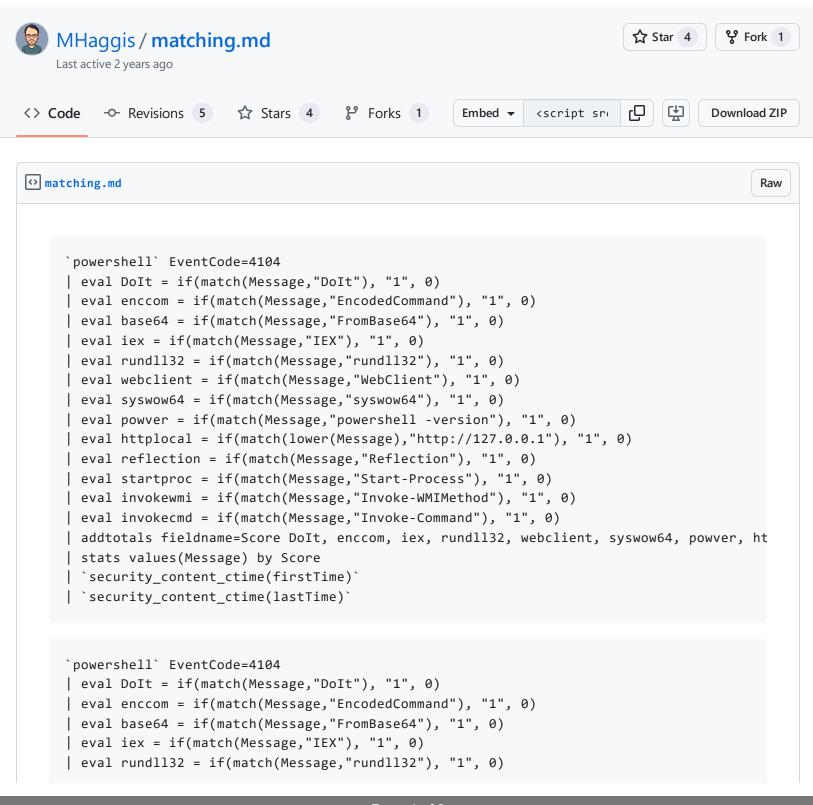
GitHub Gist Search... All gists Back to GitHub Sign in Sign up

Instantly share code, notes, and snippets.



```
| eval webclient = if(match(Message,"WebClient"), "1", 0)
| eval syswow64 = if(match(Message,"syswow64"), "1", 0)
| eval powver = if(match(Message,"powershell -version"), "1", 0)
| eval httplocal = if(match(lower(Message),"http://127.0.0.1"), "1", 0)
| eval reflection = if(match(Message,"Reflection"), "1", 0)
| eval startproc = if(match(Message,"Start-Process"), "1", 0)
| eval invokewmi = if(match(Message,"Invoke-WMIMethod"), "1", 0)
| eval invokecmd = if(match(Message,"Invoke-Command"), "1", 0)
| addtotals fieldname=Score DoIt, enccom, iex, rundll32, webclient, syswow64, powver, httpl
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
```

lower all

```
`powershell` EventCode=4104
| eval DoIt = if(match(lower(Message), "doit"), "1", 0)
| eval enccom = if(match(lower(Message), "encodedcommand"), "1", 0)
| eval base64 = if(match(lower(Message), "frombase64"), "1", 0)
| eval iex = if(match(lower(Message), "iex"), "1", 0)
eval rundll32 = if(match(lower(Message), "rundll32"), "1", 0)
| eval webclient = if(match(lower(Message), "webclient"), "1", 0)
| eval syswow64 = if(match(lower(Message), "syswow64"), "1", 0)
| eval powver = if(match(lower(Message), "powershell -version"), "1", 0)
eval httplocal = if(match(lower(Message), "http://127.0.0.1"), "1", 0)
| eval reflection = if(match(lower(Message),"reflection"), "1", 0)
| eval startproc = if(match(lower(Message), "start-process"), "1", 0)
| eval invokewmi = if(match(lower(Message), "invoke-wmimethod"), "1", 0)
| eval invokecmd = if(match(lower(Message), "invoke-command"), "1", 0)
addtotals fieldname=Score DoIt, enccom, iex, rundll32, webclient, syswow64, powver, ht
stats values(Score) by DoIt, enccom, iex, rundll32, webclient, syswow64, powver, httpl
`security content ctime(firstTime)`
| `security_content_ctime(lastTime)`
```

Latest

```
`powershell` EventCode=4104
| eval DoIt = if(match(lower(Message), "doit"), "1", 0)
| eval enccom = if(match(lower(Message), "encodedcommand"), "1", 0)
| eval base64 = if(match(lower(Message), "frombase64"), "1", 0)
| eval empire=if(match(lower(Message), "system.net.webclient") AND match(lower(Message), eval mimikatz=if(match(lower(Message), "mimikatz") OR match(lower(Message), "-dumpcr")
| eval iex = if(match(lower(Message), "iex"), "1", 0)
```

Sign up for free

to join this conversation on GitHub. Already have an account? Sign in to comment

Terms Privacy Security Status Docs Contact Manage cookies Do not share my personal information



© 2024 GitHub, Inc.