





/Atbroker.exe

☆ Star

7,060

Execute

Helper binary for Assistive Technology (AT)

Paths:

C:\Windows\System32\Atbroker.exe
C:\Windows\SysWOW64\Atbroker.exe

Resources:

- <http://www.hexacorn.com/blog/2016/07/22/beyond-good-ol-run-key-part-42/>

Acknowledgements:

- Adam ([@hexacorn](#))

Detections:

- Sigma: [proc_creation_win_lolbin_susp_atbroker.yml](#)
- Sigma: [registry_event_susp_atbroker_change.yml](#)
- IOC: Changes to HKCU\Software\Microsoft\Windows NT\CurrentVersion\Accessibility\Configuration
- IOC: Changes to HKLM\Software\Microsoft\Windows NT\CurrentVersion\Accessibility\ATs
- IOC: Unknown AT starting C:\Windows\System32\ATBroker.exe /start malware

Execute

Start a registered Assistive Technology (AT).

```
ATBroker.exe /start malware
```

Use case:	Executes code defined in registry for a new AT. Modifications must be made to the system registry to either register or modify an existing Assistive Technology (AT) service entry.
Privileges required:	User
Operating systems:	Windows 8, Windows 8.1, Windows 10, Windows 11
ATT&CK® technique:	T1218: System Binary Proxy Execution