DGA DynDNS Domain Kryptik Malware Delivery Report

Wednesday June, 19 2013 @ 12:53 PM

Prepared for RSA First Watch

NetWitness Informer

DGA DynDNS Domain Kryptik Malware Delivery Report

Ran at	Wednesday June, 19 2013 @ 12:53 PM
Source	concentrator-sb
Time Range	**2013-May-29 00:00:00** to **2013-Jun-19 12:00:00**

This report shows the activity of a particular flavor of the Kryptik Botnet. This is detected by looking for two server banners, apache and nginx, where the user-agent string was missing.

Good examples of this activity are listed over at VirusTotal. Simply search the site for a domain name to see the detection rate.

What makes this variant unique is that it appears that scores of dynamically generated domain names have been previously registered. The botnet distributor will assign several of his IPs to each domain name and will dynamically load balance them to distribute the malware. After a few days, he withdraws the IP assignments to those domains, rendering them unresponsive.

DGA Fastfluxing Kryptik Domains

alias.host	Session Count
1. vegysca.com	23
1. ip.dst 46.149.187.135	2
2. ip.dst 200.83.203.239	1
3. ip.dst 194.143.137.152	1
4. ip.dst 188.119.73.177	1
5. ip.dst 181.47.234.63	1
1. filename traff01.exe	5
2. filename newmay4.exe	3
3. filename prestij.exe	2
4. filename newmay5.exe	2
5. filename instal2.exe	2
2. lujipyv.com	21
1. ip.dst 200.104.110.4	1
2. ip.dst 195.174.5.11	1
3. ip.dst 190.18.232.18	1
4. ip.dst 176.121.224.83	1
5. ip.dst 176.117.245.218	1
1. filename ballsof.exe	3
2. filename newmay5.exe	2
3. filename newmay3.exe	2
4. filename userid1.exe	1
5. filename traff01.exe	1
3. paxodvy.com	18
1. ip.dst 188.237.92.153	1
2. ip.dst 186.35.14.49	1
3. ip.dst 178.165.83.157	1
4. ip.dst 178.54.91.165	1
5. ip.dst 176.103.209.160	1
1. filename rasta01.exe	2
2. filename newmay3.exe	2
3. filename khgkg01.exe	2
4. filename ballsof.exe	2
5. filename b0ber01.exe	2
4. urtokzi.com	15
1. ip.dst 92.52.131.81	2
2. ip.dst 219.49.44.1	1
3. ip.dst 200.83.203.239	1
4. ip.dst 188.138.154.163	1
5. ip.dst 176.8.38.76	1
1. filename traff01.exe	4
2. filename angrim2.exe	3
3. filename khgkg01.exe	2
4. filename newmay4.exe	1
5. filename newmay2.exe	1
5. qujatyz.com	13
1. ip.dst 93.79.75.115	2
2. ip.dst 221.154.191.151	1
3. ip.dst 178.165.83.157	1
4. ip.dst 178.54.91.165	1
5. ip.dst 178.44.211.151	1
1. filename newmay2.exe	2
2. filename goodtr1.exe	2
3. filename userid1.exe	1
4. filename traff01.exe	1
5. filename prestij.exe	1
6. puvfuvi.com	12
1. ip.dst 190.100.246.32	1

2. ip.dst 186.218.89.163	1
3. ip.dst 178.150.170.64	1
4. ip.dst 141.138.102.230	1
5. ip.dst 141.101.20.245	1
1. filename angrim2.exe	3
2. filename prestij.exe	2
3. filename newmay2.exe	2
4. filename traff01.exe	1
5. filename rasta01.exe	1
7. nygmygi.com	9
1. ip.dst 176.100.162.121	1
2. ip.dst 98.15.219.203	1
3. ip.dst 93.89.211.216	1
4. ip.dst 92.52.131.81	1
5. ip.dst 87.110.96.177	1
1. filename b0ber01.exe	2
2. filename rasta01.exe	1
3. filename newmay3.exe	1
4. filename moon003.exe	1
5. filename instcod.exe	1
8. xifisyh.com	7
1. ip.dst 176.194.165.168	1
2. ip.dst 159.224.91.130	1
3. ip.dst 115.43.229.135	1
4. ip.dst 98.15.219.203	1
5. ip.dst 95.56.94.193	1
1. filename newmay5.exe	2
2. filename newmay4.exe	2
3. filename rasta01.exe	1
4. filename nothin2.exe	1
5. filename newmay3.exe	1
9. lujiwyt.com	6
1. ip.dst 103.3.82.239	1
2. ip.dst 89.114.116.17	1
3. ip.dst 79.175.240.238	1
4. ip.dst 79.135.180.94	1
5. ip.dst 46.119.217.208	1
1. filename newmay2.exe	2
2. filename instcod.exe	2
3. filename newmay5.exe	1
4. filename goodtr1.exe	1
10. uvlasow.com	5
1. ip.dst 213.231.17.114	1
2. ip.dst 176.36.77.77	1
3. ip.dst 94.153.81.189	1
4. ip.dst 77.123.42.134	1
5. ip.dst 37.115.73.62	1
1. filename rasta01.exe	2
2. filename userid1.exe	1
3. filename ivanp66.exe	1
4. filename boris01.exe	1
11. ushuvap.com	5
1. ip.dst 176.124.13.91	1
2. ip.dst 176.8.230.241	1
3. ip.dst 141.138.102.230	1
4. ip.dst 79.135.180.94	1
5. ip.dst 59.18.216.101	1
1. filename newmay4.exe	2
2. filename newmay2.exe	1
3. filename goodtr1.exe	1
4. filename angrim2.exe	1
12. qohyhodi.us	5
1. ip.dst 202.95.182.235	1
2. ip.dst 110.132.27.30	1
3. ip.dst 109.162.72.108	1
4. ip.dst 77.123.61.154	1
5. ip.dst 5.248.92.4	1
1. filename rasta01.exe	1
2. filename instcod.exe	1
3. filename goodtr1.exe	1
4. filename forav_2.exe	1
5. filename boris01.exe	1
13. ynpabgax.us	4
1. ip.dst 210.148.165.67	1

2.	ip.dst 91.234.73.134	1
3.	ip.dst 87.97.224.40	1
4.	ip.dst 77.123.25.82	1
1.	filename forav_1.exe	2
2.	filename instcod.exe	1
3.	filename forav_3.exe	1
14.	xaylfydy.us	4
1.	ip.dst 193.107.132.19	1
2.	ip.dst 159.224.128.7	1
3.	ip.dst 94.153.18.211	1
4.	ip.dst 84.46.188.241	1
1.	filename rasta01.exe	1
2.	filename instcod.exe	1
3.	filename forav_2.exe	1
4.	filename angrim2.exe	1
15.	toztale.com	4
1.	ip.dst 176.100.80.31	1
2.	ip.dst 109.122.13.92	1
3.	ip.dst 88.222.177.66	1
4.	ip.dst 85.186.41.222	1
1.	filename rasta01.exe	2
2.	filename userid1.exe	1
3.	filename newmay3.exe	1
16.	ohziqtow.us	4
1.	ip.dst 94.244.148.25	1
2.	ip.dst 94.27.79.92	1
3.	ip.dst 46.211.211.235	1
4.	ip.dst 31.129.107.246	1
1.	filename angrim2.exe	2
2.	filename rasta01.exe	1
3.	filename b0ber01.exe	1
17.	lypognen.us	4
1.	ip.dst 123.240.87.174	1
2.	ip.dst 93.170.34.44	1
3.	ip.dst 77.123.29.236	1
4.	ip.dst 46.185.54.105	1
1.	filename goodtr1.exe	1
2.	filename forav_3.exe	1
3.	filename boris01.exe	1
4.	filename b0ber01.exe	1
18.	konaxkex.us	4
1.	ip.dst 141.138.105.155	1
2.	ip.dst 118.233.249.236	1
3.	ip.dst 118.170.42.16	1
4.	ip.dst 77.122.95.250	1
1.	filename angrim2.exe	2
2.	filename newmay3.exe	1
3.	filename goodtr1.exe	1
19.	izejvuz.com	4
1.	ip.dst 176.36.77.77	1
2.	ip.dst 95.180.58.111	1
3.	ip.dst 91.219.80.253	1
4.	ip.dst 24.133.254.184	1
1.	filename traff01.exe	1
2.	filename newmay3.exe	1
3.	filename moon003.exe	1
4.	filename goodtr1.exe	1
20.	hesogfyr.us	4
1.	ip.dst 200.63.37.134	1
2.	ip.dst 178.165.49.141	1
3.	ip.dst 31.133.57.163	1
4.	ip.dst 31.128.110.86	1
1.	filename forav_3.exe	1
2.	filename forav_2.exe	1
3.	filename forav_1.exe	1
4.	filename ballsof.exe	1
21.	xecsonil.us	3
1.	ip.dst 178.74.208.236	1
2.	ip.dst 79.135.211.87	1
3.	ip.dst 31.42.116.202	1
1.	filename forav_3.exe	1
2.	filename forav_1.exe	1
3.	filename b0ber01.exe	1

22. welygwy.com	3
1. ip.dst 125.14.86.43	1
2. ip.dst 116.64.168.227	1
3. ip.dst 46.118.102.145	1
1. filename userid1.exe	1
2. filename rasta01.exe	1
3. filename forav_1.exe	1
23. dusseva.com	3
1. ip.dst 89.44.116.23	1
2. ip.dst 77.127.4.136	1
3. ip.dst 61.70.76.130	1
1. filename khgkg01.exe	1
2. filename ballsof.exe	1
3. filename angrim2.exe	1
24. cytpaxiz.us	3
1. ip.dst 176.63.124.55	1
2. ip.dst 93.77.13.42	1
3. ip.dst 50.72.216.211	1
1. filename userid1.exe	1
2. filename rasta01.exe	1
3. filename angrim2.exe	1
25. xaxwuex.com	2
1. ip.dst 176.8.65.117	1
2. ip.dst 112.197.252.9	1
1. filename prestij.exe	1
2. filename goodtr1.exe	1
26. serelfyh.us	2
1. ip.dst 176.36.109.106	1
2. ip.dst 109.162.59.102	1
1. filename b0ber01.exe	1
2. filename angrim2.exe	1
27. iptaxov.com	2
1. ip.dst 221.188.59.206	1
2. ip.dst 178.172.198.70	1
1. filename rasta01.exe	1
2. filename newmay3.exe	1
28. ighazihy.us	2
1. ip.dst 117.18.153.193	1
2. ip.dst 110.132.27.30	1
1. filename rasta01.exe	2
29. epfusgy.com	2
1. ip.dst 111.254.106.169	1
2. ip.dst 31.129.111.181	1
1. filename rasta01.exe	2
30. ypliheg.com	1
1. ip.dst 178.137.102.242	1
1. filename rasta01.exe	1
31. yjqacce.com	1
1. ip.dst 86.100.243.29	1
1. filename newmay3.exe	1
32. xehokgus.us	1
1. ip.dst 141.170.249.126	1
1. filename b0ber01.exe	1
33. winarfud.us	1
1. ip.dst 77.122.209.75	1
1. filename rasta01.exe	1
34. uzuchuaw.us	1
1. ip.dst 81.22.136.165	1
1. filename dun0001.exe	1
35. tyniliv.com	1
1. ip.dst 69.244.255.163	1
1. filename newmay3.exe	1
36. tunpyyn.com	1
1. ip.dst 94.153.23.243	1
1. filename newmay3.exe	1
37. pozluyw.com	1
1. ip.dst 95.69.208.245	1
1. filename newmay3.exe	1
38. gaanwar.com	1
1. ip.dst 113.255.235.80	1
1. filename newmay3.exe	1
39. enygnaq.com	1
1. ip.dst 2.132.69.80	1
1. filename rasta01.exe	1

40. elkihmes.us	1
1. ip.dst 220.142.125.130	1
1. filename newmay3.exe	1

Rule took 0:0:0.421 to complete. (Actions took 0:0:29.16)

DGA Fastfluxing Kryptik IPs

ip.dst	Session Count
1. 93.79.75.115	5
1. alias.host qujatyz.com	2
2. alias.host vegysca.com	1
3. alias.host urtokzi.com	1
4. alias.host paxodvy.com	1
1. filename traff01.exe	1
2. filename newmay4.exe	1
3. filename newmay3.exe	1
4. filename moon003.exe	1
5. filename angrim2.exe	1
2. 93.79.112.78	3
1. alias.host xifisyh.com	1
2. alias.host urtokzi.com	1
3. alias.host lujipyv.com	1
1. filename newmay4.exe	1
2. filename ivanp66.exe	1
3. filename instcod.exe	1
3. 92.52.131.81	3
1. alias.host urtokzi.com	2
2. alias.host nygmygi.com	1
1. filename traff01.exe	1
2. filename newmay4.exe	1
3. filename forav_3.exe	1
4. 46.119.217.208	3
1. alias.host urtokzi.com	1
2. alias.host nygmygi.com	1
3. alias.host lujiwyt.com	1
1. filename newmay2.exe	1
2. filename moon003.exe	1
3. filename instcod.exe	1
5. 200.83.203.239	2
1. alias.host vegysca.com	1
2. alias.host urtokzi.com	1
1. filename khgkg01.exe	1
2. filename instal2.exe	1
6. 200.59.41.15	2
7. 178.165.83.157	2
1. alias.host qujatyz.com	1
2. alias.host paxodvy.com	1
1. filename userid1.exe	1
2. filename angrim2.exe	1
8. 178.54.91.165	2
1. alias.host qujatyz.com	1
2. alias.host paxodvy.com	1
1. filename newmay5.exe	1
2. filename newmay2.exe	1
9. 176.36.77.77	2
1. alias.host uvlasow.com	1
2. alias.host izejvuz.com	1
1. filename rasta01.exe	1
2. filename goodtr1.exe	1
10. 176.8.230.241	2
1. alias.host ushuvap.com	1
2. alias.host paxodvy.com	1
1. filename goodtr1.exe	1
2. filename ballsof.exe	1
11. 176.8.65.117	2
1. alias.host xaxwuex.com	1
2. alias.host qujatyz.com	1
1. filename newmay2.exe	1
2. filename goodtr1.exe	1
12. 141.138.102.230	2
1. alias.host ushuvap.com	1
2. alias.host puvfuvi.com	1
1. filename newmay4.exe	1
2. filename boris01.exe	1

13. 110.132.27.30	2
1. alias.host qohyhodi.us	1
2. alias.host ighazihy.us	1
1. filename rasta01.exe	1
2. filename instcod.exe	1
14. 98.15.219.203	2
1. alias.host xifisyh.com	1
2. alias.host nygmygi.com	1
1. filename newmay5.exe	1
2. filename angrim2.exe	1
15. 94.153.63.162	2
1. alias.host vegysca.com	1
2. alias.host urtokzi.com	1
1. filename traff01.exe	1
2. filename newmay3.exe	1
16. 93.177.169.149	2
1. alias.host paxodvy.com	1
2. alias.host lujipyv.com	1
1. filename moon003.exe	1
2. filename instcod.exe	1
17. 93.79.45.10	2
1. alias.host qujatyz.com	1
2. alias.host paxodvy.com	1
1. filename goodtr1.exe	1
2. filename b0ber01.exe	1
18. 89.44.116.23	2
1. alias.host paxodvy.com	1
2. alias.host dusseva.com	1
1. filename newmay3.exe	1
2. filename khgkg01.exe	1
19. 88.135.139.58	2
1. alias.host puvfuvi.com	1
2. alias.host lujipyv.com	1
1. filename traff01.exe	1
2. filename newmay2.exe	1
20. 87.110.96.177	2
1. alias.host vegysca.com	1
2. alias.host nygmygi.com	1
1. filename rasta01.exe	1
2. filename b0ber01.exe	1
21. 79.135.180.94	2
1. alias.host ushuvap.com	1
2. alias.host lujiwyt.com	1
1. filename newmay4.exe	1
2. filename goodtr1.exe	1
22. 77.123.42.134	2
1. alias.host vegysca.com	1
2. alias.host uvlasow.com	1
1. filename prestij.exe	1
2. filename boris01.exe	1
23. 46.211.59.59	2
1. alias.host qujatyz.com	1
2. alias.host nygmygi.com	1
1. filename b0ber01.exe	2
24. 46.149.187.135	2
1. alias.host vegysca.com	2
1. filename traff01.exe	1
2. filename newmay5.exe	1
25. 37.221.131.154	2
1. alias.host vegysca.com	1
2. alias.host urtokzi.com	1
1. filename traff01.exe	2
26. 31.170.154.120	2
1. alias.host vegysca.com	1
2. alias.host nygmygi.com	1
1. filename traff01.exe	1
2. filename rasta01.exe	1
27. 24.133.254.184	2
1. alias.host paxodvy.com	1
2. alias.host izejvuz.com	1
1. filename newmay3.exe	1
2. filename khgkg01.exe	1
28. 221.188.59.206	1

1. alias.host iptaxov.com	1
1. filename newmay3.exe	1
29. 221.154.191.151	1
1. alias.host qujatyz.com	1
1. filename userid1.exe	1
30. 220.142.125.130	1
1. alias.host elkihmes.us	1
1. filename newmay3.exe	1

Rule took 0:0:0.405 to complete. (Actions took 0:0:20.857)

Total Kryptik DGA Domains

	# of Values
Total number of unique values	40

Rule took 0:0:0.46 to complete. (Actions took 0:0:0.0)

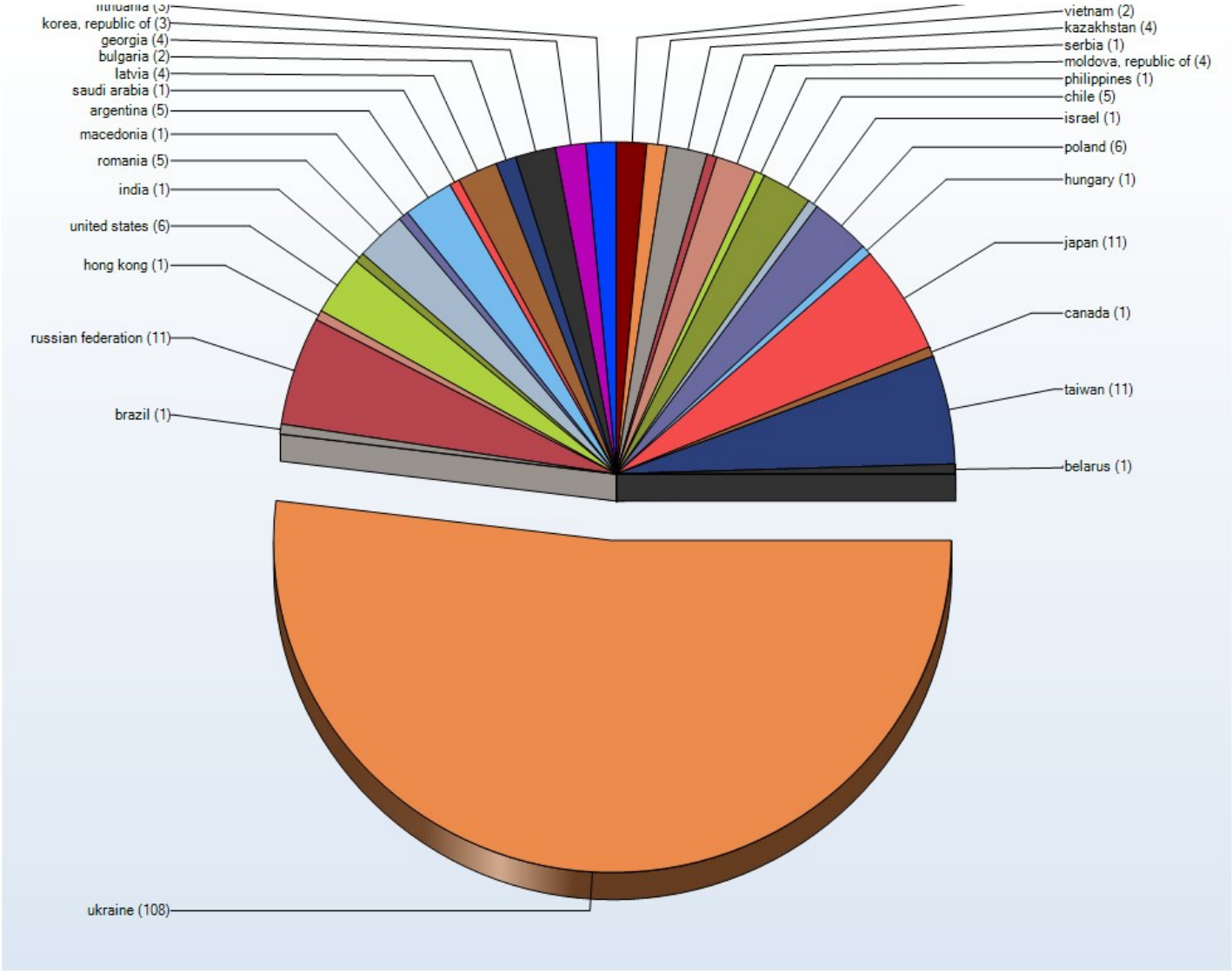
Total Kryptik DGA IPs

	# of Values
Total number of unique values	178

Rule took 0:0:0.421 to complete. (Actions took 0:0:0.0)

The bulk of the IP space is Ukrainian and Russian. A breakdown of the distribution of this dynamically generated domain botnet is shown below.

DGA Fastfluxing Kryptik Country Distro



Rule took 0:0:0.405 to complete. (Actions took 0:0:0.0)