SDBbot Unpacker

github.com/Tera0017/SDBbot-Unpacker

Tera0017

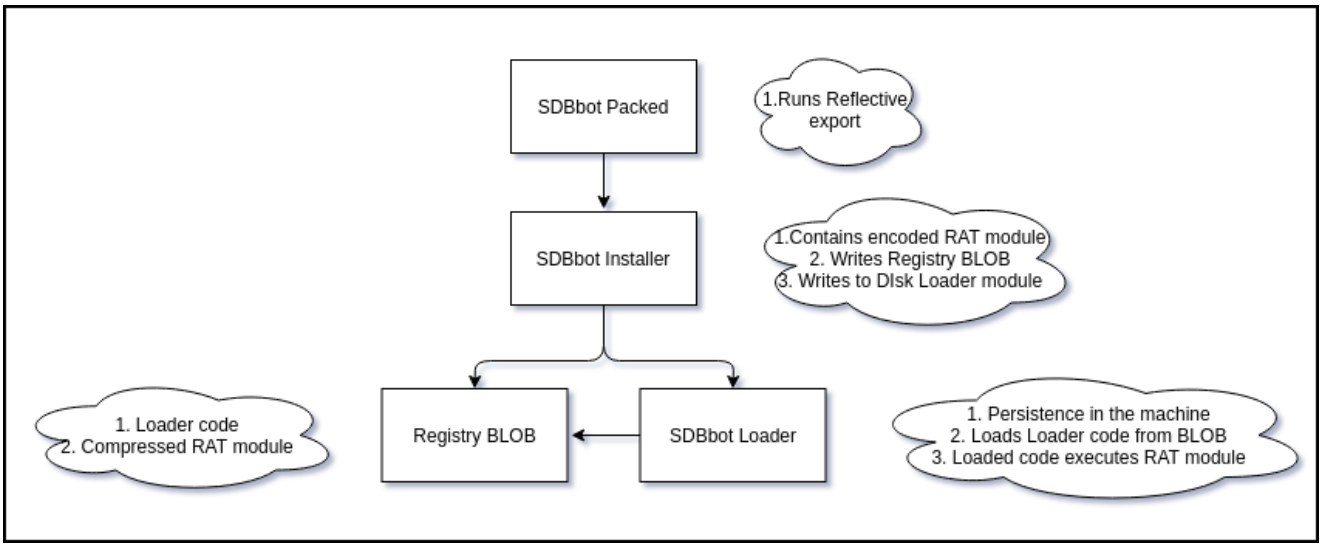
Tera0017/**SDBbot-Unpacker**

SDBbot Unpacker Python 2.7

1 Contributor | 0 Issues | 9 Stars | 2 Forks

SDBbot Unpacker is a python 2.7 script that is able to unpack/dump statically modules of x86 and x64 SDBbot packed samples.

SDBbot Infection process



More information:

> Proofpoint https://www.proofpoint.com/us/threat-insight/post/ta505-distributes-new-sdbbot-remote-access-trojan-get2-downloader

Usage

```
$ python sdbbot_unpacker.py --help


  ____  ____  ____  _           _     _   _                  _
 / ___||  _ \|  _ )| |__   ___ | |_  | | | |_ __  _ __   ___| | ___ __
 \___ \| | | |  _ \| '_ \ / _ \| __| | | | | '_ \| '_ \ / __| |/ / '__|
  ___) | |_| | |_) | |_) | (_) | |_  | |_| | | | | |_) | (__|   <| |
 |____/|____/|____/|_.__/ \___/ \__|  \___/|_| |_| .__/ \___|_|\_\_|
                                                  |_|
|--> SDBbot Unpacker
usage: sdbbot_unpacker.py [-h] [-f FILE]

SDBbot Modules Unpacker

optional arguments:
  -h, --help            show this help message and exit
  -f FILE, --file FILE  File to unpack modules.
```

Example x86

```
$ python sdbbot_unpacker.py -f png1


  ____  ____  ____  _           _     _   _                  _
 / ___||  _ \|  _ )| |__   ___ | |_  | | | |_ __  _ __   ___| | ___ __
 \___ \| | | |  _ \| '_ \ / _ \| __| | | | | '_ \| '_ \ / __| |/ / '__|
  ___) | |_| | |_) | |_) | (_) | |_  | |_| | | | | |_) | (__|   <| |
 |____/|____/|____/|_.__/ \___/ \__|  \___/|_| |_| .__/ \___|_|\_\_|
                                                  |_|
|--> SDBbot Unpacker
|--> Encoded code ROL 3
|--> Encoded code XOR Key: 0X1D24
|--> Encoded code Size: 0X270
|--> Encoded Binary ROL 3
|--> Encoded Binary XOR Key: 0X7178
|--> Encoded Binary Size: 0XF432
|--> SdbInstallerDll successfully dumped: SDBbot_SdbInstallerDll_png1
|--> RegCodeLoader successfully dumped: SDBbot_RegCodeLoader_png1
|--> RegBlob successfully dumped: SDBbot_RegBlob_png1
|--> BotDLL successfully dumped: SDBbot_RAT_BotDLL_png1
```

Example x64

```
$ python sdbbot_unpacker.py -f png2


  ____  ____  ____  _           _     _   _                    _
 / ___||  _ \| __ )| |__   ___ | |_  | | | |_ __  _ __   ___| | ___ __
 \___ \| | | |  _ \| '_ \ / _ \| __| | | | | '_ \| '_ \ / __| |/ / '__|
  ___) | |_| | |_) | |_) | (_) | |_  | |_| | | | | |_) | (__|   <| |
 |____/|____/|____/|_.__/ \___/ \__|  \___/|_| |_| .__/ \___|_|\_\_|
                                                  |_|
|--> SDBbot Unpacker
|--> Encoded code ROL 7
|--> Encoded code XOR Key: 0XA82
|--> Encoded code Size: 0X375
|--> Encoded Binary ROL 7
|--> Encoded Binary XOR Key: 0X55EE
|--> Encoded Binary Size: 0X12786
|--> SdbInstallerDll successfully dumped: SDBbot_SdbInstallerDll_png2
|--> RegCodeLoader successfully dumped: SDBbot_RegCodeLoader_png2
|--> RegBlob successfully dumped: SDBbot_RegBlob_png2
|--> BotDLL successfully dumped: SDBbot_RAT_BotDLL_png2
```

Requirements

- lznt1 (https://github.com/you0708/lznt1)
- pefile
- yara-python

Support

In case some files are not working, please make sure it is a packed SDBbot, if yes please provide me the hash in a DM @Tera0017.

Regards