codewhitesec / **SysmonEnte** Public

Files

main

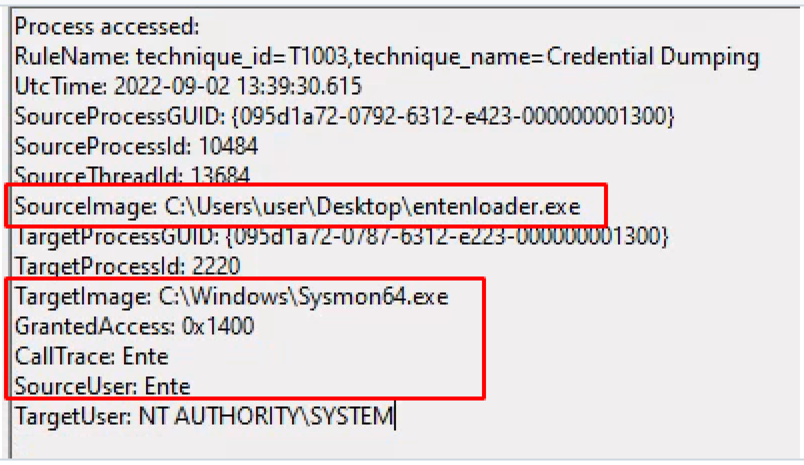
Go to file

- SACLProtect
- bin
- helpers
- screens
  - 1.png
- src
- DISCLAIMER.md
- Makefile
- Readme.md

SysmonEnte / screens / **1.png**

cwdel Initial Commit 4d317a8 · 2 years ago History

74.8 KB



```
Process accessed:
RuleName: technique_id=T1003,technique_name=Credential Dumping
UtcTime: 2022-09-02 13:39:30.615
SourceProcessGUID: {095d1a72-0792-6312-e423-000000001300}
SourceProcessId: 10484
SourceThreadId: 13684
SourceImage: C:\Users\user\Desktop\entenloader.exe
TargetProcessGUID: {095d1a72-0787-6312-e223-000000001300}
TargetProcessId: 2220
TargetImage: C:\Windows\Sysmon64.exe
GrantedAccess: 0x1400
CallTrace: Ente
SourceUser: Ente
TargetUser: NT AUTHORITY\SYSTEM
```