

The Pennsylvania State University
College of Information Sciences and Technology

Shawn Clark

**Domain Name Abuse:
Today and Tomorrow**

Chris Griffith

January, 2010

Abstract

Domain names have been used for various types of profit and soliciting for years. They are used as new portals for most information, knowledge, marketing and collaboration. However, they have also been the subject of abuse in various ways. Domain Names have been used in marketing ploys, advertising schemes even Cybercrime. Their misuses range from unethical, such as Domain Kiting, to illegal in use of botnets or Cybersquatting. Both legal and illegal abuse need to be hindered to make the internet a friendlier and safer environment.

Table of Contents

Abstract	2
Introduction.....	4
Areas of Interest.....	6
Domain Kiting	6
Cybersquatting	10
Botnets	12
Future of Domain Name Abuse	14
Domain Kiting	14
Cybersquatting	15
Botnet.....	16
Conclusion	18
Bibliography	19

Introduction

Within the past three decades the Internet has grown exponentially from DARPA net to the literal World Wide Web. Across the Internet's history, standards have evolved and policies have changed. These policies have been developed for the prevention of cybercrime, which has also grown with the expansion of the internet. With these changes, Domain Names are starting to adapt to securer, stricter and more beneficial guidelines.

Domain Names act as a portal for many different people and organizations. They have been the brains behind the internet, allowing people to remember names and phrases instead of a list of numbers. These names are essential to keeping a sensible internet. Envision having to type in `http://74.125.43.99/` instead of `http://google.com/`, it could become very hard very fast to try and remember someone's favorite websites. To make life easier, the Domain Name Service (DNS) was initiated. However, since its inauguration the DNS has been abused, making life less enjoyable for many. To understand how they are being abused, one must first understand how they operate.

There were originally seven general top-level Domain Names (TLDs) for the internet designated in the 1980s; these TLDs consist of `.com`, `.edu`, `.gov`, `.int`, `.mil`, `.net` and `.org`. fifteen years after the first registered Domain Name, ICANN (Internet Corporation for Assigned Names and Numbers) released thirteen new TLDs to combat the need for increased room and more precise Domain Names in cyberspace.

Domain Names act as a way to always direct traffic to a particular web host. When a client computer is connected to the internet and a domain is entered into the URL bar of a browser, the client's computer itself does not know the location of the requested server. Instead of scouring

every server on the internet until the matching name is found, a Domain Name Server (DNS) is used. The URL is sent to the DNS, and if a website with that Domain Name is found, the DNS will send a message back to the client's computer that contains the location of the server by its IP address.

This is very useful for many reasons:

- If the physical or IP address of the server is prone to change for the server, the client computer does not have to constantly update its location.
- The client's computer does not have to search every server every time a user enters a URL.
- There is less chance of a computer being taken to an illegitimate site, such as a phishing site, if a controlling body monitors where the clients are redirected too.

To better explain how this is useful, imagine an old friend that is prone to moving all around the world. You want to send him some mail or keep in touch with him somehow. He would feel it a burden with all his travels to inform all his friends to update their records each time he moves. Instead, both of you use Facebook and keep updated phone and mailing address. This way, each time he moves all his friends can simply check his Facebook page to see where to send mail instead of relying on him to update his friends on his location at all times. Nevertheless, with this convenient system there are also ways to abuse it.

Cybercrime attempts to keep ahead of the security curve. There are also ways that only legally abuse the system, making it less convenient and a more hostile environment. Either way, these areas need to be addressed that should hinder them so they cannot continue.

Areas of Interest

Predicting and analyzing the future of Domain Names rest in understanding and examining what Domain Names have been through and what the current plans for them entail. There are three areas that are currently talked about concerning Domain Names.

- Domain Kiting
- Cybersquatting
- Botnets

These items have and/or will determine how the internet will be arraigned and accessed in years to come.

Domain Kiting

A large issue for many years was due to a loophole in the ICANN's Domain Name registration process. ICANN allows for a 5 day "Add Grace Period" (AGP) which allowed a newly registered Domain Name to unregister and receive a full refund. The intention of the AGP was so that if a user misspelled their domain or found that what they bought wasn't what they wanted, they could simply have their money back. However, this system could be easily exploited.

Each TLD is overviewed by different operators. These operators allow registrars to buy and sell Domain Names within their domain and enter the data into the DNS servers. Each of these registrars are required to gain certain information from the buyer, and deal with transferring the client's money to both them and the operator, and distributing the Domain Name(s) to the purchaser.

Some registrars took initiative and decided to not only sell Domain Names directly from ICANN, but also to register some domains for themselves and collect data to see if the domain could possibly be worth more than their standard price. A popular method to do so would be when a user goes onto a registrar's site, and checks for a Domain Name, if they do not register within 24 hours, then the registrar would register it for itself. Then, during the five day AGP they would put up a generic page and see how many unique page views there were visiting the site. This process is referred to as domain tasting, because the website is 'taste tested' to see if it is worth purchasing. If the website received a lot of page views, it could be bought by the registrar and sold as a 'premier' webpage; whereas if the page has a low number of page views, they could simply not register it again. With the AGP loophole, the registrar could simply re-buy the website every five days, and be refunded the full amount. This abuse is known as Domain Kiting and is more destructive to potential buyers, forcing them to pay a higher price for an unregistered Domain Name (Parsons 2006, Messmer 2009).

This means the registrar could practically own a website without having to pay for it. The AGP effectively gave a way to collect profitable web traffic information without having to pay ICANN anything. This could appear to be something negligible, however the statistics say otherwise.

Figure 1.1, courtesy of ICANN, shows that between four popular TLDs, over 17 million domains were registered than dropped.

Fig. 1.1 - AGP Deletes Activity per TLD

TLD	Operator	8-Jun
.COM	VeriSign, Inc.	15,738,292
.INFO	Afilias Limited	32,384
.NET	VeriSign, Inc.	1,860,164
.ORG	Public Interest Registry	35,052
Total Dropped		17,665,892

ICANN found this to be outrageous and a clear abuse of the system. For every Domain Name registered it cost approximately \$0.20 for ICANN to insert the domain into the DNS. In July of 2008, ICANN took action and wrote a provision to not refund the twenty cents it cost them to update the information (Taranfx 2009).

Twenty cents does not seem like a lot of money, but if a registrar was collecting data on upwards of 50,000 domains, it would cost them 10,000 dollars now, when it used to be free. There were dramatic improvements overnight.

Fig. 1.2 - AGP Deletes Activity per TLD

TLD	Operator	8-Jun	8-Jul
.COM	VeriSign, Inc.	15,738,292	2,483,953
.INFO	Afilias Limited	32,384	18,945
.NET	VeriSign, Inc.	1,860,164	249,958
.ORG	Public Interest Registry	35,052	30,255
Total		17,665,892	2,783,111

Figure 1.2 shows that in a single month, more than 14 million less domains were deleted during the AGP. This is obvious proof that there was a heavy use or misuse rather, of the Add Grace Period. ICANN considered this a successful step to stop domain tasting; however it was only the first step to end domain tasting. In April of 2009, ICANN released a new policy that eliminated the Domain Kiting practice.

On August 12th, 2009, ICANN released a status report entitled "The End of Domain Tasting." This report details the previous two revisions of the AGP, and a new action which has statistically been proven that it stopped domain tasting. Instead of a registrar only owing twenty cents to the operator for each AGP delete, they now are given 10% of their net registered

domains worth of free add grade period drops. Any excess domains removed over that 10% would result in no refund for the registrar. The example below of this will demonstrate how both the provision and policy would impact a registrar (ICANN).

A registrar who registers 1000 new domains, and drops 200 of them during the Add Grade Period would have a net of 800 new domains.

- Originally there would be no cost to the registrar
- After the provision was in place, they would owe \$40 to the operator
 - \$0.20 penalty x 200 removed domains
- After the new policy, the registrar would owe \$810
 - \$6.75 (example price of an .org domain) x 120 (10% of net domains are free, in this case 80 is 10% of the net 800. The remaining 120, 200 dropped - 80, have to be paid for by the registrar)

Fig. 1.3 - AGP Deletes Activity per TLD

TLD	Operator	8-Jun	8-Jul	9-Apr
.COM	VeriSign, Inc.	15,738,292	2,483,953	37,519
.INFO	Afilias Limited	32,384	18,945	4,460
.NET	VeriSign, Inc.	1,860,164	249,958	6,202
.ORG	Public Interest Registry	35,052	30,255	2,591
Total		17,665,892	2,783,111	50,772

This policy made it no longer practical for registrars to include domain tasting in their business model (Whitney 2009).

Fig. 1.4 - AGP Deletes Trend

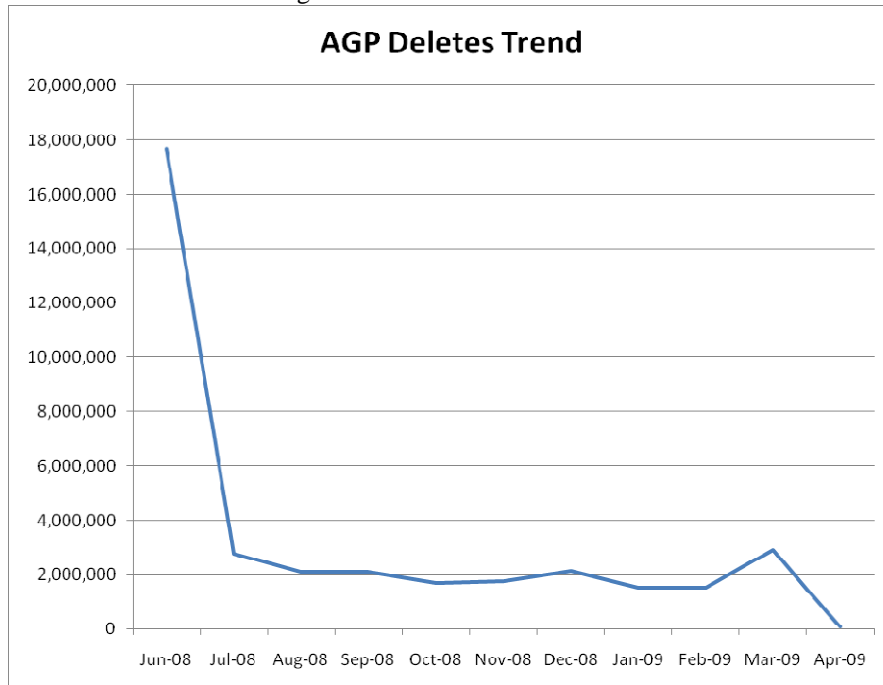


Figure 1.3 shows the dramatic reduction of domain tasting over the previous two years. Figures 1.4 also clearly illustrate the dramatic impact that both the provision and policy had on Domain Kiting. ICANN's newest policy has done exactly what they claimed; ICANN has ended the practice of Domain Kiting.

Cybersquatting

The battle over Domain Tasting is over, but the fight over Cybersquatting continues.

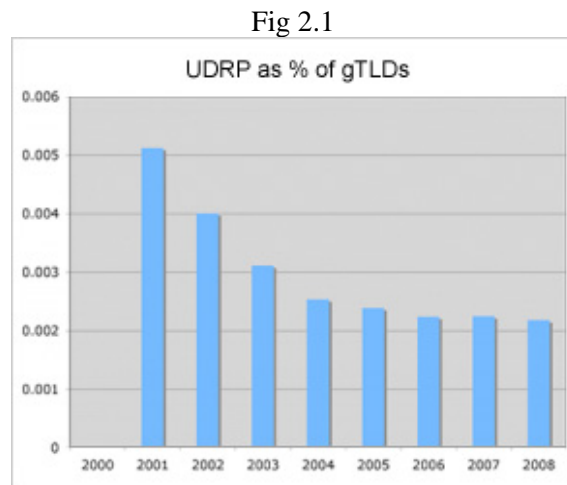
Cybersquatting is the practice of registering and/or using a Domain Name in bad faith, generally aimed at an existing website. A more specific type of Cybersquatting, called typosquatting, are sites that sound, look or are a close mistype of an existing site.

Cybersquatting is an illegal action that is classified as Domain Name Abuse. The actions of Cybersquatting can deter business from an already existing site, or can even be used for Cybercrime. This will result in either lost business to companies or even lost money to a

competing site. A site that is capitalizing on Cybersquatting commonly has pay-per-click advertisements that are related to a product or service that the site they are mimicking offers.

The Coalition Against Domain Name Abuse (CADNA) has been trying to help raise awareness of Cybersquatting, along with helping existing sites fight Cybersquatters. They will assist websites file complains under ICANN's Uniform Domain-Name Dispute-Resolution Policy (UDRP) which all registrar's must comply with. However this process is lengthy, generally six months long, expensive, average \$1,500 per complaint, and has minimal penalties or deterrence for the perpetrators (Jamison 2009).

World Intellectual Property Organization (WIPO) collects statistis of the number of Uniform Domain-Name Disputes each yeah. Statistically we are almost identical to previous years.



This chart, courtesy of WIPO, shows a downward trend overall, but it can be interpreted multiple ways. More domains are registered each year than the previous year, so even if the percentage stays the same, that means there are still a large number more being reported over the previous year. On the other side, the ability for the registrars to not allow and manage to keep the same percentage and lower than previous years is considered impressive (WIPO 2009).

Cybersquatting is defined as illegal, but there are also legal practices that can be similarly close to Cybersquatting, such as keeping parked domains and domaining. Parked sites are usually sites that are currently on the market by a third party, generally sold at auction. Here are some example scenarios of what would and would not constitute Cybersquatting.

- psu.edu - Penn State's main web address
- psu.com - Playstation Universe
 - Even though it has the same initials, they clearly represent different things making it perfectly legal.
- psuu.com - Parked domain
 - This domain is currently parked and potentially for sale. It has generic ads and a search feature on it to try and bring in revenue while it is being auctioned.
 - If this site were to be bought and labeled with a penn state logo and items that match Penn State's homepage, it would become illegal if it didn't explicitly say it was not affiliated with PSU.

The key difference between Cybersquatting and Domaining is one brings in that Cybersquatters bring in revenue because of imitation, instead of for Domain Name quality.

Botnets

Cybercrime is continuously on the rise and Domain Names are now being used to command botnets and phishing attacks. A botnet is a series of computers that are networked together under one's control. Generally botnets gain access to individuals computer illegally through malware and are non destructive to the user's computer. Botnets do not aim to harm an individual's computer, but rather to gain its computational and networking power. A single PC may not have

much to offer, but when thousands are infected a botnet controller will have the same computational abilities a supercomputer facility has (Uses of Botnets).

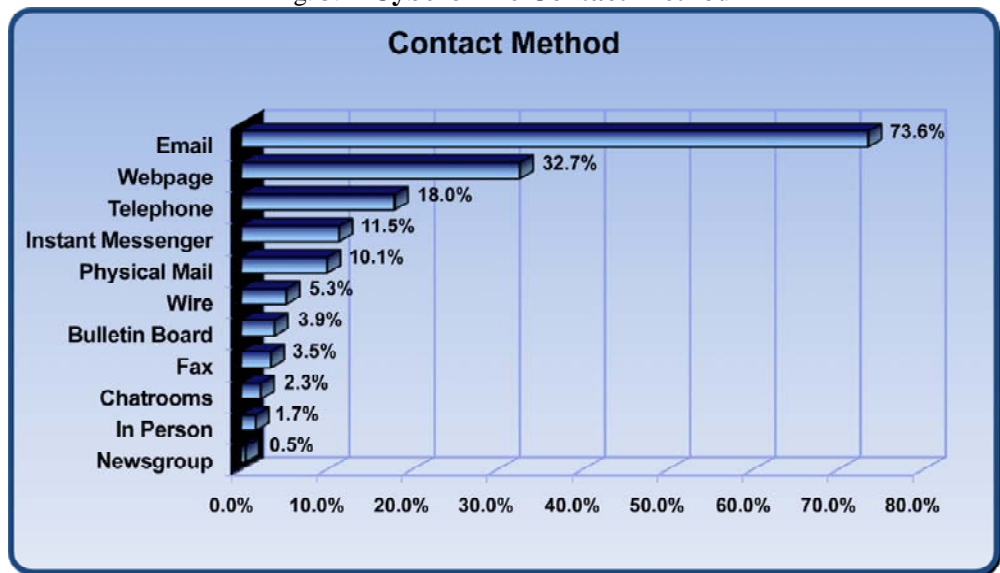
Botnets are always evolving and recently have had a trend of using Domain Names to contact and retrieve instructions from their controller. Having a static IP address for the controller programmed into the code could cripple a botnet if those servers are taken offline. However, newer botnets have algorithms built in to check certain Domain Name patterns. That way both the Domain Name and controllers address can change.

An example: An infected computer, otherwise known as a zombie, will have the malware with the new algorithm. It is told to check the domain ILoveDomainNames[x].com and it will have code to change the value of [x] and check sites until it hits one with instructions on it. A simple way to do this would be to code it for prime numbers. It would start checking domains in the following order:

- ILoveDomainNames1.com
- ILoveDomainNames2.com
- ILoveDomainNames3.com
- ILoveDomainNames5.com
- ILoveDomainNames7.com
- ILoveDomainNames11.com

A Domain Name can point to whatever computer address it is told to, so the zombie machine can connect to the DNS and even if a controller's server is taken offline, another one would be put online and the IP for that server would be updated in the DNS.

Fig. 3.1- Cybercrime Contact Method



The largest number of reported Cybercrime is through email and web pages, as shown in Fig. 3.1. Generally this would either happen through a botnet that could be controlled through rouge Domain Names, or hacked domains that appear to be valid.

Future of Domain Name Abuse

Domain Kiting

In the immediate future, the general practice we know as domain tasting will taper off and cease to exist as a business practice. With the increased cost to 'taste' a domain, it is no longer economical to try it without buying it. Registrars will instead increase security for people who register domains and try to cut down on any fake or potentially harmful Domain Names.

This trend could forever continue, and no more domain tasting could occur. However, with the value of Domain Names increasing, registrars and entrepreneurs will want to find a way to again

be ahead of the curve. New business practices will most likely develop and evolve until a few proven techniques are used industry wide.

Registrars may adapt their tasting techniques to only buy a site if multiple people search for it. Another way one might register Domain Names is search trending topics in the news and social networks. If there are enough people talking about something, it could easily become a website name. In this model, the registrar would actually buy the domain, monitor the traffic to the site, and sell it at that market price.

Cybersquatting

Cybersquatting will become a more and more popular trend as the number of short, sensical Domain Names are running out. There will be a higher demand for these names along making for a very profitable market. Some domains will accept this change and simply expand to larger Domain Names while other will instead expand as the ICANN expands to allow more Domain Names. ICANN recently announced their plan to allow multiple character sets to be used in URLs. With different extensions, many reseller will continue to gather the smaller, sensical Domain Names and make as much profit as possible.

Illegal cybersquatting will also continue to prosper until there are stricter and more black and white legal definitions. There is also a large push for domains caught cybersquatting to have hefty fines plus to pay for any legal expenses. Several companies have voiced their opinion that they want a more reformed process. They believe that larger penalties and better system in place to check registered Domain Names are needed to reduce fraudulent sites.

With clear definitions and high fines cybersquatters will be less hasty to continue pulling in revenue from their illegal business practice. The last and simplest way to deter cybersquatting is

user awareness. If every user that stumbled upon a cybersquatting site simply went to another page instead of clicking on their pay-per-click advertisement, a large percent of their business would be lost. They may still pull in revenue from banner ads that are based on number of unique site hits, either way it would be another way to help prevent them from them pulling in revenue illegally. Eventually cybersquatters will be so discouraged from not being able to safely make a profit, their practice will die.

Botnet

In the near future, cybercrime will increase as more and more exploits and incompetent users surf the internet, according to "World Intellectual Property Organization". They estimate crime will continue to increase, and the UDRP's continue to rise.

There have recently been exploits that are not fixed that could easily compromise a domain. For example, TLS renegotiation has a large hole that every browser and server needs to patch, as of now, only the web browser Opera has fixed the bug. Every time a new exploit is found, a "proof of concept" code usually follows. The proof of concept code is meant to show the vulnerability, that code though, my nature can be turned malicious due to the fact it's exploiting a program. These exploits will be popular in the hacking community for fun or profit, and need to be addressed quickly and uniformly across software companies (Kirk 2009).

The main concern right now is using botnets on actual Domain Names to control possible attacks. Abusing the DNS in such a manor also needs to be addressed uniformly across all registrars. Registrars need to become smarter than the criminals. Simply tracking who bought the site for the botnet isn't enough, considering most of these sites would be bought with fake credit cards. Instead, registrars will need to try and identify patterns of Domain Names or high amounts

of nonsensical domains being bought. there are other issues as well that need to be addressed.

While buying a Domain Name, more user credentials plus more sophisticated sign up software could catch potentially dangerous domains before they are even bought (McQuade 2009).

Cybercrime may never stop, but it can be impeded. To reduce the number of those at risk and to hinder cyber criminals, it will require a conscious effort from several fronts. It may even require constant surveillance of all networks and user activity. However, the price of security comes with the lack of privacy. What price is the public willing pay to be 'secure'?

Conclusion

To protect from future Domain Name abuse both users, systems, polices and laws need constant adaptation. ICANN has successfully ended domain taster, and proved their authority over Domain Names. They will need to continue leveraging their power, while remaining fair and ethical. WIPO has also stepped up to help stop cybersquatting, and currently aids with thousands of cases each year. However they will need to make the process more streamlined while working with ICANN and governments to increase penalties for those breaking the law.

We will eventually see a more secure internet; however it may come with security tradeoffs, like constant monitoring. It will remain up to the public in some nations to decide on what freedoms the internet will have to give up to become more secure. This will obviously spill out from the technical realm to that of politics. However, international security will not only rely on policy but on individuals vigilance and knowledge of internet operations. From each nation to each internet user, everyone will have to decide exactly how paranoid to be when using the internet. Some will argue that we need to have security from those who are trying to attack us, while others may align with Benjamin Franklin, "He who sacrifices freedom for security deserves neither."

Bibliography

Anhoury, Max. "Domain Name Abuse—An important component of fraud as a service." 5 October 2009. io.blog. 23 December 2009 <<http://blog.iovation.com/2009/10/05/domain-name-abuse/>>.

ICANN. Internet Naming System Goes Global. News Release. Seoul, South Korea, 2009.

—. "The End of Domain Tasting ." Status Report on AGP Measures . 2009.

Jamison, Shaun M. "Cybersquatting." Samuel C. McQuade, III. Encyclopedia of Cybercrime. Westport, CT: Greenwood Press, 2009. 53-55.

Kirk, Jeremy. Five indicted in long-running cybercrime operation. 2 September 2009. 12 December 2009 <<http://www.networkworld.com/news/2009/090209-five-indicted-in-long-running-cybercrime.html>>.

McQuade, Samuel C., III. "Cybercrime." Samuel C. McQuade, III. Encyclopedia of Cybercrime. Westport, CT: Greenwood Press, 2009. 43-44.

Messmer, Ellen. "Domain-name abuse proliferates; rogue registrars turn a blind eye ." 14 September 2009. Network World . 4 January 2010 <<http://www.networkworld.com/news/2009/091409-domain-name-abuse.html?ts0hb&story=abuse>>.

Parsons, Bob. "Getting the Drop on Domain-Name Abuse ." 5 June 2006. Business Week. 22 December 2009 <http://www.businessweek.com/technology/content/jun2006/tc20060605_633379.htm>.

Record Number of Cybersquatting Cases in 2008, WIPO Proposes Paperless UDRP. 16 March 2009. 20 December 2009 <http://www.wipo.int/pressroom/en/articles/2009/article_0005.html>.

Taranfx . "No Domain Name Abuse – ICANN’s new policy has killed ‘Domain Tasting’." 15 August 2009 . www.taranfx.com. 23 December 2009 <<http://www.taranfx.com/blog/no-domain-name-abuse-icanns-new-policy-has-killed-domain-tasting>>.

Uses of Botnets. 10 August 2008 . 14 December 2009 <<http://www.honeynet.org/node/52>>.

Whitney, Lance. New ICANN policy stops domain tasting. 13 August 2009. 16 December 2009 <http://news.cnet.com/8301-13578_3-10309051-38.html>.

WIPO, (World Intellectual Property Organization). WIPO Domain Name Dispute Resolution Statistics. 2009. 2 January 2010 <<http://www.wipo.int/amc/en/domains/statistics/>>.