Dynamic DNS - A survey of the abuse mechanisms affecting it and the growing problem for Network Defenders defending against them.

Kevin Orrey MSc

Abstract

Dynamic DNS although generally used to provide legitimate services has, like so many other technologies in use today, been exploited for a variety of criminal purposes. Dynamic DNS is being actively and extensively used today for Botnet Command and Control, (C&C), Advanced Persistent Threat (APT) Attacks, (Operation Aurora, RSA etc.), Drive-by downloads, Exploit Pack utilisation and varied Phishing activities.

The attribution of such attacks is increasingly difficult for law enforcement (LE) and network defenders, especially the initial identification of malicious domain registrants who use dynamic DNS providers that require little or no identification to initially setup accounts, privacy protection services and aliases to cover their tracks.

Proactive defence in depth techniques should be employed to defend a network in addition to more specific measures to try and identify abuse of the dynamic DNS service. Passive DNS Monitoring, malicious resource checking, website takedown and the employment of Content and Web Filtering Technologies are some of the many methods that can be used to fulfil this function.

Key Words: Dynamic DNS, Botnet C&C, Advanced Persistent Threat, Drive-by downloads, Exploit Pack, Phishing, Abuse of Dynamic DNS Services, DynDNS and Defensive Options.

1 Introduction

Dynamic Doman Name Service (DNS) providers offer a free and paid service which allows the aliasing of dynamic (DHCP) IP addresses to static hostnames and the provision of Uniform Resource Indicator (URI) redirection services etc. As the name suggests, it allows Internet Protocol (IP) address changes to be dynamically altered to ensure the static hostname a user has registered always resolves to the end-registered host or entity.

The dynamic updating of IP addresses can be achieved in multiple ways predominantly with the use of pre-installed software which provides an agent-based IP change notification service that detects changes on a host immediately notifying the dynamic DNS service provider who then updates their own DNS records accordingly. Dynamic DNS is an added layer that's runs atop the standard DNS system currently in use today.

The list of Dynamic DNS providers is diverse and growing with a plethora of providers offering a wide range of services with disparate free and paid for service offerings[1].

Dynamic DNS although generally used to provide legitimate services has, like so many other technologies in use today, been exploited and is used for a variety of nefarious purposes. Typical abuse includes resolving and redirection of victims enabling the following to be carried out using alone or in combination with each other:

a. Botnet Command and Control, (C&C),

b. Advanced Persistent Threat (APT) Attacks, (Operation Aurora, RSA etc.)

[1] Lists are available from: http://www.dmoz.org/Computers/Internet/Protocols/DNS/DNS_Providers/Dynamic_DNS/ and http://www.dyndnsservices.com/tech.htm

c. Drive-by downloads,

d. Exploit Pack utilisation,

e. Phishing activities.

Dynamic DNS is also utilised, in conjunction with other DNS providers, in a growing and convoluted redirection circle designed to make life difficult for network defenders. Avast, (2010) when analysing the Kroxxu botnet recently identified 15 such redirections, passing an unsuspecting victim through seven countries over three continents before finally landing at the actual exploit server.

URI shortening services[2], although again extensively used for legitimate purposes and increasingly useful on such platforms as Twitter, where character count is at a premium, can also be thrown into the mix to confuse matters further. This obfuscation technique can be used to direct unwary users to sites they would not normally browse to should the full URI become known to them. Varied browser-based utilities, long-url-please[3], view thru[4] etc. and other web resources are available to decode these but are seldom used by the masses as users tend to be trusting within their browsing habits and not be aware of the potential threats these services may open them up to[5].

Dynamic DNS services are predominantly used for a number of reasons, they are:

a. Cheap,

b. Easy to setup,

c. Easy to manage,

d. Provide anonymity,

e. Allow interoperability with other services.

2 Scope

The attribution of attackers is becoming increasing difficult for law enforcement (LE) and network defenders; identifying the likely source of illegal and malicious activities from which suitable legal actions can be brought to bear against the perpetrators is difficult. This is not just technologically difficult, but can be time consuming, fraught with geo-graphical, legal and budgetary considerations and pitfalls to name a few hurdles that may need to be addressed. These factors taken alone or in combination with each other may even outweigh the potential gain, compensation or other perceived benefit or motive for carrying out this process to fruition and thus its use as a deterrent is limited.

This paper will endeavour to identify the problems behind tracing the ownership of registrants who use Dynamic DNS and other DNS solutions, using DynDNS as an example. It will list potential tools and resources that are available to assist LE and network defenders to actively secure and protect their users, resources and networks. It will also provide an overview of web filtering technologies and discuss the pros and cons of their usage.

[2] Lists are available from: http://www.creativeramblings.com/ultimate-list-shortening-services/ and http://www.hongkiat.com/blog/url-shortening-services-the-ultimate-list/
[3] https://addons.mozilla.org/en-US/firefox/addon/long-url-please/
[4] https://chrome.google.com/extensions/detail/jkncfnbcgbclefkbknfdbngiegdppgdd?hl=en
[5] http://techteachtoo.com/url-decoders/

Whilst this paper will discuss how dynamic DNS works and is subsequently abused and overview the techniques utilised, it will also discuss the specific measures that could be implemented to try and thwart these types of attacks. It will not discuss general network security preventative measures as these have been discussed in great detail elsewhere. These measures should be part and parcel of an effective defence in depth strategy and should ideally include:

a. Antivirus Software Protection (regularly updated, on-access protection enabled and regular scans carried out),

b. Date Leakage Prevention (including egress filtering of outbound connections),

c. Firewalls (incorporating a regular review of rule sets that ensure only the minimum amount of ports/ services are open to enable the business to effectively function),

d. Intrusion Prevention Systems (IPS) (utilising rule and behavioural monitoring of network traffic, with the ability to implement reactive response mechanisms)

e. Intrusion Detection Systems (IDS) (utilising rule and behavioural monitoring of network traffic and identifying attempts to make changes to the file system, creation of new services),

f. Incident Response Plan (effective procedures should be in place and regularly practiced),

g. Maintaining effective security policies and procedures,

h. Patch Management Regime (regularly updated, tested and implemented both at the operating system (OS) and application level),

i. Potential employment of Honeypots,

j. Regular vulnerability assessments to be carried out to ensure no obvious vulnerabilities exist within the network,

k. Sandboxing,

l. User Education Programs,

m. Use of alternate OS which may have a reduced attack surface than the more mainstream OS in use (Orrey, 2011)

For the purpose of this paper the following domain was registered with DynDNS 1234testing.DynDNS.org which relays to the authors own website http://www.vulnerabilityassessment.co.uk. Any identification from this can then be carried out using a known entity and benign web presence.

3. Abuse of Dynamic DNS Services

There are many millions of users and corporations utilising dynamic DNS services for legitimate purposes, however, they continue to be abused by the criminal underground in a number of ways:

Botnet C&C

Dynamic DNS has been typically used for many years by Botnet herders as a simple and easy to use solution to coral and control bots via C&C servers though, according to Damballa, (2010), the use of this service may be changing; now being utilised by entry-level botnet herders in conjunction with pre-configured malware distribution kits procured from the criminal underground. Damballa intimate the trend and drop off in use of dynamic DNS recently from Botnet professionals is mainly due to:

a. Effective and timely response mechanisms from providers on receipt of cease and desist notices from LE.

b. Robust log retention policy providing easy to obtain availability of evidence for LE practitioners.

c. Active monitoring by providers of network abuses and effective remediation action taking place on detection of such.

d. More extensible and dynamic solutions on offer with botnet professionals able to buy and utilise tens of thousands of domains.

e. The use of social networking sites such as Twitter for communications between C&C servers and the bots, (Alcatel-Lucent, 2011).

Limited evidence exists to showing this emerging trend but with the increased commercialisation of botnet services and exploit frameworks, it is opined that at the entry level this is the easiest solution to “get into the game”. As a bot herders experience within the field grows, more ingenious and extensible solutions will be utilised offering a more stable and administratively less intensive platform which may make domain takedown or seizure and DNS sinkholing difficult. Botnet proliferation and usage is set to rise again during 2011 to what industry professionals believe will be approximately 7000 disparate botnets, (ESET, 2010). During the last 2 years there has been a marked doubling of the amount of botnets in this area this is due to the relatively low costs of set compared to the disproportionately large sums of money that can be made from using bots to supply criminal services.

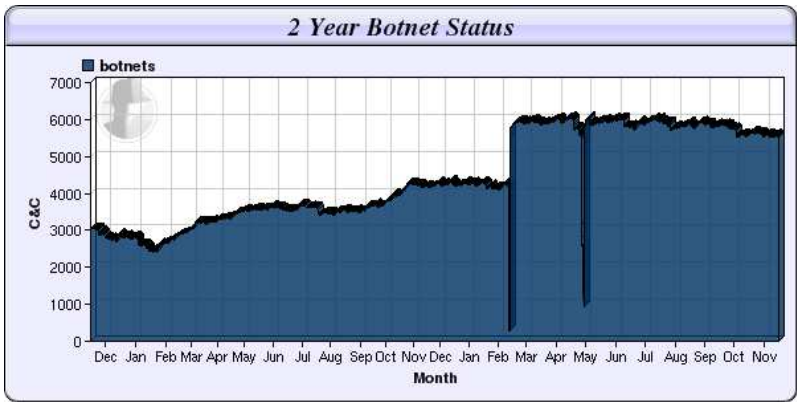


Figure 1 2 Year Botnet Status, (ESET, 2010)

Advanced Persistent Threat (APT) Attacks

So called APT attacks are becoming more prevalent with attackers intentionally, persistently and all too often very effectively targeting a specific individual or

corporation usually in a stealthy manner. These types of attacks are usually prolonged, sophisticated, coordinated and may go undetected by conventional antivirus, firewalls and intrusion detection/ prevention systems for many months or more, (Wired, 2010).

Dynamic DNS has seen on many occasions being utilised in such attacks as the call back beacon domain and C&C server, (Contagio, 2011). RSA suffered a massive attack at the start of the year, resulting in further attacks against Lockheed Martin, L3 and Northrup Grumman utilising information regarding SecureID being exfiltrated out of the network. A plethora of dynamic DNS domains registered with ChangeIP.com[6] were used in this attack as C&C servers with exploited hosts calling out to them after being successfully exploited utilising a zero-day vulnerability which was delivered via a phishing email sent to specific users, (KrebsonSecurity, Infowar Monitor, US Cert, 2011). Another specific example of dynamic DNS usage is the part it played for the Hydraq Trojan used in Operation Aurora against Google and many other domains. The update process for this particular backdoor Trojan called out to dynamic DNS domains registered with Dyn Inc.[7], which were subsequently taken down by the company, to update itself, (Dumballa and Symantec, 2010). A third such example of dynamic DNS usage is Global Energy Cyber-attack "Night Dragon" where these domains were used as C&C communication relays or to temporarily associate DNS addresses with remote servers, McAfee, (2011).

Drive-by Downloads

Drive-by downloads usually occur in two distinct formats, either the injection of malicious code into legitimate websites via hidden iframes; servers having been compromised via stolen file transfer protocol (FTP) passwords or access gained via SQL injection techniques or other methods, or via the use of tainted malicious web advertisements as was seen employed recently on the London Stock Exchange, a Nasdaq portal, (TheRegister, 2011), and MSN, Double-click in the US (Armorize, 2010). The latter's use has sharply risen in 2010, and servings of tainted ads have doubled from Q3 to Q4 to 3 million per day (Dasient, 2011). Both of these methods start the initial process of exploitation for unwary users and have utilised dynamic DNS services extensively; drive-by downloads usually occur in three distinct stages, (although extra stages involving multiple redirections other than the example specified may occur):

a. Stage 1 – User visits a site that has injected malicious code/ tainted advert being served which points to a registered dynamic DNS domain.

b. Stage 2 – Dynamic DNS domain sets varied cookies and a further redirection occurs to another domain.

c. Stage 3 – Site attempts to exploit browser if found to be vulnerable.

[6] http://www.changeip.com/
[7] http://dyn.com/

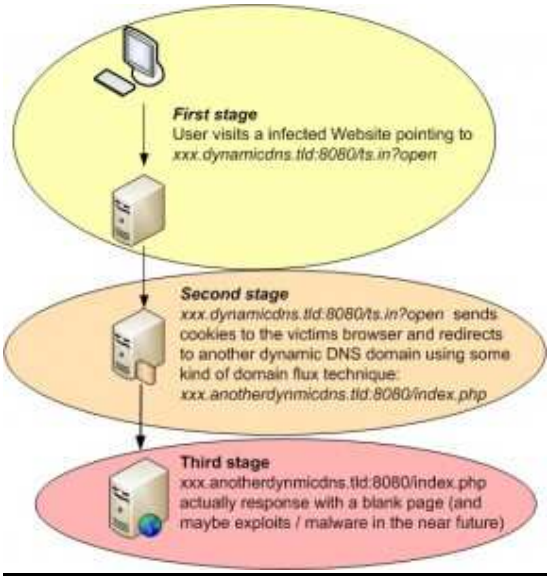


Figure 2 Drive-by Campaigns, (Abuse.ch, 2009)

Exploit Pack Utilisation

Dynamic DNS has been used by the criminal underground in numerous attacks with URI forwarding redirecting unwary victims to pre-registered domains hosting a variety of crimeware exploit packs, (Black hole, Crimepack, Eleonore, Fragus, K0de and Phoenix et al) (Softpedia, 2010). This process has been used similarly very effectively with other DNS free registration services, with Symantec, (2010), noting 12 Million potential exploit attacks originating from the co.cc domain which offers a similar service to dynamic DNS with the same potential for abuse.

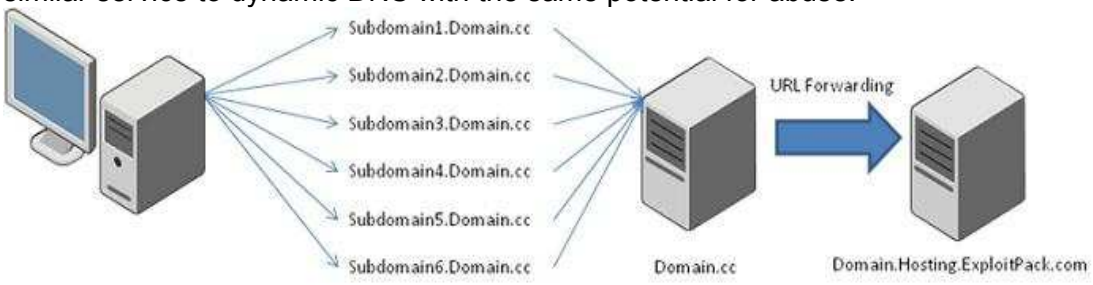


Figure 3 URI Forwarding to Exploit Pack Attack Sites, (Symantec, 2011)

Malwaredomainlist[8] provide a free lookup and reporting service for identified malware domains, with numerous malicious websites and resources being added on a daily basis.

http://www.malwaredomainlist.com/mdl.php?search=dyn&colsearch=All&quantity=50

Date (UTC)	Domain	IP	Reverse Lookup	Description	Registrant	ASN
2011/06/28_19:28	733t.dyndns.biz/gate.php	204.13.248.125	hop.mywebhop.org.	zeus v2 drop zone	DynDNS Hostmaster / hostmaster@dyndns.com	33517
2011/06/28_19:18	733t.dyndns.biz/config.bin	204.13.248.125	hop.mywebhop.org.	zeus v2 config file	DynDNS Hostmaster / hostmaster@dyndns.com	33517
2011/06/26_12:06	gorenmonszk.dynamicdns.biz/index.php?tp=94df3dd696eea086	174.37.210.229	174.37.210.229-static.reverse.softlayer.com.	Blackhole exploit kit	Sam Norris / nsi@changeip.com	36351
2011/06/26_12:06	gorenmonszk.dynamicdns.biz/d.php?f=50&e=2	174.37.210.229	174.37.210.229-static.reverse.softlayer.com.	trojan	Sam Norris / nsi@changeip.com	36351

Figure 4 Dynamic DNS utilised by Exploit Packs

[8] http://www.malwaredomainlist.com/mdl.php?search=dyn&colsearch=All&quantity=50

Phishing Activities

The criminal underground utilise dynamic DNS services in phishing attacks and subsequent drop sites to seamlessly redirect traffic from one phishing site to another. This is especially useful as a business continuity measure should their original phishing site be taken down. As network defenders and LE become more proactive in conjunction with brand owners and service providers in shutting down these sites, the use of such services is becoming one of their many preferred options, (US-CERT, 2011). The shutting down of a redirector only closes one shut route to the intended phishing site and full takedown requires the revoking of the fully qualified domain name with the registrar.

4 DynDNS Case Study[9]

DynDNS is one of the largest established and well-known providers of such services. It, like many other providers offers free, alongside more extensible paid for services. With DynDNS their services provide the ability to register a domain name which can either resolve to a specific IP address or allow a re-direct to a user defined URI resource or web site utilising a service they call webhop. The DynDNS service is managed via the web and a software-based agent can be installed to sync IP address changes thus ensuring registered domains always resolve to the correct address.

Free Service

A user can only chose two domains or initiate two webhop's after first providing and authenticating a valid email address when they first register on the site. To complete the registration process, a user must click on the link sent from DynDNS to their specified email account. DynDNS also resends these links every 30 days to the registered email address which the user must click. This is carried out for numerous reasons, predominantly to ensure that the account and service is still required, the user has a valid email address, and the service is not being abused, to reduce overheads promoting URI re-use etc.

Currently a user may register two free static domains from the following available list:

- DynDNS-at-home.com
- DynDNS-at-work.com
- DynDNS-blog.com
- DynDNS-free.com
- DynDNS-home.com
- DynDNS-ip.com
- DynDNS-mail.com
- DynDNS-office.com
- DynDNS-pics.com
- DynDNS-remote.com
- DynDNS-server.com
- DynDNS-web.com
- DynDNS-wiki.com
- DynDNS-work.com
- DynDNS.biz
- DynDNS.info
- DynDNS.org
- DynDNS.tv

[9] http://www.dyndns.com

Their registered site will now immediately resolve to the destination IP address or be re-directed to the selected resource. One point of note on re-directions is that when using the webhop service the physical re-direction is shown at the top of the browser so the user is aware that it has taken place:

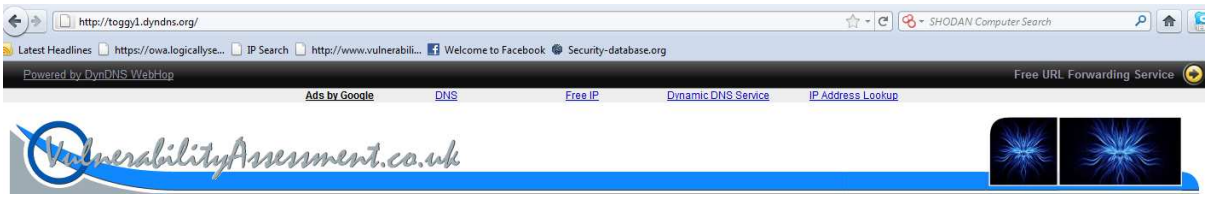


Figure 5 Webhop Notification

A registrant may enable cloaking on this service which uses browser frames designed to prevent visitors from seeing the redirect, but as shown above it is very obvious that this is taking place when landing at the intended registrant's site.

There are a number of exceptions to this, with limited experimentation, jpg, gif, txt and pdf files do not display any notification of a re-direction, nor do pdf files open correctly. Malformed gif and jpeg files have in the past been hosted on varied websites and have been used to exploit vulnerable computers leading to the execution of arbitrary code, (SANS, 2007), (Microsoft, 2010). Zero height iframes have been used extensively in the past as a way to re-direct users to external resources. Drive-by downloads for example may use dynamic DNS to resolve the source of a malformed image from an attacker's external web resource.

Premium Services

The premium service provides even more variety with 261 extra pre-registered domains that may be selected and in conjunction with wildcarding, provides a huge raft of domain space that a network defender potentially has to risk manage or defend against[10]. Three paid for services exist each providing more and more dynamic and customised hosting solutions:

a. DynDNS Pro – Allows up to 30 different hostnames/ webhop re-directions to be used, in addition the ability to create wildcard CNAME *.yourdomain.DynDNS.org for yourdomain.DynDNS.org entries.

b. Custom – Allows up to 75 records to be created, not just limited to the domains owned by DynDNS, may utilise any domain.

c. Dynect SMB – Allows up to 50 zones and 500 records to be managed, in addition geographically dispersed servers may be used dependant on the location of the required services enabling geographic targeting.

DynDNS also offers other paid services including the setup of Simple Mail Transport Protocol (SMTP) services, alternatively offering the user a choice of host their own mail server. DynDNS also offer domain registration service with privacy options if required and can provide Secure Sockets Layer (SSL) Certificates on request.

5 Identifying Registrants

[10] The full list is available from: http://www.dyndns.com/services/dns/dyndns/premium.html

The ability to identify site registrants can be difficult with many anonymising and privacy options available coupled with the ability for registrants to initially supply false and misleading information. Obviously once a user or corporation has been identified further research can be carried out to identify their location, address, contacts and other related information which may help network defenders and LE alike. For the purpose of this paper, the initial steps to try and identify the registrant are only discussed. These would normally take the form of reviewing and carrying out:

a. Domain Whois Record Lookups

b. Network Whois Records Lookups

c. Web Crawling, Spidering and Indexing

d. Reverse DNS Lookups

e. Virtual Host Enumeration

f. Further Enumeration

Given there is no requirement to specify any user details upon registration with DynDNS and other similar providers together with the prevalence of so-called throw away one-time use email accounts such as hushmail[11], malinator[12], guerillamail[13] etc, it is hard to glean from a defender's perspective, even given access to the DynDNS registration data who the account has been actually registered by. DynDNS, may store the IP of the host used to register this account, however, with IP spoofing, use of anonymity services (tor et al[14]), proxy services[15], cybercafé usage etc. this IP cannot realistically provide a guarantee of where the original registrant is geo-located and thus from a defenders perspective initial attempts at attribution are looking less than fruitful at this early stage.

Domain WHOIS Records

Using domain enumeration services, (CentralOps[16] and similar providers), the DynDNS registrant details are listed as generic with entries usually referring to the DynDNS Hostmaster, more specific references to the ID of this individual (or team) are not obvious and resolve with obfuscated details:

```
Registrant ID:tuS1YVbjHUItqeQX
Admin ID:tubgysz6e0j39tbh
Tech ID:tuUKSB5sYEFqoZ6Z
```

From the details identified, simple open-source queries match the Domain Whois record as the registrant of the base DynDNS.org domain and multiple other third-level domains registered with DynDNS SLD dyndns.org domain name, any specific details that may identify individual registrants are not available[17]. Alternate purely Whois lookup services also do not allow third level domain names to be resolved and reference the DynDNS.org domain only. From a defenders perspective this is less than helpful.

[11] http://www.hushmail.com/
[12] http://mailinator.com/
[13] http://www.guerrillamail.com/
[14] A Tor node checker is available at: https://www.dan.me.uk/torcheck?ip=
[15] Proxy Lists can be found at: http://www.proxy-list.org/en/index.php
[16] http://centralops.net/co/DomainDossier.aspx
[17] http://www.google.co.uk/#q=Registrant+ID:tuS1YVbjHUItqeQX

In combination with the above, other DNS service providers could be used in conjunction with DynDNS services to further obfuscate the true registrant of the site a user is finally redirected to. These other services, being used as an intermediary, may also offer their own domain registrant anonymising services; these being extremely prevalent and provided for a fee; godaddy[18], networksolutions[19] et al. Domain Whois record queries against these domains identify that a registrant wishes to remain private (anonymous); any resulting identification would require an official request to the service provider through legal counsel to be pursued. Even after gaining this information, it may prove fruitless if the registrant has supplied false and misleading information to further hinder their identification and cover their tracks.

Network Whois Records

Dependant on the DynDNS service being utilised different results are produced, some of which are more useful than others for furthering registrant identification.

a. Webhop

Using domain enumeration service, (CentralOps[20]), the network Whois record does not provide any details about the "real" website redirected to, providing only details of the IP address of the DynDNS server in the US which carries out the webhop service. In contrast a domain enumeration against the "real" website correctly identifies the registrant and IP address of the server hosting the website. For those not used to following DNS records and analysing such information this may be confusing and may result in incorrect assumptions being made.

b. Static Hosts

Using the domain alias service which lands a visitor at the static IP address that the registrant specified, the Network Whois record does provide details of the registrants Internet Service Provider (ISP) and thus provides a further avenue to explore. This, though as was intimated in the previous example, is subjective as the type of information returned to the analyst could potentially cause them to follow false leads. Having the details of a valid ISP can provide an avenue for LE to pursue further through legal channels.

Note: - Bear in mind this is rather a simple scenario, multiple wild carded hosts and intermediaries added into the mix can make this a very complex process indeed.

Web Crawling and Indexing

Web crawling, Spidering and Indexing of websites and the review of their source code may provide contact details, development code and other information which may help to identify those responsible for its creation. The process of carrying this out though is fraught with pitfalls.

Although the domain 1234testing.DynDNS.org is valid, it is opined that unless it is linked from a number of other sites, is mentioned on varied forums etc., it will potentially never be cached and indexed by the varied amount of web crawlers

[18] http://www.godaddy.com/domainaddon/private-registration.aspx
[19] https://www.networksolutions.com/domain-name-registration/private.jsp
[20] http://centralops.net/co/DomainDossier.aspx

trawling the net on a daily basis. As such queries for the name and cached copies of the domains content may not be registered with the major search engines, Google, Bing et al. Manual registration can be carried out on these search engines, however, if the site is being used for malicious purposes or is an intermediary service this will never potentially be carried out. Statistics such as page and site rankings available from many providers including Alexa[21], uptime and server information from Netcraft[22] are also thus unlikely to be possible to determine and closes another avenue for LE.

The ability to use facilities such as the Wayback machine[23]to view cached copies of the site over time which can be extremely useful in certain circumstances would thus be difficult to carry out as the site has potentially never been indexed by the web crawler from site. (A similar query against the "real" website does provide the resultant history of the website correctly.) In addition using the DynDNS webhop service a custom robots.txt file is utilised with the following parameters, disallowing robots from indexing the resource:

```
User-agent: *
Disallow: /
```

Malicious URI's may also point to individual resources and not full sites, alternatively to other sites which the user is then re-directed to. There may be re-directs to legitimate websites that have unfortunately had their pages altered to enable drive-by downloads to occur so in these cases indexing, spidering and review may only identify the malicious code and the end-points of the potential attacks but not any details of the true registrant who setup the initial re-direction and gained access to the site to carry out the modification. Further links to domains may have been registered by others within the same criminal fraternity alternatively by varied syndicates who use the end-points to try and push pay per click software, pharmacy products etc. It can, in this case, be a very extensive trail that needs to be followed with potentially a number of avenues that may or may not be related to the original individual trying to be identified.

Reverse DNS Lookup

Dependant on the network Whois returns, it may be necessary to correlate these findings from other sources or to try and glean further information, one way of doing this is to carry out a reverse DNS lookup. Having an IP address to resolve to a service provider is generally very easy to do with multiple sources allowing this to be easily carried out; zoneedit[24], dnsstuff[25] etc.

Virtual Host Enumeration

Having identified a static IP address and potentially following leads with varied ISP's and hosting providers etc. it may be determined that the IP address identified may be hosting a number of other websites (virtual hosting), some of these may be registered to the registrant that we are trying to identify, however, the vast percentage of these sites will just belong to everyday users that have signed up for hosting services and are just sharing the same web server. It may be that the registrant hasn't anonymised details on all domains that they own so it may be wise to enumerate them further to try and gather any clues and identify any linkages.

[21] http://www.alexa.com/siteinfo/
[22] http://uptime.netcraft.com/
[23] http://wayback.archive.org/web/
[24] http://legacy.zoneedit.com/
[25] http://www.dnsstuff.com/

Multiple web resources are available to try and determine any pertinent information that can be found if virtual servers have been detected and include:

a. http://www.my-ip-neighbors.com/

b. http://www.myipneighbors.net/

c. http://www.myipneighbors.com/

d. http://www.robtex.com et al

Note: - In the authors experience the DNS records returned by Robtex can be somewhat stale and as such should be confirmed from other sources.

Further Enumeration

Should any valid names, email addresses, other domains etc. be identified from any of the previous steps it may then be possible to use varied Whois, open-source search engines and other tools i.e. Maltego[26], FOCA[27], the Harvester[28] and Metagoofil to name but a few to try and build a profile identifying the web presence of the individual the sites may be linked to.

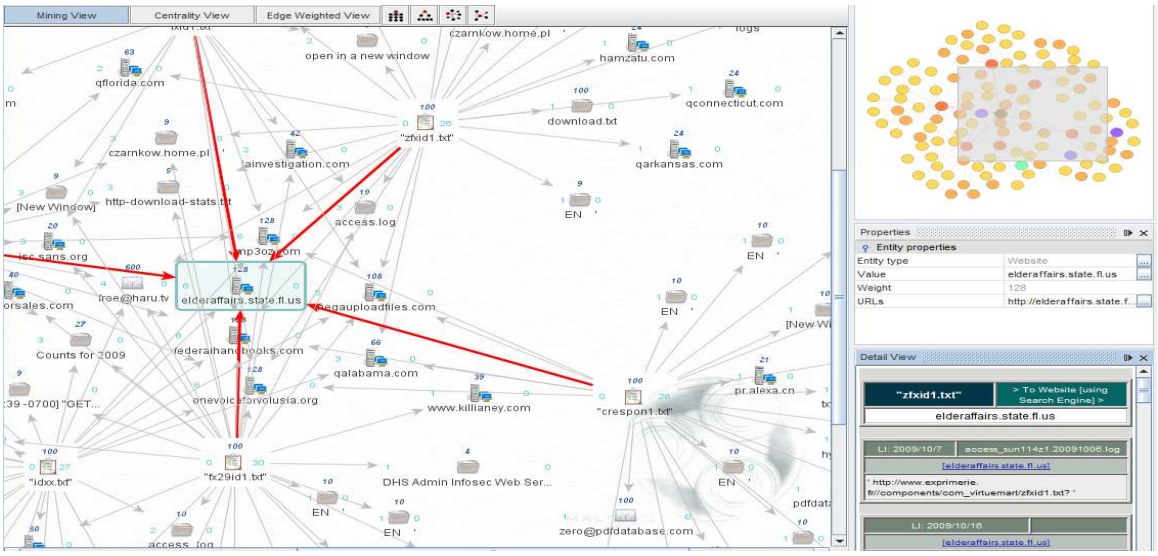


Figure 6 Maltego Enumeration (HolisticInfosec, 2009)

Maltego can be used to potentially find related sites and registrant information in a similar fashion to that mentioned later with regards to passive DNS monitoring. FOCA, Metagoofil and varied Exchangeable Image File Format, (exif), tools and resources may identify metadata housed within images and documents that may provide evidence that may further identification.

Guha and Francis, (2007) in their paper identified ways to potentially track individuals and gain more information about their identity, habits and movements which may eventually assist in their identification. This was based on a scenario whereby the registrants DNS record resolves to their own computer. In this scenario the computer is mobile and regularly connected to the web via varied Wireless Access Points

[26] http://www.paterva.com/web5/
[27] http://www.informatica64.com/DownloadFOCA/
[28] http://www.edge-security.com/soft.php

(WAP) and fixed networks with disparate IP addresses being assigned. These IP's dynamically updating the registrants DNS records; regular lookups can thus be performed with the hope of geo-locating the approximate position of the individual which may provide enough evidence to identify them[29]. Whilst this scenario is not seen as something that will be utilised by the vast majority of registrants it is included for brevity.

6 Defensive Options

Before deciding on the course of action to take to defend against malicious resources using dynamic DNS services, the key driver to consider in Information Security today is risk. The most common equation to try and work out an organisations exposure is the Risk Equation:

Risk = Threat x Vulnerability x Cost (International Charter, 2011)

In this equation each of these can be defined as:

a. Threat - Frequency of potentially adverse events.

b. Cost - Total cost of the impact experienced from a particular threat.

c. Vulnerability – Likelihood a particular threat will succeed when tried against a particular individual/ organisation.

Dependant on the type of network or resource a defender is protecting, and the need to ensure Confidentiality, Integrity and Availability of the data it protects and the potential downsides that could be experienced from a breach of such, be they loss of face, business, kudos or financial penalties from it being unavailable, altered or stolen will determine how risk averse they may be and from this what mitigation and remedial action will be instigated.

Each asset whether it be a resource, user, host, domain, enterprise or platform will score differently and thus any protective measures must be tailored to each. These measures ideally will be pro-active as they offer better protection rather than being purely reactive. Pro-active measures would provide active defensive mechanisms to thwart attacks, reactive measures would be the implementation of incident response mechanisms in a worst case scenario should an attack be experienced.

A number of options are available that may be proactive in trying to defend against attacks using Dynamic DNS including:

a. Passive DNS Monitoring

b. Malicious Resource Checking

c. Website takedown

d. Employment of Content and Web Filtering Technologies

Passive DNS Monitoring

[29] http://www.ippages.com/?host=

(The bash script utilised by Guha and Francis doesn't currently work due to a loss of functionality within this web resource.)

Hunt, (2010) demonstrated in his paper the utility of passive DNS record monitoring and the ability to identify pivots, relationships to (ISPs), and the power of link-nodal visualisation. This could help, from a network defenders perspective, when trying to identify pro-active rather than reactive mechanisms to establish defences against attacks utilising dynamic DNS. In his paper he demonstrates varied tools and resources that exist which can be utilised to draw links between malware domains and other related entities.

Normal filtering and blocking may blacklist individual domains with varied wildcard derivations included, which may stop a fair amount of traffic and potential for exploit, however, identifying varied and related IP blocks and blocking these may be a more pro-active and effective security mechanism. IP blocks related to malware domains will most probably be hosting multiple domains and services, some of which may also be legitimate, but they may also be hosting domains that may be sitting dormant pre-registered and resolvable for the next campaign of attack or potentially utilised for C&C botnet or other nefarious activities.

One important consideration for implementing mass blocking is that it must be carefully considered and risk managed ensuring that it will not impact access to valid businesses or operational services. The latter is especially important when fast-flux and other DNS technologies are in use and the corresponding IP addresses of malicious domains change frequently hence the linkages with different nodes and blocks previously identified may now not be extant.

Jiang et al, (2010) suggested possible ways to identify suspicious activities (and infected hosts) within a network using anomaly detection techniques. These techniques actively try and identify installed malware initiating numerous and frequent DNS queries, the vast majority of which fail potentially providing an indication for network defenders that a host either is misconfigured or could be infected. Conversely those hosts that make multiple and frequent failed resolution attempts will have a limited amount of successful queries fulfilled which would then identify valid C&C or beacon domains utilised by the malware and thus attempts to initiate blocking and remedial action can then be instigated. These domains are not limited to just those offered by dynamic DNS providers but affects all DNS providers and will be dependant on the implementation used by the malware developer on their penchant and preference that best suit their particular strain.

Malicious Resource Checking

Regular review of malware and phishing URI listings from varied resources[30] together with manually enumerating URI's[31] from your own organisations web access and proxy logs may provide an indication of IP addresses and domains that are being utilised for malicious purposes. Whilst the URI listings are comprehensive the one vector that may be lacking is a definitive listing of beacon domains that post exploitation an infected host will call back to their C&C server supplying it with host and network information or for instructions of what to do next.

Post detection and forensic examination of malware may provide beacon and other malware related domains and IP addresses which could be added to varied web filtering technologies to block access. One drawback of this though is that very complicated pieces of malware have in the past utilised hundreds/ thousands of

[30] http://www.malware.com.br/lists.shtml, http://www.malwaredomainlist.com/hostslist/hosts.txt, http://www.surbl.org/lists, http://mirror1.malwaredomains.com/files/domains.txt etc.
[31] http://www.malwareurl.com/listing.php?domain=domain_details

rotating pre-bought domains to maintain their networks and enable self-propagation. The Kroxxu botnet for example uses 100,000 plus domains, (Avast 2010), with 10,000 re-directors, 2,500 PHP re-directors, and 700+ malware distribution sites in this process and consideration needs to be given to differentiate the so called pure malware distribution domains operated by their authors and hacked zombie domains which are used as re-directors. Blocking all such domains may disrupt normal business activity and access to legitimate services.

Website takedown

Dependant on the location of the servers and the ISP's hosting phishing and exploit attack websites; it may be possible to have the website or resource taken offline by engaging with and reporting abuse to the service providers directly. If this is not possible it may be possible to alter DNS records, as was done by Symantec for Stuxnet recently who gained permission from the service provider to redirect traffic destined for the C & C domains to IP addresses within its Dublin response centre. Their intention was to identify and log the information being exfiltrated out of networks by infected hosts, (ITNews, 2011).

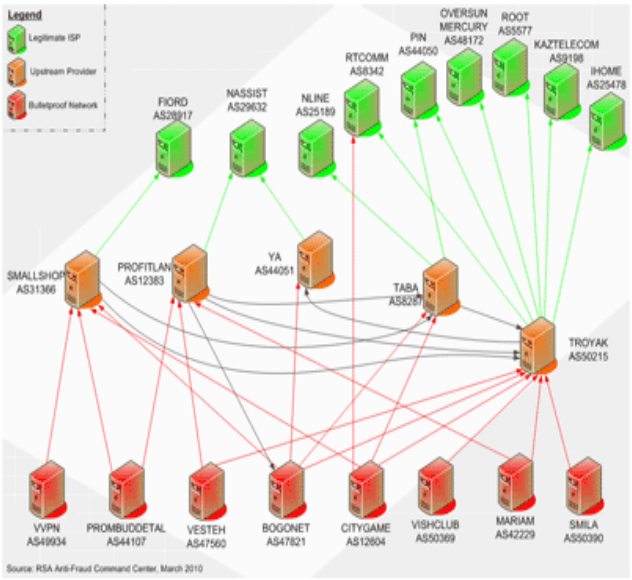
Alternatively the Federal Bureau of Investigation, (FBI) U.S. Immigration and Customs Enforcement and the Department of Homeland Security has been very active recently seizing domains (Wired 2011) mostly related to the supply of counterfeit goods, Intellectual Property Rights, (IPR) breaches and Peer to Peer piracy but also has included the seizure of domains related to Botnet C&C infrastructure, (notably the Rustock and Coreflood botnets. (PIR, Microsoft, 2011)).

Moore et al, (2008), noted that, alongside the standard abuse notification and requests to desist notices sent to service providers when trying to take down phishing websites, the early notification and cooperation of the actual brand owners would help remedial action process potentially ensuring that "spoof" websites are taken down within 4 hours.

-	Sites	Lifetime (hours)	
		Mean	median
Free web-hosting			
all	395	47.6	0
brand owner aware	240	4.3	0
brand owner missed	155	114.7	29
Compromised machines			
all	193	49.2	0
brand owner aware	105	3.5	0
brand owner missed	155	103.8	10
Rock-phish domains	821	70.3	33
Fast-flux domains	314	96.1	25.5

Figure 7 Phishing Website Lifetimes by Attack Type (Moore et al, 2008)

Although Moore's findings are generalist, they technically do not take into account huge swathes of malware domains that utilise so-called bullet-proof (BP) hosting services. BP hosting essentially guarantees that registrant's websites and resources will not be taken down, regardless of the type of abuse complaints received or the content that is stored and hosted upon them, (InfosecIsland, 2010). BP services have multiple connections to both upstream and downstream providers to ensure they stay online and provide where possible 100% availability.



Key

Bulletproof Network where malware is actually hosted, shown in the dark red cloud with the Trojan horse's icon;

Upstream Providers are orange-colored clouds;

Legitimate ISPs are shown as green clouds.

Figure 8 Malicious Bulletproof Networks Connection Scheme (Mesh Topology) (EMC Corporation, 2010)

The criminal fraternity realise that it is worth paying for these services even though they are comparatively expensive compared to normal hosting services but on balance with the potential gain that can be realised from their illicit activities it is well worth the time, effort and expense involved. A large percentage of BP service providers exist within the former Soviet "Bloc" and China and it may prove difficult to take remedial action against these (EMC Corporation, 2010), (Norman, 2010).

7 Employment of Content and Web Filtering Technologies

Web Filtering Technologies are utilised to provide a safer Internet experience not just for the user but for the corporation alike whose infrastructure is placed in constant danger by allowing access to this medium. There are many processes and tools that can be employed to restrict or monitor Internet access, a survey of these are as follows, (Bloxx, 2010):

a. Web Filtering Firewalls.

Black and Whitelisting may be employed within firewalls to limit or allow access to web resources, this type of employment and the reporting and alerting mechanism may be a little basic; dedicated appliances and applications can be more useful.

b. URI Database Web Filtering.

These typically contain millions of web addresses, and are categorised according to their content. Problems associated with this have been touched upon previously with regards to the dynamic rotating of beacons domains by certain strains of malware. Keeping the lists up to date as resources change, together with the fact that the sheer vastness of resources offered over the Internet today it is a daunting task to spider and prepare specific filters based on their findings.

One further consideration is the scale and size of the database utilised; .is it based on the perceived risk with a corporation employing and implementing the largest and most restrictive database possible on its web filtering appliances and applications. This may provide the maximum amount of protection to the user and consequently the network itself but will this affect the business function, this depends on the surfing habits and end resources users require from an operational perspective. Using a

smaller database may be more beneficial but may provide less protection and thus may leave the user and organisation open to web based threats or allow access to inappropriate web sites or content. This is termed overblocking and underblocking, the former may hint that the currently enabled filters are being too restrictive, the latter that inappropriate content is being able to be accessed, a fine line must be trodden and tuning of filters must be carried out on a regular basis.

Another area to consider is the URI database supplier itself and their classification procedure, a corporation blanket enabling all rules or the disabling of varied categories for certain users may allow access to those that are deemed inappropriate for an organisation but the fault in this may lie with the supplier when they initially categorised the resource. The URI database supplier may deem something appropriate to themselves so not implement a filter rule but unbeknownst to them, the context is such that from an end-user perspective it is inappropriate. Categorising in this way can be a very subjective process and open to differences of opinion.

c. Image Scanning.

Processor intensive, expensive and potentially prone to false positives, image scanning can be used as a content filtering solution both for browsing and as part of an email security solution. This can either be carried out on the fly and may use digital signatures, first converting images which are subsequently compared against known bad image database.

d. URI Keyword Scanning Technology.

Often used in conjunction with URI databases to provide extra protection for the network, user input is analysed and validated before access is provided to a web resource.

e. In-line Keyword Scanning Technology

Web and content filtering service that will analyse the content of a web resource based on a pre-defined list of acceptable and unacceptable words; attribute a score and providing the page does not exceed the defined thresholds allow or block a user having access to it.

8 Conclusion

Attributions are difficult and as the tools and techniques evolve to attempt make this process easier, as do the ways that attackers employ to stay hidden become more complicated and convoluted. A never ending arms race exists between attacker and defender the former trying to stay one step ahead and the latter predominantly playing catch up. Even when individuals have been identified it may be counter-productive and cost prohibitive, dependant on the size of the organisation taking further action against them. This may be for many reasons and sometimes it may be better, having identified an attacker to build up a bigger picture on their activities, contacts and relationships which from a strategic perspective may reap greater dividends.

Many tools, techniques and processes are there to try and assist both LE and network defenders alike, passive monitoring and collaboration with others parties may be a way forward but these tend to be reactive measures and although they can enhance the security within a network they reach a natural limit of usefulness. Proactively seeking out actual threat intelligence of upcoming attacks would be a preferred solution but with the Internet so

dynamically and diversely spread with many areas that aren't indexed or policed this is proving difficult and more research is required in this area.

URI database web filters are excellent tools to try and thwart attacks and access to inappropriate material but they do have there limits. The dynamicity of the web, its exponential growth make indexing and categorising threats that much harder and just noting changes within the current system is huge task and very much a slow reactive mechanism. Research into more proactive methods to maintain and make these databases more affective should be carried out.

Dynamic DNS does get abused using many angles, sometimes in combination with each other, however, so do mainstream DNS solutions, so from a LE and defenders perspective it would be over-zealous and a fruitless situation to blanket ban such services in their entirety. Banning select domains carries with it an administrative burden when attackers naturally rotate pre-registered alternatives to enhance their survivability and simply replace the ones currently blocked. This potentially leaves an organisation with a web filtering platform using outdated and stale blocking rules marginally slowing processing time, not to mention not fully protecting users from new potential threats in the wild.

Web filtering technologies need to be used and must form part of the normal defence in depth strategy an organisation uses to protect itself, (and its users), but it must be a hybrid approach pulling together real-time keyword and image analysis in combination with more mainstream URI database filters which have been tuned to suit the context of the organisation that is using them. This must be married to any collaborative and actual threat intelligence received and a trade-off made using the risk equation of what security mechanisms should be implemented.

9 References

Abuse.ch, (2009) “Drive-by campaign using dynamic DNS domains “[online] Available: http://www.abuse.ch/?p=1801 [accessed 29 Jun 11]

Alcatel-Lucent, (2011) *“Security: On the Trail of the Elusive Botnet“* [online] Available: http://www2.alcatel-lucent.com/blogs/techzine/2011/security-on-the-trail-of-the-elusive-botnet/ [accessed 29 Jun 11]

Armorize, (2010) “"*HDD Plus" malware spread through major ad networks, using malvertising and drive-by download*” [online] Available: http://blog.armorize.com/2010/12/hdd-plus-malware-spread-through.html [accessed 29 Jun 11]

Avast, (2010) *“AVAST: Kroxxu botnet infects 100,000 domains without a money trail“* [online] Available: http://www.avast.com/pr-avast-kroxxu-botnet-infects-100000-domains-without-a-money-trail [accessed 29 Jun 11]

Bloxx, (2010) “*Understanding Web filtering Technologies*” [online] Available: http://www.bloxx.com/assets/downloads/US/bloxx_whitepaper_webfilter_us.pdf [accessed 29 Jun 11]

Contagio, (2011) “*Targeted attacks against personal accounts of military, government employees and associates*” [online] Available: http://contagiodump.blogspot.com/2011/02/targeted-attacks-against-personal.html [accessed 29 Jun 11]

Damballa, (2010) “*The Command Structure of the Aurora Botnet*” [online] Available: http://www.damballa.com/downloads/r_pubs/Aurora_Botnet_Command_Structure.pdf [accessed 29 Jun 11]

Dasient, (2011) “*The Dasient Q4 Malware Update: Significant Rise in Malvertising Attacks, Social Networking Sites Easy Distribution Platforms for Malware“* [online] Available: http://blog.dasient.com/2011/03/dasient-q4-malware-update-significant.html [accessed 29 Jun 11]

EMC Corporation, (2010) “AS-Troyak Exposes a Large Cybercrime Infrastructure” [online] Available: http://blogs.rsa.com/rsafarl/as-troyak-exposes-a-large-cybercrime-infrastructure/ [accessed 29 Jun 11]

Eset, (2010) “*Trends for 2011: Botnets and Dynamic Malware*“ [online] Available: http://www.eset.com/us/resources/white-papers/Trends-for-2011.pdf [accessed 29 Jun 11]

Guha, Saikat, Francis, Paul, (2007) “Identity Trail: Covert Surveillance Using DNS” [online] Available: http://www.mpi-sws.org/~francis/pet07-idtrail-cameraready.pdf [accessed 29 Jun 11]

HolisticInfosec, (2009) “*Maltego is the 2009 Toolsmith Tool of the Year*“ [online] Available: http://holisticinfosec.blogspot.com/2009/11/maltego-is-2009-toolsmith-tool-of-year.html [accessed 29 Jun 11

Hunt, Andrew, (2010) “*Visualizing the Hosting Patterns of Modern Cybercriminals*” [online] Available: http://www.sans.org/reading_room/whitepapers/dns/visualizing-hosting-patterns-modern-cybercriminals_33498 [accessed 21 Jun 2011

InfosecIsland.com, (2010) “*Bullet Proof Hosting: A Theoretical Model*” [online] Available: https://www.infosecisland.com/blogview/4487-Bullet-Proof-Hosting-A-Theoretical-Model.html [accessed 29 Jun 11]

Infowar Monitor, (2011) "*The RSA Cyber Attack and the Emergence of the Cyber Military Industrial Complex*" [online] Available: http://www.infowar-monitor.net/2011/04/6987/ [accessed 29 Jun 11]

International Charter, (2011) “*The Risk Equation*“ [online] Available: http://www.icharter.org/articles/risk_equation.html [accessed 29 Jun 11]

ITNews, (2011) “*Analysis: Stuxnet dissected*“[online] Available: http://www.itnews.com.au/News/249061,analysis-stuxnet-dissected.aspx/0 [accessed 29 Jun 11]

Jiang, Nan, (2010) “*Identifying Suspicious Activities through DNS Failure Graph Analysis*” [online] Available: http://www-users.cs.umn.edu/~zhzhang/Papers/Jiang-ICNP10-DNS-Failure-Graph-Analysis.pdf [accessed 29 Jun 11]

KrebsonSecurity, (2011), "*Domains Used in RSA Attack Taunted U.S.*" [online] Available: http://krebsonsecurity.com/2011/03/domains-used-in-rsa-attack-taunted-u-s/ [accessed 29 Jun 11]

McAfee, (2011) "*Global Energy Cyber-attacks: “Night Dragon”*" [online] Available: http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf [accessed 29 Jun 11]

Microsoft, (2010) “*Exploit:Win32/MS04028!jpeg*” [online] Available: http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Exploit%3AWin32%2FMS04028!jpeg [accessed 29 Jun 11]

Microsoft, (2011) “*Taking Down Botnets: Microsoft and the Rustock Botnet*” [online] Available: http://blogs.technet.com/b/microsoft_on_the_issues/archive/2011/03/18/taking-down-botnets-microsoft-and-the-rustock-botnet.aspx [accessed 29 Jun 11]

Moore, Tyler, Clayton, Richard, (2008) “The Impact of Incentives on Notice and Take-down” Seventh Workshop on the Economics of Information Security (WEIS 2008), June 25–28 2008.

Norman, (2010) “*Safe crime*” [online] Available: http://www.norman.com/security_center/security_center_archive/2010/129791/en [accessed 29 Jun 11]

Orrey, (2011) “*Cyber Attack: Exploiting the User - There are so many ways!* ” [online] Available: http://www.vulnerabilityassessment.co.uk/education/Thesis.pdf [accessed 29 Jun 11]

PIR, (2011) “*US Federal Bureau of Investigation (FBI) Takedown Orders*” [online] Available: http://www.pir.org/news/2011/0412 [accessed 29 Jun 11]

RSA, (2011) "*Anatomy of an Attack*" [online] Available: http://blogs.rsa.com/rivner/anatomy-of-an-attack/ [accessed 29 Jun 11]

SANS, (2007) “*PHP Exploit Code in a GIF*” [online] Available: http://isc.sans.org/diary.html?storyid=2997 [accessed 29 Jun 11]

Softpedia, (2010) "*DynDNS Abused by Malware Pushers*"[online] Available: http://news.softpedia.com/news/DynDNS-Abused-by-Malware-Pushers-147269.shtml [accessed 29 Jun 11]

Symantec, (2010) "*Symantec Intelligence Quarterly January - March 2010*" [online] Available: http://eval.symantec.com/mktginfo/enterprise/other_resources/b-symc_intelligence_quarterly_jan-mar_2010_20949851.en-us.pdf [accessed 29 Jun 11]

Symantec, (2011) "*12 Million Exploit Attacks Originating from the CO.CC Domain*" [online] Available: http://www.symantec.com/connect/blogs/12-million-exploit-attacks-originating-cocc-domain [accessed 29 Jun 11]

TheRegister, (2011) "*Nasdaq admits hackers planted malware on web portal*" [online] Available: http://www.theregister.co.uk/2011/02/07/nasdaq_malware_breach/ [accessed 29 Jun 11]

US-CERT, (2011) "*Early Warning and Indicator Notice (EWIN)-11-077-01"* [online] Available: http://www.fbiic.gov/public/2011/mar/EWIN-11-077-01.pdf [accessed 29 Jun 11]

US-CERT, (2011) "*Technical Trends in Phishing Attacks*" [online] Available: http://www.us-cert.gov/reading_room/phishing_trends0511.pdf [accessed 29 Jun 11]

Villeneuve, Nart (2010) "*SHADOWS IN THE CLOUD: Investigating Cyber Espionage 2.0*" [online] Available: http://www.nartv.org/mirror/shadows-in-the-cloud.pdf [accessed 29 Jun 11]

WebmasterWorld, (2008) "*Free Dynamic DNS Services Pose Massive Security Threats*" [online] Available: http://www.webmasterworld.com/webmaster/3642155.htm [accessed 29 Jun 11]

Wired, (2010) "*Report Details Hacks Targeting Google, Others*" [online] Available: http://www.wired.com/threatlevel/2010/02/apt-hacks/ [accessed 29 Jun 11]

Wired, (2011) "*Feds Seize 8 More Domains in Piracy Crackdown*" [online] Available:http://www.wired.com/threatlevel/2011/05/eight-domains-seized/ [accessed 29 Jun 11]