BEST CURRENT PRACTICES FOR ACQUIRING AND USING DOMAIN NAMES

ANSSI GUIDELINES

ANSSI-BP-038-EN
10/11/2017

TARGETED AUDIENCE:

Developers **Administrators** **IT security managers** **IT managers** **Users**

Information

Warning

This document, written by the ANSSI, presents the **"Best Current Practices for Acquiring and Using Domain Names"**. It is freely available at `www.ssi.gouv.fr/en/`. It is an original creation from the ANSSI and it is placed under the "Open Licence" published by the Etalab mission (`www.etalab.gouv.fr`). Consequently, its diffusion is unlimited and unrestricted.

This document is a courtesy translation of the initial French document **"Bonnes pratiques pour l'acquisition et l'exploitation de noms de domaine"**, available at `www.ssi.gouv.fr`. In case of conflicts between these two documents, the latter is considered as the only reference.

These recommendations are provided as is and are related to threats known at the publication time. Considering the information systems diversity, the ANSSI cannot guarantee direct application of these recommendations on targeted information systems. Applying the following recommendations shall be, at first, validated by IT administrators and/or IT security managers.

Document changelog:

VERSION	DATE	CHANGELOG
1.0	24/05/2014	Initial French revision.
1.1	01/06/2014	Fixing some typos.
1.2	02/15/2015	Adding a recommendation about glues.
1.3	10/11/2017	Initial English revision.

Contents

1
Introduction

This document is a guide for those responsible for the security of information systems and system and network architects of organisations of all sizes who have to circulate information, like IP addresses, via domain names that they hold and DNS [1] protocol.

It details the security considerations relating to selecting service providers working on the administrative or technical management procedure for domain names.

Among these service providers the following can be identified:

- **the registry**;
- **the registrars**;
- a possible **hosting provider**;
- a possible **reseller**.

These entities can have a strong impact on the security level (integrity and confidentiality) and the resilience (availability) of a domain name and the services which depend on it, like a website or an electronic messaging service.

The registry and the registrar are, in particular, two essential service providers for acquiring and using a domain name.

The service providers for the querying and resolution of domain names are considered as not being within the scope of this document.

It is important to note that the recommendations given in this document are under no circumstances exhaustive and are only one part of the security basics of a DNS hosting infrastructure. The reader is encouraged to also consult the "40 essential measures for a healthy network" [GuideHygiene] guide, in particular if he or she is responsible for the hosting provider role.

1. Domain Name System

2
A reminder on DNS

The domain name system, managed by DNS protocol, has the essential aim of associating a name that users find legible and memorable to an IP address. It is also able to provide stability to the identifiers of computing resources.

DNS is now also used to store various data: information essential to delivering emails (DNS MX records), security policies like SPF [2] to combat email address spoofing [rfc7208] and even cryptographic information like the circulation of fingerprints for SSH keys [rfc4255].

The DNS can therefore be viewed as a vast database, which is scaled-up thanks to two intrinsic properties in the protocol: its hierarchical organisation and the distributed nature of the data.

The hierarchical organisation means that the data is spread out in the form of a tree diagram [3], which ensures the uniqueness of domain names. The domains lower down in the tree than a certain domain are called sub-domains of this domain, and the domains higher up in the tree are called parent domains.

At the same time, to decentralise the data, each of the nodes of this tree can delegate their authority over a sub-domain to a third party administrative entity (natural or legal person). This mechanism therefore allows the root of the DNS tree, symbolised by a ".", to entrust the management of the sub-domains, like `.org`, `.eu` or even `.fr`, to independent bodies, generally called registries. The domains delegated by the root are called TLD [4]. The registries can, in turn, delegate their authority over sub-domains, like `france.fr` or `wikipedia.org`, to domain name holders who acquire a usage right for it, generally upon payment of a fee.

The delegations of authority form administrative barriers. Each delegation symbolises the end of the authority of the delegating entity and the start of the authority of the entity receiving the delegation. The sub-divisions of the tree that are therefore obtained are called *zones*.

Therefore, in diagram 2.1, the names with the same colour and linked by a continuous line are in the same zone and under the responsibility of the same administrative entity. For example, `europa.eu`, `legifrance.gouv.fr`, `france.fr` and `wikipedia.org` receive an authority delegation from their respective parent domains and are therefore in a different zone to their parent domain. However, `gouv.fr` and `fr.wikipedia.org` are sub-domains, of `.fr` and of `wikipedia.org` respectively, yet they remain under the responsibility of the administrative entity of the parent domain. They are therefore both part of the same zone as their respective parent domains.

Taking into account the significant number of holders of second-level domain names, the registries generally accredit bodies, called registrars, who play the role of proxies. They collect information

2. Sender Policy Framework
3. Traditionally, the root of this reversed tree is represented at the top of diagrams and the leaves at the bottom. A representation example is provided with diagram 2.1.
4. Top-Level Domains

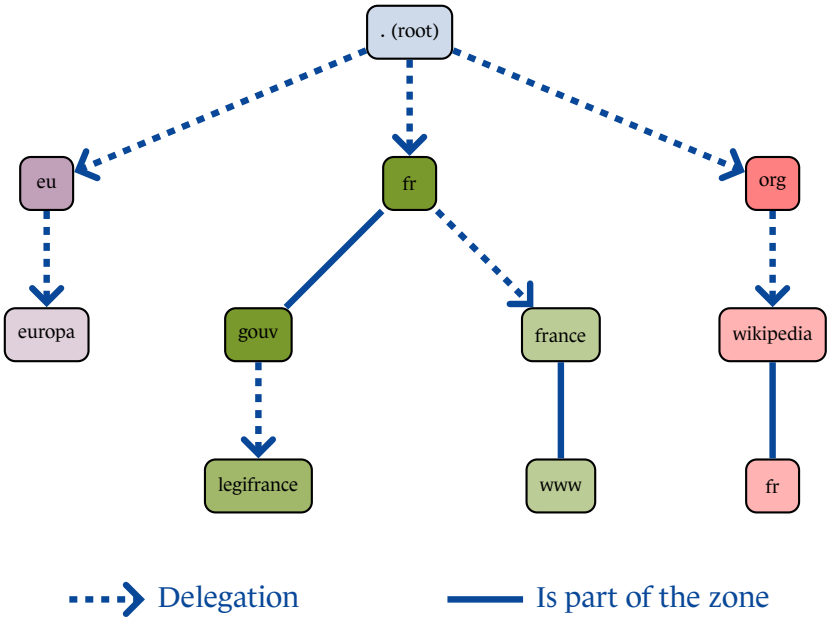

Figure 2.1: Domains and zones: the role of delegations

relating to the domain name holders and their payments and pass them on to the registries via dedicated channels.

Once a domain has been acquired, the domain name holder is in charge of the content of the zone under his or her authority, and more specifically the DNS records that he or she publishes on there. He or she may proceed with self-hosting from machines serving this content or designate hosting providers.

Finally, a reseller is a body that can intervene between the domain name holder on the one hand and the registrar and hosting provider on the other, in order to mask the complexity of the administrative and technical management of the DNS or provide added value by offering additional services and benefits, like the management of domain name portfolios or the application of domain name renewal policies.

The role and responsibilities of the different parties (registries, registrars, hosting providers), which have just been presented, are summarised by diagram 2.2. The roles are studied in detail in section 3.

It is important to note now that due to the nature of the DNS tree diagram, the failing of one or several of these stakeholders can lead to an incident in all the domains over which they intervene. Each of them must therefore be selected with care by the domain name holder, in order to reduce or avoid the risks affecting his or her domain name.

By way of an example, and to illustrate the responsibility of each of the intermediaries in keeping a domain name in working order, here is a list of recent incidents:

- The IEDR registry, in charge of the top-level national Irish domain name `.ie`, suffered a security incident in October 2012, leading to the pharming[5] of `google.ie` and `yahoo.ie` web-

5. This type of attack aims to engage in phishing via redirecting the user, thanks to the DNS, to a server controlled by the attacker.

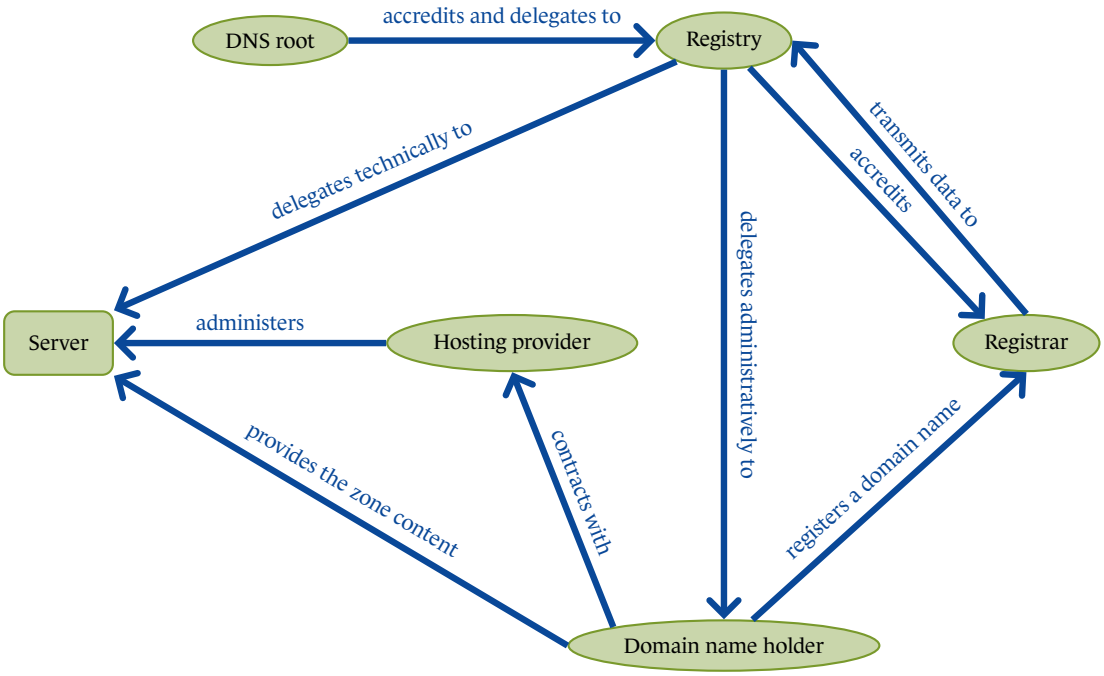

Figure 2.2: Summary of the relationships between the DNS stakeholders

sites. This incident was not isolated, as over the last few years, numerous other registries have noted incidents, including the Moroccan (`.ma`), Qatari (`.qa`) and Malaysian (`.my`) registries [mynic, googlereport]…

- The Network Solutions registrar committed a configuration error in June 2013, in response to a distributed denial of service attack, leading to the accidental modification of information on domain name delegations of nearly five thousand customers to servers not having authority over these names. All the domain names concerned therefore suffered a great loss in availability [networksolutions]. In October 2013, this same registrar suffered an attack leading to the modification of delegation information and the unavailability of several very popular websites [dnshijack].

  In December 2013, the NameCheap registrar corrected a vulnerability in its administration interface that would have allowed for arbitrary modification by an attacker of domain name delegation information [namecheap].

  The Mark Monitor registrar suffered an attack in January 2014 leading to the modification of delegation information for the `ebay.co.uk` and `paypal.co.uk` domain names. Neither the registrar nor the victims commented publicly on the incident [mmonitor1, mmonitor2].

- The hosting provider Go Daddy, also a registrar, experienced a network incident in 2012 rendering all of its services, including hosting customer domain names, inaccessible for six hours. This breakdown, in turn, rendered services to its customers inaccessible, their domain names could not therefore be resolved, even if said services were not hosted by Go Daddy [godaddy].

- The reseller responsible for the `nytimes.com` domain name had their access credentials to the MelbourneIT registrar stolen. This compromise led, in August 2013, to the phishing of services dependant on this domain name for half a day [melbourneIT].

3
The different DNS roles and stakeholders

This chapter introduces the different roles that DNS stakeholders may assume. It is worth noting that while these roles are independant, stakeholders may assume several of them at once. For instance, it is common practice for registrars to include a DNS hosting service in their domain name bundles. Also, some registrars may act as resellers for other registrars, for instance when some registrar accreditation criteria are complex to fulfill.

3.1 The registries

The registries are the entities responsible for top-level domain names, such as `.fr`, `.com`, `.org` or certain second-level names like `.co.uk` [listeTLD]. They are referenced by the ICANN[6], a not-for-profit association under Californian law, in charge of the management of the root zone. The registries in charge of generic top-level domain names, like `.com` are accredited by the ICANN, while those in charge of geographical or regional domain names, like `.fr` or `.eu` are designated according to procedures specific to each country or region.

Some registries offer a service called "registry lock". This service allows an a domain name holder to indicate to the registry that he or she wishes to freeze information relating to his or her domain name, until a new strongly authenticated order comes from the domain name holder.

This security mechanism is implemented to protect the domain names from possible attacks targeting the accredited registrars. The attacker can seek to take advantage of the dedicated communication channel that the registries provide them with. Therefore, once a registrar is compromised, the attacker could modify the authority delegation information on domain names that they manage. These attacks are called DNS hijacking.

The "registry lock" service is generally deployed for domain names, which are a choice target for attackers, like bank, government or even critical infrastructure domains. For example, it would have been able to prevent, in October 2013, the modification of delegation information for certain popular domain names, despite the compromise of the Network Solutions registrar [dnshijack].

Its implementation is carried out by the registry. Ideally, it relies on a secret shared exclusively between the domain name holder and the registry. This secret is therefore used by the registry to verify that the holder is indeed behind an unlocking request. So that the authentication is strong, the verification must not involve the registrar.

6. Internet Corporation for Assigned Names and Numbers

The setting up of such a mechanism can take several forms, and the following examples are only provided as an example: an interactive phone service put in place by the registry, the sending of an SMS confirmation code to the holder who must then enter it into a trusted interface, or even the sending of a fax confirmation from the holder to the registry.

R1

Use registry lock when available

Choose a registry offering a registry lock service and get contractual commitments or assurances as to the level of service guaranteed for this functionality.

The availability of the registry lock service must be confirmed with each registry, as no official list of registries who take responsibility for this has been published by the ICANN.

3.2 The registrars

The registrars are intermediaries between the domain name holders and the registries. They are accredited by the registries, in order to allow natural or legal persons to become the holders of new domain names located under the authority of a registry for a fee.

The domain name acquisition operation is called domain name registration. To do so, a registrar is responsible for:

- verifying the registration conditions for new domain names in accordance with the parent registry policy of the registered names;
- receiving the possible payments associated with the domain name registration;
- sending technical information inherent to the DNS, thanks to specific protocols like RRP [7] [rfc2832] or EPP [8] [rfc5730].

The information sent by the registrars to the registries is of vital importance as it allows the registry to:

- know onto which DNS servers the technical delegation of a domain name must be carried out;
- collect information on the domain name holder which may be listed in the registry directories [9].

The number of DNS hijacks has increased significantly over the last few years [GoogleSurvey1, GoogleSurvey2]. As a consequence, failing a registry lock or in accordance with the principle of defence-in-depth, a registrar offering a hardened authentication should be selected by the domain name holders or the possible reseller.

R2

Select a registrar offering a hardened authentication mechanism

Choose a registrar offering a logged and strong authentication mechanism, for example thanks to two-factor authentication and access filtering to the administration interface.

7. Registry Registrar Procotol
8. Extensible Provisioning Protocol
9. These directories are then consultable thanks to the Whois protocol.

Like with the registry lock, registrars can ask the registry to freeze data relating to a domain name, in order, in particular, to prevent the involuntary or fraudulent transfer of a domain name from one registrar to another, or from one holder to another.

This mechanism is sometimes called a registrar lock. It is separate from a registry lock as the lifting of the lock is controlled by the registrar, without any communication between the registry and the domain name holder. The compromise of a registrar can therefore lead to the lifting of this kind of lock and the alteration of data. This lock, if it is well implemented, therefore only contributes to the defence-in-depth but only offers a very inferior level of protection compared with the registry lock.

R3 +

Use registrar lock when available

Choose a registrar offering a registrar lock mechanism in order to prevent the fraudulent transfer of domain management.

No official list of registrars implementing this functionality has been published. The domain name holder must therefore inquire as to its availability with registrars.

The registrars also play an important role in securing the DNS and notably in the implementation of DNSSEC [10]. DNSSEC is a technology allowing domain name holders to ensure the integrity of data contained in their zone via the use of cryptographic signatures. It is therefore able to compensate for the weak security of the DNS protocol [rfc3833], especially faced with network attacks attempting to replace the data of a DNS response during its transit, like cache poisoning attacks or man-in-the-middle attacks.

The information relating to the different signature keys implemented during cryptographic operations, like their fingerprints, must therefore be sent to the entity with authority over the parent zone in order to create a chain of trust. The registrars are therefore the traditional transmission vehicle for information relating to DNSSEC between the domain name holder and the registry.

The absence of responsibility for information linked to DNSSEC by the registrar ensuring the management of a domain prevents the implementation of this technology by the holder.

R4 +

Select a registrar accepting DNSSEC information

Select a registrar which enables the information required to use DNSSEC to be published.

3.3 The hosting providers

The hosting providers are entities in charge of the technical management of domain names and their hosting on DNS servers. Although this role is sometimes assumed by the domain name holder, it is often delegated to specialised hosting providers.

10. Domain Name System Security Extensions

The list of servers of the hosting provider are part of the delegation information provided to the registry. Chapter 4 gives more details regarding the architectures recommended in order to increase the resilience of the DNS service that they provide.

It is important to note that the same domain name can be hosted by several hosting providers at the same time. In this case, one of the providers is responsible for the original version of the zone and the others must go through it in order to obtain duplicates of it. Stronger contractual demands must therefore be requested from the operator responsible for the original version. An incident affecting this provider could prevent the distribution of duplicates to other providers designated by the domain name holder and eventually lead to the whole zone becoming unavailable. The distribution of a fraudulently altered original version following the compromise of the provider responsible is another attack scenario to consider.

3.4 The resellers

The resellers are intermediaries able to provide a comprehensive service offer, that masks, for example, the administrative or technical complexity of the DNS. They therefore ensure the role of proxy with the registrars and hosting providers.

The security of resellers can influence the security of the domain names of a domain name holder. Their compromise can lead to the loss of control of a domain name. This may be the case if an attacker obtains their access password to registrars' interfaces, which allows him to therefore alter the technical data relating to the delegation of the domain or the DNSSEC chain of trust [melbourneIT].

Using the services of a reseller is optional when using a domain name. The reader is therefore invited to assess the benefits provided by the subscription to such a service and to compare them with the risks and the transfer of responsibility that it brings about. In particular, it is necessary to ensure that the security demands are clearly stipulated in the contract and that they are in accordance with the quality of the service expected. The domain name holder can, moreover, confirm the implementation of security practices from the provider via security audits.

R5

Assess the security risks of contracting with a reseller

When a domain name holder uses a service provider, like a reseller, he or she must undertake a risk assessment and control approach.

4
DNS resiliency

The following considerations relate to improving the resilience of the DNS service, notably via technical measures and architectural choices. These recommendations apply to the hosting of all DNS zones, including reverse zones. They, for the most part, come from studies carried out by the Internet Resilience Observatory in France [obsresanssi].

The application of these recommendations must be carried out by the hosting providers to which the registry technically delegates a domain. If the domain name holder does not administer his or her own authoritative name servers, it is up to him or her to verify that the hosting providers that he designates contractually commit to the application of the best current security practices detailed in this chapter.

4.1 Topological diversification of server names

The DNS protocol defines a standard data replication method between DNS servers. This method allows system administrators to benefit from a standard means of circulating data relating to a domain name on multiple DNS servers. The impact of a breakdown on one of the name servers is therefore reduced. The RFC [11], de facto standards developed by the IETF [12], recommend the use of at least two distinct name servers [rfc1035].

R6

Use at least two authoritative name servers

Serve domain names from at least two authoritative name servers.

Ideally, these multiple DNS servers should be organised and deployed so that they are not all dependent on the same installations.

Therefore, the location of different servers should be taken into consideration in order to limit the impact of environmental incidents, like power cuts, optical fibre damages, floods and even earthquakes.

Likewise, network connectivity should be studied in order to prevent single point failures, whether in terms of routing (BGP [13] incidents) or dependence on unique transit providers. This issue is

11. Request For Comments
12. Internet Engineering Task Force
13. Border Gateway Protocol

covered in-depth in the report from the Internet Resilience Observatory in France. The anycast technique was notably expanded upon in the 2012 report [obsresanssi].

R7 +

Spread authoritative name servers over several prefixes

Spread the authoritative name servers over several prefixes (blocks of IP addresses) or use the anycast routing technique.

R8 +

Distance the name servers to avoid environmental risks

Distance the name servers, for example, by placing them in different datacentres, in order to better resist environmental threats and technical incidents.

4.2 Transport protocols

Although the DNS transport protocol is, to date, mainly UDP [14], RFC 1035 [rfc1035] recommends supporting TCP [15] as a transport protocol. RFC 7766 [?] strengthens this recommendation and makes TCP support obligatory for all DNS implementations and for all types of DNS communication, including DNS queries from recursive name servers to authoritative name servers.

The support of TCP is, to date, especially important to face the following problems:

- the increase in size of DNS responses which sometimes cannot be transported in a standard way over UDP;
- the use of protection mechanisms against distributed denial of service attacks, deployed notably on the root servers and the most prominent hosting providers of top-level domain names, which use TCP as a fallback strategy (see section 4.9);
- the use of protection mechanisms against some cache poisoning attacks, exploiting IP fragmentation [shulmanfrag].

Failure to support TCP exposes infrastructures configured in this way to denial of service attacks.

R9

Enable TCP support

Configure infrastructures as a whole, notably the servers, the load sharers and the filtering equipment to support TCP, in addition to UDP, as a transport protocol for DNS.

4.3 EDNS0

EDNS0 [rfc6891] is an extension of the DNS protocol, which enables an increase of the maximum size of DNS responses from 512 bytes to a value specified by the sender of a request [16].

14. User Datagram Protocol
15. Transport Control Protocol
16. This value may however be scaled down by the server responding to the query.

The increase in the maximum size of the responses is also able to limit the use of TCP, when too large responses are generated. Although the use of TCP is essential, it is advisable to favour the use of UDP, as this does not require the maintenance of a memory state table. EDNS0 therefore contributes to improving the availability of the service.

This extension also enables the deployment of DNSSEC: it adds new flag fields, and specifies the DO flag [17] allowing the sender of a request to specify if he or she wants to add to the response possible data relating to DNSSEC, and the result of the DNSSEC validation carried out by the queried server.

R10

Enable EDNS0 support

Configure infrastructures, notably the DNS servers, the load sharers, the intrusion detection systems and firewalls, in order to support EDNS0.

4.4 Cache time-to-live

The cache TTL [18] of DNS records designates the maximum time period during which the data should be kept in the cache by the devices querying authoritative name servers. After this time period, these devices must consider the cached data as obsolete and ask again for the DNS records from the authoritative name servers.

The TTL value of each record is a local policy matter: it comes from the consideration of the administrator of a DNS zone who is the only one able to determine the frequency of data updates that he or she publishes in the DNS. A TTL value that is not respected can therefore have an impact on the stability (impact on the availability) or even the security (integrity) depending on the type of data contained in the cached record (for example, cryptographic data).

It is, however, worth noting that the TTL plays a role in the resilience and availability of a service. The longer the TTL is, the more the information can remain accessible despite a temporary unavailability of the servers with authority over it.

Values between one hour and two days should be adopted in the majority of cases [RipeTTLKoch].

R11

Set high TTL values during normal operations

Set relatively high TTL values, in the normal context of operations.

4.5 Backups

The DNS servers are generally organised according to a master/slave diagram, with the master server hosting the original version of the DNS data and the slave servers storing duplicates of this same data.

17. DNSSEC OK.
18. Time To Live

In accordance with the standard data replication mechanism, called zone transfer, the slave DNS servers request a duplicate of the zone from the master server, and overwrite their local version with the most recent original version.

These requests with the master server are undertaken, by default, at predefined intervals, but the master can also notify the slaves of the presence of fresh data in order to accelerate the replication process.

If an error or a malicious act are committed on the original version, the alteration may therefore be copied very quickly by the slave servers, destroying their still untainted versions of the zone. The replication mechanism on its own therefore cannot be considered as a reliable way of carrying out backups of DNS zones.

The implementation of other backup methods for DNS zones is therefore necessary to get round the accidental or fraudulent alteration of data.

The backup could therefore take the form of a simple copy of the database containing the information on the zone, like the master file [rfc1035], or be undertaken with the help of the zone transfer mechanism from a backup server, keeping a log of the zone versions.

R12

Backup zone data

Implement a regular backup procedure of the data contained in the DNS zones.

4.6 Monitoring

The administration of a DNS server is a complex task involving replication mechanisms and possible cryptographic signatures.

The introduction of an error into a zone file or the malfunction of the replication mechanism can therefore lead to the circulation of invalid information (corrupt or obsolete). As the DNS relies on information caching strategies, invalid data can, moreover, take a long time to purge.

The rapid and automated detection of incidents is therefore necessary, in order to limit the incorrect data publication time and reduce the number of DNS servers caching them.

Given the hierarchical nature of the DNS, incidents affecting the intermediaries located upstream can also have an impact on the services hosted under a domain name. The automated detection of incidents upstream can therefore be an advantage in order to react effectively and restore the availability of affected services as soon as possible.

Such monitoring tools should be deployed from different networks to the one hosting the DNS service, in order to be able to detect losses in connectivity and allow for the sending of warnings in any event. The detection in itself can be carried out with simple DNS service query scripts, thanks

to sophisticated tools like ZoneMaster [zonemaster], or even with the help of specialised platforms like Nagios [nagios].

R13

Monitor zones and parent zones for failures

Implement an automated monitoring system for data provided by name servers authoritative over a zone and by those of parent zones.

4.7 Software diversity

Each software vulnerability requires the attacker to write a specific exploit code for the implementation targeted. A code carrying out denial of service on an implementation will not necessarily have an effect on another implementation.

Software diversity describes the act of using several implementations to provide the same service. It is therefore able to reduce the impact of a software failure on the whole service.

In practice, this means using different DNS server software stacks on the different authoritative name servers of a zone. Different authoritative name server implementations are available, among them are Bind [bindwebsite], Knot [knotwebsite], Microsoft DNS [microsoftdnswebsite], NSD [nsdwebsite], and PowerDNS [powerdnswebsite].

It is worth noting that this best current practice increases the workload and requires additional skills.

R14 +

Employ various DNS software stacks

Employ at least two different DNS server software stacks on all the authoritative name servers.

4.8 Role separation

Some DNS server implementations are able to provide services of a different nature to the local users of a body and the users coming from the Internet.

For example, implementations like Bind and Microsoft DNS offer the DNS recursive query service and can also respond to queries over domains which they have authority over.

The query service is ensured by forwarders or recursive DNS servers, sometimes incorrectly called cache servers. These servers are in charge, following queries from users, of carrying out domain name resolutions. The diagram 4.1 illustrates a DNS query from a user and the resolution of the `www.gouvernement.fr` name in the IP address 185.11.125.117. To do this, the recursive server queries the root, then follows delegations of authority until it gets the address sought from the DNS server responsible for the `gouvernement.fr` zone. This is then returned to the user, after being cached by the recursive DNS server.

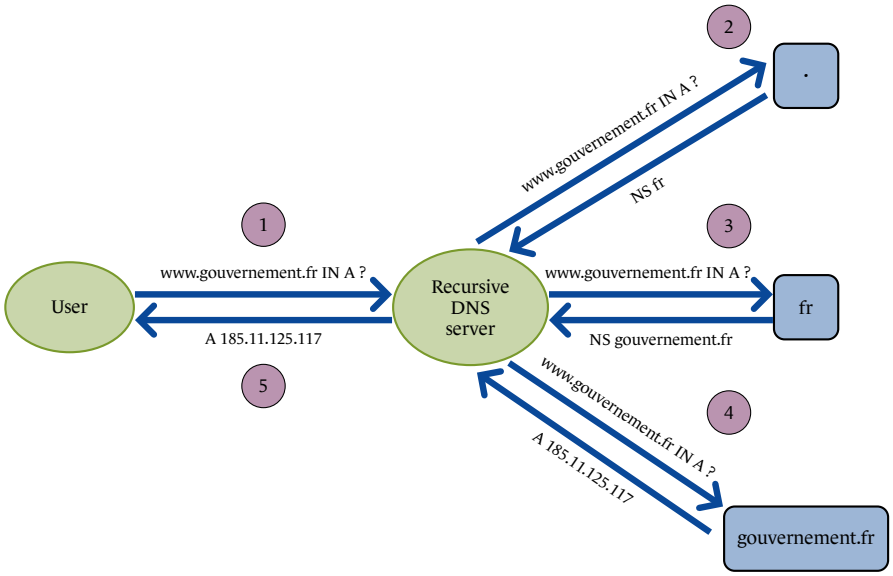

Figure 4.1: Example of recursive DNS resolution

As these implementations ensure both the roles of the authoritative DNS servers and the recursive servers, they present an increased attack surface due to the multiple services provided. Exploiting a vulnerability in one of the parts (authoritative server or recursive server) could therefore have an impact on the availability for the other service. It is worth noting, however, that this risk is decreased if the DNS servers configured in this way are only accessible from trusted networks and that they only query servers over trusted networks.

It is preferable to separate the roles of authoritative DNS servers and recursive servers into two separate software instances, for example, by using separated or isolated processes or servers, in order to reduce the interactions.

R15 +

Isolate the querying service from the authoritative one

The DNS query service should be undertaken by a isolated server or process separate from that providing the DNS authoritative service.

The Bind DNS server offers a view mechanism, which gives it the option of responding with different data depending on the information present in the query. These parameters can be the source IP address of the query or specific cryptographic signatures [19].

This mechanism offers a configuration flexibility able to ease the administration task of the DNS server. It can, however, present a risk in the event that the different data present different levels of sensitivity or if the bodies likely to query the DNS server benefit from a different level of trust. This is the case when a view presents data relating to the internal network of the body, while another view provides data relating to the services exposed to the Internet.

In this kind of infrastructure, the isolation of information is only logical. Therefore, the exploitation of a vulnerability allowing access to the memory of the server would allow an attacker located on a less trusted network to access indifferently all the data present in all the views of this server.

19. This cryptographic signature is based on a shared secret and implements the mechanism called TSIG [20]. It is not linked to the DNSSEC cryptographic signatures and is more generally used to secure the zone transfers between DNS master and slave servers.

In the same way, if the vulnerability exploited was to lead to a denial of service, the DNS service would be interrupted for all the networks to which the DNS server offered its service.

It is possible to free yourself from the collection of risks brought about by each of the networks to which the server is connected by using distinct and isolated processes. The data contained in each view will therefore be segregated according to its sensitivity and the level of trust of the networks on which they will be served.

R16

Avoid using views as an isolation mechanism

Divide up the internal data on the one hand, and external data on distinct servers or distinct and isolated processes on the other.

4.9 Anti-distributed denial-of-service solutions

Authoritative name servers can be exploited as reflecting servers for distributed denial of service attacks with traffic amplification [prolexic].

The attackers use these techniques in order to increase their throughput against victims. To do this, they take advantage of the asymmetry offered by the DNS protocol, between the size of the questions and responses and the possible spoofing of IP addresses.

Having no other choice than to respond to questions concerning the domains for which they are responsible, authoritative name servers must employ rate-limiting solutions in order to reduce the impact of their exploitation.

Among the solutions available, RRL[21] offers a moderated and targeted approach, based on the detection of identical DNS responses sent in bulk to groups of IP addresses. This mechanism also offers a fallback strategy in the event of a false positive (wrongly triggered mechanism). RRL is available for Bind, NSD, Knot and a similar approach may be scripted into PowerDNS [bindrrl, nsdrrl, knotrrl, pdnsrrl].

The principle of the fallback strategy (called slipping) is to send truncated DNS responses, causing a retry of the query over TCP. As the source IP address of a query sent over TCP is a lot more difficult to spoof than over UDP, this fallback mechanism effectively combats amplification attacks.

R17

Use RRL when available

Employ the RRL anti-distributed denial of service mechanism on the implementation supporting it.

The Bind, NSD and PowerDNS RRL implementations, including the most recent versions on the date this guide was written, are, by default, configured to only respond to a fraction of the queries received, once a tolerance threshold has been exceeded.

21. Response Rate Limiting

```
example.com. IN NS dns1.example.com. ; delegation using a glue
dns1.example.com. IN A 192.0.2.1      ; glue record
```

Figure 4.2: Example of a domain name delegation using a glue record

Although it is better to avoid answering requests emitted by attackers, and thus to prevent the unwilling participation to DDoS attacks, it is sometimes next to impossible to distinguish attack traffic from legitimate one. Unfortunately, a study carried out by ANSSI[22] has shown that the absence of a response to DNS queries could increase the effectiveness of some cache poisoning attacks [rrlslip]. As a consequence, when in doubt about the legitimacy of a DNS request, one must provide an answer to it.

The configuration of the RRL mechanism, when the Bind, NSD and PowerDNS servers are used, should therefore be modified manually. This is undertaken by configuring the response sending frequency (called "slip" for Bind, "rrlslip" for NSD, and "tcrate" for PowerDNS) to the value "1".

The DNS Knot server has taken into consideration the ANSSI recommendations and adapted its default configuration.

R18

Configure the hosting platform to never drop DNS messages on purpose

If RRL is implemented, use a "slipping" value of 1, in order to always respond to the DNS queries.

It is worth noting that the risk discovered by the ANSSI study is not limited to implementations employing RRL, but rather to all the infrastructures with a mechanism leading to the loss of DNS messages. This includes the use of firewalls limiting the number of incoming packets.

4.10 Delegations and third-party dependency

The addition of NS records in a zone allows for a sub-domain to be delegated. These records designate the DNS servers that must be queried by the recursive DNS servers to look up a name that is part of the delegated sub-domain. Therefore, in practice, in the `.com` zone, NS records indicate the DNS servers of the hosting provider designated by the domain name holder and to which are delegated the management of the sub-domain `example.com`.

If the name indicated to the right in the NS record is a part of the delegated domain, A or AAAA additional records, called "glue records", are required. An example of such records is provided in figure 4.2. The query server gathers these glue records at the same time as the delegation and can immediately continue the name resolution.

If the name indicated in the NS record is outside of the delegated domain, then this name must be resolved before being able to start again on the original search. This delegation mode called

22. Agence nationale de la sécurité des systèmes d'information

```
example.com.  IN  NS  ns1.example.net.
example.com.  IN  NS  ns2.example.net.
```

Figure 4.3: Glueless delegation example

"glueless delegation" can bring additional risks by creating a dependency on the availability and integrity of this third-party domain.

In order to illustrate this risk, let us take the case study of a user requesting the resolution of the IP address associated with the `example.com` domain name. This domain is delegated as indicated in figure 4.3.

When a recursive server collects these delegations, it must pause its `www.example.com` search to get the address of one of the two DNS servers located in the `example.net` domain. If the `example.net` domain is unavailable or compromised, the `example.com` domain also becomes so as a consequence. It is worth noting that this risk is, however, negligible if all the organisational and technical stakeholders, in other words, the registry, registrar, reseller and servers hosting the domains, are identical for the delegated domain name and domain names used in the glueless delegation.

An integrity risk also hovers over `example.com` if the domain name holder of `example.net` does not timely renew their domain name, and an attacker becomes the new holder in their stead. The attacker is then capable of answering arbitrary fraudulent data for the `example.com` domain name, if `example.com` is not protected with DNSSEC.

R19

Favour the use of glue delegations

Favour glue delegations when using glueless delegations introduces new third-party dependencies.

Following this recommendation may result in an increase of operational costs and delays during migrations if the hosting provider cannot modify delegation information by themselves.

4.11 Hardening of the technical platform

In addition to a hardened configuration of the DNS services, the operating system on which they are installed must be hardened adequately.

ANSSI publishes several guides relating to the security of operating systems and network infrastructures. The reader is encouraged to refer to the appropriate section of the ANSSI website for guides and technical notes [anssiwebsiteguide].

R20

Harden the hosting operating system

Harden the operating system hosting the DNS software.

Bibliography

[zonemaster] Afnic and IIS.
ZoneMaster.
<http://www.zonemaster.net>.

[anssiwebsiteguide] ANSSI.
ANSSI Best Current Practices.
<https://www.ssi.gouv.fr/en/best-practices/>.

[GuideHygiene] ANSSI.
Guide d'hygiène informatique.
<http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/l-anssi-publie-la-version-finalisee-du-guide-d-hygiene-informatique.html>, janvier 2013.

[obsresanssi] ANSSI.
L'observatoire de la résilience de l'Internet français.
<http://www.ssi.gouv.fr/fr/anssi/presentation/l-observatoire-de-la-resilience-de-l-internet-francais.html>, juillet 2013.

[rfc3833] D. Atkins and R. Austein.
Threat Analysis of the Domain Name System (DNS).
RFC 3833 (Informational), août 2004.

[dnshijack] Avira.
Major DNS hijacking affecting major websites, including avira.com.
<http://techblog.avira.com/2013/10/08/major-dns-hijacking-affecting-major-websites-including-avira-com/en/>, octobre 2013.

[melbourneIT] CNET.
Melbourne IT tells how hacker launched NY Times cyberattack.
<http://news.cnet.com/8301-1023_3-57600368-93/melbourne-it-tells-how-hacker-launched-ny-times-cyberattack/>, août 2013.

[knotwebsite] CZNIC.
Knot Website.
<https://www.knot-dns.cz/>.

[rfc6891] J. Damas, M. Graff, and P. Vixie.
Extension Mechanisms for DNS (EDNS(0)).
RFC 6891 (INTERNET STANDARD), avril 2013.

[mmonitor2] Fran Berkman.
Syrian Electronic Army: We Hacked eBay and PayPal.
<http://mashable.com/2014/02/01/syrian-electronic-army-ebay/>, février 2014.

[microsoftdnswebsite] Jim Groves.
Guide des opérations du serveur DNS.
<http://technet.microsoft.com/fr-fr/library/cc816603%28v=ws.10%29.aspx>, mai 2008.

[namecheap] Henry Hoggard.
Hijacking DNS on NameCheap Domains.
<https://henryhoggard.co.uk/?p=77>, décembre 2013.

[shulmanfrag] Amir Herzberg and Haya Shulman.
Fragmentation Considered Poisonous: or one-domain-to-rule-them-all.org.
In *IEEE CNS 2013. The Conference on Communications and Network Security.*, 2013.

[rfc5730] S. Hollenbeck.
Extensible Provisioning Protocol (EPP).
RFC 5730 (INTERNET STANDARD), août 2009.

[rfc2832] S. Hollenbeck and M. Srivastava.
NSI Registry Registrar Protocol (RRP) Version 1.1.0.
RFC 2832 (Informational), mai 2000.
Updated by RFC 3632.

[googlereport] Maarten Van Horenbeeck.
Update on DNS hijackings.
<http://durban47.icann.org/meetings/durban2013/presentation-dns-hijacking-horenbeeck-15jul13-en.pdf>, juillet 2013.

[listeTLD] ICANN.
List of Top-Level Domains.
<http://www.icann.org/en/resources/registries/tlds>.

[bindwebsite] ISC.
Bind Website.
<https://www.isc.org/downloads/bind/>.

[bindrrl] ISC Support.
A Quick Introduction to Response Rate Limiting.
<https://kb.isc.org/article/AA-01000>, juin 2013.

[rfc7208] S. Kitterman.
Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1.
RFC 7208 (Proposed Standard), avril 2014.

[knotrrl] Knot Team.
Using Response Rate Limiting (Knot Documentation).
<https://www.knot-dns.cz/static/documentation/knot.html/Using-Response-Rate-Limiting.html>.

[GoogleSurvey2] Maarten Van Horenbeeck.
Update on DNS hijackings.
<http://durban47.icann.org/meetings/durban2013/presentation-dns-hijacking-horenbeeck-15jul13-en.pdf>, juillet 2013.

[rrlslip] Florian Maury and Mathieu Feuillet.
Démonstration d'un détournement possible de technologies anti-déni de service distribué (DDoS).
<http://www.ssi.gouv.fr/fr/anssi/publications/publications-scientifiques/articles-de-conferences/demonstration-d-un-detournement-possible-de-technologies-anti-deni-de-service.html>, octobre 2013.

[rfc1035] P.V. Mockapetris.
Domain names - implementation and specification.
RFC 1035 (INTERNET STANDARD), novembre 1987.
Updated by RFCs 1101, 1183, 1348, 1876, 1982, 1995, 1996, 2065, 2136, 2181, 2137, 2308, 2535, 2673, 2845, 3425, 3658, 4033, 4034, 4035, 4343, 5936, 5966, 6604.

[GoogleSurvey1] Morgan Marquis-Boire.
A Brief History of DNS Hijackings.
<http://costarica43.icann.org/meetings/sanjose2012/presentation-dns-hijackings-marquis-boire-12mar12-en.pdf>, mars 2012.

[mynic] MyNic.
.my domain name incident resolved.
<http://www.mynic.my/upload_media/51d2a8d4edd6a.pdf>, juillet 2013.

[nagios] Nagios Enterprise.
Nagios - The Industry Standard In IT Infrastructure Monitoring.
<http://www.nagios.org/>.

[nsdwebsite] NLNet Labs.
NSD Website.
<http://www.nlnetlabs.nl/>.

[RipeTTLKoch] Peter Koch.
Recommendations for DNS SOA Values.
<http://www.ripe.net/ripe/docs/ripe-203>, juin 1999.

[powerdnswebsite] PowerDNS.
PowerDNS Website.
<https://www.powerdns.com/>.

[pdnsrrl] PowerDNS Team.
A Lua policy engine example intended to be a faithful implementation of Vixie's RRL specification.
<https://github.com/PowerDNS/pdns/blob/master/pdns/policy-example-rrl.lua>, juin 2013.

[prolexic] Prolexic.
Global DoS and DDoS Attack Reports, Trends and Statistics.
<http://www.prolexic.com/knowledge-center-dos-and-ddos-attack-reports.html>.

[rfc4255] J. Schlyter and W. Griffin.
Using DNS to Securely Publish Secure Shell (SSH) Key Fingerprints.
RFC 4255 (Proposed Standard), janvier 2006.

[networksolutions] Jaeson Schultz.
'Hijacking' of DNS Records from Network Solutions.
<http://blogs.cisco.com/security/hijacking-of-dns-records-from-network-solutions/>, juin 2013.

[godaddy] Scott Wagner.
Go Daddy Site Outage Investigation Completed.
<http://www.godaddy.com/news/article/go-daddy-site-outage-investigation-completed.aspx>, septembre 2012.

[mmonitor1] Waqas.
Ebay and Paypal hacked by Syrian Electronic Army for not providing services in Syria.
<http://hackread.com/ebay-paypal-hacked-by-syrian-electronic-army/>,
février 2014.

[nsdrrl] Wouter (W.C.A. Wijngaards).
DNS Response Rate Limiting as implemented in NSD.
<http://www.nlnetlabs.nl/blog/2012/10/11/nsd-ratelimit/>, octobre 2012.

Recommendation List

ANSSI-BP-038-EN
Version 1.3 - 10/11/2017

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP
www.ssi.gouv.fr / conseil.technique@ssi.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
SGDSN