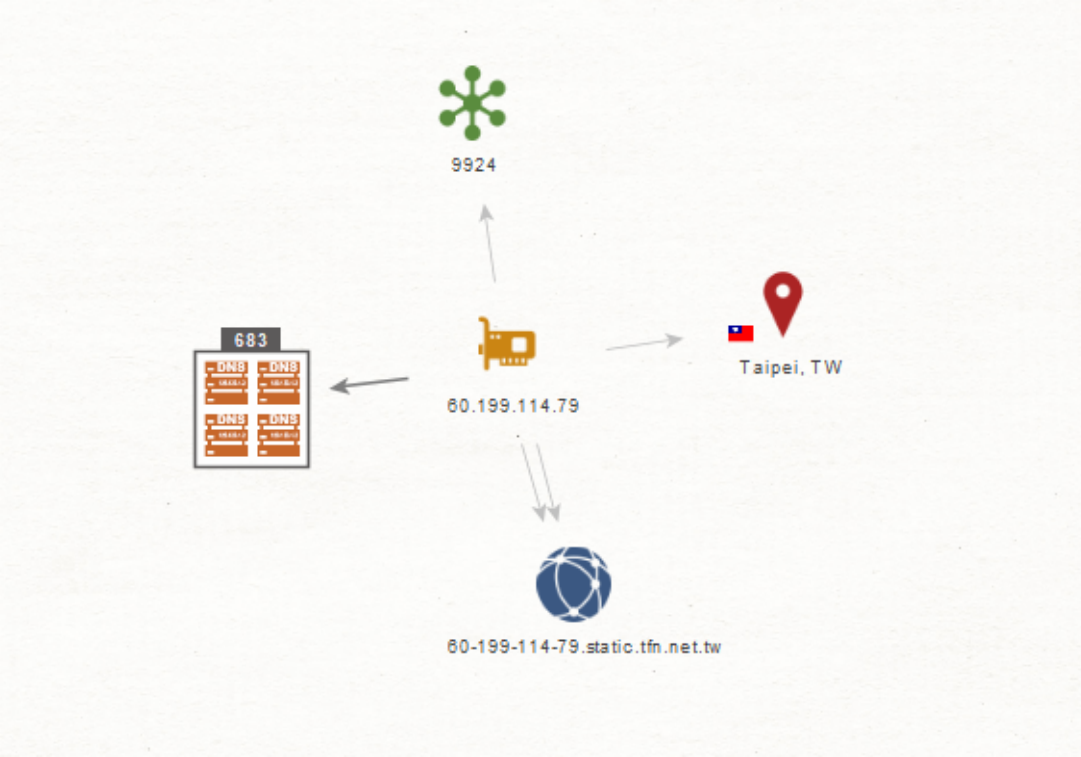
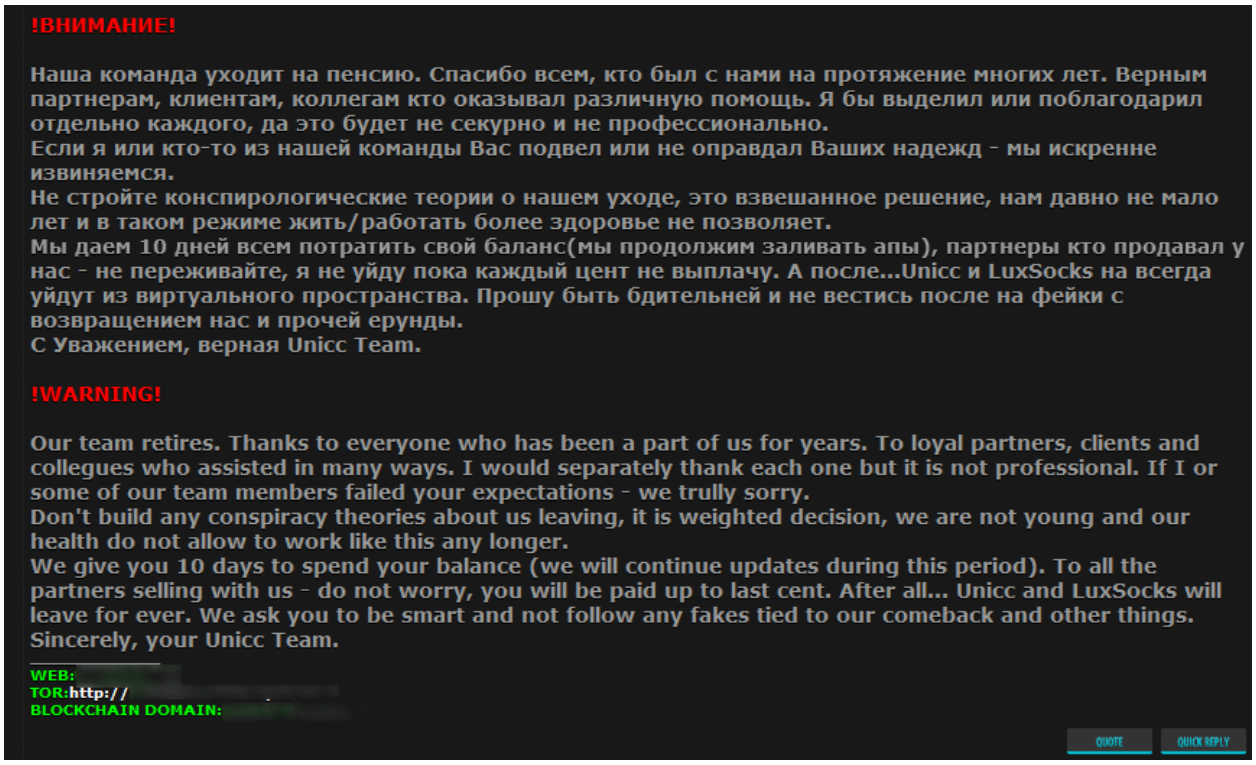
00. The Recent Infraud Cybercrime Organization Bust and The Internet-Connected Infrastructure of the Cybercrime Syndicate - An OSINT Analysis



In the wake of the recent bust of the high-profile cybercriminal organization known as the Infraud Organization we've decided to take a deeper peek inside our archives of current and historical intelligence and offer an in-depth and never discussed before discussion on the Internet-connected infrastructure of the InFraud cybercriminal organization which was basically a high-profile cybercrime-friendly forum communities with variety of extremely popular "value-added" services in the form of a multi-tude of fully working online E-Shops for stolen and compromised credit cards information.

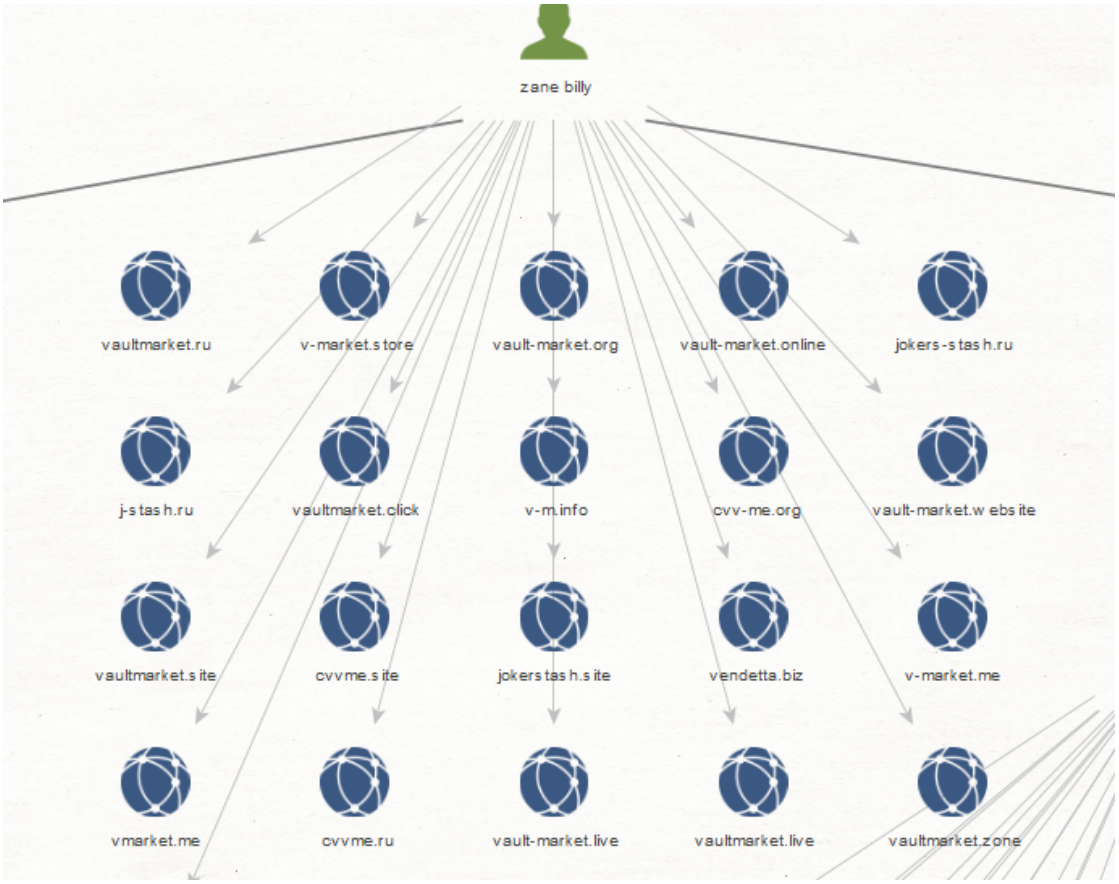


In this analysis we'll use Maltego in combination with WhoisXML API' vast and in-depth real-time and historical WHOIS database and offer an in-depth peek and discussion on the Internet-connected infrastructure of the InFraud organization.

Primary domains part of the InFraud Organization known to have been in circulation include:

infraud[.]su
infraud[.]ru
infraud[.]us
infraud[.]org
infraud[.]biz
infraud[.]net
infraud[.]info
jabber[.]ms
infraud[.]ws
infraud[.]cc
infraud[.]name

The primary responding IP for the InFraud Organization's primary forum domain includes:
60[.]199[.]114[.]79



We were also able to find a variety of other online E-Shops for stolen and compromised credit cards information that are actually known to be using the same infrastructure as the InFraud Organization's infrastructure such as for instance:

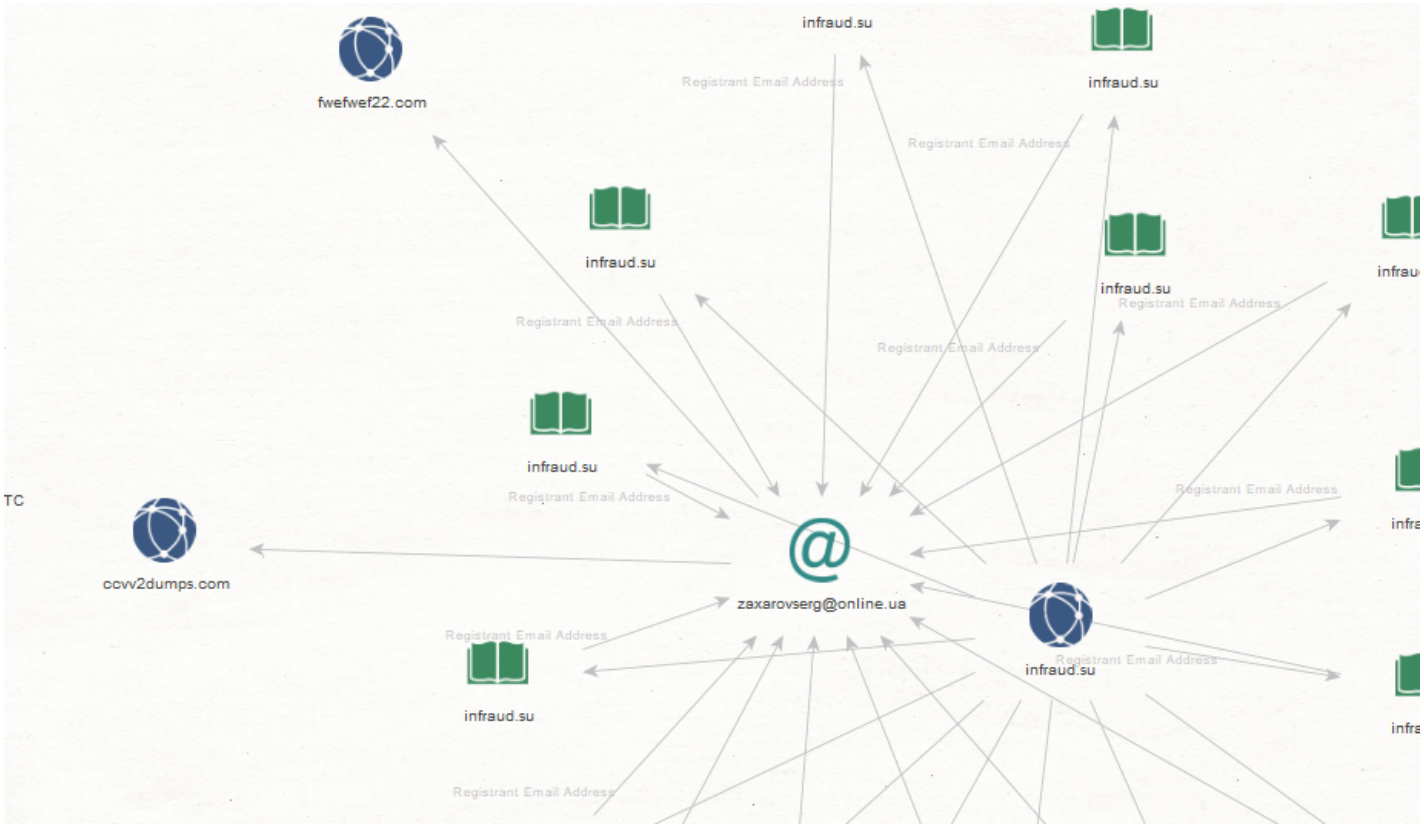
vaultmarket[.]ru
vaultmarket[.]click
jokers-stash[.]ru
j-stash[.]ru
vault-market[.]website
vaultmarket[.]site
v-m[.]info
cvv-me[.]org
vault-market[.]online
vaultmarket[.]live
vaultmarket[.]zone
vault-market[.]live
vault-market[.]org
infraud[.]world
vendetta[.]biz
v-market[.]store

v-market[.]me
cvvme[.]site
jokerstash[.]site
cvvme[.]ru
vmarket[.]me

Including the following domains are known to have been using InFraud Organization's online infrastructure for hosting related E-Shops for stolen and compromised credit cards information which we managed to find out using WhoisXML API's vast and in-depth real-time and historical WHOIS database:

jokers-stash[.]su
vault-market[.]sale
vaultmarket[.]club
vaultmarket[.]domains
infraud[.]us
vendeta[.]shop
cvv-me[.]us
jokers-stash[.]com
jokersstash[.]us
cvvme[.]us
joker-stash[.]us
jokers-stash[.]us
jstash[.]me
vaultmarket[.]market

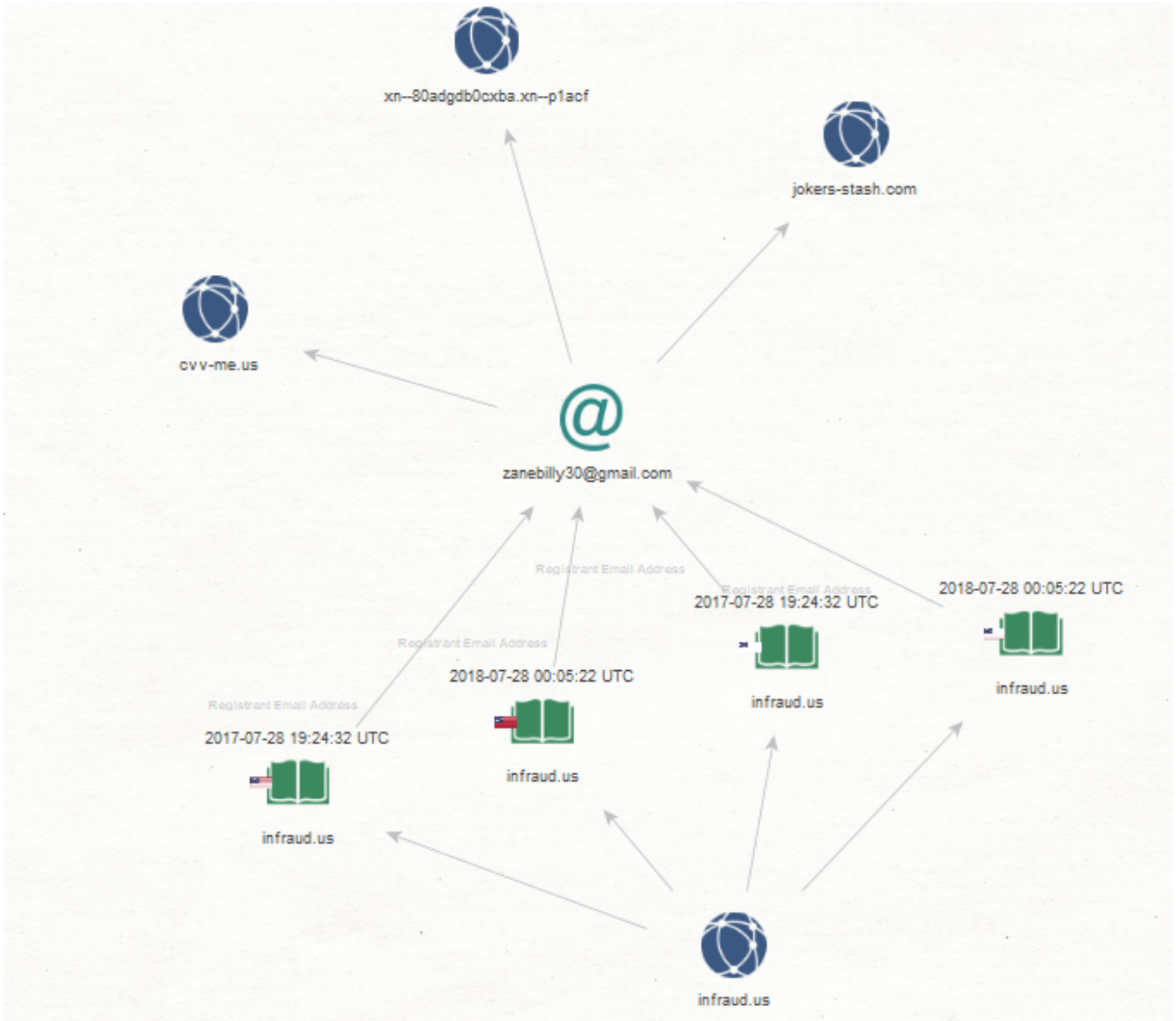
v-m[.]shop
vaultmarket[.]me
vendeta[.]us
cvv-market[.]us
j-stash[.]us
cvv2[.]us
vaultmarket[.]tech
v-market[.]us
vault-market[.]tech
vault-market[.]us
vaultmarket[.]us
vaultmarket[.]su
jstash[.]us
jokerstash[.]us
vault-market[.]su
vendetta[.]su



Including the following related malicious and fraudulent domain names which we found using WhoisXML API's vast and in-depth real-time and historical WHOIS database once again part of InFraud Organization's online infrastructure:

jokerstash[.]website
jokerstash[.]online

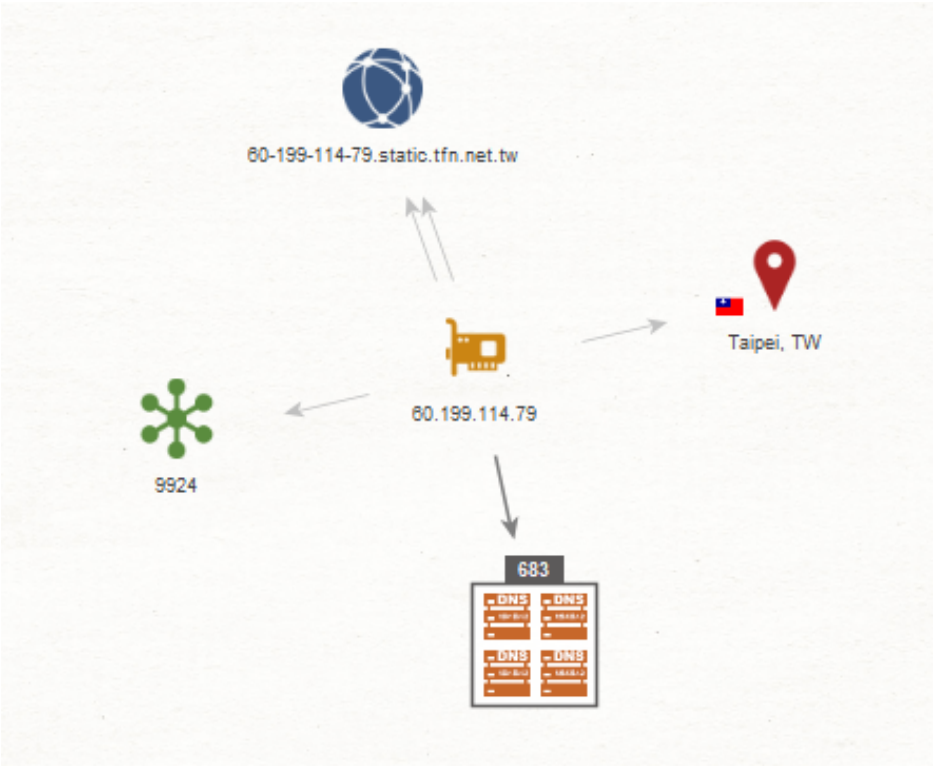
j-stash[.]online
jokerstash[.]tech
j-stash[.]tech



Including yet another batch of malicious and fraudulent domains which offer access to E-Shops for stole and compromised credit cards information which we found using WhoisXML API's vast and in-depth real-time and historical WHOIS database:

crimemarket[.]su
bphosting[.]su
dogshops[.]su
cvvshops[.]su
approved-xxx[.]su

wt1shop[.]su
buycvv[.]su
blockichain[.]su
sky-fraud[.]su
myfeshop[.]su
load-file[.]su
unidumps[.]su
godtor[.]su
dumpsvendor[.]su
monogo[.]su
ktmstore[.]su
blackservice[.]su
goldplastic[.]net
infraud[.]su
fwefwef22[.]com
ccvv2dumps[.]com
thugcarders[.]su
dichvusocks[.]su
uas-store[.]su
stuffex[.]su
ulow[.]su
uas-shop[.]su
8dollar[.]su
1337zone[.]su
qualitytools[.]su
madb[.]su



Including the following responding IPs part of InFraud Organization's online infrastructure:

198[.]54[.]121[.]112
103[.]136[.]42[.]76
149[.]129[.]129[.]211
47[.]74[.]137[.]231
161[.]117[.]7[.]46
144[.]76[.]169[.]106
185[.]162[.]131[.]61
162[.]219[.]51[.]2
162[.]255[.]119[.]132
198[.]54[.]116[.]206
199[.]188[.]200[.]47
192[.]64[.]119[.]200
149[.]129[.]225[.]92
92[.]53[.]77[.]141
212[.]47[.]195[.]232
138[.]68[.]149[.]101
46[.]183[.]217[.]204
198[.]54[.]117[.]216
54[.]72[.]130[.]67
208[.]91[.]197[.]44
119[.]28[.]137[.]123

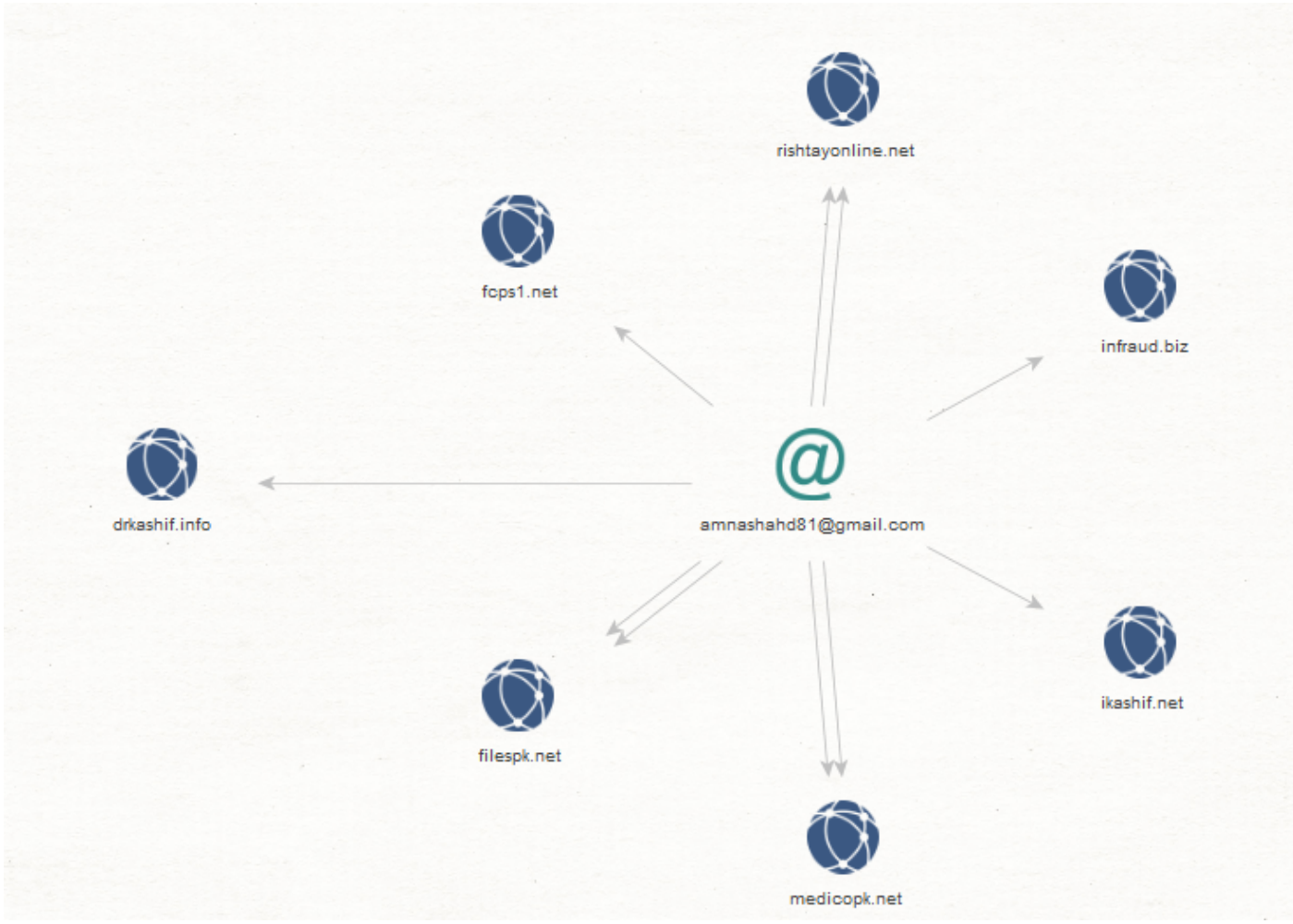
104[.]28[.]17[.]97
119[.]28[.]69[.]169
82[.]221[.]129[.]133
8[.]209[.]108[.]128
194[.]147[.]34[.]2
93[.]170[.]130[.]136
149[.]154[.]69[.]218
51[.]89[.]114[.]5
78[.]155[.]206[.]161
208[.]91[.]197[.]241
85[.]119[.]150[.]155
172[.]104[.]104[.]241
49[.]51[.]192[.]130
198[.]54[.]117[.]215
94[.]229[.]72[.]118
162[.]210[.]196[.]171
94[.]229[.]72[.]121
45[.]153[.]73[.]8
93[.]189[.]45[.]52
35[.]204[.]138[.]31
194[.]85[.]61[.]76
27[.]102[.]128[.]115
185[.]99[.]133[.]20
91[.]195[.]240[.]117
192[.]64[.]119[.]87
198[.]54[.]117[.]212
198[.]54[.]117[.]218
77[.]246[.]156[.]116
45[.]63[.]40[.]156
161[.]35[.]221[.]28
198[.]54[.]117[.]217
190[.]97[.]166[.]165
198[.]54[.]117[.]200
198[.]105[.]244[.]11
192[.]64[.]119[.]105
23[.]202[.]231[.]168
23[.]195[.]69[.]108
217[.]70[.]184[.]38
195[.]39[.]197[.]202
5[.]39[.]10[.]93
192[.]64[.]119[.]253
195[.]39[.]196[.]44
213[.]167[.]231[.]2
104[.]239[.]213[.]7

23[.]195[.]69[.]112
199[.]59[.]243[.]200
217[.]70[.]184[.]50
198[.]105[.]254[.]11
83[.]222[.]14[.]207
23[.]217[.]138[.]112
207[.]244[.]67[.]215
199[.]59[.]242[.]153
37[.]48[.]65[.]149
185[.]183[.]96[.]247
103[.]224[.]182[.]242
192[.]254[.]190[.]243
94[.]75[.]240[.]174
104[.]21[.]61[.]28
5[.]79[.]68[.]107
207[.]244[.]67[.]218
193[.]70[.]95[.]200
62[.]109[.]19[.]78
45[.]32[.]157[.]131
92[.]242[.]40[.]127
172[.]67[.]149[.]237
172[.]67[.]205[.]242
92[.]38[.]135[.]251
192[.]64[.]119[.]172
82[.]202[.]241[.]20
45[.]139[.]186[.]87
198[.]54[.]120[.]111
178[.]79[.]187[.]121
192[.]64[.]119[.]171
64[.]227[.]102[.]101
47[.]254[.]197[.]213
162[.]255[.]119[.]115
198[.]54[.]117[.]199
146[.]112[.]61[.]107
192[.]64[.]119[.]37
47[.]74[.]188[.]120
47[.]52[.]233[.]0
47[.]89[.]58[.]141
185[.]143[.]174[.]19
45[.]142[.]212[.]24
192[.]64[.]119[.]170
216[.]128[.]146[.]177
162[.]255[.]119[.]98
95[.]141[.]36[.]178

27[.]102[.]128[.]114
60[.]199[.]114[.]79
149[.]129[.]136[.]150
198[.]105[.]254[.]74
149[.]129[.]223[.]249
198[.]105[.]244[.]74
194[.]67[.]71[.]176
45[.]139[.]186[.]233
90[.]156[.]128[.]133
185[.]178[.]208[.]165
23[.]236[.]62[.]147
149[.]129[.]134[.]51
216[.]185[.]152[.]158
107[.]172[.]46[.]71
88[.]119[.]179[.]216
185[.]177[.]218[.]136
99[.]83[.]154[.]118
45[.]8[.]230[.]94
78[.]138[.]31[.]80
88[.]119[.]179[.]132
185[.]154[.]53[.]119
195[.]133[.]48[.]60
94[.]130[.]10[.]95
40[.]121[.]200[.]45
69[.]195[.]137[.]250
185[.]159[.]130[.]7
109[.]70[.]26[.]37
23[.]217[.]138[.]108
23[.]202[.]231[.]167
213[.]179[.]214[.]122
49[.]51[.]33[.]70
47[.]74[.]177[.]133
194[.]147[.]35[.]176
95[.]213[.]203[.]64
92[.]53[.]126[.]190
192[.]64[.]119[.]119
161[.]117[.]12[.]56
149[.]129[.]226[.]244
213[.]183[.]61[.]45
162[.]255[.]119[.]114
162[.]255[.]119[.]7
198[.]54[.]117[.]211
198[.]54[.]117[.]197
198[.]54[.]117[.]198

47[.]74[.]153[.]70
49[.]51[.]85[.]205
193[.]187[.]174[.]103
47[.]52[.]142[.]249
46[.]21[.]248[.]49
216[.]239[.]34[.]21
185[.]53[.]177[.]9
91[.]237[.]88[.]232
199[.]188[.]200[.]88
35[.]198[.]119[.]28
185[.]231[.]153[.]127
47[.]74[.]235[.]179
198[.]251[.]89[.]144
90[.]156[.]128[.]111
185[.]8[.]173[.]73
194[.]58[.]56[.]182
158[.]255[.]3[.]157
47[.]88[.]156[.]38
81[.]171[.]8[.]6
92[.]53[.]77[.]40
217[.]16[.]27[.]181
87[.]242[.]73[.]102
46[.]166[.]184[.]101
188[.]40[.]76[.]96
172[.]67[.]160[.]80
47[.]91[.]72[.]137
194[.]58[.]56[.]97
68[.]66[.]248[.]11
172[.]64[.]95[.]2
104[.]27[.]169[.]231
194[.]58[.]56[.]189
194[.]58[.]56[.]40
107[.]161[.]23[.]204
72[.]52[.]179[.]175
104[.]27[.]161[.]246
47[.]254[.]213[.]246
47[.]254[.]201[.]251
149[.]129[.]219[.]23
195[.]186[.]210[.]241
185[.]61[.]153[.]99
185[.]181[.]104[.]82
198[.]27[.]68[.]160
192[.]64[.]119[.]101
88[.]212[.]208[.]67

68[.]183[.]38[.]101
162[.]255[.]119[.]12
5[.]188[.]29[.]36
184[.]168[.]221[.]57
91[.]218[.]115[.]152
50[.]63[.]202[.]48
91[.]212[.]124[.]25



Including the following malicious and fraudulent name servers known to have been offering services and providing infrastructure hosting for InFraud Organization's Internet-connected infrastructure:

ns4[.]unlim[.]com
ns1[.]expired[.]r01[.]ru
ns2[.]unlim[.]com
ns3[.]unlim[.]com
ns2[.]dddnsdomens[.]su
ns1[.]florenciyas[.]su
ns2[.]expired[.]r01[.]ru

ns1[.]dddnsdomens[.]su
ns1[.]r01[.]ru
ns2[.]r01[.]ru
c[.]dnspod[.]com
ns1[.]unlim[.]com
a[.]dnspod[.]com
b[.]dnspod[.]com
ns2[.]magpiedns[.]com
dns101[.]registrar-servers[.]com
ns1[.]wombatdns[.]com
dns102[.]registrar-servers[.]com
ns2[.]chookdns[.]com
dns21[.]name-services[.]com
ns1[.]magpiedns[.]com
dns22[.]name-services[.]com
ns2[.]wombatdns[.]com
ns1[.]nameself[.]com
ns2[.]nameself[.]com
cdn6[.]infraud[.]cc
dns1[.]yandex[.]ru
cdn7[.]infraud[.]cc
dns2[.]yandex[.]ru
jack[.]ns[.]cloudflare[.]com
ns1[.]x10hosting[.]com
ns1[.]chookdns[.]com
ns2[.]x10hosting[.]com
primaryns[.]kiev[.]ua
adi[.]ns[.]cloudflare[.]com
ns[.]secondary[.]net[.]ua
ns2[.]dnsnuts[.]com
cdn1[.]infraud[.]cc
c[.]dns[.]gandi[.]net
ns1[.]dnsnuts[.]com
cdn4[.]infraud[.]cc
dns1[.]registrar-servers[.]com
cdn5[.]infraud[.]cc
dns2[.]registrar-servers[.]com
cdn2[.]infraud[.]cc
cdn3[.]infraud[.]cc
nsc1[.]srv53[.]com
nsc1[.]srv53[.]org
a[.]dns[.]gandi[.]net
b[.]dns[.]gandi[.]net
nsd3[.]srv53[.]net

nsa2[.]srv53[.]com
pns2[.]cloudns[.]net
pns3[.]cloudns[.]net
nsb3[.]srv53[.]net
nsb4[.]srv53[.]org
nsb2[.]srv53[.]com
ns1[.]cloudns[.]net
ns4[.]infraud[.]cc
ns4[.]cloudns[.]net
pns1[.]cloudns[.]net
ns2[.]cloudns[.]net
ns3[.]cloudns[.]net
ns5[.]ciph[.]su
ns6[.]ciph[.]su
ns3[.]ciph[.]su
ns4[.]ciph[.]su
ns2[.]infraud[.]cc
ns3[.]infraud[.]cc
ns7[.]ciph[.]su
ns1[.]infraud[.]cc
ns1[.]ciph[.]su
ns2[.]ciph[.]su
ns2[.]xmail[.]sx[.]jabber[.]ms
ns1[.]xmail[.]sx
ns2[.]xmail[.]sx
ns42[.]domaincontrol[.]com
ns1[.]xmail[.]sx[.]jabber[.]ms
ns41[.]domaincontrol[.]com
phil[.]ns[.]cloudflare[.]com
ns1[.]cybercastco[.]com
ns2[.]renewyourname[.]net
dawn[.]ns[.]cloudflare[.]com
ns2[.]cybercastco[.]com
ns1[.]renewyourname[.]net
ns3[.]byet[.]org
1-you[.]njalla[.]no
ns1[.]byet[.]org
ns2[.]byet[.]org
2-can[.]njalla[.]in
3-get[.]njalla[.]fo
dns6[.]parkpage[.]foundationapi[.]com
albert[.]ns[.]cloudflare[.]com
dns5[.]parkpage[.]foundationapi[.]com
jill[.]ns[.]cloudflare[.]com

may[.]ns[.]cloudflare[.]com
cns2005[.]webhostbox[.]net
ns4[.]active-dns[.]com
art[.]ns[.]cloudflare[.]com
cns2006[.]webhostbox[.]net
ns3[.]imena[.]com[.]ua
ns1[.]imena[.]com[.]ua
ns2[.]imena[.]com[.]ua
ns2[.]active-dns[.]com
ns3[.]active-dns[.]com
ns1[.]active-dns[.]com
nsc4[.]srv53[.]com
nsd1[.]srv53[.]com
nsc2[.]srv53[.]net
nsc3[.]srv53[.]org
dns1[.]pochemu[.]ru
dns2[.]pochemu[.]ru
nsd1[.]srv53[.]net
nsd1[.]srv53[.]org
nsa1[.]srv53[.]com
nsa1[.]srv53[.]org
nsb4[.]srv53[.]com
nsb4[.]srv53[.]net
nsa3[.]srv53[.]net
nsb2[.]srv53[.]org
graham[.]ns[.]cloudflare[.]com
marjory[.]ns[.]cloudflare[.]com
dns1[.]magicwebindia[.]com
dns2[.]magicwebindia[.]com
idns1[.]ihc[.]ru
idns2[.]ihc[.]ru
expirepages-kiae-1[.]nic[.]ru
expirepages-kiae-2[.]nic[.]ru
master2[.]ispmgr[.]ihc[.]ru
ara[.]ns[.]cloudflare[.]com
slave2[.]ispmgr[.]ihc[.]ru
ns2[.]gooddnsserver[.]com
ns3[.]gooddnsserver[.]com
zeus[.]ns[.]cloudflare[.]com
ns1[.]gooddnsserver[.]com
ns1[.]expired[.]reg[.]ru
alpha[.]nickhost[.]com
ns2[.]hosting[.]reg[.]ru
ns2[.]expired[.]reg[.]ru

ns1[.]hosting[.]reg[.]ru
ns2[.]domain[.]ru
ns2[.]reg[.]ru
ns1[.]domain[.]ru
ns4[.]infobox[.]org
beta[.]nickhost[.]com
ns3[.]infobox[.]org
ns1[.]reg[.]ru
ns3[.]afraid[.]org
ns-57-a[.]gandi[.]net
ns1[.]afraid[.]org
ns2[.]afraid[.]org
ns4[.]afraid[.]org
ns-119-c[.]gandi[.]net
ns-140-b[.]gandi[.]net
expired1[.]privacy[.]com[.]ua
expired2[.]privacy[.]com[.]ua
dns4[.]name-services[.]com
dns5[.]name-services[.]com
dummysecondary[.]pleasecontactsupport[.]com
blockedforabuse[.]pleasecontactsupport[.]com
irma[.]ns[.]cloudflare[.]com
ns9[.]orangewebsite[.]com
ns02de[.]santrex[.]net
lee[.]ns[.]cloudflare[.]com
dns2[.]name-services[.]com
dns3[.]name-services[.]com
ns10[.]orangewebsite[.]com
dns1[.]name-services[.]com
ns3[.]ukrnames[.]com
ns1[.]ukrnames[.]com
ns2[.]ukrnames[.]com
ns01de[.]santrex[.]net
ns1[.]domenddnss[.]su
ns2[.]domenddnss[.]su
katja[.]ns[.]cloudflare[.]com
ns1[.]kak-prigotovit-spagetti[.]ru
anton[.]ns[.]cloudflare[.]com
ns2[.]kak-prigotovit-spagetti[.]ru
chad[.]ns[.]cloudflare[.]com
ns2[.]suspend-domain[.]me
bella[.]ns[.]cloudflare[.]com
kara[.]ns[.]cloudflare[.]com
newt[.]ns[.]cloudflare[.]com

ns3[.]us[.]editdns[.]net
ns2[.]eu[.]editdns[.]net
ns2[.]us[.]editdns[.]net
dnsproxy2[.]fm[.]nic[.]ru
ns1[.]suspend-domain[.]me
dnsproxy1[.]fm[.]nic[.]ru
pns21[.]cloudns[.]net
ns1[.]dnsprivatecontrol[.]su
pns22[.]cloudns[.]net
ns2[.]dnsprivatecontrol[.]su
dns1[.]infraud[.]su
ns1[.]parkexpired[.]dns[.]ws
dns2[.]infraud[.]su
ns2[.]parkexpired[.]dns[.]ws
ns1[.]eu[.]editdns[.]net
ns1[.]us[.]editdns[.]net
pns23[.]cloudns[.]net
pns24[.]cloudns[.]net
ns1[.]dnscontrolfff[.]to
ns2[.]dnscontrolfff[.]to
ns1[.]yootube[.]me
ns1[.]mydogphotoss[.]su
ns2[.]yootube[.]me
ns2[.]mydogphotoss[.]su
ns1[.]perlddns[.]ru
ns1[.]dsredirection[.]com
ns2[.]perlddns[.]ru
ns2[.]dsredirection[.]com
ns1[.]ddnsddos[.]su
kia[.]ns[.]cloudflare[.]com
ns2[.]ddnsddos[.]su
coby[.]ns[.]cloudflare[.]com
ns100[.]webnic[.]cc
ns101[.]webnic[.]cc
ns1[.]infobox[.]org
ns2[.]infobox[.]org
ns1[.]parkingcrew[.]net
ns2[.]parkingcrew[.]net
ns1[.]zuno-store[.]ru
ns2[.]zuno-store[.]ru
ns1[.]dynadot[.]com
ns2[.]dynadot[.]com
ns1[.]above[.]com
ns2[.]above[.]com

ns2[.]cdndns[.]ru
ns1[.]domain[.]tld
ns2[.]domainxueinsssss[.]to
ns1[.]cdndns[.]ru
ns2[.]domain[.]tld
ns2[.]mycardriveng[.]ru
ns1[.]controlndssdsss[.]se
ns2[.]florenciyas[.]su
ns1[.]mycardriveng[.]ru
jocelyn[.]ns[.]cloudflare[.]com
ns1[.]domainxueinsssss[.]to
ns2[.]controlndssdsss[.]se
lars[.]ns[.]cloudflare[.]com

Including yet another batch of responding IPs part of InFraud Organization's Internet-connected infrastructure:

47[.]254[.]213[.]246
92[.]53[.]77[.]40
185[.]154[.]53[.]119
199[.]188[.]200[.]47
69[.]64[.]147[.]10
217[.]16[.]27[.]181
193[.]187[.]173[.]23
35[.]204[.]138[.]31
198[.]54[.]117[.]215
82[.]202[.]236[.]154
198[.]54[.]117[.]212
49[.]51[.]132[.]122
198[.]54[.]117[.]216
94[.]130[.]10[.]95
47[.]52[.]142[.]249
82[.]202[.]236[.]65
92[.]38[.]135[.]251
49[.]51[.]192[.]130
199[.]188[.]201[.]203

185[.]162[.]131[.]61
90[.]156[.]128[.]133
91[.]235[.]143[.]155
96[.]43[.]138[.]58
150[.]109[.]48[.]71
188[.]225[.]27[.]46
82[.]202[.]242[.]67
47[.]91[.]94[.]171
199[.]59[.]242[.]153
88[.]218[.]16[.]242
5[.]178[.]87[.]29
198[.]54[.]121[.]92
34[.]102[.]136[.]180
46[.]21[.]248[.]49
188[.]40[.]76[.]96

Including the following personal email address accounts which we were able to identify as part of InFraud Organization's Internet-Connected infrastructure:

zanebilly30@gmail[.]com
amnashahd81@gmail[.]com
zaxarovserg@online[.]ua

Including the following malicious MD5s which are known to have phoned back or interacted with InFraud Organization's online infrastructure in specific an E-Shop for stolen and compromised credit cards information:

c067490db85026aa91d7c93e33063ef97528315ce1b493ab2757dcc288a97a82
bca9650004eedd86eec303cf4a6d1900d45d0eba950c58e0ccc15702e6ea5165

We'll continue monitoring the campaign and InFraud Organization's online infrastructure and post updates as soon as new developments take place.