DeleteShadowCopies

LICENSE

README.md

README MIT license

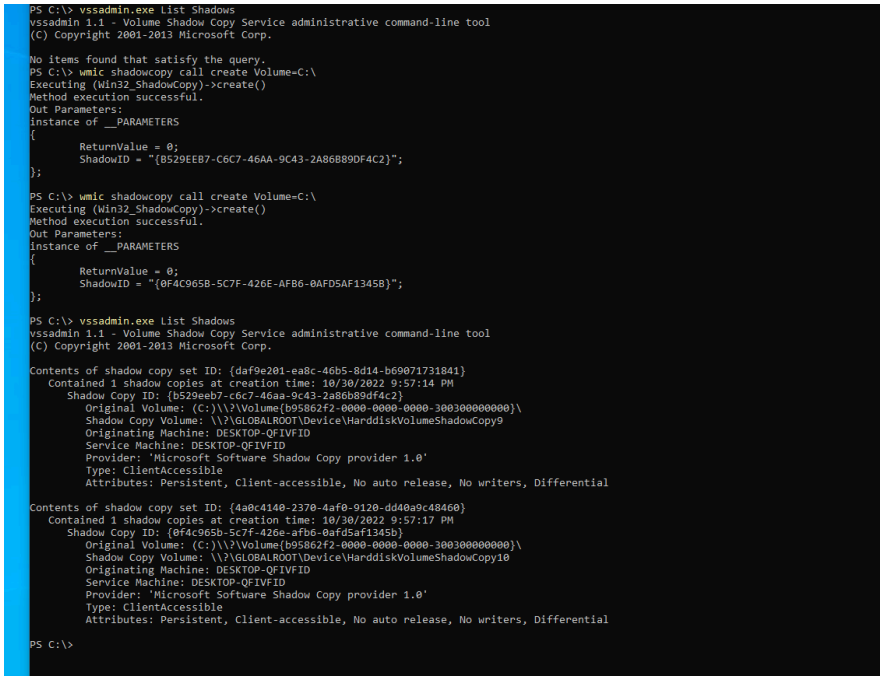
DeleteShadowCopies: Deleting Shadow Copies In Pure C++

After Looking at some of the leaked ransomware code, i noticed that (at least for the samples i've seen), that the ransomware is using wmic or vssadmin via command line to delete shadow copies, so out of curiosity i had to look for something else, and thus this repo (so im not helping ransomware authers) ...

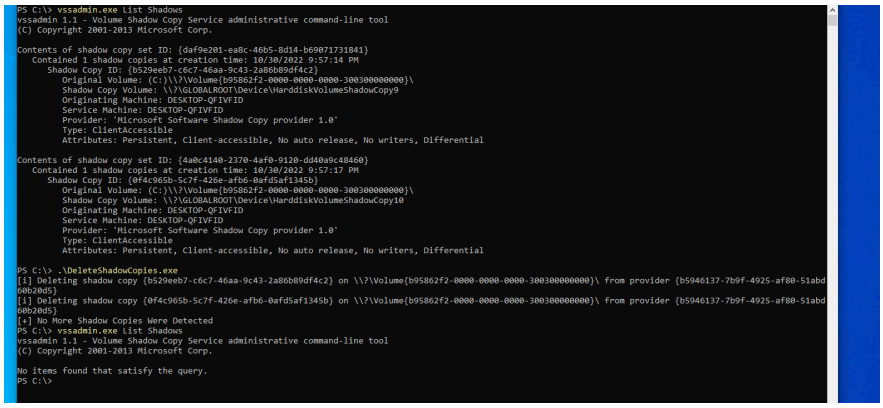
```
Example:
  - conti: wmic shadowcopy where "ID='{XXXXXXXX
```

```
    - babuk: vssadmin delete shadows /all /quiet
```

Demo (Creating):



Demo (Deleting):



Based On vshadow