Practical Queries for Malware Infrastructure - Part 3 (Advanced Examples)

embee-research.ghost.io/practical-queries-for-malware-infrastructure-part-3/

Matthew November 22, 2023

Advanced

More interesting and practical queries for identifying malware infrastructure.

Practical and real-world examples of queries for identifying malware infrastructure. The primary tooling used is Censys.io.

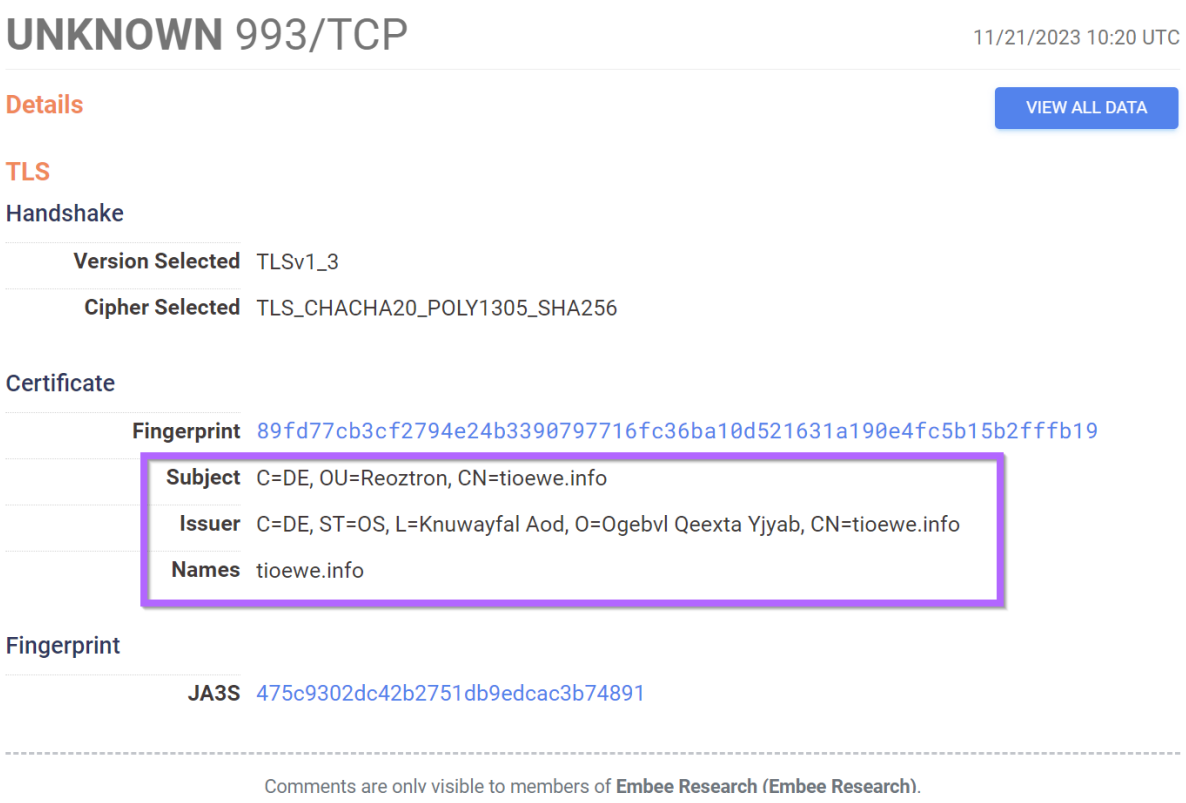
- Redline Stealer
- Qakbot
- NJRat
- Remcos
- BianLian Go Trojan
- XTreme RAT
- SuperShell Botnet

Qakbot Command and Control Servers

Censys Link

- Empty Banner Produces Unique Hash
- Particular Structure to TLS certificates
- Qakbot server typically on port 443,993 or 995
- Server name all lower case letters with no subdomain
- No identified operating system on servers
- Same ja3s across malicious servers.

> services: (banner_hashes="sha256:e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855" and tls.certificates.leaf_data.subject_dn:/C=[^,]+, OU=[^,]+, CN=[^,]+/ and tls.certificates.leaf_data.issuer_dn:/C=[^,]+, ST=[^,]+, L=[^,]+, O=[^,]+, CN=[^,]+/ and (port:443 or port:993 or port:995)) and services.tls.certificates.leaf_data.names:/[a-z]{3,15}.[a-z]{2,5}/ and not operating_system.product:* and services.tls.ja3s: 475c9302dc42b2751db9edcac3b74891



IOC's

45[.]62[.]69[.]55
50[.]99[.]8[.]5
59[.]88[.]27[.]148
77[.]49[.]187[.]148
77[.]124[.]85[.]166
79[.]107[.]159[.]93
84[.]155[.]8[.]44
85[.]97[.]84[.]158
93[.]210[.]162[.]76
95[.]147[.]160[.]184
95[.]149[.]166[.]38
102[.]156[.]106[.]202
105[.]102[.]21[.]121
105[.]102[.]106[.]170
117[.]195[.]17[.]160
117[.]215[.]23[.]136
141[.]164[.]186[.]22
141[.]164[.]198[.]216
154[.]246[.]62[.]35

154[.]246[.]116[.]114
154[.]246[.]230[.]147
161[.]142[.]98[.]51
186[.]182[.]15[.]91
187[.]233[.]184[.]144
188[.]161[.]234[.]48
190[.]133[.]143[.]232
197[.]2[.]10[.]236
197[.]26[.]188[.]179
197[.]204[.]133[.]11
197[.]204[.]157[.]205
217[.]165[.]233[.]123

BianLian GO Trojan

Censys Link

- Empty Banner on Main Service
- Very particular structure to certificate names (both Issuer and Subject) eg `C=zHNWYSaBumxjPKPY, O=KcUnN1CdTgEOxr6h, OU=FtVXN2EyNbwlXUP8`
- Service always unidentifed, presumably due to lack of headers.

> services:
> (banner_hashes="sha256:e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855" and tls.certificates.leaf_data.subject_dn=/C=[^,]{10,20}, O=[^,]{10,20}, OU=[^,]{10,20}/ and tls.certificates.leaf_data.issuer_dn=/C=[^,]{10,20}, O=[^,]{10,20}, OU=[^,]{10,20}/ and service_name:UNKNOWN)

IOC's

3[.]76[.]100[.]131
13[.]59[.]168[.]154
13[.]215[.]227[.]78
13[.]215[.]228[.]73
23[.]152[.]0[.]64
34[.]207[.]174[.]202
34[.]219[.]121[.]232
43[.]139[.]241[.]58
45[.]45[.]219[.]141
45[.]56[.]165[.]27
45[.]56[.]165[.]30
45[.]86[.]163[.]188
45[.]86[.]163[.]224
54[.]193[.]91[.]232
65[.]109[.]3[.]80
65[.]109[.]166[.]117
66[.]29[.]155[.]44
85[.]13[.]118[.]11
87[.]247[.]185[.]109
89[.]23[.]107[.]110
91[.]102[.]162[.]229
94[.]131[.]98[.]34
94[.]198[.]50[.]195
103[.]20[.]235[.]195

103[.]57[.]250[.]152
104[.]36[.]229[.]15
104[.]238[.]34[.]130
104[.]238[.]35[.]163
104[.]238[.]60[.]64
104[.]238[.]60[.]84
104[.]238[.]61[.]150
108[.]174[.]60[.]151
120[.]48[.]110[.]233
143[.]198[.]46[.]29
149[.]154[.]158[.]34
149[.]154[.]158[.]199
149[.]248[.]14[.]201
151[.]236[.]22[.]64
157[.]245[.]48[.]209
168[.]119[.]88[.]236
185[.]240[.]103[.]195
188[.]34[.]130[.]46
192[.]52[.]166[.]233
193[.]31[.]28[.]88
194[.]213[.]18[.]45
195[.]2[.]92[.]206
195[.]128[.]235[.]20
198[.]199[.]76[.]216
208[.]123[.]119[.]123
213[.]139[.]205[.]146

NJRat/Xworm Botnet Servers

Censys Link

- Extremely high number of running services (typically 200-400)
- At least one dns.name pointing to an ngrok address
- Most ports running GStreamer Service

> service_count:[200 to 2000] and dns.names:*ngrok* and services.banner:GStreamer

IOC's

3[.]64[.]4[.]198
3[.]66[.]38[.]117
3[.]67[.]15[.]169
3[.]67[.]62[.]142
3[.]67[.]112[.]102
3[.]67[.]161[.]133
3[.]68[.]56[.]232
3[.]68[.]171[.]119
3[.]69[.]115[.]178
3[.]69[.]157[.]220
3[.]121[.]139[.]82
3[.]124[.]67[.]191
3[.]124[.]142[.]205
3[.]125[.]102[.]39
3[.]125[.]188[.]168
3[.]125[.]209[.]94
3[.]125[.]223[.]134
3[.]126[.]37[.]18
3[.]126[.]224[.]214
3[.]127[.]59[.]75
3[.]127[.]138[.]57
3[.]127[.]181[.]115
3[.]127[.]253[.]86
18[.]156[.]13[.]209
18[.]158[.]58[.]205
18[.]158[.]249[.]75
18[.]192[.]31[.]165
18[.]192[.]93[.]86
18[.]197[.]239[.]109
18[.]198[.]77[.]177
35[.]157[.]111[.]131

35[.]158[.]159[.]254
52[.]28[.]112[.]211
52[.]28[.]247[.]255

Redline Stealer C2

Censys Link

- Initial Redline stealer c2 on `77.91.124[.]86:19084`
- Running 3 services, DNS and 2 Valve Related services.
- Reverse DNS pointing to a Russian VPN Service
- Searching on DNS Forwarding + .ru dns + Valve Service + 3 total services results in 18 servers with 3 marked as known malware.
- Other 15 results are "clean", but may be reserved for later malicious use.

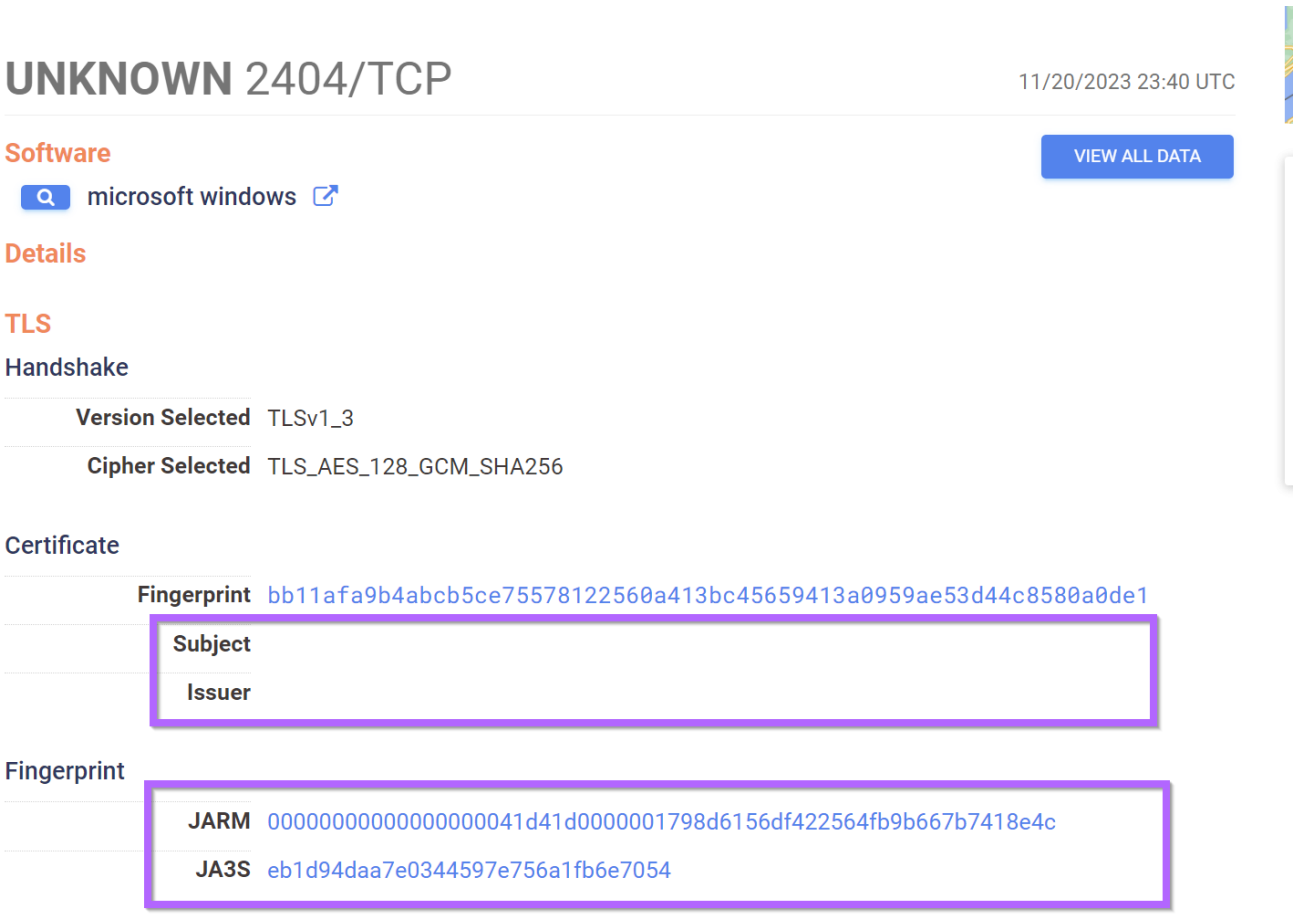
> services.dns.server_type="FORWARDING" and dns.reverse_dns.names:*.ru and services.extended_service_name="VALVE" and service_count:3

Remcos C2 Servers, Overlap with other RAT Families

Censys Link

- Empty Banner Produces Unique-ish hash value
- Same Jarm fingerprint across services
- Same Ja3s
- Almost always on port 2404

> services:
> (banner_hashes="sha256:e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855" and jarm.fingerprint="00000000000000000041d41d0000001798d6156df422564fb9b667b7418e4c" and port:2404 and tls.ja3s: eb1d94daa7e0344597e756a1fb6e7054)



IOC's

5[.]2[.]68[.]80
5[.]39[.]222[.]61
31[.]220[.]90[.]137
38[.]242[.]251[.]178
45[.]15[.]156[.]172
45[.]15[.]156[.]232
45[.]61[.]128[.]201
45[.]62[.]170[.]4
45[.]76[.]46[.]64
45[.]95[.]169[.]140
46[.]175[.]167[.]116
51[.]161[.]105[.]243
51[.]195[.]71[.]9
65[.]109[.]229[.]216
66[.]248[.]206[.]187
79[.]124[.]8[.]6
85[.]206[.]161[.]12
88[.]119[.]170[.]153
91[.]92[.]242[.]130
91[.]92[.]245[.]131
91[.]92[.]245[.]219
91[.]92[.]245[.]220
91[.]92[.]247[.]118

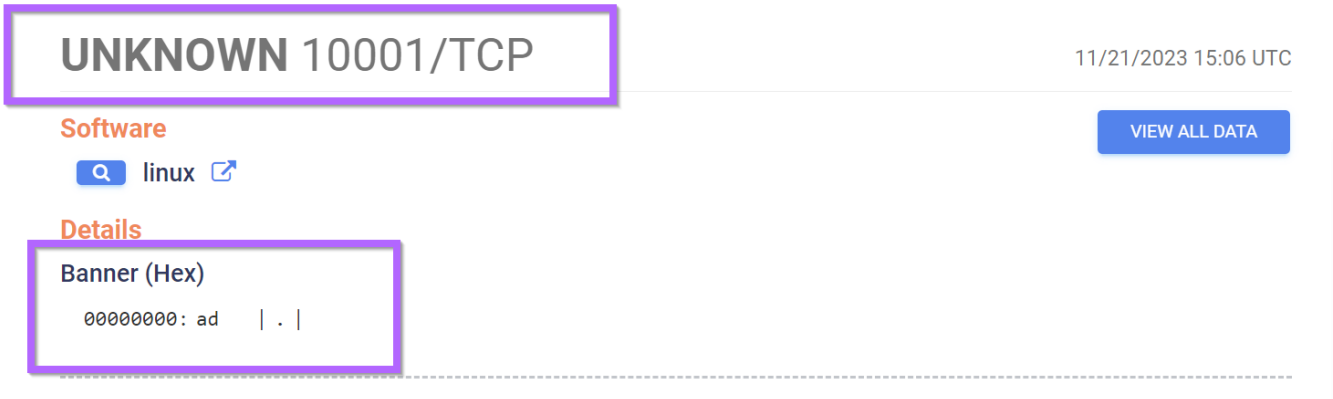
91[.]92[.]248[.]93
91[.]134[.]150[.]152
91[.]148[.]135[.]184
91[.]151[.]88[.]7
92[.]223[.]106[.]203
94[.]130[.]249[.]123
103[.]212[.]81[.]157
107[.]150[.]18[.]101
107[.]150[.]18[.]214
109[.]248[.]151[.]170
121[.]177[.]29[.]204
154[.]26[.]130[.]12
161[.]97[.]64[.]199
162[.]55[.]91[.]58
172[.]93[.]164[.]62
172[.]93[.]187[.]227
172[.]93[.]217[.]218
172[.]96[.]14[.]18
176[.]9[.]23[.]50
185[.]56[.]83[.]208
185[.]114[.]21[.]175
185[.]196[.]8[.]157
185[.]202[.]175[.]170
185[.]255[.]114[.]39
193[.]142[.]59[.]81
198[.]55[.]113[.]202
205[.]234[.]181[.]73

XTreme RAT

Censys Link

- Banner is a single 0xAD character
- Always running on port 10001

> services.banner_hashes="sha256:22adaf058a2cb668b15cb4c1f30e7cc720bbe38c146544169db35fbf630389c4" and services.port:10001



IOC's

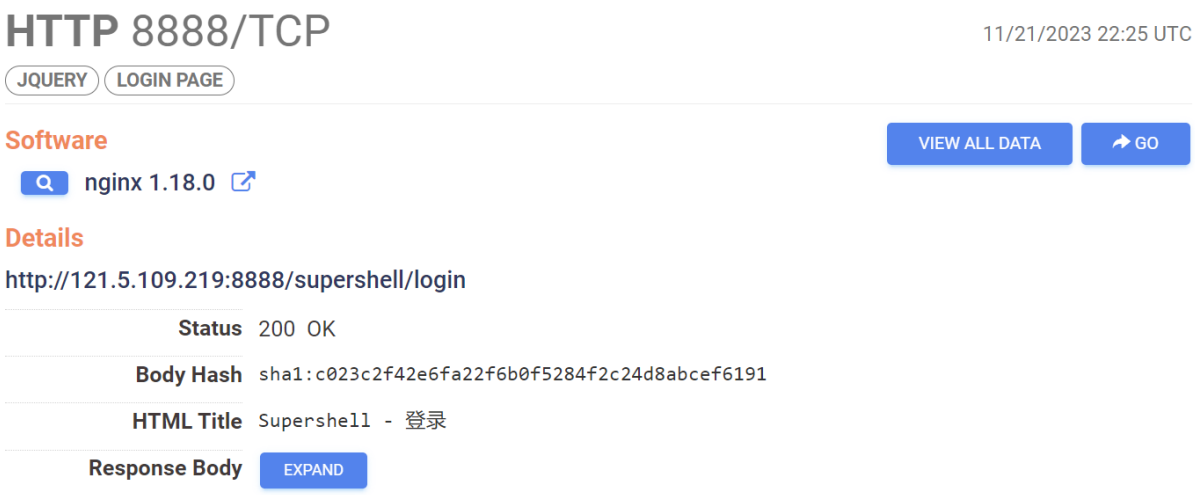
3[.]125[.]130[.]75
8[.]222[.]212[.]126
42[.]157[.]163[.]133
60[.]204[.]168[.]6
110[.]43[.]39[.]130
178[.]162[.]199[.]83

SuperShell BotNet

Censys Link

- Presence of "Supershell" in html title
- re-used favicon across panels

> services.http.response.html_title:"Supershell" or
> services.http.response.favicons.md5_hash="cb183a53ebfc2b61b3968c9d4aa4b14a"



IOC's

1[.]12[.]226[.]211
1[.]15[.]245[.]245
4[.]224[.]84[.]20
5[.]255[.]119[.]163
8[.]130[.]24[.]41
8[.]130[.]34[.]53
8[.]134[.]207[.]212
8[.]210[.]134[.]250
8[.]217[.]92[.]212
8[.]217[.]200[.]158
23[.]95[.]233[.]140
23[.]95[.]233[.]180
23[.]224[.]131[.]86
27[.]124[.]53[.]64
38[.]6[.]163[.]11
38[.]6[.]177[.]117
38[.]6[.]184[.]125

38[.]6[.]216[.]13
38[.]47[.]124[.]83
38[.]54[.]40[.]156
38[.]54[.]57[.]79
38[.]181[.]25[.]62
39[.]98[.]115[.]22
39[.]100[.]79[.]80
39[.]103[.]150[.]56
39[.]107[.]91[.]7
42[.]192[.]145[.]232
42[.]192[.]233[.]229
42[.]193[.]17[.]127
42[.]194[.]178[.]221
43[.]128[.]88[.]112
43[.]138[.]25[.]144
43[.]139[.]47[.]123
43[.]139[.]225[.]42
43[.]139[.]249[.]124
43[.]143[.]166[.]173
43[.]143[.]246[.]38
43[.]153[.]207[.]85
43[.]159[.]49[.]100
43[.]163[.]240[.]112
43[.]249[.]8[.]99
45[.]11[.]47[.]243
45[.]32[.]42[.]214
45[.]42[.]215[.]230
45[.]76[.]50[.]94
45[.]76[.]182[.]234
45[.]144[.]138[.]129
45[.]145[.]228[.]177
45[.]145[.]229[.]203
45[.]152[.]66[.]151
45[.]207[.]53[.]224
47[.]57[.]239[.]230
47[.]74[.]157[.]112
47[.]74[.]242[.]253
47[.]88[.]14[.]60
47[.]94[.]158[.]69
47[.]96[.]252[.]193
47[.]97[.]6[.]61
47[.]98[.]157[.]247
47[.]98[.]158[.]167
47[.]100[.]240[.]145
47[.]102[.]97[.]231
47[.]103[.]142[.]250
47[.]120[.]35[.]131
47[.]236[.]36[.]154
47[.]242[.]95[.]207
47[.]243[.]240[.]115
49[.]233[.]249[.]195

49[.]235[.]104[.]106
52[.]141[.]25[.]85
52[.]196[.]231[.]84
59[.]110[.]219[.]204
60[.]204[.]202[.]69
60[.]204[.]211[.]173
62[.]234[.]41[.]101
64[.]31[.]63[.]239
64[.]32[.]30[.]205
64[.]176[.]37[.]32
74[.]48[.]30[.]78
74[.]48[.]31[.]182
74[.]48[.]60[.]99
74[.]48[.]78[.]38
81[.]68[.]98[.]217
81[.]71[.]68[.]50
82[.]156[.]157[.]182
82[.]157[.]196[.]111
85[.]206[.]172[.]151
85[.]208[.]118[.]169
93[.]188[.]164[.]249
101[.]34[.]71[.]193
101[.]34[.]209[.]73
101[.]34[.]229[.]123
101[.]35[.]252[.]249
101[.]42[.]141[.]237
101[.]43[.]149[.]73
103[.]38[.]83[.]75
103[.]73[.]161[.]131
103[.]106[.]190[.]156
103[.]143[.]28[.]35
103[.]143[.]28[.]36
103[.]143[.]28[.]37
103[.]209[.]129[.]193
103[.]230[.]15[.]224
103[.]234[.]72[.]31
103[.]234[.]72[.]49
103[.]234[.]72[.]216
104[.]152[.]209[.]148
104[.]225[.]232[.]136
104[.]233[.]140[.]138
106[.]12[.]146[.]25
106[.]52[.]216[.]39
106[.]55[.]107[.]93
107[.]151[.]245[.]165
107[.]172[.]16[.]106
107[.]172[.]34[.]126
107[.]172[.]43[.]167
107[.]172[.]141[.]153
107[.]173[.]201[.]235
107[.]174[.]90[.]202

107[.]174[.]95[.]93
107[.]175[.]172[.]131
107[.]189[.]11[.]113
110[.]40[.]196[.]45
110[.]41[.]185[.]246
110[.]42[.]218[.]211
110[.]42[.]222[.]61
110[.]72[.]96[.]130
111[.]180[.]199[.]252
111[.]230[.]89[.]66
111[.]231[.]28[.]30
112[.]121[.]164[.]202
112[.]121[.]164[.]203
112[.]121[.]164[.]204
112[.]121[.]164[.]205
112[.]121[.]164[.]206
113[.]125[.]131[.]151
113[.]207[.]105[.]235
114[.]115[.]180[.]116
115[.]227[.]22[.]82
116[.]62[.]47[.]216
117[.]50[.]184[.]22
118[.]24[.]128[.]204
118[.]89[.]118[.]234
118[.]89[.]125[.]171
119[.]45[.]190[.]210
119[.]91[.]45[.]113
120[.]27[.]225[.]229
120[.]46[.]197[.]194
121[.]5[.]109[.]219
121[.]36[.]97[.]135
121[.]36[.]105[.]186
121[.]36[.]219[.]56
121[.]36[.]248[.]151
121[.]37[.]165[.]107
121[.]37[.]237[.]40
121[.]40[.]111[.]130
122[.]51[.]46[.]61
122[.]51[.]46[.]83
122[.]51[.]215[.]152
123[.]57[.]182[.]3
123[.]60[.]74[.]61
123[.]60[.]168[.]74
123[.]60[.]176[.]96
123[.]249[.]87[.]1
124[.]70[.]69[.]50
124[.]70[.]158[.]176
124[.]70[.]216[.]108
124[.]156[.]185[.]41
124[.]220[.]210[.]155
124[.]221[.]15[.]219

124[.]221[.]50[.]188
124[.]221[.]78[.]9
124[.]221[.]214[.]132
124[.]222[.]5[.]128
124[.]222[.]40[.]141
124[.]222[.]80[.]204
124[.]223[.]38[.]97
124[.]223[.]170[.]107
139[.]9[.]117[.]78
139[.]84[.]226[.]182
139[.]155[.]134[.]117
139[.]159[.]236[.]228
139[.]180[.]194[.]27
139[.]198[.]174[.]173
139[.]199[.]212[.]224
139[.]224[.]198[.]190
140[.]143[.]147[.]47
140[.]238[.]248[.]106
141[.]11[.]229[.]61
142[.]171[.]75[.]208
142[.]171[.]158[.]253
147[.]78[.]13[.]240
149[.]88[.]80[.]228
150[.]107[.]2[.]9
150[.]158[.]92[.]16
152[.]32[.]219[.]243
152[.]136[.]128[.]162
154[.]3[.]1[.]226
154[.]3[.]32[.]249
154[.]8[.]193[.]47
154[.]9[.]249[.]166
154[.]39[.]150[.]181
154[.]92[.]18[.]45
154[.]204[.]35[.]13
154[.]204[.]35[.]82
154[.]204[.]35[.]83
154[.]204[.]35[.]128
154[.]204[.]59[.]208
154[.]222[.]227[.]127
155[.]94[.]133[.]104
156[.]245[.]11[.]145
156[.]245[.]11[.]169
156[.]245[.]11[.]249
159[.]138[.]56[.]8
162[.]14[.]107[.]61
162[.]14[.]107[.]218
167[.]179[.]108[.]80
172[.]105[.]226[.]35
172[.]245[.]81[.]206
172[.]245[.]156[.]157
172[.]247[.]189[.]100

175[.]178[.]248[.]243
175[.]178[.]249[.]249
183[.]255[.]43[.]126
185[.]81[.]68[.]90
185[.]171[.]120[.]49
185[.]171[.]120[.]183
185[.]227[.]68[.]176
185[.]228[.]1[.]237
192[.]121[.]162[.]86
192[.]227[.]191[.]47
193[.]84[.]248[.]79
194[.]87[.]69[.]132
194[.]104[.]146[.]24
195[.]133[.]53[.]90
198[.]13[.]36[.]40
198[.]74[.]113[.]195
198[.]211[.]99[.]78
206[.]119[.]179[.]40
206[.]237[.]0[.]49
206[.]237[.]29[.]177
212[.]129[.]223[.]209
222[.]88[.]186[.]81