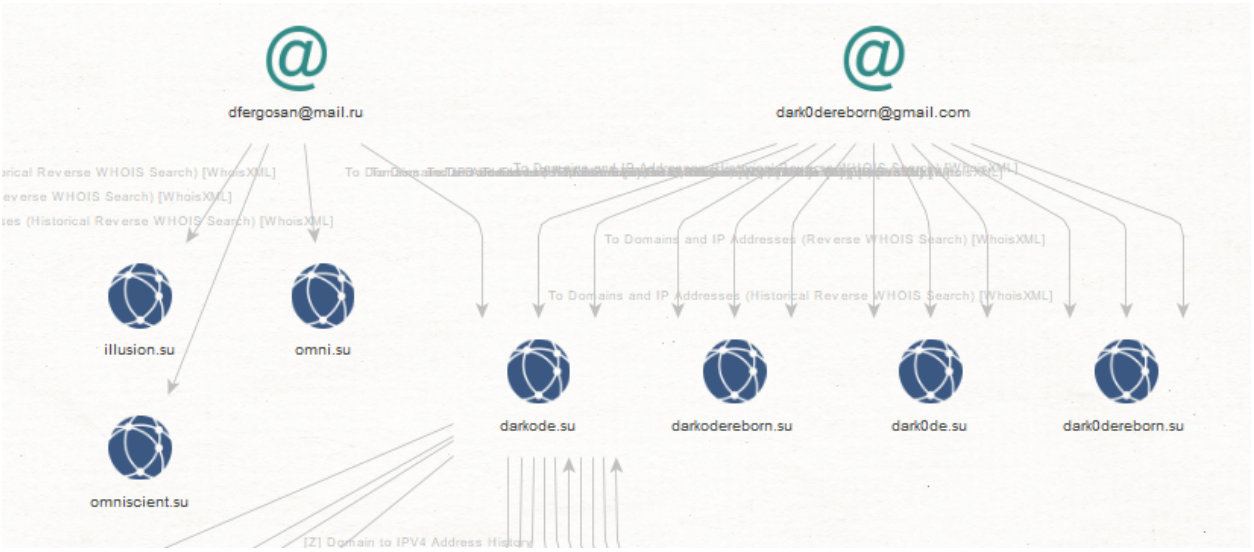
00. Exposing the Darkode Forum Community - An OSINT Analysis

We've decided to provide actionable intelligence on the Internet-connected infrastructure of the infamous Darkode cybercrime-friendly forum community with the idea to assist U.S Law Enforcement and the security industry on its way to properly attribute and track down and monitor various campaigns launched by these cybercriminals.

Sample domains known to have been involved in the campaign include:

darkode.pro
darkode.com
darkode.me
darkode.cc
darkode.su
darkode.com



Sample responding IPs known to have been involved in the campaign include:

174.129.233.242
5.254.116.163
37.48.65.153
162.159.242.50
172.93.103.100
5.254.116.164
172.96.187.181
67.227.227.156
186.2.163.64
146.112.61.107
172.67.164.122
104.21.34.200
37.48.65.149
103.224.212.220
195.242.169.8
184.168.131.241
108.167.172.189
217.70.184.38
199.115.115.116
162.210.196.168
185.107.56.198
185.181.104.82
5.254.116.166
185.11.145.5

207.244.67.174
198.100.144.122
5.135.163.149
178.175.143.28
5.254.116.165
37.187.112.166
162.255.119.249
107.191.60.122
104.31.77.190
185.28.193.195
186.2.163.54
5.39.90.132
94.198.97.198
46.166.147.13
61.120.147.206
158.255.2.40
185.178.208.186
46.28.205.17
217.23.196.90
94.242.198.31
186.2.165.142

Sample personally identifiable email address accounts known to have been involved in the campaign include:

gh0stmarket@mail.ru
dfergosan@mail.ru
ctouma2@gmail.com
dark0dereborn@gmail.com
briankrebson@gmail.com

Related malicious and fraudulent domains known to have been involved in the campaign include:

365online-monitoring.com
365online-debit-card.com
corp-storage.com
365online-cardcare.com
bancobpm-autenticazione.com
365online-reviewnow.com
365online-review-transaction.com
worldmobiletesters.com

youweb-bancobpm.com
365online-updatemobile.com
365online-suspended.com
sprlngcreekcc.com
365online-debitcard-review.com
365online-updating.com
365-online-charges.com
securitytestpin.com
365online-charges.com
open24-update.com
365online-deactivated.com
365online-fraudreview.com
irxsx.com
irssx.com
atunesdor.net
transactions-365online.com
365online-reviewcharge.com
365online-card-review.com
aauaaaeieiieepn.su
aaaeieiiiofffpn.su
xiheiufisd.su
365-online-review.com
baszarkacorp.com
givan.su
podisong.su
aeiziaezieidiebg.su
wwwcoinbase.su
eoufaoeuhoauengi.su
rempoint.su
loads.su
accountsgoogle.su
euauueuueuruudg.su
purpurant.com
fineconera.com
aerulonoured.su
verifyidentity-coinbase.com
bestccbalance.su
amazonverifprocess.com
office365-en-update.com
amazon-customerverified.com
apobrodas.com
zzruuoooshfrohu.su

365online-fraudcheck.com
przelewyallegro.com
veilige-toegang.com
zimmerton.su
koentacist.com
mertonera.su
wp-gdpr-complience.com
plpanaifheaighai.su
au-q2.com
tespaqltd.net
amazon-deutschland-safer-certification-security-info.com
prepaidproccessingverifiededd.su
au-q1.com
softsportal.su
seweablosi.com
loginblockchain.su
gigistoloi.com
banusdore.su
remltano.com
afeifieuuufufufuf.su
loginlive.su
zimbabwe.su
r2cia9ovmrqnwe5b.com
fafhoafouehfufh.su
blacknode.su
ouhfuosuoosrhfzr.su
rupertok.su
exploit.su
kentona.su
bfbaiefiheil.su
unicredit.su
cugwinery.su
scotiatrinidad.com
darkjabber.su
evux.su
flumenco.com
tortalk.su
net-validator.com
papersstory.com
officesupportdoc.com
thipissney.com
technicalpreviews.com

agliesc.com
rutratrang.com
commerzebank.net
psardernes.com
trailandra.com
amazon-deutschland-safer-certification-info.com
aspendok.com
uvuladitur.com
amazon-security-deutschland-safer-certification-info.com
update-pkey.in
nexyownmexxfinla.su
01vikings.su
hsbc-auth38.su
jokester.su
noomredmsadik.su
expert-bankers.com
newaeon.su
prx.su
koluminatorspice.su
jjolasretokermas.su
velocon.su
wizoidiazi.com
vodafone.su
yvex.su
doxagram.su
ads-banner.com
expediapartnership.com
begeptis.com
meersteng.com
google-free-dns.com
megasfu.com
arlagent.com
jokuusers.com
belennanet.com
ajax-loads.com
hsbc-auth4.su
hsbc-auth-3.su
p0s3id0n.su
cbl-delivery.com
darkode.pro
bgu-logistics.com
netserv-dns2.com

darkode.com
iwcplus.com
asia-cni.com
darkode.me
auromantofont.com
transportit.net
darkode.cc
maxigolon.com
sld-consult.com
darkode.su
marinzer-3.com
moloborov.com
asia-cni.net
microsads.net
ladadensuarupddipl12343423233.info
blendrun.com
svl-trusted.com
lipjion.com
serkilopa.com
molokinga.com
sofitasaonline.com
muodlox.com
sarminual.com
verikanam.com
nertioklin.com
secures-list.net
molding-autos.com
lba-delivery.com
jwitdukznswzbksz.net
darkode.com
man-pan.com
secure-billing-page.com
all-ebook.com
belendomas.com
sembadarison.com
bestcapshop.com
dark0de.su
dark0dereborn.su
darkodereborn.su
omni.su
illusion.su
omniscient.su

ulefieskil.com
securedpccheck.com
navectrece.com
imgurl.su
rackz.su
delkijembu2.su
menorukis.su
rbcrewards.su

Sample personally identifiable email address accounts known to have been used in the campaign include:

pxu@foxmail.com
aviatut@hotmail.com
ilona4gold@gmail.com
maximaximov@ukr.net
kirovsk1@yandex.ru
sofetin975@royandk.com
ctouma2@gmail.com
atybrc@cock.li
pachendale@gmail.com
tostar1993-unicredit@yandex.ru
kirdeeva.1986@mail.ru
rromatt@yandex.ru
igorenko@safe-mail.net
geraregaettemu@mail.ru
securepage@live.com
dfergosan@mail.ru
anothonny@yahoo.com
bignames@mail.ru
info@r01.ru
boschat@mail.ru
info@masterlead.ru
dark0dereborn@gmail.com
oove1949@cuvox.de
irssx.com@rongfeistudio.com
gh0stmarket@mail.ru
irssx.com@cxwz.com
semik@protonmail.com
abuse@gmo.jp
emmail@bk.ru
amolewaris@gmail.com

stevesmanpan@gmail.com
contact@whoissecure.net
snackletac@yahoo.com
briankrebson@gmail.com
jj456567456@protonmail.ch

Sample related domains known to have been involved in the campaign include:

xn--80ahntvec.xn--80adxhks
xn--80aalqabyj2ajl4c8g.xn--80adxhks
xn--24-6kcajk8b3a1ak.xn--80adxhks
xn--c1aidajugk1a5b.xn--80adxhks
xn--c1adanheqhrdr2kg7a.xn--80adxhks
irssx.com
xn--80aff8bd2h.xn--80adxhks
xn--80ajijdgo6an6f.xn--80adxhks
xn--b1ae4ad.xn--80adxhks
xn--80aeam7bsfe.xn--80adxhks
xn--24-6kch4ezb.xn--80adxhks
xn--d1aaly0e.xn--80adxhks
xn--80aaxgrq.xn--80adxhks
xn--80aa8agek3a.xn--80adxhks
xn--80aanlmfdj2a.xn--80adxhks
xn--80aakrzq.xn--80adxhks
xn--80ag4adi.xn--80adxhks
xn--80aqfcgmg9d.xn--80adxhks
voprosy-putinu.com
xn--24-6kcm3bencbyld.xn--80adxhks
xn--d1ab0aafeo.xn--80adxhks
xn--24-6kcay4a7ay.xn--80adxhks
xn--d1aifpfmn.xn--80adxhks
xn--e1aajycefnb6g.xn--80adxhks
xn--h1addksgd.xn--80adxhks
xn--80afhj6bcm6e.xn--80adxhks
taxi.support
rggaming.com
pokersss.com
777o777.com
vdpo.moscow
xn--80akrd6ad3d.xn--80adxhks
xn--80afqi2a.xn--80adxhks
xn--j1amb.xn--80adxhks

xn--80aovq.xn--80adxhks
mpgboost.info
led.holdings
cat.kitchen
xxx0xxx.com
diamondsfund.com
murmansk.club
russia.boutique
bank.dating
spb.agency
spb.lighting
taxi.photography
xn--80aaf6aofaxhc8l.xn--80adxhks
xn--80ajofxh.xn--80adxhks
xn--80aaff3bepbltf.xn--80adxhks
taxi.solar
xn--24-dlcm9dva2b.xn--80adxhks
nanowebcams.com
softwarerussia.com
denmark2014eurovision.com
denmarkeurovision2014.com
picturenano.com
nanocreditcards.com
xxxhxxx.com
eurovision2014denmark.com
com-nic.com
xxx--xxx.com
putin-prezident.com
nevadasale.net
nevadasale.org
chrisbjorin.com
pokerstarshelp.com
mpgboost.net
777xxx777.com
denmarkeurovision.com
yysexyy.com
xxx7777xxx.com
goldinmoscow.com
wsopnevada.com
hulinada.com
xxxmenxxx.com
222x222.com

nanowebcom.com
www777www.com
mucaltin.com
imchristos.com
ichristos.com
benimanketi.com
eurovision-denmark2014.com
nanopharm.org
nevadapokerstars.com
fulltiltpokerlasvegas.com
nevadafulltiltpoker.com
fulltiltgaming.us
kreditkartenschuld.com
51region.com
nevadagame.org
nevadahome.net
nevadagame.net
eurovision-denmark.com
sauce1234.com
lcdnano.com
xxmenxx.com
777sex777.com
365online-reviewnow.com
365online-suspended.com
sprlngcreekcc.com
youweb-bancobpm.com
365online-updatemobile.com
365-online-charges.com
securitytestpin.com
365online-debitcard-review.com
365online-updating.com
delkijembu2.su
rackz.su
menorukis.su
rbcrewards.su
aauaaaeieiieepn.su
aaaeieiiiofffpn.su
365online-reviewcharge.com
365online-card-review.com
baszarkacorp.com
givan.su
xiheiufisd.su

365-online-review.com
corp-storage.com
365online-cardcare.com
365online-monitoring.com
365online-debit-card.com
365online-review-transaction.com
worldmobiletesters.com
bancobpm-autenticazione.com
connexion-populaire.com
bankid-aterstalla.com
stadion.su
0c76lz.com
bankid-uppdatering.com
ssofhoseuegsgrfnj.su
itiahshahsur.com
uaubfwua.com
risk.su
yaacb6.com
bnz-helpinet.com
aktivering-bankid.com
impencosh.com
cajeniste.com
bbva-particulares-seguridad.com
info-panteracapital.com
rogaey.com
ltoubg.com
mobilepayment-rbc.com
acces-client-fr.com
netfiix-ciient.com
ripple-event2022.com
netflixsupportauth.com
espace-adherant.com
zahlung-h309r110289.su
zahlung-h309r110213.su
simx6z.com
www-kucoln.com
natwest-bankllne.com
commbank-app.com
e5ewrv.com
chargement-page.com
ashihsijaediaehf.su
bankid-aktivering.com

cf52bp2.com
sense.su
mo10bs2.com
alertas-moviles-bbva.com
cf72gs2.com
uk-paymentid1975.com
espace-epargne.com
rdrctorlbrml.com
rbcmobileaccess.com
rai.su
2buterin.com
sparkasse-aktualisierung.com
aktualisierung-sparkasse.com
47khy9.com
fhbd5s.com
connexion-epargne.com
fein-n101r120192.su
hdhjdoeiroi.com
my-commonwealthbank.com
securite-sociaie.com
beliale232634.at
belialw869367.at
ameii-documentationfr.com
md44pu2.com
cisco.su
connexion-caisse-epargne.com
ruralvia-movil.net
megaupdatesystemservice.at
uk-nhs-covid.com
hisuqzzg.com
myupdatesystemservice.at
spkkundendevise.com
sila.su
rbcsbanking-mobile.com
alerta-clientes-bbva.com
qd52bs5.com
monespacevitale-documentation.com
2micro.net
abanca-seguridad.online
yedigopbupruxgy.com
secure-caisse-epargne.com
x2terra.net

awto.net
2saylor.com
tracheachronica.net
micro-bnb.com
bnb-strategy.com
correos-aviso.com
secure-banque-popuiaire.com
fgwiuyos.at
abaeubuegs.su
2stepn.com
impotsgouv-fr.com
uk-paymentholds.com
uk-payments-gsa-idv3.com
uk-payments-gsa-idv2.com
uk-payments-services.com
aib-helpinets.com
uk-paymentid933.com
zilx2.com
verifizierung-sparkasse.com
dpdtrackmyparcel.com
rdrctstscl.com
ltsme-identify.com
aruba-riattivare-mail.com
australia-citi.com
cancel697616-binance.com
postbank-verwaltung.com
pushtan-verwaltung.com
id48662.com
id17d710.com
vtakte.com
booking-request9420183.com
dpdmanageparcel.com
hloya.com
id-481725.com
ameii-assurance.com
vkusnov.com
tracking-redelivery.com
id17d711.com
bed.su
slngpass.com
crypto-up22.com
business-bni.com

together-for-ukraine.com
postoffice-deliverymanager.com
baraholka.su
ltsme-reactivate.com
mnyam.com
csob-sprava.com
izysk.com
id-498179.com
8marta.net
fbwqhqwfqxc.com
id48665.com
train.su
officebankings.com
bnz-login-secure2.com
citi-australia.com
https-shoplfy.com
id18664.com
rdrctlbrom.com
id18665.com
id18667.com
id18660.com
id18668.com
x2-musk.com
kinotracker.com
postoffice-manageparcel.com
sdayu.com
marktplaats-nl-verificatie.com
shadesofmagic.com
officebanking-getnet.com
ex-press.net
caixa-movil-seguridad.com
cargodistri.com
dx61hc.com
au-cb.com
citionline01.com
cloudmanagmentservice.com
csob-smartkey.com
cp6sam.com
compliance-commbank.com
hzxy462.com
luxury.su
h5n91c.com

fz83uw.com
kz3bxc.com
bestcar.su
lux-nordic.com
hv1cxl.com
ig1zxt.com
chargeback-commbank.com
security-commverify.com
7xwl1e.com
app-anz.com
25m9fv.com
gamma.su
8469xe.com
asfwqeffwegwe.com
2tv1as.com
0cq4me.com
8q7keg.com
vivat.su
13n8bu.com
1v3aco.com
banza20.com
065vai.com
bk-personal-secure.com
b3f650.com
ra-secure.com
axieinfinitydownload.net
mdnb-norge.com
fr-santeacpam.com
id-check-no.com
nmkb-si.com
portal-ch.com
beachtung-creditsuisse.com
fr-informationmoncompte.com
dzen.su
spk-service-division.com
fraudcheck-raiffeisen.com
fr-assurancevitale.com
fraudteam-commbank.com
commau-portal.com
antifraud-commbank.com
kontopostbank.net
fraud-creditsuisse.com

uberprufen-bawag.com
cler-login-ch.com
fraud-commbank.com
fraudcheck-commbank.com
tarkistus-opmobiili.com
beachtung-bawag.com
idcheck-bawag.com
chargeback-bawag.com
fraud-bawag.com
anydest.net
verification-commbank.com
incidents-trustwallet.com
stoly.net
portal-au.com
kolyaski.net
att-biii.com
fraudreversal-commbank.com
credit-du-nord-vpass.com
bettingexclusive.com
de-banking-id-517cb17gag19gauzffa7d1gf.com
sparkasse-onlineverifizieren.com
onlineverifizieren-sparkasse.com
ogntrcmrctsmarr.com
att-bill.com
databreach-trustwallet.com
zzruuoooshfrohu.su
att-biiiing.com
recovery-trustwallet.com
seguridad-movil-santander.com
movil-bbva-particulares.com
securekey-authentification-forte.net
frode-intesasanpaolo.com
netfiix-app.com
assurance-servicemacarte.com
assurance-macartevital.com
referenz-h309r110287.su
order-uktest-kit.com
lrs-rebate.com
vr-zentralisierte-umstellung.com
stroymarket.su
agnediuaeuidhegsf.su
secure010bchase.com

dpd-redeliveryservicegb.com
libero-mail-riattivare.com
fm5817.com
rlbrmit.com
lzim3q.com
cheat.su
personal-id-secure.com
cuororeresteadntno.com
spk-zertifizierte-umstellung.com
wageorebe.com
vinchoics.com
spkservicereiter.com
tehsimarsa.com
spkserviceleistung.com
spkserviceverteiler.com
spkserviceneuerung.com
spkkundenzugang.com
netfiix-clientsecure.com
sparkasse-servicesystem.com
postbankde.net
netfiix-clientmyaccount.com
yourbrowserinformation.com
gte-financial.com
uk-ordertest-kit.com
shield-renewal.com
notice-panteracapital.com
bankid-fornyelse.com
movil-bancosantander.com
irwiaibauis.net
uuwuaauiie.net
movil-caixabank.com
sparkasse-servicetechnik.com
particulares-bancosantander.com
spk-servicedivision.com
spk-serviceverteiler.com
spkservicewartung.com
spkservicedivision.com
sparkasse-serviceverteiler.com
spk-servicehandlangung.com
verwalten-online.com
sparkasse-serviceumstellung.com
beineth.com

songs.su
beinada22.com
komod.su
aviso-santander.com
krepost.su
beincardano.com
soul.su
com-id-471gd13425r14at71fd7821g.com
frameli-info.com
prostore.su
amelifr-formulaire.com
official.su
alpha-sniper.com
clientsboursorama-id.com
clients-boursorama-login.com
clients-sfr.com
clients-boursorama-id.com
2xzil.com
devapp-newdev.com
id-481723.com
aktualisieren-sparkasse.com
fornyelse-bankid.com
houses.su
macarte-ameii.com
luna.su
amazon-fr-clients.com
coffee.su
x2elontesla.su
chronoposi.com
charm.su
idboursorama-clients.com
magnum.su
frcarte-ameii.com
major.su
chronoposl.com
mmo.su
ameii-smsfr.com
resource.su
ameii-gouv.com
com-id-471gd17a34dfadf64371fd7821g.com
flyboard.su
yfiowqhftsnqc.com

vek.su
com-id-471gd17ag1zadsdf54s1fd7821g.com
kazna.su
com-id-471gd17agfe3at71fd7821g.com
stroi.su
beinethereum.com
uniform.su
icasinowins.com
halloween.su
vhhvhsqwf.com
321.su
fr-ameli-support.com
ink.su
utabwbazuu.com
zhilstroy.su
uk-payments-service.com
deal.su
wyqwqwqchdsk.com
tor.su
twydbsjwqw.com
kleopatra.su
beinripple.com
steel.su
wyiqwodqw.com
perfectworld.su
combankverify-au.com
snasti.su
beinxrp22.com
hybrid.su
aktualisieren-online.com
selhoz.su
combankupdate-au.com
kolorit.su
2x-zil.com
clonex-nft.com
dubstep.su
2x-musk.com

Related malicious MD5s known to have been involved in the campaign include:

b760592aab4ab06641aa06b0de67b4e5

3282f6c806a89359ec94f287cf6c699c
801a2821323917868c5dffc7ca558c73
ac6034506b16e938e490cdf9c1e0add2
6e7b867646c6188a3d2bb60464ac8d60
bdc5f7a20d1a2c0fe40db1cce1b17697
cbf3942cc02766e65d72d69a3b5bd5d7
b5ad0f65110f7deb0a40278dc58b79ab
ef816da4763b0cbd0de07c1151ab408d
5b292031d963f41fa4a593bb1aa67b16
1457ccfd0d89c2eb047eb8bd5d619848
4c70c5d03509975dcd547b747e4c0c4f
094312be0a71a292a4670bcda23b2500
9ad2cb1c4b67864ba0f810f1e474887c
5a62970c821a2d2b542ed94df4da85af
ad0ad3ef9bfddcf0acac4774290f4403
eba63845dc5e111a36bf5007f312adc5
96d6c3254399bddc59f6fd815a7d3bc6
4493809649318bd66e73c69dded845c8
6f5f6fc341a50546a3f2aca98f556d3c
0dcc897f8170247d9c0cb6e6b9831ae5
1c1365bf596b70af7d84914aa951a39c
59de54129d0ea26aae2c87ad3df48300
c1f9d19b0bbf0a6bdefbf72bb1df7595
ca68eadc18565d245627f0c9c216ebbe