

ioc/Manjusaka at master · gendigitalinc/ioc

By michalsalat

Archived: 2026-04-05 23:02:41 UTC

Manjusaka is web based imitation of the Cobalt Strike framework.

More info: <https://blog.talosintelligence.com/2022/08/manjusaka-offensive-framework.html>

Manjusaka github: <https://github.com/YDHCUI/manjusaka>

Table of Contents

- [Framework content unpacking](#)
- [Framework Go build IDs](#)
- [Binaries PDB](#)
- [Yara rule](#)
- [Samples \(SHA-256\)](#)
- [Network indicators](#)
- [OSINT data](#)

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
```

Up to v04 the last two hardcoded data blobs are EXE and ELF binaries, since v05 all EXE and ELF binaries are stored inside plugins folder.

Payloads unpacking example:

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

```
r = re.compile(b'1f8b080000000000ff[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_s
payload_2_buff = buff[payload_2_start+20:payload_2_end]
```

2. 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
y0MW5jt0EkawUK5kk112/Zh446aeMzbHG70sV0fqu/m_XtCR229uKgZbQeD5Ct/xfGJGaYN1_6nNv2XZSb - ELF v02
0306BSKBqnqKtMQqgSXM/hLj4wvVVJLyBCaJB_8M0/stfbGsFZXgNkPwZKLqRe/MIFhigzePSeV5d_RmfC5 - ELF v03 (dev)
654gijPAUKeazJpjD9NU/gDuHF1xfdp91Sf6SYQHx/vsnn7ekg0TKXWi0ScF0D/Sam0sQmfyCaDC8qCfYx5 - ELF v03
erRGOJVHe87XgmyOVwHD/BpxVvpyDXtLddyWFd8N9/oYwdpsmFEDX92XJURLUz/bbXY8CvkDMriB32dI6SX - EXE v03
GnBKocLwvWZnC_UmIr-r/6P-0zFbQ79oYyyaDRHV4/8tmFwxcSdcccmpfsZc3hb/w4-6IRPpuBfuhazPcL52 - ELF v04
NPWAdPbWmnXr0a6gD7Kz/TtnYdOyCjvcCQuZ9GiDr/FCm0i8A066RPC6SOWvaM/CpW700s8aQ2BFVdfFebTJ - ELF v05
```

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
6082bf26bcc07bf299a88eaa0272022418b12156cd987adfdf9fa1517afc3d - EXE v03 unpacked
14dfb43a1782b0b8d93c3d67d63b6c786b0a223bc50c3ec68106bd18d43652a4 - ELF v04 upx
4a0f47132867c12a6d009e43812729a1bb41f4eb83472ac352fc5b20fe937bef - ELF v04 unpacked
bb1b7d506559c783ed747da461f58ea5256ba0a083768ae6aa1a2325017c4387 - ELF v05 upx
bd0e09e9ee4db74ada6433f00024a543f799046c15f635216ca4ae5e1f0c42e2 - ELF v05 unpacked
```

Hardcoded payload Rust binaries

```
0063e5007566e0a7e8bfd73c4628c6d140b332df4f9afbb0adcfc0c832dd54c2b - ELF v01, v02
d5918611b1837308d0c6d19bff4b81b00d4f6a30c1240c00a9e0a9b08dde1412 - ELF v03 (dev)
0a5174b5181fcd6827d9c4a83e9f0423838cbb5a6b23d012c3ae414b31c8b0da - ELF v03
63e7f6fa89faa88b346d0ccedd2ef2e3ebf5d5828aa0087663c227422041db7 - ELF v04
4eb337c12f0e0ee73b3209bed4b819719c4af9f63f3e81dbc3bbf06212450f1c - ELF v05
400855b63b8452221869630c58b7ab03373dabf77c0f10df635e746c13f98ea9 - ELF v05
443abf66039c6686b50e5091ac218810798a21884aa6bc0d5b6dd8782b0311a8 - ELF v05
6839180bc3a2404e629c108d7e8c8548caf9f8249bbb6f658b47c00a15a64758f - EXE v01
cd0c75638724c0529cc9e7ca0a91d2f5d7221ef2a87b65ded2bc1603736e3b5d - EXE v02
76eb9af0e2f620016d63d38ddb86f0f3f8f598b54146ad14e6af3d8f347dd365 - EXE v03 (dev)
2b174d417a4e43fd6759c64512faa88f4504e8f14f08fd5348fff51058c9958f - EXE v03
377bacba69d2bec770599ab21a202b574b92fb431fc35bbdf39080025d6cf2d6 - EXE v04
51857882d1202e72c0cf18ff21de773c2a31ee68ff28385f968478401c5ab4bb - EXE v05
86c633467ba7981d3946a63184dbfabce587b571f761b3eb1e3e43f6b1df6f2c - EXE v05
e07aa10f19574a856a4ac389a3ded96f2d78f41f939935dd678811bd12b5bd03 - EXE v05
9e7144540430d97de38a2adcef16ad43e23c91281462b135fcc56cafc2f34160 - EXE v05
```

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.WIN7-20210VWRCZ\.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/AQYAAEoVSAjZ35xwIeusxAmY6Qm2wKXvvjp6Ed7stK20rUIl-a6Czezc4QYv6GS
https[:]//profile-counter[.]glitch[.]me/DaxiaMM-new/count.svg
```

Framework author

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