

Files

2cc01b0

Go to file

>

.github

>

Archive-Old-Version

>

Logo

>

yml

>

HonorableMentions

>

OSBinaries

Addinutil.yml

AppInstaller.yml

Aspnet_Compiler.yml

At.yml

Atbroker.yml

Bash.yml

Bitsadmin.yml

Certoc.yml

Certreq.yml

Certutil.yml

Cmd.yml

Cmdkey.yml

Cmdl32.yml

Cmstp.yml

Colorcpl.yml

ConfigSecurityPolicy.yml

Conhost.yml

Control.yml

Csc.yml

Cscript.yml

CustomShellHost.yml

DataSvcUtil.yml

Desktopimgdownldr.yml

DeviceCredentialDeployment.y...

Dfsvc.yml

Diantz.yml

Diskshadow.yml


Dnscmd.yml

Esentutl.yml

Eventvwr.yml

LOLBAS / yml / OSBinaries / Wbadmin.yml

...


 LetMeFeastyOnYourYeasty and wietze

Create wbadmin...

...

 ✓
 fc23c99 · 7 months ago
 History

Code

Blame

26 lines (26 loc) · 1.31 KB

Raw

Copy


Download


Diff


```


1      ---
2      Name: wbadmin.exe
3      Description: Windows Backup Administration utility
4      Author: Chris Eastwood
5      Created: 2024-04-05
6      Commands:
7          - Command: wbadmin start backup -backupTarget:C:\temp\ -include:C:\Windows\NTDS\NTDS.
8            Description: Extract NTDS.dit and SYSTEM hive into backup virtual hard drive file (
9            Usecase: Snapshotting of Active Directory NTDS.dit database
10           Category: Dump
11           Privileges: Administrator, Backup Operators, SeBackupPrivilege
12           MitreID: T1003.003
13           OperatingSystem: Windows Server
14          - Command: wbadmin start recovery -version:<VERSIONIDENTIFIER> -recoverytarget:C:\tem
15            Description: Restore a version of NTDS.dit and SYSTEM hive into file path. The comm
16            Usecase: Dumping of Active Directory NTDS.dit database
17            Category: Dump
18            Privileges: Administrator, Backup Operators, SeBackupPrivilege
19            MitreID: T1003.003
20            OperatingSystem: Windows Server
21      Full_Path:
22          - Path: C:\Windows\System32\wbadmin.exe
23      Detection:
24          - IOC: wbadmin.exe command lines containing "NTDS" or "NTDS.dit"
25      Resources:
26          - Link: https://medium.com/r3d-buck3t/windows-privesc-with-sebackupprivilege-65d2cd1e


```


 Expand.yml

 Explorer.yml

 Extexport.yml

 Extrac32.yml

 Findstr.yml

 Finger.yml