Product Solutions Resources Open Source Enterprise Pricing Sign in Sign up

microsoft / **MSTIC-Sysmon** Public

Notifications Fork 27 Star 146

Code Issues 3 Pull requests 3 Actions Projects Security Insights

Files

f1477c0

Go to file

- linux
  - configs
    - _events
    - attack-based
      - collection
      - command_control
      - defense_evasion
      - discovery
      - execution
      - impact
      - lateral_movement
      - persistence
        - T1037_BootLogonInitScripts...
        - T1053.003_Cron_Activity.xml
        - T1136.001_CreateLocalAcco...
        - T1505.003_WebShell_SuspS...
        - T1543.002_CreateModSyste...
      - privilege_escalation
      - ConvertTo-MainConfig.ps1
      - README.md
      - Split-XmlConfig.ps1
      - collect-all.xml
      - main.xml
  - schemas
  - README.md
- windows
- .gitignore
- CODE_OF_CONDUCT.md
- LICENSE
- README.md
- SECURITY.md
- SUPPORT.md

MSTIC-Sysmon / linux / configs / attack-based / persistence / **T1053.003_Cron_Activity.xml**

Cyb3rWard0g tagged rules, updated README and scripts to split and ... 75e131c · 3 years ago **History**

Code Blame 35 lines (34 loc) · 1.55 KB Raw

```xml
<!--
  Created: 10/15/2021
  Modified: 10/17/2021

  Technique: Scheduled Task/Job: Cron
  Reference:
  - https://github.com/bfuzzy1/auditd-attack/blob/master/auditd-attack/auditd-attack.ru
  - https://attack.mitre.org/techniques/T1053/003/
-->
<Sysmon schemaversion="4.81">
  <EventFiltering>
    <RuleGroup name="" groupRelation="or">
      <ProcessCreate onmatch="include">
        <Rule name="TechniqueID=T1053.003,TechniqueName=Scheduled Task/Job: Cron" group
          <Image condition="end with">crontab</Image>
        </Rule>
      </ProcessCreate>
    </RuleGroup>
    <RuleGroup name="" groupRelation="or">
      <FileCreate onmatch="include">
        <Rule name="TechniqueID=T1053.003,TechniqueName=Scheduled Task/Job: Cron" group
          <TargetFilename condition="is">/etc/cron.allow</TargetFilename>
          <TargetFilename condition="is">/etc/cron.deny</TargetFilename>
          <TargetFilename condition="is">/etc/crontab</TargetFilename>
          <TargetFilename condition="begin with">/etc/cron.d/</TargetFilename>
          <TargetFilename condition="begin with">/etc/cron.daily/</TargetFilename>
          <TargetFilename condition="begin with">/etc/cron.hourly/</TargetFilename>
          <TargetFilename condition="begin with">/etc/cron.monthly/</TargetFilename>
          <TargetFilename condition="begin with">/etc/cron.weekly/</TargetFilename>
          <TargetFilename condition="begin with">/var/spool/cron/crontabs/</TargetFilen
        </Rule>
      </FileCreate>
    </RuleGroup>
  </EventFiltering>
</Sysmon>
```