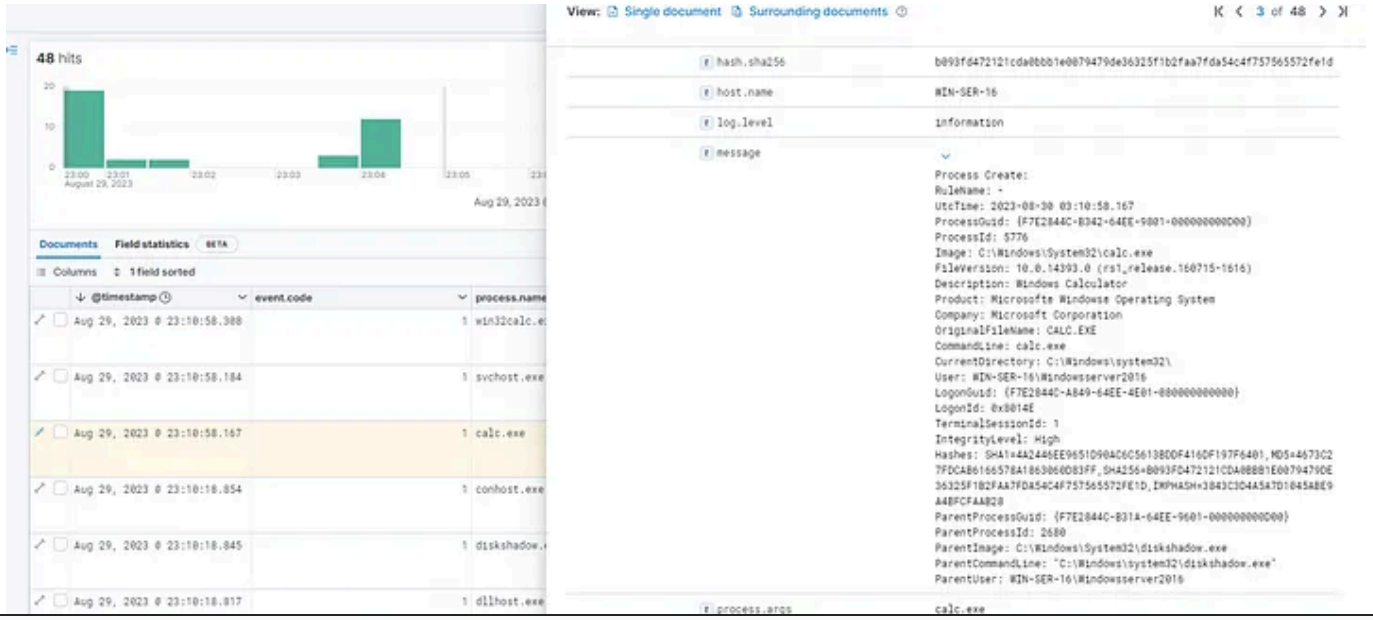
Harjot Shah Singh · Follow
2 min read · Aug 30, 2023

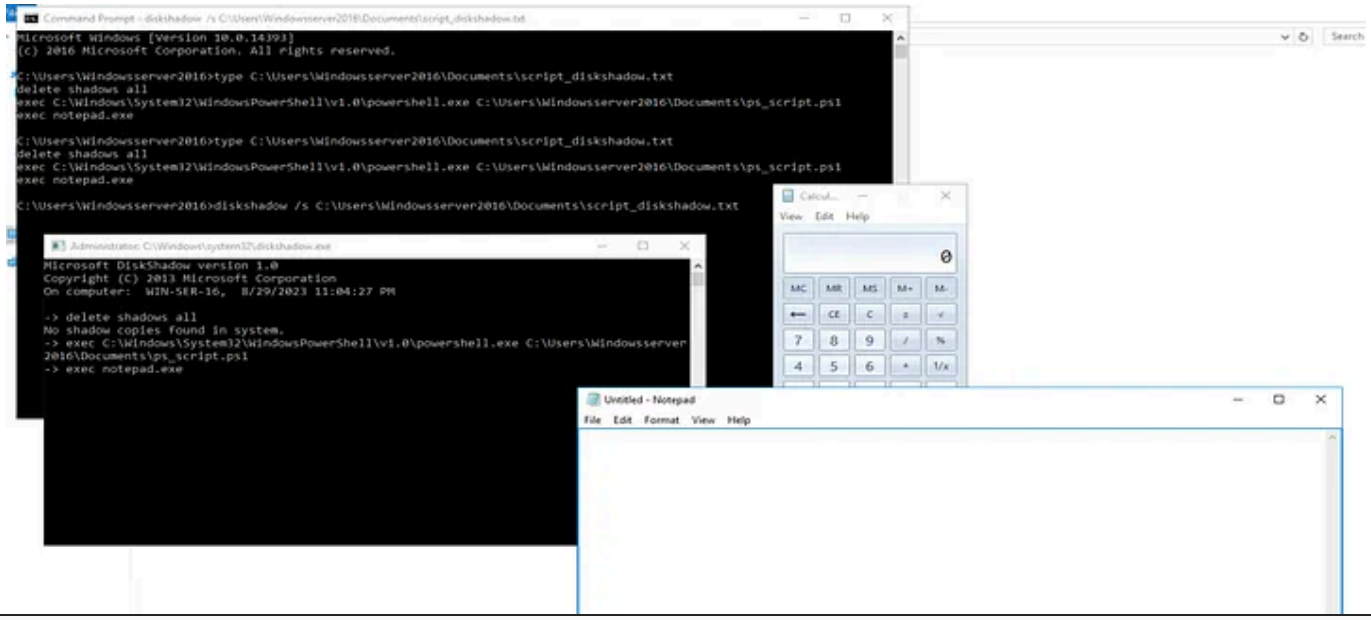
```
diskshadow
```

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

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







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

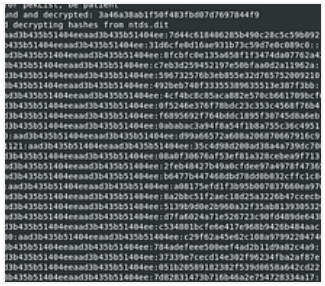
```
Kibana Query: event.code: 1 AND ParentImage: *\diskshadow.exe
```

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

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



Windows Diskshadow Proxy Execution

System Binary Proxy Execution

research.splunk.com

Written by Harjot Shah Singh

Follow