Measuring Botnets in the Wild: Some New Trends

Wentao Chang[1] Aziz Mohaisen[2]* An Wang[1] Songqing Chen[1]
[1]George Mason University [2]Verisign Labs
{wchang7, awang10, sqchen}@gmu.edu amohaisen@verisign.com

ABSTRACT

Today, botnets are still responsible for most large scale attacks on the Internet. Botnets are versatile, they remain the most powerful attack platform by constantly and continuously adopting new techniques and strategies in the arms race against various detection schemes, . Thus, it is essential to understand the latest of the botnets in a timely manner so that the insights can be utilized in developing more efficient defenses. In this work, we conduct a measurement study on some of the most active botnets on the Internet based on a public dataset collected over a period of seven months by a monitoring entity. We first examine and compare the attacking capabilities of different families of today's active botnets. Our analysis clearly shows that different botnets start to collaborate when launching DDoS attacks.

1. INTRODUCTION

Botnets are one of today's most challenging cybersecurity threats, and promise to remain a serious threat for many years to come. A botnet is typically comprised of a network of infected machines called bots, which are often under the control of a malicious entity, called the botmaster. Botnets are notoriously known as one of the primary attack platforms that cybercriminals use to carry out malicious and harmful actions, such as distributed denial of service (DDoS) attacks, spam distribution, phishing, scanning and network exploration, against pieces of infrastructures and services. Reports have highlighted the devastating operational impact, size, and consequences that a botnet attack can bring to Internet services. For example, it was recently reported that a collection of just 3,000 open Domain Name System (DNS) resolvers were capable of generating 300 Gbps DDoS attack traffic [19], and taking down Spamhaus, a popular spam tracking service.

On the botnet analysis front, significant research efforts have been made to gain a better understanding of the botnet phenomenon and landscape. A common approach to study botnets is to perform passive analysis of abnormal behaviors produced by bot-infected machines [14, 16, 17] . While the passive analysis approach does reveal much valuable information about particular botnet-related behaviors, some of the insight on longitudinal activities is absent since the approach only considers a small portion of bots at a given time [28, 8]. Infiltration is another technique adopted in recent studies [4, 1, 10], where an actual malware sample or a client is to simulate a bot. However, attackers have unfortunately learned to adapt, and most current botnets use stripped-down IRC or HTTP servers as their centralized command and control channels. It is unlikely to obtain a lot of information about other bots by simply joining the botnet. An effective effort to understand botnets would require reverse engineering, passive and active measurements.

On the defense front, a lot of efforts have been made to detect bots and botnets. While many detection schemes have been developed [25, 16, 22], attackers have been constantly adopting new technologies and improving their attacking schemes. For example, various generations of botnets have been shown to use HTTP and P2P technologies, instead of IRC, for their operations [11, 15, 27].

The arms race between malware developers and defenders is endless. Thus, it is essential to continuously track and understand the latest strategies of attackers in manipulating botnets for attacks. A timely understanding can provide important insights to guide the building of effective defenses. To this end, in this study we perform an in-depth analysis of botnet strategies based on recent botnet traffic, resources enumeration and activities profiling. Data used in this study is obtained by utilizing active and passive monitoring, and using state-of-the-art reverse-engineering and protocol analysis techniques for 23 different botnet families. The data obtained in this study is enriched by traffic observed at a large number of Internet vantage points on the Internet in about seven months of monitoring.

Our study reveals several interesting new trends of botnet management. In this paper, our contributions include the following:

- We conduct a large-scale measurement study to investigate botnet characteristics and describe botnet behaviors. The analysis results help make better comprehension of the wide variety of existent botnet families in the wild.
- Some bots are dedicated and heavily re-used by different botnet families. Similar collaborations are also found within various generations of the same botnet family.

To the best of our knowledge, some of the insights and operation aspects of botnets in this paper are not reported before. We expect these results can help improve our understanding of botnet operations and devise new defense schemes.

The remainder of the paper is organized as follows. Section 2 describes our dataset and section 3 presents characterization of botnet families. In Section 4, we discuss the possibility of collaborations among the botnets by identifying reused bots, while Section 5 dis-

*The views and opinions expressed in this paper are the views of the author, and do not necessarily represent the policy or position of VeriSign, Inc.

ASIA CCS'15, April 14–17, 2015, Singapore..

http://dx.doi.org/10.1145/2714576.2714637.

cusses related work. We conclude in Section 6 with a discussion about future work.

2. DATASET

Some research efforts on botnet measurements have focused on the taxonomy and classification of botnets by analyzing botnet behavior and common characteristics, such as architecture, command and control channels, communication protocols and evasion techniques [12, 20]. These efforts have mainly been done via passive measurement or infiltration. Thus, they usually focused on specific botnets. Different from these approaches, our dataset is provided by the Team Cymru Community Service [26]. The dataset is based on Team Cymru's constant monitoring of Internet critical infrastructure to aid intelligence gathering concerning the state of the art of attack posture, using both active and passive measurement techniques. For active measurements and attribution, malware families used in launching various attacks are reverse engineered, and labeled to a known malware family using best practices. Hosts participating in the given botnet, by either communicating with pieces of infrastructure infected by that malware family (e.g. the command and control) are then enumerated and monitored over time, and their activities are logged and analyzed.

As each botnet evolves over time, new generations are marked by their unique (MD5 and SHA-1) hashes. Traces of traffic associated with various botnets are then collected at various anchor points on the Internet, via the cooperation of many ISPs all over the world, and analyzed to attribute and characterize attacks. The collection of traffic is guided by two general principles: 1) that the source of the traffic is an infected host participating in a botnet attack, and 2) the destination of the traffic is a targeted client, as concluded from eavesdropping on C&C of the campaign using a live sample.

By tracking temporal activities of 23 different known botnet families in the wild, the monitors of the company generate a log dump every hour from 08/29/2012 to 03/24/2013, a total of 207 days, or about 7 months. There are 24 hourly reports per day for each botnet family. The set of bots or controllers listed in each report are cumulative over past 24 hours. The 24-hour time span is counted from time stamp of last known bot activity and time of log dump.

3. CHARACTERIZATION OF BOTNET FAMILIES

In this section, we examine the botnet families included in our dataset, focusing on their attacking capacities from the perspective of their size, stability, elasticity and activeness. While the monitoring unit targets the 23 most prevalent botnet families, we found 7 of them, namely `Asprox`, `Gumblar`, `Myloader`, `Redgirl`, `Storm`, `Tdss`, and `Waledac`, to have zero traffic within our collection window. Thus, we exclude them from our analysis below. Table 1 summarizes some information of the 16 remaining botnet families.

3.1 Botnet Size, Stability, and Elasticity

A first and very important metric to evaluate different botnets is the number of bots that a botnet can utilize. Thus, we can use it to weigh the significance of different botnet families in regards to their impact on network security. There are more than one counting techniques and standards available to estimate the size of botnets. In our analysis, we simply count the number of unique IP addresses when estimating the size of botnets and the maximum number of simultaneous online bots of a botnet. Note that we ignore the case that multiple infected machines might hide behind the NAT and treat them as one single IP in counting.

Table 1: Summary statistics of 16 Botnet Families

Family Name	Active Period	Botnet Size
Aldibot	11/01/12-03/24/13	12,075
Armageddon	08/29/12-03/24/13	171
Blackenergy	08/29/12-03/24/13	498,925
Colddeath	08/29/12-12/19/12	1,859
Conficker	08/29/12-03/24/13	667,523
Darkcomet	12/02/12-03/24/13	4,019
Darkshell	08/29/12-03/24/13	4,886
Ddoser	11/13/12-03/07/13	35
Dirtjumper	08/29/12-03/24/13	837,297
Illusion	08/29/12-03/24/13	47,887
Nitol	08/29/12-03/24/13	15,230
Optima	08/29/12-03/24/13	362,157
Pandora	10/11/12-03/24/13	17,418
Torpig	08/29/12-03/24/13	1,260
Yzf	08/29/12-02/11/13	7,937
Zeus	08/29/12-03/24/13	175,343

Similar to the metrics used in [1], we define the botnet size as the total number of unique IP addresses that were once recruited in their lifetime by the specific botnet. As the last column of Table 1 shows, the botnet size of different families varies significantly. The botnet size is as large as 837 thousand for Dirtjumper or as small as 35 for Ddoser. Based on the botnet size, we can classify them into different groups. The `large` botnet families own more than 100 K bots with unique IP addresses, including `Dirtjumper`, `Conficker`, `Blackenergy`, `Optima` and `Zeus` in descending order. 90% of bots found in our dataset are employed by these large botnet families at least once. The `medium` group includes botnet families with the number of bots ranging from 10 thousands to 100 thousands, such as `Illusion`, `Pandora`, `Nitol` and `Aldibot`. The `small` group owns less than 10 thousands bots. In descending order of their botnet size, they are `Yzf`, `Darkshell`, `Darkcomet`, `Colddeath`, `Torpig`, `Armageddon` and `Ddoser`.

Since the botnet size does not give us a very accurate estimate of the potential attack capability because those bots may not be online simultaneously, we also examine the number of bots that are simultaneously online, termed as "live bots". Figure 1 shows the number of simultaneous live bots over time. Note the y-axis is in log scale. The left sub-figures show the number of live bots hourly, while the right sub-figures show the corresponding results daily. To some extent, the live bots distribution over time can indicate the `stability` of the corresponding botnet family. As shown in the figure, besides the difference on the absolute numbers, both the hourly and daily results indicate that the botnets in `large` group have maintained a relatively stable army of active bots by showing only a few spikes, while there are more fluctuations in botnets in the `medium` and `small` groups. While this is to be expected, it raises a new question whether the relative stability in large botnets is due to the same sets of bots being active all the time or more sophisticated strategies being used by botnets.

As previously mentioned, Figure 1 also shows a few steep spikes for botnets in `large` groups. By further looking into the data, we find out those spikes can be attributed to some ongoing campaigns started during that time period. Take `Blackenergy` as an example, Figure 2 compares the botnet stability curves for `Blackenergy` with and without certain live bots. The top figure depicts the stability curve with all live bots from `Blackenergy`, from which we observe a transient burst of live bots that are derived from two

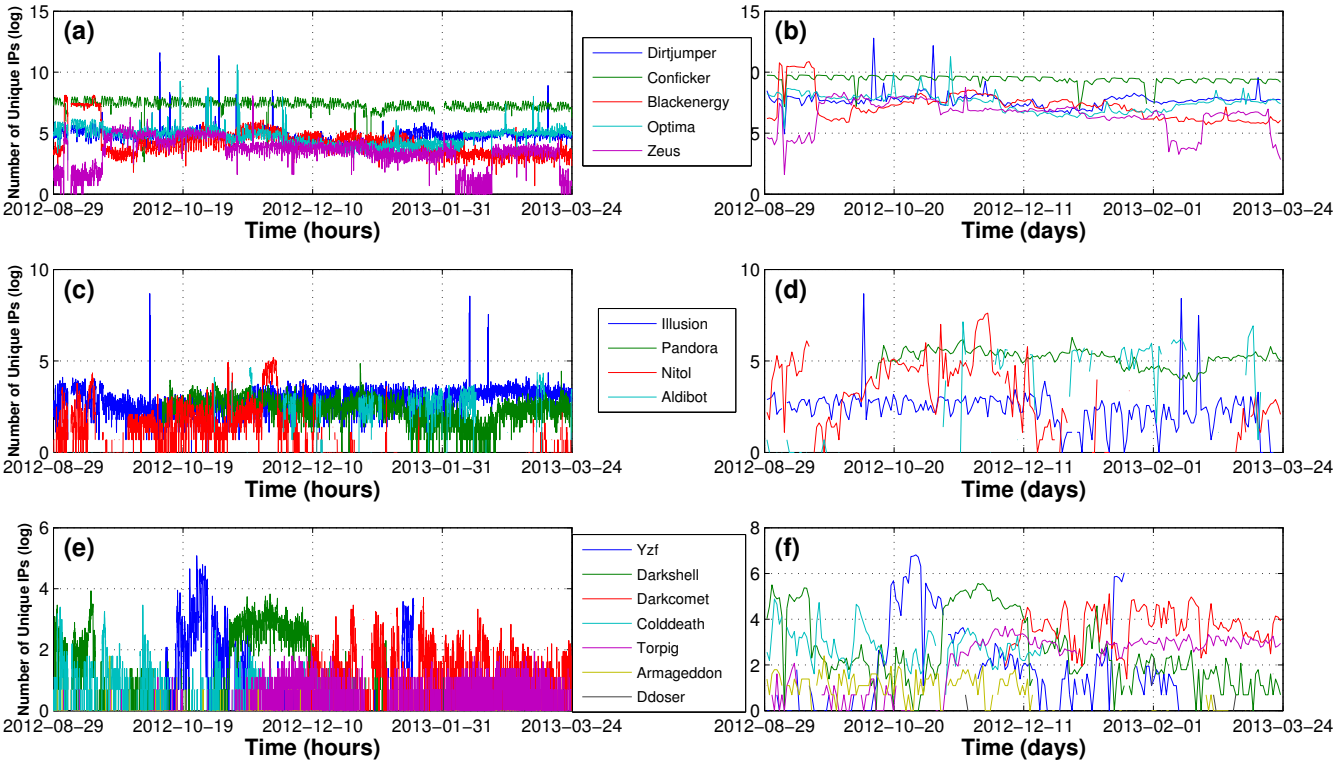

Figure 1: Botnet stability of three groups (based on botnet size)

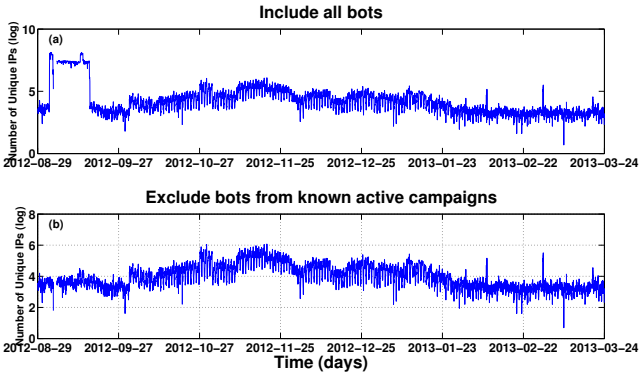

Figure 2: Simultaneous live bots of Blackenergy

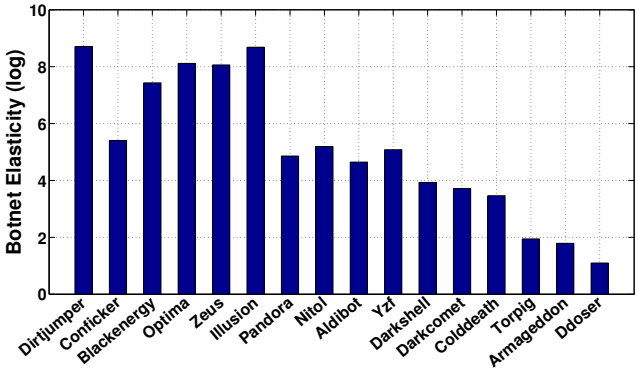

Figure 3: Botnet Elasticity

specific botnets. We speculate those two botnets are very likely to participate in a potential campaign. In the comparison figure at the bottom we draw the stability curve again excluding bots from those two botnets. The new curve unveils that when the `Blackenergy` is not instructed to participate in campaigns, the number of live bots keeps at a relatively stable level. A plausible explanation would be that the botnet requires a minimum number of live bots to preserve its presence (e.g., for business) or the communication (e.g., C&C channels). The number of live bots can surge within a very short time frame, usually a couple of days, when the botnet is instructed to engage in certain attacks. In our observation, a well managed botnet could rapidly recruit new bots in the order of hundreds of thousands. This is another important perspective when we evaluate the potential of a botnet's attacking power, particularly as today botnets are moving to "botnets-as-a-service" [9]. Therefore, we define another metric `elasticity` of a botnet, which is the ratio of the maximum number over the minimum number of live bots.

Figure 3 shows the elasticity result for all families—sorted by size in a descending order. As indicated by the figure, overall, the elasticity decreases with the decreasing botnet size. An exception is `Conficker`. As Figure 1 shows, compared to other large botnets, `Conficker` maintains a very stable army of bots. From the service perspective, the larger the elasticity value, the more capable a botnet is upon a demand for attacks. From the defense perspective, the more elastic a botnet, the harder to shut it down.

3.2 Botnet Activeness

The size of a botnet is one aspect of botnet activity: the scale and the stability, which reflect the potential attacking capability of botnets. Another important aspect to examine botnets' activity is to

see whether or not a botnet is always live, i.e., the duration of their activity. Table 1 shows the activity periods of observed botnets in our dataset.

To further characterize botnet activeness, we plot in Figure 4 the total number of days for each family those live bots remain active. They are listed in the descending order of botnet size. 7 out of 16 families are `extremely active` and their activities are reported in our dataset for more than 200 days out of 207 days. They are `Blackenergy`, `Conficker`, `Darkshell`, `Dirtjumper`, `Illusion`, `Optima` and `Zeus`. 6 families (including `Armageddon`, `Darkcomet`, `Nitol`, `Pandora`, `Torpig` and `Yzf` stay active over 50% of time. We consider them `moderately active` families. The other 3 families, `Aldibot`, `Colddeath` and `Ddoser`, whose activity is less than 104 days, are classified as `marginally active` families. In conjunction with family grouping based on botnet size, we notice that although there is no one-to-one mapping, large- and medium-sized botnets also tend to be more active than the small-sized botnets.

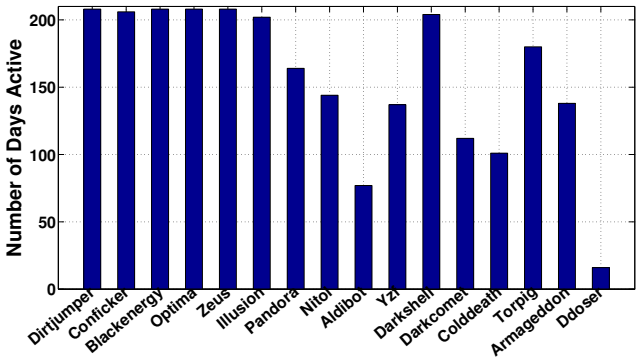

Figure 4: Botnet Activeness

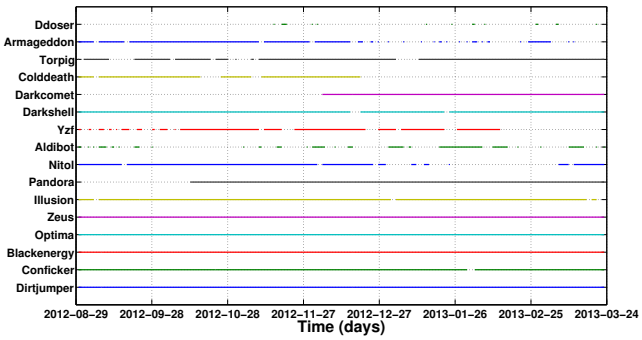

Figure 5: Botnet family activeness pattern

Figure 5 further shows the activeness pattern of different botnet families over time. While the top 5 botnet families in botnet size, including `Dirtjumper`, `Conficker`, `Blackenergy`, `Optima`, and `Zeus`, are almost constantly active in our observation period, `Aldibot` and `Ddoser` show clear intermittent activity pattern over the entire observation period. The rest of botnet families present a mix of continuous and periodical patterns. Considering that many effective detection and defense tools are already in use, the mixture of continuous and periodical patterns is likely to be the outcome of arms race between defenses and attacks. This is because bots are taken down in random pace, and botnets keep recruiting new ones to compensate. In other words, to maintain a simple continuous or periodic pattern is a non-trivial task, because it would require some defense-aware strategies from the botnet to guide the process of bots recruitment.

4. BOTNET COLLABORATION

One of the most challenging facets of the botnet behavior problem lies in discerning the relationship among (seemingly) different botnet families. To highlight this issue, we examine the infected hosts in our data collection to detect the existence of hidden relationships among the families we tracked. After performing a cross-family analysis, one interesting observation we have is the presence of a fair amount of reused bots – bots used by multiple botnet families, which could be potentially due to multiple infections, the NAT effect, or due to using paid infrastructure (i.e., pay-per-install) [7]. Even within the same family, some subsets of bots are also reused by different botnets (a family often contains multiple different botnets identified by the unique botnet ID in our dataset). The findings imply a possible inter-family and intra-family botnet collaboration. By identifying the set of reused bots, the defender could blacklist attacking machines in cost-effective ways.

4.1 Inter-family collaboration

As a first step analysis, we aim to identify bots that are reused across different families. In our analysis, we assume each IP address serves as the unique identifier of a bot and if the same IP is ever used by different botnet families, we consider the bot as a reused bot. Note that we are aware that multiple infected physical machines (bots) might operate behind a single NAT; there's a possibility that those machines are plagued by more than one botnet family over 7 months, thus the total number of reused bots might contain some false positives. Moreover due to DHCP, there's a slim chance that the same IP might be randomly assigned later to another bot that happens to be infected by a different family, which will also increase false positive rates of our classification. However, the analysis shows that the percentage of reused bots over all bots is relatively significant (14%, or 320,340 out of 2,280,369), much higher than what would result from coincidence.

We cross-compare specific botnet families to highlight a set of reused bots and monitor their participation in the botnet activities. Since the total number of unique bots identified in our dataset is over 2.2 million and the majority of them have been employed by only one botnet family, as the first step of inter-family collaboration analysis, we try to reduce the number of candidate bots that we need to closely track. To this end, we perform two data preprocessing steps. First, we filter out all bots that have not been shown to be used by more than two families over their life-cycle, thus reducing the total number of bots to about 320,000 (about 85% reduction). Second, using the outcome of the first step, we group IP addresses into /24 subnet, thus reducing the total number of IPs to 78,837. Aggregation of IPs into /24 subnets might inevitably introduce some false positives when two or more different IPs within the subnet are infected by different botnet families. But the chances are very slim if we assume those 256 IPs are assigned to normal and innocent machines of Internet users.

In our inter-family collaboration analysis, we aim to identify whether there exists a subset of the 78,837 subnets that are reused by various combinations of different botnet families. Also if such sets of bots exist, a second aim is to understand the status of those bots over time to reveal possible inter-family collaboration behaviors.

The top 6 active families we identified in Section 3 are our candidates for inter-family collaboration. Accordingly, we closely track every subnets in our dataset to record the time of their activity and what botnet family employs them. We assume that if the same bot is recorded active in the past 24 hours by two or more different families, they are recruited and are operated concurrently by those families. To make the figure more informative and to ac-

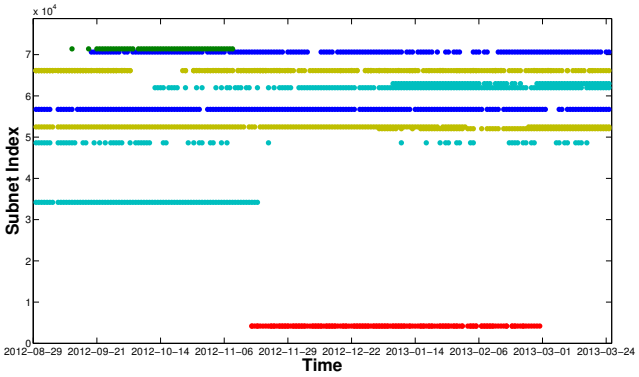

Figure 6: Activity of reused bots over four families

curately pinpoint subnets that are constantly reused or dedicated as collaboration resources, we set a minimum occurrence threshold to rule out less contributing resources (/24 subnets). That is, if the reused subnets do not engage in collaboration operations more than 25% of our observation period, we do not include them or show them in the figure. In our inter-family collaboration analysis of all top 6 families, there are only two subnets (aaa.57.68.xxx and aaa.57.190.xxx*) that are 75% of the time employed by those 6 families.

When excluding Conficker and Zeus from our analysis and only investigating inter-family collaboration between the other four families, we find significantly more /24 subnets are detected as reused ones. We depict concurrently reused /24 subnets and their status over time in Figure 6. The x-axis shows the time (207 days) while the y-axis represents the corresponding subnet index in our subnet set. When the subnet y is concurrently reused by all 4 families at a given time x, we mark the (x, y) point in the scatter plot. To make the grouping of reused subnets more visually impressive, the adjacent 2000 subnets are painted in the same color. We can observe from Figure 6 that a significant number of subnets are reused by all 4 families more than 75% of time. Two subnets (aaa.38.216.xxx and aaa.229.0.xxx) are active more than 95% of time and they are the backbone of inter-family collaboration between those 4 families. Another interesting finding from the figure is the shift of activity from one or many subsets to another set of subsets. For example, the subset aaa.107.232.xxx was heavily reused to engage in botnet activity until approximately day 79, and suddenly two adjacent /24 subnets (aaa.215.36.xxx and aaa.215.36.xxx) that were never reused before become reused in collaboration and served as the replacement of those 2 ceased subnets. This evident successor relationship suggests that the shift was not just a random incident but a deliberate action premeditated by a botmaster. We suspect that they could be an immediate reaction to a bot take-down event or a proactive detection evasion measure.

4.2 Intra-family collaboration

In our second step analysis, we focus on intra-family collaboration, and aim to understand how different botnet generations (identified by a unique botnet identifier) within the same family collaborate closely by reusing the same set of bots. In this section, we conduct our trace analysis on 13 out of the 16 most active botnet families in our dataset. Families `Armageddon` and `Torpig` report botnet activity from only one botnet generation, and all traffic for `Conficker` targets a DNS sinkhole server. For each family, we have a list of botnet identifiers derived from different malware signatures from the dataset. Similar to the methodology we used in inter-family analysis, we cross-compare the set of active bots from different botnet identifiers over time. The measurement results show that some botnet identifiers have extremely high concurrent usage rate over the same set of bots, while some other botnet identifiers show a clear temporal pattern.

*The first 8-bit segment of IP address is hidden for anonymization.

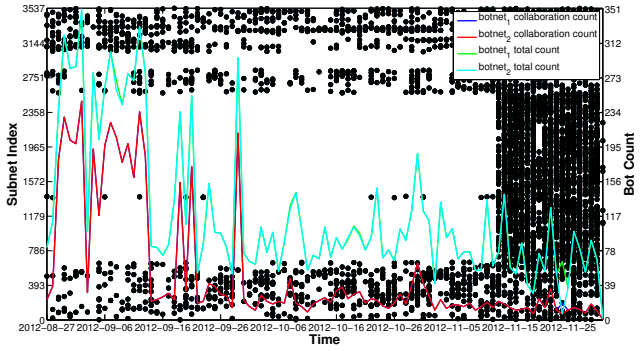

Figure 7: Intra-family collaboration for Blackenergy

Figure 7 shows the collaborations of two botnets with different identifiers within the `Blackenergy` family. In this figure, the x-axis represents daily timestamps when collaboration happened, the y-axis on the left represents the index of subnet involved in the collaborations, and the y-axis on the right represents the count of bots involved in the collaboration. For the scatter plot, each dot with different colors shows which botnet the subnet is involved in, and the black color means that those subnets are employed concurrently by both botnets. We plotted two more curves for each botnet involved in collaborations: the number of live bots for each botnet and the number of collaborating bots. In comparison of the collaboration curve and the live bots curve, it is evident that activities of both botnets are synchronized. Another finding is that a dedicated group of bots that are reused by both botnets are responsible for the spikes in the curve.

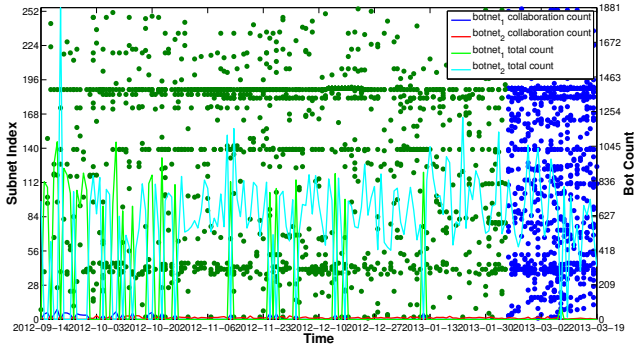

Figure 8: Intra-family collaboration for Zeus

Figure 8 describes the collaborations of two botnet identifiers from the family `Zeus`. Although these two botnet identifiers own a large number of the same bots, those bots are rarely used concurrently. They were solely used by botnet 1 before Feb. 10, 2013, and suddenly nearly all of those bots are transferred to botnet 2. We suspect the root cause is that the same set of bots are instructed to participate in another, different campaign. This evident temporal pattern suggests that botnet 1 and botnet 2 are likely to be managed by the same botmaster. Thus, they are essentially the same botnet, with a difference in their code base that resulted in a different signature.

5. RELATED WORK

Botnets pose one of the most severe threats to the health of the Internet. To collect and analyze bots, researchers widely utilize two common techniques: infiltration [3, 10] and passive traffic monitoring [1]. To facilitate the botnet detection and provide effective countermeasures against malicious botnet activities, it is crucial to have a good understanding of botnets in the wild including their behaviors and coordination strategies. Dagon et al. [12] conducted a taxonomy study of botnet structure based on their utility to the botmaster in 2007, and also ranked botnets based on key measurement metrics they proposed on botnets. Some other security researchers endeavor to conduct an in-depth case study of botnet by putting one specific botnet family under the microscope [6, 23, 2, 24]. The trend that the state-of-art botnets have become more and more sophisticated and applied various evasion techniques to hide their activity, further complicates the detection and defense mechanisms. Many existing botnet studies [21, 5] are targeted at the most common IRC-based bots relying on a centralized control. However, numerous new botnets begin to use http-based C&C channels and leverage the more stable P2P based communication architecture [27, 18, 15] to avoid single point of failure. Some recent work focused on large scale measurements of network traffic to develop methods for revealing more properties of botnets, such as their size [13] and activeness [24]. In our work, with the assistance of top level ISPs, we observed large-scale bot activity data from multiple well-known botnet families, and reveal several new trends and activity patterns of botnets.

6. CONCLUSION

Botnets have been widely used for various Internet attacks. To remain active and profitable, today botnets are very versatile and adaptive by constantly and continuously adopting new techniques to evade from being detected. In this study, we have performed an in-depth analysis of botnet behavior patterns based on a large botnet dataset collected from various Internet anchor points by a commercial monitoring unit for about seven months. By analyzing the data of the most active 16 botnet families, we have reported some new observations and insights of today's botnets. Such results not only add to the existing botnet literature for a better understanding, but also offer timely help for botnet detection and defenses.

7. REFERENCES

[1] M. Abu Rajab, J. Zarfoss, F. Monrose, and A. Terzis. A multifaceted approach to understanding the botnet phenomenon. In *IMC*, 2006.

[2] M. M. Andrade and N. Vlajic. Dirt jumper: A key player in today's botnet-for-ddos market. In *WorldCIS*. IEEE, 2012.

[3] P. Bacher, T. Holz, M. Kotter, and G. Wicherski. Know your enemy: Tracking botnets. http://www.honeynet.org/papers/bots, 2005.

[4] P. Baecher, M. Koetter, T. Holz, M. Dornseif, and F. Freiling. The nepenthes platform: An efficient approach to collect malware. In *RAID*, pages 165–184. Springer, 2006.

[5] P. Barford and V. Yegneswaran. An inside look at botnets. In *Malware Detection*, pages 171–191. Springer, 2007.

[6] H. Binsalleeh, T. Ormerod, A. Boukhtouta, P. Sinha, A. Youssef, M. Debbabi, and L. Wang. On the analysis of the zeus botnet crimeware toolkit. In *PST*, pages 31–38. IEEE, 2010.

[7] J. Caballero, C. Grier, C. Kreibich, and V. Paxson. Measuring pay-per-install: The commoditization of malware distribution. In *USENIX Security*, 2011.

[8] J. Caballero, P. Poosankam, C. Kreibich, and D. Song. Dispatcher: Enabling active botnet infiltration using automatic protocol reverse-engineering. In *CCS*, pages 621–634. ACM, 2009.

[9] W. Chang, A. Wang, A. Mohaisen, and S. Chen. Characterizing botnets-as-a-service. In *Proceedings of the 2014 ACM conference on SIGCOMM*, pages 585–586. ACM, 2014.

[10] C. Y. Cho, J. Caballero, C. Grier, V. Paxson, and D. Song. Insights from the inside: A view of botnet management from infiltration. In *USENIX LEET*, 2010.

[11] N. Daswani, M. Stoppelman, the Google Click Quality, and S. Teams. The anatomy of clickbot.a. In *USENIX HotBots*, Cambridge, MA, April 2007.

[12] C. P. L. David Dagon, Guofei Gu and W. Lee. A taxonomy of botnet structures. In *ACSCA*, 2007.

[13] M. A. R. J. Z. Fabian and M. A. Terzis. My botnet is bigger than yours (maybe, better than yours): why size estimates remain challenging. In *USENIX HotBots*, 2007.

[14] J. Goebel and T. Holz. Rishi: Identify bot contaminated hosts by irc nickname evaluation. In *USENIX HotBots*, pages 8–8. Cambridge, MA, 2007.

[15] J. B. Grizzard, V. Sharma, C. Nunnery, B. B. Kang, and D. Dagon. Peer-to-peer botnets: Overview and case study. In *USENIX HotBots*, pages 1–1, 2007.

[16] G. Gu, P. Porras, V. Yegneswaran, M. Fong, and W. Lee. Bothunter: Detecting malware infection through ids-driven dialog correlation. In *USENIX Security*, page 12, 2007.

[17] G. Gu, J. Zhang, and W. Lee. Botsniffer: Detecting botnet command and control channels in network traffic. In *NDSS*, 2008.

[18] T. Holz, M. Steiner, F. Dahl, E. Biersack, and F. C. Freiling. Measurements and mitigation of peer-to-peer-based botnets: A case study on storm worm. In *USENIX LEET*, volume 8, pages 1–9, 2008.

[19] Info Security Magazine. Spamhaus suffers largest ddos attack in history – entire internet affected. http://bit.ly/1bfx3ZH, March 2013.

[20] L. Jing, X. Yang, G. Kaveh, D. Hongmei, and Z. Jingyuan. Botnet: classification, attacks, detection, tracing, and preventive measures. *EURASIP JWCN*, 2009.

[21] A. Karasaridis, B. Rexroad, and D. Hoeflin. Wide-scale botnet detection and characterization. In *USENIX HotBots*, volume 7. Cambridge, MA, 2007.

[22] A. Moshchuk, T. Bragin, D. Deville, S. Gribble, and H. Levy. Spyproxy: Execution-based detection of malicious web content. In *USENIX Security*, 2007.

[23] J. Nazario. Blackenergy ddos bot analysis. *Arbor*, 2007.

[24] S. Shin and G. Gu. Conficker and beyond: a large-scale empirical study. In *ACSAC*, pages 151–160. ACM, 2010.

[25] E. Stinson and J. C. Mitchell. Characterizing the remote control behavior of bots. In *DIMVA*, 2007.

[26] Team Cymru. Team cymru community services. http://www.team-cymru.org/Monitoring/, May 2013.

[27] P. Wang, S. Sparks, and C. C. Zou. An advanced hybrid peer-to-peer botnet. *TDSC*, 7(2):113–127, 2010.

[28] Z. Zhu, G. Lu, Y. Chen, Z. Fu, P. Roberts, and K. Han. Botnet research survey. In *COMPSAC*, pages 967–972. IEEE, 2008.