Behavioral Analysis of Fast Flux Service Networks

Alper Caglayan
Milcord LLC
1050 Winter St. Suite 1000
Waltham, MA
(781) 839-7138
acaglayan@milcord.com

Mike Toothaker, Dan Drapaeau
Milcord LLC
20 Godfrey Drive
Orono, ME 04473
(207) 866-6532
mtoothaker@milcord.com

Dustin Burke, Gerry Eaton
Milcord LLC
1050 Winter St. Suite 1000
Waltham, MA 02451
(617) 868-0440
dburke@milcord.com

ABSTRACT

Here we present a behavioral analysis of fast flux service networks (FFSNs) using our database of FFSNs collected over a period of 9 months. FFSNs exploit a network of compromised machines (zombies) for illegal activities such as spam campaigns, phishing scams and malware delivery using DNS record manipulation techniques. In this paper, we use our fast flux domain and IP database collected using our real-time fast flux network detection algorithm to analyze the behavior of fast flux networks [1]. Our results show that such networks share common lifecycle characteristics, and form clusters based on size, growth and type of malicious behavior.

Categories and Subject Descriptors

K.6.5 [Security and Protection]: Invasive software – botnets.

General Terms

Algorithms, Measurement, Experimentation. Security.

Keywords

Botnets, fast flux, behavior, phishing, spam, malware.

1. INTRODUCTION

ICANN describes [2] 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'. While fast flux methods do have a legitimate use as a load balancing technique for high availability and high volume Web sites, its malicious use enables concealment of the Command and Control server using compromised machines ('zombies') that are used in DDoS, spam, phishing, malware delivery. 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 [3].

2. RELATED WORK

Published works on fast flux databases include the ISOC Network and Distributed System Security Symposium (NDSS) paper [4] on measuring and detecting fast flux service networks, the FluXOR paper [5] on detecting and monitoring fast-flux service networks , and our CATCH paper detecting and classifying fast flux service networks in real time. 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 detailed in [1] 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. We employ a Bayesian classifier that fuses multiple indicators including fast flux activity index, network footprint index, TTL, guilt by association, and others. In addition, our approach is able to differentiate and classify all three fast-flux variants, including name server flux and double-flux.

3. FAST FLUX BEHAVIOR

3.1 Data Collection

We collected our fast flux database using our Fast Flux Monitor (FFM); a Web service application 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.

We have employed multiple sensors for our FFM active sensors: (1) FF Activity Index, (2) Footprint Index, and (3) Time To Live (TTL), and (4) Guilt by Association Score. In active monitoring,

CSIIRW '09, April 13-15, Oak Ridge, Tennessee, USA

we perform DNS lookup with `dig`, and record the A records returned with each query. 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 that we have been monitoring.

3.2 Short Term Behavior

Figure 1 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. Fast Flux Activity Index for domains is an empirical belief function that weighs the evidence for fast flux (i.e. new A records) against the evidence of not fast flux (i.e. A records previously seen) over a moving window of 10 minutes. We compute the Activity Index roughly every 2 minutes by using the past 10 minutes of data. The red bar shows the presence of fast flux activity, and green shows the absence of fast flux activity, while the yellow bar shows the border line behavior. The height of the bar signifies the confidence level associated with the labeled activity.

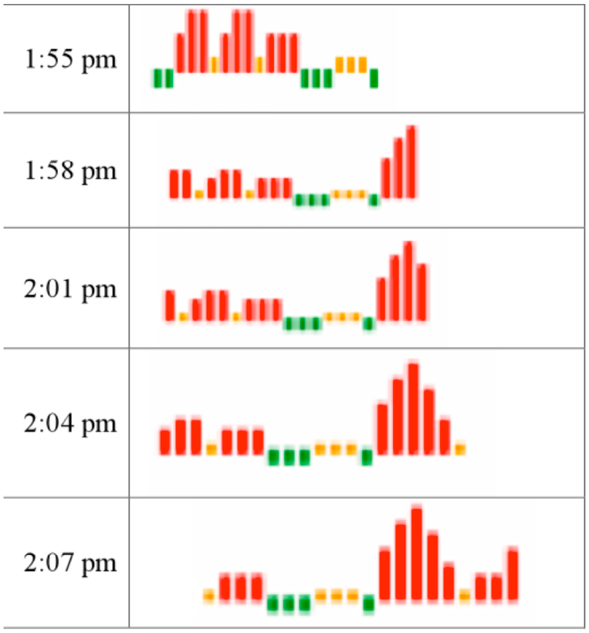

Figure 1. Fast Flux Activity Index

The use of a sparkline gives us the ability to show large amounts of data in a small space. Figure 1 shows 12 minutes of activity sampled every 2 minutes. As seen, the monitored domain does not consistently exhibit fast flux behavior, but there are intervals where such behavior is dominant. 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.

3.3 Long Term Behavior

We analyzed the long-term behavior of fast flux service networks. Figure 2 shows the lifespan distribution of fast flux botnets. Here the x-axis scale denotes the lifespan of an inactive fast flux botnet in number of days. The y-axis shows the number of inactive domains corresponding to specific lifespan measured in days. As shown in the figure, we found most fast flux botnet domains have a shelf life of 2 weeks to 2 months. In addition, the number of fast flux botnets decreases with increasing lifespan.

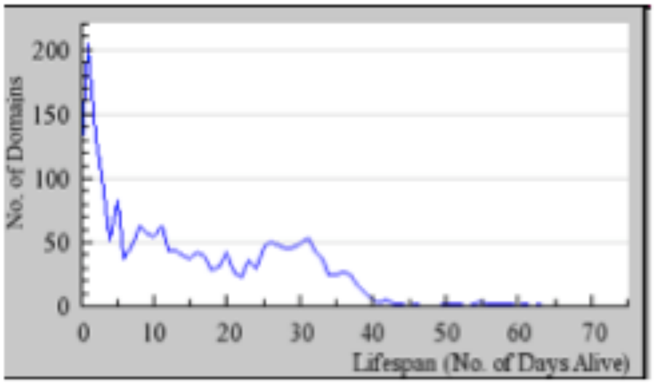

Figure 2. Lifespan Distribution of Fast Flux Botnets

Figure 2 shows the lifespan distribution for the general population of botnets. We also analyzed the lifespan distribution of fast flux botnets used for spam campaigns, phishing scams, and malware delivery separately. Figure 3 shows the lifespan of fast flux malware (blue), phishing (green), and spam (red) botnets. In terms of the fast flux botnet lifespan, spam botnets outlive malware botnets, which, in turn, outlive phishing botnets. Phishing fast flux botnets tend to die out very quickly, most living less than a week. We suspect that this is because phishing botnet domains target well established brands, which are protected by takedown services. In contrast, spam and malware delivery attack the general population, and do not have well defined targets for retaliation.

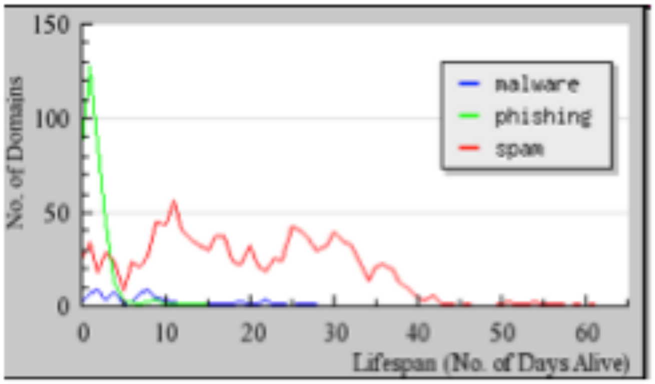

Figure 3. Lifespan: Malware vs. Phishing vs. Spam

Figure 4 shows the semi-log plot of fast flux botnet domain size against lifespan in number of days lived. As seen from the figure, the network size is clustered between 100 to 1,000 zombie botnets. It is worth noting that we are referring to the size of the fast flux domain used in the specific malware delivery, phishing spam, and spam campaigns. The botnet sizes are much larger than the domain sizes as multiple campaigns are conducted by the same botnet. The larger botnet domains tend to live longer than their smaller counterparts. The data shows that the network size seems to converge to an asymptote after 1,000 zombies, which implies that lifespan gained per number of additional zombies recruited diminish. Our data also shows the truncation of lifespan after 2 months. This observation agrees with the findings of other researchers in the field. It is not clear whether this behavior is forced as a result of takedowns, or voluntary on the part of criminal organizations to avoid detection.

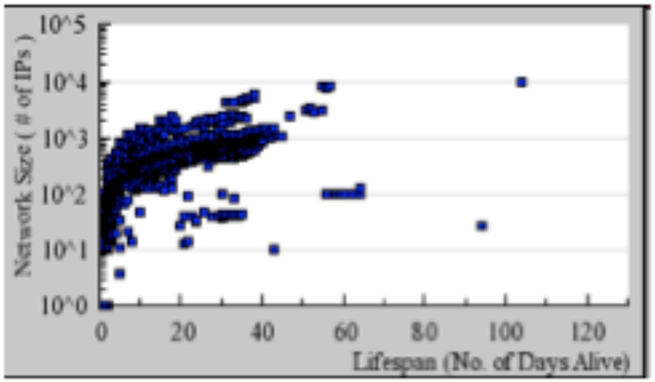

Figure 5. Fast Flux Botnet Domains: Size vs. Lifespan

Figure 4 shows the composite picture of botnet domain size vs. lifespan. If we look at the same distribution across different types of botnets like malware, phishing and spam, some differences emerge. Figure 5 shows the same distribution for fast flux botnet domains used for spam campaigns. The exponential asypmtotic convergence is more evident in this graph shows that the network size seems to converge to an asymptote after 1,000 zombies, which implies that lifespan gained per number of additional zombies used diminish.

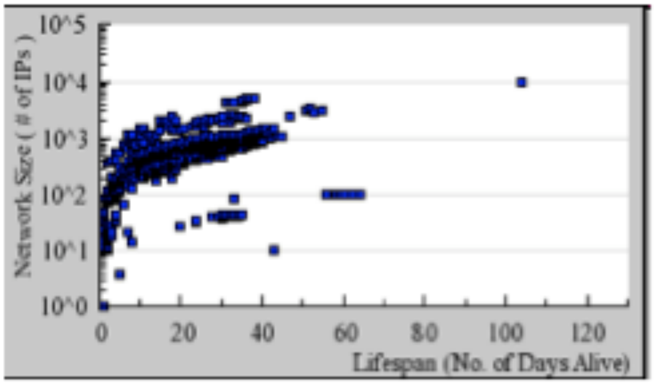

Figure 6. Spam FF Domains: Size vs. Lifespan

3.4 Organizational Behavior

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

Using these analytical sensors, we analyze the organizational structure of fast flux botnets in our database. Figure 6 shows the number shared IP addresses across fast flux domains using a log-log scale. The plot shows a linear trend in this scale in that the number of IP addresses shared decreases with increasing number of fast flux domains. For instance, there are 100 botnet domains sharing 100 IP addresses whereas there are only 10 botnet domains sharing 1,000 IP addresses, resulting from having more smaller botnets than larger ones.

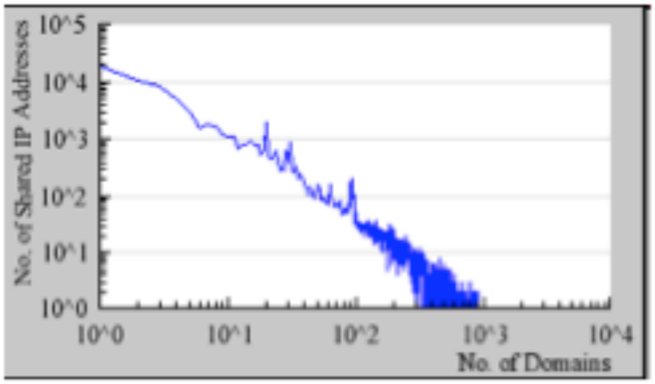

Figure 4. Distribution of IPs Shared

3.5 Operational Behavior

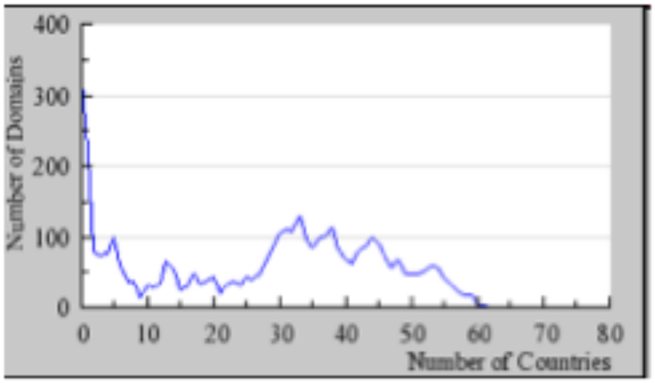

Figure 7. Operations in Multiple Countries

We analyzed each botnet’s distribution across different countries, and ASNs. Figure 7 shows the number of countries where fast flux botnets operate. While there are a large number of botnets operating in a few (less than 5) countries, most of the botnets operate in between 30 and 60 countries. The number of botnets operating in more than 60 counties falls off sharply.

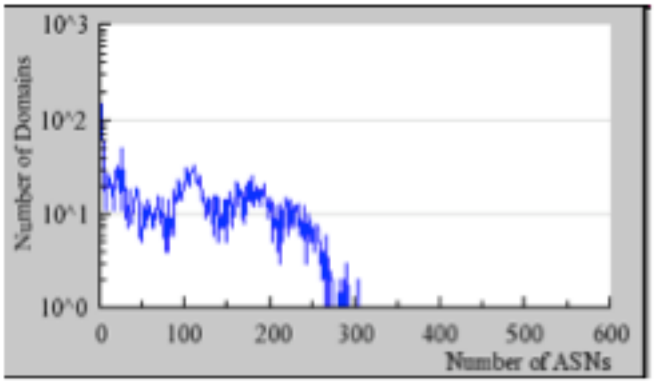

Figure 8. Operations in Multiple ASNs

We also analyzed the distribution of fast flux botnet across ASNs. Figure 8 shows the number of ASNs in which fast flux botnets operate. While there are a large number botnets (100) operating in less than 10 ASNs, the distribution of fast flux botnets operating in 10 – 250 ASNs is uniformly distributed with a sharp fall off after 250 ASNs with practically no botnets operating in more than 300 ASNs. We suspect that his behavior is due to the limited size of the botnet ASN targets, namely, ISPs and universities.

4. CONCLUSIONS

In this paper, we presented a behavioral analysis of fast flux service networks using our botnet database collected over 9 months. Our results show that such networks share common lifecycle characteristics, and form clusters based on size, growth and attack campaigns.

5. ACKNOWLEDGMENTS

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

6. REFERENCES

[1] Caglayan, A., Toothaker, M., Drapeau, D., Burke, D., and Eaton, G., “Real-time Detection and Classification of Fast Flux Service Networks”, Cybersecurity Applications and Technology Conference for Homeland Security (CATCH)March 3 - 4, 2009, Washington, DC.

[2] ICANN. GNSO Issues Report on Fast Flux Hosting, March 2008.

[3] ICANN Security and Stability Advisory Committee. SAC 025: SSA Advisory on Fast Flux Hosting and DNS, March 2008.

[4] Holz, T. Gorecki, C. Rieck, C. Freiling, F. “Measuring and Detecting Fast-Flux Service Networks.” Presented at NDSS Symposium (2008).

[5] 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.