FEDERAL BUREAU OF INVESTIGATION
SITUATIONAL INFORMATION REPORT
Cyber Crime Alert

Phoenix Division

29 April 2011

(U//LES) Botnet Owners Share Honeypot Internet Protocol Addresses in Attempt to Avoid Law Enforcement and Security Vendor Scrutiny

(U//LES) Between 23 February, 2011 and 15 March, 2011, Botnet owners posting on the website ryan1918.com shared internet protocol (IP) addresses they believed were associated with honeypots used by law enforcement and anti-virus, anti-malware, and security research vendors[1].[a,b]

(U//LES) The Botnet owners warned the data collected by honeypots could be used by law enforcement agencies for criminal indictments. Botnet owners were further advised to be suspicious of blind "GET" requests and to use firewall rules in order to drop requests originating from the IP addresses and IP address ranges listed below.[c]

(U//LES) The ryan1918.com website was identified in previous law enforcement reporting as the location of a collaboration forum for hackers and owners of botnets.[d] The website allows hackers to claim credit for defacements, post hacking tools, and share hacking success stories.

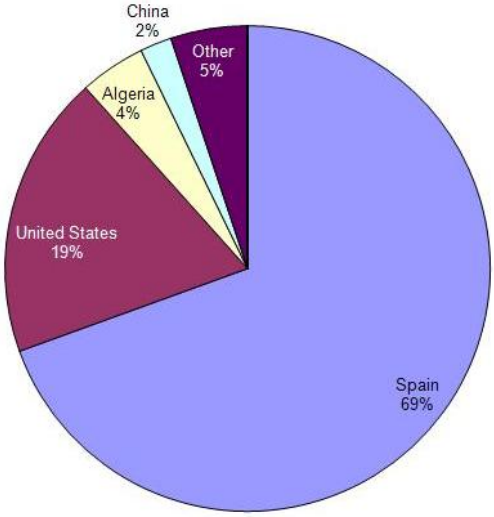
(U) Law Enforcement Sensitive: This information is the property of the FBI and may be distributed to state, tribal, or local government law enforcement officials with a need-to-know. Further distribution without FBI authorization is prohibited. Precautions should be taken to ensure this information is stored and/or destroyed in a manner that precludes unauthorized access.

(U) Warning: This is an information report, not finally evaluated intelligence. It is being shared for informational purposes but has not been fully evaluated, integrated with other information, interpreted, or analyzed. Receiving agencies are cautioned not to take actions based solely on this raw reporting unless the information is independently verified. A presumption of innocence still exists for any person being reported on in this report.

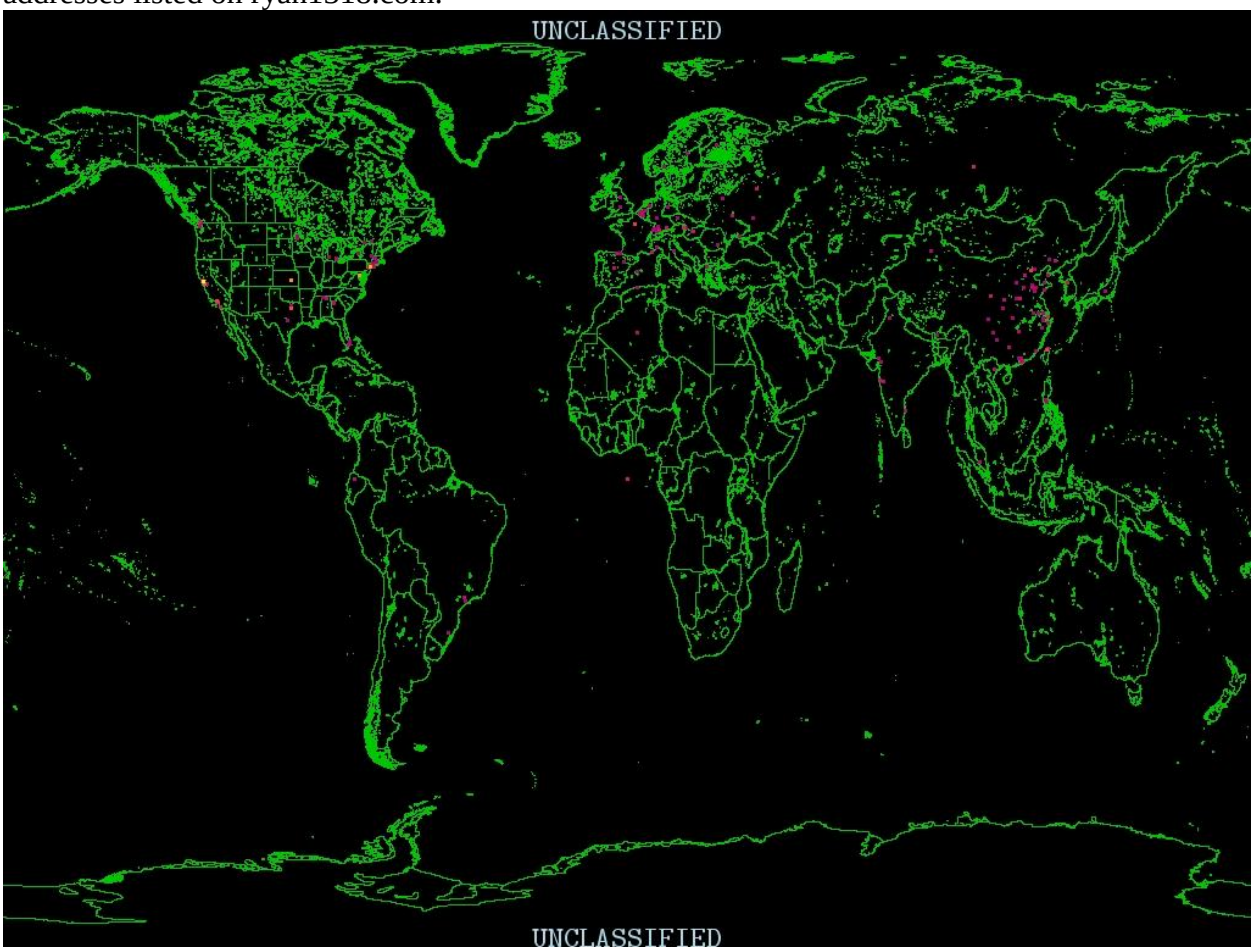
(U) Note: This product reflects the views of FBI Phoenix and has not been vetted by FBI Headquarters.

[1] A honeypot is a decoy server or system set up to gather, log, and trace information regarding an attacker or intruder into a computer system.

(U//LES) A graphical representation showing the percentage of the top five countries to which the suspected honeypot IP addresses listed on ryan1318.com resolved.



(U//LES) A geographical representation for locations of the list of suspected honeypot IP addresses listed on ryan1318.com.



(U//LES) The following list contains the individual honeypot IP addresses and IP address ranges suspected to be associated with law enforcement and security research vendors which were listed on the website ryan1318.com.

8.17.84.53	8.116.x.x	24.6.0.0 - 24.6.255.255
24.6.61.231	27.188.224.187	38.105.71.114
38.105.71.72	38.229.0.75	46.0.0.0 - 46.255.255.255
46.5.225.121	46.5.31.193	58.216.206.62
58.53.131.186	59.92.68.2	60.182.169.74
60.213.136.122	60.215.157.32	60.52.96.99
61.163.230.239	62.10.117.169	62.194.131.137
62.67.194.0	62.67.194.255	63.240.0.0
63.242.255.255	63.240.91.179	64.124.203.72
64.124.203.77	64.160.0.0	64.160.0.12
64.175.255.255	64.175.35.3	64.235.144.0
64.235.144.20	64.235.159.255	64.235.157.234
64.237.49.72	66.216.8.67	67.112.0.0
67.112.0.0 - 67.127.255.25	67.112.0.0 - 67.127.255.255	67.116.236.0
67.116.239.255	67.121.127.114	67.121.127.120
67.121.127.228	67.121.127.36	67.121.127.44
67.124.36.0	67.124.36.22	67.124.39.255
67.124.37.250	67.124.37.89	67.124.38.158
67.124.38.51	67.127.255.25	67.127.255.255
67.231.254.19	67.79.193.250	68.62.208.0
68.62.208.0 - 68.62.223.255	68.62.212.103	68.62.223.255
68.71.52.49	69.119.109.216	69.163.129.35
69.164.192.0	69.164.223.255	69.164.192.0 - 69.164.223.255
69.164.194.188	69.28.48.0	69.28.58.2
69.28.48.20	69.28.58.3	69.28.58.6
69.28.58.9	69.28.58.10	69.28.58.11
69.28.58.41	69.28.63.255	71.56.58.47
72.1.196.184	74.45.163.47	74.50.3.205
74.92.0.0 - 74.95.255.255	74.211.165.68	75.127.67.240
76.119.101.56	76.195.147.119	76.96.0.0
76.96.0.0 - 76.127.255.255	76.127.255.255	77.121.0.3
78.97.35.180	80.108.65.8	80.201.238.34
81.93.167.102	81.240.20.154	82.75.58.63
82.169.28.225	84.14.214.192	84.14.214.192 - 84.14.214.223
84.14.214.223	84.14.214.213	84.127.116.154

84.158.131.139	84.158.132.168	84.158.132.191
84.177.108.x	84.197.30.65	84.222.66.12
85.48.0.0	85.48.0.0 - 85.55.255.255	85.54.230.6
85.55.255.255	85.84.0.0	85.84.0.0 - 85.87.255.255
85.85.187.243	85.87.255.255	87.179.30.194
89.217.104.62	91.176.232.84	91.182.132.233
91.182.35.169	91.202.72.226	91.213.143.250
92.9.231.169	92.113.246.92	93.122.64.100
92.140.43.101	94.67.209.184	94.227.11.160
95.133.42.146	95.169.186.80	96.31.87.253
96.50.0.167	96.50.0.168	98.143.144.x
98.143.144.91	99.30.82.190	99.50.91.143
109.129.189.25	110.212.10.83	111.85.145.67
112.237.14.255	113.70.91.171	113.89.160.108
113.106.106.131	113.111.46.40	113.225.187.144
113.240.31.69	114.246.65.21	114.246.94.130
114.248.93.229	115.60.8.23	115.213.74.17
116.236.201.122	116.238.231.239	117.22.203.191
117.136.9.173	118.32.89.208	118.81.3.97
118.100.233.137	118.169.32.150	118.169.32.89
118.169.34.98	118.169.34.183	118.169.36.211
118.169.40.24	118.213.83.50	119.192.191.117
120.0.196.204	120.69.249.188	120.89.55.3
121.29.121.203	122.169.71.53	122.169.76.19
122.173.11.26	122.224.129.146	123.101.50.131
123.117.20.224	123.119.238.120	123.134.170.169
123.134.175.46	123.161.193.186	123.175.177.156
123.188.187.249	123.237.8.146	123.247.158.181
123.252.235.208	123.252.235.215	123.252.235.208 -
123.252.235.215	123.252.235.210	123.67.48.107
124.107.147.138	124.130.0.7	124.134.102.51
124.89.51.12	124.94.211.119	125.89.75.100
125.93.76.242	125.125.190.176	125.224.199.18
128.151.238.70	128.241.111.20	143.215.130.53
149.5.0.0	149.5.255.255	149.5.0.0 - 149.5.255.255
149.5.168.2	149.9.0.0	149.9.0.0 - 149.9.255.255
149.9.0.58	149.9.255.255	150.70.66.181
150.70.75.37	150.70.172.103	166.205.15.248
178.125.148.201	178.191.242.67	178.191.251.56
178.255.248.155	183.91.2.8	183.191.217.78

186.46.17.199	186.42.141.207	188.23.93.79
188.98.64.4	188.99.229.153	188.165.140.240
189.67.191.43	193.173.137.253	193.200.150.125
195.134.168.251	195.177.247.202	195.214.79.22
195.228.45.0	195.228.45.0 - 195.228.45.255	195.228.45.78
195.228.45.255	195.243.67.18	196.20.64.0
196.20.64.0 - 196.20.127.255	196.20.73.60	196.20.127.255
198.172.203.249	200.215.222.234	201.53.194.175
201.82.88.189	202.144.154.34	203.210.153.11
204.93.130.x	204.95.105.214	204.118.31.201
204.181.64.8	205.212.79.43	207.6.44.37
207.46.0.0	207.46.0.16	207.46.193.37
207.46.255.255	208.48.224.0	208.48.224.19
208.49.0.0	208.49.0.16	208.50.0.0
208.50.0.17	208.50.101.153	208.50.127.255
208.80.192.0	208.80.199.255	208.80.192.0 - 208.80.199.255
208.80.192.56	208.80.194.28	208.80.194.30
208.80.194.33	208.80.194.35	208.115.138.0
208.115.139.255	208.123.40.0	208.123.40.0 - 208.123.41.255
208.123.41.255	209.17.131.104	209.17.131.125
209.17.173.90	209.76.0.0	209.76.0.14
209.79.65.238	209.79.255.255	211.236.246.220
212.56.95.253	212.92.4.44	213.30.189.64
213.30.189.64 - 213.30.189.71	213.30.189.66	213.30.189.71
213.41.252.223	213.88.151.72	213.119.53.117
216.18.100.157	216.155.158.171	216.157.208.146
216.245.192.0	216.245.192.19	216.245.222.28
216.245.222.36	216.245.223.255	217.23.128.0
217.23.128.19	217.23.132.187	217.23.140.58
217.23.159.255	217.75.75.99	218.108.10.235
218.4.211.134	218.22.173.88	218.202.219.8
219.139.148.108	219.151.9.139	220.152.129.221
220.178.18.166	220.225.70.109	221.11.46.91
221.137.218.249	222.183.15.230	222.240.216.1

(U//LES) The list of IP address ranges with comments below were also posted by botnet owners on the website ryan1318.com. These IP address ranges resolve to multiple, geographically separate locations and are listed here for reference only.

START IP RANGE	END IP RANGE	POSTED COMMENTS
46.0.0.0	46.255.255.255	Blind get request from Germany; Can't trust this range anymore
67.112.0.0	127.255.25	NONE
67.112.0.0	67.127.255.255	Redacted US Business Name
74.92.0.0	74.95.255.255	NONE
76.96.0.0	76.127.255.255	Researchers

(U) This report was prepared by the Phoenix Division of the FBI. Comments and queries may be addressed to FBI Phoenix SIA Mary L. Martinez at (602) 650-3046

(U) Endnotes

[a] (U) Internet site; Tapout; ryan1918; "[LIST] Honeypot Domains"; 15 March 2011; www.ryan1918.com; accessed on 15 March 2011; the website ryan1918 is a collaboration forum for owners of botnets. The ryan1918.com hacker forum website allows hackers to claim credit for defacements, post hacking tools, and share hacking success stories.

[b](U) FBI Electronic Communication.

[c] (U) Ibid.

[d] (U) FBI Electronic Communication.

Distribution

FBI Intranet
LEO
Phoenix Infraguard **Attn**:
Chief Technology Officers
Chief Information Officers
IT Security Directors

FBI Customer Satisfaction Survey

Please take a moment to complete this survey and help evaluate the quality, value, and relevance of our intelligence product. Your response will help us serve you more effectively and efficiently in the future. Thank you for your cooperation and assistance. Please return to:
Federal Bureau of Investigation
Production Services Unit
935 Pennsylvania Ave, NW, Room 11079C
Washington, DC 20535

Customer and Product Information

Intelligence Product Title: _____

Dated: _____

Customer Agency: _____

Relevance to Your Intelligence Needs

1. The product increased my knowledge of an issue or topic. (Check one)

___5. Strongly Agree

___4. Somewhat Agree

___3. Neither Agree or Disagree

___2. Somewhat Disagree

___1. Strongly Disagree

Actionable Value

2. The product helped me decide on a course of action. (Check one)

___5. Strongly Agree

___4. Somewhat Agree

___3. Neither Agree or Disagree

___2. Somewhat Disagree

___1. Strongly Disagree

Timeliness Value

3. The product was timely to my intelligence needs. (Check one)

___5. Strongly Agree

___4. Somewhat Agree

___3. Neither Agree or Disagree

___2. Somewhat Disagree

___1. Strongly Disagree

PSU INTERNAL USE ONLY
Product Tracking #: _____
Return To:

Comments (please use reverse or attach separate page if needed):

_____

_____