

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division**

MICROSOFT CORPORATION, a
Washington corporation, and FS-ISAC, INC.,
a Delaware corporation,

Plaintiffs,

v.

JOHN DOES 1-3 CONTROLLING A
COMPUTER BOTNET THEREBY
INJURING PLAINTIFFS AND THEIR
CUSTOMERS AND MEMBERS,

Defendants.

Civil Action No: 1:15 cv 240

**FILED UNDER SEAL PURSUANT TO
LOCAL CIVIL RULE 5**

**EX PARTE TEMPORARY RESTRAINING ORDER AND
ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION**

Plaintiffs Microsoft Corp. (“Microsoft”) and Financial Services – Information Sharing And Analysis Center, Inc. (“FS-ISAC”) (collectively “Plaintiffs”) have filed a complaint for injunctive and other relief pursuant to: (1) the Computer Fraud and Abuse Act (18 U.S.C. § 1030); (2) the Electronic Communications Privacy Act (18 U.S.C. § 2701); (3) the Lanham Act (15 U.S.C. §§ 1114(a)(1), 1125(a), (c)); and (4) the common law of trespass, unjust enrichment and conversion. Plaintiffs have moved *ex parte* for an emergency temporary restraining order and an order to show cause why a preliminary injunction should not be granted pursuant to Rule 65(b) of the Federal Rules of Civil Procedure, 15 U.S.C. § 1116(a) (the Lanham Act), and 28 U.S.C. § 1651(a) (the All-Writs Act).

FINDINGS OF FACT AND CONCLUSIONS OF LAW

Having reviewed the papers, declarations, exhibits, and memorandum filed in support of Plaintiffs' Application for an Emergency Temporary Restraining Order, the Court hereby makes the following findings of fact and conclusions of law:

1. This Court has jurisdiction over the subject matter of this case and there is good cause to believe that it will have jurisdiction over all parties hereto; the Complaint states a claim upon which relief may be granted against Defendants John Does 1-3 ("Defendants") under the Computer Fraud and Abuse Act (18 U.S.C. § 1030), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125) and the common law of trespass to chattels, unjust enrichment and conversion.

2. There is good cause to believe that Defendants have engaged in and are likely to engage in acts or practices that violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125) and constitute trespass to chattels, unjust enrichment and conversion, and that Plaintiffs are, therefore, likely to prevail on the merits of this action;

3. Microsoft owns the registered trademarks "Internet Explorer," "Microsoft," and "Windows" used in connection with its services, software and products. FS-ISAC's member organizations have invested in developing their brands, trademarks, and trade names in association with the financial services they offer.

4. There is good cause to believe that, unless Defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from the Defendants' ongoing violations. The evidence set forth in Plaintiffs' Brief in Support of Application for a Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("TRO Application"), and the accompanying declarations and exhibits, demonstrates that Plaintiffs are likely to prevail on their claim that Defendants have engaged in violations of the foregoing law by:

- a. intentionally accessing and sending malicious software to the protected computers and operating systems of the customers or associated member organizations of Microsoft and FS-ISAC, without authorization or exceeding authorization, in order to infect those computers and make them part of the computer botnet known as the “Ramnit” botnet (the “botnet”);
- b. sending malicious code to configure, deploy and operate a botnet;
- c. deploying computers and Internet domains to establish a command and control infrastructure for a botnet;
- d. using the command and control servers and Internet domains to actively manage and control a botnet for illegal purposes;
- e. intercepting Plaintiffs’ webpages and altering them to deceptively induce victims to enter sensitive credentials, while falsely indicating that the webpages are created or approved by Plaintiffs or Plaintiffs’ member organizations;
- f. stealing personal and financial account information and files from computer users; and
- g. using stolen information to steal money from the financial accounts of those users.

5. There is good cause to believe that if such conduct continues, irreparable harm will occur to Plaintiffs, Plaintiffs’ customers and member organizations, and the public. There is good cause to believe that the Defendants will continue to engage in such unlawful actions if not immediately restrained from doing so by Order of this Court;

6. There is good cause to believe that immediate and irreparable damage to this Court’s ability to grant effective final relief will result from the sale, transfer, or other disposition or concealment by Defendants of botnet command and control software that is hosted at and otherwise operates through the Internet domains listed in Appendix A to this Order (“Appendix A”) and from the destruction or concealment of other discoverable evidence

of Defendants' misconduct available via those domains, including on user computers infected with Ramnit, if Defendants receive advance notice of this action. Based on the evidence cited in Microsoft's TRO Application and accompanying declarations and exhibits, Plaintiffs are likely to be able to prove that:

- a. Defendants are engaged in activities that directly violate United States law and harm Plaintiffs and the public, including Plaintiffs' customers and member-organizations;
- b. Defendants have continued their unlawful conduct despite the clear injury to the foregoing interests;
- c. Defendants are likely to delete or to relocate the botnet command and control software at issue in Plaintiffs' TRO Application and the harmful, malicious, and trademark infringing software disseminated through the Internet domains listed in Appendix A;
- d. Defendants are likely to issue a "kill" command to computers infected with Ramnit botnet malware, thereby damaging them irreparably and making any evidence on them irretrievable; and
- e. Defendants are likely to warn their associates engaged in such activities if informed of Plaintiffs' action.

7. Plaintiffs' request for this emergency *ex parte* relief is not the result of any lack of diligence on Plaintiffs' part, but instead based upon the nature of Defendants' unlawful conduct. Therefore, in accordance with Fed. R. Civ. P. 65(b), 15 U.S.C. § 1116(a) and 28 U.S.C. § 1651(a), good cause and the interest of justice require that this Order be Granted without prior notice to Defendants, and accordingly, Plaintiffs are relieved of the duty to provide Defendants with prior notice of Microsoft's motion;

8. There is good cause to believe that Defendants have specifically directed their activities to computers of Plaintiffs' customers and member organizations located in the Eastern District of Virginia, have engaged in illegal activity using the Internet domains identified in

Appendix A to this Order by directing malicious botnet code and content to said computers of Plaintiffs' customers and member organizations, to further perpetrate their fraud on Plaintiffs' customers and member organizations. There is good cause to believe that Defendants have directed said malicious botnet code and content through certain instrumentalities – specifically the domain registration facilities of the domain registries identified in Appendix A.

9. There is good cause to believe that Defendants have engaged in illegal activity by using the domain registration facilities of the domain registries identified in Appendix A to register the Internet domains identified in Appendix A, so as to deliver from those domains the malicious botnet code, content, and commands that Defendants use to maintain and operate the botnet to the computers of Plaintiffs' customers and member organizations, and to receive the information stolen from those computers.

10. There is good cause to believe that Defendants have engaged in illegal activity by using deceptive and fake methods to steal computer users' login and/or financial account credentials and to use such credentials to steal funds from such users.

11. There is good cause to believe that to immediately halt the injury caused by Defendants, Defendants must be prohibited from sending malicious botnet code, content and commands from the Internet domains identified in Appendix A to computers of Plaintiffs' customers.

12. There is good cause to believe that Defendants have engaged in illegal activity using the Internet domains identified in Appendix A to host the command and control software and content used to maintain and operate the botnet. There is good cause to believe that to immediately halt the injury caused by Defendants, each of Defendants' current and prospective domains set forth in Appendix A must be immediately redirected to the Microsoft-secured name-servers named NS11.microsoftinternetsafety.net and NS12.microsoftinternetsafety.net, thus making them inaccessible to Defendants for command and control purposes.

13. There is good cause to believe that to immediately halt the injury, the execution of this Order should be carried out in a coordinated manner by Plaintiffs and by the domain

registries identified in Appendix A on or about 10:00 a.m. Eastern Standard Time on February 24, 2015, or such other date and time within eight days of this Order as may be reasonably requested by Plaintiffs.

14. There is good cause to believe that Defendants will routinely update the Internet domains associated with the Ramnit Botnet, and that Plaintiffs may identify and update the domains listed in Appendix A as may be reasonably necessary to account for additional Internet domains associated with the Ramnit Botnet just prior to the February 24, 2015 execution of this Order.

15. There is good cause to permit notice of the instant Order, notice of the Preliminary Injunction hearing and service of the Complaint by formal and alternative means, given the exigency of the circumstances and the need for prompt relief. The following means of service are authorized by law, satisfy Due Process, and satisfy Fed. R. Civ. P. 4(f)(3) and are reasonably calculated to notify Defendants of the instant order, the Preliminary Injunction hearing and of this action: (1) by personal delivery upon Defendants who provided accurate contact information in the U.S., if any, (2) personal delivery through the Hague Convention on Service Abroad or similar treaties upon defendants who provided accurate contact information in foreign countries that are signatory to such treaties, if any, (3) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to their domain registrars and hosting companies and as agreed to by Defendants in their domain registration and/or hosting agreements, (4) publishing notice on a publicly available Internet website and/or in newspapers in the communities where Defendants are believed to reside.

TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE

IT IS THEREFORE ORDERED that, Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from: (1) intentionally accessing and sending malicious software or code to Plaintiffs and the protected computers and operating systems of Plaintiffs' customers and associated member organizations, without authorization, in order to infect those computers and make them part of

any botnet, (2) sending malicious code to configure, deploy and operate a botnet, (3) intercepting and altering Plaintiffs webpages such that they falsely indicate that they are associated with or approved by Plaintiffs or Plaintiffs' member organizations; (4) configuring, deploying, operating, or otherwise participating in or facilitating the botnet described in the TRO Application, including but not limited to the command and control software hosted at and operating through the Internet domains set forth in Appendix A and through any other component or element of the botnet in any location; (5) stealing information, money, or property from Plaintiffs, Plaintiffs' customers, or Plaintiffs' member organizations; (6) misappropriating that which rightfully belongs to Plaintiffs, their customers, or their associated member organizations or in which Plaintiffs, their customers, or their associated member organizations has a proprietary interest; or (7) undertaking any similar activity that inflicts harm on Plaintiffs, Plaintiffs' customers or member associations, or the public.

IT IS FURTHER ORDERED that, Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from (1) using and infringing Microsoft's trademarks, including specifically Microsoft's registered trademarks "Internet Explorer," "Microsoft" or "Windows," bearing registration numbers 2872708, 2463526 and 2277112; the trademarks of financial institution members of FS-ISAC and/or other trademarks, trade names, service marks, or Internet Domain addresses or names; (2) using in connection with Defendants' activities, products or services any false or deceptive designation, representation or description of Defendants' or of their activities, whether by symbols, words, designs or statements, which would damage or injure Plaintiffs or their member organizations or give Defendants an unfair competitive advantage or result in deception of consumers; or (3) acting in any other manner which suggests in any way that Defendants' activities, products or services come from or are somehow sponsored by or affiliated with Plaintiffs, or passing off Defendants' activities, products or services as Plaintiffs' or their member organizations.

IT IS FURTHER ORDERED that, with respect to any currently registered Internet

domains set forth in Appendix A, the domain registries located in the United States shall take the following actions:

A. Maintain unchanged the WHOIS or similar contact and identifying information as of the time of receipt of this Order and maintain the domains with the current registrar;

B. The domains shall remain active and continue to resolve in the manner set forth in this Order;

C. Prevent transfer or modification of the domains by Defendants or third parties at the registrar;

D. The domains shall be redirected to secure servers by changing the authoritative name servers to NS11.microsoftinternetsafety.net and NS12.microsoftinternetsafety.net and, as may be necessary, the IP address associated with name server or taking other reasonable steps to work with Microsoft to ensure the redirection of the domains and to ensure that Defendants cannot use them to control the botnet.

E. Take all steps required to propagate to the foregoing changes through the DNS, including domain registrars;

F. Preserve all evidence that may be used to identify the Defendants using the domains.

G. Refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives and refrain from publicizing this Order until this Order is executed in full, except as necessary to communicate with domain registrars and registries to execute this order.

IT IS FURTHER ORDERED that, with respect to any domains set forth in Appendix A that are *currently unregistered*, the domain registries and registrars located in the United States shall take the following actions:

A. Transfer the domains to the control of Microsoft, such that Microsoft is the registrant with control over hosting and administration of the domains. Domains should be transferred to Microsoft's account at the sponsoring registrar MarkMonitor.

B. The WHOIS registrant, administrative, billing and technical contact and identifying information should be the following;

Domain Administrator
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
United States
Phone: +1.4258828080
Facsimile: +1.4259367329
domains@microsoft.com

C. The domains shall be made active and shall resolve in the manner set forth in this order or as otherwise specified by Microsoft.

D. The domains shall be assigned the authoritative name servers NS11.microsoftinternetsafety.net and NS12.microsoftinternetsafety.net and, as may be necessary, the IP address associated with name servers or taking such other reasonable steps to work with Microsoft to ensure that the domains and subdomains are put within Microsoft's control, and to ensure that Defendants cannot use them to control the botnet.

E. Refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives and refrain from publicizing this Order until this Order is executed in full, except as necessary to communicate with domain registrars or registries to execute this order.

IT IS FURTHER ORDERED that copies of this Order, notice of the Preliminary Injunction hearing and service of the Complaint may be served by any means authorized by law, including (1) by personal delivery upon Defendants who provided accurate contact information in the U.S., if any; (2) personal delivery through the Hague Convention on Service Abroad or similar treaties upon defendants who provided accurate contact information in foreign countries that are signatory to such treaties, if any, (3) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to their domain registrars and/or hosting companies and as agreed to by Defendants in their domain registration and/or hosting agreements, (4) publishing notice on a publicly available Internet website and/or in

newspapers in the communities where Defendants are believed to reside.

IT IS FURTHER ORDERED, pursuant to Federal Rule of Civil Procedure 65(b) that the Defendants shall appear before this Court on March 5, 2015 at 11:00am to show *AMB* cause, if there is any, why this Court should not enter a Preliminary Injunction, pending final ruling on the Complaint against the Defendants, enjoining them from the conduct temporarily restrained by the preceding provisions of this Order.


IT IS FURTHER ORDERED that Microsoft shall post bond in the amount of \$200,000 as cash to be paid into the Court registry *by 3:00 pm. Monday February 23, 2015 - AMB*

IT IS FURTHER ORDERED that Plaintiffs may identify and update the domains in Appendix A to this Order as may be reasonably necessary to account for additional Internet domains associated with the Ramnit Botnet just prior to the February 24, 2015 execution of this Order.

IT IS FURTHER ORDERED that the Defendants shall file with the Court and serve on Plaintiffs' counsel any answering affidavits, pleadings, motions, expert reports or declarations and/or legal memoranda no later than two (2) days prior to the hearing on Microsoft's request for a preliminary injunction. Plaintiffs may file responsive or supplemental pleadings, materials, affidavits, or memoranda with the Court and serve the same on counsel for the Defendants no later than one (1) day prior to the preliminary injunction hearing in this matter. Provided that service shall be performed by personal or overnight delivery, facsimile or electronic mail, and documents shall be delivered so that they shall be received by the other parties no later than 4:00 p.m. (Eastern Standard Time) on the appropriate dates listed in this paragraph.

IT IS SO ORDERED

Entered this 20th day of February, 2015

AMB
/s/ 

Leonie M. Brinkema
United States District Judge

APPENDIX A

REGISTRY FOR .COM DOMAINS

Verisign Naming Services
21345 Ridgetop Circle
4th Floor
Dulles, Virginia 20166
United States

Verisign Global Registry Services
12061 Bluemont Way
Reston Virginia 20190
United States

CURRENTLY REGISTERED .COM DOMAINS

anxsmqyfy.com
campbrusderapp.com
jhghrlufoh.com
khllpmpmare.com
knpqxlxcwtlvgrdyhd.com
nvlyffua.com
ppyblaohb.com
riaaiysk.com
santabellasedra.com
tqjhvylf.com
vrndmdrdrjoff.com

DEFENDANTS JOHN DOES 1 – 3 CONTACT INFORMATION

caewoodydr@uymail.com
campmorgenapp@arcticmail.com
carmiller@mail.com
redswoodster@engineer.com
gromsmoothe@arcticmail.com

UNREGISTERED .COM BACKUP DOMAINS GENERATED BY BOTNET

acuhjbadvnmhthwnlxv.com
advvpbrtyw.com
aflgqgddfi.com
apbhwiохqbvoxlumdh.com
apkdwbdpickk.com
aprocqhqmml.com
asldoqoolcgm.com
aufdloglxlqoxlepp.com
avxvatwmxwbyiepwwo.com

ayketyjlsaeu.com
bltolwbwychlyt.com
bmaucdrfpmnh.com
bmjjksysowdwmoy.com
bmjvrxrqpkiwdrdv.com
bpiwebgqddyvgcnjgh.com
briujbxmkjeusvslrn.com
bseboouatanfddgbrdv.com
bvqdvfihwnaja.com

cbxyvrxewvlnxhkadfg.com
ccylbclg.com
cgwootylkoyxe.com
cjagpjgd.com
ckgvnbwdywbxvlnk.com
clkcdjjmyylwib.com
cqvylephudwsuqjhge.com
croxxnrtvrqt.com
cuhbjlgw.com
cyanlvwkuatvmw.com
dbygksqtu.com
dfalxqubjhl.com
dfvxuvljbykia.com
dhfejwhoj.com
dledwgrxiiqspx.com
dnqjposxrelhqplwli.com
duhjqituiokycypi.com
dwbdecmppklvbevjtq.com
dwksmbrq.com
dxktegertgbgeoi.com
dxzteubknwecsdutlp.com
ealxbraobohxb.com
ebrfoys.com
ecsgmpariu.com
edvxemrsvvycwt.com
egopuefrdsefc.com
eipvatwwexl.com
ejfrcfwdbsaahtdt.com
emlxeirx.com
emxwjwpcb.com
ersbvvdxdamjotwpm.com
etjdsnpjvb.com
euvyalbkwahxxjn.com
evrlsscrxvmd.com
exmfhgyv.com
eyvvpstmcwwwsyjtif.com
facmttjcdq.com
fgcdhqgcdomle.com
fjdmkqvralmgorinc.com
fkcfkcygpldjcr.com
fmdjnmskmjhjq.com
fmjboahxkasxdl.com
fmqegimr.com
fsxgwfwychemrgrmhwo.com
fuogcmhewqer.com
fvkercflhy.com

fxngienbgebck.com
fycecyuksgjfxy.com
gaqqerty.com
gbcpynphvropsyu.com
gdekatkjjihi.com
gmsxrgagrfgivh.com
gqnoupteuivrwte.com
grbfrnxxej.com
gtiswnukb.com
guifymdmxj.com
gunqwxgyrl.com
gwmjxjueqme.com
gwnppapgwhtidegx.com
hajqfvvqjkkajwi.com
hjahmdueyebf.com
hjlshhecwshpfxwfl.com
hlcololi.com
hllnakmxmgoyh.com
hlrsxdakvl.com
hoeqosqeicddv.com
hskceeltsbbnc.com
hvkxvhkmfsdgd.com
hvyfjjqdlwhnlrpa.com
hwruujnk.com
ibvtknxochoyjidm.com
icqkxusbfdwhy.com
ifbomanec.com
ijfwbyvcirepgd.com
ikkjjgbqgts.com
ilpvrpxwfauqaxyq.com
imvfakaudq.com
iqhafgpvsrj.com
ixwnsfmyg.com
iylelocfsj.com
jherkljcsloepd.com
jhfykbugtthmdkgga.com
jhrqfnrlpyvo.com
jjdvasey.com
jkgvbneenmrbklortr.com
jkyyolccexfy.com
jmesrbwtcjev.com
jmmurxyktxvegsxid.com
jnjjlojgnvxesr.com
jvmckcospyqedcsjny.com
jycxmcdof.com
jymqfxgwfhyms.com

kavkwpjdndsk.com
kcilhmepervm.com
kdjsnsre.com
kdkdpwql.com
kjpsjoxqsutgewlrah.com
kuwkdqstblavept.com
kvcovjrpsb.com
kvfkfxakmqoof.com
kynknfyngikfno.com
kyskhoopsmkmbenau.com
labxpyvtwuijwghie.com
lcqavndroo.com
lehmgspxp.com
liedjckipkehqxwtdl.com
llgnygbqhv.com
llurxdkpkbvjx.com
lorwmtrf.com
lpivbutq.com
lpvdauemfexnvoyh.com
lsvnoumbqcsjl.com
ltrpfybf.com
luvrqdhavhxcbtc.com
lvqdhqrhfxlsglkf.com
lvrjjmbdtfapwev.com
lwnnggpwjlvyagmu.com
lybfxrtkcdkbbqr.com
lyftposyknpigp.com
lyvxrtpkchmddb.com
lyxbotuappfreadkfk.com
mbpnjenhxgcimx.com
mchpmdywgs.com
mfnaqngqorgbxbnsc.com
mhuvivlyndmsx.com
mioqhqvmduqicvoey.com
mkdnthyiqlq.com
mktxegrucbkv.com
mlgdwljfmnkt.com
mqojcxmnnxy.com
muabyljiutasgqedl.com
mxgainbmtvariv.com
myhyfpuoh.com
myqenkelfk.com
nbkqygsfvri.com
nfbodxdevgpjba.com
nfqhufvxysyda.com
nglqogrh.com

nhcdrnwpsasnaar.com
nqgsmbkwvniifyost.com
nqnyteqxqgqohvco.com
ntikqcjtehpih.com
nvgmdyabspq.com
nwuqfobauwsyuppii.com
nxhdmugxeiht.com
nxlakdliamyuejsss.com
nxxuwtws.com
ocvqccdhenkjs.com
odcenmfimwibhrfvxy.com
oexdjxjdoiplmxfybbm.com
ogfavxwxus.com
ogmwrgryk.com
okfatclblpl.com
ootuujaep.com
optiidevdabtlewjd.com
otdvlbjeucwyqkfbn.com
ovhlfqcpfxoyjgjb.com
ovtindng.com
ovypjimjcnvwoiamj.com
owerubvhcinavarinm.com
oyuqibrjowbfmvj.com
oyxmxbsppuucbtium.com
pacffcnx.com
pbdlfskjrclqjo.com
pgnpuktbnmrybjsv.com
pgtujjyovgffyfrn.com
pnfnkahiocdseewyen.com
ppvrnfkbarbnlm.com
ptvaolhg.com
pxjjwmhlmptbsvhuq.com
qdboaveuhwabhwik.com
qglhlsyskvufb.com
qhnhlgmfepeuelxtpkv.com
qiisbgyqkrokokwrbq.com
qnyyirhtuautt.com
qprfvbstn.com
qtyvbditfgmkxqjrik.com
qvberjspofqsxdnr.com
qwmqyrcvkseyvrgdnv.com
qxqkdvwayhengiqm.com
qyuylvjwh.com
replinjqsbrnf.com
rgrtvwsalmhx.com
rijfxtotkuysyfh.com

rjbejalpcsgghdm.com
rmdmqetbpbpgpufhql.com
rmjkunxkbcsltbc.com
rrewytfucjjylju.com
rwcdlyemxplouufjvd.com
sblbtuqtiavvtrkrn.com
sbpvpuwoxevjjiy.com
scfxvdlmfbgf.com
sdjvmbngpgwnpdj.com
shnlojyteocltymxe.com
slvmktdpxdd.com
smisifkrfkyccnlk.com
snpryjitnos.com
strjkrxvkmkuql.com
srvmkdeaerccaffs.com
ssclrhiiifeodm.com
sthspflawbhacxp.com
tbajypaiecloxihf.com
tjslktadjklb.com
tnqtdfodepctna.com
todyennhm.com
twwrktawwgpito.com
typmylojdcxtdxd.com
ucfenxbryboqwbmlxke.com
udiivoyrbugyfruq.com
uehhvrdnuc.com
ugkrxtjrflfbxmakmt.com
uoidxmhugvidc.com
upnsdndflqokigybd.com
uuofllccd.com
uvkejdrigublbsst.com
vcssgidqhdkar.com
vdbtvdpujtfhwa.com
vefqerywsov.com
veymlvyoknk.com
vffamysgfsodw.com
vfrpojablkkqrx.com
vilapacdnnohdsehneh.com
vlglwuyqoxjn.com
vpwxxqwenvdrxpc.com
vrvfonqdkfjo.com
vwlcnujosuovul.com
wacwpqxq.com
wehtwbqu.com
wgvmlyfygec.com
wjpsxawqxomokepfbw.com

wknfjeopkdj.com
wldlrwlygck.com
wnftxxhnwiugtvwyo.com
wvmmvpbkjrds.com
wxkeojjdshd.com
wxnufbeacmrdam.com
xbjersli.com
xcpvexsyqjsf.com
xdtfqohfbskcgxameg.com
xdyowsheht.com
xirrlpllrccosqsf.com
xktepjxakoyq.com
xlqaburwns.com
xmlonthptunynnxf.com
xnttexmtc.com
xoqxabqb.com
xrtgqevawtlmulghjj.com
xsmypdmnacrqxkdb.com
xtbwxayxxvqpspo.com
xuajockq.com
ybgpdikdudmdfr.com
ycafyovxdnlsa.com
yemusvulvknobwhvp.com
yctgocejemh.com
yctkhjksne.com
ycvmwjae.com
ydgsadpgvne.com
yembvbgmdipfwjmd.com
yovkoaxsana.com
yoxbjnpgmkjirj.com
yxiiibnav.com
yxkhvhehtjfoqrmedi.com
yytbonkxjwy.com