Joint Indicator Bulletin (JIB) – INC260425-2

February 26, 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@us-cert.gov.

Document Overview

This Joint Indicator Bulletin is comprised of sections covering domain names 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 compromised IP addresses and domains used by such actors.

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
****
100[.]42[.]216[.]230
108[.]166[.]200[.]130
108[.]171[.]211[.]152
108[.]171[.]251[.]102
113[.]196[.]231[.]13
12[.]11[.]239[.]25
12[.]14[.]129[.]91
12[.]15[.]0[.]131
12[.]167[.]251[.]84
12[.]2[.]49[.]115
12[.]232[.]138[.]23
12[.]30[.]41[.]134
12[.]33[.]114[.]160
12[.]33[.]114[.]224
121[.]55[.]220[.]79
122[.]146[.]219[.]130
129[.]44[.]254[.]139
140[.]112[.]19[.]195
140[.]116[.]72[.]95

161[.]58[.]177[.]111
161[.]58[.]93[.]50
163[.]20[.]172[.]230
172[.]254[.]222[.]138
173[.]10[.]39[.]53
173[.]160[.]48[.]149
173[.]163[.]133[.]177
173[.]224[.]213[.]184
173[.]224[.]213[.]247
173[.]224[.]215[.]177
173[.]231[.]45[.]231
173[.]254[.]222[.]138
199[.]119[.]201[.]124
203[.]170[.]198[.]56
204[.]11[.]236[.]81
204[.]111[.]73[.]150
204[.]111[.]73[.]155
204[.]12[.]248[.]2
204[.]13[.]68[.]10
204[.]14[.]142[.]210
204[.]14[.]88[.]45
204[.]215[.]64[.]28
204[.]249[.]169[.]4
204[.]249[.]169[.]5
204[.]45[.]16[.]204
204[.]74[.]218[.]145
204[.]9[.]208[.]14
205[.]159[.]83[.]12
205[.]209[.]161[.]13
205[.]209[.]172[.]204
205[.]234[.]168[.]48
207[.]173[.]155[.]44
207[.]36[.]209[.]221
207[.]40[.]43[.]102
207[.]71[.]209[.]148
208[.]109[.]50[.]151
208[.]185[.]233[.]163
208[.]239[.]156[.]123
208[.]37[.]108[.]211
208[.]53[.]100[.]162
208[.]68[.]171[.]220
208[.]69[.]32[.]231
208[.]77[.]45[.]131
208[.]77[.]45[.]142
208[.]77[.]45[.]82

208[.]77[.]51[.]210
208[.]87[.]241[.]135
209[.]113[.]219[.]6
209[.]18[.]107[.]90
209[.]208[.]114[.]83
209[.]208[.]95[.]7
209[.]247[.]221[.]40
209[.]247[.]221[.]50
209[.]25[.]220[.]42
209[.]74[.]45[.]226
209[.]75[.]160[.]64
210[.]244[.]193[.]249
211[.]21[.]210[.]220
216[.]1[.]59[.]4
216[.]143[.]158[.]107
216[.]145[.]228[.]153
216[.]213[.]199[.]194
216[.]215[.]103[.]2
216[.]36[.]123[.]11
216[.]62[.]168[.]249
216[.]65[.]11[.]111
218[.]32[.]87[.]100
219[.]87[.]141[.]74
24[.]249[.]171[.]231
46[.]105[.]227[.]80
50[.]62[.]130[.]15
58[.]86[.]239[.]103
60[.]251[.]74[.]9
61[.]218[.]144[.]43
61[.]221[.]67[.]184
63[.]102[.]52[.]130
63[.]111[.]125[.]50
63[.]114[.]150[.]17
63[.]120[.]209[.]85
63[.]126[.]244[.]253
63[.]134[.]229[.]137
63[.]134[.]229[.]138
63[.]134[.]233[.]60
63[.]134[.]233[.]62
63[.]138[.]249[.]244
63[.]139[.]221[.]130
63[.]139[.]221[.]26
63[.]147[.]185[.]40
63[.]147[.]31[.]178
63[.]162[.]4[.]2

63[.]162[.]42[.]46
63[.]163[.]61[.]9
63[.]171[.]89[.]5
63[.]195[.]112[.]159
63[.]200[.]159[.]118
63[.]211[.]192[.]150
63[.]211[.]192[.]181
63[.]225[.]225[.]42
63[.]228[.]128[.]19
63[.]245[.]62[.]11
63[.]246[.]147[.]11
63[.]64[.]175[.]136
63[.]73[.]10[.]130
63[.]73[.]11[.]15
63[.]82[.]1[.]226
63[.]84[.]24[.]72
63[.]84[.]24[.]77
63[.]97[.]51[.]121
64[.]122[.]68[.]213
64[.]126[.]12[.]2
64[.]14[.]81[.]30
64[.]184[.]2[.]3
64[.]25[.]15[.]226
64[.]32[.]164[.]43
64[.]34[.]172[.]210
64[.]4[.]217[.]138
64[.]50[.]130[.]74
64[.]65[.]230[.]242
64[.]81[.]194[.]171
64[.]81[.]252[.]163
65[.]107[.]54[.]158
65[.]112[.]75[.]130
65[.]114[.]195[.]226
65[.]116[.]58[.]5
65[.]119[.]5[.]3
65[.]124[.]105[.]76
65[.]17[.]233[.]30
65[.]207[.]215[.]10
66[.]0[.]167[.]105
66[.]153[.]38[.]202
66[.]155[.]114[.]145
66[.]16[.]75[.]201
66[.]167[.]118[.]29
66[.]179[.]156[.]10
66[.]181[.]8[.]162

66[.]23[.]224[.]213
66[.]28[.]12[.]144
66[.]55[.]14[.]78
66[.]85[.]185[.]201
66[.]92[.]12[.]252
66[.]93[.]91[.]235
67[.]102[.]7[.]3
67[.]109[.]132[.]202
67[.]109[.]90[.]99
67[.]132[.]222[.]231
67[.]133[.]107[.]131
67[.]19[.]22[.]82
67[.]88[.]107[.]8
67[.]93[.]14[.]2
68[.]165[.]209[.]227
68[.]72[.]242[.]130
69[.]11[.]244[.]91
69[.]152[.]184[.]182
69[.]20[.]4[.]85
69[.]20[.]5[.]223
69[.]20[.]6[.]142
69[.]20[.]61[.]230
69[.]25[.]176[.]110
69[.]25[.]50[.]10
69[.]28[.]168[.]10
69[.]3[.]32[.]220
69[.]39[.]133[.]114
69[.]39[.]133[.]115
69[.]39[.]133[.]117
69[.]5[.]38[.]37
69[.]53[.]120[.]170
69[.]55[.]180[.]4
69[.]69[.]94[.]3
69[.]74[.]43[.]87
69[.]90[.]123[.]6
69[.]95[.]204[.]2
70[.]62[.]232[.]98
70[.]86[.]21[.]146
71[.]130[.]117[.]49
71[.]16[.]27[.]212
71[.]6[.]141[.]230
71[.]6[.]51[.]180
71[.]6[.]51[.]181
71[.]63[.]28[.]61
72[.]167[.]162[.]96

72[.]167[.]33[.]182
72[.]22[.]11[.]30
72[.]236[.]177[.]171
72[.]242[.]59[.]163
72[.]245[.]176[.]82
72[.]9[.]145[.]216
72[.]91[.]193[.]160
72[.]94[.]51[.]6
74[.]115[.]0[.]29
74[.]115[.]6[.]20
74[.]165[.]93[.]5
74[.]200[.]213[.]110
74[.]206[.]99[.]189
74[.]208[.]227[.]72
74[.]208[.]45[.]82
74[.]211[.]195[.]39
74[.]213[.]52[.]10
74[.]55[.]160[.]98
74[.]55[.]178[.]42
74[.]63[.]87[.]106
74[.]86[.]197[.]56
74[.]86[.]31[.]98
74[.]9[.]137[.]146
74[.]92[.]102[.]227
74[.]94[.]16[.]166
74[.]94[.]52[.]114
75[.]126[.]166[.]204
75[.]145[.]139[.]19
75[.]148[.]254[.]114
75[.]52[.]208[.]225
75[.]77[.]82[.]115
75[.]77[.]82[.]219
76[.]160[.]133[.]60
76[.]161[.]97[.]99
77[.]247[.]180[.]154
94[.]195[.]239[.]81
98[.]126[.]107[.]34
****

Domain Name Awareness List
****

advanbusiness[.]com
aoldaily[.]com
applesoftupdate[.]com
arrowservice[.]net
articles[.]twilightparadox[.]com

aunewsonline[.]com
bechtel[.]chickenkiller[.]com
bigish[.]net
businessconsults[.]net
businessformars[.]com
canadatvsite[.]com
canoedaily[.]com
chileexe77[.]com
climate[.]undo[.]it
cnndaily[.]com
cnndaily[.]net
comrepair[.]net
defenceonline[.]net
downloadsite[.]me
e-cardsshop[.]com
economic[.]mooo[.]com
firefoxupdata[.]com
freshreaders[.]net
honeycow[.]keren[.]la
hugesoft[.]org
info[.]serveusers[.]com
issnbgkit[.]net
jobsadvanced[.]com
marsbrother[.]com
mcafeepaying[.]com
news[.]trickip[.]org
newsonet[.]net
newsonlinesite[.]com
niemannews[.]com
nytimesnews[.]net
pop-musicsite[.]com
rssadvanced[.]org
satellitebbs[.]com
staycools[.]net
symanteconline[.]net
thehealthmood[.]net
todayusa[.]org
upload[.]ignorelist[.]com
usabbs[.]org
usnewssite[.]com
voiceofman[.]com
work[.]myftp[.]name
yahoodaily[.]com