IoC for Manjusaka

github.com/avast/ioc/tree/master/Manjusaka

avast

Manjusaka is web based imitation of the Cobalt Strike framework.

More info: Talos blogpost
Manjusaka github: https://github.com/YDHCUI/manjusaka

Table of Contents

Framework content unpacking

Payloads, binaries, and other hardcoded framework components are compressed (raw deflated) and encoded as hex strings.

Each data blob start with header:

```
1F 8B 08 00 00 00 00 00 00 FF
```

The last two hardcoded data blobs a EXE and ELF binaries.

Payloads unpacking example:

1. Parse payload data blobs and remove header (20 chars)

```
    r = re.compile(b'1f8b08000000000000ff[0-9a-f]{1024,}?')
    data_blobs = re.finditer(r, buff)
    payloads = list(data_blobs)[-2:]

    payload_1_start = payloads[0].start()
    payload_1_end = payloads[1].start()
    payload_1_buff = buff[payload_1_start+20:payload_1_end]

    payload_2_start = payload_1_end
    payload_2_end = re.search(b'[0-9a-f]{4}?\x00', buff[payload_2_start:]).start() +
4 + payload_2_start
    payload_2_buff = buff[payload_2_start+20:payload_2_end]
```

1. Decode and decompress payload

```
    raw_data = binascii.unhexlify(payload_1_buff)
    data = zlib.decompressobj(wbits=-15) # -15 = no headers and trailers
    decompressed_data = data.decompress(raw_data)
    decompressed_data += data.flush()
```

You can also use our rip.py script.

Framework Go build IDs

```
Wy_vibDZv2wm5bL2qsjJ/4PMVyM99vavXhzeZ4lv-/NYl_KmuSEbSNJk9EaRt1/-EMPWdjs0Nl7sygAAteT -
ELF v01
y0MW5jt0EkawUK5kkl12/Zh446aeMzbHG7OsVOfqu/m_XtCR229uKgZbQeD5Ct/fxfGJGaYN1_6nNv2XZSb -
ELF v02
0306BSKBqnqKtMQqgSXM/hLj4wvVVJLyBCaJB_8M0/stfbGsFZXgNkPwZKLqRe/MIFhigzePSeV5d_RmfC5 -
ELF v03 (dev)
654gijPAUkEazJpjD9NU/gDuHF1xfdp91Sf6SYQHX/vsnn7ekg0TKXWiOScF0D/Sam0sQmfyCaDC8qCfYx5 -
ELF v03
erRGOJVHe87XgmyOVwHD/BpxVvpyDXtLddyWFd8N9/oYwdpsmFEDX92XJURLUz/bbXY8CvkDMriB32dI6SX -
EXE v03
```

Binaries PDB

```
Z:\Code\NPSC2\npc\target\release\deps\npc.pdb
D:\CodeProject\hw_src\NPSC2\npc\target\release\deps\npc.pdb
```

Yara rules

```
manjusaka_framework_go_build_id
manjusaka_payload_encoded_hexstring
manjusaka_payload_elf
manjusaka_payload_mz
```

You can download whole ruleset here.

Samples (SHA-256)

Framework GoLang binaries

```
955e9bbcdf1cb230c5f079a08995f510a3b96224545e04c1b1f9889d57dd33c1 - ELF v01
f275ca5129399a521c8cd9754b1133ecd2debcfafc928c01df6bd438522c564a - ELF v02 upx
637f3080526d7d0ad5eb41bf9331fb51aaafd30f2895c00a44ad905154f76d70 - ELF v02 unpacked
b5c366d782426bad4ba880dc908669ff785420dea02067b12e2261dd1988f34a - ELF v03 (dev) upx
107b094031094cbb1f081d85ec2799c3450dce32e254bda2fd1bb32edb449aa4 - ELF v03 (dev)
unpacked
fb5835f42d5611804aaa044150a20b13dcf595d91314ebef8cf6810407d85c64 - ELF v03 upx
ff20333d38f7affbfde5b85d704ee20cd60b519cb57c70e0cf5ac1f65acf91a6 - ELF v03 unpacked
3581d99feb874f65f53866751b7874c106b5ce65a523972ef6a736844209043c - EXE v03 upx
6082bf26bcc07bf299a88eaa0272022418b12156cd987adfdff9fa1517afcf3d - EXE v03 unpacked
```

Hardcoded payload Rust binaries

```
0063e5007566e0a7e8bfd73c4628c6d140b332df4f9afbb0adcf0c832dd54c2b - ELF v01, v02
d5918611b1837308d0c6d19bff4b81b00d4f6a30c1240c00a9e0a9b08dde1412 - ELF v03 (dev)
0a5174b5181fcd6827d9c4a83e9f0423838cbb5a6b23d012c3ae414b31c8b0da - ELF v03
6839180bc3a2404e629c108d7e8c8548caf9f8249bbbf658b47c00a15a64758f - EXE v01
cd0c75638724c0529cc9e7ca0a91d2f5d7221ef2a87b65ded2bc1603736e3b5d - EXE v02
76eb9af0e2f620016d63d38ddb86f0f3f8f598b54146ad14e6af3d8f347dd365 - EXE v03 (dev)
2b174d417a4e43fd6759c64512faa88f4504e8f14f08fd5348fff51058c9958f - EXE v03
```

ITW payload Rust binaries

```
056bff638627d46576a3cecc3d5ea6388938ed4cb30204332cd10ac1fb826663
399abe81210b5b81e0984892eee173d6eeb99001e8cd5d377f6801d092bdef68
3a3c0731cbf0b4c02d8cd40a660cf81f475fee6e0caa85943c1de6ad184c8c31
8e9ecd282655f0afbdb6bd562832ae6db108166022eb43ede31c9d7aacbcc0d8
90b6a021b4f2e478204998ea4c5f32155a7348be4afb620999fa708b4a9a30ab
a8b8d237e71d4abe959aff4517863d9f570bba1646ec4e79209ec29dda64552f
ecbe098ed675526a2c22aaf79fe8c1462fb4c68eb0061218f70fadbeb33eeced
```

Network indicators

C2 IPs

```
45[.]137.117.219
39[.]104.90.45
95[.]179.151.49
71[.]115.193.247:9000
119[.]28.101.125
104[.]225.234.200
```

User Agents

```
Mozilla/5.0 (Windows NT 8.0; WOW64; rv:40.0) Gecko
Mozilla/5.0 (Windows NT 8.0; WOW64; rv:58.0) Gecko/20120102 Firefox/58.0
Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
```

OSINT data

Binaries

```
C:\Users\Administrator.WIN7-2021OVWRCZ\.cargo\registry\src\mirrors.ustc.edu.cn-
C:\Users\root\.cargo\registry\src\mirrors.ustc.edu.cn-
/root/.cargo/registry/src/mirrors.ustc.edu.cn-
```

Github

```
h5[.]qianxin[.]com
https[:]//weixin[.]qq[.]com/g/AQYAAEoVSAjZ35xwIeusxAmY6Qm2wKXvvjp6Ed7stK2OrUIl-
a6Czezgc4QYv6GS
https[:]//profile-counter[.]glitch[.]me/DaxiaMM-new/count.svg
```

Framework author

```
#codeby     道长且阻
#email      @ydhcui/QQ664284092
```