TrendLabs

Malicious Chrome Extensions Found in Chrome Web Store, Form Droidclub Botnet

Appendix

TrendLabs Security Intelligence Blog

January 2018

Chrome Extensions related to Droidclub

Chrome Extension ID	Extension Name
aedobkofagambpnhibndgllabmkhiink	Cheesy Barbecue Bacon
ahcodkopnoolabmeeddimaccfbbgbnkg	Inspired Wall Hanging
ahgfcgbmapkkfkkngkbgdhmefglhhoch	Seafood Cioppino
ajfmifgcjbdlifbbcoocbagcpbpbafip	Chalkboard Serving Tray
alcemhodmihppbkoipjoiigeladbmfab	Perfect Steaks
amhboafopmbeaiifkcmolgielebplddn	Cute Reindeer Cake
bajpajaplkkmfohgfckjdcmjaodhigbm	New bag from t-shirt
bbjnbbkmmlfamopoapkcbhknhjolebll	Toss Carnival Game
bbklochlbdnjkepkogifmlaaejfgnjhf	Holiday Scene
caepkodhijhgkecbklgldhkdaepalahh	Christmas Paper Lantern
chnfpgfeobeekbnpmaajncohmppfpfjb	Salad Garden
ckcnkbhdcgbfjjpomejcknjflkggmpjm	a Birch Wood Reindeer
cklihcncoeagchmooepokamfkjfofkep	Peaches and Plums
clcemeljdlfkhddlfcplkibelopdhdik	Cookie Dough
clglkelnalggbnimiglpodkhledoenfk	To Deodorize Laundry
ddllmjjlakacffbeidndbdogijobmble	Homemade Carpet Cleaner
dkmddfhmoocfdhcogjagaijjcinbdmeb	How to Make Gumbo
edbkkbdfomalmbjdpfhaiciheppjihgo	Pinwheel Rosettes
edndmdgfkambceallfcifndcnihfkhce	Ideas to Beautify Your Apartment
eefgplhbgoepdkcjhlbpedgpchkgfedo	Zipper in a Sweatshirt
egdcgagkkckipplmpfdfimmcipjjfkko	Pickled Jalapenos
egjmkjdlkbjjenockdaamogoiioojgjp	Edible Eyeball Pizza
egoalalhadillklokiiennmdflbhehoh	A Turkey Napkin
ekeimjfcakmhnblboldknbnnhedjehjo	Shrunken Head Apple Martini
emdcmoghepkahnnlfmejnibfbmeoogmb	Watch Strap
eodhkpnifohleagpkpkkihmokkcncokf	Charming Hanging Lanterns
fegiafbcldadckahemhlfcopplfdlmkp	Sugar Cookie Icing
ffkenifflcedlgdkgilddnkaimmbhnec	Homemade Drawer Freshener
fghmmljkejbamjhomoodegbepogpheef	Homemade Frozen Pizza
fhnpncldijeifoiefkimdjebgkgidpgd	Black Tap Copycat
fmhocfhibfmddhnfcflkodjdnflcgkdp	Desert Style Basket

Chrome Extension ID	Extension Name
fppfjlcbcjhfobfaichenmodmadgmbne	Air Plant Holder
gbhkbbffliokhhhibdedjcjoecnikiml	Homemade Freshen Up
ghcogfnebgohebaklihmafkofhldcebl	Candied Pecans
gidollmkeombihcojmdjgfekbipejkoj	Cherry Blueberry Pie
gmpceckpipekimgkonhmhoidfffbeinh	Croissant French Toast
gnkieagafibgmfdefcbedaeplecddjkd	Italian Skewers
gpmgeepeilllooepnckccihefopjbebb	Outdoor Garbage Cans
hjlbdangjggpfmhjbcccnnpnhhhpgpdf	Spin Art Machine
hnokbehlbjkbhlihbldeojhjpekehmmf	Orange Pomegranate Sangria
hofflgideggmbkicgkniefmmhkhelefj	Star Shaped Pies
hpfpmcafjghjgdilidipkfgpomphgekf	Applesauce Christmas Ornaments
iamfjjibfikiafdleojocafoaejhpljk	Cake Pop Patriotic
iheagohkldggdkggihjljdcfnfhfgiah	a Snowman Out of a Tomato Cage
iikbadloeacgcpjdnnockinpepkmcjap	Cinnamon Roll Wreath
ikfmcoipokjnmjoofngdnmkkhopjhehg	Clean Grill Grates
iomommpnoplgaihpbjpfpmcaabgccbna	When Dylan “Went Electric”
ipilkhafbndhbphcecjldjilhegnjcja	Spinach Artichoke Dip
ipoeoopnckpoaoeghdgehhbbipnccoap	Clay Gift Tags
jhahdjelgjmpekbclkcgbgibkgdifaml	Coasters on a Cardboard Loom
jiibdgiopnflbpbdpmgpjnpdooekonjc	Cuban Sandwich
jmcccnnkmflngcfeebnbhfbjehglldlf	Coconut Cookies
jnjapnhdnkmdmgandniokkjpggpfalog	Fabric Sachets
kabhgijpbgkpbegomdihijdcocimlnkf	Summer Fairy Lanterns
kcbempkceemjmcfgicdofhcmkojdfbjl	Cuban Ropa Vieja
kdndbohghpcpdkbpjhdphniglgppjakd	How to Make a Kissing Ball
khkcgpbajgkfmkilijbhfinfeapcannh	Pink Lemonade
kjhgjfbokhfadnlnagimjabemfdgdfdh	Patriotic String Lights
kjhppechdhnchkcjbaboglblnfihenjf	Glow in the Dark
klbelohlhkobpoeaimclnpikbdphkdhn	Avocado to Your Meals
kmfcjjkgokeekaohiijgnilbaihnifpc	Soup Bowl Hot Pads
kpoobaeilcfcjfkbaaapdnkmaifmffkk	Portable Camp Stove
lbflgehklpfnaofgfjhcbjajhckdoogc	Layer Hot Chocolate Mix
lhpcjiffachihfbhkabenpcpehkpoeid	11 Pumpkin Flavored Foods
lifjihfdppaeaegemoefheidgcnjkadn	Drumsticks on the Grill

Chrome Extension ID	Extension Name
ligldfbjaakcmbjbbbnnacjgaenggfph	Italian Pasta Salad
ljgnhmdnjbmnghlfimcnmkieohlflpgd	DIY Cleaning Wipes
lnmfepglldbolfelhbmiohockghoabpc	Homemade Dole Whip
lojgfkjekmbmndapleelbbemgjbdcjjm	Swirled Pumpkin Cheesecake
mafmpgcoinifjbepiknmnogefcomjpph	Peach Sangria
mccbmgbbkpcnpblacndlfcgokbklkiam	School Notebooks
mhjbpgjmhcaemdakpgmpffblohinegji	Ironing Board Cover
mjheoiainplbfjnjclkjifhjdahfejaj	Chocolate Peanut Butter
mjpmldmndlkbacfaaiamcgnfbllhdnbc	Gingerbread Freakshake
mkmkhjdmkaeffpfgfljelahfogghkgol	Holiday Reindeer Mugs
mldmghlinbmofcdhopfmkgnhohomodgi	Homemade Stress Balls
mmnhdabiapbgbcbagdncjehjdbpkigeh	Turkey from Flowers
ndhgnlodmpalhnfdopckpolhinaafkgh	Birch Branch Menorah
nllbbpmplfhdpdnmoiigegjicamfhnhn	Cinnamon Toast Crunch Coffee Cake Recipe
nolggnmhlagghnfpellfnkcmkgeoiepj	Star Wars Christmas Cookies
obnjngpeldplgkenihhhdicoeplcfbeg	Chicken for a Barbecue
ooialhjmccmllnifoiblbjgcnbgdejpm	DIY Cement Candle
paokbggdacflkaiddinlhpkpegklgolc	Halloween Masterpiece
pbgdknbinlcbjkbiihcakedepnbonnce	Cookies and Ice Cream
pdbdlcjiihinipmeijmccidamciifhag	Star Wars Christmas Sweater
penlocnbkkkcaingngkjmdlkikeklemm	Unique Outdoor Christmas Decorations
pfcidoolgbfidgaclhiipeleagglabpc	Easy Ribbon Bow
poecefgcfhghjbdifplpcaapkfnakfkk	Desktop Air Conditioner
pplcbeendgbblphgmdgfcofdbfiocfgb	Candle Wax

Domains related to Droidclub

Domain	Use by Droidclub
77mleq3.club	C&C Domain
accuracy.party	C&C Domain
adama.space	C&C Domain
alary.accountant	C&C Domain
ameer.bid	C&C Domain
antimaterialistically.men	C&C Domain
areopagitica.club	C&C Domain
atonal.club	C&C Domain
bertolt.club	C&C Domain
chiru.trade	C&C Domain
cholon.club	C&C Domain
coatee.club	C&C Domain
copley.club	C&C Domain
cyclotrimethylenetrinitramine.cricket	C&C Domain
domain092.club	C&C Domain
domain157.club	C&C Domain
domain291.club	C&C Domain
domain352.club	C&C Domain
droidclub.net	C&C Domain
esterifiable.club	C&C Domain
exterra.host	C&C Domain
fledge.live	C&C Domain
fratchy.host	C&C Domain
frija.faith	C&C Domain
groomishly.club	C&C Domain
huambo.club	C&C Domain
invoicegyp.club	C&C Domain
inwrap.club	C&C Domain
isobardubbin.club	C&C Domain
ithun.bid	C&C Domain
jurez.site	C&C Domain
kench.download	C&C Domain
laing.club	C&C Domain

Domain	Use by Droidclub
lichenin.top	C&C Domain
litho.cricket	C&C Domain
lomax.top	C&C Domain
lucullus.pro	C&C Domain
meredyth.racing	C&C Domain
mycol.club	C&C Domain
narrated.pw	C&C Domain
navig.site	C&C Domain
niellist.top	C&C Domain
odious.club	C&C Domain
ornis.site	C&C Domain
parsec.news	C&C Domain
phenylethylmalonylurea.loan	C&C Domain
pian.stream	C&C Domain
refilm.club	C&C Domain
salal.stream	C&C Domain
satrap.top	C&C Domain
shoji.club	C&C Domain
shoji.site	C&C Domain
somoza.club	C&C Domain
spinifex.club	C&C Domain
sqq.trade	C&C Domain
stk.science	C&C Domain
subframe.tech	C&C Domain
superdeficit.press	C&C Domain
swinking.top	C&C Domain
tomah.press	C&C Domain
tursha.club	C&C Domain
understress.loan	C&C Domain
undroider.com	C&C Domain
unetched.racing	C&C Domain
visually.pw	C&C Domain
x73w7k6.club	C&C Domain
872voluum-trk.win	Malvertising Domain (First Stage)

Domain	Use by Droidclub
amazn-srv432.host	Malvertising Domain (First Stage)
amazn-srv993.club	Malvertising Domain (First Stage)
cloudflre-domain232.club	Malvertising Domain (First Stage)
cpa-track103.host	Malvertising Domain (First Stage)
onclick392.club	Malvertising Domain (First Stage)
pxl058trk.top	Malvertising Domain (First Stage)
srv230bid.site	Malvertising Domain (First Stage)
abie.me	Malvertising Domain (Second Stage)
acle.me	Malvertising Domain (Second Stage)
agba.me	Malvertising Domain (Second Stage)
alae.me	Malvertising Domain (Second Stage)
alag.me	Malvertising Domain (Second Stage)
aton.me	Malvertising Domain (Second Stage)
avdp.me	Malvertising Domain (Second Stage)
badb.me	Malvertising Domain (Second Stage)
bawd.me	Malvertising Domain (Second Stage)
bhut.me	Malvertising Domain (Second Stage)
boac.me	Malvertising Domain (Second Stage)
bukh.me	Malvertising Domain (Second Stage)
cack.me	Malvertising Domain (Second Stage)
cagy.me	Malvertising Domain (Second Stage)
camb.me	Malvertising Domain (Second Stage)
carn.me	Malvertising Domain (Second Stage)
cete.me	Malvertising Domain (Second Stage)
copt.me	Malvertising Domain (Second Stage)
cuyp.me	Malvertising Domain (Second Stage)
dard.me	Malvertising Domain (Second Stage)
dmod.me	Malvertising Domain (Second Stage)
dpnh.me	Malvertising Domain (Second Stage)
duad.me	Malvertising Domain (Second Stage)
dyak.me	Malvertising Domain (Second Stage)
emeu.me	Malvertising Domain (Second Stage)
excl.me	Malvertising Domain (Second Stage)
eysk.me	Malvertising Domain (Second Stage)

Domain	Use by Droidclub
fahr.me	Malvertising Domain (Second Stage)
faur.me	Malvertising Domain (Second Stage)
galv.me	Malvertising Domain (Second Stage)
genk.me	Malvertising Domain (Second Stage)
genl.me	Malvertising Domain (Second Stage)
gibe.me	Malvertising Domain (Second Stage)
gwyn.me	Malvertising Domain (Second Stage)
hond.me	Malvertising Domain (Second Stage)
howf.me	Malvertising Domain (Second Stage)
huly.me	Malvertising Domain (Second Stage)
icbm.me	Malvertising Domain (Second Stage)
inyl.me	Malvertising Domain (Second Stage)
jebb.me	Malvertising Domain (Second Stage)
jimp.me	Malvertising Domain (Second Stage)
jute.me	Malvertising Domain (Second Stage)
kerf.me	Malvertising Domain (Second Stage)
kval.me	Malvertising Domain (Second Stage)
ller.me	Malvertising Domain (Second Stage)
llud.me	Malvertising Domain (Second Stage)
lowl.me	Malvertising Domain (Second Stage)
ludd.me	Malvertising Domain (Second Stage)
lzen.me	Malvertising Domain (Second Stage)
miae.me	Malvertising Domain (Second Stage)
mlos.me	Malvertising Domain (Second Stage)
mown.me	Malvertising Domain (Second Stage)
nccl.me	Malvertising Domain (Second Stage)
oast.me	Malvertising Domain (Second Stage)
odra.me	Malvertising Domain (Second Stage)
onas.me	Malvertising Domain (Second Stage)
opis.me	Malvertising Domain (Second Stage)
payt.me	Malvertising Domain (Second Stage)
peag.me	Malvertising Domain (Second Stage)
pheb.me	Malvertising Domain (Second Stage)
pily.me	Malvertising Domain (Second Stage)

Domain	Use by Droidclub
pore.me	Malvertising Domain (Second Stage)
puir.me	Malvertising Domain (Second Stage)
quod.me	Malvertising Domain (Second Stage)
ramc.me	Malvertising Domain (Second Stage)
salk.me	Malvertising Domain (Second Stage)
scag.me	Malvertising Domain (Second Stage)
shii.me	Malvertising Domain (Second Stage)
shtg.me	Malvertising Domain (Second Stage)
sial.me	Malvertising Domain (Second Stage)
suet.me	Malvertising Domain (Second Stage)
sugh.me	Malvertising Domain (Second Stage)
suiy.me	Malvertising Domain (Second Stage)
surt.me	Malvertising Domain (Second Stage)
syll.me	Malvertising Domain (Second Stage)
teth.me	Malvertising Domain (Second Stage)
tufa.me	Malvertising Domain (Second Stage)
umpy.me	Malvertising Domain (Second Stage)
waaf.me	Malvertising Domain (Second Stage)
wast.me	Malvertising Domain (Second Stage)
wctu.me	Malvertising Domain (Second Stage)
weka.me	Malvertising Domain (Second Stage)
whig.me	Malvertising Domain (Second Stage)
yedo.me	Malvertising Domain (Second Stage)
yhwh.me	Malvertising Domain (Second Stage)
ywis.me	Malvertising Domain (Second Stage)
zoea.me	Malvertising Domain (Second Stage)
zoug.me	Malvertising Domain (Second Stage)

Securing Your Journey to the Cloud

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.

Created by:

TrendLabs

Global Technical Support & R&D Center of TREND MICRO