New Trends in FastFlux Networks

Wei Xu
Palo Alto Networks, Inc.
3300 Olcott Street
Santa Clara, CA, 95054
408-753-4135
wei.xu@paloaltonetworks.com

Xinran Wang
Palo Alto Networks, Inc.
3300 Olcott Street
Santa Clara, CA, 95054
408-753-4108
xwang@paloaltonetworks.com

Huagang Xie
Palo Alto Networks, Inc.
3300 Olcott Street
Santa Clara, CA, 95054
408-753-4109
hxie@paloaltonetworks.com

ABSTRACT

Fast-flux networks have been adopted by attackers for many years. Existing works focus on characteristics such as the fast changing rate of the IP addresses (e.g. A record) and the name server addresses (NS records); the single flux/double flux structure etc. In this work, we tracked and analyzed over 200 fast flux domains and we discovered that the features of the fast-flux networks has shifted. More specifically, we discovered that the changing rate of the IP addresses and name server addresses are slower than reported before, in some cases even slower than some benign applications that leverage fast-flux alike techniques. We also discovered that IP addresses and name servers are shared among different families of fast-flux domains indicating that there is a well-established underground economic model for fast-flux domains. Moreover, we also noticed that instead of using single or double flux, current fast-flux domains exhibit "n-levels" of flux behavior, i.e., there appears to be "n" levels of name servers in the DNS system for fast-flux domains. Finally, we also studied the similar benign applications that look alike fast-flux domains but are not. In light of these new characteristics, we proposed several new detection approaches that can help to identify the fast-flux domains.

Categories and Subject Descriptors

K.6.5 [**Management of Computing and Information Systems**]: Security and Protection

General Terms

Security

Keywords

Fastflux Networks

1. INTRODUCTION & BACKGROUND

Fastflux domains leverage DNS system to create a more robust system to engage malicious activities such as delivering malicious content, spreading spams and setting up phishing websites, etc. A fast-flux network is a distributed system that consists of mainly two types of elements: 1) master server(s), so called "mothership" that controls all the other hosts in the system; 2) infected/controlled hosts, whose roles include: providing name server, proxying traffic to the next level, delivery malicious contents. In [1], the authors explained two typical fast-flux networks, namely single-flux and double-flux networks.

Since fast-flux networks are frequently adopted by various malicious campaigns, it has become part of the underground economic system. That is, fast-flux networks have become a paid service that can be purchased by attackers to facilitate their malicious activities. Previous works such as [7] [8] has discussed some characteristics on FF. Characteristics include: rate of change, the location of change and the sharing of FF networks among different malicious campaigns.

In this work, we discuss the new trends discovered in FF networks.

2. DATA COLLECTION

Our data collection process consists of three steps:

1. Collect fast-flux domains candidates. We use different sources: malware domains extracted from malware samples; published lists for fast-flux domains (e..g, Arbor Networks FF list; spamhaus list), etc.
2. Actively monitoring the fast-flux domains using active DNS queries. Periodically query candidate domains on different public DNS servers
3. Aggregate the data based on name servers, authoritative name servers and malware families.

In total, we identified and tracked 207 fast-flux domains. We observed over 423667 unique IP addresses being resolved to these domains, and we have seen 94491 unique name server names.

3. OVERVIEW

In this work, we investigate the Fast-flux networks from several different perspectives:

- Slower change rate

Table 1: Change Rate of Monitored FF Domains

type	Minutes/IP	IP/Day	A-TTL	NS-TTL
average	73.55	55.90	1832.84	37348.75
max	634.50	261.54	21598.03	65535.00
min	5.51	2.27	0	0

- Sharing of IP address, name servers
- Double-flux OR n-flux
- One IP at a time
- Benign systems that look alike FF networks

4. NEW FEATURES IN FF NETWORKS

4.1 Not So Fast Fast-Flux Networks

We listed the change rate of the FF domains in Table 1.

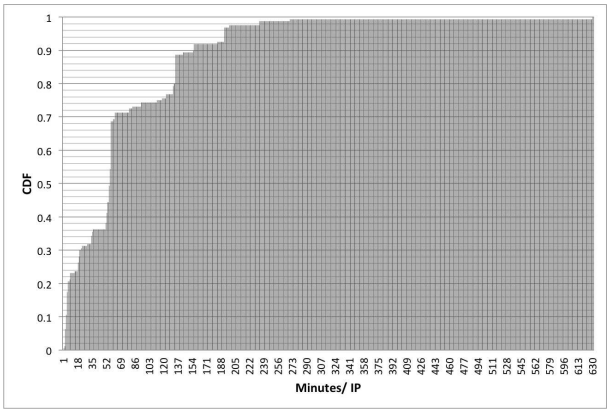

Figure 1: CDF of Change rate of IP

The results show that 95% of the fast-flux domains that we are tracking have a change rate of IP address larger than 10 minutes/IP (i.e., on average, each IP address will be used for 10 minutes). Over 80% of fast-flux domains have changing rate of IP addresses that is larger than 33 minutes/IP. Over 61% of fast-flux domains have changing rate of IP addresses that is larger than 60 minutes/IP. The changing rate is slower than the values that were reported in [7], which is around 10 minutes/IP. This suggests that the value of a domain name to attackers is not as much as it use to be. Since one of the assumptions of applying fast-flux networks is that the domain names are valuable assets to attackers such that attackers are willing to map the same domain name to many different IP addresses to preserve the availability of the domain.

As for the rational behind this shift, we believe this is because the increase in the number of registrars and the expand of domain name space (i.e. the development of new tad, cctld,etc.), the cost for registering a domain now (e.g. $10 per year) is much less than several years before (e.g., $100) [3]. Meanwhile, the cost to infect, control and keep a bot/zombie is increasing because the advance of various defense mechanisms and the increase of risk in engaging malicious activities.

Table 2: Statistic on Name Servers and IPs

type	number	share-factor (average)
domain	207	n/a
name server	134	1.54
authoritative name server	44	4.71
IP	14440	4.52

Table 3: IP Addresses Being Shared between Domains Reside on the Same Authoritative Name Server.

Auth. Name Server	# of domains	% of shared IPs
atw.kz	2	68.85%
biocacces.ru	5	96.15%
biwcacecca.ru	10	98.23%
blo.kz	2	99.91%
xincacec.ru	10	100%
xginzecac.ru	10	98.03%
solisalo.net	8	80.83%
sccacxoec.ru	9	97.81%
needhed.com	15	20.32%
myhappyplants.com	8	81.33%
mkijsppc.ru	5	98.41%
kamisca.com	11	6.65%
breakwinner.com	12	98.29%

4.2 Sharing, Clustering

We further check the following characteristics: the statistic of the name servers, the statistic of the authoritative name servers and the statistic of IPs. The results are listed in Table 2. The "share-factor (average)" means on average how many domains share the same resource (e.g., name server, IP address).

On average, every 4.7 fast flux domains share the same authoritative name server and every 4.5 fast-flux domains share one IP address. One of the potential reasons is these authoritative name servers are normally "bullet-proof" hosting servers and the registration expenses on these servers (e.g. $100 per year) are higher than the expense on the fast-flux domains (e.g., around $10 per year depending on the tld). On the contrary, the name servers are bearly shared among fast-flux domains.

Besides, we also found a high level of sharing of IP addresses between name servers and the domains. For example, on average, over 70% of the name servers actually share IP addresses with the fast-flux domains. This indicates that the infected hosts are serving as both the front proxy and the DNS server at the same time.

Moreover, we identify the two levels of sharing of IP addresses. The first level of sharing of IP addresses happens among different fast-flux domains that reside on the same authoritative name server; the second level of sharing of IP addresses happens among different authoritative name servers. As shown in Table 3. In most authoritative name servers (11 out of 13 authoritative name servers), over 80% of the IP addresses are actually shared between the domains resided on this name server. On the second level, we calcu-

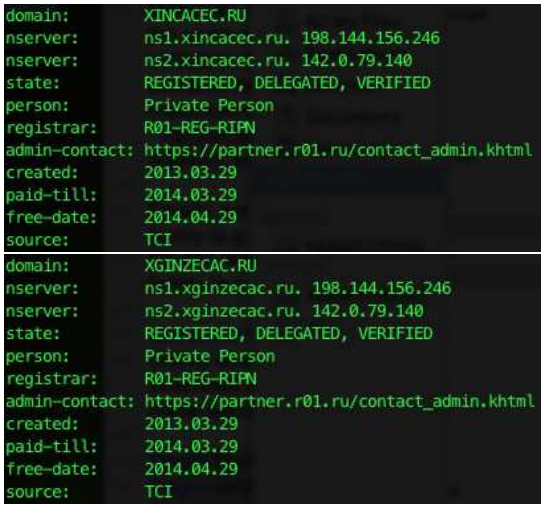

Figure 2: Registration Information of "xginzecac.ru" and "xincacec.ru"

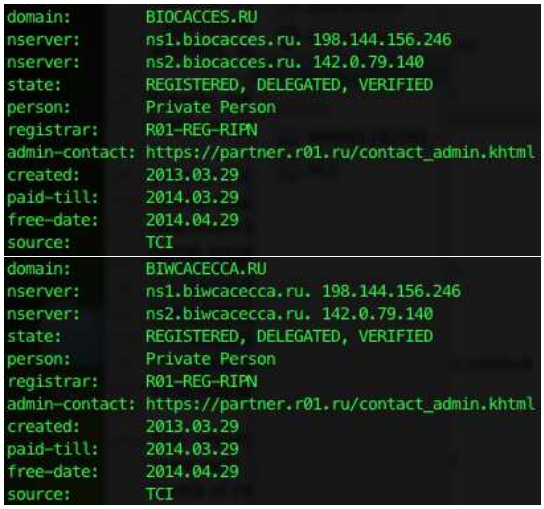

Figure 3: Registration Information of "biocacces.ru" and "biwcacecca.ru"

lated the IP addresses shared between each pair of the 13 authoritative name servers. The maximum shared percentage of IP addresses is 76.27%, which is between "biocacces.ru" and "biwcacecca.ru". The next highest percentage of shared IP address is between "xginzecac.ru" and "xincacec.ru". Further investigation (Figure 2 and Figure 3) shows that "biocacces.ru" and "biwcacecca.ru" are actually registered using the same name server IP address, so does "xginzecac.ru" and "xincacec.ru". This results suggest that the percentage of shared IP addresses is larger between domains sharing the same authoritative name servers than between different authoritative name servers.

Finally, we also discovered the sharing that happens among inter-malware-family (e.g., sharing IP addresses among different malware families) and intra-malware-family (e.g., sharing IP addressed among different fast-flux domains within the same malware family). The results are listed in Table 4. We list the four Trojan families and all the spam domains. We noticed that for Trojan, the percentage of intra-family shared IP address is between 10% to 20%. For spam, the percentage of intra-family shared IP address is much higher, around 45%. This suggests that among different spam families, IP addresses are more frequently shared. We believe this is because spams, despite different family, often focus on the similar and limited number of topics (e.g., pharmaceuticals, dating, financial, etc.) For inter-family sharing between different Trojan families, we found that most of the Trojan families do not share any IP addresses with other families. This is different from spam because different Trojan families may serve very different malicious purposes which require the infected hosts to be uniquely owned, hence less IP addresses are shared among different Trojan families.

Table 4: IP Addresses Being Shared between Domains in the Same Family.

Type/Family	# of domains	% of shared IPs
TrojanDownloader.waledac	8	12.36%
Trojan.GenericKDZ	2	21.04%
Trojan-Psw.tepfer	2	20.30%
Trojan-Spy.zbot	4	12.51%
spam	18	45.71%

4.3 Double-flux OR N-flux?

Unlike double-flux network, we noticed many fast-flux domains actually appear to be using "n-level flux". For example, the definition of double-flux network describes both A, and NS records changing. However, we observed that the level of NS records appears to be "endless". That is, there seems to be "n-levels" of name servers as Figure 4 shows.

The understand the reason behind this case, we also compared the returned IP addresses of different levels of name servers. At the beginning, the IP addresses seem irrelevant. Later, the IP addresses from different levels of the name servers start to overlap. For example, in the case of "larstor.com", we track the ip addresses of 3 levels of name servers, e.g. "ns*.larstor.com", "ns*.ns*.larstor.com" and "ns*.ns*.ns*.larstor.com". The results show that for name servers with level equal or larger than two, over 50% of their IP addresses are resolved to more than one name servers. All these facts suggest that the "n-level" of name servers are probably wildcard like DNS response to flux the IP addresses of bot/zombie.

Another characteristic is that the number of the IP addresses mapped to the first level name server is almost the sum of IP addresses mapped to the higher levels name servers.

4.4 One IP at A Time

Unlike traditional fast-flux networks that response with a list of IP addresses (e.g., round-robin DNS). We noticed that the DNS queries to some fast-flux domains we monitored only return one IP address at a time with TTL=0. This scheme seems to maximize the flux change rate, but the fact is the total number of IP addresses after observing for certain time does not increase comparing with the name servers that

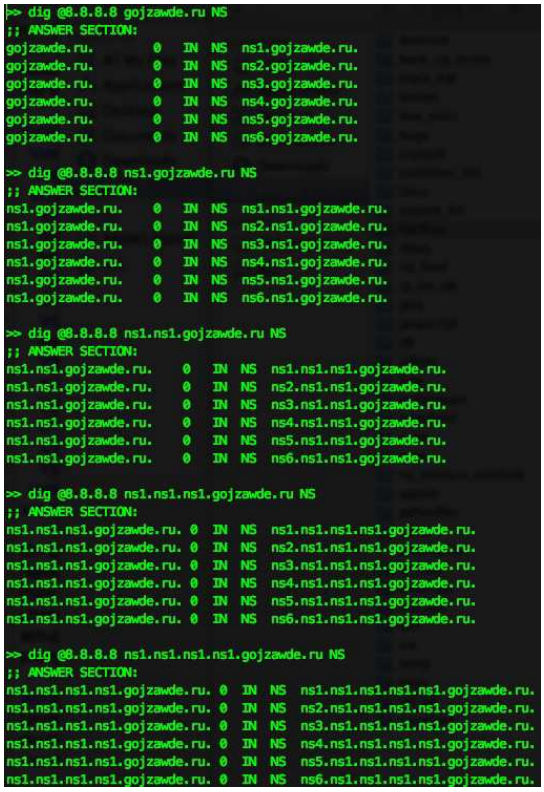

Figure 4: An Example of n-flux domain

return a list of IP addresses. Therefore, we believe the only benefit for attackers to set TTL equals to zero is to nullify the local DNS cache to achieve better control.

5. BENIGN SYSTEMS LOOK ALIKE FF NETWORKS

5.1 Distributed Service

BitCoin DNS seed

As mentioned in [6]: "Upon startup, if peer node discovery is needed, the client then issues DNS requests to learn about the addresses of other peer nodes. The client includes a list of host names for DNS services that are seeded. As-of May 17, 2012 the list (from net.cpp[1]) includes":

- bitseed.xf2.org
- dnsseed.bitcoin.dashjr.org
- dnsseed.bluematt.me
- seed.bitcoin.sipa.be

Among these 4 servers, we tracked the two "dnsseed.bluematt.me" and "seed.bitcoin.sipa.be". "dnsseed.bluematt.me" is resolved to 7747 different IPs and "seed.bitcoin.sipa.be" is resolved to 17061 different IPs. The statistics on the IPs and A & NS DNS records are listed in Table 5.

NTP Pool As mentioned in [4, 5]: "pool.ntp.org uses DNS round robin to make a random selection from a pool of time servers who have volunteered to be in the pool. This is usually good enough for end-users". We tracked "pool.ntp.org" and five of its sub-domains "asia.pool.ntp.org", "europe.pool-.ntp.org","north-america.pool.ntp.org","oceania.pool.ntp.org" and "south-america.pool.ntp.org". The statistic on these NTP pool servers are similar, we only list the "pool.ntp.org" in Table 5.

CDN We also find several domains using CDN. One example is "download.phoenixai.com.au", which use the name server "ns-01.cloudfront.net", "ns-02.cloudfront.net". The details are listed in Table 5.

5.2 Censorship Bypass

Another special type of benign domains that behave like fast-flux domains is so-called anti-censorship domains. These domains are more like fast-flux domains than the above three types of benign domains, because this type of domains also leverage dynamics of DNS to prevent itself from being blocked or suspended. One example is "Dynamic Internet Technology" [2]. This company sets up many subdomains under "ziyouforever.com". The average changing rate is listed in Table 5.

In summary, the DNS records in these three distributed systems change faster than the average values in the fast-flux networks. This is because: 1) special purposes in the use of DNS system require faster change of DNS records, such as providing constantly updating server information and peer discovery; 2) providing high availability for benign content delivery. This observation indicates: 1) "fast" (in terms of the changing rate of both A and NS records) may no longer be the dominant characteristics of malicious Fast-flux networks; 2) reputation based detection approaches should be adopted in future since the behavior in DNS system between benign fast-flux alike domains and malicious fast-flux domains is very similar.

6. DEFENSE

Given the new characteristics of the Fast-flux network. We propose the following suggestions on the defense mechanisms:

- Not relying on the changing rate of IP addresses and name server addresses. As we have demonstrated, fast-flux domains have shown slower changing rate than they used to be. Besides, the changing rate of addresses in benign applications have passed that of fast-flux. Therefore, we suggest that the detection of fast-flux should not rely on the chaining rate of addresses. In the same sense, the geographically distribution of addresses is also not a reliable indicator for fast-flux domains. In stead, the detection should based on the accumulation of evidence of fast-flux domains. Such evidence includes the maliciousness of the name servers, the reputation of the registrar and the nature of the IP addresses (e.g., residential IP addresses).
- Introduce name server reputation score that can measure the probability of hosting fast-flux domains. Since we noticed that name servers often reside on so-called "bullet-proof" servers. These name servers are not

Table 5: Change Rate of Benign System

domain	type	Minutes/IP	IP/Day	A-TTL	NS-TTL
dnsseed.bluematt.me	average	3.26	442.05	55.85	86400
seed.bitcoin.sipa.be	average	1.91	754.70	55.79	39148
pool.ntp.org	average	14.79	97.39	80.2696	3600
download.phoenixai.com.au	average	17.73	81.23	59.81	65535
*.1.ziyouforever.com	average	7.32	196.66	59.98	38400

likely to be taken down as often as fast-flux domains and have been observed in the hosting of multiple fast-flux domains. It is clear that these name servers are more valuable assets for the owners of the fast-flux networks. Therefore, we should build reputation on known malicious name servers to identify and block domains using these name servers for DNS resolving. Such reputation can be build by the accumulation of historical evidence that show involvement in the identified fast-flux domains.

- Based on our discoveries of the sharing and clustering among different fast-flux domains, we also suggest building a connection between different domains by the number of their shared IP addresses. In such, when one domain is identified as fast-flux domain, all connected domains that share a large enough portion (e.g., a threshold on the percentage of shared IP addresses) of the IP addresses are very likely fast-flux domains as well. Moreover, by maintaining the connection between domains, we can also identify the family/type of fast-flux domains by inferring from one domain to another when the number of shared IP addresses between two domains passes the threshold for intra-malware-family.

- leveraging the appeared "n-flux" structure in the DNS system for fast-flux domain detection. Although fast-flux domains are not actually implementing the "n-flux" structure as their name resolving process, it is a unique feature of the fast-flux domains. Therefore, we suggest that by actively testing the existence of "n-flux" structure, we can identify the fast-flux domains or at least suspicious fast-flux domains.

7. CONCLUSIONS

In this work, we discovered several new features of fast-flux domains/networks by tracking over 200 fast-flux domains and their name servers. We present these features and also discuss the rationale behind these features. Meanwhile, we also identified and studied three representative benign applications that exhibit similar behavior as fast-flux domains. Based on our findings, we proposed four detection mechanisms that can cope with the new characteristic observed in fast-flux domains.

8. REFERENCES

[1] Know your enemy: Fast-flux service networks, 2008.

[2] Dynamic internet technology, 2013.

[3] How much do domain names cost, 2013.

[4] Ntp pool, 2013.

[5] Ntp pool time servers, 2013.

[6] Satoshi client node discovery, 2013.

[7] T. Holz, C. Gorecki, K. Rieck, and F. C. Freiling. Measuring and detecting fast-flux service networks. In *NDSS*, 2008.

[8] M. Konte, N. Feamster, and J. Jung. Fast flux service networks: Dynamics and roles in hosting online scams. In *TechReport*, 2008.