Joint Indicator Bulletin (JIB) – INC260425

February 18, 2013

Introduction

Various cyber actors have engaged in malicious activity against Government and Private Sector entities. The apparent objective of this activity has been the theft of intellectual property, trade secrets, and other sensitive business information. To this end, the malicious actors have employed a variety of techniques in order to infiltrate targeted organizations, establish a foothold, move laterally through the targets' networks, and exfiltrate confidential or proprietary data. The United States Department of Homeland Security (DHS), in collaboration with the Federal Bureau of Investigation and other partners, has created this Joint Indicator Bulletin, containing cyber indicators related to this activity. Organizations are advised to examine current and historical security logs for evidence of malicious activity related to the indicators in this bulletin and deploy additional protections as appropriate. In addition, DHS would welcome any additional information your organization may be able to share regarding this or similar activity, which may be provided to the US Computer Emergency Readiness Team (US-CERT) at soc@uscert.gov.

Document Overview

This Joint Indicator Bulletin is comprised of several sections covering malware indicators, network traffic, tool indicators, hostnames, and IP addresses known to be associated with the ongoing malicious activity. If suspicious network traffic or malware is identified based on these indicators, affected systems should be investigated for signs of compromise.

To support developing shared situational awareness of cyber threats, DHS welcomes any additional information your organization may be able to share regarding this or similar activity. Such information can be provided to the United States Computer Emergency Readiness Team (US-CERT) at soc@us-cert.gov.

NOTE: Any network defense actions should only be taken in accordance with established organizational security policies and network defense plans. Presence of one or more of these indicators on networks or systems is not necessarily a positive indication of malicious activity, but may enable an organization to identify malicious activity. A number of the indicators likely include compromised or shared systems on the Internet and, as such, may be associated with legitimate traffic. Organizations should take care to clearly establish malicious intent before taking any action; for example, preemptively blocking the IPs provided in this Bulletin could have negative consequences while failing to provide appreciable protection.

Indicator Descriptions

As a general matter, malicious cyber actors have multiple tools at their disposal and can represent a significant threat to targeted victim organizations. Such actors frequently compromise victim organizations with targeted spear-phishing campaigns, understand how to move laterally within a network to acquire targeted data, and often maintain undetected persistence on victim networks for months or even years. The indicators provided in this Bulletin include malware and compromised IP addresses and domains used by such actors.

Malware

Malicious activity like that described in this Bulletin usually originates via targeted spear phishing email campaigns that compromise victim organizations. These emails can result in the installation of one or more pieces of malware used to enable complete control of those systems. The presence of such malware is a strong indication the computer or network has been compromised.

Client Tools

During the course of a computer intrusion, malicious actors often download additional tools to victim systems for the purpose of evading local security measures and to compromise additional computers on victim networks. These tools might have legitimate uses, but, when combined with other indications of an intrusion, could indicate that the computer has been compromised. The

presence of these tools alone is not necessarily a positive indication of malicious activity, but may enable an organization to identify malicious activity.

IP Addresses, Hostnames and Second-Level Domains

Malicious actors routinely compromise hosts on the Internet for the purpose of obscuring their activity, particularly the exfiltration of computer files from end-point victims. The majority of these compromised hosts have been configured to prevent identification of the source of the intrusion activity. The traffic from these hosts is generally legitimate, but, because they have been compromised, activity to and from these IPs should be reviewed for indications of malicious traffic.

Malicious actors also make use of numerous Internet hostnames for the purpose of compromising and controlling victim systems. Actors have been known to register second-level domains for their exclusive use in these activities. In addition, malicious actors have been known to use DNS providers that allow the use of specific hostnames that are part of shared second-level domains.

Many of these hostnames and domains may be legitimate hosts or domains that have been co-opted by malicious actors. Any number of the IP addresses or domains in this Bulletin may have been remediated prior to publication of this list. In some cases, a single IP address from this indicator list may represent hundreds or even thousands of legitimate independent websites, or may represent a small business network. A number of indicators contained in this Bulletin resolve back to large scale service providers whose services are being abused. For these reasons, outright blocking of these indicators is not recommended. Rather, traffic from these IPs or domains should be investigated for signs of compromise.

Contact NCCIC/US-CERT

US-CERT is interested in any additional information that your organization may be able to share regarding this or similar activity. For any questions or feedback related to this report, please contact US-CERT at:

(UNCLASS) Phone: +1-703-235-8832
(UNCLASS) Email: soc@us-cert.gov
US-CERT's PGP key may be downloaded at us-cert.gov/contact
(SIPRNET) Email: us-cert@dhs.sgov.gov
(JWICS) Email: us-cert@dhs.ic.gov

NCCIC/US-CERT continuously strives to improve its products and services. You can help by answering a very short series of questions about this product at the following URL: https://forms.us-cert.gov/ncsd-feedback/

Contact FBI

You may also contact FBI with any questions related to this JIB:
Email: cywatch@ic.fbi.gov
Voice: +1-855-292-3937

Document FAQ

I see that this document is labeled as TLP: GREEN. Can I distribute this to other people? Recipients may share TLP: **GREEN** information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Please contact US-CERT with specific distribution inquiries.

Can I edit this document to include additional information? This document is not to be edited, changed or modified in any way by recipients. All comments or questions related to this document should be directed to the US-CERT Security Operations Center at 1-888-282-0870 or soc@us-cert.gov.

Technical Data:

Please find the indicators listed below, and included on request in a separate machine readable format as Attachment A.

****
IP Address Awareness List
****
107[.]6[.]38[.]55
108[.]171[.]207[.]62
108[.]171[.]244[.]138
108[.]171[.]246[.]87
108[.]171[.]248[.]182
108[.]171[.]248[.]83
108[.]171[.]248[.]86
108[.]171[.]252[.]41
108[.]171[.]254[.]76
112[.]121[.]164[.]2
112[.]133[.]203[.]215
112[.]133[.]203[.]250
115[.]119[.]92[.]178
115[.]178[.]60[.]19
116[.]212[.]100[.]94
117[.]121[.]241[.]186
119[.]75[.]5[.]132
119[.]75[.]5[.]134
12[.]10[.]250[.]105

12[.]10[.]250[.]109
12[.]10[.]250[.]110
12[.]10[.]250[.]97
12[.]100[.]63[.]135
12[.]147[.]51[.]99
12[.]162[.]189[.]184
12[.]173[.]220[.]231
12[.]173[.]220[.]233
12[.]182[.]10[.]124
12[.]218[.]86[.]2
12[.]233[.]148[.]145
12[.]233[.]148[.]185
12[.]235[.]72[.]138
12[.]235[.]72[.]140
12[.]36[.]96[.]236
12[.]51[.]6[.]132
12[.]7[.]168[.]121
122[.]126[.]32[.]234
122[.]155[.]3[.]147
122[.]160[.]137[.]76
124[.]122[.]156[.]219
128[.]173[.]95[.]6
128[.]95[.]9[.]2
129[.]25[.]5[.]200
129[.]44[.]254[.]145
134[.]208[.]10[.]195
141[.]151[.]164[.]87
142[.]0[.]143[.]207
146[.]145[.]183[.]100
150[.]176[.]56[.]194
158[.]255[.]208[.]211
161[.]58[.]179[.]230
164[.]106[.]102[.]188
164[.]119[.]10[.]170
164[.]119[.]11[.]2
164[.]119[.]54[.]244
164[.]119[.]54[.]247
165[.]165[.]38[.]19
168[.]215[.]137[.]6
168[.]93[.]98[.]3
173[.]10[.]48[.]243
173[.]224[.]208[.]155
173[.]224[.]211[.]14
173[.]224[.]211[.]16
173[.]224[.]214[.]70

173[.]224[.]215[.]73
173[.]224[.]216[.]217
173[.]252[.]255[.]52
182[.]173[.]77[.]26
184[.]105[.]135[.]166
184[.]22[.]26[.]50
184[.]72[.]82[.]144
184[.]82[.]164[.]104
184[.]82[.]47[.]200
189[.]87[.]87[.]3
190[.]13[.]160[.]114
193[.]219[.]90[.]29
194[.]106[.]162[.]203
195[.]22[.]21[.]72
195[.]29[.]247[.]78
196[.]36[.]199[.]217
198[.]15[.]88[.]37
198[.]15[.]88[.]39
198[.]69[.]219[.]173
199[.]119[.]201[.]162
199[.]119[.]201[.]167
199[.]119[.]201[.]67
199[.]119[.]206[.]11
199[.]119[.]206[.]111
199[.]119[.]206[.]19
199[.]119[.]206[.]99
199[.]119[.]207[.]237
199[.]15[.]113[.]218
199[.]15[.]117[.]98
199[.]67[.]16[.]122
199[.]67[.]23[.]45
199[.]71[.]213[.]17
199[.]71[.]213[.]91
199[.]83[.]88[.]98
199[.]83[.]89[.]45
199[.]83[.]93[.]22
199[.]83[.]93[.]51
199[.]83[.]93[.]88
199[.]83[.]95[.]51
199[.]83[.]95[.]60
200[.]53[.]40[.]219
202[.]176[.]81[.]175
202[.]180[.]175[.]16
202[.]43[.]33[.]5
202[.]95[.]222[.]143

202[.]95[.]222[.]145
202[.]95[.]222[.]158
202[.]95[.]222[.]182
202[.]95[.]222[.]183
203[.]118[.]56[.]213
203[.]123[.]147[.]34
203[.]146[.]102[.]166
203[.]146[.]249[.]189
203[.]150[.]230[.]121
203[.]238[.]57[.]1
203[.]64[.]84[.]226
203[.]81[.]38[.]54
203[.]81[.]53[.]14
203[.]82[.]57[.]109
204[.]111[.]73[.]156
204[.]111[.]75[.]107
204[.]12[.]11[.]212
204[.]12[.]11[.]54
204[.]12[.]116[.]166
204[.]12[.]208[.]122
204[.]12[.]208[.]125
204[.]12[.]21[.]69
204[.]12[.]22[.]114
204[.]12[.]224[.]75
204[.]12[.]236[.]182
204[.]12[.]236[.]183
204[.]12[.]63[.]133
204[.]12[.]9[.]251
204[.]13[.]24[.]14
204[.]15[.]132[.]254
204[.]152[.]198[.]194
204[.]16[.]139[.]5
204[.]17[.]34[.]150
204[.]180[.]235[.]103
204[.]180[.]235[.]106
204[.]45[.]101[.]246
204[.]45[.]108[.]237
204[.]45[.]117[.]174
204[.]45[.]123[.]141
204[.]45[.]124[.]100
204[.]45[.]124[.]162
204[.]45[.]124[.]163
204[.]45[.]137[.]74
204[.]45[.]146[.]250
204[.]45[.]147[.]19

204[.]45[.]153[.]52
204[.]45[.]190[.]89
204[.]45[.]198[.]18
204[.]45[.]201[.]107
204[.]45[.]205[.]44
204[.]45[.]230[.]75
204[.]45[.]39[.]4
204[.]45[.]52[.]20
204[.]45[.]64[.]66
204[.]45[.]75[.]250
204[.]45[.]79[.]180
204[.]45[.]79[.]20
204[.]45[.]79[.]218
205[.]159[.]83[.]11
205[.]159[.]83[.]31
205[.]159[.]83[.]91
205[.]164[.]0[.]34
205[.]172[.]20[.]42
205[.]196[.]178[.]23
205[.]209[.]161[.]195
205[.]209[.]161[.]5
205[.]237[.]192[.]123
205[.]242[.]114[.]4
206[.]125[.]45[.]187
206[.]192[.]55[.]117
206[.]204[.]190[.]237
207[.]150[.]197[.]155
207[.]179[.]111[.]5
207[.]182[.]238[.]195
207[.]210[.]252[.]17
207[.]250[.]229[.]52
207[.]250[.]49[.]172
207[.]250[.]49[.]173
207[.]36[.]0[.]193
207[.]36[.]17[.]15
207[.]46[.]17[.]125
207[.]59[.]239[.]122
207[.]65[.]231[.]21
207[.]75[.]209[.]108
207[.]97[.]226[.]130
208[.]106[.]145[.]153
208[.]106[.]146[.]98
208[.]106[.]82[.]119
208[.]109[.]238[.]15
208[.]109[.]238[.]72

208[.]109[.]238[.]80
208[.]109[.]238[.]96
208[.]109[.]49[.]66
208[.]118[.]188[.]166
208[.]118[.]188[.]179
208[.]118[.]188[.]57
208[.]186[.]112[.]40
208[.]221[.]198[.]12
208[.]43[.]154[.]7
208[.]43[.]175[.]82
208[.]43[.]208[.]14
208[.]43[.]225[.]196
208[.]43[.]255[.]135
208[.]43[.]54[.]164
208[.]43[.]71[.]116
208[.]44[.]238[.]249
208[.]57[.]237[.]141
208[.]67[.]248[.]66
208[.]69[.]32[.]230
208[.]77[.]45[.]61
208[.]77[.]45[.]69
208[.]87[.]242[.]93
209[.]104[.]217[.]69
209[.]104[.]217[.]72
209[.]104[.]217[.]76
209[.]114[.]160[.]115
209[.]114[.]222[.]100
209[.]116[.]102[.]225
209[.]158[.]71[.]20
209[.]175[.]175[.]227
209[.]175[.]175[.]230
209[.]200[.]117[.]198
209[.]208[.]95[.]158
209[.]208[.]95[.]86
209[.]212[.]104[.]171
209[.]234[.]81[.]205
209[.]242[.]13[.]230
209[.]242[.]21[.]134
209[.]34[.]224[.]52
209[.]34[.]231[.]197
209[.]34[.]231[.]59
209[.]34[.]233[.]26
209[.]67[.]56[.]252
209[.]75[.]160[.]176
209[.]75[.]160[.]98

210[.]184[.]116[.]198
210[.]193[.]52[.]160
210[.]202[.]22[.]129
210[.]205[.]6[.]219
210[.]220[.]197[.]2
210[.]245[.]64[.]107
210[.]249[.]80[.]141
211[.]115[.]70[.]114
211[.]232[.]57[.]150
211[.]232[.]57[.]235
211[.]232[.]57[.]249
211[.]233[.]58[.]69
212[.]116[.]151[.]146
212[.]150[.]22[.]228
213[.]79[.]32[.]179
216[.]134[.]222[.]200
216[.]136[.]62[.]143
216[.]174[.]25[.]177
216[.]183[.]190[.]162
216[.]183[.]40[.]56
216[.]185[.]0[.]220
216[.]185[.]0[.]9
216[.]196[.]249[.]210
216[.]213[.]99[.]218
216[.]215[.]112[.]83
216[.]226[.]191[.]103
216[.]24[.]192[.]117
216[.]24[.]192[.]121
216[.]24[.]192[.]206
216[.]24[.]192[.]28
216[.]24[.]192[.]44
216[.]24[.]192[.]7
216[.]24[.]192[.]81
216[.]24[.]192[.]83
216[.]24[.]192[.]95
216[.]24[.]196[.]113
216[.]24[.]198[.]14
216[.]24[.]198[.]20
216[.]24[.]199[.]243
216[.]24[.]199[.]62
216[.]24[.]200[.]180
216[.]24[.]201[.]166
216[.]24[.]201[.]198
216[.]24[.]203[.]58
216[.]24[.]204[.]124

216[.]24[.]205[.]30
216[.]24[.]205[.]36
216[.]24[.]205[.]69
216[.]36[.]123[.]12
216[.]68[.]165[.]14
216[.]83[.]42[.]66
216[.]9[.]65[.]6
216[.]99[.]146[.]18
216[.]99[.]148[.]18
217[.]20[.]138[.]42
217[.]22[.]119[.]13
217[.]23[.]9[.]215
218[.]233[.]206[.]2
218[.]234[.]17[.]30
218[.]234[.]21[.]219
220[.]68[.]224[.]116
222[.]231[.]46[.]51
24[.]120[.]244[.]9
24[.]123[.]91[.]130
24[.]123[.]91[.]198
24[.]123[.]91[.]206
24[.]123[.]91[.]6
24[.]123[.]91[.]70
24[.]123[.]91[.]98
24[.]129[.]188[.]158
24[.]172[.]220[.]130
24[.]173[.]220[.]130
24[.]173[.]34[.]139
24[.]199[.]240[.]74
24[.]227[.]145[.]210
24[.]248[.]197[.]112
24[.]249[.]191[.]150
24[.]39[.]42[.]50
24[.]39[.]5[.]85
24[.]43[.]98[.]12
24[.]73[.]123[.]50
24[.]96[.]236[.]182
24[.]97[.]167[.]250
27[.]254[.]34[.]246
38[.]104[.]203[.]222
38[.]104[.]203[.]242
38[.]107[.]179[.]5
4[.]22[.]103[.]26
59[.]116[.]133[.]122
59[.]12[.]137[.]111

59[.]12[.]137[.]146
59[.]12[.]137[.]148
59[.]12[.]137[.]149
59[.]12[.]137[.]150
59[.]12[.]137[.]181
59[.]12[.]137[.]182
59[.]12[.]137[.]183
59[.]12[.]137[.]194
59[.]120[.]140[.]156
59[.]120[.]199[.]82
60[.]51[.]214[.]129
61[.]19[.]248[.]201
61[.]19[.]248[.]203
61[.]218[.]191[.]55
61[.]218[.]191[.]60
61[.]219[.]136[.]132
61[.]72[.]144[.]248
61[.]78[.]60[.]130
62[.]2[.]205[.]146
62[.]244[.]209[.]98
63[.]102[.]52[.]138
63[.]105[.]34[.]53
63[.]105[.]34[.]59
63[.]126[.]12[.]3
63[.]134[.]215[.]111
63[.]134[.]215[.]34
63[.]139[.]221[.]10
63[.]139[.]45[.]83
63[.]147[.]185[.]60
63[.]147[.]31[.]177
63[.]149[.]11[.]233
63[.]149[.]120[.]135
63[.]150[.]10[.]200
63[.]175[.]119[.]46
63[.]200[.]116[.]50
63[.]202[.]58[.]43
63[.]209[.]10[.]247
63[.]224[.]141[.]199
63[.]64[.]153[.]68
63[.]73[.]10[.]131
63[.]73[.]11[.]12
63[.]73[.]11[.]6
63[.]84[.]30[.]211
63[.]86[.]122[.]121
63[.]93[.]109[.]217

63[.]97[.]151[.]230
64[.]124[.]105[.]75
64[.]14[.]253[.]120
64[.]151[.]127[.]68
64[.]151[.]127[.]70
64[.]198[.]120[.]50
64[.]2[.]115[.]238
64[.]222[.]187[.]237
64[.]233[.]222[.]39
64[.]28[.]82[.]36
64[.]3[.]53[.]146
64[.]3[.]53[.]148
64[.]30[.]223[.]147
64[.]45[.]251[.]11
64[.]5[.]38[.]17
64[.]52[.]255[.]20
64[.]6[.]188[.]250
64[.]6[.]188[.]253
64[.]62[.]136[.]154
64[.]62[.]136[.]157
64[.]73[.]238[.]72
64[.]8[.]114[.]123
64[.]80[.]153[.]108
64[.]85[.]177[.]5
64[.]85[.]19[.]6
64[.]88[.]7[.]113
64[.]9[.]204[.]233
65[.]107[.]54[.]151
65[.]114[.]166[.]37
65[.]14[.]25[.]67
65[.]183[.]217[.]55
65[.]49[.]145[.]3
65[.]66[.]118[.]57
65[.]89[.]156[.]126
65[.]97[.]169[.]210
66[.]0[.]135[.]16
66[.]109[.]21[.]182
66[.]111[.]37[.]26
66[.]116[.]58[.]230
66[.]124[.]120[.]193
66[.]129[.]222[.]10
66[.]139[.]186[.]199
66[.]140[.]144[.]70
66[.]153[.]20[.]170
66[.]159[.]250[.]224

66[.]178[.]7[.]201
66[.]181[.]65[.]4
66[.]197[.]231[.]160
66[.]197[.]242[.]218
66[.]197[.]242[.]221
66[.]197[.]242[.]222
66[.]199[.]231[.]210
66[.]199[.]231[.]243
66[.]202[.]107[.]117
66[.]202[.]29[.]73
66[.]220[.]10[.]72
66[.]220[.]10[.]93
66[.]220[.]242[.]230
66[.]228[.]114[.]54
66[.]235[.]214[.]66
66[.]35[.]32[.]70
66[.]36[.]28[.]222
66[.]39[.]205[.]171
66[.]52[.]140[.]13
66[.]55[.]14[.]77
66[.]59[.]109[.]179
66[.]79[.]165[.]158
66[.]92[.]181[.]123
66[.]92[.]241[.]200
66[.]93[.]151[.]226
66[.]93[.]75[.]206
67[.]102[.]105[.]76
67[.]102[.]7[.]4
67[.]107[.]22[.]67
67[.]112[.]49[.]250
67[.]114[.]87[.]218
67[.]135[.]235[.]198
67[.]159[.]164[.]124
67[.]159[.]49[.]188
67[.]159[.]8[.]36
67[.]210[.]105[.]137
67[.]210[.]105[.]216
67[.]210[.]68[.]122
67[.]215[.]163[.]66
67[.]215[.]181[.]130
67[.]215[.]181[.]150
67[.]222[.]165[.]4
67[.]42[.]55[.]113
67[.]76[.]57[.]77
67[.]77[.]204[.]97

67[.]91[.]212[.]115
67[.]93[.]1[.]197
67[.]93[.]1[.]204
67[.]93[.]1[.]228
67[.]93[.]15[.]229
67[.]93[.]15[.]235
67[.]93[.]15[.]240
67[.]93[.]16[.]219
67[.]93[.]255[.]249
67[.]93[.]3[.]3
67[.]93[.]30[.]146
67[.]93[.]30[.]189
67[.]93[.]4[.]27
67[.]93[.]4[.]71
67[.]93[.]4[.]72
67[.]93[.]4[.]89
67[.]93[.]54[.]130
67[.]93[.]54[.]98
69[.]105[.]31[.]51
69[.]106[.]172[.]188
69[.]175[.]28[.]12
69[.]2[.]43[.]123
69[.]2[.]71[.]205
69[.]20[.]125[.]16
69[.]20[.]20[.]129
69[.]20[.]5[.]213
69[.]20[.]57[.]71
69[.]3[.]160[.]20
69[.]3[.]160[.]30
69[.]3[.]160[.]50
69[.]3[.]160[.]60
69[.]48[.]233[.]181
69[.]48[.]233[.]187
69[.]57[.]60[.]42
69[.]68[.]56[.]35
69[.]69[.]94[.]20
69[.]72[.]146[.]33
69[.]94[.]112[.]253
69[.]94[.]65[.]101
69[.]94[.]69[.]101
70[.]166[.]13[.]132
70[.]166[.]13[.]148
70[.]168[.]88[.]230
70[.]85[.]134[.]234
70[.]86[.]77[.]114

70[.]89[.]213[.]145
70[.]89[.]213[.]181
70[.]89[.]213[.]201
70[.]89[.]213[.]22
70[.]89[.]213[.]227
70[.]89[.]213[.]241
70[.]89[.]213[.]249
70[.]89[.]213[.]66
70[.]90[.]53[.]170
71[.]183[.]201[.]26
71[.]2[.]214[.]46
71[.]4[.]109[.]162
71[.]8[.]243[.]14
71[.]8[.]243[.]16
72[.]148[.]171[.]41
72[.]151[.]101[.]55
72[.]167[.]146[.]235
72[.]167[.]34[.]212
72[.]167[.]37[.]238
72[.]167[.]47[.]217
72[.]22[.]11[.]2
72[.]242[.]187[.]211
72[.]242[.]59[.]164
72[.]248[.]173[.]82
72[.]248[.]239[.]146
72[.]32[.]197[.]150
72[.]35[.]85[.]32
72[.]37[.]215[.]244
72[.]52[.]116[.]106
72[.]52[.]209[.]143
72[.]52[.]209[.]145
72[.]52[.]221[.]158
72[.]93[.]90[.]44
74[.]10[.]186[.]7
74[.]112[.]123[.]171
74[.]117[.]58[.]92
74[.]117[.]60[.]141
74[.]117[.]62[.]210
74[.]117[.]62[.]88
74[.]117[.]63[.]250
74[.]208[.]111[.]135
74[.]208[.]148[.]125
74[.]208[.]65[.]251
74[.]208[.]67[.]95
74[.]213[.]40[.]2

74[.]52[.]63[.]114
74[.]52[.]63[.]138
75[.]146[.]252[.]217
75[.]146[.]252[.]218
75[.]148[.]254[.]115
75[.]149[.]183[.]228
75[.]52[.]111[.]62
75[.]77[.]82[.]225
75[.]77[.]82[.]242
75[.]77[.]82[.]70
76[.]12[.]37[.]97
76[.]164[.]171[.]3
76[.]164[.]171[.]5
76[.]164[.]171[.]6
76[.]76[.]146[.]89
76[.]76[.]54[.]137
8[.]4[.]112[.]2
82[.]165[.]181[.]105
83[.]238[.]134[.]58
87[.]229[.]126[.]60
89[.]175[.]175[.]186
89[.]175[.]175[.]187
89[.]175[.]175[.]188
93[.]152[.]156[.]106
96[.]10[.]19[.]210
96[.]47[.]232[.]16
96[.]47[.]232[.]161
96[.]57[.]145[.]11
98[.]110[.]71[.]108
98[.]126[.]0[.]12
98[.]126[.]0[.]163
98[.]126[.]10[.]124
98[.]126[.]103[.]164
98[.]126[.]106[.]19
98[.]126[.]114[.]4
98[.]126[.]15[.]250
98[.]126[.]18[.]74
98[.]126[.]18[.]82
98[.]126[.]18[.]83
98[.]126[.]19[.]163
98[.]126[.]203[.]45
98[.]126[.]21[.]116
98[.]126[.]25[.]35
98[.]126[.]28[.]245
98[.]126[.]3[.]235

98[.]126[.]3[.]236
98[.]126[.]3[.]237
98[.]126[.]41[.]178
98[.]126[.]5[.]35
98[.]126[.]6[.]104
98[.]126[.]6[.]105
98[.]126[.]66[.]147
98[.]126[.]68[.]186
98[.]126[.]7[.]220
98[.]126[.]7[.]250
98[.]126[.]7[.]251
98[.]126[.]91[.]27
98[.]126[.]97[.]197
99[.]13[.]110[.]214
99[.]4[.]102[.]249

****
Domain Name Awareness List
****
a-af[.]arrowservice[.]net
able[.]arrowservice[.]net
a-cl[.]arrowservice[.]net
a-dl[.]arrowservice[.]net
admin[.]arrowservice[.]net
adtkl[.]bigish[.]net
adtkl[.]gmailboxes[.]com
a-ep[.]arrowservice[.]net
a-ex[.]arrowservice[.]net
a-f[.]gmailboxes[.]com
afghanistan[.]toutges[.]us
aga[.]toh[.]info
a-gon[.]arrowservice[.]net
a-he[.]arrowservice[.]net
a-if[.]arrowservice[.]net
a-iho[.]arrowservice[.]net
aiic[.]arrowservice[.]net
a-ip[.]arrowservice[.]net
ait[.]busketball[.]com
alarm[.]arrowservice[.]net
amne[.]purpledaily[.]com
ams[.]busketball[.]com
a-ne[.]arrowservice[.]net
anglo[.]arrowservice[.]net
aol[.]arrowservice[.]net
a-ol[.]arrowservice[.]net

apejack[.]bigish[.]net
a-pep[.]arrowservice[.]net
a-rdr[.]arrowservice[.]net
arm[.]armed[.]us
ascn[.]arrowservice[.]net
asp[.]arrowservice[.]net
asp[.]busketball[.]com
a-te[.]arrowservice[.]net
atom[.]busketball[.]com
atomic[.]bigish[.]net
a-uac[.]arrowservice[.]net
auto[.]gmailboxes[.]com
a-za[.]arrowservice[.]net
backsun[.]busketball[.]com
barity[.]gmailboxes[.]com
bass[.]busketball[.]com
bbs[.]busketball[.]com
bbs[.]marsbrother[.]com
bda[.]arrowservice[.]net
blacman[.]busketball[.]com
blog[.]arrowservice[.]net
blog[.]busketball[.]com
bring[.]busketball[.]com
built[.]arrowservice[.]net
busketball[.]com
buycow[.]busketball[.]com
buyer[.]arrowservice[.]net
buywater[.]busketball[.]com
bwbc[.]bigish[.]net
center[.]arrowservice[.]net
chamus[.]gmailboxes[.]com
cirfsun[.]gmailboxes[.]com
city[.]gmailboxes[.]com
class[.]arrowservice[.]net
cleanbeef[.]gmailboxes[.]com
cliffkl[.]gmailboxes[.]com
cmf[.]busketball[.]com
cmf[.]gmailboxes[.]com
cmp[.]gmailboxes[.]com
contact[.]arrowservice[.]net
contact[.]bigish[.]net
corn[.]busketball[.]com
cov[.]arrowservice[.]net
covclient[.]arrowservice[.]net
cow[.]arrowservice[.]net

cowboy[.]bigish[.]net
crab[.]arrowservice[.]net
ctimoon[.]marsbrother[.]com
ctisu[.]bigish[.]net
ctisun[.]gmailboxes[.]com
ctx[.]bigish[.]net
ctx-na[.]purpledaily[.]com
cws[.]gmailboxes[.]com
date[.]gmailboxes[.]com
dec[.]globalsecuriy[.]org
default[.]arrowservice[.]net
demavda[.]arrowservice[.]net
diaup[.]gmailboxes[.]com
diplomatism[.]nsmp[.]ru
documents[.]busketball[.]com
domain[.]arrowservice[.]net
domain[.]busketball[.]com
dowjs[.]busketball[.]com
dowjs[.]gmailboxes[.]com
download[.]gmailboxes[.]com
downupdate[.]bigish[.]net
dowph[.]bigish[.]net
drb[.]arrowservice[.]net
drinkwater[.]gmailboxes[.]com
eatbeef[.]gmailboxes[.]com
eciie[.]marsbrother[.]com
ecliar[.]marsbrother[.]com
eclimx[.]marsbrother[.]com
ecli-mxcdb[.]arrowservice[.]net
ecli-newf[.]marsbrother[.]com
ecli-noa[.]marsbrother[.]com
ecli-tda[.]marsbrother[.]com
ecli-tmp[.]marsbrother[.]com
ecli-un[.]marsbrother[.]com
eshop[.]gmailboxes[.]com
ever[.]arrowservice[.]net
fbtel[.]gmailboxes[.]com
finekl[.]bigish[.]net
fme[.]busketball[.]com
fmp[.]bigish[.]net
fn[.]bigish[.]net
follow[.]purpledaily[.]com
food[.]busketball[.]com
foreignpolicy[.]zonet[.]us
free[.]gmailboxes[.]com

frickl[.]purpledaily[.]com
friends[.]arrowservice[.]net
fsol[.]businessformars[.]com
ftel[.]businessformars[.]com
gao[.]gaokew[.]com
gatu[.]arrowservice[.]net
gg[.]arrowservice[.]net
gl[.]gmailboxes[.]com
glj[.]purpledaily[.]com
gmailboxes[.]com
happy[.]arrowservice[.]net
help[.]gmailboxes[.]com
hill[.]arrowservice[.]net
home[.]arrowservice[.]net
honeywater[.]keren[.]la
host[.]arrowservice[.]net
house[.]gmailboxes[.]com
index[.]arrowservice[.]net
info[.]bigish[.]net
info[.]hj-spa[.]com
information[.]trickip[.]org
int[.]busketball[.]com
intel[.]busketball[.]com
intel[.]gmailboxes[.]com
invest[.]gmailboxes[.]com
itlove[.]bigish[.]net
jackhouse[.]bigish[.]net
junier[.]busketball[.]com
kbwfj[.]arrowservice[.]net
klbis[.]bigish[.]net
kl-hqun[.]gmailboxes[.]com
kllhd[.]bigish[.]net
klwest[.]purpledaily[.]com
klzafin[.]bigish[.]net
loading[.]bigish[.]net
love[.]arrowservice[.]net
love[.]busketball[.]com
lovecow[.]homenet[.]org
lovewater[.]now[.]im
mail[.]bigish[.]net
mail[.]gmailboxes[.]com
mail-na[.]businessformars[.]com
main[.]busketball[.]com
main[.]gmailboxes[.]com
max[.]arrowservice[.]net

mbc[.]busketball[.]com
mc[.]bigish[.]net
me[.]busketball[.]com
micyuisyahooapis[.]com
midstate[.]arrowservice[.]net
milk[.]arrowservice[.]net
mini[.]arrowservice[.]net
miss[.]pwnz[.]org
mko[.]busketball[.]com
mkx[.]arrowservice[.]net
mkx[.]gmailboxes[.]com
monewf[.]bigish[.]net
monlc[.]marsbrother[.]com
mos[.]arrowservice[.]net
moto[.]busketball[.]com
mpe[.]arrowservice[.]net
msdn[.]bigish[.]net
new[.]arrowservice[.]net
newfe[.]purpledaily[.]com
news[.]busketball[.]com
newspappers[.]org
nokkia[.]bigish[.]net
nousage[.]arrowservice[.]net
nrcod[.]arrowservice[.]net
oliver[.]arrowservice[.]net
omin[.]marsbrother[.]com
ope[.]coastmaritime[.]org
opp[.]coastmaritime[.]org
opp[.]globalsecuriy[.]org
orca[.]arrowservice[.]net
paekl[.]gmailboxes[.]com
pdns[.]info[.]tm
phb[.]arrowservice[.]net
pieckl[.]bigish[.]net
point[.]gmailboxes[.]com
ppt[.]arrowservice[.]net
ppt[.]ezua[.]com
purpledaily[.]com
qhun-mons[.]businessformars[.]com
records[.]marsbrother[.]com
release[.]busketball[.]com
repid[.]arrowservice[.]net
rfckl[.]bigish[.]net
rice[.]bigish[.]net
rixiokl[.]bigish[.]net

russiaactions[.]summitnato[.]ro
saltlakenews[.]org
sbasun[.]busketball[.]com
scpkl[.]bigish[.]net
sea[.]arrowservice[.]net
service[.]arrowservice[.]net
service[.]purpledaily[.]com
services[.]busketball[.]com
services[.]gmailboxes[.]com
skill[.]arrowservice[.]net
sksucc[.]arrowservice[.]net
sona[.]arrowservice[.]net
spckl[.]bigish[.]net
spcmon[.]marsbrother[.]com
sremx[.]bigish[.]net
ssun[.]arrowservice[.]net
stock[.]bigish[.]net
stoneal[.]bigish[.]net
stulaw[.]bigish[.]net
stuwal[.]gmailboxes[.]com
suicide[.]suicide-forum[.]com
sun[.]arrowservice[.]net
suncirf[.]bigish[.]net
suntop[.]arrowservice[.]net
sword[.]bigish[.]net
tclient[.]arrowservice[.]net
tia[.]gmailboxes[.]com
topbox[.]gmailboxes[.]com
topbus[.]busketball[.]com
topkl[.]bigish[.]net
topmoney[.]purpledaily[.]com
tour[.]bigish[.]net
trb[.]arrowservice[.]net
trip[.]arrowservice[.]net
ttestt[.]arrowservice[.]net
ug-rj[.]arrowservice[.]net
update[.]busketball[.]com
updating[.]ddns[.]info
usapappers[.]com
ustop[.]bigish[.]net
vipmx[.]businessformars[.]com
vockl[.]bigish[.]net
walk[.]bigish[.]net
walstb[.]gmailboxes[.]com
was[.]arrowservice[.]net

wasa[.]arrowservice[.]net
wcasekl[.]gmailboxes[.]com
web[.]arrowservice[.]net
weblog[.]bigish[.]net
webmail[.]arrowservice[.]net
westjoe[.]purpledaily[.]com
westking[.]bigish[.]net
westnew[.]marsbrother[.]com
what[.]arrowservice[.]net
whl[.]bigish[.]net
wk[.]gmailboxes[.]com
works[.]myddns[.]com
workstation[.]arrowservice[.]net
www[.]arrowservice[.]net
www[.]globalsecuriy[.]org
www-01[.]marsbrother[.]com
www-02[.]marsbrother[.]com
www2[.]dsmtp[.]com
www2[.]wikaba[.]com
www-dell[.]marsbrother[.]com
www-hp[.]marsbrother[.]com
www-ibm[.]busketball[.]com
wwww[.]arrowservice[.]net
zgrshy[.]zyns[.]com
zgrshy10[.]zyns[.]com
zgrshy11[.]zyns[.]com

****
Malware Indicator Awareness List
****
MD5 Checksum
242946ed32dc3749e5b4f7827b905e5e
b2ddcf194cacc69ee7bcd3f9989f6162
5c58a8d8cab00ad3fac419da03644b59
1cc0ce317edad8521c236c84b74e14f8
9d42ce823fc711eaeb542f4050f17125
8845cb5b4e450cb10a3b6ca41a9b4319
1fe90bd6a1092ec74f78181785e785f8
a6e7504315f5dada56189635cd7a27b1
957b13cffeea1722a2369e2bb5e79287
0e98cffc64a1e822946066f62e1fd02c
1a87d955bc876098f50b8a48d8db4aaf
a207590fdcec8018c5a902483b651302
9087f73602d81be177b568e15f6b033b
a884545277cae36928f36c372f6a18ac

051967e8a92a6e1b02a6c8b2225b01c5
314d5943e55c065e40f3a20ab56de7a3
697b18e734740ad9129ebd241040492a
7f7cc1a8d7a6bbe6a52c94bb7f41f727
b8988e23d4d8427584637d1f9ab78a8e
e6446d52e9f4b5c2c5a9ac850281cae8
bf778439895829ff986207900bfcfe02
1d69504a3d3ac32275fa4df8af25d1f7
cf96139290c09963a32506cd85825ed3
3b266b165468b810cd456cdf88ca8619
88c0e5a4ca408ac12acaaf7a9ef9eb49
08ac41ce00bf436a3dc23c4639d5f5ed
2a8f14ed1cb6fdb49ab946fc54fc8c86
4a54d7878d4170c3d4e3c3606365c42c
659fb07c70034571de7a1b4b5ac86b01
7c6443e646c973ac10a1048d521a70a9
82c598abdf848c6fef03c63f5cf7feaf
888eadff6982de01c60891ce185473b7
9a847c1f54359ffd3c335e97600f6f5d
a19e68e72084d867a39776faaa6f5fce
e27f0975fd3278e7303102783767c508
d36427db95cd055a5a25f445d80c27ee
e3faff9149fed468aa63f10a40b935d6
c7f7d8bf633a1b81088315b93831e82d
7f90942ace185ca1ba5610f6eddf3376
ad95f613fc4b644bd5e3230eb0b5dbcc
4943a255952e107fec41e9c29a5b2724
c7d5845718c7fa5a777bcd801d8e00f4
34062335f95d074272a5487be37ee701
3f82f1cba90d320af90d965a321a1187
45a4141f603c8bfa7950e15a074ef976
4bc894e369f31b7190eaeb99c23eb000
55f41be09de5dcd5aaa0132804506868
6eb99bed5b5fcb3fdb26f37aff2c9adb
87cf89742ef0a1c1f76664caa6c0a1a7
b9f20ff30ce6dbb461ab6d27fe8c4bda
bcc6addece28265390b2d535d65c49b8
fc277785c49d743697adc06a3db77c5d
2de36fa400225c39481283daf4a686d8
324a7d63a178f3ac8dde5b59675ef282
37bd6fceaf412427db8c8a34c5ad9ba7
3a33dbe37292a1cbfa760d1892812e08
c243a7c1cf23b91f73100bb9e947439e
caafdafdd17abe0f0303a456bcd4ab01
e194a6d7f1aa6671d2134047050a4322

e35414a5cb10bccf6424ee51f0cdd6cc
21e35f309f7d6368fd8346ba409fab73
3fa99e50933ce584d010ec194229764a
41b551d30321a5ae1342180d1e73e82e
7cd15bb31ff889e81f370d0535e02493
9428a54a7acd6adc3f9b662ef432edf4
f82d3b270b16780044817978f4f3fe1a
22e10cbe46f406f5f1be0d613db4c2c3
a6cba31fcca49ff9ed6fd9894644de9e
48fc61a8f94c6e7c9c8965817f57af7e
00b61db083b07a64fb6072b42aa83dc1
aea5dc22e706c836d056f4ba1f13dea3
3599a78c7e99b451c00d3490f17f842f
137aad4c7c4e0d8ba0ad74c34cf8434c
14095f921f50cf639bf00b389ea79959
2d2876bd1f263babe9d09e8e950916cc
ac9e0b2af215821f7223b6eaeaea03db
c5851c22c2a2e4bccf015a20e0af6cac
c9645367f032bf12b251e4f30e21b936
cec766518fa5b607157e92e9c24c0d03
da521200a939a9fe85f467d65d419990
6428ac60d1eea0f20073cfb869674266
affc4d42a6a66f6a745c5702608d0442
c296ae9220c44e51cfbeb029b6103d1b
cfdd9241adcda8755c54032fd2b5757d
db22512d361a339cfadaa275c550b385
e2a557b39231ee91724c150e3ec4b493
491db327f479a1a34898229811fa8a5d
6b6a9062e9c74a98a1f1a2fe7c2adcd7
D46D261EC92DAF703CD584F10037198C
ce2f4abe8b4f3a57891ca865c4fe6ece
3de1bd0f2107198931177b2b23877df4
a207590fdceb8018b5a902483b651302
0ba71b7dbf0394f509ef6174faa0bbf0
1a8ee0ec99320e213432a26a91df8811
232d1be2d8cbbd1cf57494a934628504
6ae05937bce80b7d16497cb82e6a52d6
73e81b099f9b469a07063555e822dac1
39f1ac84ad939fb72cc6e438ecea9729
3a2cdf3c09c061a5cf6a58069506955a
f3c6c797ef80787e6cbeeaa77496a3cb
217c9dc682018c7055c660dd5dd0f8ca
1cb4b79e338bec06e65ff8d37de53c55
dd2aec3803ce39c4a148325d33f575e3
5474e37159b1a438659e7e5bf1f45389

48437eb28ff1bfff5c0a4661a8c3055d
310cba19e6f7fd07adf203c27e46a0c9
9cb4ee95948292be131f7c4ee3bdcf21
7ce22cb797d2940818154ce0dcc48306
53f1e2e5f0152a3a119e112b6cf5426e
204c13f7ed2d3e5c78f3ef8a44eb561c
ca6fe7a1315af5afeac2961460a80569
53f49c58613669f25921de0b6dae1268
82e0472271500713cd2457921ab1c565
93e33bf0417a857ae894ed294aa0e15a
9e5df2cfd0c8def21c9e114d1d2696dd