Real-Time Detection of Fast Flux Service Networks

Alper Caglayan, Mike Toothaker, Dan Drapeau, Dustin Burke and Gerry Eaton
Milcord LLC
{acaglayan, mtoothaker, ddrapeau, dburke, geaton}@milcord.com

Abstract

Here we present the first empirical study of detecting and classifying fast flux service networks (FFSNs) in real time. FFSNs exploit a network of compromised machines (zombies) for illegal activities such as spam, phishing and malware delivery using DNS record manipulation techniques. Previous studies have focused on actively monitoring these activities over a large window (days, months) to detect such FFSNs and measure their footprint. In this paper, we present a Fast Flux Monitor (FFM) that can detect and classify a FFSN in the order of minutes using both active and passive DNS monitoring, which complements long term surveillance of FFSNs.

1. Introduction

ICANN describes fast flux as 'rapid and repeated changes to host and/or name server resource records, which result in rapidly changing the IP address to which the domain name of an Internet host or name server resolves'.[1] While fast flux methods do have a legitimate use as a load balancing technique for high availability and high volume Web sites such as Internet search engines and in Content Distribution Networks (CDN), fast flux has come to be associated more for its malicious use as a means of concealing the mothership (Command and Control - C&C server) using compromised machines (botnet 'zombies'). Hence, fast flux is a strong indicator of botnets, which is in effect a stealth and adaptive network of sleeper cells that can be programmed to carry out almost any large scale cyber attack such as DDoS, spam, phishing, malware delivery and exfiltration.

In fast flux, numerous (as many as thousands) IP addresses are associated with a single domain name and rapidly fluxed. It is a technique often used by botnet operators to evade identification, provide high availability and load-balancing, and foil takedown. Fast flux is considered the state-of-the-art in botnet infrastructure and is used to support multiple classes of cyber-attacks (denial of service, phishing, spam, malware injection, and exfiltration). There are three main variants of fast flux hosting: (1) basic fast flux hosting where IP addresses of malicious web sites are fluxed, (2) Name Server (NS) fluxing where IP addresses of DNS name servers are fluxed, and (3) double flux, where IP addresses of web sites and name servers are fluxed.[2] While fast-flux botnets share the same techniques as traditional IRC-based botnets, the Command and Control (C&C) of fast-flux botnets, "almost without exception", is HTTP-based.[3]

It has been estimated that as many as 10% of all PCs unknowingly operate as a drone or zombie in a botnet army. One of the most powerful botnets to date, Storm, employs fast-flux methods, while the RSA FraudAction team reports that "the Rock Phish gang has moved its infrastructure ... from its traditional botnet to the fast-flux infrastructure of the infamous Asprox botnet".[4] Dietrich, describing the Estonian attacks as a simple preview of more sophisticated attacks to come, says that fast flux evasion could make botnets "unstoppable" and notes their potential for helping "botnets evade detection in a military or political attack".[5] Internet Business Law Services (IBLSO) reports that these methods are being adopted by Jihadist cyber terrorists.[6]

There are a number of excellent articles that provide an overview of the botnet problem. For instance, CRS Report for Congress[7] spells out the vulnerabilities to botnets and policy issues for the Federal Government. The Honeynet Project paper[8] presents a high level technical overview of botnets, and discusses methods for tracking botnets. ENISA (European Network and Information Security Agency) position paper[9] presents the infection vectors of bots and provides recommendations for policy makers, infrastructure operators and end users. Li and Liao present an economic model of the botnet ecosystem

978-0-7695-3568-5/09 $25.00 © 2009 IEEE
DOI 10.1109/CATCH.2009.44

(i.e. botnet masters, renters, etc.), and propose a novel mitigation technique using virtual bots as defenders.[10]

The closest published works to our research are the ISOC Network and Distributed System Security Symposium (NDSS) paper on measuring and detecting fast flux service networks[11] and the FluXOR paper on detecting and monitoring fast-flux service networks[12]. The ISOC paper uses a direct DNS monitoring approach over seven weeks of collected data, and is based on building a linear classifier using a flux score, which is a function of number of unique A records in all lookups, number of NS records in a single lookup, and number of unique ASNs (Autonomous System Number). The FluXOR method collects domains from spam emails in honeypots, monitors their DNS over a period of 3 hours and uses a trained Naïve Bayes classifier to classify as benign or fast-flux. Our approach complements this research in that we focus on the real time (within minutes) detection and classification of fast flux service networks using both active and passive DNS monitoring. In addition, our approach is able to differentiate and classify all three fast-flux variants, including name server flux and double-flux.

2. Technical Approach

In this section, we begin with an introduction to the challenges we address, our technical architecture, and describe the operation of the main components in our architecture.

2.1. Fast Flux Challenge

Technical challenges associated with Fast Flux include monitoring changes to DNS records, classification of historical behavior, real time detection, and differentiation from legitimate behavior. One challenge in detection is that some of the behaviors that indicate fast flux are intermittent. Therefore, detection requires persistent surveillance, which creates computational and data challenges at large scale. We illustrate this particular challenge in Figure 1, which shows the cumulative number of unique IPs that resolve to a given fast flux domain on the y-axis, and the temporal sampling period on the x-axis. At the end of the observation period, it is relatively easy to see that this is a fast flux service network of about 110 bots after only 24 hours, as legitimate CDNs (Content Delivery Network) and high availability Web sites do not employ such a large number of IPs for their domain names. Since our interest is real-time detection of the fast flux service network, we would like to be able to detect fast flux activity during steeper grades of the slope while waiting for evidence of activity at the flatter grades.

The detection algorithm should not produce false alarms for legitimate behavior of high availability Web sites that use round robin DNS. This method is typically used to distribute the load of incoming requests among several servers at a given location. CDNs extend this load balancing by distributing the load among servers distributed across the globe. From a DNS monitoring perspective, this behavior may look like fast flux behavior, and needs to be accounted for in the detection algorithm.

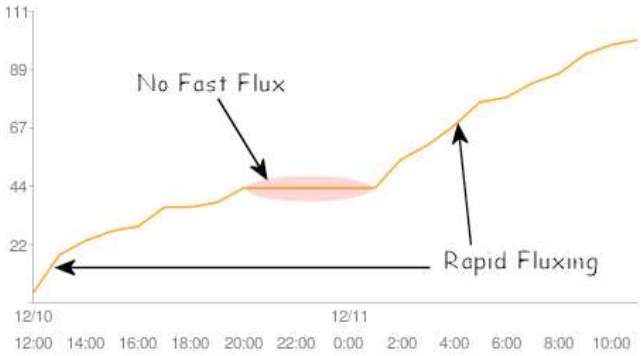


Figure 1. 24 hours in the life of a fast flux domain

2.2. Fast Flux Monitor Architecture

Our Fast Flux Monitor (FFM) is a Web service application prototype designed to detect whether a domain exhibits fast flux (FF) or double flux (DF) behavior. The primary technical components of FFM include: (1) sensors which perform real-time detection of FF service networks using behavioral analysis that examine various indicators, (2) a database of known FF service networks – zombie IPs used for domain names, nameservers, and (3) analytical knowledge harvested from the database, which can include: (i) the fast flux service network's size and growth rate estimates , (ii) the social network of a fast flux service network where IPs are shared by different fast flux service networks, (iii) the footprint of a fast flux service network for a given enterprise, (iv) the footprint of a fast flux service network for a given ISP, and (v) the footprint of a fast flux service network for a given country. To provide the scale needed by such an application, we have

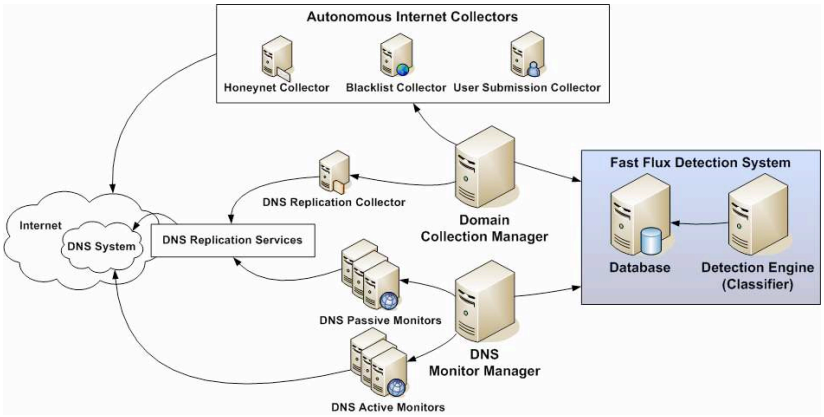


Figure 2. FFM Architecture

implemented FFM using a distributed architecture as shown in the Figure 2.

2.2. FFM Active Sensors

We have developed three active sensors for our FFM active sensors: (1) Time To Live (TTL), (2) FF Activity Index and (3) Footprint Index. In active monitoring, we perform DNS lookup with `dig`, and record the A records returned with each query. Every A record has a TTL field, which specifies the time interval in seconds that the response remains valid. Although the RFC recommends minimum TTL in terms of days, most legitimate high availability sites employ TTL values between 600 – 3,600 seconds. In contrast, fast flux service networks typically employ TTL values of less than 300 seconds. Table 1 shows the TTL of some known FFSNs and legitimate sites. It is clear that a classifier built on TTL measurement would not function with an acceptable false alarm rate as Akamai and IronPort have TTL values similar to FFSNs. Similarly, some FFSNs have TTL values comparable to those for legitimate sites, thus indicating the need for additional sensors for classifier input. Our FF Activity Index captures how aggressively the domain's DNS information changes.

Figure 3 shows the Fast Flux Activity Index, in the form of a sparkline, for a known fast flux domain involved in the Canadian Pharmacy family of spam. We chose to use a sparkline plot to display the monitored behavior as evidence. Fast Flux Activity Index for domains is a short term statistic of the change in unique A records over a moving window of 10 minutes.The use of a sparkline[16] gives us the ability to show large amounts of data in a small space. As can be seen in Figure 3 where we have shown approximately an hour's worth of classifications in what amounts to a 60 pixel by 20 pixel image. As can be seen in Figure 5, the use of sparklines allows for the displaying of more data on the screen without losing significant data evidence.

For nameservers, we perform `dig` in order to resolve a set of nameservers. For each nameserver, we perform an `nslookup` in order to resolve the set of IP addresses associated with the nameservers. We then query our database to see if any of the resultant IP addresses have been associated with other domains we have been monitoring. According to our research, fast flux activity occurs much slower at the nameserver level, sometimes as slow as once every 12-24 hours. Known safe domains had no change after weeks of monitoring.

Table 1. Comparison of FF and HA sites.

Fast Flux Sites		High Availability Sites	
Domain	TTL	Domain	TTL
safecause.com	120	google.com	300
mp3for-you.com	60	yahoo.com	300
gty5.ru	600	microsoft.com	3600
electricshore.com	120	ironport.com	20
entryrxshop.com	300	att.com	60
towardplain.com	120	akamai.net	180

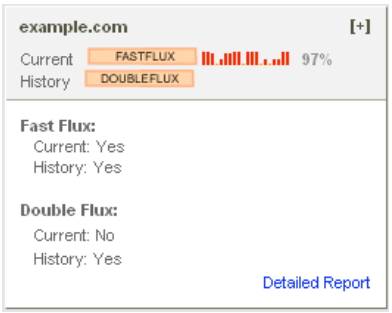


Figure 3. Example fast flux portlet

Figures 4a and 4b show the Footprint Indexes for typical legitimate and fast-flux domains, respectively. The Footprint Index captures the global dispersion of the fast flux service network similar to the ISOC indicator, which uses the number of unique ASNs for all A records. Since the infected machines of a fast flux service network are typically distributed across different ISPs in different countries, a high dispersion value indicates the presence of a FFSN. Generally, a value greater than 6 indicates a domain exhibiting fast flux behavior. If the index is zero, then the domain is currently inactive. Looking again at Figures 4a and 4b, one can see that in Figure 4a there are two distinct clusters indicating that all of the IPs associated with the domain being monitored fall into those two groups. On the other hand Figure 4b shows an example of a FFSN, where the IPs are distributed over the entire range of possible values.

Figure 4a – Legitimate Footprint Index

Figure 4b – Fast-flux Footprint Index

While it might seem that a single sensor, such as the Footprint Index, could be used alone to detect fast flux, the accumulation of this footprint takes time. Hence, the fusion of multiple sensors using a Belief Network yields better performance in detecting FFSNs in real time.

Our active monitors are set up to accept input from a general set of feeds. With this in mind we are currently getting feeds of domains from places like phishtank.com, malwaredomains.com, and shadowserver.org, alone with our own spam traps.

2.3. Passive DNS Sensors

Passive DNS sensors replicate the functionality of active FFM sensors by leveraging DNS replication services. OMB's August 22 memorandum mandates that the U.S. federal government "deploy DNSSEC to the top level .gov domain by January 2009. The top level .gov domain includes the registrar, registry, and DNS server operations."[13] The mandate is motivated in part by the recent publication by security researcher Dan Kaminsky regarding the vulnerability of the DNS infrastructure to cache poisoning attacks.[14]

DNS data is divided into zones. Each zone is served by a set of authoritative name servers, which provide authoritative answers for data contained in the zones they serve. The resolver is another type of name server, which returns non-authoritative answers to clients. Resolvers start at the root servers and follow zone delegations until reaching the final authoritative name server for the correct zone.

As many registrars for second-level domains let domain owners edit zone files, it is easy to add DNS records to a zone, and create new zones. Currently, there are no safeguards to ensure that the resource records only point to the zone owner's domain names and IP address. These deficiencies in DNS infrastructure allow the adversaries to design, develop, and launch malware delivery, spam, and phishing attacks. Passive DNS replication[15] can be used in defending against such attacks.

A typical DNS replication architecture consists of the following processes:

- A sensor captures DNS packets on the network, filters (e.g. only authoritative answers), and forwards the remaining packets to an analyzer
- An analyzer parses the DNS packets and extracts the data for further processing (e.g. domain names, IP addresses)
- A collector takes the analyzer output and updates the DNS data in memory
- A query processor executes user-supplied queries on the data in memory, and broadcasts the results in channels.

In essence, DNS replication services provide the same measurements as the active FFM sensors albeit at a non-uniform sampling period based on user queries. In our approach, the responses from authoritative servers are transformed into a format that takes into account the non-uniform sampling period.

2.4. Analytic Sensors

Analytic sensors are derived from our cumulative collection of observed activities. We have developed a

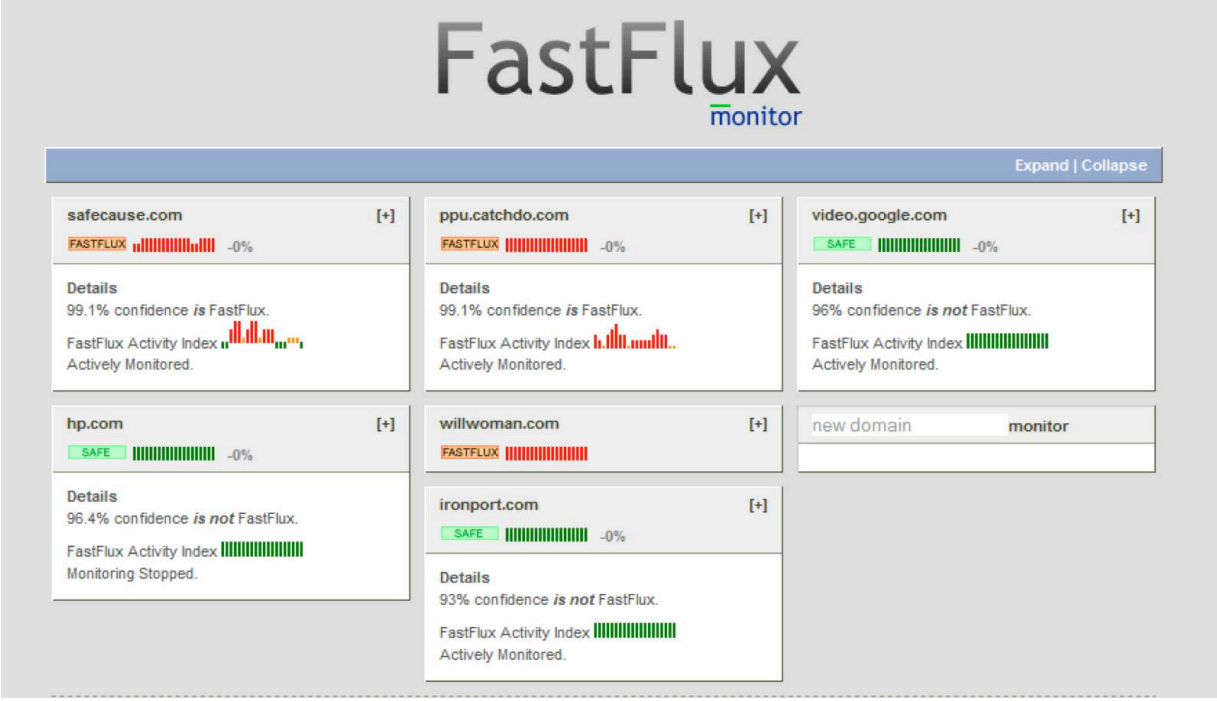


Figure 5. FFM Dashboard

number of such sensors that include 'Guilt by Association' and 'IPs Sharing Fast Flux Domain' sensors. The 'Guilt by Association' sensor examines if any of the current IP addresses of a domain have previously been associated with another fast flux domain. Any 'safe' domain should not have any IP addresses at any given time that are on the fast flux blacklist. The utility of this sensor will increase as the fast flux service network database grows. The 'IPs Sharing Fast Flux Domain' sensor resolves a set of IP addresses associated with a given domain and for each IP address, it queries the database and returns the count of fast flux domains that have also been associated with the IP address. The fast flux count for each IP address is summed together and the total is returned.

2.5. FFM Classifier

We used a Bayesian belief network to build a classifier that fuses the multiple active and passive DNS sensors. This Bayesian classifier is trained to accept the TTL, Fast Flux Activity Index, and Footprint Index values to generate a probabilistic assessment of the presence of a fast flux service network. For instance, in Figure 3, FFM classifier declares that the domain is exhibiting fast flux behavior with a confidence of 97%.

In our methodology, we lock the false alarm rate over the training set, and analyze the probability of miss detection. If probability of missed detection is a acceptable, then we release the classifier to assess the live data. Each week the training data is appended with newly observed cases, and the classifier is retrained, and released into production. The results are then combined with the results from a similar Belief Network working with nameserver data to make a double flux assessment.

Due to the difference in fast flux behavior at the domain level and nameserver level, a different Bayesian classifier is employed that gives a prediction and confidence of fast flux for each nameserver.

4. Empirical Results

In this section, we present sample results that show the capabilities of the implemented prototype.

4.1. FF Monitor Dashboard

Figure 5 shows the dashboard of the implemented Fast Flux Monitor, which gives a high level assessment of the fast flux behavior for monitored sites for a given user, and provides a UI construct to specify new sites to be monitored. In this instance, safecause.com, ppu.catchdo.com and willwoman.com are declared as exhibiting fast flux behavior. In contrast, ironport.com, which provides CDN services, hp.com, and video.google.com are declared not fast flux.

Current	History
The domain electricshore.com is not currently exhibiting fast flux behavior and is currently inactive. Last checked on October 22, 2008 at 08:27:11 PM. Last detected fast flux behavior on October 9, 2008 at 09:55:36 PM.	Since July 1, 2008 electricshore.com has been monitored for a total of 88 days. Fast flux behavior was first detected on July 1, 2008. During the surveillance period, our monitor has detected fast flux 74% of the time and double flux 24% of the time.

Figure 6. Detailed Report: Current vs. History

4.2. FF Monitor Reports

Clicking on the Details link in the FFM dashboard enables the user to review the detailed reports for the domains and nameservers as shown in Figures 6 and 9. Figure 6 shows the detailed report for a domain exhibiting fast flux behavior. The report details bot current and historical behavior. For instance, this site, which is currently dead, has been monitored for about 3 months during which it exhibited fast flux 74% of the time, and double flux 24% of the time.

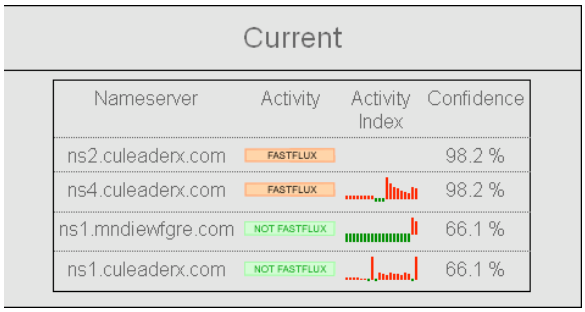


Figure 7. Example current nameserver activity

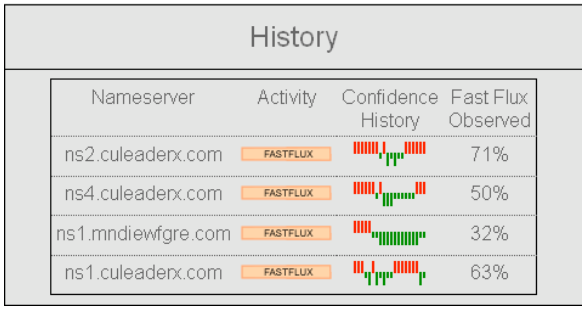
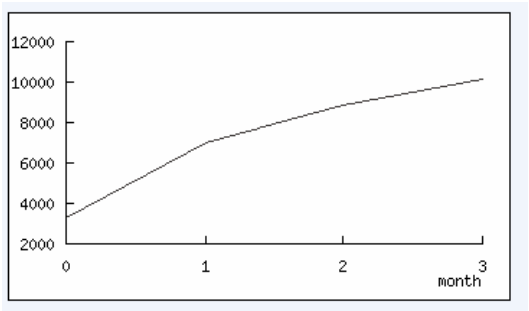


Figure 8. Example historical nameserver activity

Figures 7 and 8 show detailed reports on the nameservers associated with a double flux domain. As can be seen in Figure 7, two of the four nameservers are exhibiting fast flux behavior. Figure 8 shows that all four of the nameservers have exhibited fast flux at some time.

4.3. FFM Analytics

The FFM analytics report shown in Figure 9 describes the service network size and growth rate assessed by the FFM Monitor with respect to the universe of fast flux service networks in the database. For instance, electricshore.com is a large fast flux service network with a fast growth rate. The Network Growth chart plots the number of zombies for the botnet in question in order to give a visual indication of the fast flux service network growth over the monitored time interval. The Fact Sheet lists the network size, growth rate, number of domains sharing the IP addresses, nameserver count, and number of domains sharing nameservers. Figure 10 shows a pie chart for the country and ISP footprint distributions included in the detailed report for the domain.



FACT SHEET
Network Size: 10132 unique IP addresses
Growth Rate: 3896.9 unique IP addresses/month
Days Monitored: 88
Domains Sharing IP Addresses: 288
Nameserver Count: 16
Domains Sharing Nameservers: 0

Figure 9. Detailed Report – Footprint, Growth

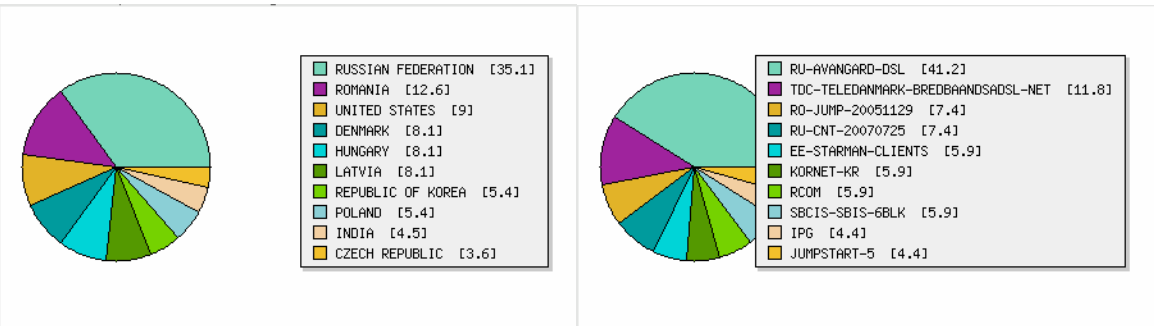


Figure 10. Country and ISP footprint

4.4. Detection Accuracy

Over the course of several weeks, we obtained an average empirical probability of detection of 96.6% over a 10-minute sampling interval after setting the probability of false alarm rate to 5% on the training data each week. In our evaluation, we count each decision of the classifier performed every 10 minutes as a separate test. For instance, if we are monitoring a fast flux domain for 24 hours, this involves 144 classifier tests. If the classifier misses the fast flux domain in only 5 tests, we declare 96.6% probability of detection. In an operational environment, analyst would start investigating such a domain long before 139 tests that yield a fast flux decision. In summary, our performance evaluation is conservative, the effective probability of detection would converge to 100% as more and more 10-minute monitoring windows are accumulated in the database, verifying the assertion of long term monitoring research reported in [11], [12].

Our initial datasets were mostly populated with spam domains as our data indicates spam domains are most likely to use fast flux. We came to the initial false alarm rate by manually analyzing a selection of domains. This collection of domains was created to mimic real world percentages representing the top countries responsible for the worlds spam shown in Table 2. This dataset was then split by a 80/20 training/testing ratio. Then while we were developing our Belief Networks, we used these two datasets for improving our predictions based on a given false alarm rate.

Table 2. Top 10 Spam Origin Countries[1]

	Country
1	United States
2	China
3	Russian Federation
4	United Kingdom
5	South Korea
6	Germany
7	Brazil
8	India
9	Japan
10	France

4.5. FF Monitor Database

Table 3 shows the number of spam, phishing, and malware zombies, and C&C servers used for the study. Phishing and malware domains are collected from phishtank.com and malwaredomains.com whereas C&C servers are collected from shadowserver.org. We have built our own spam honeypot to collect spam domains, which are combined with feeds from other locations.

Table 3. Study Counts

Type	Total(count)
Malware	22,556
Spam	21,015
CnC	1,607
Phishing	17,006
Unknown	31,374
Manually Entered	614

[1] Source: spamhaus. December 9, 2008

9. Conclusions and Future Work

In this paper, we presented a Fast Flux Monitor for real time detection of fast flux service networks based on using both active and passive DNS monitoring. Our approach uses active and passive sensors derived from DNS monitoring, and fusing the component sensors using a Bayesian classifier. Empirical results show that Fast Flux Monitor can detect single and double flux behavior in real time with operationally acceptable probability of detection and false alarm rates. Our empirical results demonstrate that the collected fast flux database can be effectively queried to build automated reports for the security analyst.

Our current research is focused on the implementation of a scalable distributed architecture. We intend to extend our research to classification (spam, phishing, malware) of zero day fast flux service networks.

Acknowledgements

This research was supported by Department of Homeland Security, Science and Technology Directorate Cybersecurity R&D program.

10. References

[1] ICANN. GNSO Issues Report on Fast Flux Hosting, March 2008.
[2] ICANN Security and Stability Advisory Committee. SAC 025: SSA Advisory on Fast Flux Hosting and DNS, March 2008.
[3] "Know Your Enemy: Fast-flux Service Networks", The Honeynet Project and Research Alliance, July 13, 2007.
[4] Prince, B. " Phishing Cyber Gang Upgrades to Fast Flux Botnet, eWeek, Sept 5, 2008.
[5] Knight, G. "Cybercrime is in a State of Flux", The Guardian. March 27, 2008.
[6] O'Connell, K. "Internet Law - Islamic Terrorist Software Released to Cloak Jihadist Communications", Internet Business Law Services, January 30, 2008.
[7] Wilson, C., "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress", *CRS Report for Congress, RL32114*, January 2008.
[8] Honeynet Project, "Know your Enemy: Tracking Botnets", March 2005. http://www.honeynet.org/papers/bots.
[9] Barroso, D., "Botnets – The Silent Threat", ENISA Position Paper No. 3., Nov. 2007.
[10] Li, Z. and Liao, Q., "Botnet Economics: Uncertainty Matters", WEIS 2008, Workshop on the Economics of Information Security, Hanover, NH, June 2008.
[11] Holz, T. Gorecki, C. Rieck, C. Freiling, F. "Measuring and Detecting Fast-Flux Service Networks." Presented at NDSS Symposium (2008).
[12] Passerini, E. Paleari, R. Martignoni, L. Bruschi, D. "FluXOR: detecting and monitoring fast-flux service networks." Detection of Intrusions and Malware, and Vulnerability Assessment (2008), pp. 186-206.
[13] OMB, "Securing the Federal Government's Domain Name System Infrastructure", August 22, 2008
[14] Dan Kaminsky, "It's The End Of The Cache As We Know It Or: "64K Should Be Good Enough For Anyone" Black Ops 2008, August 2008
[15] Weimer, F. "Passive DNS Replication", 17th Annual FIRST Conference, Singapore, 2005
[16] Tufte, E., *Beautiful Evidence*, Graphics Press, June 2006.