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

Instantly share code, notes, and snippets.

MHaggis / matching.md
Last active 2 years ago

Star 4 Fork 1

Code Revisions 5 Stars 4 Forks 1 Embed <script src="https:// Download ZIP

matching.md Raw

```
`powershell` EventCode=4104
| eval DoIt = if(match(Message,"DoIt"), "1", 0)
| eval enccom = if(match(Message,"EncodedCommand"), "1", 0)
| eval base64 = if(match(Message,"FromBase64"), "1", 0)
| eval iex = if(match(Message,"IEX"), "1", 0)
| eval rundll32 = if(match(Message,"rundll32"), "1", 0)
| 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, httplocal, reflection, sta
| stats values(Message) by Score
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
```

```
`powershell` EventCode=4104
| eval DoIt = if(match(Message,"DoIt"), "1", 0)
| eval enccom = if(match(Message,"EncodedCommand"), "1", 0)
| eval base64 = if(match(Message,"FromBase64"), "1", 0)
| eval iex = if(match(Message,"IEX"), "1", 0)
| eval rundll32 = if(match(Message,"rundll32"), "1", 0)
| 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, httplocal, reflection, sta
| stats values(Score) by DoIt, enccom, iex, rundll32, webclient, syswow64, powver, httplocal, reflection, startp
| `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, httplocal, reflection, sta
| stats values(Score) by DoIt, enccom, iex, rundll32, webclient, syswow64, powver, httplocal, reflection, startp
| `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), "frombase64string") ,1,0
| eval mimikatz=if(match(lower(Message),"mimikatz") OR match(lower(Message), "-dumpcr") OR match(lower(Message),
| eval iex = if(match(lower(Message),"iex"), "1", 0)
| eval get = if(match(lower(Message),"get-"), "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, mimikatz,iex,empire, rundll32, webclient, syswow64, powver, httplocal,
| stats values(Score) by DoIt, enccom, iex, mimikatz, rundll32,empire, webclient, syswow64, powver, httplocal, r
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
```