



Server Administration

Name resolving

Name Resolving

- Naam omzetten naar IP-adres
- Verschillende soorten namen
 - NetBIOS naam (vooral bij Windows)
 - *hosts* bestand
 - /etc/hosts (Linux) 
 - %SystemRoot%\System32\drivers\etc\hosts (Windows) 
 - Internet Host Name

Vroeger: enkel HOSTS bestand met alle hostnames

Name resolving in Linux



Verschillende bronnen in /etc/nsswitch.conf

```
hosts:      files dns wins
```

1. files: Domein naam in /etc/hosts
2. dns: Gebruikte dns uit /etc/network/interfaces
3. wins: Samba configuratie

Name resolving in Linux



Verschillende bronnen in /etc/nsswitch.conf

```
hosts:      files mdns4_minimal [NOTFOUND=return] dns
```

1. files: Domein naam in /etc/hosts
2. mdns4_minimal: gebruikt dns multicast als het adres eindigt op .local
[NOTFOUND=return]: zorgt ervoor dat gestopt wordt als het lokale adres niet gevonden werd
3. dns: Gebruikte dns uit /etc/network/interfaces



Name resolving in Windows



1. Controle of gelijk aan eigen naam
2. Zoeken in Hosts file
3. Domain Name System (DNS)
4. NetBIOS (als backup)

Name resolving



- Verschil tussen

```
ping server01.ikdoeict.be
```

en

```
net use * \\server01\share
```

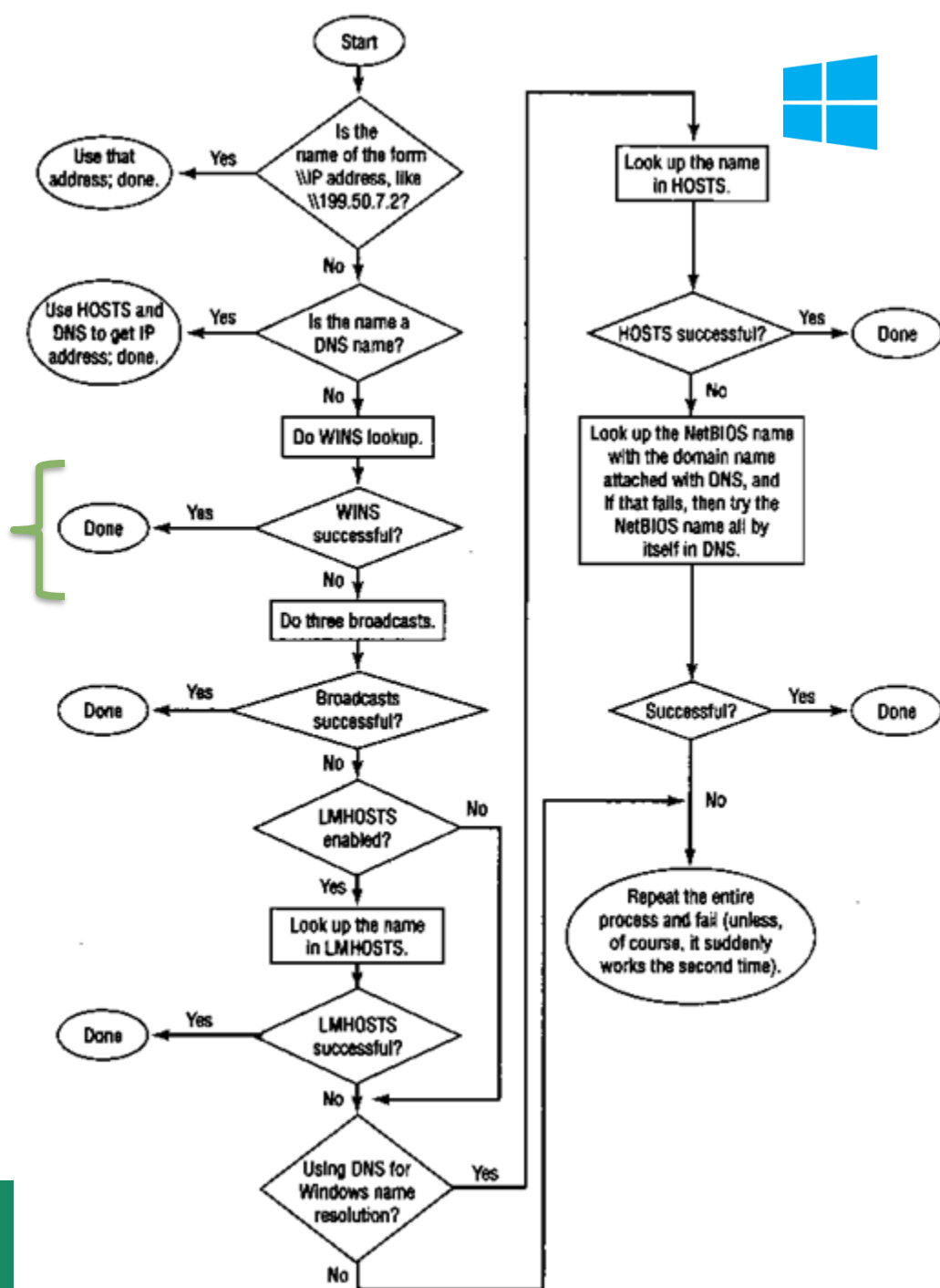
- `ping` gebruikt traditionele internet API => WinSock
- `net use` gebruikt de microsoft API => NetBios

Name resolving in Windows

- NetBIOS naam opzoeken

Enkel als WINS server beschikbaar is

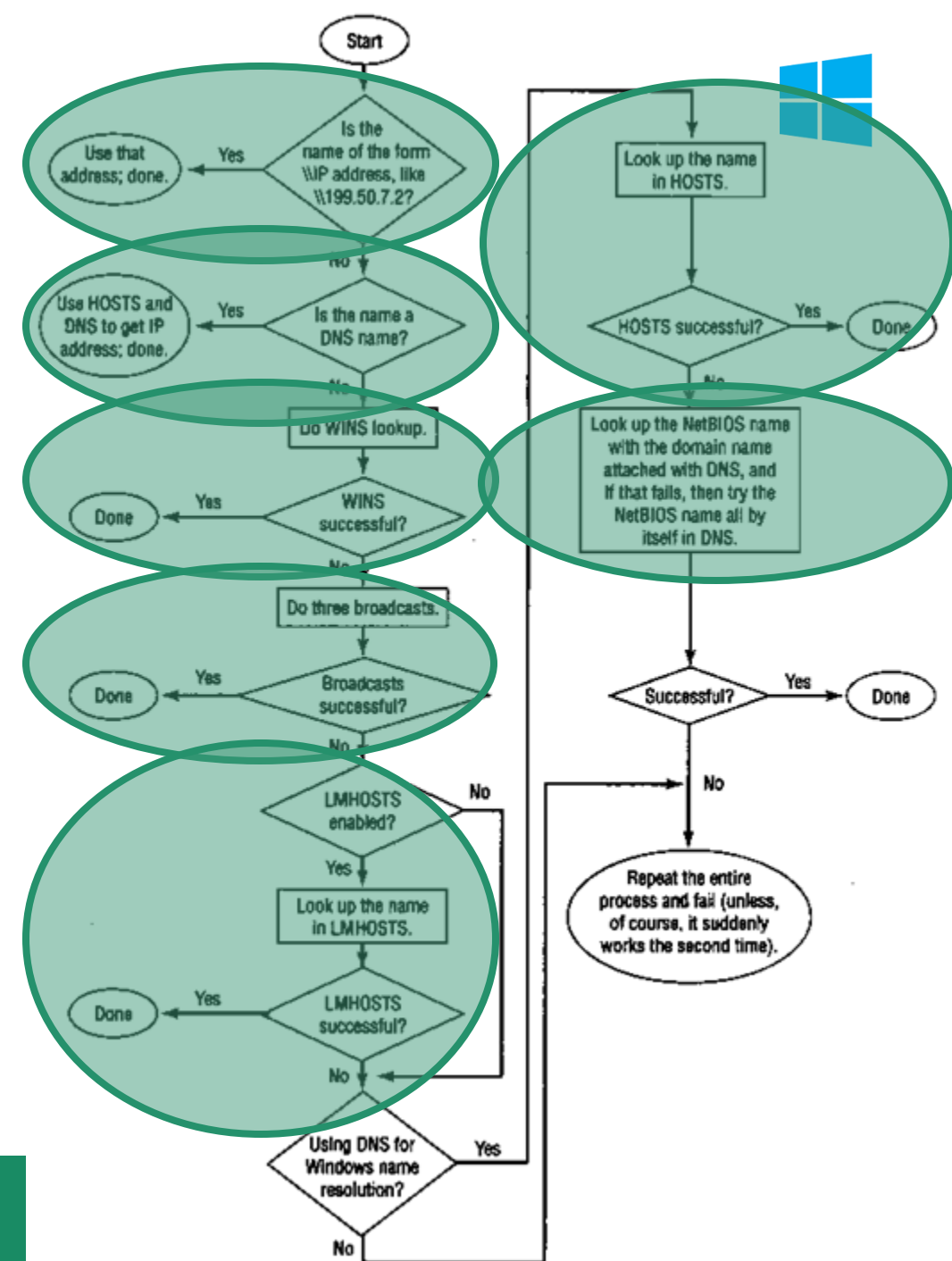
Hosts bestand voor NetBios



Name resolving in Windows

- NetBIOS naam opzoeken
 1. Eerst kijken of het toch geen adres is
 2. Als het een domeinnaam is, HOSTS en DNS gebruiken met die domeinnaam
 3. WINS server contacteren
 4. 3 lokale broadcasts
 5. LMHOSTS=oplossing voor als WINS niet aanwezig op netwerk of als WINS faalt. Vooral voor kleine netwerken.
 6. HOSTS file raadplegen
 7. Nog proberen redden door domeinnaam achter naam te plakken en daarmee eens te proberen of de netbiosnaam zonder domein aan DNS server te vragen

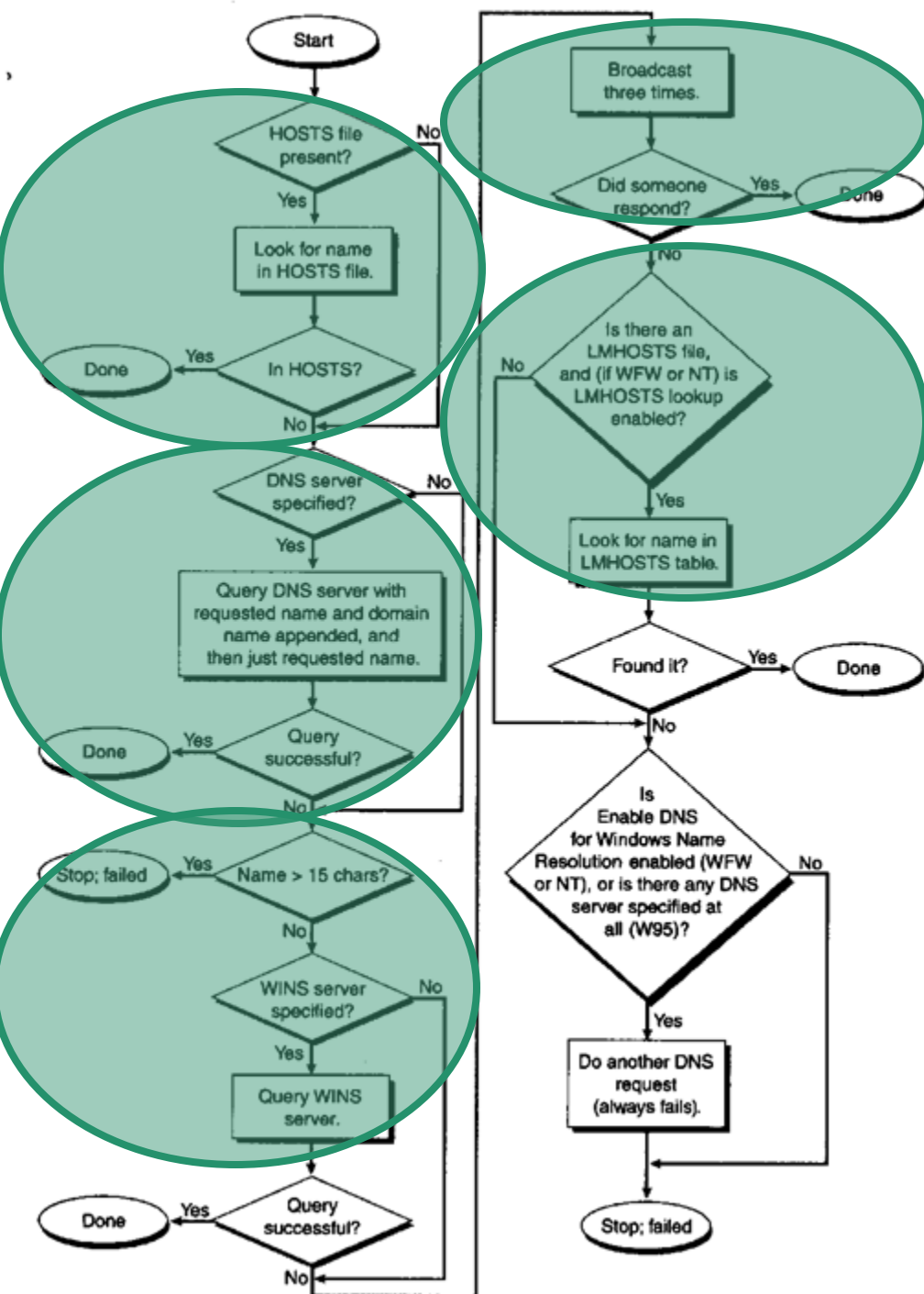
Maximaal nog 1 keer herhalen





Name resolving in Windows

- DNS naam opzoeken
 1. HOSTS file raadplegen
 2. DNS server raadplegen indien geconfigureerd
 3. Als de naam minder dan 16 tekens, WINS server raadplegen
 4. 3 broadcasts
 5. LMHOSTS
 6. Laatste stap enkel op oudere systemen





- **Network Basic Input Output System**
- Geen protocol maar API
- In een LAN – Geen routing (broadcasts)
- Meestal over TCP/IP via het NetBIOS over TCP/IP (NBT) protocol
- NetBIOS: 16 ASCII tekens
 - Meestal 15 ASCII tekens voor naam
 - Meestal 1 ASCII teken voor suffix = type resource
- Resolving door broadcast of WINS server (NetBIOS Name Server)



- **Domain Name System**
- Hiërarchische database met namen en IP-adressen
- Legt relatie tussen een IP-adres en een (hiërarchische) naam
- Belangrijk voor bijna alle huidige netwerk-communicatie (incl Active Directory,...)

Structuur en naamgeving

- Elk deel dns-suffix max. 63 karakters
- Gehele DNS-naam max. 255 karakters

server.research.odisee.be.



Toestelnaam

parent domeinnaam of DNS-suffix

- Let op met de toestelnaam! In samenwerking met Netbios enkel 15 karakters.



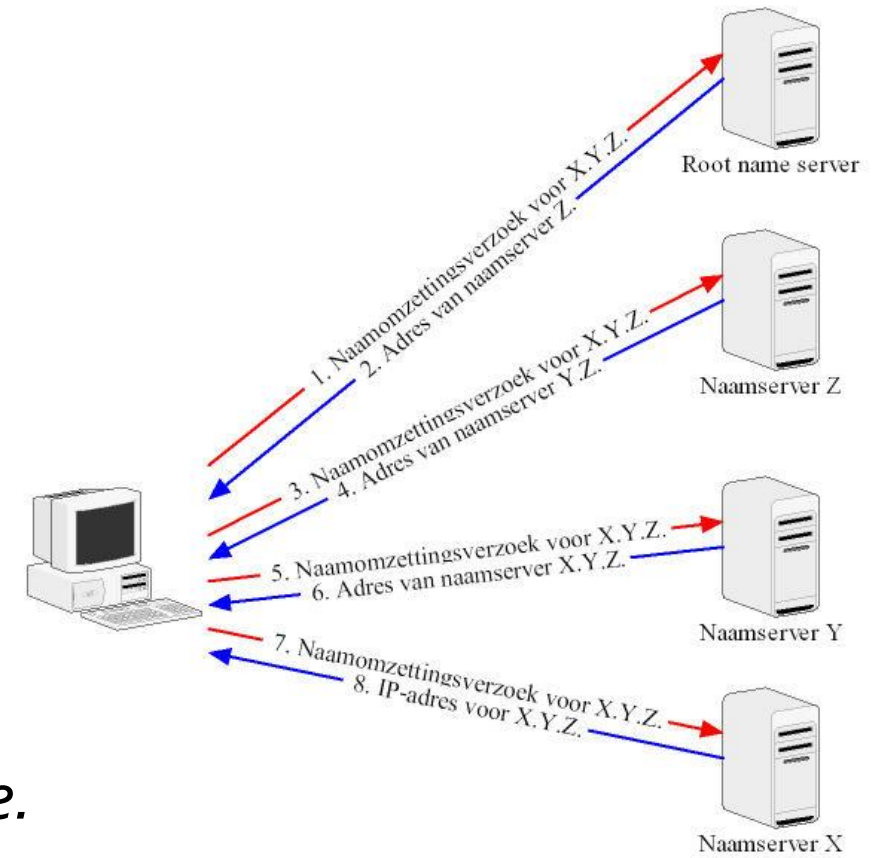
Fully Qualified Domain Name (FQDN)

- Volledig unieke, eenduidige notatie/locatie
- “Absolute domain name”
- Exacte locatie in de DNS boomstructuur
- Eindigt in de root: .

DNS Name resolving

server.research.odisee.be.

- Stap voor stap subdomeinen opzoeken
 1. Root servers vragen naar dns server voor *be*.
 2. Aan dns voor *be*. vragen naar *odisee.be*.
 3. Aan *odisee.be*. vragen naar *research.odisee.be*.
 4. Aan *research.odisee.be* vragen naar host met naam *server*
- (iteratief)



Recursive name server

server.research.odisee.be.

Aan odisee.be vragen naar server.research.odisee.be

- Gaat zelf op zoek naar het concreet gevraagde domein
- Refereert niet door naar research.odisee.be

Caching name server

- DNS lookups kunnen ook gecached worden
- Voordelen
 - Niet telkens root servers raadplegen => minder belasting
 - Minder netwerkverkeer
 - Snellere response
- Caching altijd beperken in de tijd om kans op verouderde gegevens te beperken
- Ook caching op de host of in programma's

Authoritative server

- De DNS-server heeft een **volledige kopie** van de domein-informatie
- Een volledige kopie betekent:
 - Een correct SOA-record (SOA = Start of Authority)
 - Correcte NS-records voor het domein (NS = Name Server)
 - De NS records moeten overeen komen met die in het SOA-record
 - **In de parent DNS-server moet een NS-record bestaan naar de server!!**
- Primaire of Secundaire DNS-server (zie later)
- Dus de “originele” data voor het domein

Een client kan op die manier een Authoritative of non-Authoritative antwoord krijgen van een DNS-server. In dat laatste geval kreeg de client het antwoord van een DNS-server die de “oplossing” gecached had, dus niet de originele DNS-server verantwoordelijk voor het domein.

NSLOOKUP Voorbeeld



```
C:\>nslookup
Default Server:  Unknown
Address:  10.132.1.5

> google.com
Server:      Unknown
Address:     10.132.1.5

Non-authoritative answer:
Name:   google.com
Addresses:  2a00:1450:400e:80a::200e
           172.217.20.78

>
```

Geen argumenten
Standaard DNS
server gebruikt

Gebruikte DNS server

NSLOOKUP Voorbeeld



```
C:\>nslookup - 10.132.1.5
```

```
Default Server: UnKnown
```

```
Address: 10.132.1.5
```

```
> set type=NS
```

```
> student.odisee.be
```

```
Server: UnKnown
```

```
Address: 10.132.1.5
```

DNS server gebruikt
om de gegevens op
te zoeken

student.odisee.be	nameserver = dcdm0003.hubkaho.be
student.odisee.be	nameserver = dcdm0004.hubkaho.be
student.odisee.be	nameserver = dcdm0001.hubkaho.be
student.odisee.be	nameserver = dcdm0002.hubkaho.be
dcdm0003.hubkaho.be	internet address = 10.101.6.3
dcdm0004.hubkaho.be	internet address = 10.101.6.4
dcdm0001.hubkaho.be	internet address = 10.143.1.3
dcdm0002.hubkaho.be	internet address = 10.143.1.4

NSLOOKUP Voorbeeld



```
student@debian:~$ nslookup - 10.132.1.5
```

```
> set type=NS
```

```
> student.odisee.be
```

```
Server:          10.132.1.5
```

```
Address:         10.132.1.5#53
```

DNS server gebruikt
om de gegevens op
te zoeken

```
student.odisee.be      nameserver = dcdm0001.hubkaho.be.
```

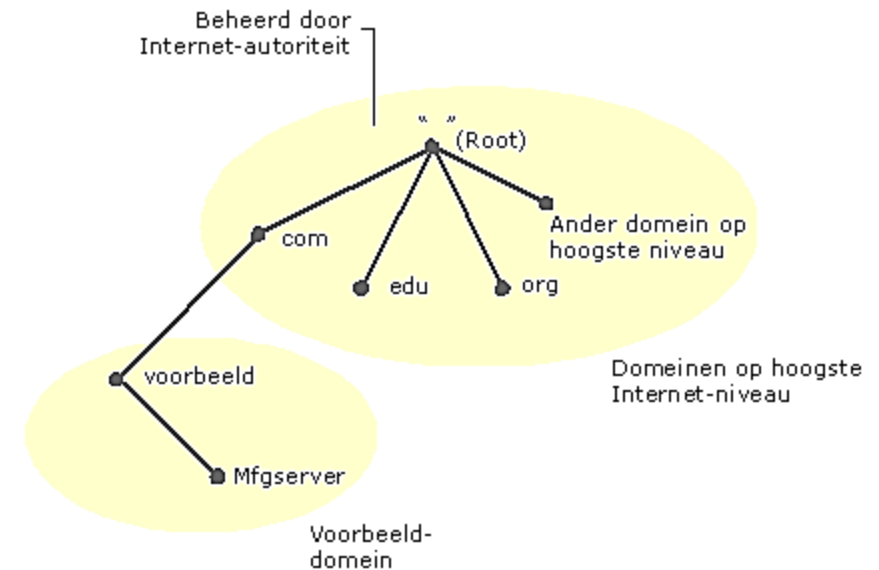
```
student.odisee.be      nameserver = dcdm0002.hubkaho.be.
```

```
student.odisee.be      nameserver = dcdm0003.hubkaho.be.
```

```
student.odisee.be      nameserver = dcdm0004.hubkaho.be.
```

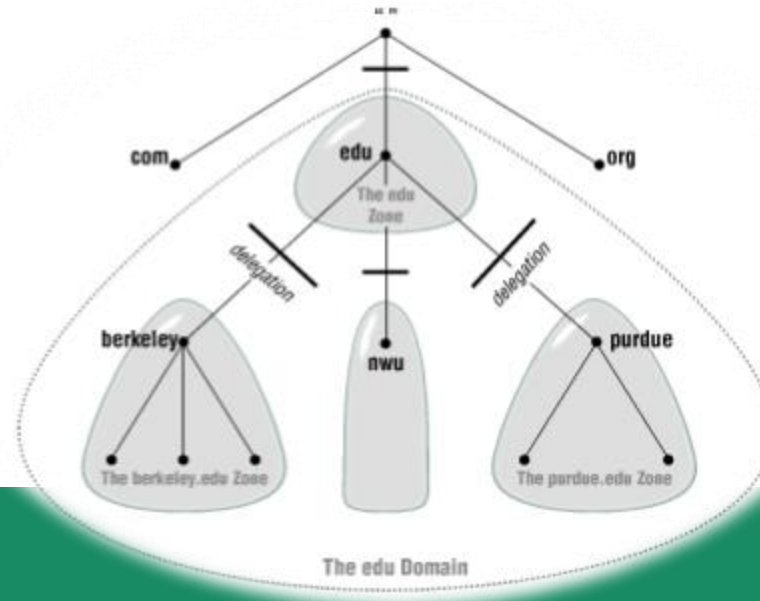
Zones

- Een zone is een groep van adressen waarvoor een DNS-server verantwoordelijk (authoritative) is binnen een bepaalde namespace
- Meestal komt een zone overeen met een domein, maar dat hoeft niet
- Vb: de domeinen "mfgserver.voorbeeld.com." en "voorbeeld.com." zitten in eenzelfde zone als ze door eenzelfde DNS-server samen beheerd worden
- Dit betekent dat er ook maar 1 zone-file (zie later) zal gemaakt worden voor deze beide domeinen



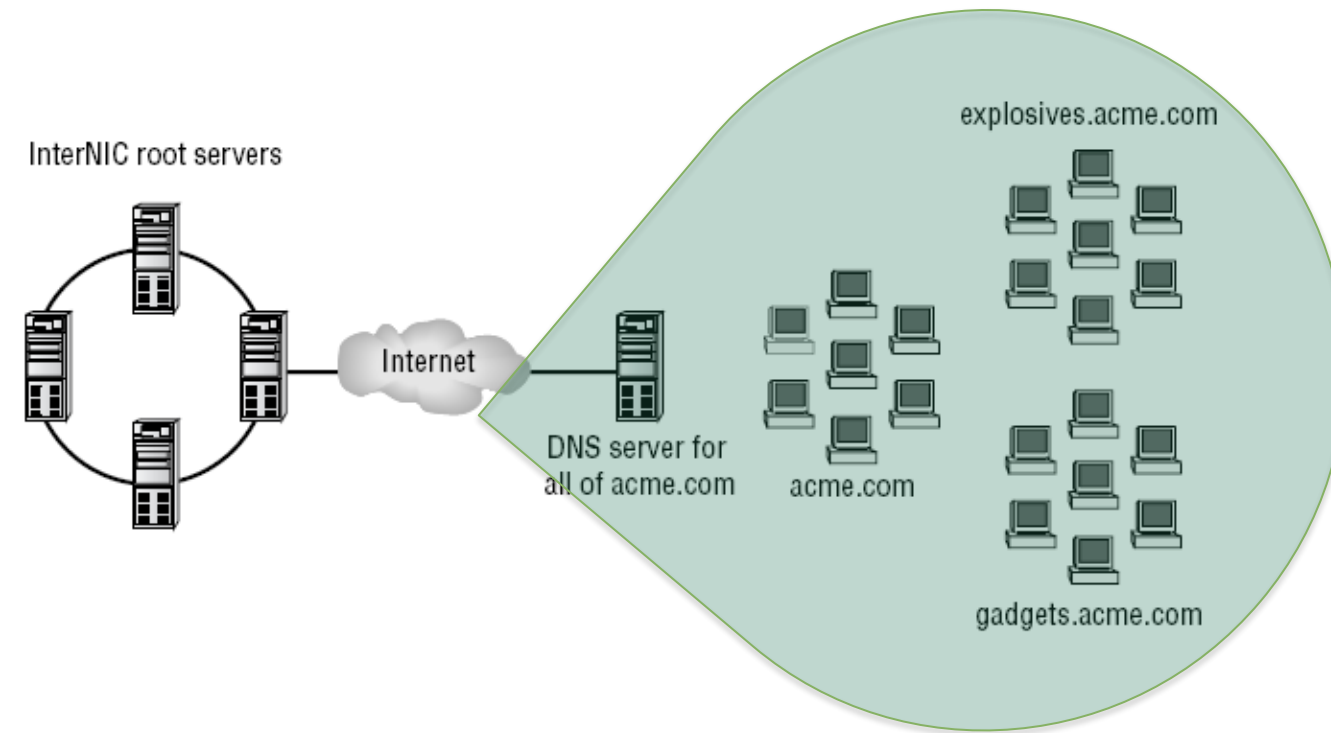
Zones

- Indien verschillende subdomeinen niet in eenzelfde zone zitten, dan moeten die subzones **gedelegeerd** worden.
- Dit betekent dat er in het “parent” domein een **verwijzing** gemaakt wordt **naar de DNS-server die verantwoordelijk is voor die subzone**.

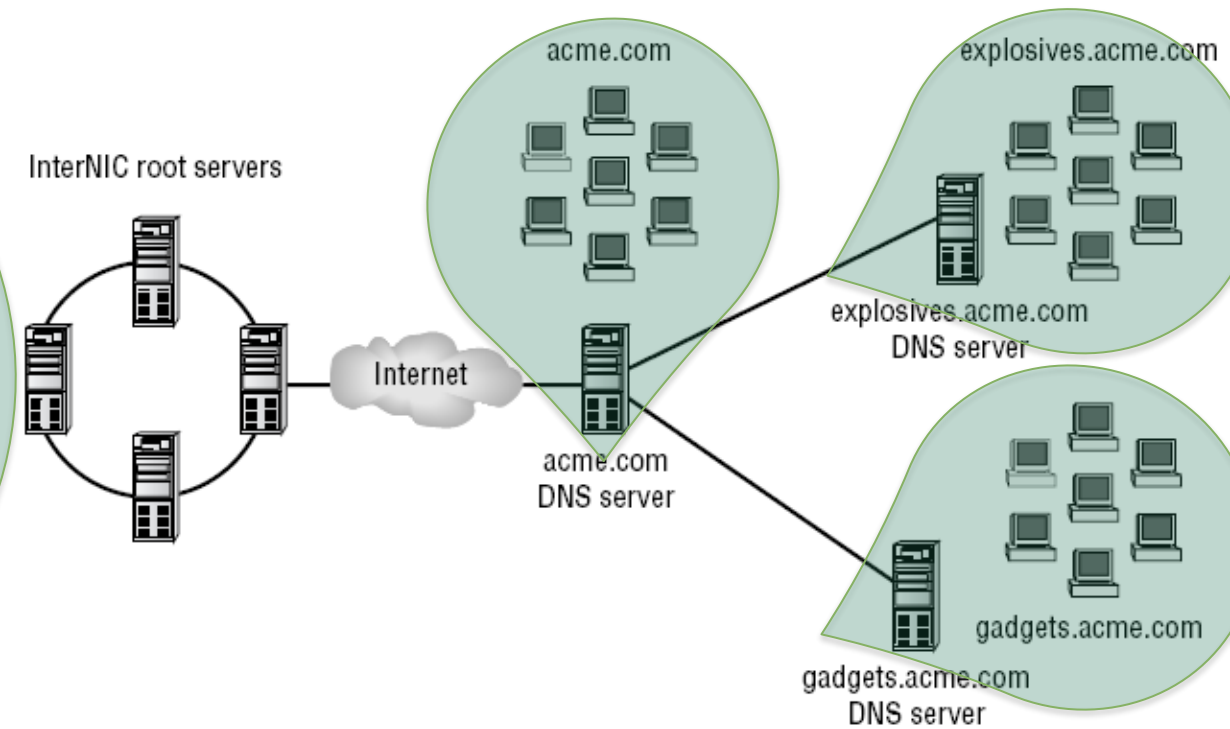


Zones

Zonder delegatie => 1 zone



Met delegatie => 3 zones



Soorten Zones

- Forward Lookup Zones
 - Zorgen voor vertaling van hostnaam naar IP-adres.
(vb: wat is IP-adres van "pop.odisee.be."?)
 - Adhv records die services aangeven: resource records
(vb A, CNAME, MX, NS, ...)
- Reverse Lookup zones
 - Zorgen voor vertaling van IP-adres naar hostnaam.
(vb: wat is de FQDN van 10.10.10.1?) (Nut!?) (nu veel gebruikt voor security in mailservers)
 - Adhv PTR-records
 - Naming convention:
 <first octets of the ip address (reversed)>.in-addr.arpa
 vb ip adres 205.133.113.87/24 ==> 113.113.205.in-addr.arpa
 vb ip adres 164.190.0.15/16 ==> 190.164.in-addr.arpa

Soorten zones

- Stub zones
 - Zone met enkel SOA, NS en een A-record van een autoritatieve zone.
 - Gebruikt om sneller een DNS-resolving uit te voeren.
 - Vb: op de DNS-server van domein mijnfirma.be. kan een stub-zone gemaakt worden voor het domein uwfirma.be. Dit heeft als gevolg dat de DNS-server onmiddellijk weet wie autoritativ is voor de zone.
 - Wordt bv. gebruikt bij fusie van 2 bedrijven

DNS Server ROLLEN

- **Primaire DNS-server**
 - Is de enige server waar de inhoud van de zone-file kan gewijzigd worden (toevoegen, verwijderen en aanpassen van records binnen een zone)
 - 1 enkele server kan maar primaire DNS-server zijn*
- **Secundaire DNS-server**
 - Alle servers die een kopie bevatten van de zone-file van de primaire DNS-server
 - Kunnen meerdere servers zijn
 - Enkel lezen!
- **Cache-only server**
 - Deze server bevat geen zone-informatie maar slaat succesvolle queries op voor toekomstige vragen van clients

(*) uitgez. Active Directory geïntegreerde zones
=> elke DC kan eenzelfde writable primary zone bevatten, deze synchroniseren onderling

DNS Server ROLLEN

- **DNS forwarder**
 - Geeft queries door aan een andere DNS-server op een recursieve manier
 - Bv: nodig in geval de DNS-server geen iteratieve queries kan uitvoeren door bv. firewallregel op poort 53

Records

- **A**

Adres-record : koppelt een ip-adres aan hostnaam (IPv4)

- **AAAA**

Adres-record: koppelt een ip-adres aan hostnaam (IPv6)

- **NS**

Name Server-record: geeft aan wat de DNS-servers zijn voor een domein (of subdomein bij delegatie)

- **SOA**

Start of Authority: bevat de naam van de primaire server, e-mailadres van verantwoordelijke, timers voor zone transfer, serieel nummer, Time-to-live (TTL)

Records

- **CNAME**

alias voor een bestaand ander record

- **MX**

Mail-exchange: deze records geven aan wat er moet gebeuren met mail voor dit domein. Meerdere records mogelijk met verschillende prioriteit.

- **SRV**

Server-records: met deze records kan je bepaalde services terugvinden die via TCP of UDP werken en binnen het domein leven (vb: kerberos, ldap, GC,...)
vb: `_kerberos._tcp.mijnbedrijf.be`.

- **PTR**

Pointer: gebruikt om IP-adres aan naam te koppelen. Voor reverse zones

Zone File

- Tekstbestand waarin de DNS-info opgeslagen wordt
- “@” vervangt de domeinnaam, kan ook leeg
- FORWARD ZONE:

NS, MX, SOA: leeg!!



```
$TTL 86400
@      IN SOA  mailer.hansenonline.net.  hostmaster.hansenonline.net. (
                                2003060919;  serial
                                21600;        refresh every 6 hours
                                3600;         retry after one hour
                                604800;       expire after a week
                                86400 );      minimum TTL of 1 day

                                IN      NS      mailer.hansenonline.net.
                                IN      MX      10      mailer.hansenonline.net.

mailer      IN      A      192.168.33.11
firewall    IN      A      192.168.33.1
switch      IN      A      192.168.33.3
replaytv    IN      A      192.168.33.200

cisco       IN      CNAME   switch
www         IN      CNAME   mailer
mrtα       IN      CNAME   mailer
```

Zone File

- REVERSE ZONE:
192.168.33.x/24

```
$TTL 86400
@      IN SOA      mailer.hansenonline.net.  hostmaster.hansenonline.net. (
                                0306190719      ; serial
                                21600             ; refresh after 6 hours
                                3600             ; retry in 1 hour
                                604800          ; expire after a week
                                86400 )         ; minimum TTL of one day

                                IN      NS      mailer.hansenonline.net.

1      IN      PTR   firewall.hansenonline.net.
3      IN      PTR   switch.hansenonline.net.
11     IN      PTR   mailer.hansenonline.net.
200    IN      PTR   replaytv.hansenonline.net.
```

Timers



Moet de volledige
FQDN zijn

vermeulen.eu Properties

WINS	Zone Transfers	Security
General	Start of Authority (SOA)	Name Servers

Serial number:

Primary server:

Responsible person:

Refresh interval:

Retry interval:

Expires after:

Minimum (default) TTL:

ITL for this record: (DDDDD:HH.MM.SS)

time to live => de tijd dat
een record mag blijven
bestaan in de **caches** van
clients die een positieve
of negatieve vraag
stelden aan deze DNS-
server

om de hoeveel tijd een secundaire
server de primaire server zal bevragen
naar zone **updates**

de tijd dat de secundaire server **wacht**
na een **mislukte poging** voor een
zone update

hoelang een secundaire zone **geldig**
mag blijven indien deze de primaire
server **niet meer** kan **bereiken**

Zone Transfers

Naar wie mag een kopie van het zone bestand gestuurd worden?

- Any server
- Servers in Name Servers list
- IP-adressen opgeven

vermeulen.eu Properties

General Start of Authority (SOA) Name Servers
WINS Zone Transfers Security

A zone transfer sends a copy of the zone to the servers that request a copy.

☒ Allow zone transfers:

- ☐ To any server
- ☐ Only to servers listed on the Name Servers tab
- ☒ Only to the following servers

IP Address	Server FQDN
192.168.1.2	<Unable to resolve>

Edit

To specify secondary servers to be notified of zone updates, click Notify.

Notify...

OK Cancel Apply Help

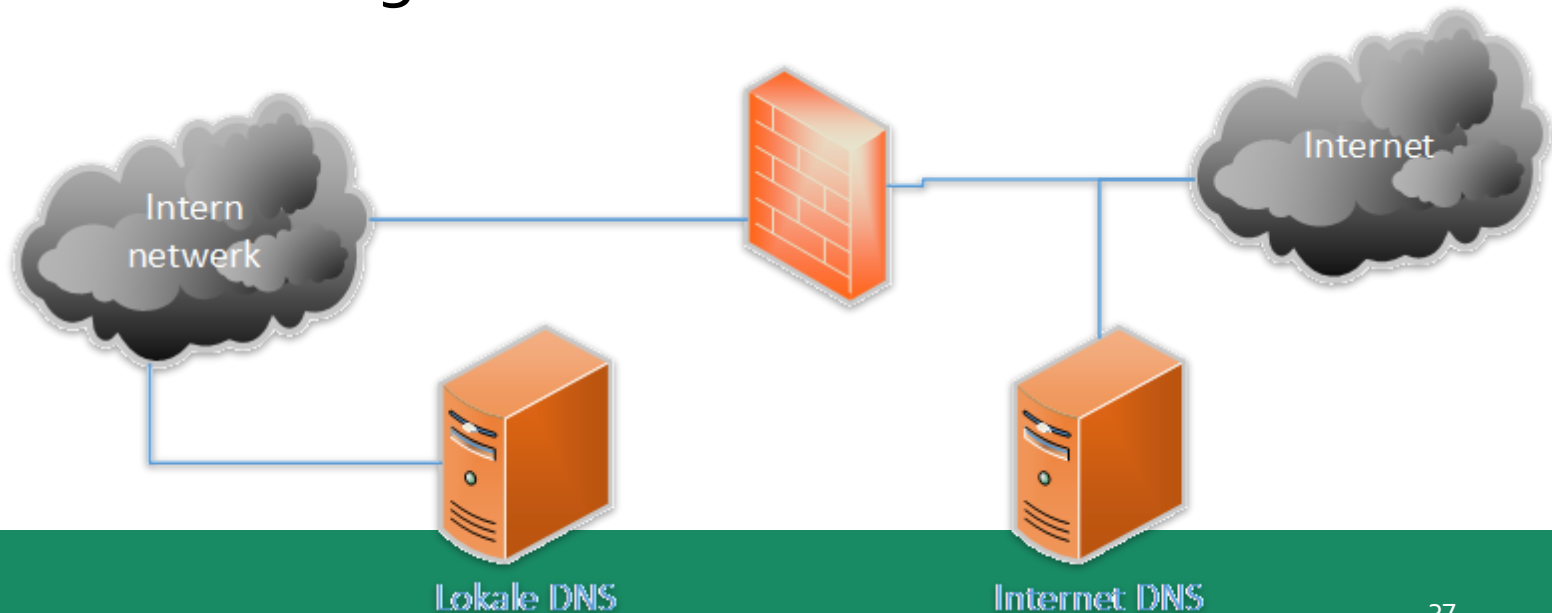
Round Robin

“Cheap Cluster” (Load Balancing/distribution met A-records)

- Meerdere servers met zelfde functionaliteit (vb 3 x webserver)
- Bij elke DNS request A-records permuteren
- clients krijgen alle records in verschillende volgorde
- Meeste clients nemen altijd eerste uit de lijst
- Gevolg: de belasting wordt over de verschillende servers gedeeld
- Probleem: caching werkt dit tegen

Split brain

- Locale en Internet DNS server
- Gescheiden door firewall
- Locale server voor interne aanvragen
- Internet server voor externe aanvragen
- Beide authoritative voor zelfde zone maar kunnen niet aan elkaar



TTL

Time To Live

- Niet te kort: belasting voor DNS server
- Niet te lang: foutieve informatie
- Bij aanpassing belangrijke gegevens: TTL tijdelijk lager zetten

DNS caching in Windows



```
Recordnaam . . . . . : www.bzn.be
Recordtype . . . . . : 1
Time-to-Live . . . . . : 75201
Gegevenslengte . . . . : 4
Sectie . . . . . : antwoord
A-record (host). . . . : 85.119.217.74
```

www.bondzondernaam.be

```
Recordnaam . . . . . : www.bondzondernaam.be
Recordtype . . . . . : 1
Time-to-Live . . . . . : 77037
Gegevenslengte . . . . : 4
Sectie . . . . . : antwoord
A-record (host). . . . : 85.119.217.74
```

www.dnstools.nl

```
Recordnaam . . . . . : www.dnstools.nl
Recordtype . . . . . : 1
Time-to-Live . . . . . : 248
Gegevenslengte . . . . : 4
Sectie . . . . . : antwoord
A-record (host). . . . : 81.26.219.100
```

```
Recordnaam . . . . . : ns1.dnstools.nl
Recordtype . . . . . : 1
Time-to-Live . . . . . : 248
Gegevenslengte . . . . : 4
Sectie . . . . . : aanvullend
A-record (host). . . . : 81.26.219.100
```

`ipconfig /displaydns`

`ipconfig /flushdns`

DNS caching in Linux













- Standaard geen OS-level caching
- Wel application-level caching (bv in browsers)
- OS-level caching mogelijk met nscd (name service cache daemon)
- Of lokaal een caching DNS server installeren en die gebruiken als DNS server

Tools

Interessante online tools

- <http://www.intodns.com/odisee.be>
- <http://www.dnssniffer.com>

Work in progress!
Follow IntoDNS on [Twitter](#)

Category	Status	Test name	Information	send feedback
Parent		Domain NS records	Nameserver records returned by the parent servers are: ns1.odisee.be. ['193.190.225.18'] [TTL=86400] ns2.odisee.be. ['193.190.225.19'] [TTL=86400] x.ns.dns.be was kind enough to give us that information.	
		TLD Parent Check	Good. x.ns.dns.be, the parent server I interrogated, has information for your TLD. This is a good thing as there are some other domain extensions like "co.us" for example that are missing a direct check.	
		Your nameservers are listed	Good. The parent server x.ns.dns.be has your nameservers listed. This is a must if you want to be found as anyone that does not know your DNS servers will first ask the parent nameservers.	
		DNS Parent sent Glue	Good. The parent nameserver sent GLUE, meaning he sent your nameservers as well as the IPs of your nameservers. Glue records are A records that are associated with NS records to provide "bootstrapping" information to the nameserver.(see RFC 1912 section 2.3)	
		Nameservers A records	Good. Every nameserver listed has A records. This is a must if you want to be found.	
NS		NS records from your nameservers	NS records got from your nameservers listed at the parent NS are: ns2.odisee.be ['193.190.225.19'] [TTL=3600] ns1.odisee.be ['193.190.225.18'] [TTL=3600]	
		Recursive Queries	Good. Your nameservers (the ones reported by the parent server) do not report that they allow recursive queries for anyone.	
		Same Glue	The A records (the GLUE) got from the parent zone check are the same as the ones got from your nameservers. You have to make sure your parent server has the same NS records for your zone as you do according to the RFC. This tests only nameservers that are common at the parent and at your nameservers. If there are any missing or stealth nameservers you should see them below!	
		Glue for NS records	OK. When I asked your nameservers for your NS records they also returned the A records for the NS records. This is a good thing as it will spare an extra A lookup needed to find those A records.	
		Mismatched NS records	OK. The NS records at all your nameservers are identical.	

BIND



- Berkeley Internet Name Domain
- Meest gebruikte DNS-software
- Daemon + tools
 - nslookup
 - host
 - dig
- OS: Linux, NetBSD, FreeBSD, OpenBSD, OS X, Windows
- Configuratiefiles (locaties voor CentOS)
 - /etc/named.conf ➡ algemene instellingen
 - /etc/named/named.conf.local ➡ forward en reverse zone verwijzingen
 - /var/named/* ➡ zone files



Beveiligingsbedrijf ontdekt trojan die communiceert via dns

Door Sander van Voorst, vrijdag 3 maart 2017 19:49, 96 reacties • [Feedback](#)

De Talos-onderzoeksafdeling van Cisco heeft malware geanalyseerd die via dns communiceert. De zogenaamde Dnsmessenger-trojan kan zo PowerShell-scripts opvragen uit de txt-record om detectie te voorkomen.

In de analyse [schrijven](#) de onderzoekers dat de trojan op deze manier communiceert met de c2-server van de aanvallers. De malware is opvallend, omdat deze variant vergaande stappen neemt om verborgen te blijven. De trojan wordt verspreid door middel van een geïnfecteerd Word-document, dat de indruk wekt beveiligd te zijn met software van McAfee. Het bestand kan bijvoorbeeld door een phishing-e-mail naar een bepaald doelwit worden gestuurd.

De malware werkt met PowerShell om een *backdoor* aan te brengen in het systeem van het slachtoffer. Om dat te bereiken, controleert de kwaadaardige software eerst of er beheerderstoegang is en welke versie van PowerShell op het systeem draait. In de volgende fase maakt de Dnsmessenger-trojan gebruik van een willekeurige voorgeprogrammeerde domeinnaam voor dns-verzoeken. Door middel van het ophalen van de txt-record is het voor de aanvallers mogelijk om de trojan van verschillende commando's te voorzien.

De in de txt-records opgenomen PowerShell-commando's laten de aanvaller op die manier Windows-functies op het geïnfecteerde systeem aansturen. Ook is het mogelijk de gegenereerde output van applicaties vervolgens weer terug te sturen via een dns-verzoek. Volgens de onderzoekers is een dergelijke aanval moeilijk te detecteren, omdat organisaties vaak geen filters gebruiken voor dns. Daardoor is deze techniek geschikt voor doelgerichte aanvallen.

MMConsole - [Console Root\DNS\S1\Forward Lookup Zones\vermeulen.eu]

File Action View Favorites Window Help

Console Root

- Event Viewer (Local)
- DNS
 - S1
 - Global Logs
 - Forward Lookup Zones
 - vermeulen.eu
 - Reverse Lookup Zones
 - Trust Points
 - Conditional Forwarders

Name	Type	Data	Actions
(same as parent folder)	Start of Authority (SOA)	[1], S1.vermeulen.eu., host...	vermeulen.eu
(same as parent folder)	Name Server (NS)	S1.vermeulen.eu.	More Actions
S1	Host (A)	192.168.1.1	

Update Server Data File

Reload

New Host (A or AAAA)...

New Alias (CNAME)...

New Mail Exchanger (MX)...

New Domain...

New Delegation...

Other New Records...

DNSSEC

All Tasks

Refresh

Export List...

View

Arrange Icons

Line up Icons

Properties

Help

Resource Record Type

Select a resource record type:

- Route Through (RT)
- Service Location (SRV)
- Signature (SIG)
- Text (TXT)
- Well Known Services (WKS)
- X.25

Description:

Text (TXT) record. Holds a string of characters that serves as descriptive text to be associated with a specific DNS domain name. The semantics of the actual descriptive text used as data with this record type depends on the DNS domain where these records are located. (RFC 1035)

Create Record... Cancel

New Resource Record

Text (TXT)

Record name (uses parent domain if left blank):

Fully qualified domain name (FQDN):

Text:

OK Cancel

Bronnen

- Round Robin - https://en.wikipedia.org/wiki/Round-robin_DNS
- De cursustext op Toledo