BlackMatter

github.com/sisoma2/malware_analysis/tree/master/blackmatter

sisoma2

sisoma2/
malware_analysis

Scripts, Yara rules and other files developed during malware investigations

2 Contributors | 0 Issues | 19 Stars | 5 Forks

In this repo you can find a small tool called `BlackMatter_hash.py` to recover the hashes hardcoded in different samples of the BlackMatter ransomware.

Usage

In order to work it needs a file with the hashes each one in a different line and the dictionary with the processes to bruteforce with the same format.

```
python BlackMatter_hash.py -d HASHES_FILE -t DICTIONARY_FILE -o OUTPUT_FILE
python BlackMatter_hash.py -m MODULE_NAME -a API_NAME
python BlackMatter_hash.py -s STRING
```

File Format

The script will calculate the hash of every string in the dictionary file.

Hashes can be prepend with 0x or not and they have to be in hexadecimal.

Lines starting with '#' will be ignored.

```
# Hashes file example
0xE99018C0
4c4b25d4

# Dict file example
$recycle.bin
```

Example

```
python BlackMatter_hash.py -d dict.txt -t hashes.txt -o cracked.json
[*] Trying to crack 98 hashes...
[+] Cracked hash 0xc5b01900 = adv
[+] Cracked hash 0xd4aaebb2 = admin$
[+] Cracked hash 0xdd801cc0 = msp
[+] Cracked hash 0xdd181cc0 = msc
[+] Cracked hash 0xc9201b40 = cmd
[+] Cracked hash 0xcbb01c80 = drv
[+] Cracked hash 0x64e29771 = diagpkg
[+] Cracked hash 0x3907099b = boot.ini
[+] Cracked hash 0xd3081d00 = hta
[+] Cracked hash 0xdd081c00 = mpa
[+] Cracked hash 0xe1a63bc0 = boot
[+] Cracked hash 0xe7801d00 = rtp
[+] Cracked hash 0xcd281e00 = exe
[+] Cracked hash 0x7f07935 = windows.old
[+] Cracked hash 0xfe9e7c10 = runonce.exe
[+] Cracked hash 0xdb301900 = ldf
[+] Cracked hash 0xc6ce6958 = appdata
[+] Cracked hash 0xa1fccbfe = deskthemepack
[+] Cracked hash 0xdd301900 = mdf
[+] Cracked hash 0xe9601c00 = spl
[+] Cracked hash 0xe3426cd7 = windows
[+] Cracked hash 0xd57818c0 = ico
[+] Cracked hash 0xdb975937 = ntldr
[+] Cracked hash 0x267078f5 = $windows.~bt
[+] Cracked hash 0x85aa57e4 = ntuser.dat.log
[+] Cracked hash 0xdd101900 = mdb
[+] Cracked hash 0x86ccaa15 = autorun.inf
[+] Cracked hash 0xfcc8ab56 = bootsect.bak
[+] Cracked hash 0xd9c81940 = key
[+] Cracked hash 0xc5481b80 = ani
[+] Cracked hash 0x26687e35 = $windows.~ws
[+] Cracked hash 0x4ae29631 = diagcfg
[+] Cracked hash 0xc9601c00 = cpl
[+] Cracked hash 0xdd481cc0 = msi
[+] Cracked hash 0x5366e694 = perflogs
[+] Cracked hash 0xf1c01c00 = wpx
[+] Cracked hash 0x2e75e394 = programdata
[+] Cracked hash 0xc7a01840 = bat
[+] Cracked hash 0x4c4b25d4 = tor browser
[+] Cracked hash 0xba22623b = all users
[+] Cracked hash 0xe9981a00 = shs
[+] Cracked hash 0xb7ea3892 = msocache
[+] Cracked hash 0xc9901d40 = cur
[+] Cracked hash 0xe1881cc0 = ps1
[+] Cracked hash 0xa6f2d1a7 = application data
[+] Cracked hash 0xc23aa6f5 = ntuser.dat
[+] Cracked hash 0xd59818c0 = ics
[+] Cracked hash 0xe9981e40 = sys
[+] Cracked hash 0xc9101840 = cab
[+] Cracked hash 0xc8cef7d1 = thumbs.db
[+] Cracked hash 0xcd101900 = edb
[+] Cracked hash 0x4aba94f1 = diagcab
[+] Cracked hash 0x5cde3a7b = public
```

```
[+] Cracked hash 0xdf981b00 = nls
[+] Cracked hash 0xdda81cc0 = msu
[+] Cracked hash 0xd5c01900 = idx
[+] Cracked hash 0xdf301900 = ndf
[+] Cracked hash 0xef3a37b3 = default
[+] Cracked hash 0x4cca7837 = nomedia
[+] Cracked hash 0x12018c0 = c$
[+] Cracked hash 0xe99018c0 = scr
[+] Cracked hash 0xc7701a40 = bin
[+] Cracked hash 0xe7681bc0 = rom
[+] Cracked hash 0x45678b17 = -wall
[+] Cracked hash 0xe1c018c0 = ocx
[+] Cracked hash 0xaf16c593 = themepack
[+] Cracked hash 0x49164931 = accdb
[+] Cracked hash 0xd56018c0 = icl
[+] Cracked hash 0x45471d17 = -path
[+] Cracked hash 0x8cf281cd = config.msi
[+] Cracked hash 0xc99eab80 = icns
[+] Cracked hash 0xd3801b00 = hlp
[+] Cracked hash 0xcbe2aa35 = ntuser.ini
[+] Cracked hash 0xcb601b00 = dll
[+] Cracked hash 0xeb9f5c34 = https
[+] Cracked hash 0x846bec00 = iconcache.db
[+] Cracked hash 0xdb581b80 = lnk
[+] Cracked hash 0xe3101900 = pdb
[+] Cracked hash 0x30a212d = $recycle.bin
[+] Cracked hash 0x452f4997 = -safe
[+] Cracked hash 0x36004e4e = program files
[+] Cracked hash 0x67b00e00 = 386
[+] Cracked hash 0x52cb0b38 = google
[+] Cracked hash 0xe3301c80 = prf
[+] Cracked hash 0xab086595 = program files (x86)
[+] Cracked hash 0xdd201bc0 = mod
[+] Cracked hash 0xeb869d00 = http
[+] Cracked hash 0xdccab8dd = mozilla
[+] Cracked hash 0x3eb272e6 = explorer.exe
[+] Cracked hash 0xf00cae96 = bootfont.bin
[+] Cracked hash 0xc9681bc0 = com
[+] Cracked hash 0x4a6bb7db = msstyles
[+] Cracked hash 0xe15ed8c0 = lock
[+] Cracked hash 0xae018eae = system volume information
[+] Cracked hash 0x82d2a252 = desktop.ini
[+] Cracked hash 0x6b66f975 = intel
[+] Cracked hash 0xb7e02438 = svchost.exe
[+] Cracked hash 0xcd2e9b7a = theme
[+] Total hashes cracked: 98
```

IOCs

Samples

```
2c323453e959257c7aa86dc180bb3aaaa5c5ec06fa4e72b632d9e4b817052009
7f6dd0ca03f04b64024e86a72a6d7cfab6abccc2173b85896fc4b431990a5984
22d7d67c3af10b1a37f277ebabe2d1eb4fd25afbd6437d4377400e148bcc08d6
c6e2ef30a86baa670590bd21acf5b91822117e0cbe6060060bc5fe0182dace99
daed41395ba663bef2c52e3d1723ac46253a9008b582bb8d9da9cb0044991720
```

C&C

```
mojobiden[.]com
paymenthacks[.]com
```