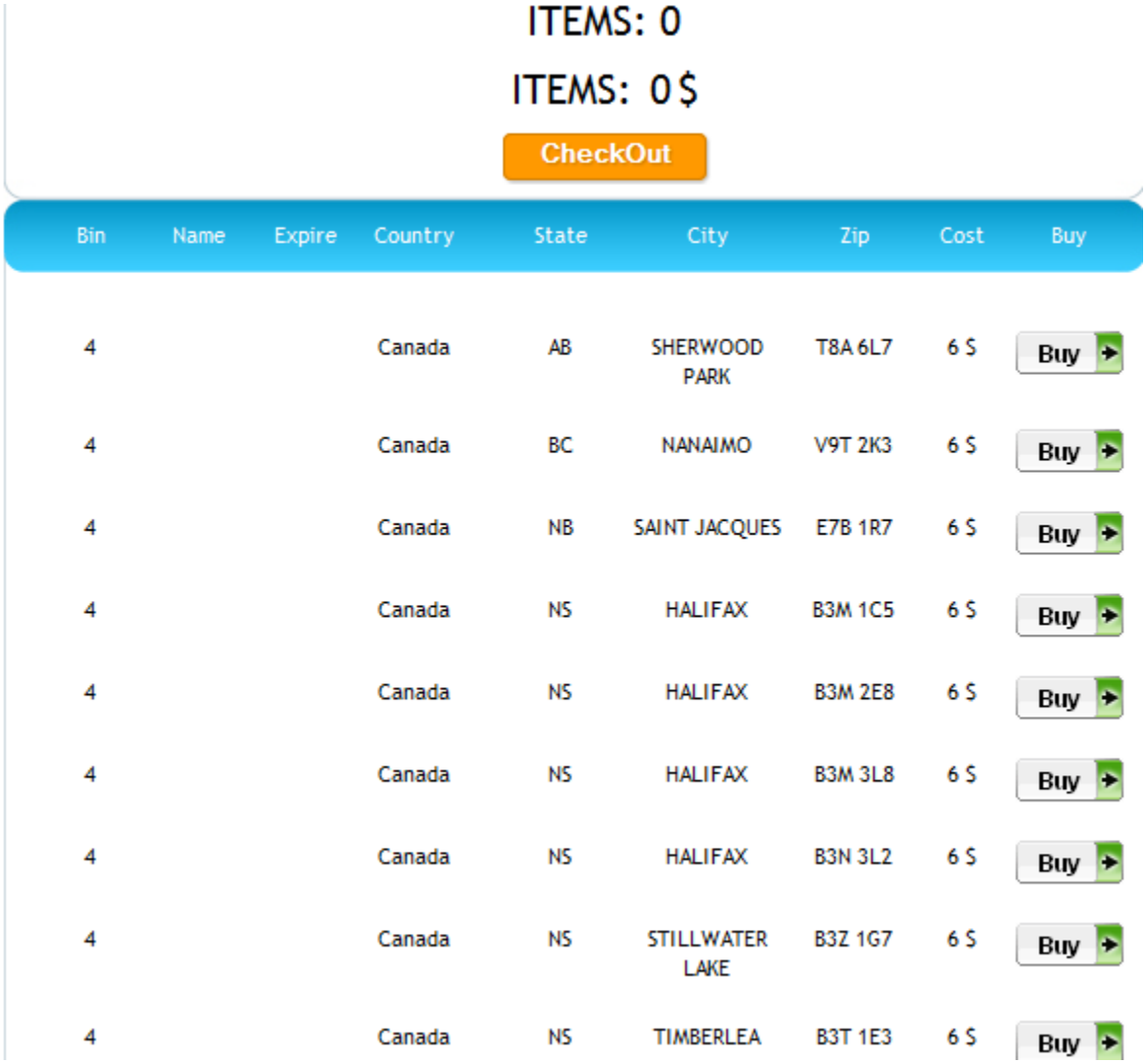
Exposing A Domain Portfolio of E-Shops for Stolen Credit Cards - An OSINT Analysis



ITEMS: 0

ITEMS: 0 $

CheckOut

Bin	Name	Expire	Country	State	City	Zip	Cost	Buy
4			Canada	AB	SHERWOOD PARK	T8A 6L7	6 $	Buy
4			Canada	BC	NANAIMO	V9T 2K3	6 $	Buy
4			Canada	NB	SAINT JACQUES	E7B 1R7	6 $	Buy
4			Canada	NS	HALIFAX	B3M 1C5	6 $	Buy
4			Canada	NS	HALIFAX	B3M 2E8	6 $	Buy
4			Canada	NS	HALIFAX	B3M 3L8	6 $	Buy
4			Canada	NS	HALIFAX	B3N 3L2	6 $	Buy
4			Canada	NS	STILLWATER LAKE	B3Z 1G7	6 $	Buy
4			Canada	NS	TIMBERLEA	B3T 1E3	6 $	Buy

We've decided to dig a little bit further and offer actionable intelligence on a currently active domain portfolio of known E-Shops for stolen credit cards with the idea to assist U.S Law Enforcement and the security community on its way to properly track down and monitor the cybercriminals behind these campaigns.

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

novlops.com
pawnsh0p.com
privateshop1.com

privateshop2.com
selldumpsshop.com
shopccdumps.com
trackgenerator.com
validforver.com
anyccard.com
zunostores.com
allmybins.com
bases-valid.com
ccgetmoney.com
cvvshop.in
cvvshop39.com
evilshop.org
freshcvv.com
good-cvv.com
jshop-pro.com

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

danny9@gmail.com
root@evilzone.org
janenetyi@gmail.com
Frances9Wolfe@gmail.com
selldumps_shop@yahoo.com
tisinekinsisi889@rambler.ru
philmahre1989@gmail.com
cai0006@aliyun.com
whois-agent@gmx.com
greg2022@mail.ru

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

47.74.186.197
47.88.156.38
46.21.249.114
92.53.77.90
47.74.137.231
119.28.41.158
149.129.219.23
80.87.97.201
95.213.252.108

185.158.152.31
47.74.236.158
49.51.192.130
47.52.233.0
185.162.131.61
45.63.40.156
149.129.216.197
35.198.119.28
5.188.90.216
49.51.35.225
149.129.225.92
95.213.252.3
37.60.177.31
92.53.77.40
194.87.103.196
161.117.7.46
47.254.213.246
46.21.248.49
194.116.216.254
49.51.85.205
78.155.207.76
172.104.104.241
47.91.72.137
95.213.203.64
185.223.163.129
185.224.212.24
149.129.223.249
92.223.105.218
193.187.128.60
108.177.235.227
172.67.144.190
178.154.240.197
47.74.176.216
27.102.118.142
78.155.206.161
95.163.250.153
47.74.235.179
119.28.137.123

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

evilzone.org

wmz.center
metodika-binary.com
documents233.com
albdfhln.com
media-gossip.com
maxubernis.com
adode-update.com
google-src.com
verification-group.com
morgunovo.com
ibisworlds.com
online-verificationteam.com
nikulino.com
rosenblumpricellc.com
jmai1.com
luierdes.com
kofeks.com
batokoubangi.net
suckmydickavvendors.com
ipc-billling.com
binar-zarabotok.net
rabota-binarka.net
binar-work.net
otvetim-mail.net
irc-billing.com
binar-blog.net
safe-canadiandrugstore.com
irs-billling.com
falandire.com
ilofre.com
privatonk.org
privateuren.org
softoronga.org
privateshop.mobi
slilpp.biz
nanojabber.net
slilpp.info
faneria.com
dis-boards.com
wwwgringos.com
diver-club.net
mcncbx8.net

herdisano.com
binary-robotrade.com
fucktheusa.net
nipolika.com
frauer-com.net
rukkalix.com
bellisimardi.net
buertalix.com
clickcenter98.com
moltenproject.com
erectiledysfunctiontabs.com
dulayvenet.com
paradiseadsfilt.com
tvincoming.com
wellsfargo-private.com
sky-n571.com
binaryopt-method.com
american-purgen.com
anerikan-regress.com
system128.com
paypalkonflikt.com
turbocc.asia
forumtalknightlife.com
pivorand.com
derbet.com
sad89a19lsq615.com
kiodlers.com
friscoserve43.com
rocket-investment.com
mabuleran.com
vundaba.com
mkdepot.com
gardbad.com
lloyds-download.com
phqocytwqchyphuivjvhdcscx.com
disk57.com
so01j18h1f7718.com
mamlodar.com
bukreggan.com
adcountservices.com
diska33.com
efax-downloads.com

durmen.com
pilokwer.com
coperdix.com
lamerisan-express.com
gamericanexress.com
data-mon.com
osmoprac.com
dialaclick.com
damneg.com
baerdalent.com
safe-med-stock.com
maxermat.com
demo-data.com
data999.net
multidnsservicesla.net
pko-check.com
maxubarda.com
luresi.com
mail-antispam.com
todarrix.com
dohod-binary.com
portulax.com
zapoio.com
elrkzdnzofsgyltwsljzlzl.com
tanowki.com
american-express.com
ercvax3.com
sfecpm.com
efax-download.com
miglok.com
safe-canadian-meds.com
canadadrugstore365.com
rxmeds-24h.com
davithuz.com
spn-pharmacy.com
worklinellc.com
baglinu.com
jrrsqrolftkizfqhovarsinlj.com
allpacifictours.com
1elmv5v54lglv18ek1x3dh5069.org
fuckedsluts.net
moviedyear.net

mobile-binary-options.com
direct99.net
gioogle.net
dpepjscjztcicmztmrdizptnz.com
safe-torontopills.com
safetorontopills.com
play-bezpieczny.com
drugstoresale24h.com
worldpharmazone24h.com
medicinesnorx.com
overnightshippingviagra.com
federko.com
orange-bezpieczny.com
rxnopharmstore.com
dergoni.com
safetorontoshop.com
pharmshop-365.com
rx-canadian-24h.com
canadianshop24h.com
noisymemo.org
berdesik.com
banguli.com
english25.biz
extra-tabs.net
norx-drugstore.com
yourmedicinesrx.com
drugstorerx24h.com
canadian-shops.com
safe-torontomeds.com
canadian-pharmacy-24hs.com
canadadrugs24h.com
all-top-meds24h.com
zertifikatkey.com
pharmacyathome365.com
germinf.com
segropa.com
claudri.com
efronad.com
pelegra.com
nuarven.com
fergula.com
serdafi.com

garbux.com
deveryok.com
fongyra.com
dedorka.com
acounts-googie.com
bulderf.com
svatik.com
bunerdes.com
ferdukan.com
dekipola.com
vilakiro.com
paterke.com
bardubar.com
derferonalis.com
fersedoba.com
soplino.com
nudrang.com
huburda.com
mapulabor.com
loprana.com
privateshop.asia
dersaeda.net
deburma.com
serferant.com
casdore.com
medsferz.com
harper-paypal.net
pinello.net
dunella.net
slowpocka.net
american-expezs.com
pirnorokiv.com
amerigan-extress.com
indalusia.com
buldunsa.com
fesdukla.net
kloppil.com
hadburg.com
furenga.com
pappiofi.com
poxmelo.com
derbantud.com

american-exprezs.com
amerizan-congress.com
carolemess.com
anerican-fortress.com
ameriqan-exprezs.com
anerican-confess.com
brainsmdl.com
amerikan-exress.com
gershvond.com
trustedtorontodrugstore.com
amerikan-sunfacess.com
american-ertress.com
american-progrecs.com
puntlax.com
american-exprezz.com
ownersdirectt.com
bapkinoma.com
ipubling.com
rxcahxobqdru.com
approvedmeds.net
pliosh.com
deboresalto.com
kolonezzia.com
kipixanta.com
amelican-excress.com
amerikano-espresco.com
manuleazzo.com
americanoexresso.com
pudinguf.com
berdelida.com
tc020.cn
pefepe02.cn
wintertrainingcamp.com
zheyoung.com.cn
digitalpitcher.net
uvtu.cn
theinnervibe.com
weepa.net
imadison.cn
asthma-allergy-news.com
027sohu.cn
themedicalguide.net

austintel.com
gxcsg.cn
ldsyw.com.cn
artisan-du-verre.com
woror.cn
brashenomics.com
justonlyjudy.com
djhzc.com
ame-services.com
js-scw.cn
bd114.com.cn
sdittc.cn
nearun.cn
shbxil.cn
thklaser.cn
ylbxul.cn
etbxul.cn
Baltimorezeitgeist.com

We'll continue monitoring the campaign and will post updates as soon as new developments take place.