Sign in

microsoft / **MSTIC-Sysmon** Public

Notifications | Fork 27 | Star 146

Code | Issues 3 | Pull requests 3 | Actions | Projects | Security | Insights

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

Cyb3rWard0g tagged rules, updated README and scripts to split and merge configs 75e131c · 3 years ago

35 lines (34 loc) · 1.55 KB

Code | Blame | 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.rules#L111-L12
  - 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" groupRelation="or
          <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" groupRelation="or
          <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/</TargetFilename>
        </Rule>
      </FileCreate>
    </RuleGroup>
  </EventFiltering>
</Sysmon>
```