MAAWG

# Messaging Anti-Abuse Working Group (MAAWG)
# Overview of DNS Security - Port 53 Protection

**Table of Contents**

## Document Revision History

| Date | Author | Version | Description |
|---|---|---|---|
| **6/3/2010** | **MAAWG DNS Sub-Committee** | **V1.0** | **Published paper** |

## Introduction

Internet Service Providers (ISPs) are uniquely positioned to ensure the security of their subscribers by carefully managing their access to network resources. The Domain Name System (DNS) is central to the proper functioning of virtually every Internet Protocol (IP)-based communication in every network across the Internet. This means managing access to the DNS is an essential part of the overall security posture of every subscriber.

Attackers have become increasingly sophisticated in *their* use of network resources. Starting two years ago maliciously intended software known as "malware" began to evolve to allow attackers to hijack the DNS settings of PCs, home gateways and applications. Hijacking these settings allows attackers to become the "man-in-the-middle" of every DNS transaction. These attacks over-write DNS settings located on the subscribers computer or home gateway to new fraudulent or malicious targets. This change effectively allows the attacker to take over traffic (hijack) for the unsuspecting Internet broadband consumer.

This class of exploit represents a serious threat because the modifications are extremely difficult to detect and when an attacker has control over the DNS they can redirect whatever subscriber traffic they want, wherever they want, whenever they want. The subscriber has no way of knowing their traffic has been redirected; most subscribers are completely unaware of the DNS, let alone the proper settings that determine which server they should use.

A paper published by researchers from Georgia Tech and Google, "Corrupted DNS Resolution Paths: The Rise of a Malicious Resolution Authority[1]," gives a sense of the scale and potential of the problem. To quote directly from the paper: "To document the rise of this 'second secret authority' on the Internet, we studied instances of aberrant DNS resolution on a university campus. We found dozens of viruses that corrupt resolution paths, and noted that hundreds of URLs discovered per week performed drive-by alterations of host DNS settings." The same research also found over 17 million open unrestricted DNS servers, of which they estimate 291,000 provide incorrect or malicious DNS service.

The prevalence of malware that can modify DNS settings coupled with the difficulty of detecting such changes and the ready availability of hosts providing incorrect and malicious answers to DNS queries represents a major threat to subscriber security on the Internet. This is a significant threat because the Internet broadband consumer is unaware of the changes made by the DNS hijacking activity and has little indication their entire broadband connection is comprised. The attacker is able to redirect the consumer to a phishing site instead of the real site without the use of malicious software, or malware, installed on the victim's computer.

To ensure success with efforts to manage access to the DNS, service providers must carefully consider the solutions and assess them based on technical dimensions, subscriber perceptions, and the viewpoint of other stakeholders in the Internet community such as advocacy groups. This is important for the ultimate success of any service. In particular service providers need to be sensitive about limiting alternative choices for DNS services that subscribers might desire. This paper will briefly discuss how the attack works, the impact of this threat, propose a solution, and discuss advantages and disadvantages from a technical, business, and regulatory standpoint.

## Compromising the DNS

DNS cache poisoning[2] is well understood as a means for compromising the DNS. Another equally insidious method is to infect a subscriber PC or home gateway with malware that is capable of changing DNS settings. Some of the vectors for distributing this malware are familiar: spam with embedded links, websites, and bots. Recently another method was observed whereby compromised machines respond to DHCP requests[3] with fake offers that include new DNS settings[4]. There are also client side malware cases where important system files such as DLL files of a PC or host files will be modified to facilitate this malicious activity. Additional cases have been identified where DNS settings are modified or static routes are inserted via cross site scripting[5] on a home gateway, which is a device providing Internet connectivity to more than one computer over a single broadband connection.

[1] http://www.citi.umich.edu/u/provos/papers/ndss08_dns.pdf

[2] http://en.wikipedia.org/wiki/DNS_cache_poisoning

[3] http://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

[4] http://www.theregister.co.uk/2008/12/05/new_dnschanger_hijacks/

[5] http://en.wikipedia.org/wiki/Cross_site_scripting

Once the settings for the DNS configuration are hijacked attackers make use of other technologies such as squid proxy servers[6] to provide connections to sites where valuable credentials can be harvested. They can insert correct DNS responses (use the real DNS records) for sites like www.google.com, and use malicious responses for sites like www.bankofamerica.com that point to proxy servers that phish for credentials and confidential information.

In all of these cases, the user is completely unaware of any redirection because all of the DNS interactions are transparent to the applications they use. In fact, for as long as the PC is hijacked or the home router comprised, updates to user credentials can be captured. This has been recorded by several service providers as a source of recurring Web mail abuse for spamming purposes.

## The Impact of Compromised DNS Resolution

DNS resolution occurs in several forms, the most common being when an Internet broadband consumer either types a domain name into their Web browser, such as www.bankofamerica.com, or the consumer clicks on a link from a Google search that contains a domain name.

There is the potential for considerable collateral damage when the DNS resolution path is hijacked by malware or other malicious techniques. The biggest exposure is that subscriber credentials and confidential information can be harvested by redirecting website locations, email traffic, messaging or other IP traffic to malicious sites that solicit the information directly using social engineering techniques or that monitor the traffic for sensitive information.

Subscriber data can either be used directly for profit or resold to other criminals, spammers or other attackers. This creates a multitude of headaches for the subscriber ranging from identity theft and financial loss to receiving even more targeted spam (which in turn can lead to additional infections and even more problems). Although the legal exposure for providers is unclear, subscribers often perceive their provider as the first stop when they have a problem on the Internet, so costs are incurred for support. Subscriber misperceptions about who is at fault may also promote churn.

Botnets[7] that hijack DNS traffic on the Internet broadband consumer's connection present a particularly vexing problem because they can carry out their exploits with no possibility of being controlled or detected. Most botnets rely on the DNS for communicating with their command and control[8] and bot mitigation is dependent on severing this link. If providers do not see attempted communications with a bot command and control on their own DNS servers and other techniques are not employed to sever this link then bots have free rein to carry out their exploits. The consequences of this are potentially devastating, especially given the extraordinary sophistication of bots now being observed in the wild.

Another consideration for service providers is that subscribers whose DNS traffic has been directed to malicious and fraudulent replacement sites by an attacker may perceive that their service quality is poor or see the service go down altogether. Off-network DNS resolution may go down because the service is hosted at an unstable IP address or is taken down by a responsible ISP. The DNS servers may also be hosted on a botnet with minimal or intermittent bandwidth available. These kinds of service outages or degradation can be very difficult and expensive to troubleshoot. ISPs may even inadvertently spend resources troubleshooting an issue not related to their own DNS servers.

[6] http://en.wikipedia.org/wiki/Squid_%28software%29

[7] http://en.wikipedia.org/wiki/Botnets

[8] http://en.wikipedia.org/wiki/Command-and-control

In addition, subscribers with hijacked DNS settings pointing at open DNS resolvers can be unwitting accomplices in amplification attacks[9] or attacks on the root servers[10].

These are only a few of a multitude of potential impacts. Once a "man-in-the-middle" is in place, traffic can be intercepted at will and redirected anywhere without being detected. The power is limited only by the attacker's imagination.

## Preventing Corruption of the DNS Resolution Path

Attacks on the DNS and the collateral damage they can cause are forcing service providers to assess solutions. The best alternative is to monitor DNS traffic (port 53) at subscriber egress points in the network and install filters that only allow subscribers to point to legitimate DNS servers. This last point is important; there are legitimate open DNS services hosted on the Internet and blocking subscriber access to them will provoke a backlash. Preserving choice is essential and can be accomplished by configuring filters that permit traffic to known legitimate open DNS resolvers. Lists of such servers are published and readily available on the Internet[11]. Filters can be updated regularly to reflect changes to the availability of services.

A service implementation could also include redirection of the IPs of popular malicious DNS servers to DNS servers hosted by the provider that can safely resolve queries and log IPs of the infected subscribers for later remediation efforts. In fact the service could also incorporate a "teaching page" to notify subscribers about the dangers they face and inform them about what is being done.

A big advantage of this approach is that PCs that are not infected are not impacted, including uninfected PCs behind a NAT device that will continue to use the proper ISP-supplied DNS server IP addresses. T he case of a home router compromise where all PCs are NATed and treated as if they are infected is also accommodated. This low impact, honey-net approach will provide valuable business justification to expand programs to manage port 53 more aggressively.

Another positive side effect of this particular implementation is that none of the queries directed at malicious DNS servers are trusted. This is important because there is no way to determine what traffic an attacker will redirect to malicious sites and what traffic they will not. For example, an attacker could create a cover page for Google search results and use it to infect PCs through injection of poison search results from a proxy server.

## Managing Traffic on Port 53 Offers Clear Benefits for the Subscriber

Assisting subscribers who are having their traffic hijacked to malicious servers clearly benefits them. Many subscribers may be struggling with malware on their PC and are either completely unaware of what is causing the problem or too embarrassed to call the help desk. More importantly, subscribers that are contributing to a botnet can also be identified and remediated. The value of eliminating their exposure to malicious sites and improving their overall Internet experience simply cannot be disputed.

Responses can be trusted, performance will be higher, latency of queries will be lower, and the service will be more reliable. Keeping these subscribers on the provider's network and away from malicious services will increase satisfaction and reduce costs associated with service related calls. Ensuring subscribers can access legitimate DNS services that are off network will alleviate concerns about eliminating subscriber choice.

[9] **http://en.wikipedia.org/wiki/Denial-of-service_attack**

[10] **http://en.wikipedia.org/wiki/Root_servers**

[11] http://80.247.230.136/dns.htm

In some cases subscribers may choose to configure their PC to point at an open recursive DNS server because they do not fully understand the risks and service implications. Although the server they choose may not be controlled by an attacker, it also may not be properly maintained. This introduces risk because the server they are using may not be protected against cache poisoning attacks such as the Kaminsky attack[12]. The performance of the server and problems with websites they are pointed to can also result in perceived ISP service problems as described above.

## Justifying the Investment to Manage Traffic on Port 53

DNS is essential to all aspects of subscribers' interaction with provider networks. Providers cannot manage the subscriber experience without managing all aspects of DNS access. This includes attacks such as the ones described in this paper.

Managing traffic on port 53 simplifies operations by removing what would otherwise be anomalous problems on the network. Help desks calls will be simplified and infections can ultimately be reduced by severing DNS communications. It also highlights and provides the reporting data and framework for identifying criminal activity on the network that can be used to justify the investment in protection.

Botnets rely on access to the DNS for command and control. Bots that use the provider's DNS can be controlled with DNS caching servers. Bots that change DNS settings to point at open resolvers can be subverted by blocking port 53 traffic at the network edge. Severing this critical communications link renders the bots useless to their owner, and unable to send spam, launch DoS attacks, or support other illegal activities. This yields several benefits: traffic on the network is reduced, outgoing spam is reduced, and calls to the help desk from subscribers that are infected are reduced.

Eliminating traffic that is ultimately destined for use in amplification attacks or attack on the root servers by managing access to port 53 at the network edge is a best practice and obligation for service providers. It protects the provider's network and the networks of peers.

Protecting the DNS protects any revenue streams that might be associated with it. If a subscriber perception exists that the DNS is unreliable or easily compromised, their appetite for DNS-based services will be correspondingly less. Managing access to port 53 ensures protection against additional DNS attack vectors.

Providers proactively implementing services to protect subscribers differentiate themselves from laggard competitors. Consumer teaching pages offer a branding opportunity and a continuous reminder to subscribers that their ISP is looking out for them. These reminders create "stickiness" for this service and other provider services which drives demand and reduces churn.

## Managing Traffic on Port 53 Is Not Intrusive to the Subscriber

An increasingly important consideration for any service that is deployed today is whether or not the service intrudes on subscriber privacy or otherwise intrudes on the user experience. Managing traffic on port 53 is completely non-intrusive.

## Choice Can Be Preserved with the Right Implementation

Subscribers, advocacy groups and content providers expect that any new services deployed by providers preserve choice. Managing traffic on port 53 is completely compatible with preserving choice, which can easily be done by deploying filters at the edge of the network that permit DNS traffic to known legitimate

[12] http://en.wikipedia.org/wiki/Dan_Kaminsky#Flaw_in_DNS

open DNS resolvers. Subscribers who knowingly choose an alternative DNS provider can take advantage of the service without any notification to their ISP. This implementation is also resilient to changes in the services.

## Implementation Options to Manage Traffic on Port 53

The implementations of this practice could include:

1. Router access control lists deployed close to the end consumer that allow connectivity to legitimate DNS servers and protect against malicious DNS servers
2. Client software that provides auditing capabilities of the proper DNS settings
3. Home router/modem filters and configurations that limit use of malicious DNS servers

## Summary

Malicious threats to subscribers have exponentially grown in the past ten years with significant increases in obfuscations that directly relates to costs in resolving the root cause.

Service providers are in the unique position of protecting subscribers from millions of malicious DNS servers on the Internet. Less than a few hundred legitimate recursive DNS servers need to be white listed to provide subscribers with choice and flexibility. This provides for ease of deployment and maintenance over time. Service providers should consider managing port 53 to mitigate malicious DNS server threats against subscribers.