Oct 05 2023

NETMANAGEIT

Intelligence Report

Return to Sender - A Brief Analysis of a US Postal Service Smishing Campaign - DomainTools

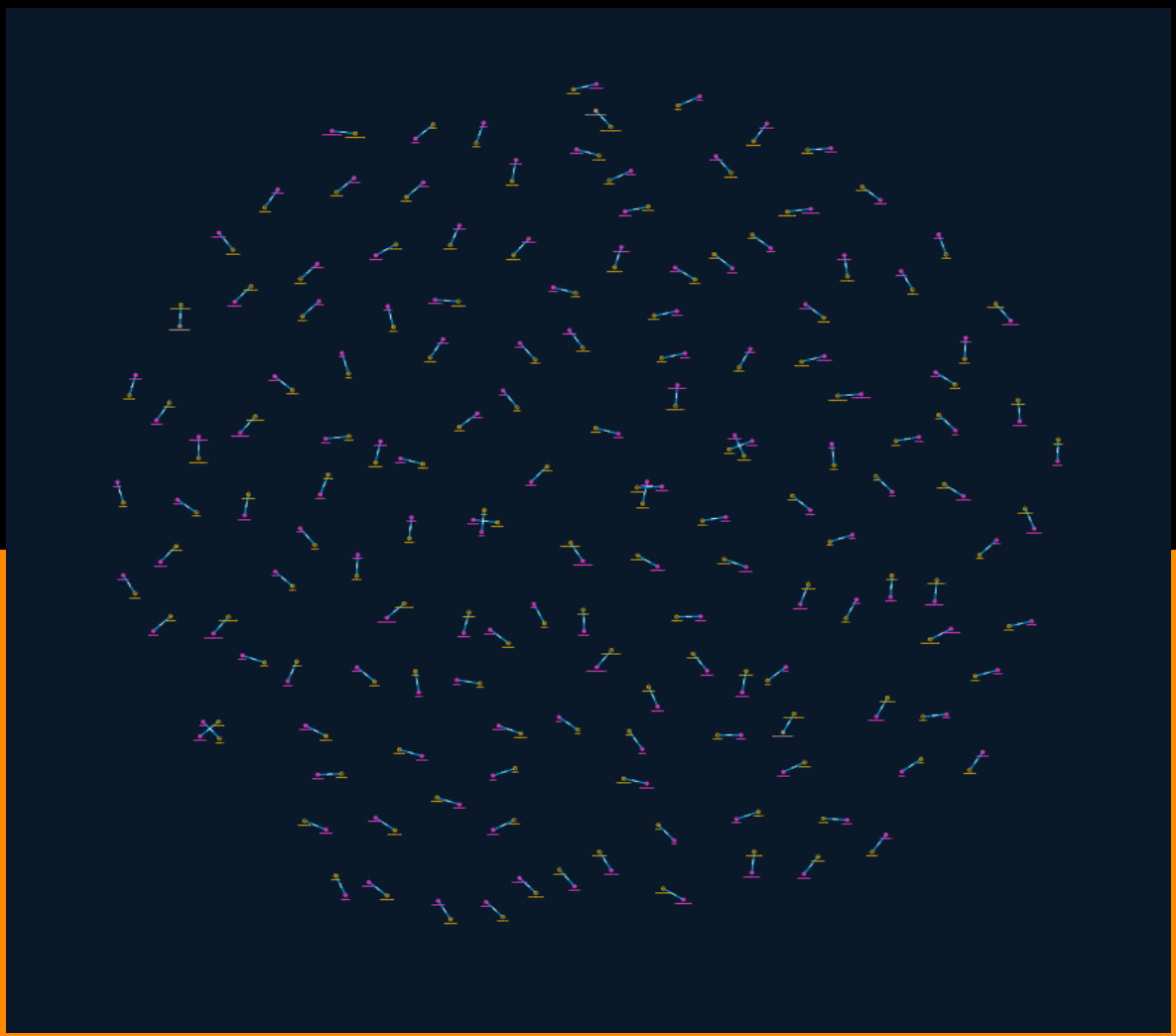

Table of contents

Overview

Entities

Observables

External References

Overview

Description

DomainTools Research has noted a noticeable uptick in phishing and smishing campaigns targeting the USPS.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Content

N/A

Indicator

Name
ropekaa.ir
Pattern Type
stix
Pattern
[domain-name:value = 'ropekaa.ir']
Name
40o.ir
Pattern Type
stix
Pattern
[domain-name:value = '40o.ir']
Name
gardeshgareirani.com

Pattern Type
stix
Pattern
[domain-name:value = 'gardeshgareirani.com']
Name
behsoo-app.ir
Pattern Type
stix
Pattern
[domain-name:value = 'behsoo-app.ir']
Name
7thart-m.com
Pattern Type
stix
Pattern
[domain-name:value = '7thart-m.com']
Name
jettaxi.click

Pattern Type
stix
Pattern
[domain-name:value = 'jettaxi.click']
Name
besigni.ir
Pattern Type
stix
Pattern
[domain-name:value = 'besigni.ir']
Name
timekook.ir
Pattern Type
stix
Pattern
[domain-name:value = 'timekook.ir']
Name
alamutstore.ir

Pattern Type
stix
Pattern
[domain-name:value = 'alamutstore.ir']
Name
saliamal.ir
Pattern Type
stix
Pattern
[domain-name:value = 'saliamal.ir']
Name
animationpress.ir
Pattern Type
stix
Pattern
[domain-name:value = 'animationpress.ir']
Name
mooyekamand.com

Pattern Type
stix
Pattern
[domain-name:value = 'mooyekamand.com']
Name
andishkademedia.com
Pattern Type
stix
Pattern
[domain-name:value = 'andishkademedia.com']
Name
mehriadarman.ir
Pattern Type
stix
Pattern
[domain-name:value = 'mehriadarman.ir']
Name
oygar.ir

Pattern Type
stix
Pattern
[domain-name:value = 'oygar.ir']
Name
avinpayamak.ir
Pattern Type
stix
Pattern
[domain-name:value = 'avinpayamak.ir']
Name
pakhshmehrbook.ir
Pattern Type
stix
Pattern
[domain-name:value = 'pakhshmehrbook.ir']
Name
meymehmarket.ir

Pattern Type
stix
Pattern
[domain-name:value = 'meymehmarket.ir']
Name
mehdi.k1989@yahoo.com
Pattern Type
stix
Pattern
[email-addr:value = 'mehdi.k1989@yahoo.com']
Name
tashstone.org
Pattern Type
stix
Pattern
[domain-name:value = 'tashstone.org']
Name
pishroyadaknovin.com

Pattern Type
stix
Pattern
[domain-name:value = 'pishroyadaknovin.com']
Name
zooby.ir
Pattern Type
stix
Pattern
[domain-name:value = 'zooby.ir']
Name
tarna.ir
Pattern Type
stix
Pattern
[domain-name:value = 'tarna.ir']
Name
amoomehdi.com

Pattern Type
stix
Pattern
[domain-name:value = 'amoomehdi.com']
Name
ebiroll.ir
Pattern Type
stix
Pattern
[domain-name:value = 'ebiroll.ir']
Name
mehdi.kh021@yahoo.com
Pattern Type
stix
Pattern
[email-addr:value = 'mehdi.kh021@yahoo.com']
Name
sepiderooz.com

Pattern Type
stix
Pattern
[domain-name:value = 'sepiderooz.com']
Name
parsiranwasher.com
Pattern Type
stix
Pattern
[domain-name:value = 'parsiranwasher.com']
Name
emdadtrip.com
Pattern Type
stix
Pattern
[domain-name:value = 'emdadtrip.com']
Name
tekinja.com

Pattern Type
stix
Pattern
[domain-name:value = 'tekinja.com']
Name
rihajeans.ir
Pattern Type
stix
Pattern
[domain-name:value = 'rihajeans.ir']
Name
instagramme.ir
Pattern Type
stix
Pattern
[domain-name:value = 'instagramme.ir']
Name
devloper.ir

Pattern Type
stix
Pattern
[domain-name:value = 'devloper.ir']
Name
instasos.ir
Pattern Type
stix
Pattern
[domain-name:value = 'instasos.ir']
Name
wordfa24.ir
Pattern Type
stix
Pattern
[domain-name:value = 'wordfa24.ir']
Name
clickbekhar.ir

Pattern Type
stix
Pattern
[domain-name:value = 'clickbekhar.ir']
Name
gdoe.ir
Pattern Type
stix
Pattern
[domain-name:value = 'gdoe.ir']
Name
avaper.ir
Pattern Type
stix
Pattern
[domain-name:value = 'avaper.ir']
Name
ghabfather.ir

Pattern Type
stix
Pattern
[domain-name:value = 'ghabfather.ir']
Name
ganjineman.com
Pattern Type
stix
Pattern
[domain-name:value = 'ganjineman.com']
Name
ghasrelebas.ir
Pattern Type
stix
Pattern
[domain-name:value = 'ghasrelebas.ir']
Name
adakcharmrasa.ir

Pattern Type
stix
Pattern
[domain-name:value = 'adakcharmrasa.ir']
Name
appomobil.ir
Pattern Type
stix
Pattern
[domain-name:value = 'appomobil.ir']
Name
siboshop.ir
Pattern Type
stix
Pattern
[domain-name:value = 'siboshop.ir']
Name
hesarakidokhtarane.ir

Pattern Type
stix
Pattern
[domain-name:value = 'hesarakidokhtarane.ir']
Name
velaati.com
Pattern Type
stix
Pattern
[domain-name:value = 'velaati.com']
Name
film-pardaz.com
Pattern Type
stix
Pattern
[domain-name:value = 'film-pardaz.com']
Name
parna-sakhteman.ir

Pattern Type
stix
Pattern
[domain-name:value = 'parna-sakhteman.ir']
Name
alocms.com
Pattern Type
stix
Pattern
[domain-name:value = 'alocms.com']
Name
sahamdaraneedalat.ir
Pattern Type
stix
Pattern
[domain-name:value = 'sahamdaraneedalat.ir']
Name
telliranshop.com

Pattern Type
stix
Pattern
[domain-name:value = 'telliranshop.com']
Name
pazinehpress.ir
Pattern Type
stix
Pattern
[domain-name:value = 'pazinehpress.ir']
Name
bartarinhoghooghdan.ir
Pattern Type
stix
Pattern
[domain-name:value = 'bartarinhoghooghdan.ir']
Name
mngg.net

Pattern Type
stix
Pattern
[domain-name:value = 'mngg.net']
Name
ghabfather.com
Pattern Type
stix
Pattern
[domain-name:value = 'ghabfather.com']
Name
nadcompelex.ir
Pattern Type
stix
Pattern
[domain-name:value = 'nadcompelex.ir']
Name
pooshbam.com

Pattern Type
stix
Pattern
[domain-name:value = 'pooshbam.com']
Name
cafe7.ir
Pattern Type
stix
Pattern
[domain-name:value = 'cafe7.ir']
Name
sajjadnameni.com
Pattern Type
stix
Pattern
[domain-name:value = 'sajjadnameni.com']
Name
modaverse.ir

Pattern Type
stix
Pattern
[domain-name:value = 'modaverse.ir']
Name
danesh-book.ir
Pattern Type
stix
Pattern
[domain-name:value = 'danesh-book.ir']
Name
amoomahdi.com
Pattern Type
stix
Pattern
[domain-name:value = 'amoomahdi.com']
Name
20web.ir

Pattern Type
stix
Pattern
[domain-name:value = '20web.ir']
Name
siboushop.ir
Pattern Type
stix
Pattern
[domain-name:value = 'siboushop.ir']
Name
toseeschool.com
Pattern Type
stix
Pattern
[domain-name:value = 'toseeschool.com']
Name
smarticoach.ir

Pattern Type
stix
Pattern
[domain-name:value = 'smarticoach.ir']
Name
coverir.ir
Pattern Type
stix
Pattern
[domain-name:value = 'coverir.ir']
Name
ariyaart.com
Pattern Type
stix
Pattern
[domain-name:value = 'ariyaart.com']
Name
parskaolin.info

Pattern Type
stix
Pattern
[domain-name:value = 'parskaolin.info']
Name
khonegi-kala.ir
Pattern Type
stix
Pattern
[domain-name:value = 'khonegi-kala.ir']
Name
tashstone.com
Pattern Type
stix
Pattern
[domain-name:value = 'tashstone.com']
Name
iranianios.com

Pattern Type
stix
Pattern
[domain-name:value = 'iranianios.com']
Name
cofeios.com
Pattern Type
stix
Pattern
[domain-name:value = 'cofeios.com']
Name
99web.ir
Pattern Type
stix
Pattern
[domain-name:value = '99web.ir']
Name
upvc-behinesazan.com

Pattern Type
stix
Pattern
[domain-name:value = 'upvc-behinesazan.com']
Name
rahnamaapp.site
Pattern Type
stix
Pattern
[domain-name:value = 'rahnamaapp.site']
Name
arsesraeika.ir
Pattern Type
stix
Pattern
[domain-name:value = 'arsesraeika.ir']
Name
maharelec.com

Pattern Type
stix
Pattern
[domain-name:value = 'maharelec.com']
Name
melkbazme.ir
Pattern Type
stix
Pattern
[domain-name:value = 'melkbazme.ir']
Name
toloezarineeghtesad.ir
Pattern Type
stix
Pattern
[domain-name:value = 'toloezarineeghtesad.ir']
Name
idsazan.ir

Pattern Type
stix
Pattern
[domain-name:value = 'idsazan.ir']
Name
ts-tarh.com
Pattern Type
stix
Pattern
[domain-name:value = 'ts-tarh.com']
Name
stakam.ir
Pattern Type
stix
Pattern
[domain-name:value = 'stakam.ir']
Name
attarionlineme.ir

Pattern Type
stix
Pattern
[domain-name:value = 'attarionlineme.ir']
Name
silverfood.ir
Pattern Type
stix
Pattern
[domain-name:value = 'silverfood.ir']
Name
20update.ir
Pattern Type
stix
Pattern
[domain-name:value = '20update.ir']
Name
sarazaccessories.com

Pattern Type
stix
Pattern
[domain-name:value = 'sarazaccessories.com']
Name
academy-fh.ir
Pattern Type
stix
Pattern
[domain-name:value = 'academy-fh.ir']
Name
arsesraeika.com
Pattern Type
stix
Pattern
[domain-name:value = 'arsesraeika.com']
Name
esetstore.shop

Pattern Type
stix
Pattern
[domain-name:value = 'esetstore.shop']
Name
parnasharifanimation.com
Pattern Type
stix
Pattern
[domain-name:value = 'parnasharifanimation.com']
Name
sibou.ir
Pattern Type
stix
Pattern
[domain-name:value = 'sibou.ir']
Name
nasrbahar.com

Pattern Type
stix
Pattern
[domain-name:value = 'nasrbahar.com']
Name
nod-tia.com
Pattern Type
stix
Pattern
[domain-name:value = 'nod-tia.com']
Name
avinpersian.com
Pattern Type
stix
Pattern
[domain-name:value = 'avinpersian.com']
Name
iranpishroasia.ir

Pattern Type
stix
Pattern
[domain-name:value = 'iranpishroasia.ir']
Name
matbazaar.se
Pattern Type
stix
Pattern
[domain-name:value = 'matbazaar.se']
Name
beautiland.net
Pattern Type
stix
Pattern
[domain-name:value = 'beautiland.net']
Name
alocms.ir

Pattern Type
stix
Pattern
[domain-name:value = 'alocms.ir']
Name
taradox.ir
Pattern Type
stix
Pattern
[domain-name:value = 'taradox.ir']
Name
meki.me
Pattern Type
stix
Pattern
[domain-name:value = 'meki.me']
Name
azinpelak.com

Pattern Type
stix
Pattern
[domain-name:value = 'azinpelak.com']
Name
tehranfoton.ir
Pattern Type
stix
Pattern
[domain-name:value = 'tehranfoton.ir']
Name
smartiweb.ir
Pattern Type
stix
Pattern
[domain-name:value = 'smartiweb.ir']
Name
tkolbet.com

Pattern Type
stix
Pattern
[domain-name:value = 'tkolbet.com']
Name
kakperess.ir
Pattern Type
stix
Pattern
[domain-name:value = 'kakperess.ir']
Name
bankesaz.com
Pattern Type
stix
Pattern
[domain-name:value = 'bankesaz.com']
Name
raadhouseoffilm.ir

Pattern Type
stix
Pattern
[domain-name:value = 'raadhouseoffilm.ir']
Name
bimesaad.ir
Pattern Type
stix
Pattern
[domain-name:value = 'bimesaad.ir']
Name
khatekhana.ir
Pattern Type
stix
Pattern
[domain-name:value = 'khatekhana.ir']
Name
salimal666.ir

Pattern Type
stix
Pattern
[domain-name:value = 'salimal666.ir']
Name
khabarejadid.ir
Pattern Type
stix
Pattern
[domain-name:value = 'khabarejadid.ir']
Name
mediageram.ir
Pattern Type
stix
Pattern
[domain-name:value = 'mediageram.ir']
Name
copycopy.ir

Pattern Type
stix
Pattern
[domain-name:value = 'copycopy.ir']
Name
web3ar.cam
Pattern Type
stix
Pattern
[domain-name:value = 'web3ar.cam']
Name
azinorder.ir
Pattern Type
stix
Pattern
[domain-name:value = 'azinorder.ir']
Name
denavasher.com

Pattern Type
stix
Pattern
[domain-name:value = 'denavasher.com']
Name
2line.ir
Pattern Type
stix
Pattern
[domain-name:value = '2line.ir']
Name
digitou.ir
Pattern Type
stix
Pattern
[domain-name:value = 'digitou.ir']
Name
datisabzar.com

Pattern Type
stix
Pattern
[domain-name:value = 'datisabzar.com']
Name
superonlineme.ir
Pattern Type
stix
Pattern
[domain-name:value = 'superonlineme.ir']
Name
sarzaminideal.ir
Pattern Type
stix
Pattern
[domain-name:value = 'sarzaminideal.ir']
Name
luxgiftlux.com

Pattern Type
stix
Pattern
[domain-name:value = 'luxgiftlux.com']
Name
addc.ir
Pattern Type
stix
Pattern
[domain-name:value = 'addc.ir']
Name
raeekala.ir
Pattern Type
stix
Pattern
[domain-name:value = 'raeekala.ir']
Name
bazarchemivevatarebar.com

Pattern Type
stix
Pattern
[domain-name:value = 'bazarchemivevatarebar.com']
Name
piktakk.ir
Pattern Type
stix
Pattern
[domain-name:value = 'piktakk.ir']
Name
drackman2027.ir
Pattern Type
stix
Pattern
[domain-name:value = 'drackman2027.ir']
Name
sharifanimation.com

Pattern Type
stix
Pattern
[domain-name:value = 'sharifanimation.com']
Name
tashstone.net
Pattern Type
stix
Pattern
[domain-name:value = 'tashstone.net']
Name
andishkadehmedia.com
Pattern Type
stix
Pattern
[domain-name:value = 'andishkadehmedia.com']
Name
clickbekhar.com

Pattern Type
stix
Pattern
[domain-name:value = 'clickbekhar.com']
Name
pnpcgart.com
Pattern Type
stix
Pattern
[domain-name:value = 'pnpcgart.com']
Name
mehriazist.com
Pattern Type
stix
Pattern
[domain-name:value = 'mehriazist.com']
Name
itunes24.ir

Pattern Type
stix
Pattern
[domain-name:value = 'itunes24.ir']
Name
hamsoraei.info
Pattern Type
stix
Pattern
[domain-name:value = 'hamsoraei.info']
Name
arsentrans.com
Pattern Type
stix
Pattern
[domain-name:value = 'arsentrans.com']
Name
c730.ir

Pattern Type
stix
Pattern
[domain-name:value = 'c730.ir']
Name
photoiran-co.com
Pattern Type
stix
Pattern
[domain-name:value = 'photoiran-co.com']
Name
asprlus.com
Pattern Type
stix
Pattern
[domain-name:value = 'asprlus.com']
Name
flowers-cake.ir

Pattern Type
stix
Pattern
[domain-name:value = 'flowers-cake.ir']
Name
superonline.click
Pattern Type
stix
Pattern
[domain-name:value = 'superonline.click']
Name
tarhopelak.com
Pattern Type
stix
Pattern
[domain-name:value = 'tarhopelak.com']
Name
hamsoraa.ir

Pattern Type
stix
Pattern
[domain-name:value = 'hamsoraa.ir']
Name
wp30.ir
Pattern Type
stix
Pattern
[domain-name:value = 'wp30.ir']
Name
bargpichak.ir
Pattern Type
stix
Pattern
[domain-name:value = 'bargpichak.ir']
Name
parname.ir

Pattern Type
stix
Pattern
[domain-name:value = 'parname.ir']
Name
giftaks.ir
Pattern Type
stix
Pattern
[domain-name:value = 'giftaks.ir']
Name
pakhshefadak.ir
Pattern Type
stix
Pattern
[domain-name:value = 'pakhshefadak.ir']
Name
azinpelak.ir

Pattern Type
stix
Pattern
[domain-name:value = 'azinpelak.ir']
Name
ts-smart-co.com
Pattern Type
stix
Pattern
[domain-name:value = 'ts-smart-co.com']
Name
sasancisco1@yahoo.com
Pattern Type
stix
Pattern
[email-addr:value = 'sasancisco1@yahoo.com']
Name
iosia.ir

Pattern Type
stix
Pattern
[domain-name:value = 'iosia.ir']

Domain-Name

Value
ghabfather.com
giftaks.ir
khonegi-kala.ir
azinorder.ir
c730.ir
amoomahdi.com
emdadtrip.com
raadhouseoffilm.ir
jettaxi.click
mediageram.ir
2line.ir
tarna.ir
besigni.ir

hamsoraei.info
behsoo-app.ir
avinpayamak.ir
mehriazist.com
clickbekhar.ir
tashstone.net
salimal666.ir
avaper.ir
tehranfoton.ir
mehriadarman.ir
superonline.click
bimesaad.ir
oygar.ir
tashstone.org
smartiweb.ir
adakcharmrasa.ir
beautiland.net
appomobil.ir

bartarinhoghooghdan.ir

denavasher.com

photoiran-co.com

iosia.ir

attarionlineme.ir

40o.ir

rahnamaapp.site

sharifanimation.com

instagramme.ir

azinpelak.com

ghabfather.ir

sarzaminideal.ir

ts-tarh.com

clickbekhar.com

ropekaa.ir

web3ar.cam

tkolbet.com

pnpcgart.com

meymehmarket.ir

superonlineme.ir

piktakk.ir

7thart-m.com

telliranshop.com

film-pardaz.com

sahamdaraneedalat.ir

asprlus.com

pazinehpress.ir

parnasharifanimation.com

itunes24.ir

zooby.ir

flowers-cake.ir

velaati.com

mngg.net

hamsoraa.ir

avinpersian.com

luxgiftlux.com

azinpelak.ir

maharelec.com

pakhshefadak.ir

parsiranwasher.com

bargpichak.ir

khabarejadid.ir

alamutstore.ir

arsentrans.com

rihajeans.ir

digitou.ir

iranpishroasia.ir

danesh-book.ir

arsesraeika.com

ganjineman.com

nadcompelex.ir

toloezarineeghtesad.ir

parname.ir

ebiroll.ir

ariyaart.com

99web.ir

siboshop.ir

gdoe.ir

wp30.ir

arsesraeika.ir

addc.ir

coverir.ir

datisabzar.com

tarhopelak.com

modaverse.ir

hesarakidokhtarane.ir

kakperess.ir

alocms.com

smarticoach.ir

silverfood.ir

animationpress.ir

esetstore.shop

iranianios.com
mooyekamand.com
alocms.ir
devloper.ir
pooshbam.com
parskaolin.info
nasrbahar.com
stakam.ir
drackman2027.ir
wordfa24.ir
taradox.ir
20update.ir
ts-smart-co.com
pakhshmehrbook.ir
melkbazme.ir
saliamal.ir
instasos.ir
20web.ir

andishkadehmedia.com

tekinja.com

andishkademedia.com

cafe7.ir

toseeschool.com

bankesaz.com

nod-tia.com

sajjadnameni.com

sepiderooz.com

academy-fh.ir

khatekhana.ir

gardeshgareirani.com

bazarchemivevatarebar.com

ghasrelebas.ir

pishroyadaknovin.com

timekook.ir

idsazan.ir

parna-sakhteman.ir

siboushop.ir

tashstone.com

raeekala.ir

meki.me

sibou.ir

cofeios.com

amoomehdi.com

matbazaar.se

copycopy.ir

upvc-behinesazan.com

sarazaccessories.com

Email-Addr

Value
mehdi.k1989@yahoo.com
mehdi.kh021@yahoo.com
sasancisco1@yahoo.com

External References

- https://otx.alienvault.com/pulse/651e82cf5ed5af844bd61ff3
- https://www.domaintools.com/resources/blog/return-to-sender-a-brief-analysis-of-a-us-postal-service-smishing-campaign/