





[Sign in](#)

 **OTRF** / **detection-hackathon-apt29** Public

 Notifications

 Fork **41**

 Star **132**

[Code](#)

[Issues](#) **49**

[Pull requests](#)

[Actions](#)

[Projects](#)

[Security](#)

[Insights](#)

3.C) Modify Registry #7

[New issue](#)[Open](#)

Cyb3rWard0g opened this issue on May 2, 2020 · 1 comment



Cyb3rWard0g commented on May 2, 2020

[Contributor](#)

Description

Finally, the attacker removes artifacts of the privilege escalation from the Registry (T1112).

```
[pupy (PowerShell)] > Remove-Item -Path HKCU:\Soft  
[pupy (PowerShell)] > exit  
[pupy (CMD)] > exit
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant



Cyb3rWard0g commented
on May 13, 2020

[Contributor](#)[Author](#)

3.C.1 Modify Registry

Procedure: Modified the Registry to remove artifacts of COM hijacking

Criteria: Deletion of of the
HKCU\Software\Classes\Folder\shell\Open\command subkey

Sysmon

```
SELECT Message
FROM apt29Host d
INNER JOIN (
    SELECT b.ProcessGuid
    FROM apt29Host b
    INNER JOIN (
        SELECT ProcessGuid
        FROM apt29Host
        WHERE Channel = "Microsoft-Windows-Sysmon/Operat
            AND EventID = 1
            AND LOWER(ParentImage) RLIKE '.*\\â€Ž|â€|â€ª
    ) a
    ON b.ParentProcessGuid = a.ProcessGuid
    WHERE b.Channel = "Microsoft-Windows-Sysmon/Operatic
        AND b.EventID = 1
    ) c
    ON d.ProcessGuid = c.ProcessGuid
WHERE d.Channel = "Microsoft-Windows-Sysmon/Operational"
    AND d.EventID = 12
    AND LOWER(d.TargetObject) RLIKE '.*\\\\\\\\\\\\\\\\folder\\\\\\\\\\\\
    AND d.Message RLIKE '.*EventType: DeleteKey.*'
```

Results

```
Registry object added or deleted:
RuleName: -
EventType: DeleteKey
UtcTime: 2020-05-02 02:59:15.911
ProcessGuid: {47ab858c-e1f8-5eac-bc03-000000000400}
ProcessId: 3832
Image: C:\windows\System32\WindowsPowerShell\v1.0\powershell.exe
TargetObject: HKU\S-1-5-21-1830255721-3727074217-2423397
```

[Sign up for free](#) to join this conversation on GitHub. Already have an account? [Sign in to comment](#)

