Annex ? – Fast Flux Metrics

Martin Hall 12/1/08 10:38 AM
Deleted: II

A number of organizations have been collecting data about fast fluxing domains. The methods and data used to detect and monitor fluxing domains vary, but each data set provides unique graphical perspectives on the scope of the issue.

The data sets presented here are based on separate research activities by Arbor and Karmasphere and include:

- New Fluxing Domains Detected by Date
- Total Number of Fluxing Domains by Date
- Total Number of Fluxing Domains by TLD
- Number of Fluxing Domains per 10,000 registered domains by TLD

Key observations:

- Fast Flux is a sustained problem.
- Take downs have a temporary impact but miscreants move to other hosting environments.
- The problem is not limited to one TLD, or to gTLD or CCTLD.
- By domain volume, the largest numbers of fluxing domains have been detected in .CN, .COM and .NET.

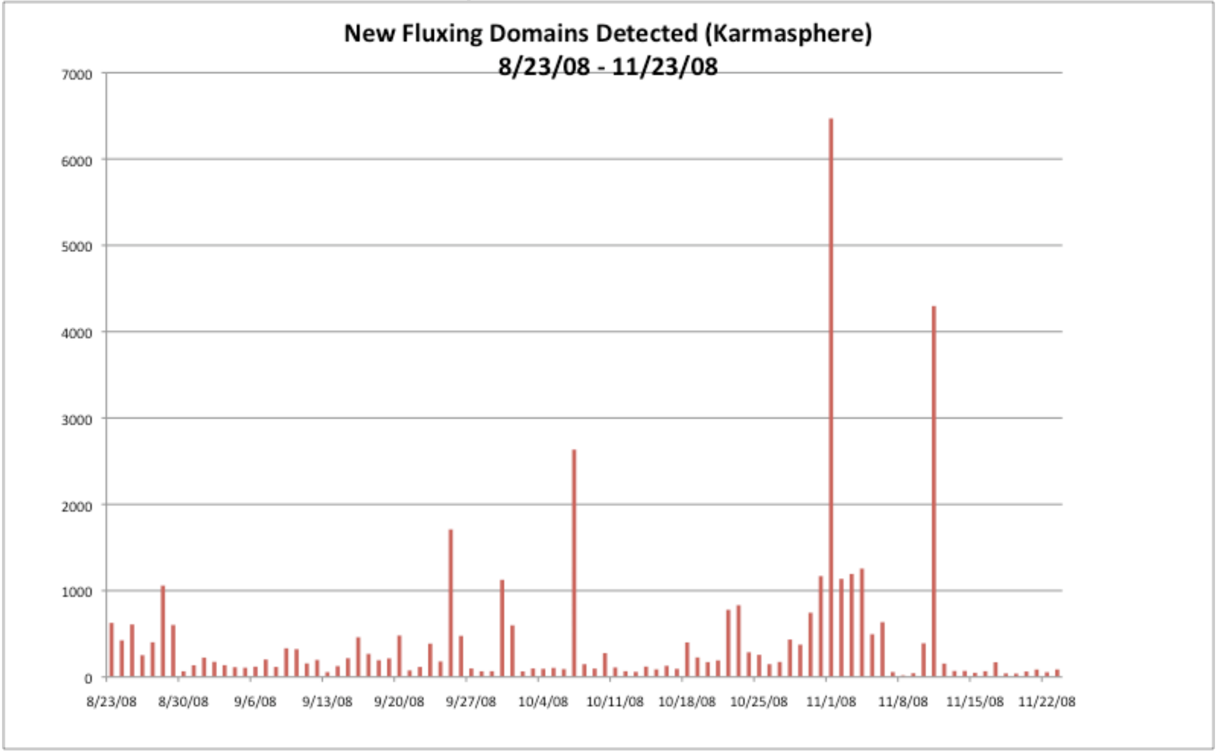
New Fluxing Domains Detected by Date

Graphs 1 and 2 illustrate the number of new domain names used in fluxing attacks each day over a period of three months. "New" means that the domains had not been previously identified by Karmasphere or Arbor's monitoring efforts as actively used in a fluxing attack. The Y-axis represents the total number of domains, ranging from 1 (various dates) to a peak in 6465 on 1 November 2008 (Karmasphere) and 3695 on 8 October (Arbor).

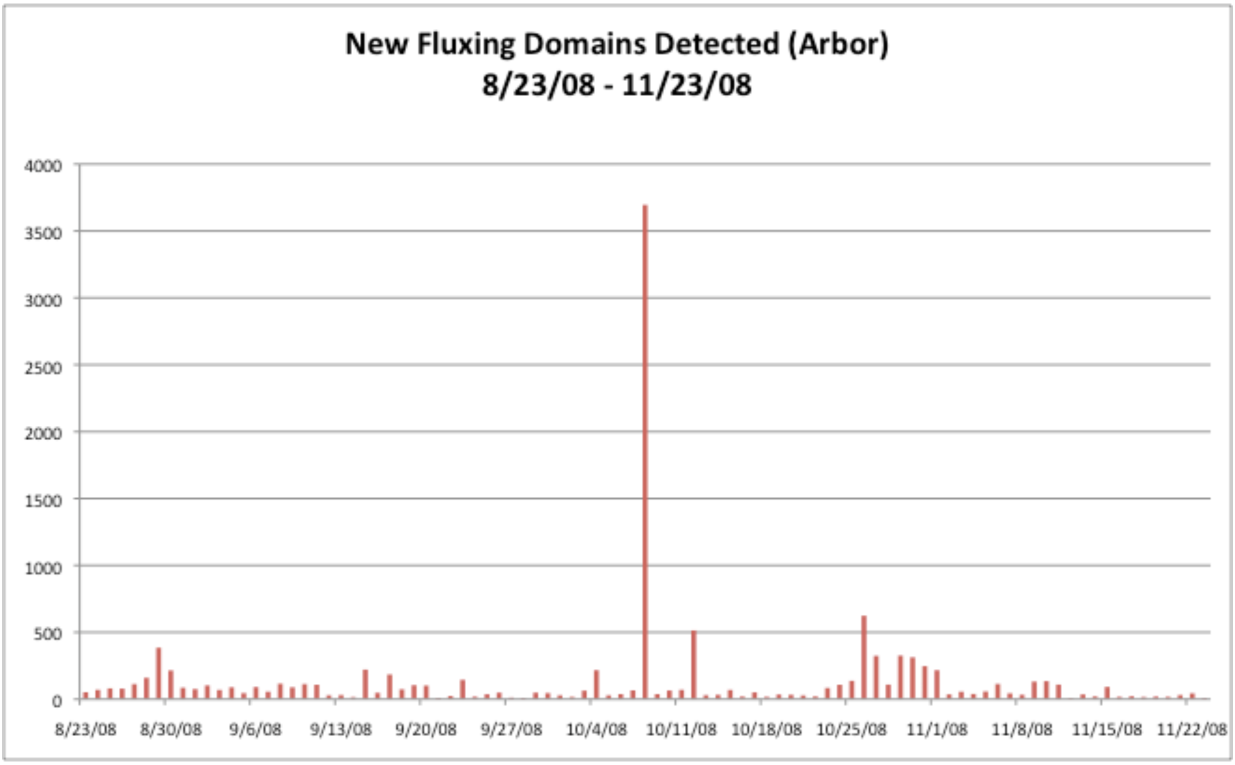
The spike on November 1 2008 in Karmasphere's detections came from an injection of a large number of .CN domains into the largest fast flux botnet being tracked by Karmasphere.

The average number of new fluxing domains detected by Karmasphere was 361 domains/day. The median was 133 domains/day.

Graph 1


New Fluxing Domains Detected (Karmasphere)
8/23/08 - 11/23/08
7000
6000
5000
4000
3000
2000
1000
0
8/23/08
8/30/08
9/6/08
9/13/08
9/20/08
9/27/08
10/4/08
10/11/08
10/18/08
10/25/08
11/1/08
11/8/08
11/15/08
11/22/08

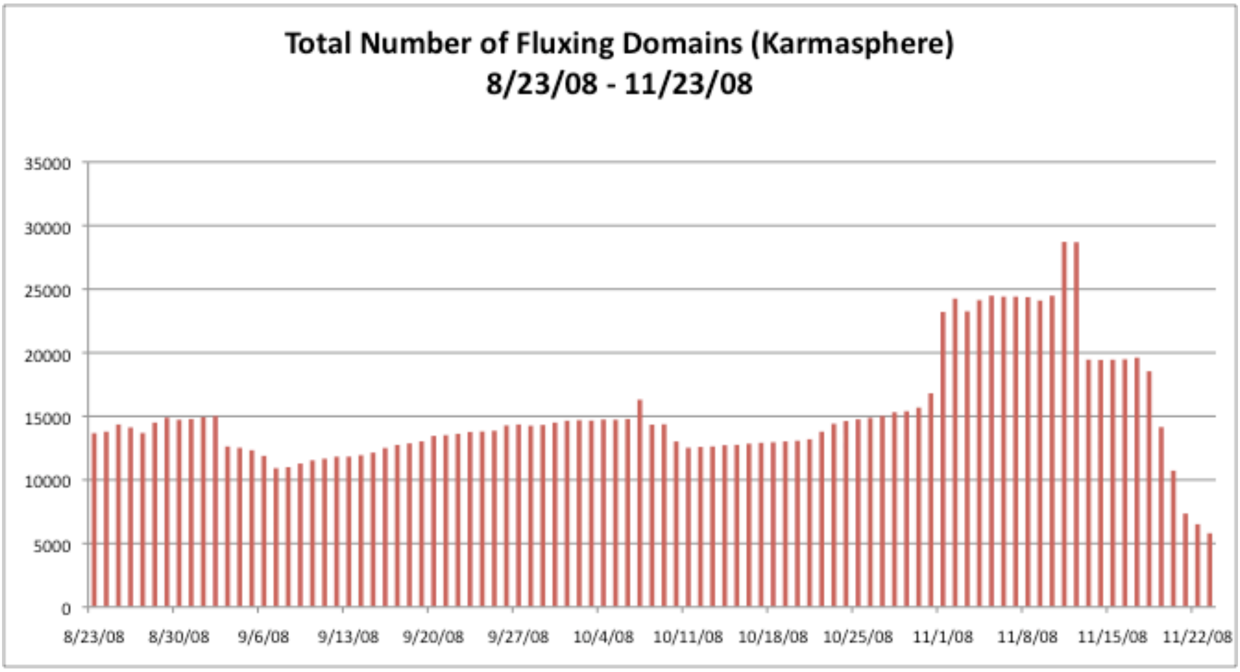
Graph 2


New Fluxing Domains Detected (Arbor)
8/23/08 - 11/23/08
4000
3500
3000
2500
2000
1500
1000
500
0
8/23/08
8/30/08
9/6/08
9/13/08
9/20/08
9/27/08
10/4/08
10/11/08
10/18/08
10/25/08
11/1/08
11/8/08
11/15/08
11/22/08

Total Number of Fluxing Domains by Date

Graph 3 illustrates the total number of fluxing domains used in fluxing attacks each day over a period of three months. For each day of the measurement period, this graph illustrates the sum of the domain names detected to date that continue to resolve using DNS and continue to exhibit malicious fluxing characteristics. The graph illustrates the persistent nature of fluxing attack networks.

Graph 3



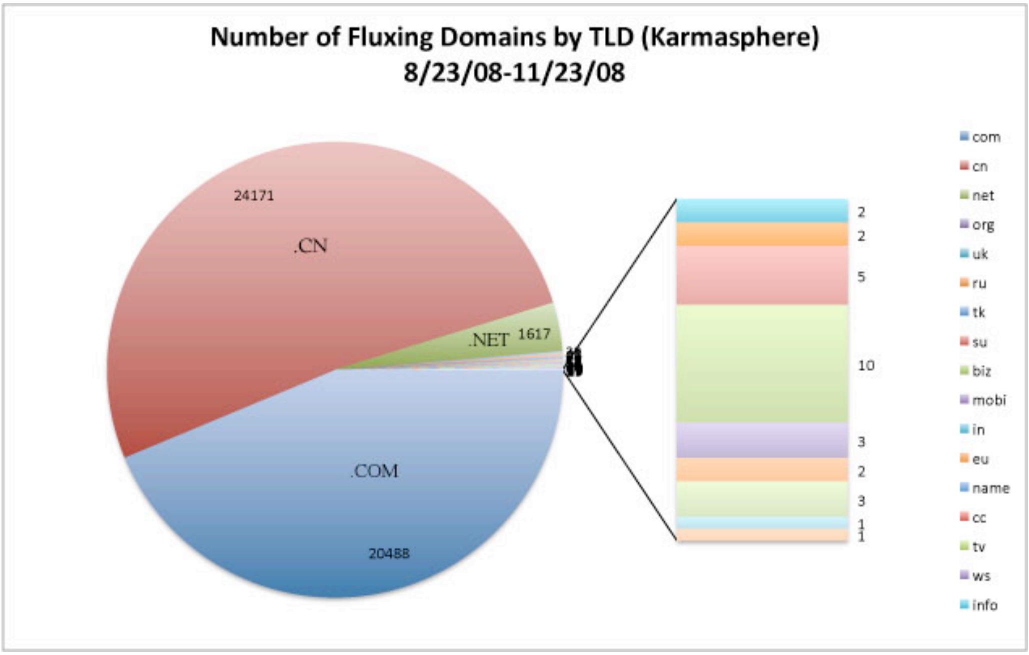
Fluxing Domains Detected by TLD

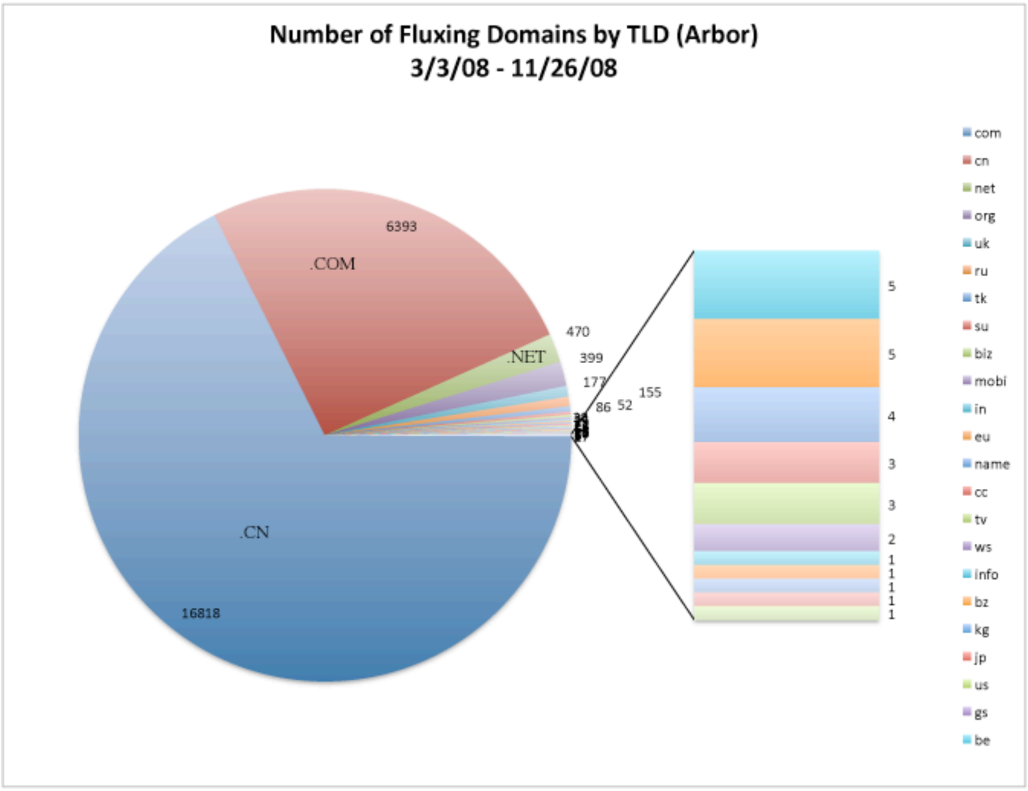
The pie charts illustrate the distribution of fluxing domains by TLD and include both generic and country-code TLDs.

During Karmasphere's three month measurement period, the largest concentration of fluxing domains discovered by Karmasphere were in the China (CN) TLD, representing 52% of overall fluxing domains. The second largest concentration was found in .COM (44 %).

During Arbor's eight month measurement period, the largest concentration of fluxing domains discovered by Arbor were in the generic .COM TLD, representing 68% of overall fluxing domains. The second largest concentration was found in .CN (26%).

The pie charts illustrate absolute counts. This does not take into consideration the total number of registered domains per TLD, and thus may not be the most accurate way to determine the incidence of fluxing domains of any TLD relative to others.




Number of Fluxing Domains by TLD (Arbor)
3/3/08 - 11/26/08
.CN
16818
.COM
6393
.NET
470
399
177
155
86
52
5
5
4
3
3
2
1
1
1
1
1
com
cn
net
org
uk
ru
tk
su
biz
mobi
in
eu
name
cc
tv
ws
info
bz
kg
jp
us
gs
be

Fluxing Domains Detected Proportionately by TLD

Using a useful metric used by the Anti Phishing Working Group in their “Global Phishing Survey: Domain Name Use and Trends in 1H2008” (See: www.antiphishing.org/reports/APWG_GlobalPhishingSurvey1H2008.pdf), the number of fluxing domains were analyzed to see how many fell into which TLDs. The absolute counts by TLD are interesting, but the sizes of the various TLDs vary widely. To place the numbers in context and measure the prevalence of fluxing in a TLD, we use the Metric “Fluxing Domains per 10,000”.

“Fluxing Domains per 10,000” is a ratio of the number of fluxing domain names in a TLD to the number of registered domain names in that TLD. This metric is a way of revealing whether a TLD has a higher or lower incidence of fluxing relative to others.

The following tables show only those TLDs that have at least 10 fluxing domains, at least 10,000 registered domains and one or more fluxing domains per 10,000 domains registered in that TLD.

Top 7 Fluxing TLDs by Score (Karmasphere)

Rank	TLD	TLD Location	Number of Fluxing Domains	Domains in Registry (July 08)	Score: Fluxing per 10,000 registered domains
1	.CN	China	24171	12,364,615	19.55
2	.SU	Soviet Union	42	68,891	6.10
3	.BZ	Belize	19	43,500	4.37
4	.COM	Generic TLD	20488	78,191,881	2.62
5	.NET	Generic TLD	1617	11,903,723	1.36
6	.ME	Montenegro	10	95,007	1.05
7	.ASIA	Pan Asia/Asia Pacific	21	209,722	1.00

Top 5 Fluxing TLDs by Score (Arbor)

Rank	TLD	TLD Location	Number of Fluxing Domains	Domains in Registry (July 08)	Score: Fluxing per 10,000 registered domains
1	.SU	Soviet Union	52	68,891	7.55
2	.CN	China	6,393	12,364,615	5.17
3	.BZ	Belize	14	43,500	3.22
4	.COM	Generic TLD	16,818	78,191,881	2.15
5	.RU	Russian Federation	155	1,535,153	1.01