Product ▾Solutions ▾Resources ▾Open Source ▾Enterprise ▾Pricing

🔍

Sign in

Sign up

sbousseaden / EVTX-ATTACK-SAMPLES

Public

 Notifications

 Fork 398

 Star 2.2k

<> Code

🕒 Issues 4


🔗 Pull requests 1


🎬 Actions

📁 Projects

🛡 Security


📈 Insights


Files


44fbe85


🔍


🔍 Go to file


> .vscode


> AutomatedTestingTools


> Command and Control


DE_RDP_Tunnel_5156.evtx


DE_RDP_Tunneling_4624.evtx


DE_RDP_Tunneling_TerminalSer...


DE_sysmon-3-rdp-tun.evtx


Tunna_rdp_tunnel_IIS.log


bits_openvpn.evtx


cmds over dns txt queries and r...


readme.md


tunna_iis_rdp_smb_tunneling_sy...


web_attack_and_isp_webshell_lo...


> Credential Access


> Defense Evasion


> Discovery


> EVTX_ATT&CK_Metadata


> Execution


> Lateral Movement


> Other


> Persistence


> Privilege Escalation


.gitignore


AIEvent.jpg


EVTX_DataSet_Stats.PNG


Evtx-to-Xml.ps1


HeatMap.PNG


LICENSE.GPL


README.md


UACME_59_Sysmon.evtx


Winlogbeat-Bulk-Read.ps1


evtx_data.csv

mitre_evtx_repo_map.png

temp-plot.html

winlogbeat_example.yml



EVTX-ATTACK-SAMPLES / Command and Control / DE_RDP_Tunnel_5156.evtx 

History

Code

Blame

68 KB

Raw

[View raw](#)

