

**Description:** This project aims to showcase how an attacker uses C2 commands to delete shadow files as part of a ransomware attack. It also covers how a SOC analyst can detect this attack and prevent it by writing a new rule. Additionally, in this project, the new rule will be tested to demonstrate its effectiveness and explain why an attacker would attempt to delete shadow files.

**Software and tools I use:** Vmware Workstation Pro, Windows 11(victim), Sliver Command (Offensive tool), LimaCharlie.

**Project:** First, I will start from the attacker's point of view by demonstrating how to delete shadow files from a victim's computer. To initiate the attack, I will use C2 commands to access the victim's terminal. I will not show the entire C2 command process because I have already covered it in the 'C2 Payloads Detection' project. I will begin by typing 'shell' into my Sliver C2 shell.

```
[server] sliver (BROAD_REPLICATION) > shell
? This action is bad OPSEC, are you an adult? Yes
[*] Wait approximately 10 seconds after exit, and press <enter> to continue
[*] Opening shell tunnel (EOF to exit) ...
[*] Started remote shell with pid 6692
PS C:\Windows\system32>
```

I will have access to the victim's Windows terminal. To delete shadow files, I will type '**vssadmin delete shadows /all**'. When the attacker encrypts the victim's files, they delete all the shadow files so that the victim cannot recover their files. As a result, the victim has only one option, which is to pay the ransom.

```
PS C:\Windows\system32> vssadmin delete shadows /all
vssadmin delete shadows /all
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:\Windows\system32>
```

I will go to LimaCharlie's detection tab to check for any signs of shadow file deletion.

```
You're up-to-date!

2024-08-18 03:43:32 Shadow Copies Deletion Using Operating Systems Utilities shouky.localdomain {"event":{"COMMAND_LINE":"C:\\Windows\\system32\\vssadmin.e
2024-08-18 03:18:52 Non Interactive PowerShell Process Spawned shouky.localdomain {"event":{"BASE_ADDRESS":140697656885248,"COMMAND_LINE":"C:\\Windows\\Syste
2024-08-18 03:18:52 HackTool - Sliver C2 Implant Activity Pattern shouky.localdomain {"event":{"BASE_ADDRESS":140697656885248,"COMMAND_LINE":"C:\\Windows\\Sy
2024-08-18 03:10:17 LSASS access shouky.localdomain {"event":{"EVENTS":[{"event":{"BASE_ADDRESS":140695338156032,"COMMAND_LINE":"C:\\Windows\\system32\\lsass
2024-08-18 02:54:38 LSASS access shouky.localdomain {"event":{"EVENTS":[{"event":{"BASE_ADDRESS":140695338156032,"COMMAND_LINE":"C:\\Windows\\system32\\lsass
2024-08-18 02:11:58 Non Interactive PowerShell Process Spawned shouky.localdomain {"event":{"BASE_ADDRESS":140697656885248,"COMMAND_LINE":"C:\\Windows\\Sys
```

I can see the ‘shadow Copies Deletion’ at the top. That SOC analyst will see when the attacker deleted shadow files. To stop that from happening anymore, I have to create a rule. I will click ‘shadow Copies Deletion’.

03c9ed0b-33dc-4fd6-a176-a1fc66c16de6

Category

Shadow Copies Deletion Using Operating Systems Utilities

Time

2024-08-18 03:43:32

Source

shouky.localdomain

View Event Timeline

Mark False Positive

~"detection": {  
 "author": "\_ext-sigma-7a14fbc3-54d9-4b4d-8700-61eddada04f0[bulk][segment]"  
 "cat": "Shadow Copies Deletion Using Operating Systems Utilities"  
 ~"detect": {  
 ~"event": {  
 "COMMAND\_LINE": "C:\\Windows\\system32\\vssadmin.exe" delete shadows /all"  
 "FILE\_IS\_SIGNED": 1  
 "FILE\_PATH": "C:\\Windows\\system32\\vssadmin.exe"  
 "HASH": "39d1bca6060207c9f8d9f3eea060428f250f4aa542c6aac6e66da24464dfc10f"  
 ~"PARENT": {  
 "BASE\_ADDRESS": 140697656885248  
 "COMMAND LINE":

I will click ‘View Event Timeline’ and then click ‘Build D&R Rule’.

```
IE": "C:\\Windows\\system32\\vssadmin.exe delete shadows /all"
"FILE_IS_SIGNED": 1
"FILE_PATH": "C:\\Windows\\system32\\vssadmin.exe"
"HASH": "39d1bca6060207c9f8d9f3eea060428f250f4aa542c6aac6e66da24464dfc10f"
"BASE_ADDRESS": 140697656885248
"COMMAND_LINE": "C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe -NoExit -Command [Console]::OutPutEncoding=[Text.UTF8Encoding]::UTF8"
"FILE_IS_SIGNED": 1
"FILE_PATH": "C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe"
"HASH": "c50057756cdb25d481cf2502abcef124f864c27618c5057468bfc6b82b2c4edd"
"MEMORY_USAGE": 65650688
"PARENT_ATOM": "3007854989e024327045d1b466c15f7a"
"PARENT_PROCESS_ID": 2172
"PROCESS_ID": 6692
"THIS_ATOM": "3f1bbf720a7841c0094f975966c1681d"
"THREADS": 16
"TIMESTAMP": 1723951132572
"USER_NAME": "shouky\\comed"
"PARENT_PROCESS_ID": 6692
"PROCESS_ID": 3852
```

In the Respond section, I will type:

- action: report  
name: vss\_deletion\_kill\_it
- action: task  
command:
  - deny\_tree
  - <<routing/parent>>

Detect

1

event: NEW\_PROCESS

2

op: and

3

rules:

4

- op: is

5

path: event/FILE\_PATH

6

value: C:\Windows\system32\vssadmin.exe

7

- op: is

8

path: event/COMMAND\_LINE

9

value: '"C:\Windows\system32\vssadmin.exe" delete shadows /all'

10

- op: is

11

path: routing/hostname

12

value: shouky.localdomain

13

Expand

Respond

1

- action: report

2

name: vss\_deletion\_kill\_it

3

- action: task

4

command:

5

- deny\_tree

6

- <<routing/parent>>

Comment

Add comment here. Comments are not included in detection content when an alert is triggered.

Save Rule

Delete Rule

The “action: report” section to send a detection report to the “Detections” tab. The “action: task” section to kill the parent process with the deny tree for ‘vssadmin delete shadows /all’ command. I will save the rule as ‘vss\_deletion\_kill\_it’.

Now I will try if the rule is working or not. I will go back to the attacker's terminal and type 'vssadmin delete shadows /all'.

```
PS C:\Windows\system32> vssadmin delete shadows /all
vssadmin delete shadows /all
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:\Windows\system32> vssadmin delete shadows /all
vssadmin delete shadows /all
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:\Windows\system32> █
```

To fully test the rule's functionality, I will type 'whoami'.

```
PS C:\Windows\system32> whoami
Shell exited
```

```
[server] sliver (BROAD_REPLICATION) > █
```

The system shell failed to return from the 'whoami' command because the parent process was terminated because of the rule I created. That is one of the rules for stopping the deletion of shadow files.