

Sign in

NUL0x4C / DeleteShadowCopies

Public

Notifications

Fork24

Star113

<>Code

Issues

Pull requests

Actions

Projects

Security

Insights

main

Go to file

<>Code

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='{XXXXXXXXX

About

Deleting Shadow Copies In Pure C++

Readme

MIT license

Activity

113 stars

3 watching

24 forks

Report repository

Releases

No releases published

Packages

No packages published

Languages

C++100.0%

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

Demo (Creating):

```
PS C:\> vssadmin.exe List Shadows
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2013 Microsoft Corp.

No items found that satisfy the query.
PS C:\> wmic shadowcopy call create Volume=C:\
Executing (Win32_ShadowCopy)->create()
Method execution successful.
Out Parameters:
Instance of __PARAMETERS
{
    ReturnValue = 0;
    ShadowID = "{B529EEB7-C6C7-46AA-9C43-2A86B89DF4C2}";
};

PS C:\> wmic shadowcopy call create Volume=C:\
Executing (Win32_ShadowCopy)->create()
Method execution successful.
Out Parameters:
Instance of __PARAMETERS
{
    ReturnValue = 0;
    ShadowID = "{0F4C965B-5C7F-426E-AFB6-0AFD5AF1345B}";
};

PS C:\> vssadmin.exe List Shadows
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2013 Microsoft Corp.

Contents of shadow copy set ID: {daf9e281-ea8c-46b5-8d14-b69071731841}
  Contained 1 shadow copies at creation time: 10/30/2022 9:57:14 PM
    Shadow Copy ID: {b529eeb7-c6c7-46aa-9c43-2a86b89df4c2}
      Original Volume: (C:\)\Volume{b95862f2-0000-0000-0000-300300000000}\
      Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy9
      Originating Machine: DESKTOP-QFIVFID
      Service Machine: DESKTOP-QFIVFID
      Provider: 'Microsoft Software Shadow Copy provider 1.0'
      Type: ClientAccessible
      Attributes: Persistent, Client-accessible, No auto release, No writers, Differential

Contents of shadow copy set ID: {4a0c4140-2370-4af0-9120-dd40a9c48460}
  Contained 1 shadow copies at creation time: 10/30/2022 9:57:17 PM
    Shadow Copy ID: {0F4C965B-5C7F-426E-AFB6-0AFD5AF1345B}
      Original Volume: (C:\)\Volume{b95862f2-0000-0000-0000-300300000000}\
      Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy10
      Originating Machine: DESKTOP-QFIVFID
      Service Machine: DESKTOP-QFIVFID
      Provider: 'Microsoft Software Shadow Copy provider 1.0'
      Type: ClientAccessible
      Attributes: Persistent, Client-accessible, No auto release, No writers, Differential

PS C:\>
```

Demo (Deleting):

```
PS C:\> vssadmin.exe List Shadows
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2013 Microsoft Corp.

Contents of shadow copy set ID: {daf9e281-ea8c-46b5-8d14-b69071731841}
  Contained 1 shadow copies at creation time: 10/30/2022 9:57:14 PM
    Shadow Copy ID: {b529eeb7-c6c7-46aa-9c43-2a86b89df4c2}
      Original Volume: (C:\)\Volume{b95862f2-0000-0000-0000-300300000000}\
      Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy9
      Originating Machine: DESKTOP-QFIVFID
      Service Machine: DESKTOP-QFIVFID
      Provider: 'Microsoft Software Shadow Copy provider 1.0'
      Type: ClientAccessible
      Attributes: Persistent, Client-accessible, No auto release, No writers, Differential

Contents of shadow copy set ID: {4a0c4140-2370-4af0-9120-dd40a9c48460}
  Contained 1 shadow copies at creation time: 10/30/2022 9:57:17 PM
    Shadow Copy ID: {0F4C965B-5C7F-426E-AFB6-0AFD5AF1345B}
      Original Volume: (C:\)\Volume{b95862f2-0000-0000-0000-300300000000}\
      Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy10
      Originating Machine: DESKTOP-QFIVFID
      Service Machine: DESKTOP-QFIVFID
      Provider: 'Microsoft Software Shadow Copy provider 1.0'
      Type: ClientAccessible
      Attributes: Persistent, Client-accessible, No auto release, No writers, Differential

PS C:\> .\DeleteShadowCopies.exe
[!] Deleting shadow copy {b529eeb7-c6c7-46aa-9c43-2a86b89df4c2} on \\?\Volume{b95862f2-0000-0000-0000-300300000000}\ from provider {b5946137-7b0f-4925-af80-51ab060200d5}
[!] Deleting shadow copy {0F4C965B-5C7F-426E-AFB6-0AFD5AF1345B} on \\?\Volume{b95862f2-0000-0000-0000-300300000000}\ from provider {b5946137-7b0f-4925-af80-51ab060200d5}
[+] No More Shadow Copies Were Detected
PS C:\> vssadmin.exe List Shadows
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2013 Microsoft Corp.

No items found that satisfy the query.
PS C:\>
```

Based On [vshadow](#)

[Terms](#) [Privacy](#) [Security](#) [Status](#) [Docs](#) [Contact](#) [Manage cookies](#) [Do not share my personal information](#)

