

4.4.1.2

???????

- عملية الأصلية لمعمل الراسم لثم ، أعضاء البائى مئاوللل ءءاملل ءقءلل ءءاز (parent process path) طئاسولل او (arguments).
- ءاناب ءاناب ءعاوق نم ءىزملا لمشيل ءىوهلا ىلإ لوصولل ءاليلء مءء عىسول ءامءال.
 - Slack وOpera وThunderbird نم لكل ءىوهلا ىلإ لوصولل ءبقارم أضى نآل مءى وVivaldi وDiscord.
- ءىوهلا ىلإ لوصولل لمشيل أعضاء البائى مئاوللل مءء عىسول.

????????

- ءمرب ءهءاوو (agents) ءالءول نىب مءءءسملا ىءءرءلل قاطنلل ضرع لىلقء REST. ءاقىبءلل
- ضعب فى (Explorer) ءافلملا فشءسم فى (canaries) ىرانءلل روهظ ءلءشم ءالصإ مءقلال Windows Server ءاراءصإ
- ءءاهشلل ءقء ءارشؤمل ءىوهلا ىلإ لوصولل ءالءس ضعب ناءقل ءلءشم ءالصإ

???? ???? WHCP/WHQL

ءامءال مء

?????? MD5

```
service.exe    = e289ef44c5a1bca39d57861ff9d05bee
assistant.exe  = d8e83309372b43ffc70feaf2bd538f36
CCRRSecMon.sys (Windows10)    = db736330f5a690a2e828472a357ee6b6
CCRRSecMon.sys (Windows8)     = b9d644930fc52495229dc7f96ffea299
CCRRSecMon.sys (Windows7)     = 7b1ece332986dadfcc6463574fd16616
```

Revision #1

Created 2026-07-24 02:30:05 UTC by Dennis Underwood

Updated 2026-07-24 02:30:05 UTC by Dennis Underwood