

RECEIVED

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

2014 JUL 14 P 4: 54

CLERK OF DISTRICT COURT  
ALEXANDRIA, VIRGINIA

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

Plaintiffs,

v.

JOHN DOES 1-8, CONTROLLING A  
COMPUTER BOTNET THEREBY  
INJURING PLAINTIFFS, AND THEIR  
CUSTOMERS AND MEMBERS,

Defendants.

Civil Action No: 1:14cv811 LOG/TCB

**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 for a preliminary injunction 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 a preliminary injunction, 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 1-8 (“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 Microsoft is, 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 and exceeding authorization, in order to infect those computers and make them part of the computer botnet known as the “Shylock” botnet (the “botnet”);

- b. sending malicious code to configure, deploy and operate a botnet;
- c. generating and sending unsolicited messages through Microsoft's Skype application and service that falsely indicate they are from or approved by Microsoft;
- d. creating false websites that falsely indicate that they are associated with or approved by Plaintiffs or Plaintiffs' member organizations;
- e. using deceptive telephone numbers purporting to be associated with FS-ISAC's member organizations, in order to steal computer users' credentials;
- f. stealing personal and financial account information from computer users;
- g. using stolen information to steal money from the financial accounts of those users; and
- h. delivering malicious code.

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 and domain name servers listed in Appendix A and the Internet Protocol (IP) addresses listed in Appendix B, and from the destruction or concealment of other discoverable evidence of Defendants' misconduct available at those locations, if the injunctive relief sought by Plaintiffs is not granted. Based on the evidence cited in Plaintiffs' 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, IP Addresses, and name servers and/or to warn their associates engaged in such activities if the injunctive relief sought by Plaintiffs is not granted; and

7. Plaintiffs' request for this 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;

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 and domain name servers identified in Appendix A to this Order by directing malicious botnet code and content to said computers of Plaintiffs' customers and member organizations; and using the IP addresses identified in Appendix B to this Order that are registered to command and control servers located at hosting companies set forth in Appendix B, 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 computer networks of the Internet Service Providers (ISPs) identified in Appendix C to this Order that customers of Microsoft and FS-ISAC's members use to access the Internet, and the hosting companies and domain registries identified in Appendices A and B to this Order.

9. There is good cause to believe that Defendants have engaged in illegal activity by

using the networks of the ISPs identified in Appendix C and the hosting facilities and domain registration facilities of the companies in Appendices A and B, to deliver from the Internet domains, domain name servers, and IP Addresses identified in Appendices A and B, the malicious botnet code and content that Defendants use to maintain and operate the botnets to the computers of Plaintiffs' customers and member organizations.

10. There is good cause to believe that Defendants have engaged in illegal activity by using deceptive and fake telephone numbers specifically 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 and content from the Internet domains, the domain name servers, and the IP Addresses identified in Appendices A and B to computers of Plaintiffs' customers. There is good cause to believe that to immediately halt the injury caused by Defendants, Defendants must also be prohibited from sending or receiving telephone calls to steal computer users' credentials and continue their fraudulent conduct on Plaintiffs' customers and member organizations.

12. There is good cause to believe that Defendants have engaged in illegal activity using the Internet domains and domain name services identified in Appendix A to this Order 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 NS9.microsoftinternetsafety.net and NS10.microsoftinternetsafety.net and thus made inaccessible to Defendants.

13. There is good cause to believe that to immediately halt the injury caused by Defendants, the ISPs identified in Appendix C and the hosting companies identified in Appendix B should take reasonable steps to block incoming and/or outgoing traffic on their respective networks that originates or has been sent from and/or to the IP Addresses identified in Appendix B and the ".su" domains identified in Appendix A, such that said traffic will not reach

victim end-user computers on the ISPs' respective networks and/or the computers at the foregoing IP Addresses and domains.

14. There is good cause to believe that Defendants have engaged in illegal activity using the IP Addresses identified in Appendix B to host the command and control software and content used to maintain and operate the botnet. There is good cause to believe that in order to immediately halt the injury caused by Defendants and to ensure the future prosecution of this case it not rendered fruitless by attempts to delete, hide, conceal, or otherwise render inaccessible the software components that create, distribute, and are involved in the creation, perpetuation, and maintenance of the botnet and prevent the creation and distribution of unauthorized copies of the registered trademarks of Microsoft and FS-ISAC's member organizations and carry out other harmful conduct, with respect to the Defendants' most current, active command and control servers hosted at the IP Addresses, the following actions should be taken. The ISPs identified in Appendix C and the hosting companies identified in Appendix B should take reasonable steps to block incoming and/or outgoing traffic on their respective networks that originates or has been sent from and/or to the IP Addresses identified in Appendix B, such that said traffic will not reach victim end-user computers on the ISPs' respective networks and/or the computers at the IP Addresses in Appendix B, and should take other reasonable steps to block such traffic to and/or from any other IP addresses to which Defendants may move the botnet infrastructure, identified by Plaintiffs and which the Court may order to be subject to this Order, to ensure that Defendants cannot use such infrastructure to control the botnet.

15. There is good cause to believe that Defendants will attempt to update the Internet domains, domain name servers, and IP addresses associated with the Shylock Botnet, and that Plaintiffs may identify and update the domains and IP addresses to this Order as may be reasonably necessary to account for additional Internet domains, domain name servers, and IP addresses associated with the Shylock Botnet, as the case proceeds.

16. There is good cause to permit notice of the instant Order 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.

### **PRELIMINARY INJUNCTION**

**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) generating and sending unsolicited messages that falsely indicate said messages are from or approved by Microsoft or others; (4) creating false websites that falsely indicated that they are associated with or approved by Plaintiffs or Plaintiffs' member organizations; (5) 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, domain name servers, and IP addresses set forth herein and through any other component or element of the botnet in any location; (6) using deceptive telephone numbers purporting to be associated with Plaintiffs' member organizations in order to

steal computer users' credentials; (7) stealing information, money, or property from Plaintiffs, Plaintiffs' customers, or Plaintiffs' member organizations; (8) 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 (9) 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 Microsoft, 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 and domain name servers 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 NS9.microsoftinternetsafety.net and NS10.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.

**IT IS FURTHER ORDERED** that, with respect to the currently registered Internet domains and domain name servers set forth in Appendix A, the non-U.S. domain registries set forth at Appendix A are respectfully requested, but not ordered, to comply with the foregoing steps, in order to protect the integrity and security of the Internet, to protect the domain registries' own systems, to protect end-user victims of the botnet in all countries, to advance the public interest and to protect Plaintiffs and their customers and members from the botnet.

**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 NS9.microsoftinternetsafety.net and NS10.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 are put within Microsoft's control, and to ensure that Defendants cannot use them to control the botnet.

**IT IS FURTHER ORDERED** that, with respect to the currently unregistered Internet domains and domain name servers set forth in Appendix A, the non-U.S. domain registries set forth at Appendix A are respectfully requested, but not ordered, to comply with the foregoing steps, in order to protect the integrity and security of the Internet, to protect the domain registries' own systems, to protect end-user victims of the botnet in all countries, to advance the public interest and to protect Plaintiffs and their customers and members from the botnet.

**IT IS FURTHER ORDERED** that, with respect to any of the IP Addresses set forth in Appendix B to this Order and with respect to any of the ".su" domains set forth in Appendix A, the ISPs identified in Appendix D to this Order shall take reasonable best efforts to implement the following actions:

A. Without the need to create logs or other documentation, take reasonable steps to identify (1) incoming and/or outgoing Internet traffic on their respective networks that originates and/or is being sent from and/or to the IP Addresses identified in Appendix B and (2) incoming and/or outgoing Internet traffic on their respective networks that originates and/or is being sent from and/or to the ".su" domains identified in Appendix A, that is directed to and/or from computers that connect to the Internet through the ISPs' respective networks;

B. Take reasonable steps to block (1) incoming and/or outgoing Internet traffic on

their respective networks that originate and/or are being sent from and/or to the IP Addresses identified in Appendix B, and (2) incoming and/or outgoing Internet traffic on their respective networks that originates and/or is being sent from and/or to the “.su” domains identified in Appendix A, that is directed to and/or from computers that connect to the Internet through the ISPs’ respective networks;

C. Take other reasonable steps to block such traffic to and/or from any other IP addresses or domains to which Defendants may move the botnet infrastructure, identified by Microsoft in a supplemental request to this Order, to ensure that Defendants cannot use such infrastructure to control the botnet.

D. Not enable, and shall take reasonable steps to prevent, any circumvention of this order by Defendants, Defendants’ representatives or any other person;

E. Provide reasonable assistance in implementing the terms of this Order and take no action to frustrate the implementation of this Order;

**IT IS FURTHER ORDERED** that, with respect to the IP Addresses set forth in Appendix B and the “.su” domains identified in Appendix A, the non-U.S. ISPs set forth at Appendix C are respectfully requested, but not ordered, to comply with the foregoing steps, in order to protect the integrity and security of the Internet, to protect the domain registries’ own systems, to protect end-user victims of the botnet in all countries, to advance the public interest and to protect Plaintiffs and their customers and members from the botnet.

**IT IS FURTHER ORDERED** that, with respect to the IP Addresses in Appendix B, the hosting companies located in the United States shall take the following actions:

A. Take all reasonable steps necessary to completely block all access to and all traffic to and from the IP Addresses set forth in Appendix B by Defendants, Defendants’ representatives, resellers, and any other person or computer, except as explicitly provided for in this Order;

B. Completely disable the computers, servers, electronic data storage devices, software, data or media assigned to or otherwise associated with the IP Addresses set forth in

Appendix B and make them inaccessible from any other computer on the Internet, any internal network, or in any other manner, to Defendants, Defendants' representatives and all other persons, except as otherwise ordered herein;

C. Completely preserve the computers, servers, electronic data storage devices, software, data or media assigned to or otherwise associated with the IP Addresses set forth in Appendix B, and preserve all evidence of any kind related to the content, data, software or accounts associated with such IP addresses and such computer hardware, such that such evidence of Defendants' unlawful activities is preserved.

D. Completely, and until further order of this Court, suspend all services associated with the IP Addresses set forth in Appendix B;

E. Not enable, and shall take all reasonable steps to prevent, any circumvention of this order by Defendants or Defendants' representatives associated with the IP Addresses or any other person;

F. Log all attempts to connect to or communicate with the IP Addresses set forth in Appendix B;

G. Preserve, retain and produce to Plaintiffs all documents and information sufficient to identify and contact Defendants and Defendants' representatives operating or controlling the IP Addresses set forth in Appendix B, including any and all individual or entity names, mailing addresses, e-mail addresses, facsimile numbers and telephone numbers or similar contact information, including but not limited to such contact information reflected in billing, usage, access and contact records and all records, documents and logs associated with Defendants' or Defendants' Representatives' use of or access to the IP Addresses.

H. 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 explicitly provided for in this Order;

I. Transfer any content and software hosted at the IP Addresses listed in Appendix B that are not associated with Defendants, if any, to new IP Addresses not listed in Appendix B;

notify any non-party owners of such action and the new IP addresses, and direct them to contact Microsoft's counsel, Gabriel M. Ramsey, Orrick Herrington & Sutcliffe, 1000 Marsh Road, Menlo Park, CA 90425-1015, [gramsey@orrick.com](mailto:gramsey@orrick.com), (Tel: 650-614-7400), to facilitate any follow-on action;

J. Provide reasonable assistance in implementing the terms of this Order and take no action to frustrate the implementation of this Order.

**IT IS FURTHER ORDERED** that, with respect to the IP Addresses in Appendix B, the non-U.S. hosting companies set forth at Appendix B are respectfully requested, but not ordered, to comply with the foregoing steps, in order to protect the integrity and security of the Internet, to protect the hosting companies' own systems, to protect end-user victims of the botnet in all countries, to advance the public interest and to protect Plaintiffs and their customers and members from the botnet.

**IT IS FURTHER ORDERED** that copies of this Order 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.

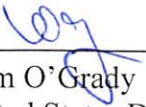
**IT IS FURTHER ORDERED** that Microsoft shall post bond in the amount of \$200,000 as cash to be paid into the Court registry.

**IT IS FURTHER ORDERED** that Plaintiffs may identify and update the domains and IP addresses to this Order as may be reasonably necessary to account for additional Internet domains, domain name servers, and IP addresses associated with the Shylock

Botnet, as this case proceeds.

**IT IS SO ORDERED**

Entered this 15<sup>th</sup> day of July, 2014.

  
\_\_\_\_\_  
Liam O'Grady  
United States District Judge

## **APPENDIX A**

### **.BIZ DOMAINS**

#### **Registry**

NeuStar, Inc.  
21575 Ridgetop Circle  
Sterling, VA 20166  
United States

NeuStar, Inc.  
Loudoun Tech Center  
46000 Center Oak Plaza  
Sterling Virginia 20166  
United States

#### **Hardcoded Domains**

fasttrackcrowlingss.biz  
fieldsocrossing.biz  
midjunelists.biz  
rotatingads.biz

#### **Configuration File Domains**

express-shippingus.biz  
modern-shipping.biz  
skylineinc-inc.biz  
topchoiceshippinginc.biz

#### **Money Mule Domains**

artable.biz  
brandnewshippinginc.biz  
bstrategic.biz  
business-shipping.biz  
capital-business-systems.biz  
client-spec-usa.biz  
consolidated-holdingsuk.biz  
dft-shipment.biz  
enterprise-holdingsuk.biz  
express-shippingus.biz  
fastlaneshipping.biz

financeconsulting-inc.biz  
finmurano.biz  
firstchoice-inc.biz  
first-consultansinc.biz  
flyhigh-inc.biz  
globalconnect-inc.biz  
global-holdings.biz  
global-techsolution.biz  
globeshippinginc.biz  
groupholdings-ltd.biz  
highland-holdingsltd.biz  
inn-technology.biz  
internetresources-us.biz  
interprolimited.biz  
inttechus.biz  
it-business-inc.biz  
itglobalserv-ltd.biz  
it-solutions-inc.biz  
jtsolutionsinc.biz  
leveauxgroupinc.biz  
mancapconsulting-ltd.biz  
modern-shipping.biz  
newlinesolutionsinc.biz  
new-source-unlimited.biz

new-york-finance.biz  
novatex-finanze.biz  
outsource-consultingus.biz  
outsourcemarketing-us.biz  
parcelzoneinc.biz  
partner-fingroup-inc.biz  
postexpressinc.biz  
primary-internationalltd.biz  
rexship-llc.biz  
sa-consulting.biz  
shiplandllc.biz  
shippinglineinc.biz  
skylineinc-inc.biz  
strout sourcing.biz  
topchoiceshippinginc.biz  
tradeglobe-ltd.biz  
usacapital-oneoutsourcing.biz  
usa-financial-trust.biz  
us-internationalgroup.biz  
usparcel service.biz  
wirelessgenerationinc.biz  
zonecapitalinc.biz

**.ORG DOMAINS**

**Registry**

**Public Interest Registry (PIR)**  
**1775 Wiehle Avenue**  
**Suite 200**  
**Reston Virginia 20190**  
**United States**

**Hardcoded Domains**

expressshipping.org  
durationuninstaller.org  
sterchelloness.org

**Configuration File Domains**

ac-shippingllc.org

**Money Mule Domains**

ac-shippingllc.org  
artcolors-ltd.org  
art-for-anyone.org  
baltic-shippingexpress.org  
expressshipping.org  
fbf-services.org  
feature-solutionuk.org  
finance-counts-uk.org  
fintechin-program.org  
horwardexpress-shipping.org

interpride-ltd.org  
it-campaign.org  
king-inntech.org  
premier-group-ltd.org  
stock-holderz-uk.org  
transaction-innovations.org  
uk-accessgroup.org  
ukpower-ltd.org  
usparcelservice.org



**.COM, .NET, .CC DOMAINS****Registry**

**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**

**Hardcoded Domains**

|                    |                 |                  |
|--------------------|-----------------|------------------|
| abp.cc             | edal.cc         | mch.cc           |
| acow.cc            | eewuiwiu.cc     | mkn.cc           |
| ac-shippingllc.com | eilahcha.cc     | mny.cc           |
| adix.cc            | elg.cc          | mwr.cc           |
| adra.cc            | enp.cc          | nafe.cc          |
| afn.cc             | e-protection.cc | nbh.cc           |
| agra.cc            | erp-cloud.cc    | nel.cc           |
| ahthuvuz.cc        | estat.cc        | nitecapvideo.net |
| aingo.cc           | eux.cc          | nmbc.cc          |
| ajo.cc             | eym.cc          | ognelisblog.net  |
| akf.cc             | fiq.cc          | omp.cc           |
| alphard-info.net   | fooyuo.cc       | onei.cc          |
| ambi.cc            | gah.cc          | online-upd.net   |
| amia.cc            | gdm.cc          | oonucoog.cc      |
| asale.cc           | giuchito.cc     | oras.cc          |
| avar.cc            | gmz.cc          | orx.cc           |
| bgx.cc             | goc.cc          | paly.cc          |
| big-web-svcs.cc    | guodeira.cc     | pare.cc          |
| bo0keego.cc        | gva.cc          | perahzoo.cc      |
| bogs.cc            | iestats.cc      | pfh.cc           |
| cene.cc            | ihl.cc          | pmr.cc           |
| ciz.cc             | ioh.cc          | puv.cc           |
| ckr.cc             | irm.cc          | rgf.cc           |
| coob.cc            | isohotel.net    | rgk.cc           |
| coti.cc            | jeo.cc          | rhk.cc           |
| cuapoemi.cc        | jub.cc          | rwn.cc           |
| cutes.cc           | kico.cc         | sags.cc          |
| cvl.cc             | kinz.cc         | smis.cc          |
| deit.cc            | kirr.cc         | soks.cc          |
| deloxnerviox.net   | kity.cc         | solt.cc          |
| doks.cc            | kls.cc          | sorg.cc          |
| drg.cc             | kre.cc          | sted.cc          |
| duti.cc            | lej.cc          | tohk5ja.cc       |
| dvo.cc             | liem.cc         | tram.cc          |
| dza.cc             | lji.cc          | uab.cc           |
|                    | mbn.cc          | ubd.cc           |

uceebeerl.cc  
 updbrowser.com  
 uvo.cc  
 vbp.cc  
 veeceefi.cc  
 visite-mexico.net  
 wahemah.cc  
 wownthing.cc  
 coob.cc  
 stik.cc  
 buna.cc

### **Configuration File Domains**

express-shippingus.net  
 flyhigh-inc.net  
 rexship-llc.net  
 skylineinc-inc.net  
 solutionsshippinginc.com  
 topchoicesshippinginc.net  
 useushippinginc.com

### **Plug-in Domains**

agy.cc  
 envy-svcs.cc  
 fooyuo.cc  
 hoks.cc  
 ohyeaah.cc  
 safety-for-all.cc

### **Money Mule Domains**

1st-consultansinc.net  
 ac-shippingllc.com  
 adestaventurez.com  
 advanced-techinc.cc  
 aiwae.cc  
 aiwae.com  
 aiwae.net  
 artable-ltd.com  
 artable-uk.net  
 artcolors-ltd.com  
 artcolors-ltd.net  
 art-yard-uk.com  
 avid-techresources.cc  
 avid-techresources.com  
 avid-techresources.net  
 baltic-shippingexpress.com  
 bestway-solutions.com  
 bestway-solutions.net  
 bidei.cc  
 brandnewshippinginc.net

businesschoicellc.net  
 business-shipping.net  
 capitalbusiness-systems.com  
 chahuz.com  
 client-specusa-inc.net  
 consolidated-holdingsuk.net  
 cyndirocks.com  
 dft-shipment.net  
 enterprise-holdingsuk.com  
 enterprise-holdingsuk.net  
 enterprisetechinc.com  
 enterprisetechinc.net  
 equitytech-partners.cc  
 equity-techpartners.com  
 equitytech-partners.net  
 eshipperus.com  
 express-shippingus.net  
 fastlaneshipping.net  
 fbf-services.net  
 finacial-futures.net  
 financeconsultinginc.net  
 financeheads.com  
 fincounts-ltd.com  
 finmarintltd.cc  
 finmarint-ltd.net  
 finmurano.com  
 finmurano.net  
 fintechin-program.com  
 fintech-inprogram.net  
 fin-trustinc.com  
 firstchoice-inc.net  
 first-consultansinc-usa.com  
 flyhigh-inc.net  
 global-techsolution.net  
 globalus-united.net  
 globeshippinginc.net  
 groupholdings-ltd.com  
 groupholdings-ltd.net  
 guojo.cc  
 highland-holdings-ltd.net  
 infotech-xpert.com  
 inn-technology.com  
 inn-technology.net  
 internetresources-us.com  
 interpride-ltd.com  
 interpride-ltd.net  
 interprofinance.com  
 inttechus.com  
 it-alliance-ltd.com  
 it-business-inc.net

it-genies.net  
 it-genies-limited.com  
 itglobalserv-ltd.com  
 itglobalserv-ltd.net  
 itg-solutions-ltd.com  
 itg-solutions-uk.net  
 it-investmentgrouppllc.com  
 it-made-easy-limited.com  
 it-made-easy-ltd.net  
 it-merge-ltd.com  
 itprofessionals-group.com  
 it-smart-uk.com  
 it-solutions-inc.net  
 jtsolutionsinc.net  
 king-innovative.com  
 king-innovative.net  
 labbarra-holdings.com  
 legalgeneralgroup-plc.com  
 leibi.cc  
 liverinvestments-ltd.com  
 liverinvestments-ltd.net  
 mabcomuk.com  
 mancapconsultingltd.com  
 mancapconsulting-ltd.com  
 meridian-international.net  
 meridianus-inc.com  
 modern-shipping.net  
 neopro-inc.com  
 neopro-inc.net  
 newlinesolutionsinc.net  
 new-source-unlimited.net  
 newyork-finance.net  
 novatex-finanze.com  
 novatex-finanze.net  
 nycfinanceinc.com  
 onlineshippinginc.net  
 originalconsultinginc.com  
 originalconsultinginc.net  
 outsource-consultingus.com  
 outsource-consultingus.net  
 outsource-marketing-us.com  
 outsourcemarketing-us.net  
 paradigmcore.net  
 parcelzoneinc.net  
 partner-financialgroup.com  
 personaltouch-us.com  
 personaltouch-us.net  
 postexpressinc.net  
 premier-group-ltd.com  
 primary-internationalltd.net

rexship-llc.net  
 rickolexpressshipping.com  
 sabi-consulting.com  
 sa-consulting.cc  
 shiplandllc.net  
 shippinglineinc.net  
 shippingxtrainc.com  
 shippingxtrainc.net  
 shoph.cc  
 sky-edgeitsolutions.cc  
 sky-edgeitsolutions.com  
 sky-edgeitsolutions.net  
 skylineinc-inc.net  
 solutionsshippinginc.com  
 solutionsshippinginc.net  
 stockholderzzz.com  
 strategic-inc.net  
 stroutsourcing.com  
 stroutsourcing.net  
 systems-and-communications.com  
 systems-and-communications.net  
 technology-inc.net  
 topchoicesshippinginc.net  
 tradeglobe-ltd.com  
 tradeglobe-ltd.net  
 transaction-innovations.net  
 uk-accessgroup.com  
 uk-accessgroup.net  
 ukfeature-solutions.com  
 uk-financecounts.net  
 ukglobal-holdings.com  
 ukglobal-holdings.net  
 uk-infotech-xpert.net  
 uk-ns-free.cc  
 ukpower-ltd.com  
 uk-stock-holderz.net  
 united-technologiesusa.com  
 united-technologiesusa.net  
 usa-capital-one-outsourcing.com  
 usa-countrywide-financial.net  
 usa-financialtrust.net  
 usa-zonecapital.com  
 us-capital-business.net  
 useushippinginc.com  
 useushippinginc.net  
 us-internationalgroup.com

usstrategic-inc.com  
 vale-usshipping.com  
 wirelessgenerationinc.net  
 xohze.cc  
 xohze.com  
 zone-capital-usa.net

**Dedicated Name Server**

**Domains**

abp.cc  
 adestaventurez.com  
 adix.cc  
 agra.cc  
 agy.cc  
 aiwae.cc  
 aiwae.com  
 aiwae.net  
 ajo.cc  
 akf.cc  
 alax.cc  
 alphard-info.net  
 ambi.cc  
 avar.cc  
 bara.cc  
 bestmanta.net  
 bidei.cc  
 bogs.cc  
 buna.cc  
 cas-gallery.net  
 ckr.cc  
 clickmonopoly.net  
 clickmonopoly.net  
 coob.cc  
 cude.cc  
 deloxnerviox.net  
 drg.cc  
 dvo.cc  
 dza.cc  
 edal.cc  
 elg.cc  
 eym.cc  
 fiq.cc  
 freg.cc  
 gah.cc  
 gdm.cc  
 goc.cc  
 hoks.cc  
 ihl.cc  
 isohotel.net

kico.cc  
 kls.cc  
 lanegovonline.net  
 lavo.cc  
 lej.cc  
 librarymdp.com  
 liem.cc  
 liveathcr.net  
 macdegredo.com  
 mahe.cc  
 mch.cc  
 merand.cc  
 micatoge.net  
 mikemanser.net  
 mkn.cc  
 mny.cc  
 mwr.cc  
 nafe.cc  
 nbh.cc  
 nintendowiionline.net  
 nitecapvideo.net  
 ognelisblog.net  
 omp.cc  
 onei.cc  
 oras.cc  
 orx.cc  
 paradigmcore.net  
 pare.cc  
 pikeautomation.net  
 prai.cc  
 puppy.cc  
 rgf.cc  
 rhk.cc  
 slac.cc  
 sted.cc  
 stik.cc  
 tram.cc  
 trendei.net  
 uab.cc  
 uvo.cc  
 veso.cc  
 visite-mexico.net  
 webercountyfairr.net  
 xidungee.cc  
 xohze.cc  
 xohze.com  
 zoneoffsilence.com  
 xidungee.cc

## **.SU DOMAINS**

### **Registry**

#### **Технический Центр Интернет**

Ул. Зоологическая д.8  
123242, Москва  
Российская Федерация  
тел.: 737 92 95  
факс: 737 06 84  
e-mail: [ru-tech@tcinet.ru](mailto:ru-tech@tcinet.ru)

#### **Technical Center of Internet**

Technical Center of Internet  
8, Zoologicheskaya str  
Moscow 123242  
Russian Federation  
Tel: +7 495 737 92 95  
Fax: +7 495 737 06 84  
e-mail: [ru-tech@tcinet.ru](mailto:ru-tech@tcinet.ru)

### **RIPN/РосНИИРОС**

Алексей Платонов  
Академика Курчатова пл., д. 1  
123182, Москва  
Российская Федерация  
тел.: 196 9614  
факс: 196 4984  
e-mail: [adm@ripn.net](mailto:adm@ripn.net), [su-adm@fid.su](mailto:su-adm@fid.su)

### **RIPN/Russian Institute for Development of Public Networks (ROSNIROS)**

Dr. Alexei Platonov  
1, Kurchatov Sq.  
Moscow 123182  
Russian Federation  
Tel: +7 499 196 9614, +7 499 196 7278  
Fax: +7 499 196 4984  
e-mail: [adm@ripn.net](mailto:adm@ripn.net), [su-adm@fid.su](mailto:su-adm@fid.su)

### **Hardcoded Domains**

aisuvied.su  
bern.su  
caf.su  
eca.su  
eprotect.su  
feat.su  
grs.su  
igate.su  
iprotect.su  
klr.su  
lbb.su  
sito.su  
tco.su  
vng.su  
wand.su

### **Plug-in Domains**

apb.su  
axr.su  
cif.su  
egu.su  
gasu.su

### **Money Mule Domains**

jan.su  
tech-support-llc.su

### **Dedicated Name Server**

#### **Domains**

azr.su  
bcv.su  
cdn-store.su  
eimiecha.su

greencloud.su  
maw.su  
mue.su  
ohy.su  
rnz.su  
strong-service.su  
teighoos.su  
vun.su  
wbx.su  
wyp.su  
yiequeih.su  
yimgscores.su  
ahbee.su  
ajeic.su  
choop.su  
tagoo.su

**APPENDIX B****IP ADDRESSES**

| <b>IP Addresses</b>   | <b>Hosting Companies</b>  |
|---|---|
| 103.254.139.250   | <p>Dreamscape Networks Pty Ltd.<br/> 8 Howlett Street<br/> North Perth, Western Australia 6006<br/> Australia<br/> Phone: +61 8 9422 0808<br/> Fax: +61 8 9422 0808<br/> <a href="mailto:abuse@dreamscapenetworks.com">abuse@dreamscapenetworks.com</a><br/> <a href="mailto:abuse@syrahost.com">abuse@syrahost.com</a><br/> <a href="mailto:phishing@syrahost.com">phishing@syrahost.com</a></p> <p>Aust Domains International Pty Ltd.<br/> PO Box 3333<br/> Perth, Western Australia 6832<br/> Australia<br/> <a href="mailto:help@austdomains.com.au">help@austdomains.com.au</a><br/> <a href="mailto:customercare@austdomains.com.au">customercare@austdomains.com.au</a><br/> Phone: +61 (08) 9422 0888<br/> Fax: +61 (08) 9422 0889</p> |
| 88.198.57.178<br>85.10.192.137<br>88.198.6.90<br>85.10.192.156<br>46.4.189.188<br>46.4.47.20<br>88.198.52.109<br>88.198.6.88<br>88.198.6.91<br>46.4.47.22 | <p>Hetzner Online AG<br/> Stuttgarter Strasse 1<br/> D-91710 Gunzenhausen<br/> Germany</p> <p>Hetzner Online AG<br/> Industriestrasse 25<br/> 91710 Gunzenhausen<br/> Germany</p> <p>Phone: +49 9831 61 00 61<br/> Fax: +49 9831 61 00 62<br/> <a href="mailto:abuse@hetzner.de">abuse@hetzner.de</a><br/> <a href="mailto:info@hetzner.de">info@hetzner.de</a></p>   |
| 69.64.55.162<br>199.189.87.71<br>50.30.47.104   | <p>Hosting Solutions International, Inc.<br/> 210 North Tucker Blvd., Suite 910<br/> Saint Louis, MO 63101</p> <p>Hosting Solutions International, Inc.</p>   |

| IP Addresses   | Hosting Companies   |
|--|---|
|  | <p>Jeffrey H. Pass<br/>710 N Tucker Blvd. Ste. 610<br/>Saint Louis, MO 63101</p> <p><a href="mailto:abuse@hostingsolutionsinternational.com">abuse@hostingsolutionsinternational.com</a><br/> <a href="mailto:s.wintz@hostingsolutionsinternational.com">s.wintz@hostingsolutionsinternational.com</a><br/> Phone: +1-314-480-6840<br/> Phone: +1-314-266-3638</p> <p>Timoney Sinitsin<br/>Wienerbergstrasse 11-070<br/>Wien, 1100<br/>Austria</p> <p>Sinitsin, Timoney Vladimirovich<br/>Phone: +43.720.883321<br/> <a href="mailto:abuse@multiservers.eu">abuse@multiservers.eu</a></p> |
| 80.86.88.144<br>188.138.10.29<br>188.138.10.30<br>188.138.91.23<br>62.75.235.244<br>80.86.88.145 | intergenia AG / BSB Service GmbH / NMC PlusServer AG<br>Daimlerstr. 9-11<br>50354 Huerth<br>Phone: +49 2233 612-0, +49 1801 119991<br>Fax: +49 2233 612-144, +49 2233 612-53500<br><a href="mailto:abuse@plussserver.de">abuse@plussserver.de</a><br><a href="mailto:abuse@ip-pool.com">abuse@ip-pool.com</a>   |
| 85.17.175.101<br>46.165.225.8<br>46.165.250.206<br>46.165.250.244<br>85.17.175.83                | LeaseWeb Netherlands B.V.<br>Luttenbergweg 8<br>1101 EC Amsterdam<br>The Netherlands<br>Phone: +31 20 316 2880<br>Fax: +31 20 3162890<br><a href="mailto:abuse@leaseweb.com">abuse@leaseweb.com</a> <p>LeaseWeb<br/> P.O. Box 93054<br/> 1090BB Amsterdam<br/> The Netherlands</p>  |
| 91.121.180.145<br>87.98.140.188<br>91.121.199.45<br>178.33.152.199                               | OVH SAS<br>2 rue Kellermann<br>59100 Roubaix<br>France<br>Phone: +33 9 74 53 13 23<br><a href="mailto:abuse@ovh.net">abuse@ovh.net</a>  |

| IP Addresses   | Hosting Companies  |
|--|--|
| 37.220.22.212<br>80.84.56.2<br>5.152.195.74<br>5.152.196.186<br>5.152.196.188<br>5.152.196.189<br>88.150.208.122<br>80.84.56.3<br>80.84.56.5 | Redstation Limited<br>2 Frater Gate Business Park<br>Aerodrome Road<br>Gosport<br>Hampshire<br>PO13 0GW<br>United Kingdom<br><a href="mailto:abuse@redstation.com">abuse@redstation.com</a>  |
| 192.3.20.89  | ColoCrossing<br>8469 Sheridan Drive<br>Williamsville, NY 14221<br><a href="mailto:abuse@colocrossing.com">abuse@colocrossing.com</a><br><a href="mailto:support@colocrossing.com">support@colocrossing.com</a><br><a href="mailto:avial@colocrossing.com">avial@colocrossing.com</a><br><br>Ethernet Servers<br>19 Bennetts Hill<br>Sidmouth<br>Devon EX109XH<br>United Kingdom<br>Phone: +44.7811233318<br><a href="mailto:george@ethernetServers.com">george@ethernetServers.com</a> |
| 189.206.56.114   | 66260 – San Pedro Garza Garcia – NL<br>Mexico<br><br>Ave. Eugenio Clariond Garza, 175, Cuauhtemoc<br>66450 - San Nicolas de los Garza - NL<br>Mexico<br>Phone: +52 81 87486201 [6201]<br><a href="mailto:inetadmin@alestra.net.mx">inetadmin@alestra.net.mx</a>  |

APPENDIX C

| No. | Internet Service Provider          | Contact Information  |
|-----|------------------------------------|--|
| 1.  | Century Link                       | <p>Attn: Legal Dept.<br/> 100 CenturyLink Dr.<br/> P.O. Box 4065<br/> Monroe, LA 71203<br/> (318) 388-9000<br/> <a href="mailto:abuse@centurylink.com">abuse@centurylink.com</a></p> <p>CT Corporation System<br/> 5615 Corporate Blvd. Ste 400B<br/> Baton Rouge, LA 70808-2536</p>   |
| 2.  | Comcast Cable Communications, Inc. | <p>Attn: Legal Dept.<br/> Comcast Center<br/> 1701 JFK Blvd.<br/> Philadelphia, PA 19103<br/> <a href="mailto:abuse@comcast.net">abuse@comcast.net</a></p> <p>C T Corporation System<br/> 116 Pine Street<br/> Suite 320<br/> Harrisburg, PA 17101<br/> Phone: 717-234-6</p>   |
| 3.  | Cox Communications, Inc.           | <p>Attn: Legal Dept.<br/> 6205 Peachtree Dunwoody Road<br/> Atlanta, GA 30328<br/> 1400 Lake Hearn Drive<br/> Atlanta, GA 30319<br/> <a href="mailto:cei_cis_dns_admin@cox.com">cei_cis_dns_admin@cox.com</a><br/> <a href="mailto:abuse@cox.net">abuse@cox.net</a></p> <p>Corporation Service Company<br/> 40 Technology Pkway South, #300<br/> Norcross, GA 30092</p> <p>Corporation Service Company<br/> 2711 Centerville Rd. Ste 400<br/> Wilmington, DE 19808</p> |
| 4.  | Time Warner Cable                  | <p>Attn: Legal Dept.<br/> Time Warner Cable, Inc.<br/> 60 Columbus Cir. Fl. 17<br/> New York, NY 10023</p>   |



| No. | Internet Service Provider | Contact Information   |
|-----|---------------------------|---|
|     |                           | <p>(212) 364-8200<br/> <a href="mailto:abuse@twcable.com">abuse@twcable.com</a><br/> <a href="mailto:abuse@rr.com">abuse@rr.com</a></p> <p>The Corporation Trust Company<br/> Corporation Trust Center<br/> 1209 Orange St.<br/> Wilmington, DE 19801</p> <p>Time Warner Cable Inc.<br/> C T Corporation System<br/> 111 Eighth Avenue<br/> New York, NY 10011</p>  |
| 5.  | Verizon                   | <p>Attn: Legal Dept.<br/> Attn: Timothy Vogel<br/> 1095 Ave. of Americas<br/> New York, NY 10036<br/> Fax: (325) 949-6916<br/> <a href="mailto:abuse@verizon.com">abuse@verizon.com</a><br/> <a href="mailto:domainlegalcontact@verizon.com">domainlegalcontact@verizon.com</a><br/> <a href="mailto:timothy.vogel@verizon.com">timothy.vogel@verizon.com</a></p> <p>The Corporation Trust Company<br/> Corporation Trust Center<br/> 1209 Orange St.<br/> Wilmington, DE 19801</p> |