SAC 025
SSAC Advisory on Fast Flux Hosting and DNS

An Advisory from the ICANN
Security and Stability
Advisory Committee
(SSAC)
January 2008

Introduction

"Fast flux" is an evasion technique that cyber-criminals and Internet miscreants use to evade identification and to frustrate law enforcement and anticrime efforts aimed at locating and shutting down web sites used for illegal purposes. Fast flux hosting supports a wide variety of cyber-crime activities (fraud, identity theft, online scams) and is considered one of the most serious threats to online activities today. One variant of fast flux hosting, "double flux", exploits the domain name registration and name resolution services.

This Advisory describes the technical aspects of fast flux hosting and fast flux service networks. It explains how the DNS is exploited to abet criminal activities that employ fast flux hosting, identifying the impacts of fast flux hosting, and calling particular attention to the way such attacks extend the malicious or profitable lifetime of the illegal activities conducted using these fast flux techniques. It describes current and possible methods of mitigating fast flux hosting at various points in the Internet. The Advisory discusses the pros and cons of these mitigation methods, identifies those methods that SSAC considers practical and sensible, and recommends that appropriate bodies consider policies that would make the practical mitigation methods universally available to registrants, ISPs, registrars and registries (where applicable for each).

Background

Security professionals, the anti-cybercrime community, and law enforcement agencies have studied fast flux hosting for some time. Fast flux hosting operates on top of a large, distributed network of compromised systems that may very well span the globe. A thriving underground business leases dozens to thousands of compromised systems to Internet miscreants as fast flux service networks[1]. Operators of these service networks utilize hierarchical covert (encrypted) communications channels and proxy techniques. They manage these networks with some diligence by routinely querying the status of compromised systems and base adds and deletes to the networks based on the presence or absence of a response. Of particular concern to the domain name community is the way these operators automate domain name service updates to hide the location of web sites where illegal activities – IP Piracy (music, videos, games), hosting of child pornography, hosting of phishing systems, sales of illegal pharmaceuticals, and execution of identity theft and fraud – are performed.

One variant of fast flux hosting uses rapid updates of DNS information to disguise the hosting location of web sites and other Internet services that host illegal activities. In a second variant, called "double flux", Internet miscreants complement the service network that hosts web sites with a second service network that hosts DNS servers. The operation of these service networks is described in available detail in the ensuing sections of this Advisory.

[1] Security organizations use a variety of terms when describing fast flux hosting in their literature and publications. In this Advisory, we apply the terminology from a Honeynets Project Report, *Know Your Enemy: Fast Flux Service Networks*, see http://www.honeynet.org/papers/ff/

Terminology

To describe this complicated, multi-faceted fast flux technique to the extent currently possible, SSAC begin by identifying some of the terms the Internet security community associates with fast flux hosting:

botnet. A botnet is a network of compromised third-party computers running software (ro)bots. These bots can be remotely controlled – initially by the actual attacker, and subsequently by a party who pays the attacker for use of the botnet – for any number of unauthorized or illegal activities. The attacker is typically associated with an organized criminal element. The attacker will install "bot software" without notice or authorization on a PC via a spyware download or virus attached to an email message, and more commonly, through browser or other client-side exploits (e.g., compromised banner advertising). Once the bot is able to execute, it establishes a back-channel to a control infrastructure setup by the attacker. The traditional botnet design employed a centralized model, and all back-channels connected to an attacker's command-and-control center (C&C). Recently, botnet operators have employed peer-to-peer models for back-channel operation to thwart detection of the C&C via traffic analysis.

bot-herder. The architect and perpetrator of the distributed attack that is used to create, maintain, and exploit a botnet for financial or other (political) gain. Once a botnet is established, the bot-herder leases use of their botnet to a facilitate a **Fast Flux service operator**

Fast flux. This phrase is used to represent the ability to quickly move the location of a web, email, DNS or generally any Internet or distributed service from one or more computers connected to the Internet to a different set of computers to delay or evade detection.

Fast Flux facilities. In this paper, the term *facility refers* to a software agent that has been installed without consent onto large numbers of computers across the Internet.

Fast Flux service network. In this paper, a service network refers to a subset of bots that the bot-herder assigns to a given Fast Flux service operator who in turn provides its customer with facilities for fast flux hosting or name service. Note that this service network is often times operated by a "middle man", not by the customer themselves.

Anatomy of Fast Flux Hosting

The description that follows is representative of fast flux hosting. Other manifestations and variations are likely, and attackers may alter future fast flux hosting to evade methods to detect fast flux hosting as it is described here, or add additional layers of hierarchy or abstraction.

While considerable attention is paid to the technical aspects of fast flux, an associated set of "business" activities exists and begs description as well. We consider the case where a miscreant wants to conduct a phishing attack.

The business aspects of fast flux hosting begin with malware authors. Some malware authors develop phishing kits, software packages that can be customized to deliver phishing email to a list of recipients and host the associated illegal web site where the phish email sends victims. Others farm email addresses and sell lists for spam. Still others develop bot software. Bot software is a flexible, remotely controllable agent that can be directed to perform arbitrary functions on behalf of a corresponding **command and control center** (C&C) software: once covertly installed on a compromised system, bot software facilitates subsequent downloads and remote execution of additional, attack-specific software. Bot-herders often use email borne worms to infect and compromise thousands of systems, although client-side compromises, such as browser-based exploits, are the most prominent today.

Malware authors and bot-herders are *goods providers* in the cyber-criminal community. Goods providers use encrypted and private/secure Internet Relay Chat (iRC) channels or similar underground meeting places to advertise and find buyers for their criminal goods[2]. A bot-herder's criminal goods are essentially the facilities he can make available for fee or lease. The herder leases the command and control of a negotiated number of compromised systems to a customer, who may use them directly or manage them on behalf of yet another miscreant; in the latter case, the bot-herder's customer serves as a provider of fast flux hosting services. In this complex and covert economy, a party who is interested in conducting criminal activities may negotiate with several parties to obtain a spam (phish) list, deploy a phishing system or other attack kit, and a botnet and conduct the attack himself, or he may negotiate with one party, a fast flux service network operator, to direct the phishing attack on his behalf.

In fast flux hosting, fast flux service networks are used for two purposes:

1) **To host referral web sites**. Bots in this service network typically do not host the fast flux customer's content but will redirect web traffic to the web server where the fast flux customer hosts unauthorized or illegal activities. When this is the only network operated for fast flux hosting, the term *single flux* is applied.

2) **To host name servers**. Bots in this service network run name server referrers for the fast flux customer. These name servers forward DNS requests to hidden name servers that host zones containing DNS A resource records for a set of referral web sites. The hidden name servers do not relay responses back through the referring name server but reply directly to the querying host. When this second network is operated in conjunction with (1) to enhance the deception, the term *double flux* is used.

[2] See "Market Activity" as described in *An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants, see http://*www.cs.cmu.edu/~jfrankli/acmccs07/ccs07_franklin_eCrime.pdf

Figure 1 illustrates these relationships.

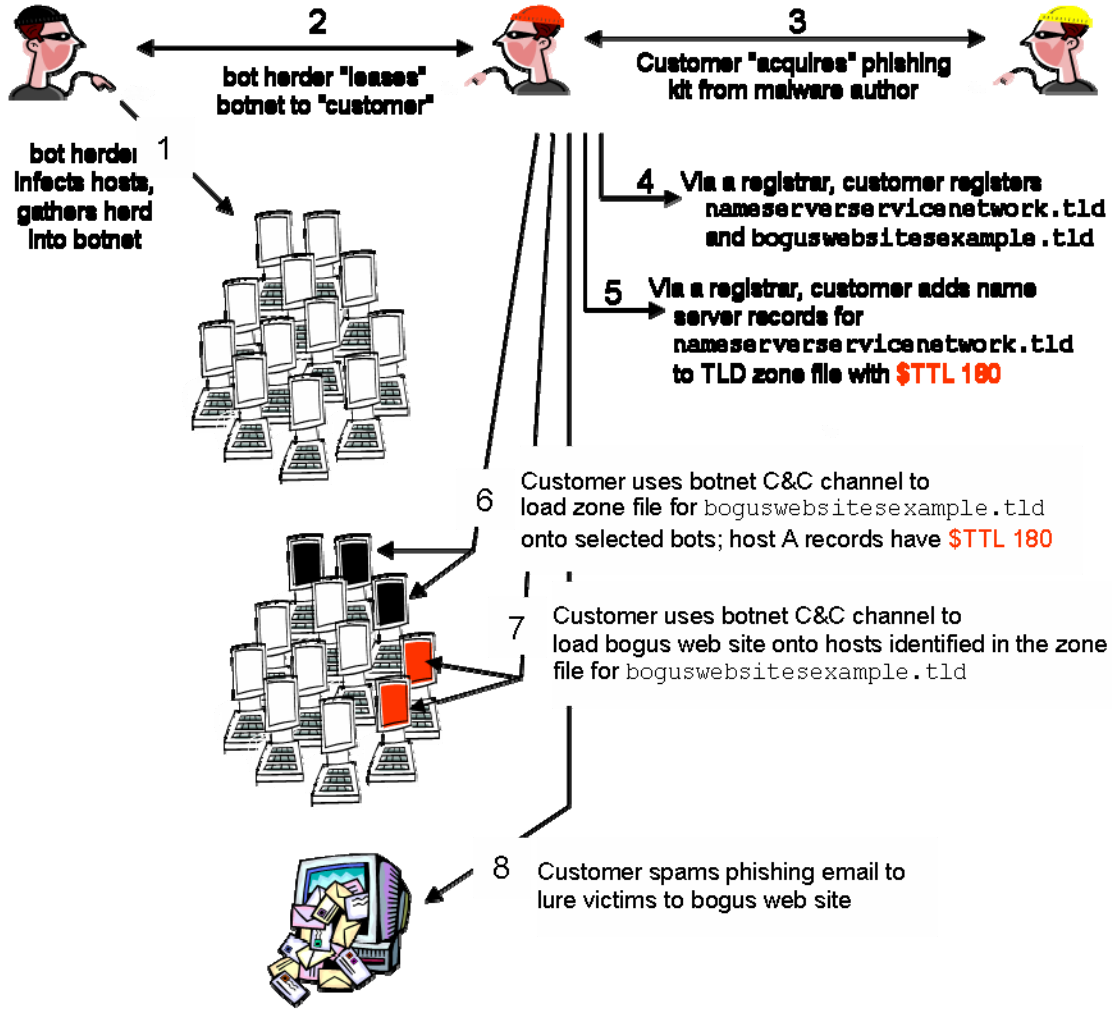

Figure 1. Elements of a "double flux" hosting attack

Exploiting Name Service: Double Flux Hosting

Fast flux customers often register domain names for their illegal activities at an accredited registrar or reseller. In one form of attack, the fast flux customer registers a domain name (for a flux service network) to host illegal web sites (`boguswebsitesexample.tld`) and a (second or several) domain name(s) for a flux service network to provide name resolution service (`nameserverservicenetwork.tld`). The fast flux customer identifies these domains to his fast flux service network operator. The fast flux service network operator uses automated techniques to rapidly change name

server information in the registration records maintained by the registrar for these domains; in particular, the fast flux service network operator

- changes the IP addresses of the domain's name servers to point to different hosts in the domain `nameserverservicenetwork.tld` and
- sets the times to live (TTLs) in the address records for these name servers to a very small value (1-3 minutes is common).

Resource records associated with a name server domain used in fast flux hosting might appear in a TLD zone file as:

```
$TTL 180
boguswebsitesexample.tld.       NS  NS1.nameserverservicenetwork.tld
boguswebsitesexample.tld.       NS  NS2.nameserverservicenetwork.tld
…
NS1.nameserverservicenetwork.tld.    A  10.0.0.1
NS2.nameserverservicenetwork.tld.    A  10.0.0.2
```

Note that the time-to-live (TTL) for the resource records is set very low (in the example, 180 seconds). When the TTL expires, the fast flux service network operator's automation assures that a new set of A records for name servers replaces the existing set:

```
$TTL 180
boguswebsitesexample.tld.       NS  NS1.nameserverservicenetwork.tld
boguswebsitesexample.tld.       NS  NS2.nameserverservicenetwork.tld
…
NS1.nameserverservicenetwork.tld.    A  192.168.0.123
NS2.nameserverservicenetwork.tld.    A  10.10.10.233
```

The window of opportunity to identify and shut down the name servers that support this fast flux attack is thus very small.

Resource records in `nameserverservicenetwork.tld` point to proxy or referrer hosts rather than the bots that provide name resolution for `boguswebsitesexample.tld`. The referrer hosts listen to port 53 and forward DNS queries to a "DNS" bot that hosts a zone file for `boguswebsitesexample.tld`. The "DNS" bot resolves the domain name of the scam web site to the IP address of a host in the web flux service network and returns the response message directly to the querying resolver. At this point, IP address of the DNS bot is known only to a potentially large pool of referrer hosts, and the IP addresses of the referrers are changing every 180 seconds.

Referral Web Flux Hosting

In the previous section, we describe how double flux hosting adds a level of evasion by employing bots in the `nameserverservicenetwork.tld` network and rapidly changing the A records of the referral web server hosts in the `boguswebsitesexample.tld` network. The A resource records of the referral web servers are also configured with short TTLs. When the TTLs of the web server hosts expire, the fast flux service network operator's automation once again assures that a new set of A records for web servers

replaces the existing set. Thus the window of opportunity to identify and shut down the referral web servers that support this fast flux attack is very small.

Records associated with the illegal web site might appear in a zone file hosted on a DNS bot in the `nameserverservicenetwork.tld` network as:

```
boguswebsitesexample.tld.     180   IN    A     192.168.0.1
boguswebsitesexample.tld.     180   IN    A     172.16.0.99
boguswebsitesexample.tld.     180   IN    A     10.0.10.200
boguswebsitesexample.tld.     180   IN    A     192.168.140.11
```

Note again that the time-to-live (TTL) for each A resource record is set very low (in the example, 180 seconds). When the TTL expires, the resource records would be automatically modified to point to other bots that host this illegal web site. Only minutes later, the zone file might read:

```
boguswebsitesexample.tld.     180   IN    A     192.168.168.14
boguswebsitesexample.tld.     180   IN    A     172.17.0.199
boguswebsitesexample.tld.     180   IN    A     10.10.10.2
boguswebsitesexample.tld.     180   IN    A     192.168.0.111
```

The combined effects of rapidly updating A records in the `boguswebsitesexample.tld` zone and name server A records in the TLD zone is frustratingly effective in keeping illegal sites in operation for longer periods of time than sites that do not use fast flux.

Fast Flux Hosting: Related to Domain Name Tasting?

To some, domain name tasting and phishing are related activities[3]. The Anti-Phishing Working Group (APWG) has published a report on the relationship between tasted domain names and phishing attacks. The report summarizes the findings of two studies that sought to determine whether parties who taste domain names also use these names to facilitate phishing attacks. One APWG member began with a set of domain names that had been used in phishing attacks and tried to determine if these names had been cancelled during the Add Grace Period. A second APWG member matched domain names used in phishing attacks against a list of approximately three million domain names that were tasted during a one week period. The results of both studies indicate that "there are very few cases of possible domain name tasting performed by phishers and that the cases that do exist have possible explanations that are not related to tasting"[4].

Phishing attacks increasingly use fast flux hosting (especially attacks against major financial institutions); thus, SSAC concludes that there is no meaningful relationship between domain name tasting and fast flux hosting. SSAC also observes that the goals of fast flux hosting and domain name tasting are not identical. A primary objective of fast flux hosting is to extend the lifetime of a site that hosts illegal activities that are historically proven to be profitable and these include financial information and credit card theft. Stolen credit cards are used to pay phish site domain name registration fees, so

[3] See CADNA Background, http://www.cadna.org/en/index.html
[4] APWG: The Relationship of Phishing and Domain Name Tasting, http:// www.antiphishing.org/reports/DNSPWG_ReportDomainTastingandPhishing.pdf

there is no incentive to register a name and dispose of it. By comparison, domain tasters are only interested in paying registration fees for domain names that will prove to be profitable in a trial window of a few days.

Current and Possible Mitigation Alternatives

Several mitigation alternatives can be implemented to reduce the threat fast flux hosting poses.

Shut down the bots that host fast flux facilities

Bot-herders compromise computers on business and residential networks. However, a bot-herder typically exploits poorly secured computers that are connected to residential broadband access circuits (cable modem and DSL) as the likelihood of finding an exploitable host is greater here than on networks managed by experience IT staff. Education, government, or enterprise hosts are vulnerable to system compromise, but they are, on average, less susceptible to compromise and exploitation attempts are at greater risk of detection by network administrators.

Mitigation methods that are available today and can be widely implemented to reduce the number of PCs that can be exploited and used to host bot software include (but are certainly not limited to):

a) Improved desktop security measures (antivirus, antispyware, personal firewall software, host intrusion detection software) on hosts in both private and public (i.e., residential broadband access service) networks.
b) Deployment of anti-malware gateways by ISPs for residential broadband access customers; by managed security service providers or internal security administrators for business networks and increased adoption of anti-malware gateways by security administrators of private networks.
c) Education, awareness and training, with a particular focus on understanding and applying stringent egress traffic enforcement policies.

Additional mitigation methods to consider include:

d) Process and executable white listing.
e) Network access/admission controls.
f) Analysis of known botnet behaviors, development of detection technique (e.g., signature) that can be used to block the activity at a "threat management" security gateway. This is a logical extension to (b), above.)

While seemingly the most practical, methods (a) and (b) have not proven effective in mitigating the malware threat. Storm[5] and similarly designed malware can be altered and distributed on a periodic basis by its creators using yet undetected bots[6] and signature-

[5] Storm Worm DDoS Attack, http://www.secureworks.com/research/threats/view.html?threat=storm-worm
[6] *Imperfect Storm aids spammers*, http://www.securityfocus.com/news/11442

based anti-malware measures have not been effective in eradicating malicious software such as the Storm trojan program[7]. PCs these malware infect expand the herd more quickly than the community can identify and disinfect compromised PCs. Education and awareness (c) is a painfully slow process. The CSI/FBI Computer Crime and Security Survey reports that 97% of PCs run antivirus software and 79% run antispyware software, but bot infections are alarmingly high: in June 2007, the US FBI announced that its ongoing cybercrime initiative to combat botnets had identified over one million PCs compromised with bot software, within the FBI's U.S. jurisdiction alone[8]. These figures apply to enterprise/business networks. Among residential broadband users, the use of antivirus and antispyware software is not as high, security and network configurations are more likely neglected, and subscriptions for anti-malware definition updates are often allowed to lapse.

Process and executable white listing is a malware prevention technique that enforces an executable policy; specifically, all but a trusted set of applications and related processes will be prevented from running on a PC. Executable white listing is not widely implemented, especially among consumer/residential Internet users. The diversity of applications, pace of introduction of new applications, the lack of commercial offerings that are consumer-friendly, and services that would serve as trusted authorities for white lists (if this model is even tractable) are factors that inhibit adoption.

Today, network access/admission control solutions are being developed that aim to prevent unsecured endpoints from connecting to LANs and WLANS. A security assessment is performed on a computer to determine if it is free of malicious executables prior to allowing that computer to connect to the Internet. If the computer is compromised, it is quarantined and cannot reconnect until the security violation is corrected for residential broadband (e) is not widely implemented and would require additional standards and software development. ISPs and residential broadband access providers indicate that they cannot bear the cost to implement and manage network access and ingress traffic filtering.

Shut down the fast flux hosts

A considerable number of compromised hosts used in such attacks are PCs connected to residential broadband services. These PCs typically host referrer web and name server bot software.

Incident detection, isolation and response are the most common mitigation procedures practiced today. First, a system is identified or reported as hosting illegal activities. In the fast flux hosting scenario, this might be a referrer web or name server or the system that host the illegal web site, anticrime responders gather information about the site: location and jurisdiction of the hosting system; the domain owner, site administrator and ISP; and the type of illegal activity. The responders use WHOIS services and other means to

[7] Common Malware Enumeration CME-711trojan downloader. http://cme.mitre.org/data/list.html
[8] *Over 1 Million Potential Victims of Botnet Cyber Crime,* http://www.fbi.gov/page2/june07/botnet061307.htm

identify and contact several parties - in parallel and repeatedly – until they receive assistance in shutting down the illegal activity[9]:

- In cases where illegal activities appear to be hosted on a compromised system (e.g., on a web server that is conducting legitimate business and the administrator is unaware that the server is also hosting an illegal site), the domain owner is contacted to assist in the shut down.
- The ISP or hosting provider is contacted to request that service to the host be terminated
- In cases where responders require local assistance (language interpretation, corroboration that the responders are good faith actors, or assistance in obtaining further information), local Computer Emergency or Incident Response Teams (CERT/CIRT) are contacted. (In some countries, CERTs encourage responders to contact them as early in the process as possible).
- In cases where bots on PCs host name servers, registrars or registries are contacted to remove NS records from TLD zone files or suspend domains.

The illegal sites themselves may operate from compromised servers in legitimate domains, shared-hosting web site providers, or (quasi-)legitimate, "bulletproof" web hosting facilities[10]. In cases where cooperation is not forthcoming - where operators and local authorities do not acknowledge or trust the responders, or are unwilling to act based on information responders and CERTs provide – responders may ask law enforcement agents (LEAs) for assistance or seek court orders to compel the operator to take down the site. These are typically last-resort actions since the time frames required to identify and coordinate with LEAs and obtain court action in the appropriate jurisdiction is often days and weeks, and responders seek to take down illegal sites in hours.

Rapid modification of A resource records that resolve to the fluxed referral web servers thwarts detection and hampers measures to shut down fast flux hosting sites. In many cases, the life time of a fast-flux hosted illegal site is extended well beyond the average of approximately 4 days[11].

Improvements to this form of mitigation include:

[9] This scenario, related through personal correspondence with responders, is representative of methods used to respond to phishing attacks where fast flux hosting is aggressively employed.

[10] Bulletproof hosting refers to web and bulk email hosting providers who impose little or no terms of service governing the content and activities hosted on their servers. The term "bulletproof" is used to emphasize that services hosted at such providers will not be taken down. Many bulletproof hosting providers do not act in perfectly good faith with law enforcement and anticrime organizations, and they operate in jurisdictions where local authorities and Internet laws offer a relatively safe harbor for illegal activities.

[11] APWG monthly statistics from December 2006 to August 2007 report that phishing sites have average online time of between 3.3 and 4.5 days, see http://www.apwg.org/phishReportsArchive.html; however the average is computed without distinguishing between conventionally hosted phishing sites and those that use fast flux. Since the IPs of the fast flux hosts change rapidly, fast flux hosting has contributed to *lowering* the metric.

1) Adopting procedures that accelerate the suspension of a domain name, to eliminate the problem of illegal sites that are shut down but are quickly re-hosted on a different server, at a different ISP.
2) Better coordination and information sharing across responders, LEAs, and CERTs. Including a database(s) containing points of contact (languages spoken), information about jurisdictional requirements, conventions, and other information that is useful in typical suspension activities.

Remove domains used in fast flux hosting from service

In some take down scenarios, anticrime responders determine that a domain name is being used for fast flux attacks, go to the registrar or registry where the domain name is registered, explain the nature of the problem, and convince the registrar to take the domain name out of service.

Registries and registrars are not bound by policy to respond in a particular way to complaints regarding fast flux hosting and the fast flux hosting technique in and of itself is not an illegal activity until it is clearly associated with an illegal activity (computer abuse and fraud, identity theft). Registries and registrars set their own policies regarding abuse and implement response procedures independently. However, some common practices exist. Registries will require sufficient information to clearly demonstrate that the domain name is being abused or is abetting criminal behavior and will typically conduct their own investigations. If the registry's own investigation corroborates the data presented by the responder or claimant, the registry may take that evidence to the registrar of record who will typically act quickly to resolve the trouble reported. The registrar's own policy and the ICANN RAA (if applicable for the TLD in which the domain name is registered) affect the registrar's response, which may be to suspend the domain (i.e., use HOLD status to prevent the DNS from resolving the name); suspend the domain name and change the registration record to reflect that the domain name is dispute or the registration policy has been abused; or suspend the domain name and delete it from the zone. Registries typically respond to requests from law enforcement, subpoenas, and court orders in an expeditious manner. Many registries and registrars have general abuse departments, and FAQs and contact forms are often browser-accessible. Registries and registrars might provide similar FAQs and forms to facilitate and expedite communication with LEA and anticrime responders.

Rapid modification of A resource records that resolve to the fluxed referral name servers thwarts detection and hampers measures to shut down fast flux hosting sites.

Mitigations methods that are practiced today, but not uniformly, include:

- Authenticate contacts before permitting changes to name server configurations.
- Implement measures to prevent automated (scripted) changes to name server configurations.
- Set a minimum allowed TTL (e.g., 30 minutes) that is long enough to thwart the double flux element of fast flux hosting.

- Implement or expand abuse monitoring systems to report excessive DNS configuration changes.
- Publish and enforce a Universal Terms of Service agreement that prohibits the use of a registered domain and hosting services (DNS, web, mail) to abet illegal or objectionable activities (as enumerated in the agreement).

Additional detection and mitigation have been suggested. These include:

- **Quarantine (and honeypot) domain names.** Based on a set of to-be-determined criteria, have the registrar suspend name server updates for domain names suspected of being affiliated with a fast flux attack. During the suspension period, observe and log (record) all registrant account activity and record update attempts. This expands the incident analysis window and gives investigators an opportunity to track down the origin of the updates and to identify bots.

- **Rate-limit or (limit by number per hour/day/week) changes to name servers associated with a registered domain name**. Registries and registrars already apply rate-limiting techniques on query-based WHOIS services to discourage abuse. Determine a rate of change that (a) accommodates legitimate applications of short TTLs for NS records in TLD zone files, (b) provides investigators with a window of opportunity to track down the origin of updates and identify bots, and (c) makes short TTLs less useful to fast flux attackers.

- **Separate "short TTL updates" from normal registration change processing.** Treat requests to set TTLs below a certain limit as special requests that require some form of verification.

- **Use suspended domains to educate consumers.** Do not immediately return domains proven to be used for illegal purposes; rather, establish and redirect visitors to a landing page explaining that this domain was suspended because it was used for illegal or objectionable activities, and inform users on ways to detect and avoid being victimized by phishing and other criminal activities.

Findings

SSAC offers the following findings for consideration by the community:

1) Fast flux hosting enables a highly sophisticated attack launching infrastructure that increasingly exploits domain name resolution and registration services to abet illegal and objectionable activities.

2) Current methods to thwart fast flux hosting by detecting and dismantling botnets are not effective.

3) Double flux further thwarts detection and hampers measures to shut down fast flux hosting web sites.

4) Frequent modifications to name server (NS) records by a domain name registrant and short TTLs in name server A records in TLD zone files are signatures that can be monitored to identify potential abuses of name services.

5) Measures that prevent automated changes to DNS information and that set longer minimum TTLs for name server A records in TLD zone files appear to be effective but are not uniformly practiced.

6) Additional measures have been suggested to combat fast flux hosting and merit further study.

Recommendations

Fast flux hosting is a serious and mounting problem that can affect name services in all TLDs. SSAC encourages ICANN, registries and registrars to consider the practices mentioned in this Advisory, to establish best practices to mitigate fast flux hosting, and to consider whether such practices should be addressed in future agreements.