6.B) Private Keys #14

New issue

Open Cyb3rWard0g opened this issue on May 2, 2020 · 2 comments

Cyb3rWard0g commented on May 2, 2020 • edited Contributor ···

Description

The attacker then harvests private keys (T1145)

```
Steal PFX certificate:

[meterpreter (PowerShell)\*] > Get-PrivateKeys

[meterpreter (PowerShell)\*] > exit
```

Cyb3rWard0g changed the title ~~6.B) Private Keys, Credential Dumping~~ 6.B) Private Keys on May 2, 2020

Cyb3rWard0g commented on May 14, 2020 Contributor Author ···

6.B.1 Private Keys

Procedure: Exported a local certificate to a PFX file using PowerShell
Criteria: powershell.exe creating a certificate file exported from the system

Cyb3rWard0g commented on May 14, 2020 Contributor Author ···

Sysmon

```
SELECT Message
FROM apt29Host f
INNER JOIN (
    SELECT d.ProcessGuid
    FROM apt29Host d
    INNER JOIN (
      SELECT a.ProcessGuid, a.ParentProcessGuid
      FROM apt29Host a
      INNER JOIN (
        SELECT ProcessGuid
        FROM apt29Host
        WHERE Channel = "Microsoft-Windows-Sysmon/Operational"
            AND EventID = 1
            AND LOWER(Image) LIKE "%control.exe"
            AND LOWER(ParentImage) LIKE "%sdclt.exe"
      ) b
      ON a.ParentProcessGuid = b.ProcessGuid
      WHERE a.Channel = "Microsoft-Windows-Sysmon/Operational"
        AND a.EventID = 1
        AND a.IntegrityLevel = "High"
    ) c
    ON d.ParentProcessGuid= c.ProcessGuid
    WHERE d.Channel = "Microsoft-Windows-Sysmon/Operational"
      AND d.EventID = 1
```

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

1 participant

```
      AND d.Image LIKE '%powershell.exe'
) e
ON f.ProcessGuid = e.ProcessGuid
WHERE f.Channel = "Microsoft-Windows-Sysmon/Operational"
AND f.EventID = 11
AND LOWER(f.TargetFilename) LIKE "%.pfx"
```

Results

```
File created:
RuleName: -
UtcTime: 2020-05-02 03:04:57.460
ProcessGuid: {47ab858c-e23d-5eac-c603-000000000400}
ProcessId: 3876
Image: C:\windows\system32\WindowsPowerShell\v1.0\powershell.exe
TargetFilename: C:\Users\pbeesly\Downloads\coyn5igj.3io.pfx
CreationUtcTime: 2020-05-02 03:04:57.460
```