

**IN THE CIRCUIT COURT OF THE TWENTIETH JUDICIAL CIRCUIT  
ST. CLAIR COUNTY, ILLINOIS  
LAW DIVISION**

PEG LEG PRODUCTIONS, LLC,

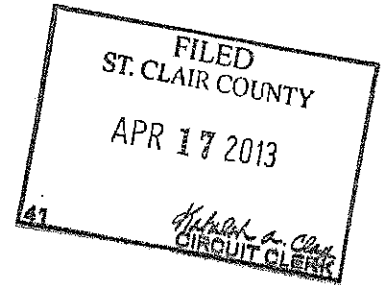
Petitioner,

v.

CHARTER COMMUNICATIONS, LLC,

Respondent.

No. 13 MR 142



**PETITION FOR DISCOVERY BEFORE SUIT TO IDENTIFY RESPONSIBLE  
PERSONS AND ENTITIES**

1. Petitioner Peg Leg Productions, LLC, through its undersigned attorney, hereby petitions this Court for entry of an Order requiring Respondent Charter Communications, LLC ("Charter") to provide the identifying information of the subscribers associated with the Internet Protocol ("IP") addresses listed on Exhibit A attached hereto, and in support thereof, states as follows:

**NATURE OF THE ACTION**

2. Petitioner brings this petition pursuant to Illinois Supreme Court Rule 224 to identify unidentified John Does ("Does") so that Petitioner may file an action for computer fraud and abuse, computer tampering, and civil conspiracy against them.

**THE PARTIES**

3. Petitioner is a limited liability company formed under the laws of the State of Delaware with its principal place of business in St. Clair County, Illinois. Petitioner's computer systems are accessible in St. Clair County, Illinois.

4. Respondent Charter is an Internet Service Provider ("ISP") that provides Internet services to the Does that Petitioner seeks to identify. Does are known to Petitioner solely by an

Internet Protocol ("IP") address given to Does by Charter. An IP address is a unique number that is assigned to Internet users by an ISP at a given date and time.

5. Charter records the time and date that it assigns an IP address to a subscriber and maintains in logs for a period of time a record of the assignment. Charter also maintains records which typically include the name, one or more addresses, one or more telephone numbers, and one or more e-mail addresses of the subscriber. However, these records are not public and are not available to Petitioner at this time. Charter is the only entity that can link the Does' IP address to the Does' true identities.

### **JURISDICTION AND VENUE**

6. Pursuant to 134 Ill. 2d R. 224 "[t]he action for discovery shall be initiated by the filing of a verified petition in the circuit court of the county in which the action or proceeding might be brought or in which one or more of the persons or entities from whom discovery is sought resides." Respondent Charter resides in this county and transacts business in this county. Further, some or all of the Does reside in this county, committed acts in this county and directed unlawful activity towards this county.

7. This Court has subject matter jurisdiction over this matter because a petition for pre-suit discovery falls within the exclusive original jurisdiction of the Circuit Court. Ill. Const., Art. VI, § 9; 134 Ill. 2d R. 224; *see also Shutes v. Fowler*, 584 N.E.2d 920, 923 (Ill. App. Ct. 1991) ("Rule 224 is constitutional and confers subject-matter jurisdiction on the circuit court.")

### **BACKGROUND**

8. Petitioner operates a private "members only" website that delivers content to paying members. Petitioner does not own the copyrights in the content it distributes. Instead, Petitioner licenses content from third-parties.

9. A core concern for website operators, such as Petitioner, is computer security. Petitioner's computers are its key business assets. They deliver content to Petitioner's paying customers. Without properly functioning computers, Petitioner's business cannot function.

10. Petitioner faces an epidemic that threatens the very nature and livelihood of its business. Petitioner's computer systems are targeted by unauthorized individuals on a daily basis. The efforts of these individuals result in considerable damage to Petitioner's computer systems and business reputation, and Petitioner is forced to spend considerable resources in responding to these attacks.

11. Computer crimes have become a serious threat to anyone maintaining private or protected computer systems. *See* Michael Mimoso, *Cybercrime Gang Recruiting Botmasters for Large-Scale MiTM Attacks on American Banks*, THE THREAT POST, Oct. 4, 2012, attached hereto as Exhibit B (explaining that "[a]s many as 30 banks have been targeted" recently by cyber hackers.); Bryon Acohido, *No Slowdown in Sight for Cyberattacks*, USA TODAY, July 30, 2012, attached hereto as Exhibit C (Eddie Schwartz, chief security officer of security firm RSA stating that "[i]t's easier and safer for a criminal to steal money from an online bank account, rather than have to walk into a bank — or to steal intellectual property in an online setting, rather than have to send in a human spy.").

12. Even large corporations and governmental agencies are not immune from hacking attacks. *See* Kim Zetter, *Hackers Release 1 Million Apple Device IDs Allegedly Stolen From FBI Laptop*, WIRED, Sept. 4, 2012, attached hereto as Exhibit D (explaining that a hacker group obtained "1 million Apple device IDs that" were "obtained from an FBI computer they hacked.").

13. The courts have an important role to play in discouraging computer misuse. *See* Glenn Chapman, *Cyber Defenders Urges to go on the Offense*, AMERICAN FREE PRESS, July 26, 2012, attached hereto as Exhibit E (former FBI cyber crime unit chief Shawn Henry explaining that “I believe the threat from computer network attack is the most significant threat we face as a civilized world, other than a weapon of mass destruction.” and Black Hat founder Jeff Moss proposing that “cyber attackers also be fought on legal fronts, with companies taking suspected culprits to court.”).

14. Even the United States government is taking important steps to protect itself against cyberattacks. *See* Mark Mazzetti and David E. Sanger, *Security Leader Says U.S. Would Retaliate Against Cyberattacks*, THE NEW YORK TIMES, March 12, 2013, attached hereto as Exhibit F (“the nation’s top intelligence official, James R. Clapper Jr., warned Congress that a major cyberattack on the United States could cripple the country’s infrastructure and economy. and suggested that such attacks now pose the most dangerous immediate threat to the United States, even more pressing than an attack by global terrorist networks.”).

### FACTUAL ALLEGATIONS

15. Petitioner’s computer systems are secured by user authentication systems. Individuals seeking to legitimately access Petitioner’s computer systems must possess valid username and password credentials. These credentials are not publicly available. Petitioner did not provide Does with credentials to its computer or access to the content thereon.

16. The unknown Does in this case belong to hacking community where hacked usernames and passwords are passed back and forth so the members can gain unauthorized access to computer systems and websites they would not normally be able to access. Once the Does gained unauthorized access to Petitioner’s computer system they were able to gain access

to Petitioner's and Petitioner's clients' private information. Petitioner wants to file an action for computer fraud and abuse, computer tampering, and civil conspiracy against these Does in order to protect itself from these attacks.

17. Does agreed to assist one another in gaining unauthorized access to Petitioner's computer systems and then share with one another the information stored on those systems. Does agreed with one another to collaborate in gaining unauthorized access to Petitioner's computer systems and to distribute the information stored on Petitioner's computer systems amongst one another. Specifically, on information and belief Does shared information about vulnerabilities in Petitioner's computer systems, encouraged one another on Internet chat rooms to proceed with breaching Petitioner's computer systems, and then collaborated to distribute the information they secured from Petitioner's computer systems.

18. Petitioner does not know the identities of the unknown Does, but does know their IP addresses. Petitioner used publicly available reverse-lookup databases on the Internet to determine that Charter is the ISP that provided the IP addresses to the Does listed in Exhibit A.

19. Petitioner anticipates filing an action for computer fraud and abuse, computer tampering, and civil conspiracy against the Does once they are identified.

#### **A. Computer Fraud And Abuse**

20. The allegations contained in the preceding paragraphs are hereby re-alleged as if fully set forth herein.

21. Petitioner owns and operates computer systems that distribute licensed content. Petitioner generates revenue by requiring third-parties to pay a fee for accessing its systems. Members are assigned a username and password in order to access the system.

22. The Does obtained usernames and passwords from a website that allows its members to trade stolen usernames and passwords amongst one another. The Does used the stolen usernames and passwords to intentionally gain unauthorized access to Petitioner's protected computer systems. Once they gained unauthorized access to Petitioner's protected computer systems, they permitted others to do the same.

23. The Does accessed Petitioner's computer systems as though they were paying members. The Does became privy to private information, including information regarding the identities of Petitioner's customers, account information, financial information, and computer programs and security information.

24. Since Does accessed the website through a hacked password, they are not required to provide any identifying personal information, such as their true names, addresses, telephone numbers or email addresses. Does can only be identified by their IP addresses.

25. The individuals committing these unlawful activities are identified by their IP addresses as well as the dates and times they unlawfully accessed Petitioner's computer systems. This information is set forth in Exhibit A.

26. Petitioner used publicly available reverse-lookup databases on the Internet to determine what ISP issued the IP address. The Does Petitioner seeks to identify through this petition are all subscribers of Charter.

27. Petitioner has suffered a loss due to the Does' fraud and abuse of Petitioner's computer systems in excess of \$250,000. The loss to Petitioner includes, but is not limited to, 1) costs associated with detecting the unauthorized breaches and identifying the IP addresses of those associated, 2) costs associated with restoring its computer systems to their condition prior

to the breach of its computer systems and preventing future breaches, and 3) lost revenue and costs incurred due to interruption of computer service.

28. Petitioner has been damaged due to the Does' fraud and abuse of Petitioner's computer systems in excess of \$250,000. The damage to Petitioner includes, but is not limited to, 1) harm to its business reputation, and 2) impairment to Petitioner's computer systems made by changes to the systems caused by the Does and their hacking programs.

29. The above alleged facts support a claim of computer fraud and abuse by Petitioner against the Does under 18 U.S.C. § 1030.<sup>1</sup>

#### **B. Computer Tampering**

30. The allegations contained in the preceding paragraphs are hereby re-alleged as if fully set forth herein.

31. The Does knowingly, and without the authorization of Petitioner, inserted hacking computer programs into Petitioner's computer systems that allowed them to gain access to the private computer systems. The Does' computer programs altered Petitioner's computer systems by disabling its security protocols.

32. Once the Does gained unauthorized access, they knowingly, and without the authorization of Petitioner, obtained data and services as though they were paying members.

33. Petitioner has suffered a loss due to the Does unauthorized tampering of Petitioner's computer systems in excess of \$250,000. The loss to Petitioner includes, but is not limited to, 1) costs associated with detecting the unauthorized breaches and identifying the IP addresses of those associated, 2) costs associated with restoring its computer systems to their

---

<sup>1</sup> A private right of action exists under the Act under 18 U.S.C. § 1030(g).

condition prior to the breach of its computer systems and preventing future breaches, and 3) lost revenue and costs incurred due to interruption of service.

34. The above alleged facts support a claim of Computer Tampering under 720 ILCS 5 § 16D-3.<sup>2</sup>

### **C. Civil Conspiracy**

35. The allegations contained in the preceding paragraphs are hereby re-alleged as if fully set forth herein.

36. The Does colluded with one another and other members of a hacking community to gain unauthorized access to Petitioner's protected computer systems. The hacking community's members shared hacked usernames and passwords among other members to ensure that they had access to Petitioner's protected computer systems.

37. The Does reached an agreement with their fellow co-conspirators to gain unlawful access to Petitioner's computer systems and gain access to private and protected information. The Does were aware that the hacked usernames and passwords they used did not belong to them and that they did not have Petitioner's permission to access its computer systems and electronic communications.

38. The Does committed overt tortious and unlawful acts by using hacked usernames and passwords to impermissibly obtain access to Petitioner's protected computer systems and electronic communications.

39. As a proximate result of this conspiracy, Petitioner has been damaged, as is more fully alleged above.

---

<sup>2</sup> A private right of action exists under the Statute under 720 ILCS 5 § 16D-3(c).



## **PRE-SUIT DISCOVERY**

40. The allegations contained in the preceding paragraphs are hereby re-alleged as if fully set forth herein.

41. Each Doe used one or more hacked passwords to gain unauthorized access to Petitioner's protected computer systems in direct violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, and Computer Tampering, 720 ILCS 5 § 16D-3.

42. The above alleged facts support claims of computer fraud and abuse, computer tampering, and civil conspiracy by Petitioner against the Does. Petitioner will be an actual party, and not merely a witness or other third party to the claims brought against the Does.

43. Petitioner does not know the Does' true identities. Each of the Does' true identities is known only to each Doe and by Charter, to which each Doe subscribes.

44. Petitioner seeks the name, address, telephone number, email address, MAC address and any other form of information that may be used to identify the Does. Petitioner is interested in and entitled to this information so that Petitioner may bring claims of computer fraud and abuse, computer tampering, and civil conspiracy against the Does in this county.

45. Petitioner has a right to the relief sought in order to identify the unknown Does, which is a condition precedent to Petitioner filing an action against the Does, who will be defendants.

46. The discovery sought is material to Petitioner's anticipated actions at law.

**WHEREFORE**, Petitioner respectfully requests that the Court enter a judgment:

(A) Entering an Order requiring Charter to turn over the following identifying information of the subscribers associated with the IP addresses listed on Exhibit A, attached hereto:

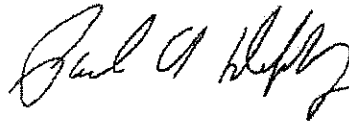
- True Name;
- Address;
- Telephone Number;
- E-mail Address; and
- Media Access Control Address.

(B) Granting Petitioner further relief as this Court deems just and proper.

Respectfully submitted,

Peg Leg Productions, LLC

DATED: April 15, 2013



By:

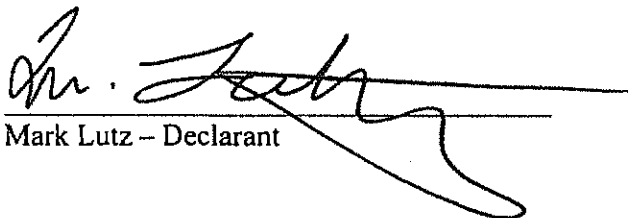
---

Paul A. Duffy, Esq. (Bar No. 6210496)  
 2 N. LaSalle Street  
 13th Floor  
 Chicago, IL 60602  
 312-476-7645  
*Attorney for Petitioner*

Kevin T. Hoerner, #6196686  
 Becker, Paulson, Hoerner & Thompson, P.C.  
 5111 West Main Street  
 Belleville, IL 62226  
 (618) 235-0020  
*Attorney for Petitioner*


### VERIFICATION

Under penalties of perjury as provided by law pursuant to section 1-109 of the code of civil procedure, the undersigned certifies that the statements set forth in this instrument are true and correct, except as to matters herein stated to be on information and belief and as to such matters the undersigned certifies as aforesaid that the undersigned verily believe the same to be true.

  
Mark Lutz – Declarant

SUBSCRIBED and SWORN TO

Before Me This 12th day of April, 2013.

  
\_\_\_\_\_  
Notary Public



**RAUL L. CHAVARRA**  
MY COMMISSION # EE 173519  
EXPIRES: March 6, 2016  
Bonded Through Budget Notary Services

# EXHIBIT A

IP Address	Date/Time (UTC)
75.133.94.42	2013-03-13 03:07:09
24.107.216.125	2013-03-19 23:47:30
68.185.197.201	2013-03-17 09:46:27
75.138.236.245	2013-03-20 13:58:42
96.37.158.177	2013-03-16 02:59:20
71.86.99.27	2013-03-14 00:27:39
66.168.108.230	2013-03-04 18:55:26
24.151.140.196	2013-03-22 01:11:24
24.196.238.86	2013-03-12 02:10:12
75.143.152.47	2013-03-11 02:19:32
97.94.210.121	2013-03-18 22:50:19
66.169.6.8	2013-03-12 13:23:12
75.130.106.77	2013-03-13 19:20:07
75.141.101.69	2013-03-07 12:03:55
75.138.106.96	2013-03-22 15:42:45
71.84.45.190	2013-03-01 15:11:13
24.158.114.25	2013-03-20 06:50:47
68.119.148.129	2013-03-22 15:44:08
71.8.75.42	2013-03-12 04:05:29
71.81.177.240	2013-03-22 05:50:43
71.84.171.167	2013-03-13 19:38:52
24.151.197.103	2013-03-16 05:00:30
97.89.25.0	2013-03-12 00:51:47
24.205.10.159	2013-03-18 21:42:30
68.114.1.162	2013-03-14 22:30:27
71.13.17.143	2013-03-16 04:54:37
75.131.46.137	2013-03-14 00:27:45
24.241.54.245	2013-03-19 11:14:10
24.151.142.73	2013-03-11 03:10:56
71.87.151.224	2013-03-20 06:41:09
75.136.162.213	2013-03-22 09:46:27
75.135.192.204	2013-03-04 03:24:42
24.236.217.107	2013-03-11 04:53:46
71.90.208.202	2013-03-05 01:41:16
71.93.165.74	2013-03-03 02:21:34
68.190.19.53	2013-03-15 10:08:20
97.94.113.195	2013-03-22 05:29:00
68.187.116.46	2013-03-07 01:29:35
66.191.221.86	2013-03-02 21:17:45
75.141.134.181	2013-03-07 11:52:27
24.205.183.38	2013-03-17 01:35:36
75.128.60.91	2013-03-13 23:56:59
68.191.132.183	2013-03-21 15:11:27
71.94.167.60	2013-03-19 07:10:54
24.176.137.211	2013-03-09 15:38:04
71.91.72.187	2013-03-18 05:27:50

68.112.186.168	2013-03-20 08:42:59
75.137.250.16	2013-03-01 06:52:24
71.83.240.189	2013-03-18 21:42:55
68.186.65.70	2013-03-13 15:04:42
68.118.39.240	2013-03-19 08:47:04
68.184.118.70	2013-03-10 21:26:24
96.37.244.228	2013-03-19 23:47:39
71.91.41.149	2013-03-05 21:00:05
97.92.120.94	2013-03-11 04:34:08
97.95.36.104	2013-03-02 22:50:36
75.131.195.85	2013-03-15 03:23:27
71.85.228.141	2013-03-04 21:38:17
24.197.243.103	2013-03-18 23:57:59
71.9.123.57	2013-03-02 09:18:18
71.85.2.53	2013-03-19 02:04:09
75.131.195.247	2013-03-14 01:25:54
66.188.46.228	2013-03-18 01:42:22
75.137.113.245	2013-03-04 18:23:39
75.142.110.4	2013-03-11 08:38:27
97.88.156.186	2013-03-15 08:32:12
24.205.91.8	2013-03-22 00:46:30
24.231.221.13	2013-03-10 01:02:43
68.113.99.166	2013-03-01 21:11:38
24.236.139.3	2013-03-22 07:03:40
97.85.41.86	2013-03-13 07:25:00
71.80.155.73	2013-03-18 02:59:56
96.39.32.238	2013-03-15 05:15:35
71.91.189.134	2013-03-20 16:21:51
68.116.85.69	2013-03-02 13:55:52
66.215.218.179	2013-03-04 06:11:21
24.107.128.195	2013-03-17 04:51:39
75.142.238.249	2013-03-13 05:32:32
75.134.90.191	2013-03-18 16:19:05
71.95.156.37	2013-03-20 04:33:48
24.183.92.115	2013-03-21 15:44:42
97.94.101.25	2013-03-20 01:34:01
24.205.234.140	2013-03-03 20:41:32
24.247.116.158	2013-03-04 02:34:02
24.205.241.110	2013-03-19 04:43:44
24.151.81.25	2013-03-17 23:46:30
97.81.89.254	2013-03-20 05:08:31
97.81.67.234	2013-03-17 07:35:43
75.142.242.234	2013-03-17 01:34:20
75.128.131.210	2013-03-15 06:48:45
24.182.224.12	2013-03-15 05:16:19
66.189.28.39	2013-03-22 12:45:05
96.41.27.122	2013-03-15 16:11:51

75.134.188.218	2013-03-22 09:29:01
71.92.86.62	2013-03-19 06:28:26
24.107.165.5	2013-03-04 03:52:04
97.93.77.186	2013-03-19 05:36:05
71.80.45.120	2013-03-17 02:25:23
66.168.75.172	2013-03-15 22:59:30
97.87.139.128	2013-03-11 08:03:54
66.215.252.250	2013-03-20 16:21:36
24.181.28.192	2013-03-18 08:11:30
71.82.46.147	2013-03-19 22:03:23
68.114.52.216	2013-03-15 10:19:18
96.41.83.126	2013-03-02 09:57:07
24.240.23.18	2013-03-15 15:16:40
71.83.122.248	2013-03-19 14:17:42
97.85.176.189	2013-03-07 00:47:24
75.140.109.91	2013-03-10 22:04:31
75.136.113.211	2013-03-12 21:35:21
97.92.199.9	2013-03-15 19:41:00
71.92.209.124	2013-03-04 21:15:10
68.189.219.128	2013-03-01 01:59:11
75.130.103.253	2013-03-04 09:44:28
24.217.142.108	2013-03-07 04:26:08
24.196.173.25	2013-03-19 03:28:33
75.135.0.103	2013-03-17 22:27:26
96.38.169.68	2013-03-17 02:44:00
68.191.209.210	2013-03-19 00:11:49
97.83.201.204	2013-03-22 07:21:05
68.118.7.248	2013-03-12 09:09:50
97.88.198.142	2013-03-02 01:22:23
68.185.69.36	2013-03-20 06:41:14
68.117.195.4	2013-03-03 23:25:17
24.196.36.189	2013-03-19 19:00:20
68.114.137.12	2013-03-19 09:51:29
71.11.25.161	2013-03-16 23:49:22
75.134.50.54	2013-03-04 16:56:45
24.240.21.192	2013-03-10 21:43:21
68.186.138.33	2013-03-22 12:58:57
71.14.18.196	2013-03-20 13:42:07
71.84.16.93	2013-03-22 15:43:15
97.82.134.144	2013-03-17 04:10:14
75.138.62.6	2013-03-11 07:20:24
24.178.72.188	2013-03-20 15:34:56
24.247.217.209	2013-03-01 01:16:59
71.93.107.207	2013-03-19 04:15:52
97.92.48.86	2013-03-02 08:39:46
71.82.167.9	2013-03-22 03:46:52
97.81.96.83	2013-03-19 01:00:51

71.89.147.3	2013-03-19 16:25:56
24.180.184.18	2013-03-10 06:19:49
24.176.131.46	2013-03-21 23:06:44
68.190.233.245	2013-03-15 08:31:45
66.190.49.201	2013-03-14 21:44:09
24.247.173.190	2013-03-17 03:39:36
68.119.33.13	2013-03-18 20:21:12
24.197.10.26	2013-03-03 14:33:15
24.183.93.1	2013-03-12 05:42:39
71.94.244.58	2013-03-20 12:21:59
68.184.96.132	2013-03-20 16:50:16
97.94.103.84	2013-03-05 01:57:56
75.136.36.90	2013-03-19 00:48:54
24.247.118.100	2013-03-13 06:34:49
66.189.64.40	2013-03-22 06:37:24
66.227.160.54	2013-03-14 22:53:38
96.35.125.84	2013-03-19 01:00:41
75.138.113.224	2013-03-20 14:55:17
75.134.204.135	2013-03-15 17:36:25
71.88.200.138	2013-03-10 09:22:03
68.117.41.84	2013-03-12 10:47:37
75.138.201.41	2013-03-05 01:40:00
24.159.8.201	2013-03-14 21:50:11
66.191.23.28	2013-03-01 00:49:14
24.247.184.255	2013-03-20 16:25:44
68.114.212.115	2013-03-06 22:26:33
24.183.139.87	2013-03-18 17:07:39
68.185.120.123	2013-03-20 05:08:34
71.93.186.228	2013-03-12 18:11:55
97.90.187.101	2013-03-20 16:09:56
96.35.20.42	2013-03-22 10:57:20
97.94.183.170	2013-03-22 14:59:58
75.141.99.132	2013-03-02 20:49:53
24.205.138.215	2013-03-05 00:35:10
71.93.42.87	2013-03-19 04:29:36
24.176.172.52	2013-03-20 06:34:22
71.91.78.48	2013-03-20 07:03:00
68.185.197.65	2013-03-14 19:10:57
75.134.135.229	2013-03-10 04:20:58
96.36.134.142	2013-03-12 09:51:58
96.40.133.199	2013-03-07 01:15:14
71.94.245.242	2013-03-19 23:47:38
24.171.56.233	2013-03-07 02:58:19
71.89.110.250	2013-03-11 07:08:42
71.95.102.78	2013-03-22 07:56:49
97.80.125.125	2013-03-10 00:46:11
96.38.128.122	2013-03-19 19:25:53



68.189.187.148	2013-03-03 05:36:12
75.136.121.189	2013-03-02 15:47:57
24.241.228.142	2013-03-13 03:27:29
24.176.73.93	2013-03-04 14:48:19
75.142.78.187	2013-03-05 06:16:59
24.176.21.94	2013-03-15 17:54:09
68.186.211.101	2013-03-07 10:17:50
71.85.51.17	2013-03-20 02:54:42
24.231.170.53	2013-03-05 00:52:53
71.93.229.96	2013-03-19 17:02:50
71.83.170.233	2013-03-17 08:36:42
97.83.130.172	2013-03-21 14:33:27
75.134.3.53	2013-03-12 02:09:21
68.114.242.248	2013-03-19 01:17:58
75.131.228.183	2013-03-11 06:55:47
96.32.30.182	2013-03-01 17:37:38
66.169.76.246	2013-03-04 03:28:11
97.91.154.158	2013-03-14 00:26:13
24.176.144.234	2013-03-05 00:44:17
71.83.229.226	2013-03-17 23:05:09
68.186.161.249	2013-03-20 15:34:01
68.190.155.174	2013-03-01 03:18:59
68.186.13.253	2013-03-22 01:11:23
24.197.53.97	2013-03-22 04:18:56
75.142.236.152	2013-03-14 19:32:27
97.82.248.138	2013-03-12 02:09:20
68.186.111.66	2013-03-14 05:53:57
75.137.125.34	2013-03-11 09:41:44
71.9.36.154	2013-03-13 00:27:32
71.80.9.122	2013-03-03 06:10:06
66.188.248.162	2013-03-20 16:49:19
24.205.146.159	2013-03-01 07:54:29
71.9.192.182	2013-03-14 19:54:28
68.185.225.118	2013-03-12 21:34:53
66.168.40.69	2013-03-04 09:06:22
71.95.102.221	2013-03-05 02:20:40
75.143.172.241	2013-03-11 08:44:17
71.84.33.183	2013-03-05 04:41:13
173.46.240.74	2013-03-11 12:31:22
66.214.234.154	2013-03-17 07:46:29
71.95.41.147	2013-03-16 05:26:18
97.92.3.146	2013-03-14 09:34:23
75.140.80.54	2013-03-12 06:41:04
24.182.234.141	2013-03-01 20:07:49
96.36.131.93	2013-03-17 06:57:02
75.128.195.196	2013-03-10 18:58:24
96.35.90.111	2013-03-21 23:23:58

97.94.100.45	2013-03-22 05:26:11
24.231.249.196	2013-03-02 02:11:43
24.151.44.62	2013-03-18 23:25:53
68.184.50.141	2013-03-07 08:46:55
24.158.86.218	2013-03-08 17:00:15
24.179.54.90	2013-03-09 22:22:33
96.41.52.79	2013-03-22 15:00:11
68.112.68.254	2013-03-14 02:10:29
68.186.201.166	2013-03-10 08:12:15
71.8.87.22	2013-03-03 19:51:25
75.131.167.88	2013-03-20 14:38:48
71.92.86.209	2013-03-13 13:24:52
24.205.252.186	2013-03-18 01:39:55
96.42.16.79	2013-03-02 12:25:26
68.119.137.48	2013-03-04 20:14:05
68.116.110.165	2013-03-20 14:47:20
96.37.202.208	2013-03-20 11:31:46
75.141.141.135	2013-03-02 11:56:28
24.176.85.186	2013-02-28 23:15:21
24.183.4.204	2013-03-03 04:50:49
24.217.129.78	2013-03-14 15:45:40
24.158.38.35	2013-03-02 22:00:24
24.181.132.227	2013-03-17 10:18:48
71.85.198.16	2013-03-07 12:26:20
75.142.112.112	2013-03-07 09:18:51
71.81.52.157	2013-03-17 22:07:28
97.93.123.111	2013-03-13 01:04:31
68.186.76.248	2013-03-01 00:06:04
68.184.60.75	2013-03-04 18:10:21
24.51.35.38	2013-03-18 19:45:05
71.87.50.247	2013-03-01 09:37:16
24.236.214.186	2013-03-14 23:45:41
71.84.20.202	2013-03-13 16:51:50
24.241.228.189	2013-03-10 14:16:22
71.83.181.234	2013-03-15 13:01:33
24.107.102.100	2013-03-03 03:07:32
68.185.146.159	2013-03-18 16:55:18
71.93.167.109	2013-03-17 01:15:32
24.177.13.147	2013-03-18 17:22:17
24.159.255.163	2013-03-13 19:39:41
71.8.206.216	2013-03-14 22:07:26
68.119.70.183	2013-03-01 04:51:35
66.214.19.56	2013-03-10 01:36:52
96.36.131.62	2013-03-17 15:22:05
68.185.136.208	2013-03-13 16:34:47
66.169.86.27	2013-03-15 05:36:45
96.32.56.149	2013-03-04 08:31:37

71.88.241.34	2013-03-13 00:03:32
71.85.218.66	2013-03-09 20:33:03
68.189.56.148	2013-03-07 16:31:50
96.40.163.18	2013-03-14 14:52:38
71.83.108.68	2013-03-20 16:59:40
71.94.7.230	2013-03-04 03:10:42
75.139.72.20	2013-03-09 22:49:33
75.130.215.163	2013-03-18 13:27:15
97.83.30.193	2013-03-15 08:31:45
75.141.253.132	2013-03-14 08:30:22
71.86.161.192	2013-03-15 03:45:39
75.135.220.132	2013-03-01 08:33:54
75.141.216.236	2013-03-21 21:51:22
97.88.16.248	2013-03-14 05:35:39
75.136.116.184	2013-03-04 21:02:00
96.39.145.133	2013-03-15 03:05:42
68.113.179.64	2013-03-18 20:00:13
24.231.246.173	2013-03-03 18:55:23
75.141.251.30	2013-03-20 10:44:05
68.187.210.150	2013-03-16 05:50:16
24.196.202.159	2013-03-19 04:57:00
96.37.67.236	2013-03-02 00:10:58
96.42.201.102	2013-03-22 00:53:01
24.183.239.2	2013-03-17 17:18:36
97.95.249.5	2013-03-09 11:52:39
66.191.45.9	2013-03-01 17:54:23
71.87.240.144	2013-03-13 17:21:55
24.217.101.74	2013-03-09 22:29:32
71.81.177.70	2013-03-01 01:03:57
24.107.5.246	2013-03-05 07:29:55
68.112.135.216	2013-03-22 04:18:59
71.92.240.166	2013-03-15 09:04:51
66.214.179.49	2013-03-17 07:17:46
24.183.217.66	2013-03-19 22:48:54
24.183.199.27	2013-03-01 07:35:16
68.186.130.108	2013-03-17 00:33:06
24.182.187.206	2013-03-18 23:57:55
75.142.217.211	2013-03-21 23:30:58
97.80.98.88	2013-03-18 03:33:56
71.91.77.197	2013-03-08 14:07:15
24.180.118.89	2013-03-02 07:51:34
66.189.105.21	2013-03-10 01:35:16
24.151.247.106	2013-03-09 20:00:22
97.85.54.233	2013-03-18 20:01:06
24.247.95.140	2013-03-11 01:57:48
68.114.52.175	2013-03-19 22:49:12
96.35.42.189	2013-03-10 20:37:53

96.32.141.194	2013-03-09 16:11:39
97.95.187.2	2013-03-03 03:21:54
96.35.116.186	2013-03-05 06:57:13
96.36.146.97	2013-03-13 13:13:16
96.32.144.75	2013-03-15 14:28:04
96.38.144.162	2013-03-19 04:28:54
97.90.132.176	2013-03-19 14:34:54
96.41.146.4	2013-03-04 02:13:59
24.181.27.127	2013-03-07 00:24:16
68.190.170.2	2013-03-07 12:27:31
71.12.234.36	2013-03-07 03:52:22
68.112.101.144	2013-03-12 00:31:41
68.189.50.9	2013-03-15 04:55:23
71.94.26.69	2013-03-19 20:20:45
68.117.105.108	2013-03-18 02:15:40
75.140.77.41	2013-03-09 23:01:45
24.217.85.67	2013-03-05 01:15:21
96.39.235.79	2013-03-19 15:24:16
71.14.43.17	2013-03-15 18:40:47
71.84.106.213	2013-03-20 07:30:04
68.185.114.37	2013-03-11 06:38:08
75.136.24.59	2013-03-16 02:20:23
97.90.224.76	2013-03-10 05:02:47
71.84.115.123	2013-03-02 00:17:09
71.10.75.15	2013-03-08 17:32:26
71.82.223.225	2013-03-16 04:08:20
75.142.153.214	2013-03-02 09:27:11
75.142.121.136	2013-03-05 11:50:39
75.137.99.69	2013-03-20 15:42:09
68.119.4.208	2013-03-10 02:23:11
71.82.66.185	2013-03-03 00:52:33
97.83.128.43	2013-03-05 10:01:04
66.169.86.240	2013-03-05 22:31:12
71.83.226.98	2013-03-18 03:16:03
66.227.134.57	2013-03-10 13:16:37
97.87.97.43	2013-03-22 08:54:11
75.132.160.191	2013-03-01 22:21:15
24.176.144.185	2013-03-12 11:06:08
75.139.153.105	2013-03-05 15:02:59
24.217.97.30	2013-03-18 14:18:33
24.181.166.36	2013-03-21 15:42:51
24.205.182.144	2013-03-12 21:03:29
24.196.236.205	2013-03-10 05:13:23
24.205.40.121	2013-03-12 23:07:29
71.83.184.16	2013-03-19 13:56:59
68.189.36.219	2013-03-17 09:55:01
75.131.32.72	2013-03-20 16:22:46

75.141.210.53	2013-03-03 07:12:24
68.190.183.175	2013-03-13 03:40:52
75.131.129.210	2013-03-22 15:50:05
71.8.200.226	2013-03-16 00:02:01
75.143.160.216	2013-03-19 18:39:37
24.176.18.221	2013-03-12 23:20:55
24.151.164.1	2013-03-18 14:42:02
24.151.17.92	2013-03-02 21:19:05
68.190.163.155	2013-03-16 23:24:06
75.134.188.62	2013-03-20 16:32:40
71.94.7.148	2013-03-13 08:31:02
96.40.141.253	2013-03-17 10:49:38
71.93.122.116	2013-03-10 04:50:01
68.191.215.72	2013-03-19 05:11:15
97.86.8.2	2013-03-02 21:46:28
75.143.126.69	2013-03-15 12:30:09
66.188.148.88	2013-03-14 14:53:56
97.89.29.253	2013-03-17 04:41:45
66.191.225.216	2013-03-19 07:11:54
71.11.169.237	2013-03-14 22:30:14
71.81.34.90	2013-03-11 08:17:40
71.94.175.98	2013-03-15 06:48:41
97.82.234.3	2013-03-20 11:42:16
24.151.165.7	2013-03-10 02:55:37
75.135.93.245	2013-03-13 14:07:55
96.32.56.164	2013-03-16 01:59:21
66.169.224.238	2013-03-22 11:32:24
97.89.102.156	2013-03-14 02:49:30
96.37.229.169	2013-03-15 00:22:27
75.138.61.204	2013-03-18 06:27:52
68.116.185.136	2013-03-19 10:04:23
75.135.46.94	2013-03-12 09:06:38
75.143.169.32	2013-03-19 09:55:12
75.138.8.13	2013-03-19 03:49:34
97.85.128.65	2013-03-01 23:35:12
97.94.129.100	2013-03-19 18:03:15
96.37.232.6	2013-03-09 14:56:16
68.186.77.139	2013-03-17 10:24:35
71.90.13.208	2013-03-07 16:43:33
71.92.96.206	2013-03-20 03:14:45
24.231.220.114	2013-03-12 01:52:30
24.176.3.232	2013-03-04 02:30:03
97.92.132.14	2013-03-11 03:57:33
24.236.139.204	2013-03-09 12:54:49
71.82.12.118	2013-03-17 14:19:43
97.92.4.229	2013-03-12 19:04:42
75.139.103.127	2013-03-06 19:45:19

97.89.70.8	2013-03-18 09:47:22
97.82.224.218	2013-03-16 22:46:32
96.42.243.66	2013-03-17 07:11:10
68.116.170.74	2013-03-12 05:01:46
75.138.26.174	2013-03-22 07:56:25
24.241.198.82	2013-03-07 19:02:38
75.131.88.201	2013-03-12 20:32:17
96.37.21.129	2013-03-17 11:31:17
97.84.10.177	2013-03-21 23:23:23
24.158.166.239	2013-03-17 17:57:43
24.151.68.208	2013-03-14 02:10:39
75.143.228.128	2013-03-22 04:17:46
66.190.199.110	2013-03-04 19:38:28
71.94.245.38	2013-03-11 05:29:41
75.136.121.63	2013-03-13 23:55:04
71.8.145.204	2013-03-08 20:25:04
24.183.100.230	2013-03-18 02:44:54
66.214.161.165	2013-03-14 13:10:28
71.93.81.209	2013-03-09 19:44:47
68.188.248.100	2013-03-13 17:42:39
96.36.131.44	2013-03-04 05:19:59
75.137.16.235	2013-03-03 11:20:35
71.94.228.134	2013-03-11 10:15:10
71.8.80.151	2013-03-17 04:32:21
24.179.205.157	2013-03-14 17:44:08
68.188.218.170	2013-03-13 01:54:39
24.183.94.245	2013-03-18 10:34:17
97.91.226.147	2013-03-20 04:21:23
97.81.252.118	2013-03-03 14:51:48
24.182.20.53	2013-03-22 11:00:21
75.131.215.55	2013-03-01 22:49:07
68.185.243.168	2013-03-20 16:41:25
97.80.242.183	2013-03-05 05:27:14
96.32.135.98	2013-03-20 13:19:03
97.90.118.145	2013-03-22 12:45:04
24.183.157.225	2013-03-21 22:02:18
24.241.20.155	2013-03-22 04:25:15
68.117.58.25	2013-03-17 04:41:21
97.83.207.90	2013-03-09 20:32:08
24.158.202.105	2013-03-18 01:58:02
66.188.248.82	2013-03-20 16:39:50
97.88.145.27	2013-03-05 09:20:38
24.107.213.150	2013-03-16 07:57:53
71.9.19.156	2013-03-12 21:42:17
75.139.146.164	2013-03-05 05:17:50
71.81.60.228	2013-03-13 19:01:21
71.92.161.143	2013-03-13 06:43:10

75.141.98.178	2013-03-12 13:57:01
96.37.206.27	2013-03-18 01:22:59
24.107.227.103	2013-03-07 09:24:55
71.83.241.216	2013-03-15 14:57:28
96.35.218.2	2013-03-01 07:11:19
66.191.58.134	2013-03-17 08:13:30
96.37.213.26	2013-03-19 08:01:39
75.128.97.108	2013-03-14 20:33:27
97.86.246.84	2013-03-14 02:26:29
71.88.52.165	2013-03-03 19:52:10
24.205.179.254	2013-03-20 12:38:44
24.177.220.70	2013-03-19 20:20:06
75.132.35.203	2013-03-03 20:06:06
66.191.203.218	2013-03-07 01:55:17
96.42.195.0	2013-03-19 01:01:35
97.93.26.55	2013-03-15 08:31:22
66.188.66.148	2013-03-18 20:26:53
71.85.193.220	2013-03-12 03:14:47
24.241.246.127	2013-03-01 02:36:11
75.137.120.189	2013-03-06 23:12:19
96.41.230.247	2013-03-10 04:21:43
96.35.90.51	2013-03-19 11:33:53
75.131.199.71	2013-03-12 02:08:49
71.84.123.85	2013-03-14 06:25:56
24.197.193.59	2013-03-12 19:52:58
24.158.53.229	2013-03-07 02:29:20
66.169.242.204	2013-03-04 04:48:33
24.241.115.208	2013-03-04 10:28:54
66.188.180.12	2013-03-21 23:07:17
24.183.220.33	2013-03-10 18:58:40
71.12.245.181	2013-03-10 09:11:32
24.158.71.176	2013-03-18 22:01:04
24.177.224.203	2013-03-22 15:42:45
24.180.131.219	2013-03-15 17:19:47
24.217.64.199	2013-03-18 10:52:36
68.191.179.50	2013-03-19 13:04:50
75.131.226.88	2013-03-05 12:15:07
71.82.219.80	2013-03-22 00:12:16
75.128.112.24	2013-03-17 15:27:26
71.80.117.140	2013-03-17 04:32:23
75.141.192.120	2013-03-22 15:42:55
96.40.234.129	2013-03-06 22:31:07
96.35.203.221	2013-03-05 07:44:02
97.91.231.19	2013-03-18 00:18:00
68.191.48.42	2013-03-11 00:33:31
66.215.205.153	2013-03-09 18:46:43
71.8.0.143	2013-03-02 08:01:23

24.158.219.238	2013-03-19 04:29:10
71.80.220.41	2013-03-22 07:57:32
75.138.182.249	2013-03-17 17:54:03
66.214.98.13	2013-03-12 06:40:56
24.158.69.25	2013-03-16 07:01:54
75.143.72.129	2013-03-11 00:53:29
68.118.68.162	2013-03-11 06:50:17
24.236.249.235	2013-03-20 07:27:52
68.118.230.147	2013-03-05 03:16:29
71.11.22.91	2013-03-11 12:13:16
71.95.145.204	2013-03-02 00:08:16
66.169.167.17	2013-03-12 02:09:28
75.131.140.54	2013-03-19 10:22:26
75.138.61.243	2013-03-15 21:52:36
68.186.164.216	2013-03-04 10:37:06
71.80.232.164	2013-03-16 06:18:30
96.40.132.179	2013-03-12 05:46:52
97.95.233.186	2013-03-17 05:11:01
97.94.235.142	2013-03-22 08:53:10
97.82.201.106	2013-03-12 13:55:48
68.116.197.94	2013-03-04 03:22:24
71.10.19.156	2013-03-09 17:05:43
97.93.122.69	2013-03-22 01:50:10
75.142.136.58	2013-03-20 08:43:11
96.33.144.242	2013-03-14 14:35:41
68.118.217.244	2013-03-10 13:11:22
96.32.69.207	2013-03-09 12:53:37
97.93.248.165	2013-03-14 14:52:09
71.9.65.205	2013-03-14 22:06:26
68.118.79.65	2013-03-13 08:29:33
96.41.146.19	2013-03-17 04:02:43
66.190.254.240	2013-03-11 15:10:32
97.81.196.195	2013-03-12 23:17:05
68.118.2.237	2013-03-22 09:44:54
75.142.76.95	2013-03-13 07:46:30
75.128.72.64	2013-03-02 03:58:00
97.81.29.177	2013-03-01 06:02:23
71.80.232.243	2013-03-13 11:30:20
71.81.33.165	2013-03-14 08:30:41
68.186.54.63	2013-03-21 22:41:22
71.10.115.95	2013-03-14 13:42:42
71.95.133.221	2013-03-17 02:41:05
75.128.217.23	2013-03-13 02:35:33
75.132.148.222	2013-03-03 08:54:39
75.136.42.249	2013-03-13 01:33:07
68.115.78.216	2013-03-22 07:44:42
68.119.12.209	2013-03-18 06:39:27



24.196.20.139	2013-03-02 07:06:47
96.41.105.58	2013-03-22 13:35:06
96.42.153.220	2013-03-10 11:32:11
71.91.190.224	2013-03-20 06:51:44
75.140.84.49	2013-03-19 16:46:02
24.182.231.154	2013-03-06 19:46:55
71.11.234.181	2013-03-02 04:30:59
68.191.63.186	2013-03-02 00:54:51
66.214.60.190	2013-03-12 16:39:29
68.187.43.104	2013-03-22 04:34:13
66.227.134.0	2013-03-20 17:01:02
75.128.64.46	2013-03-15 10:03:34
68.184.168.19	2013-03-09 18:27:21
97.90.93.129	2013-03-18 18:30:00
66.215.216.111	2013-03-13 05:26:28
68.115.22.156	2013-03-01 17:52:51
24.196.40.48	2013-03-01 04:27:21
71.95.122.132	2013-03-09 11:49:01
66.189.116.149	2013-03-12 07:34:53
66.191.17.210	2013-03-22 06:26:35
68.184.240.237	2013-03-20 14:08:10
66.227.164.181	2013-03-17 19:30:30
71.88.9.100	2013-03-11 01:14:11
68.112.149.12	2013-03-15 18:40:46
71.11.146.2	2013-03-06 21:37:16
68.184.31.204	2013-03-01 09:44:18
66.169.130.59	2013-02-28 22:55:29
96.40.147.112	2013-03-22 04:17:24
96.39.148.13	2013-03-16 07:13:24
24.207.129.140	2013-03-19 21:59:44
71.80.58.196	2013-03-09 20:48:30
75.129.149.39	2013-03-17 07:00:14
96.40.152.92	2013-03-18 20:00:42
75.142.234.98	2013-03-20 02:38:14
71.92.162.47	2013-03-19 09:32:11
68.118.38.102	2013-03-17 10:16:52
96.36.147.209	2013-03-17 06:34:13
66.169.33.20	2013-03-05 21:36:21
97.93.16.194	2013-03-18 03:59:51
68.190.55.19	2013-03-07 10:41:57
24.205.171.30	2013-03-02 09:57:14
96.32.10.49	2013-03-07 18:05:41
71.94.156.235	2013-03-19 07:50:31
24.183.165.24	2013-03-16 03:39:02
75.130.122.109	2013-03-11 05:35:51
68.119.35.29	2013-03-05 07:33:54
96.38.128.141	2013-03-11 09:53:25

97.84.168.187	2013-03-16 19:56:16
24.51.35.144	2013-03-12 00:32:00
71.81.5.85	2013-03-18 09:06:46
68.190.229.216	2013-03-07 03:15:55
24.182.200.8	2013-03-14 01:23:29
75.137.104.101	2013-03-19 16:09:34
66.189.237.239	2013-03-19 02:43:06
75.134.85.78	2013-03-18 07:27:17
75.138.41.7	2013-03-19 08:38:25
75.143.169.187	2013-03-14 18:13:09
66.191.24.161	2013-03-06 20:53:38
75.137.25.81	2013-03-12 06:05:04
71.89.92.213	2013-03-15 01:22:59
71.87.106.65	2013-03-07 05:21:36
71.92.218.159	2013-03-20 12:36:11
97.88.170.223	2013-03-05 20:43:53
97.89.148.15	2013-03-19 18:03:07
75.142.97.188	2013-03-06 04:03:24
97.92.152.51	2013-03-21 22:49:12
66.188.154.247	2013-03-18 16:16:20
66.214.76.114	2013-03-16 23:49:18
97.91.201.231	2013-03-03 09:51:33
96.38.154.138	2013-03-16 02:53:33
71.9.55.249	2013-03-12 03:14:59
97.92.200.173	2013-03-18 19:39:34
24.217.44.190	2013-03-15 14:09:36
68.115.90.119	2013-03-04 02:53:30
97.92.155.105	2013-03-15 13:25:50
75.137.255.111	2013-03-15 18:58:02
66.214.175.25	2013-03-15 04:21:01
71.15.38.76	2013-03-02 08:06:27
75.139.211.175	2013-03-03 07:30:04
68.185.66.70	2013-03-11 15:30:43
71.15.31.130	2013-03-15 22:29:00
71.12.170.74	2013-03-18 05:14:19
68.117.76.151	2013-03-15 18:52:18
66.169.72.73	2013-03-20 06:50:21
75.134.127.12	2013-03-04 08:12:07
24.178.116.81	2013-03-14 18:28:58
71.94.129.229	2013-03-18 06:28:07
71.91.18.137	2013-03-17 15:11:36
24.158.203.59	2013-03-13 05:13:28
66.227.227.224	2013-03-18 21:42:55
24.176.210.76	2013-03-13 18:51:34
68.184.146.121	2013-03-15 17:55:29
173.46.227.61	2013-03-12 00:51:24
24.231.185.185	2013-03-19 12:00:34

24.178.139.151	2013-03-19 13:58:36
24.158.146.28	2013-03-14 11:54:15
71.87.113.17	2013-03-19 05:37:41
75.143.232.48	2013-03-20 03:15:07
68.191.13.90	2013-03-19 03:28:36
75.134.112.230	2013-03-12 21:40:24
71.94.218.135	2013-03-20 04:06:21
68.114.223.107	2013-03-19 02:04:07
71.11.24.22	2013-03-03 21:00:13
68.191.9.141	2013-03-09 10:25:54
66.168.100.248	2013-03-17 13:19:20
66.189.93.36	2013-03-19 14:43:35
68.116.251.148	2013-03-21 15:26:59
24.158.36.119	2013-03-20 13:57:53
75.142.245.213	2013-03-09 16:14:10
71.93.118.47	2013-03-12 00:13:05
24.205.232.126	2013-03-20 02:20:56
24.223.105.154	2013-03-19 15:58:00
24.247.211.123	2013-03-16 20:30:13
75.130.227.51	2013-03-15 10:46:49
68.186.30.226	2013-03-20 16:32:37
97.81.48.94	2013-03-07 08:57:02
71.83.148.59	2013-03-15 11:15:31
97.80.33.128	2013-03-19 01:32:53
71.94.170.189	2013-03-15 07:50:16
71.91.40.208	2013-03-15 20:50:52
75.134.128.99	2013-03-17 04:22:59
71.86.122.158	2013-03-03 21:32:55
66.214.174.146	2013-03-01 19:55:22
96.38.235.118	2013-03-20 00:17:56
96.40.145.112	2013-03-22 15:45:52
97.89.75.11	2013-03-17 06:26:20
75.140.244.214	2013-03-06 09:24:12
97.81.9.112	2013-03-20 05:08:28
97.93.246.133	2013-03-20 16:50:24
71.12.196.199	2013-03-05 05:02:47
97.90.119.72	2013-03-11 07:14:23
66.214.83.234	2013-03-02 00:57:20
24.159.153.86	2013-03-03 14:43:37
97.95.89.69	2013-03-11 06:25:55
24.240.26.2	2013-03-07 01:00:39
97.82.189.204	2013-03-17 05:35:59
96.41.55.126	2013-03-13 14:57:03
96.35.47.44	2013-03-17 20:25:07
66.169.242.184	2013-03-22 05:52:18
24.205.15.54	2013-03-22 02:10:26
75.136.148.149	2013-03-18 13:27:17

96.39.227.52	2013-03-16 18:09:18
97.88.165.237	2013-03-20 16:33:59
71.95.34.65	2013-03-13 18:41:42
66.169.64.213	2013-03-12 14:38:57
68.184.242.60	2013-03-15 09:19:20
66.189.143.50	2013-03-18 01:24:43
24.205.189.212	2013-03-20 16:54:05
71.10.33.157	2013-03-18 17:22:00
71.8.116.55	2013-03-21 23:08:40
66.214.25.105	2013-03-20 09:09:32
68.185.41.200	2013-03-01 12:47:23
96.41.24.187	2013-03-20 00:19:50
66.189.210.169	2013-03-07 11:34:34
71.94.131.143	2013-03-03 18:07:07
71.12.2.1	2013-03-09 21:39:26
24.181.12.74	2013-03-20 06:26:15
96.39.249.168	2013-03-20 03:52:20
66.189.78.63	2013-03-09 10:20:13
71.93.83.154	2013-03-17 23:41:07
68.185.176.173	2013-03-16 03:48:56
71.87.201.13	2013-03-20 04:06:17
24.159.34.243	2013-03-16 19:20:50
68.188.245.243	2013-03-05 13:38:00
68.186.170.35	2013-03-12 06:23:50
68.184.192.226	2013-03-02 07:11:28
96.41.2.68	2013-03-19 14:17:47
68.187.85.22	2013-03-15 15:36:19
24.205.65.243	2013-03-19 04:17:39
71.10.170.20	2013-03-21 23:10:05
71.83.111.220	2013-03-08 20:35:22
96.41.169.86	2013-03-02 22:44:25
68.190.114.182	2013-03-01 19:09:10
24.231.242.20	2013-03-05 15:09:11
97.82.218.146	2013-03-13 18:41:41
71.9.62.117	2013-03-01 09:11:39
71.90.160.7	2013-03-17 11:15:50
97.93.103.161	2013-03-02 04:11:32
68.191.58.158	2013-03-14 23:59:22
24.207.183.168	2013-03-19 10:56:44
24.151.21.16	2013-03-19 22:23:26
24.207.254.187	2013-03-12 03:59:05
75.142.162.3	2013-03-13 07:29:15
75.129.226.75	2013-03-22 07:45:49
71.10.162.171	2013-03-03 15:45:40
71.85.206.108	2013-03-12 17:55:43
71.90.57.230	2013-03-19 03:59:01
97.88.61.246	2013-03-18 03:14:36

75.128.85.186	2013-03-02 19:50:59
71.92.60.2	2013-03-20 16:34:01
97.94.238.174	2013-03-16 22:49:28
75.138.56.49	2013-03-11 00:42:21
71.94.66.50	2013-03-05 17:12:44
97.92.1.204	2013-03-01 07:26:23
75.132.11.17	2013-03-14 15:12:29
97.91.232.207	2013-03-10 15:17:48
71.95.2.26	2013-03-03 19:26:48
68.190.188.200	2013-03-12 12:53:02
71.89.85.254	2013-03-12 20:53:30
97.92.64.155	2013-03-17 07:56:06
71.95.36.220	2013-03-07 13:50:28
75.136.228.200	2013-03-12 18:46:31
24.205.81.245	2013-03-20 14:37:37
96.39.225.223	2013-03-07 06:37:41
97.93.231.170	2013-03-03 23:55:50
97.88.0.83	2013-03-20 02:19:06
71.90.170.159	2013-03-21 14:33:26
68.188.185.66	2013-03-18 18:30:10
68.116.80.13	2013-03-14 02:26:13
71.83.124.221	2013-03-19 07:50:37
71.84.107.8	2013-03-21 23:07:17
68.186.87.183	2013-03-22 05:50:41
97.93.217.155	2013-03-10 07:05:44
68.113.90.15	2013-03-08 20:30:41
75.128.71.57	2013-03-19 22:01:13
66.214.174.134	2013-03-12 00:10:36
68.186.155.231	2013-03-10 20:20:46
68.117.203.4	2013-03-07 07:37:03
68.184.210.61	2013-03-20 00:41:39
75.131.203.126	2013-03-19 04:14:19
68.188.251.157	2013-03-12 18:32:15
75.141.139.5	2013-03-15 04:55:23
68.191.242.249	2013-03-16 00:48:33
75.136.160.196	2013-03-10 10:56:01
96.40.135.232	2013-03-03 05:08:07
97.87.163.47	2013-03-22 00:41:42
24.205.185.195	2013-03-12 03:37:38
24.176.22.107	2013-03-19 15:39:28
75.131.161.39	2013-03-02 11:02:20
24.181.234.52	2013-03-22 04:25:18
24.182.231.48	2013-03-18 14:28:00
97.93.241.116	2013-03-07 16:55:13
68.190.229.137	2013-03-22 15:42:54
71.9.128.231	2013-03-09 16:17:20
68.119.73.53	2013-03-13 11:57:16

24.181.84.70	2013-03-17 01:05:31
68.187.154.224	2013-03-15 14:01:17
75.128.179.234	2013-03-09 15:19:46
68.185.226.192	2013-03-02 07:11:35
75.141.204.62	2013-03-21 15:39:52
75.135.193.39	2013-03-03 18:19:42
24.216.226.3	2013-03-20 02:00:17
71.10.163.184	2013-03-20 16:21:34
75.133.173.103	2013-03-12 11:52:49
66.189.159.233	2013-03-22 02:21:44
75.132.33.54	2013-03-01 20:51:32
66.168.162.213	2013-03-15 17:54:38
97.87.163.30	2013-03-08 21:05:29
68.184.136.37	2013-03-18 05:14:07
71.8.206.173	2013-03-18 01:39:56
97.82.139.47	2013-03-17 22:05:12
24.176.4.204	2013-03-19 04:58:04
24.107.176.239	2013-03-06 05:00:00
24.107.228.89	2013-03-04 22:33:24
71.80.185.75	2013-03-05 21:30:57
97.82.33.68	2013-03-16 22:45:43
24.196.148.125	2013-03-10 17:41:15
68.114.69.35	2013-03-09 18:55:40
71.88.115.180	2013-03-21 22:02:16
75.138.45.144	2013-03-17 08:30:06
97.85.247.242	2013-03-22 09:28:23
97.82.152.133	2013-03-11 07:15:09
68.187.69.168	2013-03-05 15:46:32
96.36.138.140	2013-03-19 01:32:53
97.85.176.8	2013-03-18 03:16:29
24.51.179.253	2013-03-01 08:32:39
71.8.122.120	2013-03-22 02:38:40
24.231.202.127	2013-03-14 09:54:45
71.14.113.23	2013-03-06 22:59:30
68.112.102.211	2013-03-12 23:50:15
75.131.23.116	2013-03-22 09:16:09
96.32.64.109	2013-03-15 05:14:35
68.191.139.249	2013-03-05 01:42:20
68.188.179.230	2013-03-16 02:47:55
24.151.197.77	2013-03-14 07:05:15
97.93.9.184	2013-03-03 23:14:47
75.141.110.157	2013-03-20 10:21:39
68.119.0.237	2013-03-12 08:49:31
24.216.75.166	2013-03-03 15:45:37
71.81.193.50	2013-03-14 20:12:25
97.90.150.131	2013-03-15 23:05:36
24.196.81.71	2013-03-04 07:57:26

75.133.163.135	2013-03-18 03:16:50
24.171.21.129	2013-03-17 07:18:24
71.87.241.49	2013-03-11 05:21:47
24.217.143.33	2013-03-12 13:46:07
68.189.79.202	2013-03-05 11:11:51
68.114.90.105	2013-03-03 09:19:46
24.217.217.1	2013-03-18 14:07:27
96.38.180.20	2013-03-19 01:33:49
68.119.72.236	2013-03-19 03:16:36
24.158.144.118	2013-03-17 19:10:25
97.92.136.195	2013-03-13 19:40:23
75.129.60.60	2013-03-14 04:24:59
96.41.79.91	2013-03-18 23:09:29
24.197.129.87	2013-03-09 21:25:24
24.205.148.209	2013-03-22 06:26:55
24.205.101.128	2013-03-18 21:42:54
24.240.38.4	2013-03-20 10:21:45
96.42.99.54	2013-03-05 04:10:10
68.117.60.124	2013-03-12 21:43:21
96.37.27.166	2013-03-05 20:59:59
24.181.95.222	2013-03-20 09:20:06
71.11.199.108	2013-03-20 00:41:31
66.190.88.230	2013-03-19 19:24:49
24.180.35.151	2013-03-05 03:00:26
75.133.172.81	2013-03-18 20:00:11
71.9.37.161	2013-03-20 09:38:53
68.118.220.190	2013-03-22 15:00:55
66.214.2.187	2013-03-20 02:37:32
75.130.179.136	2013-03-03 00:54:33
97.90.118.111	2013-03-20 09:23:06
71.80.192.104	2013-03-18 20:27:10
96.41.18.157	2013-03-22 14:41:40
96.35.43.124	2013-03-05 05:32:15
96.36.128.54	2013-03-20 10:54:07
66.169.22.115	2013-03-07 04:36:11
66.214.133.146	2013-03-18 01:22:59
66.190.101.41	2013-03-12 10:08:20
71.80.123.56	2013-03-18 00:34:22
71.12.243.100	2013-03-17 05:01:24
75.142.58.182	2013-03-10 01:35:53
66.168.211.172	2013-03-02 07:09:43
24.179.59.10	2013-03-15 06:26:34
75.128.91.73	2013-03-10 08:47:51
66.189.36.147	2013-03-13 18:02:35
75.139.9.251	2013-03-17 19:33:25
96.36.149.71	2013-03-05 07:39:36
66.189.10.39	2013-03-09 09:41:29

66.214.184.66	2013-03-17 23:05:09
75.136.43.255	2013-03-17 15:01:38
64.83.213.135	2013-03-16 00:22:42
75.138.15.79	2013-03-15 02:42:30
24.107.199.173	2013-03-19 15:00:37
66.189.28.191	2013-03-20 01:08:45
24.240.29.233	2013-03-03 00:58:22
68.188.233.90	2013-03-20 06:14:02
75.135.84.190	2013-03-11 13:16:57
68.185.203.66	2013-03-02 03:31:35
96.41.178.66	2013-03-10 10:01:35
97.94.140.212	2013-03-12 12:44:33



# EXHIBIT B

October 4, 2012, 12:15PM

# Cybercrime Gang Recruiting Botmasters for Large-Scale MiTM Attacks on American Banks

by Michael Mimoso

A slew of major American banks, some already stressed by a stream of [DDoS attacks](#) carried out over the past 10 days, may soon have to brace themselves for a large-scale coordinated attack bent on pulling off fraudulent wire transfers.

[RSA's FraudAction research team](#) has been monitoring underground chatter and has put together various clues to deduce that a cybercrime gang is actively recruiting up to 100 botmasters to participate in a complicated man-in-the-middle hijacking scam using a variant of the [proprietary Gozi Trojan](#).

This is the first time a private cybercrime organization has recruited outsiders to participate in a financially motivated attack, said Mor Ahuvia, cybercrime communications specialist for RSA FraudAction. The attackers are promising their recruits a cut of the profits, and are requiring an initial investment in hardware and training in how to deploy the Gozi Prinimalka Trojan, Ahuvia added. Also, the gang will only share executable files with their partners, and will not give up the Trojan's compilers, keeping the recruits dependent on the gang for updates

Generally, cybercrime gangs deploy as few as five individual botmasters to help in successful campaigns; with this kind of scale, banks could be facing up 30 times the number of compromised machines and fraudulent transfers, if the campaign is successful.

"This Trojan is not well known. This is not [SpyEye](#) or [Citadel](#); it's not available for everyone to buy," Ahuvia said. "Security vendors and antivirus signatures are less likely to catch it or be familiar with it. It will be tricky for vendors to detect and block it. This gang is keeping a tight hold on the compiler. By only giving up executable files, they can control how any antivirus signatures are in the wild and keep unique signatures to a minimum."

As many as 30 banks have been targeted, many of them well known and high profile, Ahuvia said. RSA said the gang is targeting American banks because of past success in beating their defenses, as well as a lack of two-factor authentication required for wire transfers. Some European banks, for example, require consumers to use two-factor authentication. She added that RSA FraudAction was unsure how far along the recruitment campaign had gone, or when the attacks would launch.

"There is the chance that once we've gone public, they may abandon their plans because there's too much buzz around it," Ahuvia said. "On the other hand, I don't think anything we know will have such

a dramatic effect on them. There are so many Trojans available and so many points of failure in security that could go wrong, that they'd still have some chance of success."

RSA's researchers were able to make the connection to the Gozi Prinimalka Trojan, which has been in circulation since 2008 and responsible for \$5 million in fraud-related losses. Prinimalka is similar to the Gozi Trojan in technical and operational aspects, RSA said, leading to speculation the HangUp Team, which was tied to previous Gozi attacks, is behind this attack as well. Prinimalka is Russian for the word "receive" and is a folder name in every URL patch given by this particular gang to its crimeware servers.

Prinimalka uses the same bot-to-server communication pattern and URL trigger list as Gozi, RSA said. But deployment of the two Trojans is different: Gozi writes a single DLL file to bots upon deployment, while Prinimalka writes two, an executable file and a DAT file which reports to the command and control server.

Once the Trojan is launched, the botmaster fires up a virtual machine synching module. The module then duplicates the victim's computer, including identifiable features such as time zone, screen resolution, cookies, browser type and version, and software identification, RSA said. This allows the botmaster to impersonate the victim's machine and access their accounts. Access is carried out over a SOCKS proxy connection installed on the victim's machine, RSA said.

The cloned virtual system then can move about on the genuine IP address of the compromised machine when accessing the bank website. Taking it a step further, the attackers deploy VoIP phone flooding software that will prevent the victim from receiving a confirmation call or text alerting them to unusual transfer activity, RSA said.

"They are looking for this to be a quick campaign," Ahuvia said. "They want to make as much as they can until the banks and users harden their systems. They want to cash out quickly."

*Commenting on this Article will be automatically closed on January 4, 2013.*

# EXHIBIT C



## No slowdown in sight for cyberattacks

By Byron Acohido, USA TODAY

Updated 7/30/2012 10:00 AM

Recommend 0

102

2


[Reprints & Permissions](#)

### Videos you may be interested in



Security thriller at  
MLB at-bat



Veterans' impact on  
difference?



Sponsored Link  
Strange Bean  
burns Fat!  
[iconsumerknowledge](#)

byTaboola  
More videos

LAS VEGAS - Cyber attacks are accelerating at a pace that suggests the Internet - already a risky environment - is likely to pose a steadily growing threat to individuals and companies for years to come.

That's the somber consensus of security and Internet experts participating in the giant Black Hat cybersecurity conference that concluded here this week.

Internet-generated attacks comprise "the most significant threat we face as a civilized world, other than a weapon of mass destruction," Shawn Henry, former head of the FBI's cybercrime unit, told some 6,500 attendees in a keynote address.

Getty Images

Internet-generated attacks comprise the most significant threat we face as a civilized world, other than a weapon of mass destruction, according to one security expert.

[Joe Stewart](#), Dell SecureWorks' director of malware research, presented research detailing the activities of two large cyber gangs, one based in Shanghai the other in Beijing, that have cracked into the networks of thousands of companies over the past half dozen years.

The attacks invariably begin by infecting the computer of one employee, then using that machine as a toehold to patiently probe deep into the company's network. The end game: to steal customer lists, patents, bidding proposals and other sensitive documents.

### Most Popular

#### Stories

HF Test  
Don't fall for Facebook 'privacy' notice  
Smart Office 2: A versatile software suite

#### Videos

Ed Balg reviews Kindle Paperwhite  
'Pregnant man' struggles through nasty divorce  
Tennis Channel Court Report 9-30-2012

#### Photos

Mayan calendar discovery  
Facebook  
Apple iPhone 5 first day sales

#### Sponsored Links

##### **BlackBerry® Bold™ 9900**

Get more of the speed, style and performance you love. Learn more.  
[BlackBerry.com](http://www.fool.com)

##### **The God Machine**

It can't create man but it can generate anything else with the click of a button.  
<http://www.fool.com>

##### **Microsoft® Windows Azure**

Discover Microsoft® Windows Azure. Sign Up for a Free 90-Day Trial!  
[www.window.azure.com](http://www.window.azure.com)

[Buy a link here](#)

Each gang is made up of dozens of employees playing complementary roles in attacks that are "stealthy and persistent," says Stewart. "Even if they do get discovered and get kicked out of a network, they come back, targeting a different employee."

Another gang, analyzed by Dell SecureWorks' researcher Brett Stone-Gross, has been blasting out spam, designed to slip past spam filters. The messages carry instructions to click on a link to read bogus delivery invoices, airline reservations or cellphone bills. The link, however, takes the user to a web page that installs malicious software.

Stone-Gross said the gang currently has access to 678,000 infected PCs, some of which are used to carry out its lucrative specialty: orchestrating fraudulent wire transfers from online banking accounts.

Meanwhile, a different category of hackers is stepping up attacks, not on individual PCs, but on company websites. Website attacks now routinely occur thousands of times each, as criminals probe for ways to breach databases carrying usernames and passwords and other valuable data, says David Koretz, general manager of website security firm Mykonos, a division of Juniper Networks.

Some successful website hackers enjoy boasting —by publically posting some, if not most, of the stolen data. That's happened recently with data stolen from online retailer Zappos, matchmaking site eHarmony, business social networking site LinkedIn and search giant Yahoo, Koretz says.

Experts say web attacks continue to escalate partly because powerful, easy-to-use hacking programs are widely available for free. What's more, opportunities for an intruder to take control of an individual's PC, or access and probe a company's network, are multiplying as society uses more Internet-delivered services and Internet-connected mobile devices.

"It's easier and safer for a criminal to steal money from an online bank account, rather than have to walk into a bank — or to steal intellectual property in an online setting, rather than have to send in a human spy," says Eddie Schwartz, chief security officer of security firm RSA, a division of EMC.

For more information about [reprints & permissions](#), visit our FAQ's. To report corrections and clarifications, contact Standards Editor Brent Jones. For publication consideration in the newspaper, send comments to [letters@usatoday.com](mailto:letters@usatoday.com). Include name, phone number, city and state for verification. To view our corrections, go to [corrections.usatoday.com](http://corrections.usatoday.com).

Posted 7/27/2012 10:34 AM | Updated 7/30/2012 10:00 AM



#### Most Popular E-mail Newsletter

##### Sign up to get:

Top viewed stories, photo galleries and community posts of the day

Most popular right now:

HF Test



Sign up for USA TODAY E-mail newsletters

#### More from USATODAY

**Man kills girlfriend for revealing she was HIV positive** [USATODAY.COM](#) in On Deadline

**More Duchess Kate topless pics out; police hunt photographer** [USATODAY.COM](#) in LifeLine Live

**Column: Christian companies can't bow to sinful mandate** [USATODAY.COM](#) in News

**5 reasons to skip iPhone 5 lines** [USATODAY.COM](#) in Tech

#### More from the web

**If You Have Gmail... You Must Have This** [The Next Web](#)

**Apple's Next Big Thing Will Be Huge** [EBN](#)

**Cloud Will Never be Cheaper Than On-Premise: Claranet** [CIO](#)

**How to Load Your Dishwasher: Common Mistakes People Make** [Dishwashers Info](#)

**4 Things You Can Learn From Segway's Notorious Product Fail** [OPEN Forum](#)

[?]

USA TODAY is now using Facebook Comments on our stories and blog posts to provide an enhanced user experience. To post a comment, log into Facebook and then "Add" your comment. To report spam or abuse, click the "X" in the upper right corner of the comment box. To find out more, read the [FAQ](#) and [Conversation Guidelines](#).

# EXHIBIT D



Threat Level

Privacy, Crime and Security Online

Hacks and Cracks

Cybersecurity

Like 213 85

22

Share

14

# Hackers Release 1 Million Apple Device IDs Allegedly Stolen From FBI Laptop

By [Kim Zetter](#) [Email](#) [Author](#)

09.04.12

12:49 PM

Follow @KimZetter



*Photo: Wired*

The hacker group AntiSec has released 1 million Apple device IDs that they say they obtained from an FBI computer they hacked.

The hackers say they actually stole 12 million IDs, including personal information, from the hacked FBI computer, but released only 1 million in an encrypted file published on torrent sites. In a [lengthy post online](#), the hackers wrote that last March, they hacked a laptop belonging to an FBI agent named Christopher K. Stangl from the bureau's Regional Cyber Action Team and the New York FBI office's Evidence Response Team.

The hackers say the IDs were stored in a file on Stangl's desktop titled "NCFTA\_iOS\_devices\_intel.csv."



The file, according to the hackers, contained a list of more than 12 million Apple iOS devices, including Unique Device Identifiers (UDID), user names, names of devices, types of devices, Apple Push Notification Service tokens, ZIP codes, cellphone numbers, and addresses. The hackers released only 1 million UDIDs, however, and did not release the accompanying personal information for the IDs.

Apple UDIDs are a 40-character alphanumeric string that is unique to each Apple device. It's not known why the FBI possessed the Apple IDs. The hackers suggested in a tweet from the @AnonymousIRC account, that the FBI was using the information to track users.



Stangl may have been targeted because he was [on an e-mail that members of Anonymous intercepted](#) last January. The e-mail was sent to several dozen U.S. and European law-enforcement personnel to participate in a conference call discussing efforts to investigate Anonymous and other hacking groups. The email included a call-in number for the discussion, which members of Anonymous recorded and [posted online last February](#).

The hackers say they released the Apple UDIDs so that people would know that the FBI may be tracking their devices and also because, they wrote in their online post, "we think it's the right moment to release this knowing that Apple is looking for alternatives for those UDID currently ... but well, in this case it's too late for those concerned owners on the list."

Apple [has been criticized](#) for hard-coding the ID's in devices, since they can be misused by application developers and others to identify a user, when combined with other information, and track them. Last April, Apple began [rejecting applications that track UDIDs](#).

The Next Web has created a tool for users to [check if their Apple UDID is among those](#) that the hackers released.

[Related](#)

[You Might Like](#)

[Related Links by Contextly](#)

# EXHIBIT E



## Cyber defenders urged to go on the offense

By Glenn Chapman (AFP) – Jul 26, 2012

**LAS VEGAS** — Computer security champions on Wednesday were urged to hunt down and eliminate hackers, spies, terrorists and other online evildoers to prevent devastating Internet Age attacks.

The first day of briefings at a prestigious Black Hat computer security gathering here opened with a former FBI cyber crime unit chief calling for a shift from defense to offense when it comes to protecting networks.

"We need warriors to fight our enemies, particularly in the cyber world right now," Shawn Henry said in a Black Hat keynote presentation that kicked off with dramatic video of hostage rescue teams training.

"I believe the threat from computer network attack is the most significant threat we face as a civilized world, other than a weapon of mass destruction."

The peril grows as water supplies, power grids, financial transactions, and more rely on the Internet and as modern lives increasingly involve working and playing on smartphones or tablet computers, according to Henry.

He rolled off a list of adversaries ranging from spies and well-funded criminals to disgruntled employees with inside knowledge of company networks.

"Cyber is the great equalizer," Henry said.

"With a \$500 laptop with an Internet connection anybody, anywhere in the world can attack any organization, any company," he continued. "The last time I checked, that was about 2.3 billion people."

After 24 years of working for the FBI, Henry in April switched to the private sector as the head of a division at startup CrowdStrike specializing in cyber attack incident responses and identifying adversaries.

The computer security industry to expand its arsenal beyond just building walls, filters and other safeguards against online intruders to include watching for, and gathering intelligence on, culprits who have slipped through.

"It is not enough to watch the perimeter," Henry said, equating computer security to protecting real world offices. "We have to be constantly hunting; looking for tripwires."

In the cyber world, that translates into monitoring system activities such as whether files have been accessed or changed and by whom.

"The sophisticated adversary will get over that firewall and walk around, like an invisible man," Henry said. "We have to mitigate that threat."

Tactics for fighting cyber intruders should include gathering information about how they operate and the tools used, and then sharing the data in the industry and with law enforcement agencies in relevant countries.

"Intelligence is the key to all of this," Henry said. "If we understand who the adversary is, we can take specific actions."

Teamwork between governments and private companies means that options for responding to identified cyber attackers can range from improved network software to political sanctions or even military strikes, according to Henry.

"You can't make every school, every mall, every university, and every workplace impenetrable," Henry said. "We have to look at who the adversary is and stop them in advance of them walking in."

Black Hat founder Jeff Moss, the self-described hacker behind the notorious Def Con gathering that starts here on Thursday, backed Henry's argument.

"Maybe we need some white blood cells out there; companies willing to push the edge and focus on threat actors," Moss said, calling on the computer security community to "raise the immunity level."

Moss is head of security at the Internet Corporation for Assigned Names and Numbers, which oversees the world's website addresses.

"So, am I Luke, or am I Darth Vader; sometimes I'm not sure," Moss quipped about his roles in the hacker realm and the computer security industry.

"It depends upon which day and who asks."

Moss proposed that cyber attackers also be fought on legal fronts, with companies taking suspected culprits to court.

"I can't print money; I can't raise an army, but I can hire lawyers and they are almost as good," Moss said. "One way to fight the enemy is you just sue them."

Henry feared that it may take an Internet version of the infamous 9/11 attack in New York City to get the world to take the cyber threat to heart.

"We need to get down range and take them out of the fight," Henry said.



Former FBI cyber crime unit chief Shawn Henry was the keynote speaker at the Black Hat computer security gathering (AFP/Getty Images/File)

### Map



10/6/12

AFP: Cyber defenders urged to go on the offense

"As well-trained, well-equipped cyber warriors you can have an impact; the stakes are high."

Copyright © 2012 AFP. All rights reserved. [More »](#)

**Man Cheats Credit Score**

1 simple trick & my credit score jumped 217 pts. Banks hate this!

[www.thecreditsolutionprogram.com](http://www.thecreditsolutionprogram.com)

**Counterterrorism Degree**

Study counterterrorism at AMU & receive an online college degree.

[www.AMU.APU.S.edu/Intelligence](http://www.AMU.APU.S.edu/Intelligence)

**Long Term Care Ins**

6 Quotes, Free Guide & Consultation. Explore Your Insurance Options Now.

[www.ltcfp.com/long-term-care-quotes](http://www.ltcfp.com/long-term-care-quotes)

**Single Woman Over 40?**

The Most Eligible Singles Over 40. Try Our Risk Free Site.

[MatureSinglesOnly.com](http://MatureSinglesOnly.com)



Add News to your Google Homepage

©2012 Google - [About Google News](#) - [Blog](#) - [Help Center](#) - [Help for Publishers](#) - [Terms of Use](#) - [Privacy Policy](#) - [Google Home](#)

# EXHIBIT F



**The New York Times**

March 12, 2013

# Security Leader Says U.S. Would Retaliate Against Cyberattacks

By **MARK MAZZETTI** and **DAVID E. SANGER**

WASHINGTON — The chief of the military's newly created Cyber Command told Congress on Tuesday that he is establishing 13 teams of programmers and computer experts who could carry out offensive cyberattacks on foreign nations if the United States were hit with a major attack on its own networks, the first time the Obama administration has publicly admitted to developing such weapons for use in wartime.

"I would like to be clear that this team, this defend-the-nation team, is not a defensive team," Gen. Keith Alexander, who runs both the National Security Agency and the new Cyber Command, told the House Armed Services Committee. "This is an offensive team that the Defense Department would use to defend the nation if it were attacked in cyberspace. Thirteen of the teams that we're creating are for that mission alone."

General Alexander's testimony came on the same day the nation's top intelligence official, James R. Clapper Jr., warned Congress that a major cyberattack on the United States could cripple the country's infrastructure and economy, and suggested that such attacks now pose the most dangerous immediate threat to the United States, even more pressing than an attack by global terrorist networks.

On Monday, Thomas E. Donilon, the national security adviser, demanded that Chinese authorities investigate such attacks and enter talks about new rules governing behavior in cyberspace.

General Alexander has been a major architect of the American strategy on this issue, but until Tuesday he almost always talked about it in defensive terms. He has usually deflected questions about America's offensive capability, and turned them into discussions of how to defend against mounting computer espionage from China and Russia, and the possibility of crippling attacks on utilities, cellphone networks and other infrastructure. He was also a crucial player in the one major computer attack the United States is known to have sponsored in recent years, aimed at Iran's nuclear enrichment plants. He did not discuss that operation during his open testimony.

Mr. Clapper, the director of national intelligence, told the Senate Intelligence C

OPEN

**MORE IN U.S.**  
**Sequester Nation'**  
Read More



American spy agencies saw only a “remote chance” in the next two years of a major computer attack on the United States, which he defined as an operation that “would result in long-term, wide-scale disruption of services, such as a regional power outage.”

Mr. Clapper appeared with the heads of several other intelligence agencies, including Lt. Gen. Michael T. Flynn of the Defense Intelligence Agency, the F.B.I. director Robert S. Mueller III, and the C.I.A. director John O. Brennan, to present their annual assessment of the threats facing the nation. It was the first time that Mr. Clapper listed cyberattacks first in his presentation to Congress, and the rare occasion since the Sept. 11, 2001, attacks that intelligence officials did not list international terrorism first in the catalog of dangers facing the United States.

“In some cases,” Mr. Clapper said in his testimony, “the world is applying digital technologies faster than our ability to understand the security implications and mitigate potential risks.” He said it was unlikely that Russia and China would launch “devastating” cyberattacks against the United States in the near future, but he said foreign spy services had already hacked the computer networks of government agencies, businesses and private companies.

Two specific attacks Mr. Clapper listed, an August 2012 attack against the Saudi oil company Aramco and attacks on American banks and stock exchanges last year, are believed by American intelligence officials to have been the work of Iran.

General Alexander picked up on the same themes in his testimony, saying that he was adding 40 cyber teams, 13 focused on offense and 27 on training and surveillance. When pressed, he said that the best defense hinged on being able to monitor incoming traffic to the United States through private “Internet service providers,” which could alert the government, in the milliseconds that electronic messages move, about potentially dangerous attacks. Such surveillance is bound to raise more debate with privacy advocates, who fear government monitoring of the origin and the addressing data on most e-mail messages and other computer exchanges.

Traditional threats occupied much of Mr. Clapper’s testimony. American intelligence officials are giving new emphasis to the danger posed by North Korea’s nuclear weapons and missile programs, which are said for the first time to “pose a serious threat to the United States” as well as to its East Asian neighbors. North Korea, which recently made a series of belligerent statements after its third nuclear test, has displayed an intercontinental missile that can be moved by road and in December launched a satellite atop a Taepodong-2 launch vehicle, Mr. Clapper’s prepared statement noted.

“The rhetoric, while it is propaganda laced, is also an indicator of their attitude and perhaps



their intent,” Mr. Clapper said during one exchange with a lawmaker, adding that he was concerned that North Korea “could initiate a provocative action against the South.”

In his discussion of terrorism, Mr. Clapper noted that while Al Qaeda’s core in Pakistan “is probably unable to carry out complex, large-scale attacks in the West,” spinoffs still posed a threat. Listed first is the affiliate in Yemen, Al Qaeda in the Arabian Peninsula, which Mr. Clapper said had retained its goal of attacks on United States soil, but he also noted militant groups in six other countries that still threaten local violence.

Mr. Clapper began his remarks by criticizing policy makers for the current budget impasse, saying that the budget cuts known as sequestration will force American spy agencies to make sharp reductions in classified programs and to furlough employees. The classified intelligence budget has ballooned over the past decade, and Mr. Clapper compared the current round of cuts to the period during the 1990s when the end of the cold war led to drastic reductions in the C.I.A.’s budget.

“Unlike more directly observable sequestration impacts, like shorter hours at public parks or longer security lines at airports, the degradation of intelligence will be insidious,” Mr. Clapper said. “It will be gradual and almost invisible unless and until, of course, we have an intelligence failure.”

The threat hearing is the only scheduled occasion each year when the spy chiefs present open testimony to Congress about the dangers facing the United States, and Mr. Clapper did not hide the fact that he is opposed to the annual ritual. President Obama devoted part of his State of the Union address to a pledge of greater transparency with the Congress and the American public, but Mr. Clapper, a 71-year-old retired Air Force general, made it clear that he saw few benefits of more public disclosure.

“An open hearing on intelligence matters is something of a contradiction in terms,” he said.

*Scott Shane contributed reporting.*



**IN THE CIRCUIT COURT OF THE TWENTIETH JUDICIAL CIRCUIT  
ST. CLAIR COUNTY, ILLINOIS  
LAW DIVISION**

PEG LEG PRODUCTIONS, LLC,

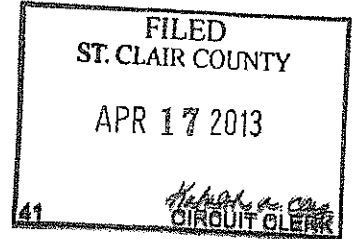
Petitioner,

v.

CHARTER COMMUNICATIONS, LLC,

Respondent.

No. 13 MR 142



**MEMORANDUM OF LAW IN SUPPORT OF PETITION FOR DISCOVERY BEFORE  
SUIT TO IDENTIFY RESPONSIBLE PERSONS AND ENTITIES**

**I. INTRODUCTION**

Through this petition for discovery, Petitioner, the owner of private websites, seeks to learn the identities of unidentified John Does ("Does") from Internet Service Provider ("ISP") Respondent Charter Communications, LLC ("Charter"), so that Petitioner may file a suit against these individuals for computer fraud and abuse, computer tampering, and civil conspiracy. Since Does used the Internet to commit their violations, Petitioner only knows Does by their Internet Protocol ("IP") addresses. Does' IP addresses were assigned to Does by Charter. Accordingly, Charter can use the IP addresses to identify Does. Indeed, Charter maintains internal logs, which record the date, time and customer identity for each IP address assignment made by Charter. Significantly, Charter only maintain these logs for a very short period of time.

Petitioner seeks an order requiring Charter to respond to a subpoena that will be served it requiring Charter to disclose the true name, address, telephone number, e-mail address and Media Access Control ("MAC") address<sup>1</sup> of the Does. Petitioner will only use this information to resolve its computer fraud and abuse and computer tampering dispute with the Does. Without

---

<sup>1</sup> A MAC address is a number that identifies the specific device used for the hacking activity.

this information, Petitioner cannot name Does in future suits nor immediately serve Does to pursue any such lawsuit to protect itself.

As explained below, Petitioner is indisputably entitled to learn the identity of Does and a petition for pre-suit discovery is a proper tool for this purpose. Accordingly, this Court should grant this petition.

## **II. FACTUAL BACKGROUND**

Petitioner operates a private website. As alleged in the Petition, Petitioner has actionable claims for computer fraud and abuse and computer tampering against each of the Does. Does used hacked passwords to gain unauthorized access to Petitioner's protected computer systems.

Although Petitioner does not know Does' true identities, Petitioner's agents identified each of the Does by a unique IP address assigned to that Doe by Charter and the date and time of the hacking activity. Charter maintains internal logs which record the date, time, and customer identify for each IP address assignment made. Charter can use the IP address provided by Petitioner to identify the Does. Charter, however, only retains the information necessary to correlate an IP address to a person for a short amount of time. Accordingly, time is of the essence with respect to getting the subpoenas to Charter so that Charter may preserve and maintain this information necessary to identify Does.

## **III. ARGUMENT**

Petitioner may obtain the identities of the Does through a petition for discovery pursuant to Illinois Supreme Court Rule 224. A petition for discovery before suit to identify responsible persons and entities may be used by "[a] person or entity who wishes to engage in discovery for the sole purpose of ascertaining the identity of one who may be responsible in damages . . ." 134 Ill. 2d R. 224. Illinois courts grant petitions for pre-suit discovery when, like in the present case,

the identities of the defendants are unknown to the plaintiff. *John Gaynor v. Burlington Northern and Santa Fe Railway*, 750 N.E.2d 307, 312 (Ill. App. Ct. 2001) (“Rule 224’s use is appropriate in situations where a plaintiff has suffered injury but does not know the identity of one from whom recovery may be sought.”); *Roth v. St. Elizabeth’s Hospital*, 607 N.E.2d 1356, 1361 (Ill. App. Ct. 1993) (“[Rule 224] provides a tool by which a person or entity may, with leave of court, compel limited discovery before filing a lawsuit in an effort to determine the identity of one who may be liable in damages.”) (Quoting 134 Ill. 2d R. 224, Committee Comments, at 188-89)).

The “identity” that Petitioner is entitled to ascertain is more than just the names of the unknown Does. *John Gaynor*, 750 N.E.2d at 312 (“on occasion, the identification of a defendant may require more than simply a name and that, on those occasions, discovery under Rule 224 is not limited to the petitioner’s ascertainment of a name only.” (Citing *Beale v. EdgeMark Financial Corp.*, 664 N.E.2d 302 (Ill. App. Ct. 1996))). Petitioner requires this additional information,<sup>2</sup> because sometimes the Internet subscriber and the actual hacker are determined to not be one and the same.<sup>3</sup> Petitioner needs all the identifying information it seeks to make this determination.

Further, Petitioner is not precluded from the information it seeks simply because it is aware of the Does’ IP addresses. The court in *Beale* explains that the pre-suit discovery is not precluded “solely on the basis of the petitioner’s knowledge of a name only.” 664 N.E.2d at 307. Knowledge of the Does’ IP addresses does not provide Petitioner with sufficient information to

---

<sup>2</sup> The address, telephone number, e-mail address, and Media Access Control address of each account holder.

<sup>3</sup> For instance, an individual who lives alone with a secure wireless Internet connection is very likely to be both the account holder and the hacker. In contrast, where the account holder is, for example, the wife of the household it is more likely the case—given the nature of Petitioner’s business—that the husband or a college-aged son is the appropriate hacker. In other words, in the latter example the account holder and the hacker are most likely not the same individual.

name and bring a lawsuit against them. If mere knowledge of the defendant's name is not enough to preclude pre-suit discovery under Rule 224, then mere knowledge of the Does' IP address is also not enough to preclude the pre-suit discovery.

In short, Petitioner is using the petition for pre-suit discovery for its intended purpose: to identify the names of the people who have harmed it. There is no legal or equitable reason why Petitioner should be prohibited from seeking the Does' identities from Charter.

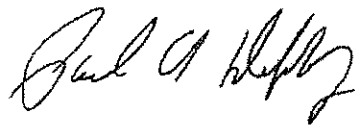
#### **IV. CONCLUSION**

For all the forgoing reasons, the Court should enter an order granting this petition.

Respectfully submitted,

Peg Leg Productions, LLC

DATED: April 15, 2013



By:

\_\_\_\_\_  
Paul A. Duffy, Esq. (Bar No. 6210496)  
2 N. LaSalle Street  
13th Floor  
Chicago, IL 60602  
312-476-7645  
*Attorney for Petitioner*

Kevin T. Hoerner  
Becker, Paulson, Hoerner & Thompson, P.C.  
5111 West Main Street  
Belleville, IL 62226  
(618) 235-0020  
*Attorney for Petitioner*