



Product ▾Solutions ▾Resources ▾Open Source ▾Enterprise ▾Pricing

🔍

Sign in

Sign up

📄

OTRF / **detection-hackathon-apt29**

Public

🔔 Notifications

🍴 Fork 41

★ Star 132

<> Code

🔴 Issues 49

🔗 Pull requests

🎬 Actions

📁 Projects

🛡 Security

📊 Insights

5.B) Registry Run Keys / Startup Folder #12

New issue

🔴 Open

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



Cyb3rWard0g commented on May 2, 2020

Contributor

⋮

Description

The attacker establishes persistent access to the victim by creating a malicious payload in the Windows Startup folder (T1060)



Cyb3rWard0g commented on May 14, 2020

Contributor

Author

⋮

5.B.1 Registry Run Keys / Startup Folder

Procedure: Created a LNK file (hostui.lnk) in the Startup folder that executes on login  
Criteria: powershell.exe creating the file hostui.lnk in the Startup folder



Cyb3rWard0g commented on May 14, 2020

Contributor

Author

⋮

Sysmon Logs

```
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
      AND d.Image LIKE '%powershell.exe'
  ) e
  ON f.ProcessGuid = e.ProcessGuid
WHERE f.Channel = "Microsoft-Windows-Sysmon/Operational"
  AND f.EventID = 11
  AND f.TargetFilename RLIKE '.*\\\\\\\\\\\\\\ProgramData\\\\\\\\\\\\\\\\Microsoft\\\\\\\\\\\\\\\\Win
```

Results

File created:  
RuleName: -

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

```
UtcTime: 2020-05-02 03:04:23.681
ProcessGuid: {47ab858c-e23d-5eac-c603-000000000400}
ProcessId: 3876
Image: C:\windows\system32\WindowsPowerShell\v1.0\powershell.exe
TargetFilename: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\host
CreationUtcTime: 2020-05-02 03:04:23.681
```

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

