

GitHub Gist

Search...


All gists

Back to GitHub

Sign in

Sign up

Instantly share code, notes, and snippets.



MHaggis / malleable\_c2\_profiles

Last active 5 months ago

☆ Star 38

🍴 Fork 12

<> Code

🔗 Revisions 4

☆ Stars 38

🍴 Forks 12

Embed <script src="https://>

📄

📄

Download ZIP

<> malleable\_c2\_profiles

Raw

```
1  spawnnto
2  https://raw.githubusercontent.com/kphongagsorn/c2-profiles/29fe50eaad655ddd0028fca06a9c7785e3ffaf41/amazon.profile
3  https://raw.githubusercontent.com/kvcallfield/Cobalt-Strike-C2-profiles/cae44634d57c0d8a099e50f6d4e9b73acaaab9d6/amazon2.profile
4  https://raw.githubusercontent.com/KevinCooper/24AF-CyberChallenge/67f531777f7912c7129f633f43e06fba79c5f3e2/CobaltStrike/cobalt.prof
5  https://raw.githubusercontent.com/webcoderz/agressor-scripts-/950064776853cf4dd7403d0f75b5306fe275fcc3/Malleable-C2-Profiles-master
6  https://raw.githubusercontent.com/hadesangel/Malleable-C2-Profiles/390937aec01e0bcdaf23312277e96e57ac925f7b/APT/meterpreter.profile
7  https://raw.githubusercontent.com/ianxtianxt/Malleable-C2-Profiles/07fd3b45c4166c9aecdcfa54cddc905c22f6ff85/APT/meterpreter.profile
8  https://raw.githubusercontent.com/seclib/Malleable-C2-Profiles/390937aec01e0bcdaf23312277e96e57ac925f7b/APT/meterpreter.profile
9  https://raw.githubusercontent.com/rsmudge/Malleable-C2-Profiles/390937aec01e0bcdaf23312277e96e57ac925f7b/APT/meterpreter.profile
10 https://raw.githubusercontent.com/mhaskar/MalleableC2-Profiles/4432c64effce56134bbcc10836b4d813c09049ac/windows-updates.profile
11 https://raw.githubusercontent.com/lee-c3x/malleable/3fd552e4373c639968f70978f327012873bd38cd/lee-malleable-skeleton.profile
12 https://raw.githubusercontent.com/yeyintminthuhtut/Malleable-C2-Profiles-Collection/b1dc3b83c018dcbf6b823f9027c928d07949a063/APT/me
13 https://raw.githubusercontent.com/federico33385/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/APT/meterpreter.prof
14 https://raw.githubusercontent.com/yeyintminthuhtut/Malleable-C2-Profiles-Collection/b1dc3b83c018dcbf6b823f9027c928d07949a063/APT/ch
15 https://raw.githubusercontent.com/yeyintminthuhtut/Malleable-C2-Profiles-Collection/b1dc3b83c018dcbf6b823f9027c928d07949a063/Crimew
16 https://raw.githubusercontent.com/federico33385/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/APT/chches_APT10.pro
17 https://raw.githubusercontent.com/federico33385/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/Crimeware/jasperload
18 https://raw.githubusercontent.com/lee-c3x/malleable/3fd552e4373c639968f70978f327012873bd38cd/meterpreter.profile
19 https://raw.githubusercontent.com/lee-c3x/malleable/3fd552e4373c639968f70978f327012873bd38cd/clean_template.profile
20 https://raw.githubusercontent.com/federico33385/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/Normal/windows-updat
21 https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/6a749f0ef99211db3812065f2b24ae023f5bd3dc/APT/meterpreter.profil
22 https://raw.githubusercontent.com/lee-c3x/malleable/3fd552e4373c639968f70978f327012873bd38cd/chches_APT10.profile
23 https://raw.githubusercontent.com/lee-c3x/malleable/3fd552e4373c639968f70978f327012873bd38cd/jasperloader.profile
24 https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/1b110729860fd7e6f37aa3e6d04e24e6539f16de/APT/chches_APT10.profile
25 https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/1b110729860fd7e6f37aa3e6d04e24e6539f16de/crimeware/jasperloader.prof
26 https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/1b110729860fd7e6f37aa3e6d04e24e6539f16de/crimeware/saefko.profile
27 https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/dddad4550180e92eb33275b5167249a74f9a22e0/Crimeware/saefko.profi
28 https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/6a749f0ef99211db3812065f2b24ae023f5bd3dc/APT/chches_APT10.profi
29 https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/6a749f0ef99211db3812065f2b24ae023f5bd3dc/Crimeware/jasperloader
30 https://raw.githubusercontent.com/yeyintminthuhtut/Malleable-C2-Profiles-Collection/b1dc3b83c018dcbf6b823f9027c928d07949a063/Social
31 https://raw.githubusercontent.com/federico33385/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/Normal/reddit.profil
32 https://raw.githubusercontent.com/federico33385/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/Normal/gotomeeting.p
33 https://raw.githubusercontent.com/federico33385/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/Normal/msu_edu.profi
34 https://raw.githubusercontent.com/federico33385/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/Normal/office365_cal
35 https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/Normal/windows-updates
36 https://raw.githubusercontent.com/yeyintminthuhtut/Malleable-C2-Profiles-Collection/b1dc3b83c018dcbf6b823f9027c928d07949a063/Misc/m
37 https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/9f1182d7f77339e2587ecc5f3e094e05bef5db20/clean_template.profile
38 https://raw.githubusercontent.com/federico33385/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/Normal/mayoclinic.pr
39 https://raw.githubusercontent.com/guidepointsecurity/RedCommander/f8dc14428886247b322552cc9e7eeffd7e4cea2d/files/custom/HTTPS/evasi
40 https://raw.githubusercontent.com/guidepointsecurity/RedCommander/f8dc14428886247b322552cc9e7eeffd7e4cea2d/files/custom/DNS/evasive
41 https://raw.githubusercontent.com/lee-c3x/malleable/3fd552e4373c639968f70978f327012873bd38cd/reddit.profile
42 https://raw.githubusercontent.com/rsmudge/Malleable-C2-Profiles/26323784672913923d20c5a638c6ca79459e8529/normal/reference.profile
43 https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/1b110729860fd7e6f37aa3e6d04e24e6539f16de/normal/reddit.profile
44 https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/6a749f0ef99211db3812065f2b24ae023f5bd3dc/Normal/reddit.profile
45 https://raw.githubusercontent.com/yeyintminthuhtut/Malleable-C2-Profiles-Collection/b1dc3b83c018dcbf6b823f9027c928d07949a063/Social
46 https://raw.githubusercontent.com/yeyintminthuhtut/Malleable-C2-Profiles-Collection/b1dc3b83c018dcbf6b823f9027c928d07949a063/Social
47 https://raw.githubusercontent.com/federico33385/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/Normal/stackoverflow
48 https://raw.githubusercontent.com/lee-c3x/malleable/3fd552e4373c639968f70978f327012873bd38cd/gotomeeting.profile
49 https://raw.githubusercontent.com/lee-c3x/malleable/3fd552e4373c639968f70978f327012873bd38cd/msu_edu.profile
50 https://raw.githubusercontent.com/lee-c3x/malleable/3fd552e4373c639968f70978f327012873bd38cd/office365_calendar.profile
51 https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/1b110729860fd7e6f37aa3e6d04e24e6539f16de/normal/gotomeeting.profile
52 https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/1b110729860fd7e6f37aa3e6d04e24e6539f16de/normal/msu_edu.profile
53 https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/1b110729860fd7e6f37aa3e6d04e24e6539f16de/normal/office365_calendar.p
54 https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/6a749f0ef99211db3812065f2b24ae023f5bd3dc/Normal/gotomeeting.pro
55 https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/6a749f0ef99211db3812065f2b24ae023f5bd3dc/Normal/msu_edu.profile
56 https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/6a749f0ef99211db3812065f2b24ae023f5bd3dc/Normal/office365_calen
57 https://raw.githubusercontent.com/federico33385/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/Normal/youtube_video
```

58 <https://raw.githubusercontent.com/lee-c3x/malleable/3fd552e4373c639968f70978f327012873bd38cd/mayoclinic.profile>

59 <https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/1b110729860fd7e6f37aa3e6d04e24e6539f16de/normal/mayoclinic.profile>

60 <https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/6a749f0ef99211db3812065f2b24ae023f5bd3dc/Normal/mayoclinic.prof>

61 [https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/0ef8cf4556e26f6d4190c56ba697c2159faa5822/crimeware/trick\\_ryuk.profil](https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/0ef8cf4556e26f6d4190c56ba697c2159faa5822/crimeware/trick_ryuk.profil)

62 <https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/1b110729860fd7e6f37aa3e6d04e24e6539f16de/crimeware/zloader.profile>

63 [https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/dddad4550180e92eb33275b5167249a74f9a22e0/Crimeware/trick\\_ryuk.p](https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/dddad4550180e92eb33275b5167249a74f9a22e0/Crimeware/trick_ryuk.p)

64 <https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/dddad4550180e92eb33275b5167249a74f9a22e0/Crimeware/zloader.prof>

65 <https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/1b110729860fd7e6f37aa3e6d04e24e6539f16de/normal/slack.profile>

66 <https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/1b110729860fd7e6f37aa3e6d04e24e6539f16de/normal/stackoverflow.profil>

67 <https://raw.githubusercontent.com/lee-c3x/malleable/3fd552e4373c639968f70978f327012873bd38cd/slack.profile>

68 <https://raw.githubusercontent.com/lee-c3x/malleable/3fd552e4373c639968f70978f327012873bd38cd/stackoverflow.profile>

69 <https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/dddad4550180e92eb33275b5167249a74f9a22e0/Normal/slack.profile>

70 <https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/6a749f0ef99211db3812065f2b24ae023f5bd3dc/Normal/stackoverflow.p>

71 <https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/7189deb738d32f073cacb47d27f64443a17d3b42/normal/mscrl.profile>

72 [https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/1b110729860fd7e6f37aa3e6d04e24e6539f16de/normal/youtube\\_video.profil](https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/1b110729860fd7e6f37aa3e6d04e24e6539f16de/normal/youtube_video.profil)

73 [https://raw.githubusercontent.com/lee-c3x/malleable/3fd552e4373c639968f70978f327012873bd38cd/youtube\\_video.profile](https://raw.githubusercontent.com/lee-c3x/malleable/3fd552e4373c639968f70978f327012873bd38cd/youtube_video.profile)

74 [https://raw.githubusercontent.com/federico33385/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/Crimeware/covid19\\_ko](https://raw.githubusercontent.com/federico33385/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/Crimeware/covid19_ko)

75 [https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/6a749f0ef99211db3812065f2b24ae023f5bd3dc/Normal/youtube\\_video.p](https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/6a749f0ef99211db3812065f2b24ae023f5bd3dc/Normal/youtube_video.p)

76 <https://raw.githubusercontent.com/Libraggbond/CS4.0-Malleable-c2-profile/fc6365924077174b33beb7645ce7ba8c1cb8c430/myhttpsc2.profile>

77 <https://raw.githubusercontent.com/threatexpress/malleable-c2/b45e1fce4d7cf46fdd199e1425f9b68b51e81e04/jquery-c2.3.14.profile>

78 <https://raw.githubusercontent.com/federico33385/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/Normal/trevor.profil>

79 [https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/1b110729860fd7e6f37aa3e6d04e24e6539f16de/crimeware/covid19\\_koadic.pr](https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/1b110729860fd7e6f37aa3e6d04e24e6539f16de/crimeware/covid19_koadic.pr)

80 <https://raw.githubusercontent.com/threatexpress/malleable-c2/b45e1fce4d7cf46fdd199e1425f9b68b51e81e04/jquery-c2.4.0.profile>

81 [https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/6a749f0ef99211db3812065f2b24ae023f5bd3dc/Crimeware/covid19\\_koad](https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/6a749f0ef99211db3812065f2b24ae023f5bd3dc/Crimeware/covid19_koad)

82 <https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/1b110729860fd7e6f37aa3e6d04e24e6539f16de/normal/trevor.profile>

83 <https://raw.githubusercontent.com/lee-c3x/malleable/3fd552e4373c639968f70978f327012873bd38cd/template.profile>

84 <https://raw.githubusercontent.com/lee-c3x/malleable/3fd552e4373c639968f70978f327012873bd38cd/trevor.profile>

85 <https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/6a749f0ef99211db3812065f2b24ae023f5bd3dc/Normal/trevor.profile>

86 <https://raw.githubusercontent.com/threatexpress/malleable-c2/c3385e481159a759f79b8acfe11acf240893b830/jquery-c2.4.2.profile>

87 <https://raw.githubusercontent.com/federico33385/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/template.profile>

88 <https://raw.githubusercontent.com/threatexpress/malleable-c2/b45e1fce4d7cf46fdd199e1425f9b68b51e81e04/jquery-c2.3.11.profile>

89 <https://raw.githubusercontent.com/bigb0sss/RedTeam-OffensiveSecurity/0a0a17f31698ab15e62249fca99a4bd1346991e3/01-CobaltStrike/malle>

90 <https://raw.githubusercontent.com/yeyintminthuhtut/Malleable-C2-Profiles-Collection/b1dc3b83c018dcbf6b823f9027c928d07949a063/Misc/i>

91 <https://raw.githubusercontent.com/threatexpress/malleable-c2/b45e1fce4d7cf46fdd199e1425f9b68b51e81e04/jquery-c2.3.13.profile>

92 <https://raw.githubusercontent.com/threatexpress/malleable-c2/b45e1fce4d7cf46fdd199e1425f9b68b51e81e04/jquery-c2.3.12.profile>

93 <https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/dddad4550180e92eb33275b5167249a74f9a22e0/Normal/jquery-c2.4.2.p>

94 <https://raw.githubusercontent.com/kphongagsorn/c2-profiles/29fe50eaad655ddd0028fca06a9c7785e3ffaf41/zillow.profile>

95 <https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/6a749f0ef99211db3812065f2b24ae023f5bd3dc/template.profile>

96 <https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/d4f85a85e047a7e29b2ae3c2b952758d47c3099c/template.profile>

97 <https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/1b110729860fd7e6f37aa3e6d04e24e6539f16de/normal/iheartradio.profile>

98 <https://raw.githubusercontent.com/kphongagsorn/c2-profiles/29fe50eaad655ddd0028fca06a9c7785e3ffaf41/duckduckgo-ramen-search-get-onl>

99 <https://raw.githubusercontent.com/lee-c3x/malleable/3fd552e4373c639968f70978f327012873bd38cd/iheartradio.profile>

100 <https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/dddad4550180e92eb33275b5167249a74f9a22e0/Normal/iheartradio.pro>

101 pipe

102 <https://raw.githubusercontent.com/KevinCooper/24AF-CyberChallenge/67f531777f7912c7129f633f43e06fba79c5f3e2/CobaltStrike/cobalt.prof>

103 <https://raw.githubusercontent.com/lee-c3x/malleable/3fd552e4373c639968f70978f327012873bd38cd/lee-malleable-skeleton.profile>

104 <https://raw.githubusercontent.com/threatexpress/cs2modrewrite/d6516e153dfd2a19cc3fba6c26b948e2b0933708/havex.profile>

105 <https://raw.githubusercontent.com/mhaskar/MalleableC2-Profiles/4432c64effce56134bbcc10836b4d813c09049ac/windows-updates.profile>

106 <https://raw.githubusercontent.com/Libraggbond/CS4.0-Malleable-c2-profile/fc6365924077174b33beb7645ce7ba8c1cb8c430/myhttpsc2.profile>

107 <https://raw.githubusercontent.com/seclib/Malleable-C2-Profiles/390937aec01e0bcdaf23312277e96e57ac925f7b/APT/havex.profile>

108 [https://raw.githubusercontent.com/lee-c3x/malleable/3fd552e4373c639968f70978f327012873bd38cd/clean\\_template.profile](https://raw.githubusercontent.com/lee-c3x/malleable/3fd552e4373c639968f70978f327012873bd38cd/clean_template.profile)

109 <https://raw.githubusercontent.com/yeyintminthuhtut/Malleable-C2-Profiles-Collection/b1dc3b83c018dcbf6b823f9027c928d07949a063/APT/ha>

110 <https://raw.githubusercontent.com/hadesangel/Malleable-C2-Profiles/390937aec01e0bcdaf23312277e96e57ac925f7b/APT/havex.profile>

111 <https://raw.githubusercontent.com/webcoderz/agressor-scripts-/950064776853cf4dd7403d0f75b5306fe275fcc3/Malleable-C2-Profiles-master>

112 <https://raw.githubusercontent.com/federico33385/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/Normal/windows-updat>

113 <https://raw.githubusercontent.com/ianxtianxt/Malleable-C2-Profiles/07fd3b45c4166c9aecdcfa54cddc905c22f6ff85/APT/havex.profile>

114 <https://raw.githubusercontent.com/lee-c3x/malleable/3fd552e4373c639968f70978f327012873bd38cd/template.profile>

115 <https://raw.githubusercontent.com/rsmudge/Malleable-C2-Profiles/390937aec01e0bcdaf23312277e96e57ac925f7b/APT/havex.profile>

116 <https://raw.githubusercontent.com/federico33385/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/template.profile>

117 <https://raw.githubusercontent.com/federico33385/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/APT/havex.profile>

118 [https://raw.githubusercontent.com/federico33385/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/Normal/msu\\_edu.profi](https://raw.githubusercontent.com/federico33385/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/Normal/msu_edu.profi)

119 <https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/Normal/windows-updates>

120 <https://raw.githubusercontent.com/lee-c3x/malleable/3fd552e4373c639968f70978f327012873bd38cd/havex.profile>

121 [https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/9f1182d7f77339e2587ecc5f3e094e05bef5db20/clean\\_template.profile](https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/9f1182d7f77339e2587ecc5f3e094e05bef5db20/clean_template.profile)

122 <https://raw.githubusercontent.com/lengjibo/RedTeamTools/134970a01f3c8e525f1ce691ca60b6b122efee3c/windows/Malleable-C2-Profiles/bing>

123 [https://raw.githubusercontent.com/lee-c3x/malleable/3fd552e4373c639968f70978f327012873bd38cd/msu\\_edu.profile](https://raw.githubusercontent.com/lee-c3x/malleable/3fd552e4373c639968f70978f327012873bd38cd/msu_edu.profile)

124 <https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/6a749f0ef99211db3812065f2b24ae023f5bd3dc/template.profile>

125 <https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/6a749f0ef99211db3812065f2b24ae023f5bd3dc/APT/havex.profile>

126 <https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/d4f85a85e047a7e29b2ae3c2b952758d47c3099c/template.profile>

127 [https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/1b110729860fd7e6f37aa3e6d04e24e6539f16de/normal/msu\\_edu.profile](https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/1b110729860fd7e6f37aa3e6d04e24e6539f16de/normal/msu_edu.profile)

128 <https://raw.githubusercontent.com/guidepointsecurity/RedCommander/f8dc14428886247b322552cc9e7eeffd7e4cea2d/files/custom/HTTPS/evasi>

129 <https://raw.githubusercontent.com/guidepointsecurity/RedCommander/f8dc14428886247b322552cc9e7eeffd7e4cea2d/files/custom/DNS/evasive>

130 [https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/6a749f0ef99211db3812065f2b24ae023f5bd3dc/Normal/msu\\_edu.profile](https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/6a749f0ef99211db3812065f2b24ae023f5bd3dc/Normal/msu_edu.profile)

131 <https://raw.githubusercontent.com/rsmudge/Malleable-C2-Profiles/26323784672913923d20c5a638c6ca79459e8529/normal/reference.profile>

132 https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/0ef8cf4556e26f6d4190c56ba697c2159faa5822/crimeware/trick\_ryuk.profil  
133 https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/1b110729860fd7e6f37aa3e6d04e24e6539f16de/crimeware/zloader.profile  
134 https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/dddad4550180e92eb33275b5167249a74f9a22e0/Crimeware/trick\_ryuk.p  
135 https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/dddad4550180e92eb33275b5167249a74f9a22e0/Crimeware/zloader.prof  
136 https://raw.githubusercontent.com/threatexpress/malleable-c2/b45e1fce4d7cf46fdd199e1425f9b68b51e81e04/jquery-c2.3.11.profile  
137 https://raw.githubusercontent.com/federico33385/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/Crimeware/covid19\_ko  
138 https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/7189deb738d32f073cacb47d27f64443a17d3b42/normal/mscrl.profile  
139 https://raw.githubusercontent.com/threatexpress/malleable-c2/b45e1fce4d7cf46fdd199e1425f9b68b51e81e04/jquery-c2.3.13.profile  
140 https://raw.githubusercontent.com/threatexpress/malleable-c2/b45e1fce4d7cf46fdd199e1425f9b68b51e81e04/jquery-c2.3.12.profile  
141 https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/1b110729860fd7e6f37aa3e6d04e24e6539f16de/crimeware/covid19\_koadic.pr  
142 https://raw.githubusercontent.com/threatexpress/malleable-c2/b45e1fce4d7cf46fdd199e1425f9b68b51e81e04/jquery-c2.3.14.profile  
143 https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/6a749f0ef99211db3812065f2b24ae023f5bd3dc/Crimeware/covid19\_koad  
144 https://raw.githubusercontent.com/kphongagsorn/c2-profiles/29fe50eaa655ddd0028fca06a9c7785e3ffaf41/zillow.profile  
145 https://raw.githubusercontent.com/bigb0sss/RedTeam-OffensiveSecurity/0a0a17f31698ab15e62249fca99a4bd1346991e3/01-CobaltStrike/malle  
146 https://raw.githubusercontent.com/threatexpress/malleable-c2/b45e1fce4d7cf46fdd199e1425f9b68b51e81e04/jquery-c2.4.0.profile  
147 https://raw.githubusercontent.com/threatexpress/malleable-c2/c3385e481159a759f79b8acfe11acf240893b830/jquery-c2.4.2.profile  
148 https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/dddad4550180e92eb33275b5167249a74f9a22e0/Normal/jquery-c2.4.2.p  
149 post-ex  
150 https://raw.githubusercontent.com/kvcallfield/Cobalt-Strike-C2-profiles/cae44634d57c0d8a099e50f6d4e9b73acaaab9d6/amazon2.profile  
151 https://raw.githubusercontent.com/rsmudge/Malleable-C2-Profiles/26323784672913923d20c5a638c6ca79459e8529/normal/reference.profile  
152 https://raw.githubusercontent.com/kphongagsorn/c2-profiles/29fe50eaa655ddd0028fca06a9c7785e3ffaf41/amazon.profile  
153 https://raw.githubusercontent.com/threatexpress/malleable-c2/c3385e481159a759f79b8acfe11acf240893b830/jquery-c2.4.2.profile  
154 https://raw.githubusercontent.com/mhaskar/MalleableC2-Profiles/4432c64effce56134bbcc10836b4d813c09049ac/windows-updates.profile  
155 https://raw.githubusercontent.com/bigb0sss/RedTeam-OffensiveSecurity/0a0a17f31698ab15e62249fca99a4bd1346991e3/01-CobaltStrike/malle  
156 https://raw.githubusercontent.com/federico33385/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/Normal/windows-updat  
157 https://raw.githubusercontent.com/Libraggbond/CS4.0-Malleable-c2-profile/fc6365924077174b33beb7645ce7ba8c1cb8c430/myhttps2.profile  
158 https://raw.githubusercontent.com/lee-c3x/malleable/3fd552e4373c639968f70978f327012873bd38cd/clean\_template.profile  
159 https://raw.githubusercontent.com/threatexpress/malleable-c2/b45e1fce4d7cf46fdd199e1425f9b68b51e81e04/jquery-c2.4.0.profile  
160 https://raw.githubusercontent.com/kphongagsorn/c2-profiles/29fe50eaa655ddd0028fca06a9c7785e3ffaf41/zillow.profile  
161 https://raw.githubusercontent.com/federico33385/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/Normal/msu\_edu.profi  
162 https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/dddad4550180e92eb33275b5167249a74f9a22e0/Normal/jquery-c2.4.2.p  
163 https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/9f1182d7f77339e2587ecc5f3e094e05bef5db20/clean\_template.profile  
164 https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/Normal/windows-updates  
165 https://raw.githubusercontent.com/lee-c3x/malleable/3fd552e4373c639968f70978f327012873bd38cd/msu\_edu.profile  
166 https://raw.githubusercontent.com/federico33385/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/template.profile  
167 https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/1b110729860fd7e6f37aa3e6d04e24e6539f16de/normal/msu\_edu.profile  
168 https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/6a749f0ef99211db3812065f2b24ae023f5bd3dc/Normal/msu\_edu.profile  
169 https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/0ef8cf4556e26f6d4190c56ba697c2159faa5822/crimeware/trick\_ryuk.profil  
170 https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/1b110729860fd7e6f37aa3e6d04e24e6539f16de/crimeware/zloader.profile  
171 https://raw.githubusercontent.com/federico33385/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/Crimeware/covid19\_ko  
172 https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/dddad4550180e92eb33275b5167249a74f9a22e0/Crimeware/trick\_ryuk.p  
173 https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/dddad4550180e92eb33275b5167249a74f9a22e0/Crimeware/zloader.prof  
174 https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/7189deb738d32f073cacb47d27f64443a17d3b42/normal/mscrl.profile  
175 https://raw.githubusercontent.com/yeyintminthuhtut/Malleable-C2-Profiles-Collection/b1dc3b83c018dcbf6b823f9027c928d07949a063/Crimew  
176 https://raw.githubusercontent.com/federico33385/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/Crimeware/jasperload  
177 https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/d4f85a85e047a7e29b2ae3c2b952758d47c3099c/template.profile  
178 https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/6a749f0ef99211db3812065f2b24ae023f5bd3dc/template.profile  
179 https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/1b110729860fd7e6f37aa3e6d04e24e6539f16de/crimeware/covid19\_koadic.pr  
180 https://raw.githubusercontent.com/lee-c3x/malleable/3fd552e4373c639968f70978f327012873bd38cd/jasperloader.profile  
181 https://raw.githubusercontent.com/lee-c3x/malleable/3fd552e4373c639968f70978f327012873bd38cd/template.profile  
182 https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/6a749f0ef99211db3812065f2b24ae023f5bd3dc/Crimeware/covid19\_koad  
183 https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/1b110729860fd7e6f37aa3e6d04e24e6539f16de/crimeware/jasperloader.prof  
184 https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/1b110729860fd7e6f37aa3e6d04e24e6539f16de/crimeware/saefko.profile  
185 https://raw.githubusercontent.com/federico33385/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/Normal/reddit.profil  
186 https://raw.githubusercontent.com/yeyintminthuhtut/Malleable-C2-Profiles-Collection/b1dc3b83c018dcbf6b823f9027c928d07949a063/Social  
187 https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/dddad4550180e92eb33275b5167249a74f9a22e0/Crimeware/saefko.profi  
188 https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/6a749f0ef99211db3812065f2b24ae023f5bd3dc/Crimeware/jasperloader  
189 https://raw.githubusercontent.com/lengjibo/RedTeamTools/134970a01f3c8e525f1ce691ca60b6b122efee3c/windows/Malleable-C2-Profiles/bing  
190 https://raw.githubusercontent.com/federico33385/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/Normal/gotomeeting.p  
191 https://raw.githubusercontent.com/federico33385/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/Normal/office365\_cal  
192 https://raw.githubusercontent.com/federico33385/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/Normal/mayoclinic.pr  
193 https://raw.githubusercontent.com/yeyintminthuhtut/Malleable-C2-Profiles-Collection/b1dc3b83c018dcbf6b823f9027c928d07949a063/Misc/m  
194 https://raw.githubusercontent.com/lee-c3x/malleable/3fd552e4373c639968f70978f327012873bd38cd/reddit.profile  
195 https://raw.githubusercontent.com/guidepointsecurity/RedCommander/f8dc14428886247b322552cc9e7eeffd7e4cea2d/files/custom/HTTPS/evasi  
196 https://raw.githubusercontent.com/guidepointsecurity/RedCommander/f8dc14428886247b322552cc9e7eeffd7e4cea2d/files/custom/DNS/evasive  
197 https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/1b110729860fd7e6f37aa3e6d04e24e6539f16de/normal/reddit.profile  
198 https://raw.githubusercontent.com/lee-c3x/malleable/3fd552e4373c639968f70978f327012873bd38cd/gotomeeting.profile  
199 https://raw.githubusercontent.com/lee-c3x/malleable/3fd552e4373c639968f70978f327012873bd38cd/office365\_calendar.profile  
200 https://raw.githubusercontent.com/federico33385/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/Normal/stackoverflow  
201 https://raw.githubusercontent.com/yeyintminthuhtut/Malleable-C2-Profiles-Collection/b1dc3b83c018dcbf6b823f9027c928d07949a063/Social  
202 https://raw.githubusercontent.com/yeyintminthuhtut/Malleable-C2-Profiles-Collection/b1dc3b83c018dcbf6b823f9027c928d07949a063/Social  
203 https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/6a749f0ef99211db3812065f2b24ae023f5bd3dc/Normal/reddit.profile  
204 https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/1b110729860fd7e6f37aa3e6d04e24e6539f16de/normal/gotomeeting.profile  
205 https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/1b110729860fd7e6f37aa3e6d04e24e6539f16de/normal/office365\_calendar.p



206 [https://raw.githubusercontent.com/federico33385/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/Normal/youtube\\_video](https://raw.githubusercontent.com/federico33385/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/Normal/youtube_video)

207 <https://raw.githubusercontent.com/lee-c3x/malleable/3fd552e4373c639968f70978f327012873bd38cd/mayoclinic.profile>

208 <https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/6a749f0ef99211db3812065f2b24ae023f5bd3dc/Normal/gotomeeting.pro>

209 [https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/6a749f0ef99211db3812065f2b24ae023f5bd3dc/Normal/office365\\_calen](https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/6a749f0ef99211db3812065f2b24ae023f5bd3dc/Normal/office365_calen)

210 [https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/6a749f0ef99211db3812065f2b24ae023f5bd3dc/Normal/office365\\_calen](https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/6a749f0ef99211db3812065f2b24ae023f5bd3dc/Normal/office365_calen)

211 <https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/6a749f0ef99211db3812065f2b24ae023f5bd3dc/Normal/mayoclinic.prof>

212 <https://raw.githubusercontent.com/lee-c3x/malleable/3fd552e4373c639968f70978f327012873bd38cd/slack.profile>

213 <https://raw.githubusercontent.com/lee-c3x/malleable/3fd552e4373c639968f70978f327012873bd38cd/stackoverflow.profile>

214 <https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/1b110729860fd7e6f37aa3e6d04e24e6539f16de/normal/slack.profile>

215 <https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/1b110729860fd7e6f37aa3e6d04e24e6539f16de/normal/stackoverflow.profil>

216 [https://raw.githubusercontent.com/lee-c3x/malleable/3fd552e4373c639968f70978f327012873bd38cd/youtube\\_video.profile](https://raw.githubusercontent.com/lee-c3x/malleable/3fd552e4373c639968f70978f327012873bd38cd/youtube_video.profile)

217 [https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/1b110729860fd7e6f37aa3e6d04e24e6539f16de/normal/youtube\\_video.profil](https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/1b110729860fd7e6f37aa3e6d04e24e6539f16de/normal/youtube_video.profil)

218 <https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/dddad4550180e92eb33275b5167249a74f9a22e0/Normal/slack.profile>

219 <https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/6a749f0ef99211db3812065f2b24ae023f5bd3dc/Normal/stackoverflow.p>

220 [https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/6a749f0ef99211db3812065f2b24ae023f5bd3dc/Normal/youtube\\_video.p](https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/6a749f0ef99211db3812065f2b24ae023f5bd3dc/Normal/youtube_video.p)

221 <https://raw.githubusercontent.com/federico33385/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/Normal/trevor.profil>

222 <https://raw.githubusercontent.com/lee-c3x/malleable/3fd552e4373c639968f70978f327012873bd38cd/trevor.profile>

223 <https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/1b110729860fd7e6f37aa3e6d04e24e6539f16de/normal/trevor.profile>

224 <https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/6a749f0ef99211db3812065f2b24ae023f5bd3dc/Normal/trevor.profile>

225 <https://raw.githubusercontent.com/yeyintminthuhtut/Malleable-C2-Profiles-Collection/b1dc3b83c018dcbf6b823f9027c928d07949a063/Misc/i>

226 <https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/1b110729860fd7e6f37aa3e6d04e24e6539f16de/normal/iheartradio.profile>

227 <https://raw.githubusercontent.com/kphongagsorn/c2-profiles/29fe50eaad655ddd0028fca06a9c7785e3ffaf41/duckduckgo-ramen-search-get-onl>

228 <https://raw.githubusercontent.com/lee-c3x/malleable/3fd552e4373c639968f70978f327012873bd38cd/iheartradio.profile>

229 <https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/dddad4550180e92eb33275b5167249a74f9a22e0/Normal/iheartradio.pro>

230 <https://raw.githubusercontent.com/threatexpress/malleable-c2/b45e1fce4d7cf46fdd199e1425f9b68b51e81e04/jquery-c2.3.14.profile>

231 any spawnto\_x64

232 <https://raw.githubusercontent.com/FortyNorthSecurity/C2concealer/97b807b0af0bc9c5bbea55e62b1b8cfead3caaf6/C2concealer/components/po>

233 <https://raw.githubusercontent.com/Sifter-Ex/cPlug/bbe96a9283c4edeadfd7e1c336338282e3316e26/CSv3/C2concealer/C2concealer/components/>

234 [https://raw.githubusercontent.com/MythicAgents/Apollo/0fa7e11b81d2783ffffeea4fd51e5ab237e92e27/Payload\\_Type/Apollo/agent\\_code/Apoll](https://raw.githubusercontent.com/MythicAgents/Apollo/0fa7e11b81d2783ffffeea4fd51e5ab237e92e27/Payload_Type/Apollo/agent_code/Apoll)

235 <https://raw.githubusercontent.com/MythicAgents/Apollo/7660439cbc8d4f18af2b564a5b7a0ac4f8f3765a/documentation-payload/Apollo/command>

236 <https://raw.githubusercontent.com/kphongagsorn/c2-profiles/29fe50eaad655ddd0028fca06a9c7785e3ffaf41/amazon.profile>

237 [https://raw.githubusercontent.com/MythicAgents/Apollo/0fa7e11b81d2783ffffeea4fd51e5ab237e92e27/Payload\\_Type/Apollo/agent\\_code/Apoll](https://raw.githubusercontent.com/MythicAgents/Apollo/0fa7e11b81d2783ffffeea4fd51e5ab237e92e27/Payload_Type/Apollo/agent_code/Apoll)

238 [https://raw.githubusercontent.com/MythicAgents/Apollo/9ca995fd0a9b7ba155bd58ce5668007443ea28a5/Payload\\_Type/Apollo/mythic/agent\\_fun](https://raw.githubusercontent.com/MythicAgents/Apollo/9ca995fd0a9b7ba155bd58ce5668007443ea28a5/Payload_Type/Apollo/mythic/agent_fun)

239 <https://raw.githubusercontent.com/TheRipperJhon/CAPE/2bc977577a8fcc81a46046fe5bf9248ed3ac0c28/modules/processing/parsers/malwarecon>

240 [https://raw.githubusercontent.com/nsquar3/malware\\_analysis/e7f3070f490bfae7dd80288e609197e7a8a41845/NTripLOL/CobaltStrikeBeacon\\_con](https://raw.githubusercontent.com/nsquar3/malware_analysis/e7f3070f490bfae7dd80288e609197e7a8a41845/NTripLOL/CobaltStrikeBeacon_con)

241 <https://raw.githubusercontent.com/Seccion7/dep-CAPEv2/51fc4ef85c74303060fd0394578fbbf79ac4bfa3/modules/processing/parsers/CAPE/Coba>

242 [https://raw.githubusercontent.com/binref/refinery/1920187f2b29309240f6c4a822748a42df92bc8c/test/units/pattern/test\\_carve\\_json.py](https://raw.githubusercontent.com/binref/refinery/1920187f2b29309240f6c4a822748a42df92bc8c/test/units/pattern/test_carve_json.py)

243 [https://raw.githubusercontent.com/MythicAgents/Apollo/b3c12b6df6fab28321ddfb39d7de770c95341ecd/Payload\\_Type/Apollo/agent\\_code/Apoll](https://raw.githubusercontent.com/MythicAgents/Apollo/b3c12b6df6fab28321ddfb39d7de770c95341ecd/Payload_Type/Apollo/agent_code/Apoll)

244 <https://raw.githubusercontent.com/kvcallfield/Cobalt-Strike-C2-profiles/cae44634d57c0d8a099e50f6d4e9b73acaab9d6/amazon2.profile>

245 <https://raw.githubusercontent.com/MythicAgents/Apollo/7660439cbc8d4f18af2b564a5b7a0ac4f8f3765a/documentation-payload/Apollo/opsec.m>

246 <https://raw.githubusercontent.com/k-vitali/Malware-Misc-RE/4b9b81e822c5b03a8733153727ed3e3238cf4201/2019-06-23-cobalt-strike-beacon>

247 <https://raw.githubusercontent.com/MythicAgents/Apollo/7660439cbc8d4f18af2b564a5b7a0ac4f8f3765a/documentation-payload/Apollo/command>

248 <https://raw.githubusercontent.com/webcoderz/agressor-scripts-/950064776853cf4dd7403d0f75b5306fe275fcc3/Malleable-C2-Profiles-master>

249 <https://raw.githubusercontent.com/bluscreenofjeff/Malleable-C2-Randomizer/eec7300949ae70b3dcfd4d95a29bdbb6a88be1651/malleable-c2-ran>

250 [https://raw.githubusercontent.com/AmnestyTech/investigations/215c9c8077edc9ac30d20f0fe6b42adb14f7384b/2020-09-25\\_finfisher/scripts/](https://raw.githubusercontent.com/AmnestyTech/investigations/215c9c8077edc9ac30d20f0fe6b42adb14f7384b/2020-09-25_finfisher/scripts/)

251 <https://raw.githubusercontent.com/KevinCooper/24AF-CyberChallenge/67f531777f7912c7129f633f43e06fba79c5f3e2/CobaltStrike/cobalt.prof>

252 <https://raw.githubusercontent.com/webcoderz/agressor-scripts-/950064776853cf4dd7403d0f75b5306fe275fcc3/Malleable-C2-Profiles-master>

253 <https://raw.githubusercontent.com/f1h0/CobStrike/4dccc4759cc9666140baf0d08fedce38147ebcc5/src/main/java/beacon/BeaconPayload.java>

254 <https://raw.githubusercontent.com/hadesangel/Malleable-C2-Profiles/390937aec01e0bcdaf23312277e96e57ac925f7b/APT/meterpreter.profile>

255 <https://raw.githubusercontent.com/ianxtianxt/Malleable-C2-Profiles/07fd3b45c4166c9aecdca54cddc905c22f6ff85/APT/meterpreter.profile>

256 <https://raw.githubusercontent.com/seclib/Malleable-C2-Profiles/390937aec01e0bcdaf23312277e96e57ac925f7b/APT/meterpreter.profile>

257 <https://raw.githubusercontent.com/f1h0/CobStrike/4dccc4759cc9666140baf0d08fedce38147ebcc5/src/main/java/c2profile/Lint.java>

258 <https://raw.githubusercontent.com/m0xbf/cs4-clone/4dccc4759cc9666140baf0d08fedce38147ebcc5/src/main/java/beacon/BeaconPayload.java>

259 <https://raw.githubusercontent.com/rsmudge/Malleable-C2-Profiles/390937aec01e0bcdaf23312277e96e57ac925f7b/APT/meterpreter.profile>

260 <https://raw.githubusercontent.com/mez-0/malleable-requests/ab2fbd2e311bee4bbb76adb2586abb8f23c37b9/README.md>

261 <https://raw.githubusercontent.com/k-vitali/Malware-Misc-RE/4b9b81e822c5b03a8733153727ed3e3238cf4201/2020-05-12-shadowdev-cobaltstri>

262 <https://raw.githubusercontent.com/m0xbf/cs4-clone/4dccc4759cc9666140baf0d08fedce38147ebcc5/src/main/java/c2profile/Lint.java>

263 <https://raw.githubusercontent.com/f1h0/CobStrike/4dccc4759cc9666140baf0d08fedce38147ebcc5/src/main/java/beacon/setup/SSHAgent.java>

264 [https://raw.githubusercontent.com/sysopfb/open\\_mal\\_analysis\\_notes/daa85b917ae55f2b827e81498d802cdc6dfa9956/f8c94e76f4d756924bf929b3](https://raw.githubusercontent.com/sysopfb/open_mal_analysis_notes/daa85b917ae55f2b827e81498d802cdc6dfa9956/f8c94e76f4d756924bf929b3)

265 [https://raw.githubusercontent.com/Te-k/analyst-scripts/40fe46359b56cfc171c7fdae452796ab7195ac27/threats/cobaltstrike\\_config.py](https://raw.githubusercontent.com/Te-k/analyst-scripts/40fe46359b56cfc171c7fdae452796ab7195ac27/threats/cobaltstrike_config.py)

266 <https://raw.githubusercontent.com/mhaskar/MalleableC2-Profiles/4432c64effce56134bbcc10836b4d813c09049ac/windows-updates.profile>

267 <https://raw.githubusercontent.com/m0xbf/cs4-clone/4dccc4759cc9666140baf0d08fedce38147ebcc5/src/main/java/beacon/setup/SSHAgent.java>

268 <https://raw.githubusercontent.com/hattmo/c2profilejs/c279a522a65a34c866419e07917858ff056f0c09/src/client/formDescription/profileDes>

269 [https://raw.githubusercontent.com/MythicAgents/Apollo/15b0bf56c7343b0a9c5dced74bfc1bfc6f0dd2e0/Payload\\_Type/Apollo/mythic/agent\\_fun](https://raw.githubusercontent.com/MythicAgents/Apollo/15b0bf56c7343b0a9c5dced74bfc1bfc6f0dd2e0/Payload_Type/Apollo/mythic/agent_fun)

270 <https://raw.githubusercontent.com/lee-c3x/malleable/3fd552e4373c639968f70978f327012873bd38cd/lee-malleable-skeleton.profile>

271 <https://raw.githubusercontent.com/yeyintminthuhtut/Malleable-C2-Profiles-Collection/b1dc3b83c018dcbf6b823f9027c928d07949a063/APT/me>

272 <https://raw.githubusercontent.com/Te-k/cobaltstrike/b5fb9c8919ce5e59b4d0f0b962a72e759295bd0c/lib.py>

273 <https://raw.githubusercontent.com/federico33385/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/APT/meterpreter.prof>

274 <https://raw.githubusercontent.com/f1h0/CobStrike/4dccc4759cc9666140baf0d08fedce38147ebcc5/src/main/java/c2profile/Loader.java>

275 <https://raw.githubusercontent.com/yeyintminthuhtut/Malleable-C2-Profiles-Collection/b1dc3b83c018dcbf6b823f9027c928d07949a063/APT/ch>

276 <https://raw.githubusercontent.com/yeyintminthuhtut/Malleable-C2-Profiles-Collection/b1dc3b83c018dcbf6b823f9027c928d07949a063/Crimew>

277 [https://raw.githubusercontent.com/federico33385/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/APT/chches\\_APT10.pro](https://raw.githubusercontent.com/federico33385/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/APT/chches_APT10.pro)

278 <https://raw.githubusercontent.com/federico33385/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/Crimeware/jasperload>

279 <https://raw.githubusercontent.com/R-Vision/rvision-hackathon-2021-q1/09c0d7d468a3fc6ec3af9c8dc8384335c5119d05/converted/2020/Target>

280 https://raw.githubusercontent.com/ctxis/CAPE/0d830d3cdc241901a9ec1e2a6bfc59eb2f202551/modules/processing/parsers/malwareconfig/Coba  
281 https://raw.githubusercontent.com/m0xbf/cs4-clone/4dccc4759cc9666140baf0d08fedce38147ebcc5/src/main/java/c2profile/Loader.java  
282 https://raw.githubusercontent.com/Apr4h/CobaltStrikeConfigParser/d82b4e3369f7b41fbd0b67ee1170332a9d6f4a82/Beacon.cs  
283 https://raw.githubusercontent.com/MythicAgents/Apollo/4a67230f370c7da83756cb28149363169dc7211e/README.md  
284 https://raw.githubusercontent.com/lee-c3x/malleable/3fd552e4373c639968f70978f327012873bd38cd/meterpreter.profile  
285 https://raw.githubusercontent.com/sysopfb/malware\_decoders/638fde09e60301a078923052d2537b0c33e32ca4/cs\_beacon/proper\_beacon\_decoder  
286 https://raw.githubusercontent.com/federico33385/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/Normal/windows-updat  
287 https://raw.githubusercontent.com/lee-c3x/malleable/3fd552e4373c639968f70978f327012873bd38cd/clean\_template.profile  
288 https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/6a749f0ef99211db3812065f2b24ae023f5bd3dc/APT/meterpreter.profil  
289 https://raw.githubusercontent.com/Apr4h/CobaltStrikeScan/6730a4d61d0d686a0e1e4736768f3210995d4803/CobaltStrikeConfigParser/Beacon.c  
290 https://raw.githubusercontent.com/JPCERTCC/MalConfScan/00a0b82e6eeec1ca2c741e604a9fc5a633ffe4c8/utils/cobaltstrikescan.py  
291 https://raw.githubusercontent.com/lee-c3x/malleable/3fd552e4373c639968f70978f327012873bd38cd/chches\_APT10.profile  
292 https://raw.githubusercontent.com/lee-c3x/malleable/3fd552e4373c639968f70978f327012873bd38cd/jasperloader.profile  
293 https://raw.githubusercontent.com/korney3/ARES\_RVision\_Hack/8a4630baa809885bad15a39e0f60a0e0831bbc3e/data/raw/2020/Targeted%20Attac  
294 https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/1b110729860fd7e6f37aa3e6d04e24e6539f16de/APT/chches\_APT10.profile  
295 https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/1b110729860fd7e6f37aa3e6d04e24e6539f16de/crimeware/jasperloader.prof  
296 https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/1b110729860fd7e6f37aa3e6d04e24e6539f16de/crimeware/saefko.profile  
297 https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/dddad4550180e92eb33275b5167249a74f9a22e0/Crimeware/saefko.profi  
298 https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/6a749f0ef99211db3812065f2b24ae023f5bd3dc/APT/chches\_APT10.profi  
299 https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/6a749f0ef99211db3812065f2b24ae023f5bd3dc/Crimeware/jasperloader  
300 https://raw.githubusercontent.com/ION28/BLUESPAWN/be2f0354f02a8d13abd8de357cbb89b3b6bc604c/BLUESPAWN-win-client/src/util/processes/  
301 https://raw.githubusercontent.com/yeyintminthuhtut/Malleable-C2-Profiles-Collection/b1dc3b83c018dcbf6b823f9027c928d07949a063/Social  
302 https://raw.githubusercontent.com/federico33385/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/Normal/reddit.profil  
303 https://raw.githubusercontent.com/JPCERTCC/aa-tools/404eceb256447e51c476a61e461c5cf386d50d16/cobaltstrikescan.py  
304 https://raw.githubusercontent.com/federico33385/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/Normal/gotomeeting.p  
305 https://raw.githubusercontent.com/federico33385/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/Normal/msu\_edu.profi  
306 https://raw.githubusercontent.com/federico33385/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/Normal/office365\_cal  
307 https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/Normal/windows-updates  
308 https://raw.githubusercontent.com/yeyintminthuhtut/Malleable-C2-Profiles-Collection/b1dc3b83c018dcbf6b823f9027c928d07949a063/Misc/m  
309 https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/9f1182d7f77339e2587ecc5f3e094e05bef5db20/clean\_template.profile  
310 https://raw.githubusercontent.com/federico33385/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/Normal/mayoclinic.pr  
311 https://raw.githubusercontent.com/guidepointsecurity/RedCommander/f8dc14428886247b322552cc9e7eeffd7e4cea2d/files/custom/HTTPS/evasi  
312 https://raw.githubusercontent.com/guidepointsecurity/RedCommander/f8dc14428886247b322552cc9e7eeffd7e4cea2d/files/custom/DNS/evasive  
313 https://raw.githubusercontent.com/Spacial/awesome-csirt/69449dd9181e490a04bd24bb9d4179d2681aabe9/scripts/grab\_beacon\_config.nse  
314 https://raw.githubusercontent.com/rsmudge/Malleable-C2-Profiles/26323784672913923d20c5a638c6ca79459e8529/normal/reference.profile  
315 https://raw.githubusercontent.com/lee-c3x/malleable/3fd552e4373c639968f70978f327012873bd38cd/reddit.profile  
316 https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/1b110729860fd7e6f37aa3e6d04e24e6539f16de/normal/reddit.profile  
317 https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/6a749f0ef99211db3812065f2b24ae023f5bd3dc/Normal/reddit.profile  
318 https://raw.githubusercontent.com/yeyintminthuhtut/Malleable-C2-Profiles-Collection/b1dc3b83c018dcbf6b823f9027c928d07949a063/Social  
319 https://raw.githubusercontent.com/yeyintminthuhtut/Malleable-C2-Profiles-Collection/b1dc3b83c018dcbf6b823f9027c928d07949a063/Social  
320 https://raw.githubusercontent.com/federico33385/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/Normal/stackoverflow  
321 https://raw.githubusercontent.com/lee-c3x/malleable/3fd552e4373c639968f70978f327012873bd38cd/gotomeeting.profile  
322 https://raw.githubusercontent.com/lee-c3x/malleable/3fd552e4373c639968f70978f327012873bd38cd/msu\_edu.profile  
323 https://raw.githubusercontent.com/lee-c3x/malleable/3fd552e4373c639968f70978f327012873bd38cd/office365\_calendar.profile  
324 https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/1b110729860fd7e6f37aa3e6d04e24e6539f16de/normal/gotomeeting.profile  
325 https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/1b110729860fd7e6f37aa3e6d04e24e6539f16de/normal/msu\_edu.profile  
326 https://raw.githubusercontent.com/xx0hcd/Malleable-C2-Profiles/1b110729860fd7e6f37aa3e6d04e24e6539f16de/normal/office365\_calendar.p  
327 https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/6a749f0ef99211db3812065f2b24ae023f5bd3dc/Normal/gotomeeting.pro  
328 https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/6a749f0ef99211db3812065f2b24ae023f5bd3dc/Normal/msu\_edu.profile  
329 https://raw.githubusercontent.com/BC-SECURITY/Malleable-C2-Profiles/6a749f0ef99211db3812065f2b24ae023f5bd3dc/Normal/office365\_calen  
330 https://raw.githubusercontent.com/federico33385/Malleable-C2-Profiles/7b97eb61dc014193c4abbc4853914d268aebe72c/Normal/youtube\_video  
331 https://raw.githubusercontent.com/aleenzz/Cobalt\_Strike\_wiki/a47e592bdd6562cb74cc3308e6801593901c97aa/3-%E7%AC%AC%E4%BA%8C%E8%8A%82%



MHaggis commented on Feb 8, 2021

Author ...

Spawnto:

```
amazon.profile:175:    #set spawnto_x86 "%windir%\syswow64\gpresult.exe";
amazon.profile:176:    #set spawnto_x64 "%windir%\sysnative\gpresult.exe";
amazon.profile:178:    #set spawnto_x86 "%windir%\syswow64\svchost.exe -k netsvcs";
amazon.profile:179:    #set spawnto_x64 "%windir%\sysnative\svchost.exe -k netsvcs";
amazon.profile:181:    set spawnto_x86 "%windir%\syswow64\FlashPlayerApp.exe";
amazon.profile:182:    set spawnto_x64 "C:\\Program Files (x86)\\Google\\Chrome\\Application\\chrome.exe";
amazon.profile:184:    #set spawnto_x86 "C:\\Program Files (x86)\\Microsoft Office\\Office16\\excelcnv.exe";
amazon.profile:185:    #set spawnto_x64 "C:\\Program Files\\Mozilla Firefox\\firefox.exe";
amazon2.profile:85:    set spawnto_x86 "%windir%\syswow64\svchost.exe -k netsvcs";
amazon2.profile:86:    set spawnto_x64 "C:\\Program Files (x86)\\Google\\Chrome\\Application\\chrome.exe";
chches_APT10.profile:133:set spawnto_x86 "%windir%\syswow64\reg.exe";
chches_APT10.profile:134:set spawnto_x64 "%windir%\sysnative\reg.exe";
clean_template.profile:352:    set spawnto_x86 "%windir%\syswow64\gpupdate.exe";
clean_template.profile:353:    set spawnto_x64 "%windir%\sysnative\gpupdate.exe";
cobalt.profile:117:##    spawnto_x86:    %windir%\syswow64\rundll32.exe
cobalt.profile:118:##    spawnto_x64:    %windir%\sysnative\rundll32.exe
cobalt.profile:130:set spawnto_x86 "%windir%\syswow64\svchost.exe -k netsvcs";
cobalt.profile:131:set spawnto_x64 "%windir%\sysnative\svchost.exe -k netsvcs";
covid19_koadic.profile:353:    set spawnto_x86 "%windir%\syswow64\rundll32.exe";
```

```
covid19_koadic.profile:354:    set spawnnto_x64 "%windir%\sysnative\rundll32.exe";
CS4.0_guideline.profile:311:    set spawnnto_x86 "%windir%\syswow64\<mfpmp>.exe";                                # Do not
specify %windir%\system32 or c:\windows\system32 directly
CS4.0_guideline.profile:312:    set spawnnto_x64 "%windir%\sysnative\<mfpmp>.exe";                                # Do not
specify %windir%\system32 or c:\windows\system32 directly
duckduckgo-ramen-search-get-only.profile:13:set spawnnto_x86 "%windir%\syswow64\gpresult.exe";
duckduckgo-ramen-search-get-only.profile:14:set spawnnto_x64 "%windir%\sysnative\gpupdate.exe";
evasive.profile:176:    set spawnnto_x86 "%windir%\syswow64\WUAUCLT.exe";
evasive.profile:177:    set spawnnto_x64 "%windir%\sysnative\WUAUCLT.exe";
gotomeeting.profile:174:    set spawnnto_x86 "%windir%\syswow64\gpupdate.exe";
gotomeeting.profile:175:    set spawnnto_x64 "%windir%\sysnative\gpupdate.exe";
iheartradio.profile:212:    set spawnnto_x86 "%windir%\syswow64\gpupdate.exe";
iheartradio.profile:213:    set spawnnto_x64 "%windir%\sysnative\gpupdate.exe";
jasperloader.profile:143:    set spawnnto_x86 "%windir%\syswow64\wscript.exe";
jasperloader.profile:144:    set spawnnto_x64 "%windir%\sysnative\wscript.exe";
jquery-c2.3.11.profile:116:##    spawnnto_x86:    %windir%\syswow64\rundll32.exe
jquery-c2.3.11.profile:117:##    spawnnto_x64:    %windir%\sysnative\rundll32.exe
jquery-c2.3.11.profile:129:set spawnnto_x86 "%windir%\syswow64\svchost.exe -k netsvcs";
jquery-c2.3.11.profile:130:set spawnnto_x64 "%windir%\sysnative\svchost.exe -k netsvcs";
jquery-c2.3.12.profile:116:##    spawnnto_x86:    %windir%\syswow64\rundll32.exe
jquery-c2.3.12.profile:117:##    spawnnto_x64:    %windir%\sysnative\rundll32.exe
jquery-c2.3.12.profile:129:set spawnnto_x86 "%windir%\syswow64\svchost.exe -k netsvcs";
jquery-c2.3.12.profile:130:set spawnnto_x64 "%windir%\sysnative\svchost.exe -k netsvcs";
jquery-c2.3.13.profile:133:##    spawnnto_x86:    %windir%\syswow64\rundll32.exe
jquery-c2.3.13.profile:134:##    spawnnto_x64:    %windir%\sysnative\rundll32.exe
jquery-c2.3.13.profile:147:set spawnnto_x86 "%windir%\syswow64\svchost.exe -k netsvcs";
jquery-c2.3.13.profile:148:set spawnnto_x64 "%windir%\sysnative\svchost.exe -k netsvcs";
jquery-c2.3.14.profile:131:##    spawnnto_x86:    %windir%\syswow64\rundll32.exe
jquery-c2.3.14.profile:132:##    spawnnto_x64:    %windir%\sysnative\rundll32.exe
jquery-c2.3.14.profile:146:##        - set spawnnto_x86 "%windir%\syswow64\svchost.exe -k netsvcs";
jquery-c2.3.14.profile:147:##        - set spawnnto_x64 "%windir%\sysnative\svchost.exe -k netsvcs";
jquery-c2.3.14.profile:152:    set spawnnto_x86 "%windir%\syswow64\dlhhost.exe";
jquery-c2.3.14.profile:153:    set spawnnto_x64 "%windir%\sysnative\dlhhost.exe";
jquery-c2.4.0.profile:117:##    spawnnto_x86:    %windir%\syswow64\rundll32.exe
jquery-c2.4.0.profile:118:##    spawnnto_x64:    %windir%\sysnative\rundll32.exe
jquery-c2.4.0.profile:135:##        - set spawnnto_x86 "%windir%\syswow64\svchost.exe -k netsvcs";
jquery-c2.4.0.profile:136:##        - set spawnnto_x64 "%windir%\sysnative\svchost.exe -k netsvcs";
jquery-c2.4.0.profile:144:    set spawnnto_x86 "%windir%\syswow64\dlhhost.exe";
jquery-c2.4.0.profile:146:    set spawnnto_x64 "%windir%\sysnative\dlhhost.exe";
jquery-c2.4.2.profile:257:##    spawnnto_x86    %windir%\syswow64\rundll32.exe
jquery-c2.4.2.profile:258:##    spawnnto_x64    %windir%\sysnative\rundll32.exe
jquery-c2.4.2.profile:278:##        - set spawnnto_x86 "%windir%\syswow64\svchost.exe -k netsvcs";
jquery-c2.4.2.profile:279:##        - set spawnnto_x64 "%windir%\sysnative\svchost.exe -k netsvcs";
jquery-c2.4.2.profile:287:    set spawnnto_x86 "%windir%\syswow64\dlhhost.exe";
jquery-c2.4.2.profile:289:    set spawnnto_x64 "%windir%\sysnative\dlhhost.exe";
lee-malleable-skeleton.profile:16:set spawnnto_x86 "%windir%\syswow64\calc.exe";
lee-malleable-skeleton.profile:17:set spawnnto_x64 "%windir%\sysnative\notepad.exe";
mayoclinic.profile:148:    set spawnnto_x86 "%windir%\syswow64\gpupdate.exe";
mayoclinic.profile:149:    set spawnnto_x64 "%windir%\sysnative\gpupdate.exe";
meterpreter.profile:13:set spawnnto_x86 "%windir%\syswow64\notepad.exe";
meterpreter.profile:14:set spawnnto_x64 "%windir%\sysnative\notepad.exe";
mscrl.profile:344:    set spawnnto_x86 "%windir%\syswow64\gpupdate.exe";
mscrl.profile:345:    set spawnnto_x64 "%windir%\sysnative\gpupdate.exe";
msu_edu.profile:293:    set spawnnto_x86 "%windir%\syswow64\gpupdate.exe";
msu_edu.profile:294:    set spawnnto_x64 "%windir%\sysnative\gpupdate.exe";
myhttpsc2.profile:501:    set spawnnto_x86 "%windir%\syswow64\gpupdate.exe";
myhttpsc2.profile:502:    set spawnnto_x64 "%windir%\sysnative\gpupdate.exe";
office365_calendar.profile:158:    set spawnnto_x86 "%windir%\syswow64\gpupdate.exe";
office365_calendar.profile:159:    set spawnnto_x64 "%windir%\sysnative\gpupdate.exe";
reddit.profile:149:    set spawnnto_x86 "%windir%\syswow64\gpupdate.exe";
reddit.profile:150:    set spawnnto_x64 "%windir%\sysnative\gpupdate.exe";
reference.profile:308:    set spawnnto_x86 "%windir%\syswow64\WerFault.exe";
reference.profile:309:    set spawnnto_x64 "%windir%\sysnative\WerFault.exe";
saefko.profile:134:    set spawnnto_x86 "%windir%\syswow64\wscript.exe";
saefko.profile:135:    set spawnnto_x64 "%windir%\sysnative\wscript.exe";
slack.profile:211:    set spawnnto_x86 "%windir%\syswow64\gpupdate.exe";
slack.profile:212:    set spawnnto_x64 "%windir%\sysnative\gpupdate.exe";
stackoverflow.profile:196:    set spawnnto_x86 "%windir%\syswow64\gpupdate.exe";
stackoverflow.profile:197:    set spawnnto_x64 "%windir%\sysnative\gpupdate.exe";
template.profile:519:    set spawnnto_x86 "%windir%\syswow64\gpupdate.exe";
template.profile:520:    set spawnnto_x64 "%windir%\sysnative\gpupdate.exe";
trevor.profile:165:    set spawnnto_x86 "%windir%\syswow64\gpupdate.exe";
trevor.profile:166:    set spawnnto_x64 "%windir%\sysnative\gpupdate.exe";
trick_ryuk.profile:368:    set spawnnto_x86 "%windir%\syswow64\gpupdate.exe";
trick_ryuk.profile:369:    set spawnnto_x64 "%windir%\sysnative\gpupdate.exe";
windows-updates.profile:72:    set spawnnto_x86 "%windir%\syswow64\wusa.exe";
windows-updates.profile:75:    set spawnnto_x64 "%windir%\sysnative\wusa.exe";
youtube_video.profile:177:    set spawnnto_x86 "%windir%\syswow64\gpupdate.exe";
youtube_video.profile:178:    set spawnnto_x64 "%windir%\sysnative\gpupdate.exe";
zillow.profile:172:    set spawnnto_x86 "%windir%\syswow64\gpresult.exe";
zillow.profile:173:    set spawnnto_x64 "%windir%\sysnative\gpresult.exe";
zloader.profile:355:    set spawnnto_x86 "%windir%\syswow64\explorer.exe";
zloader.profile:356:    set spawnnto_x64 "%windir%\sysnative\explorer.exe";
```





MHaggis commented on Feb 8, 2021

Author ...

Pipes:

```
bing.profile:68:set pipename "win_svc";
bing.profile:69:set pipename_stager "win_svc";
clean_template.profile:24:set pipename "ntsvcs##";
clean_template.profile:25:set pipename_stager "scerpc##";
clean_template.profile:34:set ssh_pipename "SearchTextHarvester##";
clean_template.profile:363:  set pipename "DserNamePipe##";
cobalt.profile:139:##    pipename: msagent_##
cobalt.profile:140:##    pipename_stager: status_##
cobalt.profile:142:##    - Do not use an existing namedpipe, Beacon doesn't check for conflict!
cobalt.profile:145:#set pipename      "wkssvc_##";
cobalt.profile:146:#set pipename_stager "spoolss_##";
cobalt.profile:147:set pipename      "mojo.5688.8052.183894939787088877##"; # Common Chrome named pipe
cobalt.profile:148:set pipename_stager "mojo.5688.8052.35780273329370473##"; # Common Chrome named pipe
covid19_koadic.profile:27:set pipename "ntsvcs";
covid19_koadic.profile:28:set pipename_stager "scerpc";
CS4.0_guideline.profile:36:set pipename "<win_svc+8546>";          # Name of pipe to use for SMB beacon's peer-to-peer
communication
CS4.0_guideline.profile:37:set pipename_stager "<win_svc+8546>";    # Name of pipe to use for SMB beacon's named pipe
stager
evasive.profile:19:set pipename "fullduplex_##";
evasive.profile:20:set pipename_stager "rpc_##";
havex.profile:21:set pipename "mypipe-f##";
havex.profile:22:set pipename_stager "mypipe-h##";
jquery-c2.3.11.profile:138:##    pipename: msagent_##
jquery-c2.3.11.profile:139:##    pipename_stager: status_##
jquery-c2.3.11.profile:141:##    - Do not use an existing namedpipe, Beacon doesn't check for conflict!
jquery-c2.3.11.profile:144:#set pipename      "wkssvc_##";
jquery-c2.3.11.profile:145:#set pipename_stager "spoolss_##";
jquery-c2.3.11.profile:146:set pipename      "mojo.5688.8052.183894939787088877##"; # Common Chrome named pipe
jquery-c2.3.11.profile:147:set pipename_stager "mojo.5688.8052.35780273329370473##"; # Common Chrome named pipe
jquery-c2.3.12.profile:138:##    pipename: msagent_##
jquery-c2.3.12.profile:139:##    pipename_stager: status_##
jquery-c2.3.12.profile:141:##    - Do not use an existing namedpipe, Beacon doesn't check for conflict!
jquery-c2.3.12.profile:144:#set pipename      "wkssvc_##";
jquery-c2.3.12.profile:145:#set pipename_stager "spoolss_##";
jquery-c2.3.12.profile:146:set pipename      "mojo.5688.8052.183894939787088877##"; # Common Chrome named pipe
jquery-c2.3.12.profile:147:set pipename_stager "mojo.5688.8052.35780273329370473##"; # Common Chrome named pipe
jquery-c2.3.13.profile:171:##    pipename: msagent_##
jquery-c2.3.13.profile:172:##    pipename_stager: status_##
jquery-c2.3.13.profile:174:##    - Do not use an existing namedpipe, Beacon doesn't check for conflict!
jquery-c2.3.13.profile:177:#set pipename      "wkssvc_##";
jquery-c2.3.13.profile:178:#set pipename_stager "spoolss_##";
jquery-c2.3.13.profile:179:set pipename      "mojo.5688.8052.183894939787088877##"; # Common Chrome named pipe
jquery-c2.3.13.profile:180:set pipename_stager "mojo.5688.8052.35780273329370473##"; # Common Chrome named pipe
jquery-c2.3.14.profile:177:##    pipename: msagent_##
jquery-c2.3.14.profile:178:##    pipename_stager: status_##
jquery-c2.3.14.profile:180:##    - Do not use an existing namedpipe, Beacon doesn't check for conflict!
jquery-c2.3.14.profile:183:#set pipename      "wkssvc_##";
jquery-c2.3.14.profile:184:#set pipename_stager "spoolss_##";
jquery-c2.3.14.profile:185:set pipename      "mojo.5688.8052.183894939787088877##"; # Common Chrome named pipe
jquery-c2.3.14.profile:186:set pipename_stager "mojo.5688.8052.35780273329370473##"; # Common Chrome named pipe
jquery-c2.4.0.profile:177:##    pipename: msagent_##
jquery-c2.4.0.profile:178:##    pipename_stager: status_##
jquery-c2.4.0.profile:180:##    - Do not use an existing namedpipe, Beacon doesn't check for conflict!
jquery-c2.4.0.profile:183:set pipename      "mojo.5688.8052.183894939787088877##"; # Common Chrome named pipe
jquery-c2.4.0.profile:184:set pipename_stager "mojo.5688.8052.35780273329370473##"; # Common Chrome named pipe
jquery-c2.4.2.profile:154:##    pipename: msagent_##
jquery-c2.4.2.profile:155:##    pipename_stager: status_##
jquery-c2.4.2.profile:158:##    - Do not use an existing namedpipe, Beacon doesn't check for conflict!
jquery-c2.4.2.profile:161:set pipename      "mojo.5688.8052.183894939787088877##"; # Common Chrome named pipe
jquery-c2.4.2.profile:162:set pipename_stager "mojo.5688.8052.35780273329370473##"; # Common Chrome named pipe
jquery-c2.4.2.profile:197:set ssh_pipename      "wkssvc##";
jquery-c2.4.2.profile:260:##    pipename      postex_####, windows\\pipe_##          CS 4.2 - Change the named pipe
names used, by post-ex DLLs, to send output back to Beacon. This option accepts a comma-separated list of pipenames. Cobalt
Strike will select a random pipe name from this option when it sets up a post-exploitation job. Each # in the pipename is
replaced with a valid hex character as well.
jquery-c2.4.2.profile:296:  # Modify our post-ex pipe names
jquery-c2.4.2.profile:297:  set pipename "Winsock2\\CatalogChangeListener-###-0,";
lee-malleable-skeleton.profile:19:set pipename "demoagent_11";
lee-malleable-skeleton.profile:20:set pipename_stager "demoagent_22";
meterpreter.profile:39: stringw "pipe";
meterpreter.profile:41: stringw "pipe";
meterpreter.profile:42: stringw "\\\\"%s\\pipe\\"%s";
mscrl.profile:23:set pipename "ntsvcs##";
mscrl.profile:24:set pipename_stager "scerpc##";
mscrl.profile:32:set ssh_pipename "SearchTextHarvester##";
mscrl.profile:354:  set pipename "DserNamePipe##, PGMessagePipe##, MsFteWds##";
msu_edu.profile:23:set pipename "ntsvcs";
```

```
msu_edu.profile:24:set pipename_stager "scerpc";
myhttpsc2.profile:28:#use different strings for pipename and pipename_stager.
myhttpsc2.profile:29:set pipename "ntsvcs";
myhttpsc2.profile:30:set pipename_stager "scerpc";
reference.profile:19:set pipename "msagent_###"; #Default name of pipe to use for SMB Beacon's peer-to-peer communication.
Each # is replaced witha random hex value.
reference.profile:20:set pipename_stager "status_##";
reference.profile:25:set ssh_pipename "postex_ssh_####";
reference.profile:312:    # change our post-ex output named pipe names...
reference.profile:313:    set pipename "msrpc_####, win\\msrpc_##";
template.profile:28:#use different strings for pipename and pipename_stager.
template.profile:29:set pipename "ntsvcs##";
template.profile:30:set pipename_stager "scerpc##";
template.profile:39:set ssh_pipename "SearchTextHarvester##";
template.profile:530:    set pipename "DserNamePipe##";
trick_ryuk.profile:26:set pipename "ntsvcs##";
trick_ryuk.profile:27:set pipename_stager "scerpc##";
trick_ryuk.profile:34:set ssh_pipename "SearchTextHarvester##";
trick_ryuk.profile:379:    set pipename "DserNamePipe##";
windows-updates.profile:90:set pipename          "windows.update.manager##";
windows-updates.profile:91:set pipename_stager    "windows.update.manager###";
zillow.profile:18:# SMB pipe settings
zillow.profile:19:set pipename    "f4c3##";
zillow.profile:20:set pipename_stager    "f53f##";
zloader.profile:26:set pipename "ntsvcs";
zloader.profile:27:set pipename_stager "scerpc";
```



MHaggis commented on Feb 8, 2021

Author ...

Compile time:

```
amazon.profile:108:    set compile_time    "25 Oct 2019 13:10:50";
chches_APT10.profile:139:    set compile_time    "23 Nov 2016 19:31:37";
clean_template.profile:272:    set compile_time    "25 Oct 2016 01:57:23";
covid19_koadic.profile:274:    set compile_time    "04 Mar 2020 17:56:00";
CS4_0_guideline.profile:223:    set compile_time    "<02 April 2020 02:35:00>";    # The build time in Beacon's PE header
evasive.profile:137:    set compile_time    "31 Jan 2020 21:37:17";
gotomeeting.profile:189:    set compile_time    "25 Oct 2016 01:57:23";
havex.profile:28:    set compile_time    "30 Dec 2013 07:53:48";
iheartradio.profile:227:    set compile_time    "25 Oct 2016 01:57:23";
jasperloader.profile:157:    set compile_time    "15 Apr 2015 01:24:00";
jquery-c2.3.11.profile:225:##    compile_time        14 July 2009 8:14:00        The build time in Beacon's PE header
jquery-c2.3.11.profile:250:    set compile_time    "11 Nov 2016 04:08:32";
jquery-c2.3.12.profile:225:##    compile_time        14 July 2009 8:14:00        The build time in Beacon's PE header
jquery-c2.3.12.profile:252:    set compile_time    "11 Nov 2016 04:08:32";
jquery-c2.3.13.profile:260:##    compile_time        14 July 2009 8:14:00        The build time in Beacon's PE header
jquery-c2.3.13.profile:287:    set compile_time    "11 Nov 2016 04:08:32";
jquery-c2.3.14.profile:266:##    compile_time        14 July 2009 8:14:00        The build time in Beacon's PE header
jquery-c2.3.14.profile:293:    set compile_time    "11 Nov 2016 04:08:32";
jquery-c2.4.0.profile:266:##    compile_time        14 July 2009 8:14:00        The build time in Beacon's PE header
jquery-c2.4.0.profile:295:    set compile_time    "11 Nov 2016 04:08:32";
jquery-c2.4.2.profile:311:##    compile_time        14 July 2009 8:14:00        The build time in Beacon's PE header
jquery-c2.4.2.profile:352:    set compile_time    "11 Nov 2016 04:08:32";
lee-malleable-skeleton.profile:29:    set compile_time    "10 November 2010 10:10:10";
mayoclinic.profile:163:    set compile_time    "25 Oct 2016 01:57:23";
meterpreter.profile:26: set compile_time    "08 May 2017 23:13:38";
mscrl.profile:263:    set compile_time    "17 Oct 2020 04:32:14";
msu_edu.profile:229:    set compile_time    "23 Nov 2018 02:25:37";
myhttpsc2.profile:405:    set compile_time    "25 Oct 2016 01:57:23";
office365_calendar.profile:173:    set compile_time    "25 Oct 2016 01:57:23";
reddit.profile:164:    set compile_time    "25 Oct 2016 01:57:23";
reference.profile:270:    set compile_time    "14 Jul 2018 8:14:00";
saefko.profile:148:    set compile_time    "12 Feb 2019 14:33:03";
slack.profile:226:    set compile_time    "25 Oct 2016 01:57:23";
stackoverflow.profile:211:    set compile_time    "25 Oct 2016 01:57:23";
template.profile:412:    set compile_time    "25 Oct 2016 01:57:23";
trevor.profile:180:    set compile_time    "25 Oct 2016 01:57:23";
trick_ryuk.profile:277:    set compile_time    "16 Apr 2020 17:56:00";
windows-updates.profile:35:    set compile_time    "26 Oct 2080 00:55:44";
youtube_video.profile:192:    set compile_time    "25 Oct 2016 01:57:23";
zloader.profile:280:    set compile_time    "16 Apr 2020 17:56:00";
```



Sign up for free

to join this conversation on GitHub. Already have an account? [Sign in to comment](#)