
Product ▼Solutions ▼Resources ▼Open Source ▼Enterprise ▼Pricing



Sign in

Sign up

 mdecrevoisier / EVTX-to-MITRE-Attack Public

 Notifications

 Fork 87

 Star 510

 Code


 Issues

 Pull requests


 Projects


 Security


 Insights


 Files


master





 Go to file


>  Antivirus


>  EVTX\_full\_APT\_attack\_steps


>  TA0001-Initial access


>  TA0002-Execution


>  TA0003-Persistence


>  TA0004-Privilege Escalation


>  TA0005-Defense Evasion


>  TA0006-Credential Access


>  TA0007-Discovery


 TA0008-Lateral Movement


>  T1021.001-Remote Desktop Pr...


>  T1021.002-SMB Windows Admi...


>  T1021.003-Distributed Compon...


 T1021.004-Remote Service SSH


 ID4-OpenSSH server listening....


 ID4103-4104-OpenSSH server...


 ID4103-4104-OpenSSH server...


>  T1021.006-Windows Remote M...


>  T1550-Use Alternate Authentic...


>  TA0009-Collection


>  TA0011-Command and Control


>  TA0040-Impact


 .gitignore





 LICENSE.md

 README.md

EVTX-to-MITRE-Attack / TA0008-Lateral Movement / T1021.004-Remote Service SSH / 



 History

Name	Last commit message	Last commit date
 ..		
 ID4-OpenSSH server listening.evtx		
 ID4103-4104-OpenSSH server act...		
 ID4103-4104-OpenSSH server ins...		

Page 1 of 2

