[September, 2012]

WORKING GROUP 4
Network Security Best Practices

FINAL Report – DNS Best Practices

Table of Contents

Table of Contents

1 Results in Brief

1.1 Charter

This Working Group was convened to examine and make recommendations to the Council regarding best practices to secure the Domain Name System (DNS) and routing system of the Internet during the period leading up to the successful global implementation of the Domain Name System Security Extensions (DNSSEC) and Secure BGP (Border Gateway Protocol) extensions.

1.2 Executive Summary

DNS is the directory system that associates a domain name with an IP (Internet Protocol) address. In order to achieve this translation, the DNS infrastructure makes hierarchical inquiries to servers that contain this global directory. These foundational systems are vulnerable to compromise through operator procedural mistakes as well as through malicious attacks that can suspend a domain name, or compromise their information and integrity. While there are formal initiatives under way to address this via implementation of DNSSEC, global adoption and implementation will take some time, and DNSSEC only solves a portion of the risks and challenges that ISPs face with DNS infrastructure, operation, and management.

This Final Report – DNS Best Practices documents the efforts undertaken by CSRIC Working Group 4 Network Security Best Practices with respect to securing DNS infrastructure that is within the purview of ISPs, including both DNS resolution services and authoritative (publishing) of DNS records. Issues affecting the security of management systems that provide control and designation of DNS records were also considered. The group also reviewed DNS security issues that may exploit an ISP's DNS infrastructure to launch attacks on third parties that are inherent to the nature of the DNS itself.

The working group identified many different potential security issues involving the DNS ranging from attacks to misconfigurations that can cause harm to ISPs, their users, and third parties. There are numerous publications, recommendations, standards, documentation, and other sources for handling these issues that have been published by industry organizations, standards bodies, DNS software providers, security practitioners and others in good standing to comment and recommend courses of action on these issues. The working group prioritized the issues it identified and surveyed these existing documents for those most appropriate to address the identified risks. Those documents, and relevant portions thereof, are then referenced both in the analysis and in the group's specific recommendations.

Issues that the working group considered included:

- Publication of falsified malicious information
- Use/dissemination of falsified malicious information published by authoritative nameservers
- Use/dissemination of falsified malicious information introduced in transit
- Insecure zone transfers (TSIG usage)
- Reflective DNS Amplification Attacks (allowing spoofed packets or amplification itself)
- Filtering/synthesized responses (potential interference with DNSSEC/unexpected client results)

- NX rewriting on resolvers (potential interference with DNSSEC/unexpected client results)
- Open resolvers - reflective distributed denial of service (DDoS) and other potential abuses
- Ghost domains - undesirable TTL refreshing on deleted domains in resolvers based on AUTH nameserver behavior
- Customers infected with DNS manipulating virus (e.g. DNSChanger)
- Customer using router with alternative DNS servers as default

The various roles that ISPs have to play with respect to these risks also had to be considered. The working group has divided up these issues into 6 categories in order to more easily enumerate them. These categories are:

1. Attacks against and issues with ISP Recursive Infrastructure
2. Attacks against and issues with ISP Authoritative DNS Infrastructure
3. Attacks against and issues with the DNS Infrastructure that ISPs provide to their customers
4. Abuse of an ISP's infrastructure to attack others or issues with an ISP's infrastructure that affect 3rd parties
5. Subscribers of ISPs with DNS issues within their premise infrastructure
6. Hygiene and other issues touching on DNS security

Working Group 4 recommends the adoption of numerous best practices for protecting ISPs' DNS infrastructures and addressing risks related to the DNS continuously faced by ISPs. DNS remains a cornerstone service provided by ISPs, both for allowing their customers to use the Internet, and for allowing customers to create and maintain their own Internet presences. As such, it is a critical service that ISPs must ensure is resilient to operational challenges and protect from abuse by miscreants. As a distributed infrastructure requiring several actors to both enable and protect it, ISPs face challenges outside of their direct control in tackling many of the issues identified. ISPs also should be taking measures to blunt the power of reflective DNS amplification DDoS attacks and the damage they can cause third parties.

SPECIAL NOTE: For brevity, and to address the remit of the CSRIC committee to make recommendations for ISPs, the term ISP is used throughout the paper. However, in most instances the reference or the recommendations are applicable to any DNS service components whether implemented by an ISP or by other organizations that peer to the Internet such as business enterprises, hosting providers, and cloud providers.

2 Introduction

CSRIC was established as a federal advisory committee designed to provide recommendations to the Commission regarding Best Practices and actions the Commission may take to ensure optimal operability, security, reliability, and resiliency of communications systems, including telecommunications, media, and public safety communications systems.

Due to the large scope of the CSRIC mandate, the committee then divided into a set of Working Groups, each of which was designed to address individual issue areas. In total, 10 different Working Groups were created, including Working Group 4 on Network Security Best Practices. This Working Group will examine and make recommendations to the Council regarding best practices to secure the Domain Name System (DNS) and routing system of the Internet during

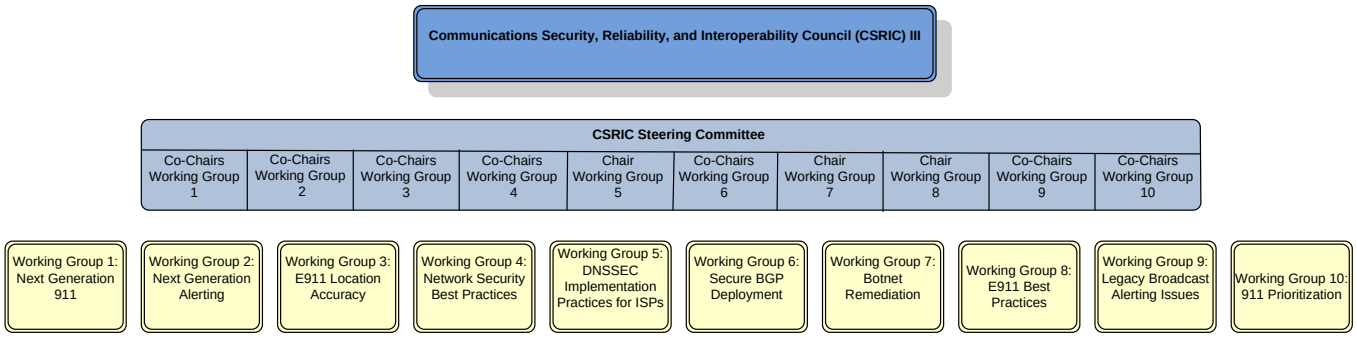
the period leading up to the successful global implementation of the Domain Name System Security Extensions (DNSSEC) and Secure BGP (Border Gateway Protocol) extensions.

This Final Report – DNS Best Practices documents the efforts undertaken by CSRIC Working Group 4 Network Security Best Practices with respect to securing DNS infrastructure that is within the purview of ISPs, including both DNS resolution services and authoritative (publishing) of DNS records. Issues affecting the security of management systems that provide control and designation of DNS records were also considered. The group also reviewed DNS security issues that may exploit an ISP's DNS infrastructure to launch attacks on third parties that are inherent to the nature of the DNS itself.

DNS and DNS related services have long been key components of most ISP operations, and there are many established practices and guidelines available for operators to consult. Thus most ISPs have mature DNS management and infrastructures in-place. Still, there remain many issues and exposures that introduce major risk elements to ISPs, since DNS services are usually critical for ISPs customers – either for access to the Internet or provisioning of their own Internet presences. This report enumerates the issues the group identified as most critical and/or that may need more attention.

The Working Group will present its report on routing issues in March 2013.

2.1 CSRIC Structure



2.2 Working Group [#4] Team Members

Working Group [#4] consists of the members listed below.

Name	Company
Rodney Joffe – Co-Chair	Neustar, Inc.
Rod Rasmussen – Co-Chair	Internet Identity
Mark Adams	ATIS (Works for Cox Communications)
Steve Bellovin	Columbia University
Donna Bethea-Murphy	Iridium
Rodney Buie	TeleCommunication Systems, Inc.
Kevin Cox	Cassidian Communications, an EADS NA Comp
John Crain	ICANN
Michael Currie	Intrado, Inc.
Dale Drew	Level 3 Communications
Chris Garner	CenturyLink
Igor Gashinsky	Yahoo, Inc.
Joseph Gersch	Secure64 Software Corporation
Jose A. Gonzalez	Sprint Nextel Corporation
Kevin Graves	TeleCommunication Systems (TCS)
Barry Greene	GETIT
Tom Haynes	Verizon
Chris Joul	T-Mobile
Mazen Khaddam	Cox
Kathryn Martin	Access Partnership
Ron Mathis	Intrado, Inc.
Danny McPherson	Verisign
Doug Montgomery	NIST
Chris Oberg	ATIS (Works for Verizon Wireless)
Victor Oppleman	Packet Forensics
Alan Paller	SANS Institute
Elman Reyes	Internet Identity
Ron Roman	Applied Communication Sciences
Heather Schiller	Verizon
Jason Schiller	Google
Marvin Simpson	Southern Company Services, Inc.
Tony Tauber	Comcast
Paul Vixie	Internet Systems Consortium
Russ White	Verisign
Bob Wright	AT&T

Table 1 - List of Working Group Members

3 Objective, Scope, and Methodology

3.1 Objective

This Working Group was convened to examine and make recommendations to the Council regarding best practices to secure the Domain Name System (DNS) and routing system of the Internet during the period leading up to the successful global implementation of the Domain

Name System Security Extensions (DNSSEC) and Secure BGP (Border Gateway Protocol) extensions.

DNS is the directory system that associates a domain name with an IP (Internet Protocol) address. In order to achieve this translation, the DNS infrastructure makes hierarchical inquiries to servers that contain this global directory. As DNS inquiries are made, their IP packets rely on routing protocols to reach their correct destination. BGP is the protocol utilized to identify the best available paths for packets to take between points on the Internet at any given moment. This foundational system was built upon a distributed unauthenticated trust model which was sufficient for the early period of the Internet.

These foundational systems are vulnerable to compromise through operator procedural mistakes as well as through malicious attacks that can suspend a domain name or IP address's availability, or compromise their information and integrity. While there are formal initiatives under way within the IETF (which has been chartered to develop Internet technical standards and protocols) that will improve this situation significantly, global adoption and implementation will take some time.

This Working Group will examine vulnerabilities within these areas and recommend best practices to better secure these critical functions of the Internet during the interval of time preceding deployment of more robust, secure protocol extensions.

This report covers the DNS portion of these overall group objectives.

3.2 Scope

Working Group 4's charter clearly delineates its scope to focus on two subsets of overall network security, DNS and routing. It further narrows that scope to exclude consideration of the implementation of DNSSEC (tasked to Working Group 5) and Secure BGP (tasked to Working Group 6). While those groups deal with protocol extensions requiring new software and/or hardware deployments; WG4 is geared toward items that either don't require these extensions or are risks which are outside the scope of currently contemplated extensions.

For this report regarding DNS, there are still a wide set of issues to consider, as DNSSEC only solves a limited set of DNS security problems. The areas considered within scope include issues presented by the protocol and implementation of DNS itself, broader network protection practices applied to DNS infrastructure and management elements, and protection of third party networks from abuses that are created by abuse of an ISP's DNS infrastructure.

3.3 Methodology

With the dual nature of the work facing Working Group 4, the group was divided into two sub-groups, one focused on issues in DNS security, another in routing security. Starting in December 2011, the entire Working Group met every two weeks via conference call(s) to review research and discuss issues, alternating between sub-groups. The group created a mailing list to correspond and launched a wiki to gather documents and to collectively collaborate on the issues. Additional subject matter experts were occasionally tapped to provide information to the working group via conference calls.

The deliverables schedule called for a series of reports starting in June 2012 that would first

identify issues for both routing and DNS security, then enumerate potential solutions, and finally present recommendations. The initial deliverables schedule was updated in March in order to concentrate efforts in each particular area for separate reports. This first report on DNS security issues is to be presented in September 2012, and the second report on routing issues will be published in March 2013.

Based on the discussions of the group, a matrix of DNS risks, potential solutions, and relevant BCP documents was created and refined over the course of the work. Subject matter experts in DNS then drove development of the initial documentation of issues and recommendations. These were then brought together into a full document for review and feedback. Text contributions, as completed, were reviewed, edited and approved by the full membership of Working Group 4.

4 Background

Note that in order to remain consistent with this other CSRIC III reports, section 4.1 "Brief Overview of the DNS" is taken verbatim from corresponding section of CSRIC III, Working Group 5 DNSSEC Implementation Practices for ISPs published March 8, 2012.

4.1 Brief Overview of the DNS

The Domain Name System (DNS) is a distributed hierarchical database which contains a listing of Internet resources and various types of information associated with those resources. Although the DNS has a variety of uses, its most important function is to bind user-friendly names of Internet resources to corresponding IP addresses of the systems that host those resources. This allows end users to conveniently depict and access Internet resources using recognizable names. The DNS also creates a logical linkage between the name of an Internet resource and its IP address, allowing a resource to retain the same name, even though its IP address and point of attachment to the network changes over time.

4.1.1 Structure of Domain Names

A domain name denotes an Internet resource, such as a website, an email address, a database server, or any machine or service that is accessible through the Internet. Domain names are hierarchically organized in a tree structure as shown in Figure 2. Each node in the hierarchy represents a domain and has a label associated with it. A domain may be the parent of subordinate domains (subdomains). The root of the DNS tree has no formal name, but is generally referred to as the DNS root domain. Below the root domain are the top-level domains (TLDs) which comprise the first-level group of domains. The TLDs include generic top-level domains (gTLDs) such as .com, .net, .org, .biz, .name, .info, .edu, etc. and country code top-level domains (ccTLDs) such as .us, .uk, .br, .de, .se and so on.

The next subordinate levels in the tree structure include the second-level domains, third-level domains, fourth-level domains, etc. There can be up to 127 levels of subordinate domains in the hierarchy.

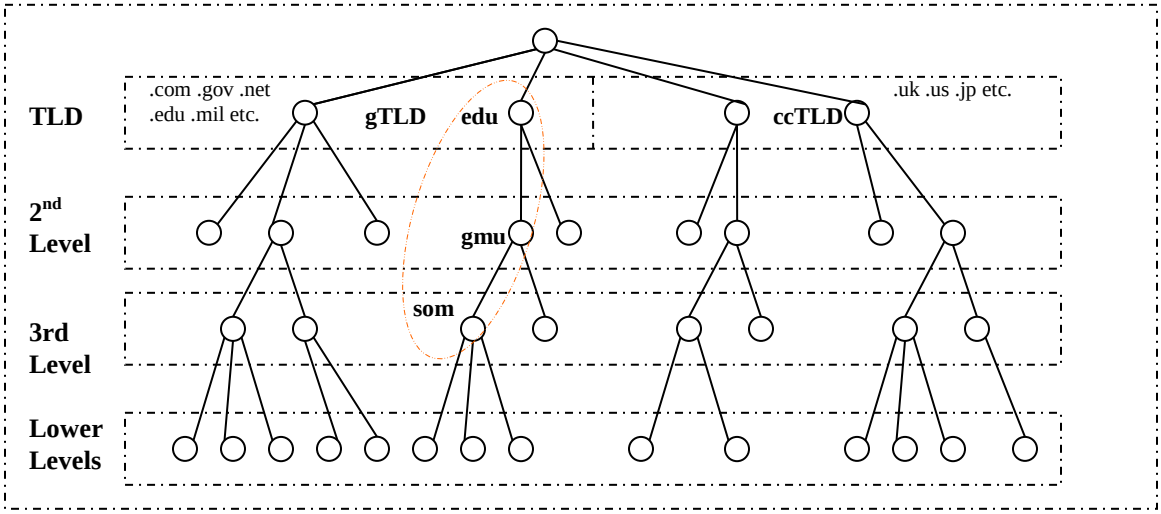


Figure 2 – Generic structure of DNS namespace

The administration of the DNS is decentralized. Each domain or subdomain can be managed by a separate organization. A domain administrator can delegate management of some of its subdomains to other entities—and this domain decomposition and delegation process can be enacted recursively. Parent domains maintain only pointers to servers that contain information about their subdomains so that DNS queries can be referred to the appropriate data sources. Each autonomously managed domain is called a zone. The syntax of a domain name consists of a sequence of labels (designating nodes in the namespace) separated by dots. Essentially, a domain name is an index entry in the DNS database. For example “som.gmu.edu” refers to the “som” subdomain under “gmu” in the “edu” gTLD.

The DNS database is distributed across a very large number of geographically dispersed nameservers that are managed by independent organizations. Each nameserver contains information pertaining to a subset of the DNS namespace and pointers to other nameservers that can lead to information in other parts of the database. Nameservers store data associated with domain names in resource records (RRs). Broadly speaking, there are two types of nameservers: (1) authoritative and (2) caching. An authoritative server has complete knowledge about a subset of the domain namespace, while caching servers improve query response time by locally caching a subset of global DNS data for a specified time interval.

4.1.2 Operation of the DNS

Operation of the DNS is based on a client-server model. Each user device contains a resolver, which is a local agent that sends and receives DNS queries on the user's behalf. The device will also have one or more designated DNS nameservers whose IP addresses are configured either automatically (e.g. using DHCP) or manually by the user or a local administrator.

From a user's perspective, the operation of the DNS proceeds as follows. First, a user or front-end software inputs a URL (e.g. a website address) into a network application (e.g. a web browser). The resource name is sent to a local resolver on the user’s device. If the resolver has a locally cached copy of the domain's IP address and other pertinent RR details for the requested resource, it passes that data back to the application. Otherwise, the resolver will query a designated nameserver. If the designated nameserver has a cached copy of the required RR, it

sends the information back to the user's resolver. Otherwise, how the server behaves will depend on whether it is configured with DNS recursion:

- If the server is NOT configured with DNS recursion, it will send the user resolver a referral to another nameserver in the DNS hierarchy. The resolver will then query the new server and this process occurs iteratively until the requested IP address and associated resource record information are obtained from a nameserver in the system.

- On the other hand, if the designated nameserver is configured with recursion, it serves as an agent for the user and recursively submits queries to other nameservers in the DNS hierarchy (each server will either furnish the RR information or issue a referral to another server). Eventually, the recursive server will fetch the information from a nameserver in the system and pass it back to the end user's resolver.

4.2 Roles and actors in provisioning and operating the DNS

Before the DNS can be used to translate between names and numbers on the Internet, the entity that wants to use a name needs to first "register" a domain name. The entity registering a domain name is referred to as the registrant. ISPs act as the registrant of the domain names they register and use to provide services.

The worldwide domain space is divided up into over 300 top level domains (TLDs), including those for countries corresponding to ISO 3166-1 alpha-2 country codes, several "generic" TLDs and various other TLDs[1]. An organization that runs the associated databases, publishes domains under its TLD into the DNS, and manages various aspects related to the domains in its TLD is called a domain name registry.

When registering a domain name within a TLD the registrant typically will use the services of a broker who collects information and payment from the registrant and works with the TLD registry to ensure the domain gets published into the overall DNS. This type of organization is referred to as a registrar. The registrant uses a registrar to both register a name and also to update any relevant DNS data with the TLD registry. The registrant will also use a registrar's services and systems to manage contact information associated with the domain (typically referred to as "whois" data) and will interact with the registrar to pay fees associated with the domain registration.

In the space of the generic Top Level Domains there are hundreds of registrars. These are accredited and operate under contract to the Internet Corporation for Assigned Names and Numbers (ICANN). Information pertaining to accredited registrars can be found at http://www.icann.org/en/resources/registrars

Aside from the Generic TLDs there are also many TLDs that do not fall directly under ICANN contracts. These are the Country Code TLDs and are managed by the respective Country Code managers. Many of those may also use a Registrant-Registrar-Registry model; however the registrars may not be ICANN-accredited and some still take direct registrations in a Registrant-Registry model.

[1] http://www.iana.org/domains/root/db

The authoritative side of the DNS is the responsibility of the zone manager. At the top level these are the TLD managers. They generate the zone file and distribute it either to DNS servers that they manage themselves or to third party operators with whom they have agreements.

This authoritative responsibility is the same at each level of the DNS hierarchy. At the second level, below the TLDs, many authoritative DNS servers are managed either by the registrant or by a third party service provider. The servers are maintained and operated by those wishing to provide responses. At each level, the names within that zone are assigned to nameservers. This allows for "walking the DNS tree" when resolving a domain name – each part of the domain is resolved by querying the designated nameservers for the next level down. At the primary operational level, ISPs will often act as zone manager for their customers' domains. Customers must update their domain names' name server entries with their registrar in order to move a domain name between authoritative nameservers.

The recursive side of DNS differs in that it is operated by the entities that wish to query and receive the DNS responses back that they can then translate to the required resource. End-user computers contain a "stub" resolver that can ask basic questions and kick off the DNS resolution process. In turn, there will be an upstream "recursive" DNS server, often on-premise, which the stub resolvers will query for cached data. If DNS data isn't cached there, an iterative process is begun to query progressive servers up a chain and eventually contact the authoritative server(s) for the desired record. Typically, if you operate a network you will also operate or have access to recursive DNS servers. ISPs typically maintain large, robust recursive DNS infrastructure. There are some well-known public servers that are used for DNS recursion as well.

4.3 ISP specific roles in DNS affected by security concerns

4.3.1 Recursive DNS server operator for customer base

ISPs typically provide DNS resolution services (DNS recursive resolvers) to their subscribers to enable them to utilize the DNS system and the Internet. This is a primary function for the vast majority of ISPs, and they will invest in server infrastructure – either physically or outsourced – to provide robust capacity and reliability to customers. It is notable, though, that customers may often choose to use an alternative recursive DNS provider if they wish, simply by updating settings on their computer or local router. ISP customers are reliant upon whatever recursive DNS servers they utilize for basic Internet connectivity – name resolution services – so this is a critical, core function for ISPs. Loss of recursive DNS service can effectively cut-off nearly all Internet access for ISP subscribers. Similar risks are inherent when issues at a customer's premise interfere with the ability of that customer to utilize the ISP's recursive nameserver infrastructure. Additional risks are introduced from 3rd party sources, when malicious, fraudulent or compromised domain names are resolved by ISP recursive servers and provided to customers. In such instances, the ISP enables potentially malicious activities via its recursive DNS infrastructure.

ISP customers as well as ISP staff and systems located on ISP networks are all reliant upon the ISP's recursive DNS infrastructure to resolve hostnames to IP addresses, look up mail server records, validate domain information, and other DNS functions necessary for communications on the Internet. There are several layers to these transactions:

1) A client computer needs to reach a location on the Internet that it has a name for, but not

the corresponding address resource. A computer may "cache" such data locally for a given time period, but when that value is unknown or stale (past its Time-to-Live, or TTL), it must ask a recursive DNS server for that answer.

2) The client computer will query one of the recursive DNS servers it is configured to query for the answer to its question about the DNS. This "stub resolver" on the client computer will iteratively ask all the recursive servers it knows until it gets a definitive response to its question.
3) The resolving nameserver is typically a "caching" nameserver that stores answers to questions it has been asked before. It will cache these answers until the TTL value for that answer expires. If the server doesn't have that information, it will then go through an iterative process up and down the authoritative DNS "tree" asking nameservers that are responsible for different levels of the DNS for the answer to the question it has about a particular domain or hostname. It will then return the answer it gets to the querying computer.
4) A recursive server itself may rely on other recursive/caching servers to get answers, and not direct queries to authoritative servers itself; that is a matter of configuration, and is often defined by operational policy. Thus there can be an entire chain of resolving servers between an end-user and the eventual authoritative servers that provide answers to DNS queries for that client.

Due to the nature of recursive DNS server operation, there is a particularly pervasive security concern in their operation. DNS queries are usually very small in size, but answers can be much larger – even several orders of magnitude larger. This provides a tool for "amplification" of packet sizes and when combined with other techniques, allows for "reflective DNS amplification," which is a very common DDoS attack. Thus operation of recursive DNS servers can lead to those servers being co-opted into attacks on an ISP's subscribers and, more often, other third parties.

4.3.2 Domain registrant and operator for ISP's own critical domains

ISPs register and maintain their own domain names at one or more domain registrars. These domains are then utilized by customers for various services, e.g. connectivity, e-mail, web publishing. Both the ISP and its customers rely on the domains that the ISP has registered and designated for primary services to be able to communicate and utilize the Internet. Interruption or interference with the provisioning of such domains within the domain registration system can in turn threaten the ability for an ISP and its customers to utilize the Internet.

4.3.3 AUTH DNS server operator for the ISP's own critical domains

An ISP provides authoritative DNS services directly for its own domains utilizing its own DNS server infrastructure. These domains are then utilized by customers for various services, e.g. Internet connectivity, e-mail, web publishing. Interruption or interference with the provisioning of such domains on the ISP's own authoritative DNS infrastructure can in turn threaten the ability for an ISP and its customers to utilize the Internet.

4.3.4 Direct AUTH DNS server operator for ISP customers' domains

An ISP will often provide authoritative DNS services directly to customers utilizing its own DNS server infrastructure. Customers rely on the ISP for provisioning and management of DNS

servers for the customers' DNS infrastructure. Interruption or interference with the provisioning of such domains on the ISP's authoritative DNS infrastructure can in turn threaten the ability for the ISP's customers to utilize the Internet, and for third parties to reach the domain names of affected customers for various services, e.g. website, e-mail, file transfer, telephony.

4.3.5 Outsourced AUTH DNS services provider to customers

An ISP can provide authoritative DNS services for its customers by providing access to a 3rd party's DNS services and server infrastructure. Customers rely on this 3rd party service for provision and management of DNS servers for customers' DNS infrastructure. Depending upon implementation, customers may also rely on the ISP for access to this service. Interruption or interference with the provisioning of such domains on the third party's authoritative DNS infrastructure can in turn threaten the ability for the ISP's customers to utilize the Internet, and for third parties to reach the domain names of affected customers for various services, e.g. website, e-mail, file transfer, telephony.

4.3.6 Provider of domain registration services to customers

ISPs often act as a domain name registrar or reseller of domain registration services to its customers. Customers register and manage their domain name registration settings via services provided by the ISP. Offering domain registration services opens an ISP up to the same risks inherent to organizations within the domain registration industry. Further, interruption or interference with the provisioning of such domains within a domain registration system provided by an ISP can in turn threaten the ability for an ISP's customers to utilize the Internet.

5 Analysis, Findings and Recommendations

The working group identified many different potential security issues involving the DNS ranging from attacks to misconfigurations that can cause harm to ISPs, their users, and third parties. There are numerous publications, recommendations, standards, documentations, and other sources for handling these issues that have been published by industry organizations, standards bodies, DNS software providers, security practitioners and others with good standing to comment and recommend courses of action on these issues. The working group prioritized the issues it identified and surveyed these existing documents for those most appropriate to address the identified risks. Those documents, and relevant portions thereof, are then referenced both in the analysis and in the group's specific recommendations.

Issues that the working group considered included:

- Publication of falsified malicious information
- Use/dissemination of falsified malicious information published by authoritative nameservers
- Use/dissemination of falsified malicious information introduced in transit
- Insecure zone transfers (TSIG usage)
- Reflective DNS Amplification Attacks (allowing spoofed packets or amplification itself)
- Filtering/synthesized responses (potential interference with DNSSEC/unexpected client results)
- NX rewriting on resolvers (potential interference with DNSSEC/unexpected client

results)
- Open resolvers - reflective DDoS and other potential abuses
- Ghost domains - undesirable TTL refreshing on deleted domains in resolvers based on AUTH nameserver behavior
- Customers infected with DNS manipulating virus (e.g. DNSChanger)
- Customer using router with alternative DNS servers as default

The various roles that ISPs have to play with respect to these risks also had to be considered. The working group has divided up these issues into 6 categories in order to more easily enumerate them. These categories are:

1. Attacks against and issues with ISP Recursive Infrastructure
2. Attacks against and issues with ISP Authoritative DNS Infrastructure
3. Attacks against and issues with the DNS Infrastructure that ISPs provide to their customers
4. Abuse of an ISP's infrastructure to attack others or issues with an ISP's infrastructure that affect 3rd parties
5. Subscribers of ISPs with DNS issues at their premise
6. Hygiene and other issues touching on DNS security

This section of the report presents various issues within these categories, listing the potential security issues the group identified and found worthy of commenting on. For each issue identified, a dedicated subsection provides a description of the issue; some level of detail including further in-depth information or background and/or examples; and any key findings. After each of the combined findings and analysis subsections per topic, there will be a list of BCPs and recommendations the working group identified for mitigating the described issue set.

For the most part, the group did not enumerate individual BCPs within industry standards documents that provide multiple practices, as those were deemed to be best examined within the full context of those documents. The group laid out the issues and directed the reader to the relevant BCPs. Some of the issues the group identified did not have consensus BCPs or may not apply across the entire spectrum of ISPs. In such cases the group recommends that ISPs be aware of the issues and consider applying the BCPs identified. The group was unable to identify industry-accepted BCPs that have been codified in widely accepted documents; in these cases, no particular BCPs were recommended, but the group felt that ISPs should be aware of these issues and look to adopt future BCPs in those areas.

5.1 Attacks against and issues with ISP Recursive Infrastructure

ISPs typically provide DNS resolution services (DNS recursive resolvers) to its subscribers to enable them to utilize the DNS system and the Internet. This is a primary function for the vast majority of ISPs, and they will invest in server infrastructure (either physically or outsourced) to provide robust capacity and reliability to customers. ISP customers are reliant upon whatever recursive DNS servers they utilize for basic Internet connectivity – name resolution services – so this is a critical, core function for ISPs. Loss of recursive DNS service due to attacks on that infrastructure or failures of that infrastructure can effectively cut-off nearly all Internet access for ISP subscribers.

Compromise of the integrity of data presented by an ISP's recursive DNS infrastructure exposes ISP customers to a myriad of security risks. With the notable exception of end-to-end DNSSEC

implementation, there is no authentication mechanism for end-users to verify the veracity of the information provided by an ISP recursive server. CSRIC III Working Group 5 is publishing various recommendations on the implementation of DNSSEC, but adoption, while growing, is still very low today. Thus, for the most part, malicious actors can successfully insert false information in ISP resolvers using a variety of attack methodologies. For example, an attacker could insert cache entries for the hostnames of popular Internet websites to direct users of those services to "drive-by download" sites that automatically install malware on victims' computers.

Another technique is to put in false entries for financial institutions or other sensitive services to redirect victims to look-alike sites to harvest access credentials – a practice called "pharming" in the security industry. Since DNS entries designate e-mail exchange servers via MX records, inserting bogus MX records into a recursive server cache can enable e-mail interception attacks. These attacks are particularly dangerous since they can be rather stealthy in nature. Pharming techniques can be implemented via man-in-the-middle scenarios that allow e-mail to be intercepted via re-routed DNS, but then forwarded back to the legitimate mail servers so e-mail recipients are unaware that their communications have been compromised. Whether done stealthily or not, use of bogus MX records to re-route e-mail is a major security concern.

These attacks can be specific to the DNS itself (the Kaminsky bug[2] or cache poisoning for example) so awareness of techniques used to poison DNS entries and practices to detect and defeat them are necessary for anyone running recursive DNS infrastructure, including ISPs. Since many of these attacks may be unique to DNS-based traffic, they wouldn't fall under more generic security monitoring tools, preventative techniques and practices. Such attacks can be detected with good monitoring tools and practices, and thwarted with configuration and operational stances that take into account the vectors used to launch them.

The largest attack surface for recursive nameserver infrastructure lies within the standard operational security paradigm that applies to any critical networked asset. Therefore the working group looked at including BCPs relating to network and operational security as part of addressing these issues, and ISPs should be aware that they are likely to see attacks against their recursive infrastructure based on these "traditional" methods of computer and network intrusion.

Recursive server responses can also be compromised by more mundane circumstances. For instance, a misconfigured server, a data transfer error, a hardware failure, or a stuck process could lead to inaccurate or stale data entries being presented by a recursive server. While the most likely outcome would be a loss of service in such circumstances, there are scenarios where incorrect resolution data could be provided to users, misdirecting their subsequent communications.

Recognition of the importance of the recursive DNS infrastructure to an ISP's core functionality for itself and its users and then treating it as a highly valuable asset are the first steps towards handling this area of risk. Standard measures to harden, monitor, respond to incidents, and make recursive DNS services resilient are the foundation needed to address most of these risks.

5.1.1 Cache Poisoning

Cache-poisoning attacks enabled via various flaws in the DNS protocol have been around for

[2] http://en.wikipedia.org/wiki/Dan_Kaminsky - Flaw_in_DNS

many years, and have been dealt with in updates to the protocol and DNS software. Typically, such attacks consist of various queries being made of a recursive server with some sort of spoofed response being returned that then gets cached by the targeted recursive nameserver. In 2008, the "Kaminsky Bug" showed that most servers were vulnerable to a specific type of external attack, leading to a massive upgrade of ISP DNS servers. However, it has been shown that even patched servers are still susceptible to an attack with a large enough botnet.[3] The good news for today is that mounting such an attack takes a massive scale of attempts to have any reasonable chance of success. DNSSEC implementation directly addresses this issue, therefore that topic is out of scope for this report.

In the absence of DNSSEC, ISPs need to be aware of such attack attempts and how to mitigate them. Unfortunately, there are no complete defenses to these attacks, and various mitigation strategies can lead to increased vulnerabilities to DDoS or other attacks. While the group was unable to identify any industry-wide published and accepted BCPs for fully defeating the latest developments in cache poisoning techniques (outside of DNSSEC), there is at least one RFC that is helpful in providing prescriptive advice for hardening recursive servers against cache poisoning attempts: RFC 5452 *Measures for Making DNS More Resilient against Forged Answers*[4]. This RFC describes and details out several DNS spoofing scenarios and then provides several potential countermeasures to be employed by DNS resolvers. While targeted primarily at vendors of DNS resolver servers, ISPs can still ensure their own servers and server operations meet the standards set forth in the document.

Beyond the industry standards identified, various DNS software vendors offer their own prescriptive advice for hardening servers against cache poisoning attempts, monitoring for such events, and mitigating them. Just as they would for any other piece of their critical infrastructures, ISPs will want to keep up-to-date on how to configure, protect and use their vendor's unique systems. Because different recursive DNS server software packages have varying susceptibility to the varied methods to launch cache poisoning attacks, it is difficult to provide any single best practice(s). Further, some recommended methods for protecting against cache poisoning could create new vulnerabilities. For example, using thresholds that trigger "ignore conditions" or cache flushes for large numbers of DNS responses for a particular query will likely stop a poisoning attack, but can be exploited for denial of service for the legitimate response on that nameserver. Thus any regime of operational, security, or configuration policies an ISP implements to protect against cache poisoning needs to be carefully evaluated based on the make-up of their server infrastructure and their risk-assessment.

One area where ISPs can look for raising their protection against cache poisoning is via monitoring of critical domain name responses across the recursive DNS infrastructure. This can be done in many ways, as ISP recursive DNS servers can be queried continuously and relatively heavily, as per their function. Thus ISP technical staff can implement a monitoring and alerting package or scripts to watch for expected answers, inconsistencies across servers, and other anomalies. This would include periodic automated polling of the DNS infrastructure to ensure expected results for key domains are found, and alerting upon detection of erroneous answers. Third party solutions and software can be utilized for this purpose, but even simple scripts can meet the basic goal of alerting ISP staff if critical domains are being tampered with.

[3] http://www.nytimes.com/2008/08/09/technology/09flaw.html?_r=1&partner=rssnyt&emc=rss
[4] http://tools.ietf.org/html/rfc5452

Regardless of measures taken to secure against cache poisoning, with the existing vulnerabilities, there is a decent chance that an ISP could face a major cache poisoning incident. Thus it is important to ensure that methods exist within the ISP's operations to respond to detected or reported successful cache poisonings. When such an event is identified, the offending entry needs to be rapidly removed (flushed) from any DNS servers that have stored it. Implementation of such measures, ability for response staff to access DNS servers, verification protocols and other considerations will vary widely depending on the organization of an ISP and their recursive DNS infrastructure, and the working group was not able to identify BCPs that could be applied universally.

5.1.1.1 Recommendations

1) ISPs should refer to the work of CSRIC III, Working Group 5 for a discussion of DNSSEC.
2) ISPs should review current ISP DNS Resolver infrastructure and ensure it meets the standards for recursive resolvers as described in RFC 5452.
3) ISPs should stay abreast of vendor recommendations for configuring, updating, and monitoring recursive DNS servers to protect against cache poisoning.
4) ISPs should ensure that methods exist within the ISP's operations to respond to detected or reported successful cache poisonings, so that such entries can be rapidly removed (flushed).
5) ISPs should consider implementing DNS-specific monitoring regimes to assess the integrity of data being reported by the ISP's recursive servers that meet the particular operational and infrastructure environments of the ISP.

5.1.2 Hacking and unauthorized 3rd party access to recursive infrastructure

ISPs and all organizations with an Internet presence face the ever-present risk of hacking and other unauthorized access attempts on their infrastructure from various actors, both on and off network. This was already identified as a key risk for ISPs, and CSRIC 2A – Cyber Security Best Practices was published in March 2011 to provide advice to address these types of attacks and other risks for any ISP infrastructure elements, including recursive DNS infrastructure. The current CSRIC III has added a new Working Group 11 that will report out an update to prior CSRIC work in light of recent advancements in cybersecurity practices and a desire of several US government agencies to adopt consensus guidelines to protect government and critical infrastructure computers and networks.

A recent SANS publication, *Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines (CAG)*[5] lays out these principals and maps them out versus prior work, including another relevant document, NIST SP-800-53 *Recommended Security Controls for Federal Information Systems and Organizations.*[6] The SANS publication appears to be a primary driver for Working Group 11's work. The entire document is available for review, and we have included the 20 topic areas here for reference:

[5] http://www.sans.org/critical-security-controls/
[6] http://csrc.nist.gov/publications/PubsSPs.html

Critical Control 1: Inventory of Authorized and Unauthorized Devices
Critical Control 2: Inventory of Authorized and Unauthorized Software
Critical Control 3: Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
Critical Control 4: Continuous Vulnerability Assessment and Remediation
Critical Control 5: Malware Defenses
Critical Control 6: Application Software Security
Critical Control 7: Wireless Device Control
Critical Control 8: Data Recovery Capability
Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps
Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services
Critical Control 12: Controlled Use of Administrative Privileges
Critical Control 13: Boundary Defense
Critical Control 14: Maintenance, Monitoring, and Analysis of Audit Logs
Critical Control 15: Controlled Access Based on the Need to Know
Critical Control 16: Account Monitoring and Control
Critical Control 17: Data Loss Prevention
Critical Control 18: Incident Response Capability
Critical Control 19: Secure Network Engineering
Critical Control 20: Penetration Tests and Red Team Exercises

Because this work is being analyzed directly by Working Group 11 to address the generic risk to ISPs of various hacking and unauthorized access issues, Working Group 4 will not be commenting in-depth in this area, and refers readers to reports from Working Group 11 for comprehensive, and updated coverage of these risks when they issue their report. We will comment upon current BCPs for ISPs to look to adopt in the interim, and provide further background around risks unique to running recursive DNS servers in this area.

An ISP's recursive nameserver infrastructure is an important asset to protect, as gaining control of it can lead to a wide variety of harms to ISP customers. Further, an ISP's staff computers, servers, and networking infrastructure also rely upon their recursive DNS servers to correctly map hostnames to the correct corresponding IP addresses. The ISP's own sensitive data and processes could be compromised via hacked recursive DNS servers. Thus recursive nameservers should be included on the list of network assets that are assigned the highest level of priority for protection under any type of ISP security program.

There are many industry standard publications pertaining to overall cybersecurity best practices available for adoption by ISPs or any organization at risk of attack, including prior CSRIC reports. It is incumbent upon ISPs to maintain their overall security posture and be up-to-date on the latest industry BCPs and adopt the practices applicable to their organization. Of particular note is the IETF's RFC 4778 - *Current Operational Security Practices in Internet Service Provider Environments*[7] which offers a comprehensive survey of ISP security practices. An older IETF publication, but still active BCP, that still applies to ISP environments can be found with BCP 46, aka RFC 3013 *Recommended Internet Service Provider Security Services*

[7] http://www.ietf.org/rfc/rfc4778.txt

and Procedures[8]. NIST also puts out highly applicable advice and BCPs for running government networks, with the most currently relevant special report, NIST SP-800-53.

NIST SP-800-81 *Secure Domain Name System (DNS) Deployment Guide*[9] addresses a wide variety of issues specific to running DNS servers in government environments. It is also highly relevant to ISPs as the BCPs and advice it provides largely apply to any organization running DNS infrastructures for large numbers of clients. This document has sound advice for handling numerous DNS threats with Section 5, *DNS Hosting Environment—Threats, Security Objectives, and Protection Approaches* being relevant to the risks presented by unauthorized access to recursive DNS servers.

The Internet Society (ISOC) has recently published a comprehensive document that addresses a wide variety of DNS risks and recommended BCPs and strategies to address them: *Towards Improving DNS Security, Stability, and Resiliency*[10]. This paper provides an excellent background on threats to and from the DNS, and a survey of relevant RFCs and practices to mitigate them; it is a solid reference for any ISP looking to identify and avoid DNS risks.

The ultimate goal of someone attempting unauthorized access to recursive DNS infrastructure would be to either deny customer use of those servers or, more likely, insert false entries within the server to misdirect the users of those servers. This is the equivalent of a DNS cache poisoning attack as already described in section 5.1.1. So the analysis and recommendations presented in section 5.1.1.1 and 5.1.1.2 with respect to monitoring for and reacting to DNS cache poisoning attacks apply in the scenario where an attacker has breached a DNS server to add incorrect DNS entries. It is also important to note that such false entries will fail DNSSEC checking, so the report on implementation of DNSSEC that Working Group 5 is germane to this risk area as well.

5.1.2.1 Recommendations

1) ISPs should refer to and implement the practices found in CSRIC 2A – Cyber Security Best Practices that apply to securing servers and ensure that recursive nameserver infrastructure is protected.
2) ISPs should adopt applicable BCPs found in other relevant network security industry approved/adopted publications. Monitor for applicable documents and update. Five documents were identified that currently apply to protecting ISP networks: IETF RFC 4778 and BCP 46 (RFC 3013); NIST special publications series: NIST SP-800-53 and NIST SP-800-81; ISOC publication: *Towards Improving DNS Security, Stability, and Resiliency*
3) ISPs should refer to the work of CSRIC III, Working Group 5 for a discussion of DNSSEC implementation.
4) ISPs should ensure that methods exist within the ISP's operations to respond to detected or reported successful cache poisonings, so that such entries can be rapidly removed (flushed).
5) ISPs should consider implementing DNS-specific monitoring regimes to assess the integrity of data being reported by the ISP's recursive servers that meet the particular

[8] http://www.apps.ietf.org/rfc/rfc3013.txt
[9] http://csrc.nist.gov/publications/PubsSPs.html
[10] http://www.internetsociety.org/sites/default/files/bp-dnsresiliency-201201-en_0.pdf

operational and infrastructure environments of the ISP.

5.1.3 ISP insiders inserting false entries into resolvers

While insider threats can be considered a subset of the more general security threat of unauthorized access and hacking, they deserve special attention in the realm of DNS security. ISP insiders have unparalleled access to any systems run by an ISP, and in the case of recursive DNS infrastructure, the ability to modify entries is both trivially easy and difficult to detect. In the most notorious cases of suspected cache poisoning to date, an ISP insider at a major Brazilian ISP is alleged to have conspired with criminals to redirect millions of ISP customers' online banking sessions to look-alike websites via false entries injected into recursive nameservers at the ISP. [11] Since recursive nameservers don't typically have company-sensitive information, are accessed by thousands of machines continuously, and are not usually hardened or monitored like other critical servers, it is relatively easy for an insider to slip something into the cache of a recursive server. Since entries in cache are typically memory-resident, and transient over time, detection of malicious entries is particularly difficult if coming from an internal source rather than an external vector where other protection mechanisms may detect poisoning or other hacking attempts.

In some special cases, an ISP's recursive nameserver infrastructure could be serving up "split DNS" where internal hostnames to the ISP's operations are resolved differently than public domains and hostnames. This is akin to an enterprise network that has its own private IP cloud but still must resolve local hostnames while providing full Internet resolution to users on that network. In such a set-up within an ISP, a malicious or unknowing insider with access to the ISP's recursive infrastructure could configure that server to resolve internal hostnames externally and potentially expose data or processes to the wider Internet.

With the exception of the "split DNS" case, the analysis and recommendations for this particular threat do not differ significantly from those presented in Section 5.1.2 of this report - Hacking and unauthorized 3rd party access to recursive infrastructure. However, it is worth paying special attention to this particular exposure given the history of prior incidents and liabilities an ISP may be exposed to from such difficult-to-detect activities of its own employees.

5.1.3.1 Recommendations

1) Refer to section 5.1.2.1 for generic hacking threats.
2) If running a split DNS configuration, an ISP should be aware of the risks of exposure a misconfigured recursive server presents and follow BCPs for detecting and mitigating issues.

5.1.4 Resiliency of ISP Recursive nameservers

DNS is by its nature distributed and highly resilient; however, ISPs can take several different

[11] See relevant stories at http://www.securelist.com/en/blog/208193214/Massive_DNS_poisoning_attacks_in_Brazil, http://threatpost.com/en_us/blogs/major-dns-cache-poisoning-attack-hits-brazilian-isps-110711 and http://www.thetechherald.com/articles/Insider-arrested-after-DNS-poisoning-attack-targets-Brazilian-ISPs.

measures to make it even more resilient to configuration errors, attacks, and service interruptions. At all levels, DNS is designed to iteratively attempt alternative servers when the one it is attempting to reach isn't available. This means that simply provisioning more servers or more alternative servers to attempt to reach within settings of clients or recursive infrastructure can obviate a range of issues. BCPs are available for ISPs to consult on how to configure and balance server infrastructure geographically, topologically, and operationally. Separation of DNS servers over network topologies, geographical locations and even differing versions of software are easy to accomplish due to the inherent properties of DNS servers to share data and load over the DNS protocol itself. That allows DNS operators to minimize many of the risks that other Internet services face based on need for proximity and lack of easy replication. Add in resiliency-enhancing network technologies like anycast, multiple peers, or redundant routing paths – or hardware-based enhancements for redundancy like RAID or multiple network interfaces – and DNS services can be made extremely resilient to any number of standard IT systems risks. There are many practices to choose from, which recommend configuring operations of servers, their networks, and environments to improve resiliency of DNS operations.

On the recursive side of the DNS resiliency equation, the areas of particular interest for ISPs include a variety of practices. These include focusing on client (stub resolver) configuration, provisioning of recursive servers and their network environments, policies for the operation of recursive servers (caching size and time limits), and upstream recursive server strategy. Provisioning of recursive DNS server infrastructure is an ongoing critical service performed by ISPs on a regular basis, so most ISPs are well aware of their current and future recursive server needs for their customer base. However, it is always good practice to keep up with the latest BCPs when it comes to provisioning and ensuring that critical services are resilient.

NIST SP-800-81 *Secure Domain Name System (DNS) Deployment Guide*[12] addresses a wide variety of issues specific to running DNS servers in government environments. It is also highly relevant to ISPs as the BCPs and advice it provides largely apply to any organization running DNS infrastructures for large numbers of clients. Many of the recommendations within this document deal directly with the resiliency of the DNS in environments of similar size and risk profiles as many ISPs.

As mentioned in 5.1.2, the Internet Society (ISOC) has recently published a comprehensive document that addresses a wide variety of DNS risks and recommended BCPs and strategies to address them: *Towards Improving DNS Security, Stability, and Resiliency*[13]. This paper provides an excellent background on threats to and from the DNS, including improving resiliency of DNS operations. The included survey of relevant RFCs and practices to mitigate them is a solid reference for any ISP looking to identify and avoid DNS risks.

5.1.4.1 Recommendations

1) ISPs should be aware of their current and anticipated operational resiliency for recursive DNS service and be prepared to provision according to these needs guided by industry-accepted BCPs.
2) ISPs should refer to and implement the BCPs relating to resiliency of DNS

[12] http://csrc.nist.gov/publications/PubsSPs.html
[13] http://www.internetsociety.org/sites/default/files/bp-dnsresiliency-201201-en_0.pdf

infrastructure found in CSRIC 2A – Cyber Security Best Practices that apply to the resiliency of recursive nameserver infrastructure.

3) ISPs should adopt applicable BCPs found in other relevant network security industry approved/adopted publications. Monitor for applicable documents and update. Two were identified that currently apply to improving the resiliency of recursive nameservers in ISP networks: NIST SP-800-81 and the ISOC publication: *Towards Improving DNS Security, Stability, and Resiliency.*

5.1.5 Denial-of-Service Attacks of ISP Recursive nameservers

Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) are some of the oldest and most prolific attacks that ISPs have faced over the years and continue to defend against today. Typically, an external actor who is targeting some Internet presence or infrastructure to make it unusable is behind such attacks. However, DoS/DDoS attacks come in many flavors that can be broadly lumped into two primary categories: logic attacks and resource exhaustion/flooding attacks.[14] Logic attacks exploit vulnerabilities to cause a server or service to crash or reduce performance below usable thresholds. Resource exhaustion or flooding attacks cause server or network resources to be consumed to the point where the targeted service no longer responds or service is reduced to the point it is operationally unacceptable. We will examine the latter type of attack in this section of analysis. Logic attacks are largely directed to break services/servers and can be largely addressed with the analysis and recommendations put forward in section 5.1.2 that cover protecting networked assets from various hacking and other attacks.

There is a large variety of flooding attacks that an ISP could face in daily operations. These can be targeted at networks or any server, machine, or even user of an ISP's network. From the perspective of recursive nameserver operations, it is helpful to differentiate between "generic" DoS attacks that could affect any server, and those that exploit some characteristic of the DNS that can be utilized to affect recursive DNS servers in particular. There are also some characteristics of recursive DNS deployment within an ISP environment that may differentiate recursive DNS servers from other network assets that could be attacked.

Due to the long history, huge potential impact, and widespread use of various DoS and DDoS attacks, there is an abundance of materials, services, techniques and BCPs available for dealing with these attacks. ISPs will likely have some practices in place for dealing with attacks both originating from their networks and that are being directed at their networks and impacting their services. The IETF's RFC 4732 *Internet Denial-of-Service Considerations*[15] provides an ISP with a thorough overview of DoS/DDoS attacks and mitigation strategies and provides a solid foundational document. The SANS Institute has published a useful document for ISPs that is another reference document of BCPs against DoS/DDoS attacks entitled *A Summary of DoS/DDoS Prevention, Monitoring and Mitigation Techniques in a Service Provider Environment*[16].

As mentioned in section 5.1.2, there are several documents that cover general ISP security concerns, and those typically include prescriptive advice for protecting a network against

[14] http://static.usenix.org/publications/library/proceedings/sec01/moore/moore.pdf
[15] http://tools.ietf.org/rfc/rfc4732.txt
[16] http://www.sans.org/reading_room/whitepapers/intrusion/summary-dos-ddos-prevention-monitoring-mitigation-techniques-service-provider-enviro_1212

DoS/DDoS attacks. Such advice can be found in previously cited documents including prior CSRIC reports: CSRIC 2A – Cyber Security Best Practices[17], the IETF's RFC 4778 - *Current Operational Security Practices in Internet Service Provider Environments*[18], BCP 46, RFC 3013 *Recommended Internet Service Provider Security Services and Procedures*[19] and NIST's special report, NIST SP-800-53.

It is worth noting that many ISPs isolate recursive DNS servers from the Internet at large, allowing them to be accessed solely by ISP customers. This is done via implementation of access control lists (ACLs), filtering of DNS packets from outside the network, and other practices outlined in various recommendations for splitting DNS services. This means that many ISPs' recursive DNS infrastructures will not be visible to attackers outside the ISP's network, and may be thought of as being "safe" from attack. However, DoS/DDoS attacks are still possible from within the network, from a malicious user, a compromised machine, or botnet members present within the ISP's network. Thus ISPs should be aware of this threat and not rely solely upon their partitioning of recursive DNS servers from the Internet as a defense for their recursive server infrastructure. The same BCPs for protecting against DoS/DDoS attacks for critical network assets still apply in the segregated model.

Recursive DNS servers don't have the same vulnerabilities that Authoritative ones do to DNS-specific attacks, since they can be restricted from general Internet access and are not "required" to respond to queries for a zone they service. However, if an ISP configures recursive DNS servers to respond to queries from any source, an "open resolver", then it is likely to be susceptible to the resource exhaustion attacks. This is also an issue if a recursive DNS server also serves as an authoritative server for publicly available zones. An attacker simply has to issue enough queries from a large enough botnet to overwhelm the server's capacity to answer queries. Since an attacker can request response records that are larger than the queries themselves, this also leads to the potential for amplification effects. There are several publications that address BCPs for splitting DNS services (AUTH and Recursive) and eliminating open recursive servers – typically for eliminating downstream attacks made possible by these attacks, but they remain practical advice for addressing these types of direct attacks to recursive DNS infrastructure. The definitive paper addressing this problem from a BCP standpoint is the IETF's BCP 140, RFC 5358 *Preventing Use of Recursive Nameservers in Reflector Attacks*[20]. This issue is also addressed in NIST's special report, NIST SP-800-81.

5.1.5.1 Recommendations

1) ISPs should implement BCPs and recommendations for securing an ISP's infrastructure against DoS/DDoS attacks that are enumerated in the IETF's RFC 4732 *Internet Denial-of-Service Considerations* and consider implementing BCPs enumerated in the SANS Institute reference document of BCPs against DoS/DDoS attacks entitled *A Summary of DoS/DDoS Prevention, Monitoring and Mitigation Techniques in a Service Provider Environment*.
2) ISPs should refer to and implement the BCPs related to DoS/DDoS protection found in CSRIC 2A – Cyber Security Best Practices that apply to protecting servers from

[17] http://www.fcc.gov/pshs/docs/csric/WG2A-Cyber-Security-Best-Practices-Final-Report.pdf
[18] http://www.ietf.org/rfc/rfc4778.txt
[19] http://www.apps.ietf.org/rfc/rfc3013.txt
[20] http://tools.ietf.org/html/bcp140

DoS/DDoS attacks.

3) ISPs should consider adopting BCPs found in other relevant network security industry approved/adopted publications that pertain to DoS/DDoS issues, and monitor for applicable documents and updates. Four that currently apply to protecting ISP networks from DoS/DDoS threats are IETF RFC 4778 and BCP 46 (RFC 3013); NIST special publications series: NIST SP-800-53; and ISOC Publication *Towards Improving DNS Security, Stability, and Resiliency*.
4) ISPs should eliminate open recursive nameservers and separate recursive DNS services from authoritative DNS services as prescribed in the IETF's BCP 140, RFC 5358 *Preventing Use of Recursive Nameservers in Reflector Attacks* and also articulated in NIST's special report, NIST SP-800-81.

5.2 Attacks against and issues with ISP Authoritative DNS infrastructure

An ISP's authoritative DNS infrastructure includes all functions necessary for provisioning of domain and host names used by an ISP for its own Internet presence. These domains and hostnames are utilized by ISP customers for various services, e.g. connectivity, e-mail, web publishing. The ISP itself is also dependent upon the domains it owns and publishes for its own internal operations and interaction with both customers and other organizations on the Internet including upstream providers. Interruption, interference, or tampering with the provisioning of such domains on the ISP's systems can in turn threaten the ability for an ISP and its customers to utilize the Internet, and to trust the integrity of communications to, within, and from the ISP.

There are several layers in publishing DNS entries for an ISP's domains and hostnames:

1) The ISP registers and maintains the domain names they need (e.g. ispname.net) at a domain name registrar.
2) The domain name registrar enters the ISP's domain names and associated primary DNS servers into the appropriate domain registry's TLD database (e.g. VeriSign in the case of .com or .net). The registry in-turn publishes information to enable resolution of domain names under its TLD via its own authoritative nameservers.
3) An ISP may act as its own domain registrar if it is accredited by the relevant domain name registry and/or ICANN (VeriSign and ICANN respectively in the case of .com or .net domains).
4) The ISP publishes the domains it needs to use via authoritative (AUTH) nameservers. These nameservers can be run by either the ISP itself or a third-party DNS provider. In some cases, hybrid solutions are put in place where the ISP may run a "master" of the zone file for a domain, and a third party sets up secondary AUTH servers that receive their configurations from the primary server.
5) The ISP subdivides the domains it uses into various zones, and assigns addresses and services (like MX records for e-mail exchange servers) via the configuration of the primary AUTH DNS server or DNS management system.
6) Zones are replicated to additional AUTH servers to provide redundant authoritative DNS service for the domains by the primary server or DNS management system.
7) DNS entries are updated, maintained and monitored by the ISP's DNS operations staff.
8) ISP renews and manages domain names with registrar to ensure continued availability.

With all the responsible parties involved along with the various levels of AUTH DNS infrastructure needed to resolve an ISP's domains, there are several avenues for attack against an

ISP's authoritative DNS infrastructure. There is also ample opportunity for operational error, configuration problems, or a myriad of other issues to arise in the standard maintenance of an ISP's DNS infrastructure.

Denial-of-service attacks, service interruptions at any level along the DNS chain, hijacking of a domain name, domain name expirations, and other issues that affect the publishing of DNS information for an ISP's domains can have immediate, severe effects on ISP customers and ISP operations. These risks can be partially mitigated via long time-to-live (TTL) values for domain information, since DNS data is cached once retrieved; but using long TTLs introduces risks as well and decreases the flexibility a domain operator has for making changes.

Corruption of published DNS data for an ISP's domain names creates even greater risks to ISPs and ISP customers. In many respects, attacks or instances that create a situation where false DNS data is published by an authoritative source create similar scenarios as cache poisoning attacks. The difference being that it is the universe of caching nameservers throughout the Internet that end up storing the corrupted data when they query the authoritative servers. In turn, these "poisoned" recursive servers end up serving users that query them this incorrect information. An attacker can use this Internet-wide scale of attack to intercept the e-mail of all of an ISP's customers, deny basic access to the Internet by the ISP's customers, and potentially introduce malware or capture access credentials via malicious websites set-up in the stead of the legitimate ISP's site.

Such corruption attacks are exacerbated when an attacker uses long TTL, so even after an incident is mitigated by the ISP, any server that has cached the incorrect values will continue presenting them until the TTL expires. An ISP that uses long TTL values may prevent some or most caching servers around the Internet from receiving false updates if they can mitigate the corruption quickly; but again, this introduces other risks and operational constraints. Such corruptions can be inserted anywhere along the DNS chain, from the authoritative servers responsible for actual publishing the detailed zone information all the way up the chain of authority back to the domain registry itself. Attackers have successfully penetrated domain registrars and registries to attack major Internet properties and ISPs in the past, making this a real-world problem that is largely out of the direct control of an ISP to prevent.

5.2.1 Denial-of-Service Attacks of ISP AUTH nameservers

As articulated by section 5.1.5, DoS/DDoS attacks against ISP infrastructure are some of the most prevalent and damaging incidents that are seen in ISP operations. The analysis and recommendations articulated in section 5.1.5 covering DoS/DDoS against recursive nameservers apply in large-part to DoS/DDoS incidents involving authoritative servers and should be reviewed for further information on the generic problem.

Unlike recursive servers, authoritative nameservers must be publicly available in order for the domains they serve to be resolved across the Internet. Thus measures to restrict access that can be implemented for an ISP's recursive servers are unavailable as options for authoritative nameservers. This leaves an ISP with limited choices for DDoS protection, including the traditional approaches of overprovisioning of equipment and bandwidth, anycast (which introduces its own risks), and various DoS/DDoS protection services and techniques. One advantage that DNS has over other Internet based services is that the DNS is, by its very nature, distributed and resilient, so a resolving server automatically and iteratively attempts to reach

alternative authoritative servers if it cannot reach the one it is currently attempting to contact. This makes it harder for an adversary (or accident) to take out all authoritative DNS servers for a particular domain; but successful attacks still occur with great regularity.

A common tactic that many administrators running authoritative server infrastructures do in order to avoid crippling attacks on primary servers is to run private or "stealth" master nameservers and have all public-facing nameservers act as secondary nameservers to those hidden masters. This also allows for performance improvements (increased resiliency) since time- and processor-intensive updates can be made to the hidden masters, even taking them offline, while the secondary's continue running as normal and merely receive a light-weight incremental update when the primary servers are back online. This configuration also allows for standard or emergency provisioning of secondary services using a 3rd party – a peering partner or outsourced DNS service, for example. Thus if a DoS/DDoS attack is launched at the ISP's public-facing nameservers, new secondary servers can be provisioned quickly at a larger number or more robust nameserver infrastructure, or even a service offering DDoS protection. The IETF has a document (BCP 16, RFC2182 *Selection and Operation of Secondary DNS Servers*[21]) that addresses this issue directly with recommendations and BCPs for adding redundant secondary nameservers and configuration of "stealth" servers.

There is another important consideration for protecting authoritative nameservers against DoS/DDoS attacks. Since authoritative DNS servers provide a public service that handles large numbers of concurrent clients and short-term connections over most available ports, placing a stateful device like a firewall between a DNS server and the Internet *requires careful analysis. Stateful methods can provide important protections for small or medium DNS deployments. For very large volume deployments, these methods may create a performance issue, so this "standard" security measure may not be an option for these large deployments.* This is often true for standard operations, and certainly in the case where an adversary is attempting to DoS an authoritative nameserver. Thus ISPs should review and apply BCPs for protecting network assets carefully to ensure they apply well to an authoritative DNS server given the volume and type of traffic it handles. The documents cited in section 5.1.5 still apply for reference sources.

5.2.1.1 Recommendations

1) ISPs should implement BCPs and recommendations for securing an ISP's infrastructure against DoS/DDoS attacks that are enumerated in the IETF's RFC 4732 *Internet Denial-of-Service Considerations* and consider implementing BCPs enumerated in the SANS Institute reference document of BCPs against DoS/DDoS attacks entitled *A Summary of DoS/DDoS Prevention, Monitoring and Mitigation Techniques in a Service Provider Environment*.
2) ISPs should refer to and implement the BCPs related to DoS/DDoS protection found in CSRIC 2A – Cyber Security Best Practices that apply to protecting servers from DoS/DDoS attacks.
3) ISPs should consider adopting BCPs found in other relevant network security industry approved/adopted publications that pertain to DoS/DDoS issues, and monitor for applicable documents and updates. Four that currently apply to protecting ISP networks

[21] http://tools.ietf.org/html/rfc2182

from DoS/DDoS threats are IETF RFC 4778 and BCP 46 (RFC 3013); NIST special publications series: NIST SP-800-53; and ISOC Publication *Towards Improving DNS Security, Stability, and Resiliency*.

4) ISPs should implement BCPs relevant to their network architecture as described in BCP 16, RFC2182 *Selection and Operation of Secondary DNS Servers*
5) ISPs should review and apply BCPs for protecting network assets against DoS/DDoS attacks carefully to ensure they are appropriate to protect an authoritative DNS server.

5.2.2 Resiliency of an ISP's own authoritative nameservers

As described in section 5.1.4, DNS is by its nature distributed and highly resilient; however, ISPs can take several different measures to make it even more resilient to configuration errors, attacks, and service interruptions. Additional analysis on general tactics for increasing the resiliency of DNS services in general can be found in that section.

On the authoritative side of the DNS resiliency equation, the areas of particular interest for ISPs encompass a variety of practices. These include items such as ample provisioning of authoritative servers in varied network environments, topologies and geographies; policies for the publication of zones provided by authoritative servers (zone splits, TTLs, views, and other operational considerations); and load distributing strategies (e.g. configuring primary/secondary servers and zone updates). The analysis in section 5.2.1 outlining configuration of "hidden master" nameservers is extremely germane to increasing resiliency of authoritative DNS servers, and should be considered as an option in this space – consulting relevant BCPs. Provisioning of an ISP's own authoritative DNS server infrastructure is an ongoing critical service performed by the ISP continuously, so most ISPs are well aware of their current and future server needs for their operations. However, it is always good practice to keep up with the latest BCPs when it comes to provisioning and ensuring that critical services are resilient.

NIST SP-800-81 *Secure Domain Name System (DNS) Deployment Guide*[22] addresses a wide variety of issues specific to running DNS servers in government environments. It is also highly relevant to ISPs as the BCPs and advice it provides largely apply to any organization running DNS infrastructures for large numbers of clients – particularly in provisioning authoritative servers. Many of the recommendations within this document deal directly with the resiliency of the DNS in environments of similar size and risk profiles as many ISPs.

The BCPs for running additional nameservers as detailed in BCP 16, RFC2182 *Selection and Operation of Secondary DNS Servers* are highly relevant to this topic space.

As mentioned in section 5.1.2, the Internet Society (ISOC) has recently published a comprehensive document that addresses a wide variety of DNS risks and recommended BCPs and strategies to address them: *Towards Improving DNS Security, Stability, and Resiliency*[23]. This paper provides an excellent background on threats to and from the DNS, including improving resiliency of DNS operations. The included survey of relevant RFCs and practices to mitigate them and is a solid reference for any ISP looking to identify and avoid DNS risks.

[22] http://csrc.nist.gov/publications/PubsSPs.html
[23] http://www.internetsociety.org/sites/default/files/bp-dnsresiliency-201201-en_0.pdf

5.2.2.1 Recommendations

1) ISPs should be aware of their current and anticipated operational resiliency for authoritative DNS service and be prepared to provision according to these needs guided by industry-accepted BCPs.
2) ISPs should refer to and implement the BCPs relating to resiliency of DNS infrastructure found in CSRIC 2A – Cyber Security Best Practices that apply to the resiliency of recursive nameserver infrastructure.
3) ISPs should implement BCPs relevant to their network architecture as described in BCP 16, RFC2182 *Selection and Operation of Secondary DNS Servers.*
4) ISPs should adopt applicable BCPs found in other relevant network security industry approved/adopted publications. Monitor for applicable documents and update. Two were identified that currently apply to improving the resiliency of authoritative nameservers in ISP networks: NIST SP-800-81 and the ISOC publication: *Towards Improving DNS Security, Stability, and Resiliency.*

5.2.3 Hacking and unauthorized 3rd party access to ISP AUTH nameserver infrastructure

As articulated by section 5.1.2, hacking and unauthorized access to any ISP infrastructure is an ever-present threat. The analysis and recommendations articulated in section 5.1.2 covering hacking and unauthorized third party access to recursive nameservers apply in large-part to authoritative servers as well, and should be reviewed for further information on the generic problem.

Unlike recursive servers, authoritative nameservers must be publicly available in order for the domains they serve to be resolved across the Internet. Thus measures to restrict public visibility or network access that can be implemented for an ISP's recursive servers are unavailable as options for authoritative nameservers. They are publicly reachable servers, and thus exposed to the full range of hacking vectors a public-facing server must handle. Making this even more challenging, since authoritative DNS servers provide a public service that should handle large numbers of concurrent clients and short-term connections over most available ports, placing a stateful device like a firewall between a DNS server and the Internet is typically inadvisable, so this "standard" security measure isn't usually an option. This is often true for standard operations, and certainly in the case where an adversary is attempting to DoS an authoritative nameserver. Thus ISPs should review and apply BCPs for protecting network assets carefully to ensure they apply well to an authoritative DNS server given the volume and type of traffic it handles. The documents cited in section 5.1.2 still apply for reference sources.

Corruption of published DNS data for an ISP's domain names creates several external risks to ISPs and ISP customers. In many respects, attacks or instances that create a situation where false DNS data is published by an authoritative source create similar scenarios as cache poisoning attacks. The difference being that it is the universe of caching nameservers throughout the Internet that end up storing the corrupted data when they query the authoritative servers. In turn, these "poisoned" recursive servers end up serving users that query them this incorrect information. An attacker can use this Internet-wide scale of attack to intercept the e-mail of all of an ISP's customers, deny basic access to the Internet by the ISP's customers, and potentially introduce malware or capture access credentials via malicious websites set-up in the stead of the legitimate ISP's site.

Such corruption attacks are exacerbated when an attacker uses long TTL values, so even after an incident is mitigated by the ISP, any server that has cached the incorrect values will continue presenting them until the TTL expires. An ISP that uses long TTL values may prevent some or most caching servers around the Internet from receiving false updates if they can mitigate the corruption quickly; but again, this introduces other risks and operational constraints. Unfortunately, there is no "global reset" button for updating all caching nameservers around the Internet to purge incorrect or malicious data they have cached during an attack or event. Some commercial services exist to provide some limited assistance in this arena, and ISPs and others who have had to deal with these issues may have networks of contacts to notify to flush caches; but there are no BCPs or full solutions available to address this Internet-wide cache poisoning issue at this time.

5.2.3.1 Recommendations

1) ISPs should refer to and implement the BCPs found in CSRIC 2A – Cyber Security Best Practices that apply to securing servers and ensure that authoritative nameserver infrastructure is protected.
2) ISPs should adopt applicable BCPs found in other relevant network security industry approved/adopted publications. Monitor for applicable documents and update. Five documents were identified that currently apply to protecting ISP networks: IETF RFC 4778 and BCP 46 (RFC 3013); NIST special publications series: NIST SP-800-53 and NIST SP-800-81; ISOC publication: *Towards Improving DNS Security, Stability, and Resiliency*
3) ISPs should review and apply BCPs for protecting network assets carefully to ensure they are appropriate to protect an authoritative DNS server.

5.2.4 ISP insiders modifying/tampering with ISP AUTH DNS servers

As articulated in section 5.1.3, while insider threats can be considered a subset of the more general security threat of unauthorized access and hacking, they deserve special attention in the realm of DNS security. Unlike the case of modifying recursive server entries, where data is usually entirely memory resident, modifying an AUTH nameserver would most likely require modifying of a configuration file and thus would be easier to detect in many cases. However, if an ISP is using a content distribution network (CDN) or some other dynamic system for propagating authoritative DNS answers, it may be more difficult to detect improper entries entered by an insider.

The analysis and recommendations for this particular threat do not differ substantively from those presented in Section 5.2.3 of this report - Hacking and unauthorized 3rd party access to ISP AUTH nameserver infrastructure. However, it is worth paying special attention to this particular exposure given the relative ease and difficult detection of such attacks, combined with the liabilities an ISP may be exposed to from such difficult-to-detect activities of its own employees.

5.2.4.1 Recommendations

Refer to section 5.2.3.1.

5.2.5 Hijacking of ISP's domain name(s)

In late May 2008, the U.S.'s largest ISP and its customers were heavily impacted by the hijacking of its primary domain name and hundreds of other domain names at its domain name registrar[24]. A trio of young hackers used social engineering and well-known structural vulnerabilities in the process and systems to manage domain names that most domain registrars are susceptible to in order to take over the ISP's domain management account. For several hours, the hackers moved the domains they had purloined to various servers to display a defacement page, denying ISP customers access to webmail and some voice services, and other services (like e-mail) dependent upon those domain names were down. Fortunately in this case, nothing more malicious was done, and the perpetrators were actually tracked down and successfully prosecuted.[25]

Unfortunately, domain name hijacking is not a rare event; many of the largest web properties[26], brand names[27] and even the worldwide domain name coordinator itself (ICANN), have had their domain names taken over via social engineering, hacks or unauthorized use of accounts at domain registrars, and numerous hacks of domain registries. Such issues continue to this day[28] despite heightened awareness of this issue. In a typical domain name hijacking event, miscreants will change the DNS server entries that are published by the domain registry that are authoritative for that domain name. This causes lookups for those domains to go to authoritative nameservers that are typically under control of the miscreants, who use those servers to redirect hostnames, MX records, and modify configurations within the DNS. If the miscreant has control of the domain management account at the registrar, they will often update the domain ownership data, and can even initiate a transfer of the domain name to another registrar. These techniques make it much more difficult to re-assert control of the hijacked domain name and can extend the take-over significantly.

Such attacks have been largely mischief-making to-date, with defacement sites published. However, in one far-reaching case in late 2008, a major backend provider of financial services domain was hijacked to redirect banking customers to a malware drop site[29], exposing the major risks to Internet users such attacks can create.

The net effect of a domain hijacking is largely the same as other attacks against authoritative infrastructure as covered in section 5.2.3. ISPs will want to consult BCPs covering techniques for monitoring and reacting to those types of attacks. These BCPs cover the general effects of a domain name hijacking – dealing with service interruptions and the worldwide caching of incorrect DNS data. Unlike an event at an authoritative nameserver, ISPs do not have direct access or control to domain registrar or registry information that has been compromised in most hijacking attacks. The ISP is dependent upon the affected registrar or registry to restore control of the ISP's management account, or in the case of a serious breach, the registrar/registry's own services. Once control is re-established, the original, correct information needs to be re-entered

[24] http://www.domainnamenews.com/legal-issues/3-charged-comcastnet-hijacking-network-solutions/6649
[25] http://www.bizjournals.com/philadelphia/stories/2010/09/20/daily44.html
[26] http://domainnamewire.com/2010/02/24/how-baidu-got-hacked-by-the-iranian-cyber-army/
[27] http://www.guardian.co.uk/technology/2009/dec/18/twitter-hijacked
[28] http://www.zdnet.com/blog/networking/dns-hack-attack-mutilates-multiple-web-sites/1423
[29] http://voices.washingtonpost.com/securityfix/2008/12/hackers_hijacked_large_e-bill.html

and published again. This will usually mean updating nameserver entries and fixing any account information that has been modified.

The domain name industry has largely been slow to adopt security measures to protect account access that are found in other online services like financial services, e-commerce, or even some ISP management systems. The industry also has hundreds of participants with a wide variety of business models, with few standards and requirements for the security of registration systems, and very limited oversight. This means it is often difficult to find support for typical online security tools like multi-factor authentication, multi-channel authentication, and verification of high-value transactions (changing nameservers in the case of a domain name).

ICANN's Security and Stability Advisory Committee (SSAC) has released two documents to address these issues and provide BCPs for avoiding and mitigating these issues. SAC 40 *Measures to Protect Domain Registration Services Against Exploitation or Misuse*[30], addresses issues faced by domain name registrars and offers numerous BCPs and recommendations for securing a registrar against the techniques being used by domain name hijackers. SSAC 44, *A Registrant's Guide to Protecting Domain Name Registration Accounts*[31], provides advice to domain name registrants to put in place to better protect their domains from hijacking. Unfortunately, there has not been widespread adoption of these recommendations by domain registrars to date, so ISPs need to carefully evaluate their security posture and the offerings of their domain registrar with these BCPs in mind.

5.2.5.1 Recommendations

1) ISPs should refer to and implement the BCPs and recommendations found in SSAC 44 *A Registrant's Guide to Protecting Domain Name Registration Accounts* with respect to managing the domain names they register and use to provide services.

5.3 Attacks against and issues with the authoritative/provisioning DNS Infrastructure that ISPs provide to their customers

ISP customers will often turn to their ISP for provisioning of their own domain names and authoritative DNS services. This is a primary service area for a majority of ISPs, so provisioning of domain names and DNS services is often considered a core service for ISPs. There are two primary roles that the ISP fills when supporting the publication of DNS data for customers. First, the ISP can act as the authoritative DNS service provider for their customers, so customers would utilize authoritative DNS server services provided by the ISP to publish zone information for domain names they have registered. The second primary ISP role in this area would be acting as a domain name registration service provider for their customers. In this scenario, customers register and manage their domain name registration settings via services provided by their ISP.

An ISP has two basic options to provide authoritative DNS for its customers. First an ISP can utilize its own DNS server infrastructure, in which case their customers rely on the ISP for provisioning and management of DNS servers either via a manual process or some sort of

[30] http://www.icann.org/en/groups/ssac/documents/sac-040-en.pdf
[31] http://www.icann.org/en/committees/security/sac044.pdf

customer-facing portal. Alternatively, many ISPs provide authoritative DNS services for its customers by providing access to a 3rd party's DNS services and server infrastructure. Customers typically rely on this 3rd party service for provision and management of DNS servers for customers' DNS infrastructure. Depending upon the implementation, customers may also rely on the ISP for access to this service.

Assuming this role means that an ISP takes on all the risks an authoritative DNS operator faces for its own domains. This is much like the situation involving the ISP's own domains as described in section 5.2 of this report. Interruption or interference with the provisioning of such domains on the ISP's authoritative DNS infrastructure can in turn threaten the ability for the ISP's customers to utilize the Internet, and for third parties to reach the domain names of affected customers for various services, e.g. website, e-mail, file transfer, and telephony. Depending upon the risk, whether a failure of service from a lack of resiliency or DDoS attack, or a corruption of data provided by authoritative servers, the ISP needs to follow a variety of BCPs to prioritize and mitigate those risks.

ISPs often act as a domain name registrar or reseller of domain registration services to its customers. Customers register and manage their domain name registration settings via services provided by the ISP. Some ISPs actually go through the process to become accredited registrars of domain name services, including contracting with ICANN and some number of gTLD registries, and with ccTLD (country code TLD) registries to provide country-specific domains. Most ISPs provide domain registrations as a domain name reseller of a particular domain name registrar, reselling that registrar's services either via the registrar's website or dedicated portal, or some back-end systems that tie an ISP's customer-facing systems to the registrar's. Offering domain registration services opens an ISP to the same risks inherent to organizations within the domain registration industry. This is particularly critical if the ISP acts as an accredited registrar, as this introduces more attack surfaces and responsibilities. Interruption or interference with the provisioning of customers' domains within a domain registration system provided by an ISP can in turn threaten the ability for an ISP's customers to utilize the Internet. Thus it becomes incumbent upon ISPs offering domain registration services to recognize all the risks involved in this unique industry, and adopt BCPs to protect against them.

5.3.1 Hacking and unauthorized 3rd party access to ISP AUTH DNS servers provided for customers' DNS

As articulated by section 5.1.2 and 5.2.3, hacking and unauthorized access to any ISP infrastructure is an ever-present threat. The analysis and recommendations articulated in section 5.2.3 covering hacking and unauthorized third party access to an ISP's own nameservers apply in large-part to authoritative nameservers provisioned for customer use as well, and should be reviewed for further information on the generic problem.

The same issues that make protection of an ISP's authoritative nameserver infrastructure a challenge apply to servers that provision customer domains. Review section 5.2.3 for further analysis of these risks.

In the case of authoritative servers that supply customer domain DNS services, these are typically shared resources for many customers. This increases risk, since a single customer targeted to hijack, interrupt, or corrupt their DNS can lead to multiple customers being affected, and this has been seen in many hacking attacks in the past. If the ISP includes DNS resolution

for the ISP's own domains, then that risk is also borne by the ISP's own DNS operations. Many ISPs partition these risks by running their own authoritative DNS infrastructure on separate servers or services from their customers' authoritative DNS. Further partitioning can be performed to separate classes of customers, often based on desired service levels, but risk considerations can drive these deployment plans as well. At the very least, an ISP should be aware of these risks and create a posture that meets their operational security needs for themselves and their customers.

5.3.1.1 Recommendations

1) ISPs should refer to and implement the BCPs found in CSRIC 2A – Cyber Security Best Practices that apply to securing servers and ensure that authoritative nameserver infrastructure is protected.
2) ISPs should adopt applicable BCPs found in other relevant network security industry approved/adopted publications. Monitor for applicable documents and update. Five documents were identified that currently apply to protecting ISP networks: IETF RFC 4778 and BCP 46 (RFC 3013); NIST special publications series: NIST SP-800-53 and NIST SP-800-81; ISOC publication: *Towards Improving DNS Security, Stability, and Resiliency*
3) ISPs should review and apply BCPs for protecting network assets carefully to ensure they are appropriate to protect an authoritative DNS server.
4) ISPs should be aware of the risks of providing authoritative nameserver services for numerous customer domains as well as commingling authoritative DNS services for the ISP itself with customer authoritative services, and mitigate these accordingly.

5.3.2 Hacking and unauthorized 3rd party access to DNS and domain management systems ISPs provide to customers

As articulated by section 5.1.2 and 5.2.3, hacking and unauthorized access to any ISP infrastructure is an ever-present threat. The analysis and recommendations articulated in section 5.2.3 covering hacking and unauthorized third party access to an ISP's own nameservers apply in large-part to the management systems for authoritative DNS and domain name management that are provisioned for customer use as well, and should be reviewed for further information on the generic problem.

Beyond the "generic" hacking issues, the domain and DNS management systems that ISPs offer their customers for managing various levels of their infrastructure are tempting targets for miscreants looking to hijack particular domain names or compromise a particular target. So an ISP takes on the responsibility of helping secure any of their customers' Internet presence when they assume the role of domain name or DNS manager for them. Unfortunately, detection and prevention of customer-owned domains being modified via a management interface can be very difficult since an ISP would often not be aware of what changes a customer may want to put in-place for their domains. This is especially difficult when the customers themselves have been compromised in some way, or if the staff of a registrar has been tricked via a social engineering scam.

For management of authoritative servers, the analysis and recommendations found in section 5.3.1 apply here, with the target being an exposed management system rather than just the authoritative DNS servers themselves. The analysis and consequences detailed in section 5.2.5

of a domain name hijacking apply in the instance of a domain name management system compromise, except these will affect a customer directly, and not necessarily an ISP's operations. So in this regard, the ISP is effectively taking on the role of a domain name registrar, whether or not they are actually an accredited registrar or a reseller of registration services. This introduces a different risk profile, but one that is well covered in SAC 40 *Measures to Protect Domain Registration Services Against Exploitation or Misuse*[32], which addresses issues faced by domain name registrars and offers numerous BCPs and recommendations for securing a registrar against the techniques being used by domain name hijackers.

Threats that ISPs will see in this space are diverse, as there are numerous methods to gain access to systems or accounts on those systems that miscreants use to hijack domains. The following list was a representative list derived from the SAC 40 report:

1. *All an attacker needs to gain control of an organization's entire domain name portfolio (and to hamper authorized access to that portfolio) is a user account name and password.*
2. *Attackers need only guess, phish, or apply social engineering techniques on a single point of contact to gain control of a domain registration account.* [CSRIC III WG4 also notes that key-logging malware can also be used to get this information from any user with access to an account or system].
3. *Attackers scan domain account registration and administration portals for web application vulnerabilities (e.g., SQL injection). A successful exploit of vulnerable application code can result in the disclosure of account credentials for many domain accounts.*
4. *Email is the preferred and often the only method by which some registrars attempt to notify a registrant of account activity.*
5. *Attackers can block delivery of email notifications to targeted registrants by altering DNS configuration information so that email notifications will not be to any recipient in the domains the attacker controls through a compromised account (e.g., registrant's identified administrative or technical contact email addresses hosted in the domain).*
6. *Access to and the ability to modify contact and DNS configuration information for all the domains in a registration account is commonly granted through a single user account and password.*

Such attacks can target an ISP customer, who has an account directly, or the staff and systems of the ISP itself.

Note that many ISPs outsource DNS management and/or domain name registration functions for their customers, and do not provide actual services, other than perhaps unified billing, so the actual security and operational risks would be born by that third party service. In this case, the ISP would need to evaluate any outsourced provider to see that they are following the recommended BCPs identified for handling these risks. In this situation, managing these risks becomes a vendor management issue, so ISPs should look towards BCPs in that space, which is outside the scope of this working group.

[32] http://www.icann.org/en/groups/ssac/documents/sac-040-en.pdf

5.3.2.1 Recommendations

1) To protect exposed DNS or domain name management systems, ISPs should refer to and implement the BCPs found in CSRIC 2A – Cyber Security Best Practices that apply to securing servers and ensure that authoritative nameserver infrastructure is protected.
2) To protect exposed DNS or domain name management systems, ISPs should adopt applicable BCPs found in other relevant network security industry approved/adopted publications. Monitor for applicable documents and update. Five documents were identified that currently apply to protecting ISP networks: IETF RFC 4778 and BCP 46 (RFC 3013); NIST special publications series: NIST SP-800-53 and NIST SP-800-81; ISOC publication: *Towards Improving DNS Security, Stability, and Resiliency*
3) ISPs should refer to and implement the BCPs and recommendations found in SAC 40 *Measures to Protect Domain Registration Services Against Exploitation or Misuse* with respect to providing domain registration and management services directly to customers.

5.3.3 Social engineering of ISP staff to obtain control to DNS and domain management systems

This risk area is clearly a subset of section 5.3.2. However, members of the working group familiar with the history of domain name hijacking felt it important to highlight this issue in particular. As described in section 5.2.5, domain name hijacking remains popular and can have devastating consequences. A favorite tactic of hijackers is to use social engineering techniques against staff members of registrars to get them to transfer control of domain name accounts. If an ISP is fulfilling the role of registrar or domain name reseller for a large number or particular set of high-value customers, this is very likely to happen at some point to their own support staff. It is thus important to be aware of this issue and have practices in-place to deal with them.

5.3.3.1 Recommendations

1) ISPs should refer to and implement the BCPs and recommendations found in SAC 40 *Measures to Protect Domain Registration Services Against Exploitation or Misuse* with respect to providing domain registration and management services directly to customers.

5.3.4 ISP insiders modifying/tampering with AUTH DNS servers provided for customer's DNS

As articulated in section 5.1.3, while insider threats can be considered a subset of the more general security threat of unauthorized access and hacking, they deserve special attention in the realm of DNS security. Unlike the case of modifying recursive server entries, where data is usually entirely memory resident, modifying an AUTH nameserver would most likely require modifying a configuration file and thus would be easier to detect in many cases. In the case of customer-owned domains this may prove more difficult, since an ISP would often not be aware of what changes a customer may want to put in-place for their domains. So ensuring a match between the published entries in the AUTH nameserver and the customer domain management account becomes an important test for security against this threat as well as to provide service accuracy. If an ISP is using a CDN or some other dynamic system for propagating authoritative DNS answers for its customers, it may be more difficult to detect improper entries entered by an insider as well.

The analysis and recommendations for this particular threat do not differ from those presented in Section 5.3.1 of this report - Hacking and unauthorized 3rd party access to ISP AUTH DNS servers provided for customers' DNS. However, it is worth paying special attention to this particular exposure given the relative ease and difficult detection of such attacks, combined with the liabilities an ISP may be exposed to from the activities of its own employees.

5.3.4.1 Recommendations

Refer to section 5.3.1 of this report.

5.3.5 ISP insiders modifying/tampering with customer DNS/domain management accounts

As articulated in section 5.1.3, while insider threats can be considered a subset of the more general security threat of unauthorized access and hacking, they deserve special attention in the realm of DNS security. Detection and prevention of customer-owned domains being modified via a management interface is extremely difficult since an ISP would often not be aware of what changes a customer may want to put in-place for their domains.

For management of customer authoritative nameservers accounts, the analysis and recommendations for this particular threat do not differ significantly from those presented in Section 5.3.1 of this report - Hacking and unauthorized 3rd party access to ISP AUTH DNS servers provided for customers' DNS. However, if domain name registration services are being provided to customers, then practices described in SAC 40 come into play to help mitigate issues. In particular, use of multi-factor authentication to manage domain name changes can thwart insiders who don't have access to the authentication system, but do have access to the account being targeted.

Again, it is worth paying special attention to this particular exposure given the relative ease and difficulty of detecting such attacks, combined with the liabilities an ISP may be exposed to from the activities of its own employees.

5.3.5.1 Recommendations

1) For the generic insider threat, refer to section 5.3.1 of this report.
2) ISPs should refer to and implement the BCPs and recommendations found in SAC 40 *Measures to Protect Domain Registration Services Against Exploitation or Misuse* with respect to providing domain registration and management services directly to customers.

5.3.6 Resiliency of ISP AUTH nameservers provided for customer DNS

As described in sections 5.2.2 and 5.1.4, DNS is by its nature distributed and highly resilient; however, ISPs can take several different measures to make it even more resilient to configuration errors, attacks, and service interruptions. Additional analysis on general tactics for increasing the resiliency of DNS services in general can be found in those sections.

On the authoritative side of the DNS resiliency equation, the areas of particular interest for ISPs encompass a variety of practices as described in section 5.2.2. The discussion of "hidden

master" nameservers in 5.2.1 and 5.2.2 is particularly germane in the case of increasing resiliency in the face of diverse and ever-changing customer requirements for authoritative DNS services.

As outlined in section 5.3.1, in the case of authoritative servers that supply customer domain DNS services, these are typically shared resources for many customers. This increases risk to the ISP given the variety of different configurations and needs of a diverse customer base. It is harder to predict overall resource demands for large numbers of customers whose needs may dramatically change overnight, or come under some sort of attack. If the ISP includes DNS resolution for the ISP's own domains on the same servers, then that risk is also borne by the ISP's own DNS operations. As mentioned in 5.3.1, partitioning of DNS services based on risks and other operational needs can help reduce shared risks, and overall risk to the ISP for unanticipated factors that could lead to an outage in DNS services. The more diverse the customer base, the greater the need to overprovision and use BCPs to maintain performance and delivery of authoritative DNS services for customers. Because of the unpredictable nature of customer DNS demands, ISPs will often outsource authoritative DNS services provided to its customers to a DNS service provider that can provide economies of scale that the ISP simply cannot afford to put in place. If not completely outsourced, provisioning of secondary servers that are public-facing and listed as authoritative for customer domains (and even ISP domains) is a common tactic to provide additional capacity, improved response time, and network/geographical diversity for authoritative DNS. This can be done with public-facing authoritative servers or "hidden masters" as previously discussed.

NIST SP-800-81 *Secure Domain Name System (DNS) Deployment Guide*[33] addresses a wide variety of issues specific to running DNS servers in government environments. It is also highly relevant to ISPs as the BCPs and advice it provides largely apply to any organization running DNS infrastructures for large numbers of clients – particularly in provisioning authoritative servers. Many of the recommendations within this document deal directly with the resiliency of the DNS in environments of similar size and risk profiles as many ISPs.

As mentioned in section 5.1.2, the Internet Society (ISOC) has recently published a comprehensive document that addresses a wide variety of DNS risks and recommended BCPs and strategies to address them: *Towards Improving DNS Security, Stability, and Resiliency*[34]. This paper provides an excellent background on threats to and from the DNS, including improving resiliency of DNS operations. The included survey of relevant RFCs and practices to mitigate them and is a solid reference for any ISP looking to identify and avoid DNS risks.

5.3.6.1 Recommendations

1) ISPs should be aware of their current and anticipated operational resiliency for authoritative DNS service and be prepared to provision according to these needs guided by industry-accepted BCPs.
2) ISPs should refer to and implement the BCPs relating to resiliency of DNS infrastructure found in CSRIC 2A – Cyber Security Best Practices that apply to the resiliency of recursive nameserver infrastructure.
3) ISPs should adopt applicable BCPs found in other relevant network security industry

[33] http://csrc.nist.gov/publications/PubsSPs.html
[34] http://www.internetsociety.org/sites/default/files/bp-dnsresiliency-201201-en_0.pdf

approved/adopted publications. Monitor for applicable documents and update. Two were identified that currently apply to improving the resiliency of authoritative nameservers in ISP networks: NIST SP-800-81 and the ISOC publication: *Towards Improving DNS Security, Stability, and Resiliency.*

5.3.7 Resiliency of domain management systems provided for customer DNS/domains

Resiliency of customer-facing management interfaces and services while important for most organizations, including ISPs, is not as critical as resiliency of core services like network access, e-mail or DNS service itself. Help desk personnel can typically cover functionality provided by management UIs if there is a system outage or other issue. Further, since DNS changes or need for customer access are fairly infrequent in comparison to other services, resiliency concerns for availability and accessibility aren't a major security or operational imperative if ISP personnel are available to cover. This issue falls under customer support and contractual concerns as drivers of any risk assessment. That being stated, it is still important to provide access to services that customers contracted for at a very high level. Therefore looking to BCPs that provide guidance on making all customer-facing services resilient would be places to turn to when questions arise or plans are made.

5.3.7.1 Recommendations

1) ISPs should refer to and implement the BCPs relating to resiliency of customer-facing controls for services found in CSRIC 2A – Cyber Security Best Practices that apply to the resiliency of recursive nameserver infrastructure.

5.3.8 Denial-of-Service Attacks of authoritative DNS servers and domain management systems provided for customer DNS/domains

As articulated by section 5.2.1, DoS/DDoS attacks against ISP infrastructure are some of the most prevalent and damaging incidents that are seen in ISP operations. The analysis and recommendations articulated in section 5.2.1 covering DoS/DDoS against an ISP's own authoritative nameservers apply in large-part to DoS/DDoS incidents involving authoritative nameservers supplied for customers and should be reviewed for further information on the generic problem.

For the case of DoS/DDoS against domain name and DNS services management platforms supplied by an ISP to its customers, standard DoS/DDoS advice as already articulated still applies. However, loss of access to these systems typically isn't as critical as loss of actual DNS services, as the two systems are typically separate. Also, the lack of a management interface for domain registration and zone data information only affects customers' ability to change settings or provision new domains and typically isn't time sensitive. There usually are no further repercussions to such attacks, unlike the loss of DNS services themselves. Further, if there are time-sensitive changes that need to be made during a service outage for the management platform, whether caused by a DoS attack or not, service personnel at an ISP can typically access the appropriate services (a domain registrar or DNS server) manually to make the needed changes. A long-term DoS/DDoS attack on such assets certainly would create additional strains on an ISP's customer service and reputation, but such a scenario is unlikely without it being a

much wider-impacting event.

5.3.8.1 Recommendations

1) ISPs should implement BCPs and recommendations for securing an ISP's infrastructure against DoS/DDoS attacks that are enumerated in the IETF's RFC 4732 *Internet Denial-of-Service Considerations* and consider implementing BCPs enumerated in the SANS Institute reference document of BCPs against DoS/DDoS attacks entitled *A Summary of DoS/DDoS Prevention, Monitoring and Mitigation Techniques in a Service Provider Environment*.
2) ISPs should refer to and implement the BCPs related to DoS/DDoS protection found in CSRIC 2A – Cyber Security Best Practices that apply to protecting servers from DoS/DDoS attacks.
3) ISPs should consider adopting BCPs found in other relevant network security industry approved/adopted publications that pertain to DoS/DDoS issues, and monitor for applicable documents and updates. Four documents that currently apply to protecting ISP networks from DoS/DDoS threats are IETF RFC 4778 and BCP 46 (RFC 3013); NIST special publications series: NIST SP-800-53; and ISOC Publication *Towards Improving DNS Security, Stability, and Resiliency*.
4) ISPs should review and apply BCPs for protecting network assets carefully to ensure they are appropriate to protect an authoritative DNS server.

5.4 Abuse of an ISP's DNS infrastructure to attack others or issues with an ISP's infrastructure that affect 3rd parties

Attackers often abuse the universal accessibility of an ISP's DNS infrastructure to launch attacks against victims. Those victims may or may not be located on the ISP's network or customer base, so ISPs may need to be vigilant to misuse of their DNS infrastructure that affect others. The Working Group identified two such attacks that merited reporting.

Reflective DNS Amplification Distributed Denial of Service (DDoS) attacks enable an attacker to flood a victim with overwhelming waves of data by "reflecting" DNS requests off open recursive DNS servers. The attacks are particularly devastating, as the use of legitimate recursive servers to both amplify (send much larger packets) and reflect towards a victim from legitimate IP space makes it difficult to mitigate from the victim's perspective. This has been one of the most prevalent and devastating methods for launching DDoS attacks for many years now, and continue to plague the Internet.

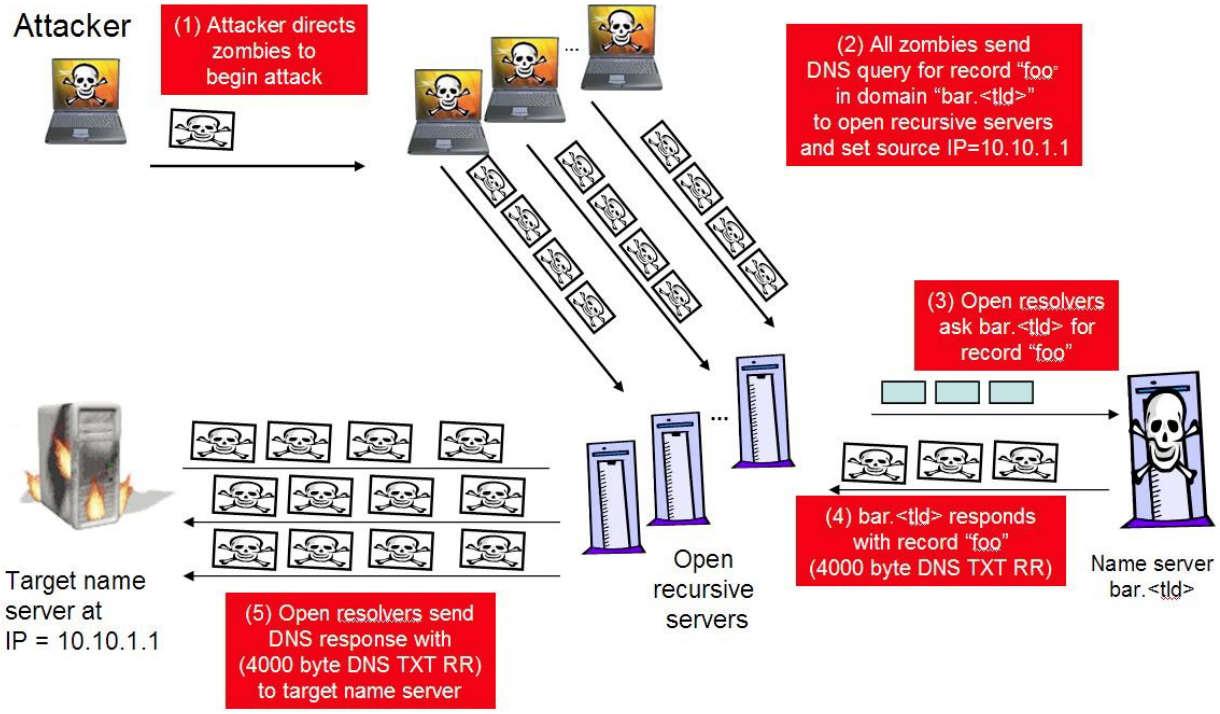
A newly discovered technique allows creators of malicious domains to prolong their lifetimes well past deletion from the authoritative zone. Attackers are able to surreptitiously refresh their entries in the targeted recursive name servers by taking advantage of DNS caching rules, which in turn mean victims' DNS queries still resolve to these "ghost domains" indefinitely.

5.4.1 Reflective DNS Amplification DDoS

In a Reflective Amplification DDoS an attacker uses a botnet to send an overwhelming amount of UDP DNS queries to open resolvers – recursive DNS servers that respond to all requests, to include queries from outside their own network. The source IP of these queries spoofs the victim's IP address. The queries trigger a flood of UDP large responses that are reflected to the

victim. A successful attack requires numerous DNS recursive name servers that will respond to the spoofed queries, a valid domain name on each server with a large text record, and a DNS query with the spoofed source IP address of the victim.

Such an attack is described as an amplification attack because the response is always larger than the request. Initial DNS implementations supported responses up to 512 bytes. Extension Mechanisms for DNS (EDNS), as described in RFC 2671, expand the possible size of supported UDP responses to 4000 bytes; DNS responses greater than 4000 bytes use TCP. UDP responses are preferred by attackers because it is easier to spoof UDP source IP addresses. DNSSEC requires EDNS, which means that all DNSSEC-compliant name servers are capable of replying with 4000-byte UDP responses in support of Reflective DNS Amplification DDoS attacks.



Source: SAC 008

The two key vectors needed to support these attacks (besides a large botnet) are a large number of open recursive servers and a lack of IP source validation on the networks those servers are located on. This allows an attacker to blast traffic with impunity at their target victim. Since the DNS resolvers used in the attack are legitimate, the victims cannot block them without denying service to the users that rely on those servers.

Numerous industry documents spell out specific solutions to these problems and have been in publication for over a decade. Most major ISPs are reported to have implemented many of the recommended solutions, but the continued use of this attack methodology implies that many more ISPs have yet to implement adequate protections against these attacks. The following documents provide information about the issues discussed here, as well as BCPs for dealing with them:

1) BCP 38/RFC 2827 *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*[35]
2) BCP 84/RFC 3704 *Ingress Filtering for Multihomed Networks*[36]
3) BCP 140/RFC 5358 *Preventing Use of Recursive Nameservers in Reflector Attacks*[37]
4) SAC 004 – *Securing the Edge*[38]
5) SAC 008 – *DNS Distributed Denial of Service (DDoS) Attacks*[39]

The primary recommendations from all of these documents boil down to these two points:

1) Do not allow open recursive DNS servers if possible.
2) Employ ingress filtering on your network to defeat IP spoofing.

5.4.1.1 Recommendations

1) ISPs should implement BCPs and recommendations for securing an ISP's recursive DNS infrastructure against Reflective DNS Amplification DDoS attacks that are enumerated in the following documents:
   a. BCP 38/RFC 2827 *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*
   b. BCP 84/RFC 3704 *Ingress Filtering for Multihomed Networks*
   c. BCP 140/RFC 5358 *Preventing Use of Recursive Nameservers in Reflector Attacks*
   d. SAC 004 – *Securing the Edge*
   e. SAC 008 - *DNS Distributed Denial of Service (DDoS) Attacks*

5.4.2 Ghost Domains

In February 2012, a new, quite effective technique for maintaining a suspended domain that has been removed from its TLD zone was discovered. Such an attack has been given the moniker of a "ghost domain".[40] An attacker can easily set up a legitimate domain (e.g. hacker.com) and control the domain's authoritative name server. The attacker will then submit DNS queries for www.hacker.com through several recursive name servers (which their botnets can query successfully from any ISP or network they reside), forcing the DNS servers to resolve www.hacker.com and cache the results, including nameserver information for that domain, and the IP address (controlled by the attacker) for the nameservers. Once hacker.com is identified as a malicious domain, remediation action will occur that will lead to the top-level domain registry (for .com in this example) removing hacker.com from their zone file. However, the recursive name servers will not query the top-level domain authoritative server (and subsequently remove hacker.com from their own records) until their cached TTLs for hacker.com and its authoritative nameservers expire. Consequently, by querying each targeted recursive name server regularly for new hostnames under hacker.com, those recursive nameservers will query the cached authority nameservers for the domain, which remains cached. The attacker will refresh the

[35] http://tools.ietf.org/html/bcp38
[36] http://tools.ietf.org/html/bcp84
[37] http://tools.ietf.org/html/bcp140
[38] http://www.icann.org/en/groups/ssac/documents/sac-004-en.pdf
[39] http://www.icann.org/en/groups/ssac/dns-ddos-advisory-31mar06-en.pdf
[40] http://*www.isc.org/files/imce/**ghostdomain**_camera.pdf*

delegation data in recursive servers' caches and include an update to the TTLs for the nameservers of hacker.com in the answer, which the targeted resolvers will update, and thus ensure they continue to resolve the malicious domain. The domain hacker.com then is known as a ghost domain because it is revoked yet still resolvable due to cached delegation data records in recursive name server caches.

This is a recently discovered attack vector, so no industry BCPs have been published to address it. Not all recursive server implementations are susceptible to these attacks, and periodic flushing of a DNS resolver's entire cache would mitigate long-lasting ghost domains.

5.4.2.1 Recommendations

1) With a lack of current BCPs in this area, ISPs should be aware of this potential attack and consider periodically flushing DNS cache to remove ghost domains. ISPs may also want to consider investigating a DNS implementation that is immune to the ghost domain attack[41].

5.5 Subscribers of ISPs with DNS issues at their premise

In the past year, the wide coverage of the DNS Changer virus/attacks and the work of the DNS Changer Working Group[42] have brought the somewhat obscure issue of attacks on DNS at the "edge" to the forefront. ISP customers having problems with DNS settings on their computers or routers or other odd stuff they do is nothing new to ISPs. However, with criminals making concerted attacks to subvert the DNS services provided by ISPs on customers' computers and networks, this has become an area to pay more attention to. Further, the recent, rapid rise of commercial/competing recursive DNS service providers like Google DNS and OpenDNS that have gained wide market share provide operational challenges to ISPs and create potential security concerns to be managed. This is especially the case when those alternative DNS services come pre-bundled in home routers that ISP customers could be installing on networks serviced by ISPs.

5.5.1 Attacks and issues that interfere with stub resolver/premise router integrity

ISP customers are typically free to choose any DNS resolvers they wish to use for DNS resolution services. This presents a convenient angle of attack for miscreants, as they know that they can use various techniques to subvert the DNS resolution path of victims, and ISPs will not be aware nor able to respond in many cases to a customer being redirected in this manner.

The DNS Changer case is a particularly good illustration of the various techniques criminals may utilize in order to subvert and eventually control DNS resolution of end users. Over the many years the people behind DNS Changer were growing their network of victims, they employed a wide range of tactics, with the most prolific being various flavors of malware that altered default DNS resolver settings on victim PCs. This took the form of classic virus infections, but also "fake anti-virus" products victims would willingly install on their machines. Other attack techniques included scanning for home routers on public IP space and trying default passwords, or brute-forcing access to the routers. It is also believed that some home routers were hacked into via known vulnerabilities. Once on the router, the miscreants

[41] Jiang, et al (2012), *Ghost Domain Names: Revoked Yet Still Resolvable*
[42] http://www.dcwg.org

reconfigured their upstream DNS resolution to use DNS Changer resolvers instead of the default ISP resolvers[43]. This is not the first or last case of similar malware and hacking attacks likely to be seen.

With control of premise or local DNS resolution, a miscreant can inject any answers they want into queries to popular or sensitive domain names. This is akin to a massive, persistent cache poisoning attack, but at a very local level, and it comes with all the attendant problems described in section 5.1 and elsewhere in this document. The DNS Changer case exposed another risk to ISPs; if attacks are large enough, shutting them down could cause a major operational impact for ISPs and a loss of Internet service for affected customers. Once the bogus resolvers were shut down, victims would no longer be able to resolve any DNS queries, effectively knocking them off the Internet for most functions. This would in-turn cause ISP customers to contact their ISP's help desk and then go through the process of identification of the problem (connection is OK, but no DNS) and clean-up of the problem at the customer's location. In the case of DNS Changer, the scale of infections was thought to be in the millions, and could have created a nightmare for ISPs' customer service operations that may have taken days or weeks to work through, exacerbating the victims' plight. So as part of the arrest of the alleged perpetrators and shut-down of their network, alternative "clean" DNS resolvers were set up to provide continued DNS resolution to victims. The hope was to provide feedback to infected users via their ISPs to get them to fix their computers and routers before they lost DNS service once the network was shut down. Several tactics were used by some ISPs like walled gardens and internal rerouting of the IP space for the DNS Changer DNS servers. No consensus BCPs have emerged from this recently concluded effort, but many lessons were learned that might lead to new ones soon.

5.5.1.1 Recommendations

1) ISPs should be aware of the risks of this type of attack/issue and consider contingency plans for handling them.
2) ISPs would be well served to stay abreast of developments around the DNS Changer case and the DNS Changer Working Group, and look to implement BCPs that are identified as a result.

5.5.2 ISP customer use of alternative DNS providers

In recent years, several companies and organizations have started offering alternative DNS resolution services. These are being offered with various claimed benefits from performance to safety and in a variety of business models. These are not typically a security issue for ISPs, as the major providers of such services run very robust, secure systems. However, there are operational impacts on ISPs when customers experience problems with those services. For example, there may be a service delivery issue (DDoS or systems failure) or a domain name being black listed by an alternative DNS provider that causes customers to believe their ISP is having issues or censoring their Internet connections. These problems can be difficult for an ISP help desk to track down, especially since customers may not remember changing their DNS settings. This becomes an even more difficult issue to diagnose when an ISP customer has installed a premise router that uses an alternative DNS provider by default. Such bundling may

[43] http://voices.washingtonpost.com/securityfix/2008/06/malware_silently_alters_wirele_1.html

turn into a trend[44]. In such cases the customer may not be aware of such settings, not understand the issue, and not know how to update the router to use an ISP's resolvers if they decide they'd prefer them.

Another concern in this space is the potential for malicious or shady actors to develop alternative DNS resolver services and create another DNS Changer type network, or engage in behavior that, while legal, the customer may not approve of. It is difficult for an ISP to stay aware of the reputation of all the various alternative DNS providers in the market; but it may be wise to understand how customers are utilizing DNS resolution services on the network so, if alerted to a rogue network like DNS Changer, they can take steps to prevent operational issues and/or notify users.

5.5.2.1 Recommendations

1) ISPs should be aware of the impacts of alternative DNS resolution services may have on their support operations.
2) ISPs would be well-served to stay abreast of developments in the alternate DNS resolution services space, and should consider planning for handling rogue provider risks.

5.6 Hygiene and other issues touching on DNS security

The working group identified several issues that didn't fall neatly into the previous categories but deserved mentioning in this paper, along with any recommendations for BCPs that we could identify. Some of these are minor points, but others are larger issues that may spur further discussion and work for future work groups.

5.6.1 Insecure zone transfers and updates

DNS Zone transfers and incremental updates are performed to replicate zone files in multiple servers to provide a degree of fault tolerance in the DNS service provided by an organization. If these are done in an insecure environment (e.g. over the public Internet), there is a chance for interception of data or attempts to inject bogus zone information, especially if an attacker can successfully spoof an originating server's IP address. Fortunately there is a mechanism called transactional signatures (TSIG) that is built into the DNS protocol to reduce these risks, and it is widely deployed as an operational standard. There are three IETF RFCs that introduce (RFC 2845 *Secret Key Transaction Authentication for DNS (TSIG)*[45]), expand upon the usage (RFC 3007 *Secure Domain Name System (DNS) Dynamic Update*[46]), and update (RFC 3645 *Generic Security Service Algorithm for Secret Key Transaction Authentication for DNS (GSS-TSIG)*[47]) this DNS resource record.

With TSIG, mutual identification of servers is based on a shared secret key. Because the number of servers involved in zone transfers is usually limited, a bilateral trust model that is based on a shared secret key may be adequate for most applications. TSIG specifies that the shared secret

[44] http://www.net-security.org/secworld.php?id=11338
[45] http://tools.ietf.org/html/rfc2845
[46] http://tools.ietf.org/html/rfc3007
[47] http://tools.ietf.org/html/rfc3645

key be used not only for mutual authentication but also for signing zone transfer requests and responses. Hence, it provides protection against tampering of zone transfer response messages[48]. NIST SP-800-81 *Secure Domain Name System (DNS) Deployment Guide*[49] provides operational BCPs for implementing TSIG to protect against several DNS security issues.

5.6.1.1 Recommendations

1) ISPs should implement BCPs and recommendations for securing DNS zone transfers and updates via TSIG as enumerated by the IETF's RFC 2845 *Secret Key Transaction Authentication for DNS (TSIG)*, RFC 3007 *Secure Domain Name System (DNS) Dynamic Update*, and RFC 3645 *Generic Security Service Algorithm for Secret Key Transaction Authentication for DNS (GSS-TSIG).*
2) ISPs should consider using the guidance provided in securing zone transfers and updates as articulated in NIST's special report, NIST SP-800-81.

5.6.2 NX-Redirect and synthesized DNS values used in-network for ISP subscribers

A practice that has become common at many ISPs is to redirect domains and hostnames that are non-existent to alternative existing destinations designated by the ISP or a service they use – NX-Redirect. This is often viewed as a way to improve user experience and often offers a revenue source for ISPs. This is typically targeted towards web browsing, as the redirect is designed to present a web surfer with alternatives to the domain they requested but does not exist.

There are some concerns with this practice, as it could create some security issues for subscribers. In particular, non-browser applications that rely on the NXDOMAIN error may attempt to connect to the redirect IP address, and, depending on the process, it could break or corrupt a process or even expose sensitive customer data. For example, people who shift between work and home, particularly if they use Windows server domains, may end up with processes that believe servers and services being requested (but which aren't actually present) are there, and reach out to the ISP-designated IP address for any myriad of requests. This will likely create a degradation of services, and, at worst, it could expose sensitive customer data to a third party server. E-mail services can also be impacted significantly if an expected "corporate" e-mail server isn't available, yet the client gets a synthesized IP address for that service. SSAC did a study of these issues in 2008 (SAC 032 *Preliminary Report on DNS Response Modification*) and it provides a good background of the issues involved.

The working group did not come to a consensus on BCPs to adopt in this space.

[48] NIST SP-800-81 *Secure Domain Name System (DNS) Deployment Guide*
[49] http://csrc.nist.gov/publications/PubsSPs.html

5.6.2.1 Recommendations

1) ISPs should be aware of the impacts of NX-Redirect and review the security issues raised by SAC 032.

5.6.3 Responding to external threats – major 3rd party domains/DNS events

As described in sections 5.2.5, 5.3.2 and 5.3.3, domain name hijackings are a potentially major security concern for ISPs. While those sections covered cases where the ISP itself is involved in the provisioning of a domain that gets hijacked and their direct affects. Another important consideration for ISPs is the hijacking of a prominent third party's domain name that could affect a large number of their customers. As detailed in section 5.2.5, such hijackings have already occurred, with several of the top brands and even financial institutions suffering from hijackings. This becomes the equivalent to a very large scale DNS cache poisoning attack in many respects because an ISP will cache the incorrect *intended* DNS resolution information for a domain name and present it to its customers when it receives the hijacked data that is functionally correct from the currently listed, but malicious authoritative servers. This then exposes an ISP's users and the ISP itself to potentially malicious Internet locations that were previously trusted. All the risks already enumerated in this report for cache poisoning and authoritative server compromises come into play once this happens. This is a policy problem that lies outside the standard DNS protocol, but a real security problem involving the DNS that would be good to address.

This problem space breaks down into two separate operational issues, neither of which has industry-accepted BCPs in place to address at this time that the working group could identify. The first goal is to prevent the caching of the bogus data for a hijacked domain. This would require either knowing that a hijacking is occurring and to then not expire old data, or not accepting data that some other source (e.g. a whitelist entry or reputation system) indicates is suspect. The second goal is to quickly purge bogus data from a cache and reload the actual DNS information as soon as the "real" authoritative data is being published by the legitimate nameservers. This would require some sort of notification system that is out-of-band of current DNS infrastructure, or else some sort of polling mechanism. Other solutions can certainly be envisioned as well.

One case of domain hijacking exemplifies these issues quite clearly, including a successful mitigation effort. In January 2010, baidu.com, the major Chinese search and auction site, and one of the largest properties on the Internet had its domain name hijacked. The primary A records were pointed to a hosting facility, where a defacement page was published. While the majority of the world resolved to that location during both the hijacking event and then the TTL of the bogus entry, most Chinese ISP users resolved to the correct site. Reports are that the Chinese government quickly organized an effort to have Chinese ISPs re-enter the correct entries for Baidu.com's domains in their caches with long TTLs while the hijacking was in progress. To be clear, Chinese government policies are certainly not being advocated as a model to emulate in this report. However the lessons learned here are still valuable and could form the basis of future work, since it is clear that remediation efforts like this can be accomplished.

Note that a malicious hijacking isn't the only cause for these issues. As previously discussed, a domain registrar, registry, or DNS operator for a domain may have some sort of corruption in

the data they publish that then leads to widespread caching of incorrect information. Typically this will result in a loss of service issue, as either the information is missing or pointing domains to resources that won't respond for them. However, the mitigation needed is essentially the same as a hijacking scenario.

5.6.3.1 Recommendations

1) With a lack of current BCPs in this area, ISPs should be aware of the impacts of hijackings of major brands and critical infrastructure domains and consider contingency plans for dealing with such events.

6 Conclusions

Working Group 4 has recommended the adoption of numerous best practices for protecting ISPs' DNS infrastructures and addressing risks related to the DNS continuously faced by ISPs. DNS remains a cornerstone service provided by ISPs for enabling their customers to use the Internet at all, as well as create and maintain their own Internet presences. As such, it is a critical service to ensure is resilient to operational challenges, and protected from abuse by miscreants. As a distributed infrastructure requiring several actors to both enable and protect it, ISPs face challenges outside of their direct control in tackling many of the issues identified. ISPs also should be taking measures to blunt the power of reflective DNS amplification DDoS attacks and the damage they can cause third parties.

7 Appendices

7.1 Appendix [1] – DNS Risks Matrix

DNS Security Risks Examined by WG 4

ISP Role	Risks	Report Sect.	Impacts
Recursive DNS server operator for customer base	DNS Cache poisoning attacks	5.1.1	Loss of service, Customers redirected to malicious locations for some domains
ISP provides DNS resolution services (DNS recursive resolvers) to its customers to enable them to utilize the DNS system and the Internet. This is a primary function of any ISP, but in many cases, customers may choose an alternative recursive DNS provider.	Hacking of ISP's recursive DNS servers	5.1.2	Loss of service, Customers redirected to malicious locations for some domains
	Insider threat at ISP - adds false entries for responses	5.1.3	Loss of service, Customers redirected to malicious locations for some domains
	Major 3rd party domain hijack/take-over/misconfigured	5.6.3	Loss of service, Customers redirected to malicious locations for some domains
	Resolvers used for reflective, DNS amplification DDoS attack (botnet on network)	5.4.1	Target domain/nameservers brought down, bandwidth impacted
	Resolvers used for reflective, DNS amplification DDoS attack (botnet anywhere)	5.4.1	Target domain/nameservers brought down, bandwidth impacted
	Rewriting of authoritative responses to other values	5.6.2	May break DNSSEC, inconsistent behavior for customers
	Rewriting of NX domain to synthesized values	5.6.2	May break DNSSEC, inconsistent behavior for customers
	Ghost domains - malicious	5.4.2	Customers continue to reach malicious domains after

	domains living indefinitely within resolvers' caches		they are mitigated
	Customer infected with virus that manipulates DNS (e.g. DNSChanger)	5.5.1	Customers redirected to malicious locations for some domains, major customer service issue if rogue DNS servers shut down
	Customer using router with alternative DNS servers as default	5.5.2	Service issues if customer experiences issues with third party recursive DNS service
	Insufficient resiliency of DNS infrastructure	5.1.4	Loss of service
Domain owner (ISP's own critical domains) *The ISP owns and maintains its own domains at one or more domain registrars. These domains are then utilized by customers for various services, e.g. connectivity, e-mail, web publishing.*	Hijacking of domain account at registrar or registrar reseller	5.2.5	ISP off-line, potential loss of company/customer data/customers offline
	Hacking of registrar/registry	5.2.5	ISP off-line, potential loss of company/customer data/customers offline
	Insider threat at registrar/registry	5.2.5	ISP off-line, potential loss of company/customer data/customers offline
	Unauthorized transfer of domain	5.2.5	ISP off-line, potential loss of company/customer data/customers offline
	Insider threat at ISP changing DNS entries	5.2.4	ISP off-line, potential loss of company/customer data/customers offline
Provider of domain registration services to customers *ISP acts as a domain name registrar or reseller of domain registration services to its customers. Customers manage their*	Hijacking of customer domain account at registrar or registrar reseller	5.3.2	Customer domain offline/redirected maliciously - customer and their users
	Hijacking of ISP reseller account at registrar	5.3.2	Many customer domains offline/redirected maliciously - customer and their users

domain names via services provided by the ISP.			
	Hacking of registrar/registry	5.3.2	Many customer domains offline/redirected maliciously - customer and their users
	Insider threat at registrar/registry	5.3.2	Many customer domains offline/redirected maliciously - customer and their users
	Unauthorized transfer of domain	5.3.2	Customer domain offline/redirected maliciously - customer and their users
	Hacking of ISP domain registration management system	5.3.2	Many customer domains offline/redirected maliciously - customer and their users
	Hijacking of customer domain account at ISP	5.3.2	Customer domain offline/redirected maliciously - customer and their users
	Insider threat at ISP	5.3.5	Many customer domains offline/redirected maliciously - customer and their users
	Insufficient resiliency of DNS infrastructure	5.2.2	Loss of service
Outsourced AUTH DNS services provider to customers	Hijacking of customer DNS management account at DNS provider	5.3.2	Customer domain offline/redirected maliciously - customer and their users
The ISP provides authoritative DNS services directly to customers by providing access to a 3rd party's DNS services and server infrastructure. Customers rely on this 3rd party service for provision and management of DNS servers for customers' DNS infrastructure. Depending upon implementation, customers may also rely on the ISP for access to this service.	Hacking of DNS provider	5.3.1	Many customer domains offline/redirected maliciously - customer and their users
	Insider threat at DNS provider	5.3.2	Many customer domains offline/redirected maliciously -

			customer and their users
	Hijacking of customer DNS management account at ISP	5.3.2	Customer domain offline/redirected maliciously - customer and their users
	Insider threat at ISP	5.3.4	Many customer domains offline/redirected maliciously - customer and their users
	Insufficient resiliency of DNS infrastructure	5.2.2	Loss of service
AUTH DNS server operator - ISP's domains	Hacking of DNS server	5.2.3	ISP off-line, potential loss of company/customer data/customers offline
The ISP provides authoritative DNS services directly for its own domains utilizing its own DNS server infrastructure. These domains are then utilized by customers for various services, e.g. connectivity, e-mail, web publishing.	Insider threat at ISP	5.2.4	ISP off-line, potential loss of company/customer data/customers offline
	Insecure zone transfers	5.6.1	Substitution of malicious data - customers redirected maliciously
	DDoS against DNS Server	5.2.1	ISP off-line, potential loss of company/customer data/customers offline
	Insufficient resiliency of DNS infrastructure	5.3.7	Loss of service
AUTH DNS server operator - customers' domains	Hacking of DNS server	5.3.1	Many customer domains offline/redirected maliciously - customer and their users
The ISP provides authoritative DNS services directly to customers utilizing it's own DNS sever infrastructure. Customers rely on the ISP for provision and management of DNS servers for customers' DNS infrastructure.	Hijacking of customer DNS management account at ISP	5.3.2	Customer domain offline/redirected maliciously - customer and their users

	Insider threat at ISP	5.3.4	Many customer domains offline/redirected maliciously - customer and their users
	Insecure zone transfers	5.6.1	Exposure of customer proprietary information, substitution of malicious data
	DDoS against DNS Server	5.3.8	Customer domain offline - customer and their users
	Insufficient resiliency of DNS infrastructure	5.3.7	Loss of service
Consumer of DNS from 3rd parties *ISP relies on 3rd party DNS service (authority or recursive) in its own role as a user of Internet services. It is reliant upon accuracy and veracity of information it obtains to provide internal operations and pass through services to customers.*	Important 3rd party domain hijack/take-over/misconfigure	5.6.3	Customers redirected to malicious locations for some domains
	Upstream cache poisoning	5.1.1	Customers redirected to malicious locations for some domains
	Upstream recursive server hack/insider threat	5.1.2	Customers redirected to malicious locations for some domains

7.2 Appendix [2] – BCP Document References

Recommendations for securing the DNS

NIST Special Publication 800-81r1 *Secure Domain Name System (DNS) Deployment Guide*

ISOC - *Towards Improving DNS Security, Stability, and Resiliency*

IETF BCP 16, RFC2182 *Selection and Operation of Secondary DNS Servers*

Network Protection Documents

WG2A - Cyber Security Best Practices

SANS: *Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines (CAG)*

NIST SP-800-53 *Recommended Security Controls for Federal Information Systems and Organizations*

IETF RFC 4778 - *Current Operational Security Practices in Internet Service Provider Environments*

IETF RFC 3013 *Recommended Internet Service Provider Security Services and Procedures*

Source Address verification/filtering

IETF BCP38/RFC 2827 *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*

BCP 84/RFC 3704 *Ingress Filtering for Multihomed Networks*

BCP 140/RFC 5358 *Preventing Use of Recursive Nameservers in Reflector Attacks*

ICANN SAC04 *Securing the Edge*

ICANN SAC08 *DNS Distributed Denial of Service (DDoS) Attacks*

DoS/DDoS Considerations

IETF BCP 140/RFC 5358 *Preventing Use of Recursive Nameservers in Reflector Attacks*

IETF RFC 4732 *Internet Denial-of-Service Considerations*

SANS *A Summary of DoS/DDoS Prevention, Monitoring and Mitigation Techniques in a Service Provider Environment*

DNS Cache Protection

IETF RFC 5452 - *Measures for Making DNS More Resilient against Forged Answers*

Jiang, et al (2012), *Ghost Domain Names: Revoked Yet Still Resolvable*

Domain Name Registration Protection

ICANN SAC40

ICANN SAC44

DNS Response Modification

ICANN SAC32

Zone Transfer Security

IETF RFC 2845 *Secret Key Transaction Authentication for DNS (TSIG)*

IEFT RFC 3007 *Secure Domain Name System (DNS) Dynamic Update*

IETF RFC 3645 *Generic Security Service Algorithm for Secret Key Transaction Authentication for DNS (GSS-TSIG)*