Hadrien Barral
Rémi Géraud-Stewart
Amaury Barral
David Naccache

École normale supérieure @ PSL University / QPSI @ Qualcomm Technologies Inc.

DNSSECTION

What is this about

- An e-mail privacy breach in the largest French cloud provider
- The first practical attack based on DNSSEC zone walking
- A cautionary tale about hash functions

Why this matters

- DNS is everywhere, tons of potentially interesting data
- Zone walking has never been demonstrated in the wild before

Who we are

- Hadrien Barral — Ecole Normale Supérieure / PSL University
- Rémi Géraud-Stewart, Ph.D, — ENS/PSL, QPSI @ Qualcomm
- This is our second Defcon talk!

Done in collaboration with Amaury Barral and David Naccache.

1. Who's behind skytalks-vidz.com?

DNS 101

DNS: Domain Name System

- Naming system for remote resources
- Distributed database system (NOT a blockchain ffs)
- Contains Resource Records (RR) and domain names
- Resolver: figures out the translation of a domain name into an IP address
- Zones: subtrees maintained by different people

Registrars and domain services 101

Scenario: you want to create a new website:

- Buy a computer
- Pay for Internet access
- Pay someone to design a fancy website running on your server
- Pay a registrar to get the domain name you want
- Pay someone to run DNS servers that connect the domain name to your server's IP
- Pay someone to maintain all of this

All-in-one: cloud hosting!

OVHcloud

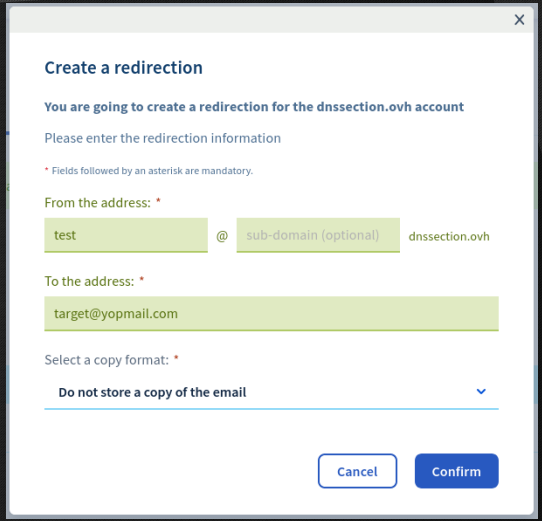
- Largest French cloud provider (2nd in Europe)
- They also sell domains
- And e-mail redirects with that

(and they host Wikileaks since 2010, just fyi)

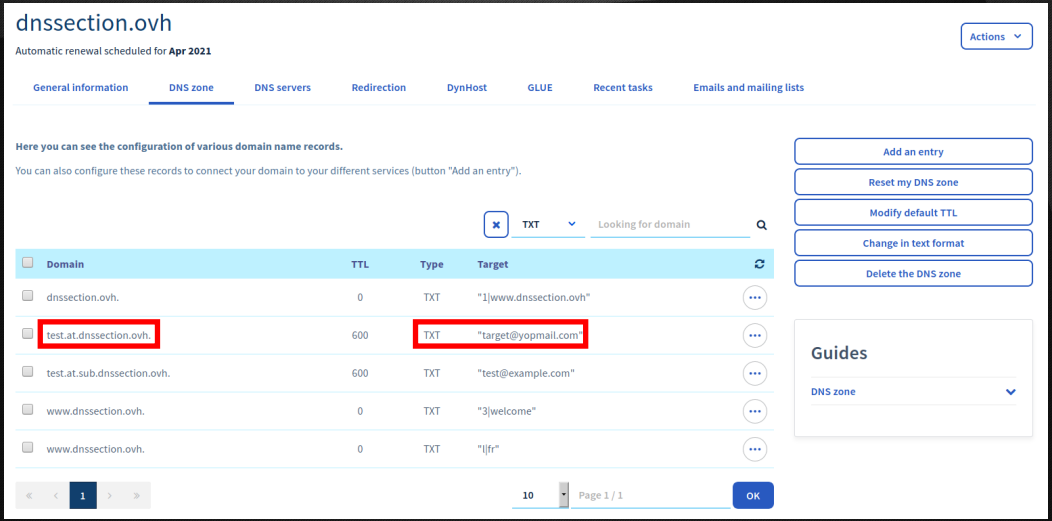
E-mail redirects at OVHcloud

From: test@dnssection.ovh →

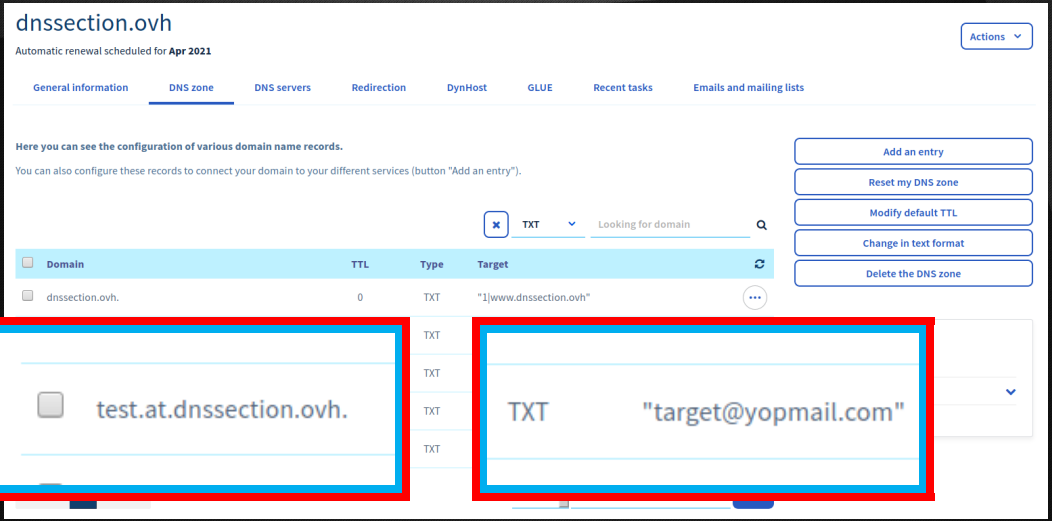
To: target@yopmail.com →



E-mail redirects at OVHcloud



E-mail redirects at OVHcloud



What harm can we do?

- Assume we access the redirection database...

What harm can we do?

- Assume we access the redirection database...
- Loads of client information: names, e-mails, billing,...

What harm can we do?

- Assume we access the redirection database...
- Loads of client information: names, e-mails, billing,...

A few ideas pop to mind:

- Spam?
- Password dumps?
- Targeted attacks?
- Find weak hosts/email providers?
- Ammo for social engineering?
- Blackmail?
- Phishing?
- Lawsuits?
- Business recon?
- ...

Sudo bruteforce

Sudo bruteforce

- Get a list of OVHcloud-handled domains

Sudo bruteforce

- Get a list of OVHcloud-handled domains
- Get a sublist of interesting domains and DNS query them (♡ `commoncrawl.org`)
  - Works fine for `.fr`, `.ovh`, less so for `.com`...

Sudo bruteforce

- Get a list of OVHcloud-handled domains
- Get a sublist of interesting domains and DNS query them (♡ `commoncrawl.org`)
  - Works fine for `.fr`, `.ovh`, less so for `.com`...
- Get redirection records for public emails (bear with us)
  - aka the emails we found on the webpage

Sudo bruteforce

- Get a list of OVHcloud-handled domains
- Get a sublist of interesting domains and DNS query them (♡ `commoncrawl.org`)
  - Works fine for `.fr`, `.ovh`, less so for `.com`...
- Get redirection records for public emails (bear with us)
  - aka the emails we found on the webpage
- Bruteforce associated DNS queries for usual e-mail addresses

`{abuse, admin, contact}@example.com`

How to do this in practice

- Do not get banned by the DNS server

How to do this in practice

- Do not get banned by the DNS server: Rate limiting $\rightarrow$ several IPs

How to do this in practice

- Do not get banned by the DNS server: Rate limiting $\rightarrow$ several IPs
- Low-tech version

How to do this in practice

- Do not get banned by the DNS server: Rate limiting $\rightarrow$ several IPs
- Low-tech version: `bash` + `dig` + filesystem

How to do this in practice

- Do not get banned by the DNS server: Rate limiting → several IPs
- Low-tech version: `bash` + `dig` + filesystem

```
while read DOMAIN; do
  dig mx "${DOMAIN}"     > "./save/mx/${DOMAIN}"
  dig    "at.${DOMAIN}" > "./save/at/${DOMAIN}"
done < "domain_list.txt"
```

How to do this in practice

- Do not get banned by the DNS server: Rate limiting → several IPs
- Low-tech version: `bash` + `dig` + filesystem

```
while read DOMAIN; do
  dig mx "${DOMAIN}"     > "./save/mx/${DOMAIN}"
  dig    "at.${DOMAIN}" > "./save/at/${DOMAIN}"
done < "domain_list.txt"
```

```
while read DOMAIN; do
  for NAME in "abuse" "admin" "contact" ...; do
    EMAIL="${NAME}.at.${DOMAIN}"
    dig TXT "${EMAIL}" +noall +answer | grep "${EMAIL}.*IN.TXT"
  done
done < "interesting_domain_list.txt"
```

Demo

Lookie here

- It works!
- Considering 14.000 potentially vulnerable domains (mostly `.fr` TLD),

Lookie here

- It works!
- Considering 14.000 potentially vulnerable domains (mostly `.fr` TLD),
- We found about 15.000 email redirects
- With about 10.000 unique target emails

Lookie here

- It works!
- Considering 14.000 potentially vulnerable domains (mostly `.fr` TLD),
- We found about 15.000 email redirects
- With about 10.000 unique target emails

Using public emails, we found (private) redirection emails!

Lookie here

- It works!
- Considering 14.000 potentially vulnerable domains (mostly `.fr` TLD),
- We found about 15.000 email redirects
- With about 10.000 unique target emails

Using public emails, we found (private) redirection emails!

What are we NOT seeing?

2. Stepping up: DNSSECTION

DNSSEC 101

- DNSSEC could be the topic of an entire talk
- Here's what you should know:
  - DNS is famously insecure, needed some fix
  - DNSSEC supported by every "good" modern device
  - Root of trust + tree derivation scheme
  - Meant to ensure authenticity (not privacy)
- Sometimes require lockpicking skills

Recent DNSSEC key rollover session

Demo

DNSViz

The issue with negative responses

- Authenticating "`example.com` is at `1.2.3.4`" is easy
- Authenticating the absence of "`bad.example.com`" record is ... trickier
- We obviously cannot put every negative possibility in the zone!
- `NSEC` to the rescue

Authenticated denial of existence

- Principle:
  - NSEC signs "there is no domain between
    `apple.example.com` and `carrot.example.com`"
  - Therefore `bad.example.com` does not exist

Zonewalking with NSEC

- But now we can enumerate all records!

Zonewalking with NSEC

- But now we can enumerate all records!
  - Pick a random name: "`fgfrd.example.com`"
  - Query the DNS server.

    Answer: nothing between "`carrot.example.com`" and "`good.example.com`"
  - Repeat with "`gooda.example.com`"
  - We do this until we loop, at which point we're done!

NSEC is already obsolete

- Did you think that's what we were about to do?... guess again!
- NSEC zone walking does not work in the real world anymore!
- Indeed, NSEC is almost not used anymore (sad reacts only)

Zone walking with NSEC3

- NSEC3 (RFC6781, RFC5155)

  "The first motivation to deploy NSEC3 *– prevention of zone enumeration (...)"*

- NSEC3 in a nutshell: $\texttt{SHA1}^{k}(\texttt{domain})$ (almost universally)
  - Intuition: same as NSEC but with hashed values instead of real names
  - Should hide the contents (assuming you can't do anything with hash values)
  - We can still dump the SHA1 hash itself, so ZW still kinda works

- NSEC3 is what is deployed in the real world currently!

So let's attack that :)

Zone walking with NSEC3

Assumption: reversing even partially the hash is difficult.

Zone walking with NSEC3

Assumption: reversing even partially the hash is difficult.

(*Laughs in Bitcoin mining farm*)

Zone walking with NSEC3

Assumption: reversing even partially the hash is difficult.

(*Laughs in Bitcoin mining farm*)

Reality: There are multiple off-the-shelf tools to crack NSEC3 hashes.

To the best of our knowledge, never been used to dig valuable data

Demo

nsec3walker

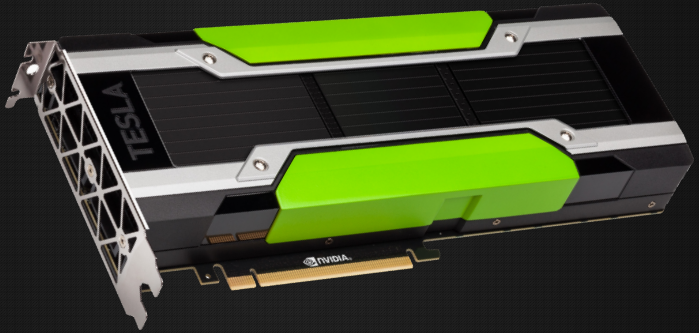
Sudo GPU bruteforce

Bringing out the GPU rig!!!

Sudo GPU bruteforce

Bringing out the GPU rig!!!

JK, we "only" have this:



Demo

hashcat

Results

Let’s consider 16.000 interesting DNSSEC hashed records

Results

Let's consider 16.000 interesting DNSSEC hashed records
Un-hashed 20% of them

Results

Let's consider 16.000 interesting DNSSEC hashed records
Un-hashed 40% of them

Results

Let's consider 16.000 interesting DNSSEC hashed records
Un-hashed 55% of them

Results

Let's consider 16.000 interesting DNSSEC hashed records
Un-hashed 66% of them

Results

Let's consider 16.000 interesting DNSSEC hashed records
Un-hashed 72% of them

Results

Let's consider 16.000 interesting DNSSEC hashed records
Un-hashed 80% of them

Results

Let's consider 16.000 interesting DNSSEC hashed records
Un-hashed 85% of them

Results

Let's consider 16.000 interesting DNSSEC hashed records
Un-hashed 88% of them

Results

Let's consider 16.000 interesting DNSSEC hashed records
Un-hashed 88% of them

Results breakdown

- 75%: reversed the hash, found an interesting email redirection
- 13%: reversed the hash, found something else
- 12%: unhash failed (sad face)

Results

Let's consider 16.000 interesting DNSSEC hashed records
Un-hashed 88% of them

Results breakdown

- 75%: reversed the hash, found an interesting email redirection
- 13%: reversed the hash, found something else
- 12%: unhash failed (sad face)

Let's look into the data !

3. All your data are belong to us

Disclaimer

- We are not here to doxx people
- All people names and domain names in the following examples have been modified

With that in mind, let's dig into the data and tell you what we found :)

Some statistics

- Most webmasters' real addresses...

Some statistics

- Most webmasters' real addresses... @gmail.com

Some statistics

- Most webmasters' real addresses... @gmail.com
- Guessing name from email...

Some statistics

- Most webmasters' real addresses... @gmail.com
- Guessing name from email... about 50%

Some statistics

- Most webmasters' real addresses... @gmail.com
- Guessing name from email... about 50%
- Name couldn't be found on the website...

Some statistics

- Most webmasters' real addresses... @gmail.com
- Guessing name from email... about 50%
- Name couldn't be found on the website... about 66%

Some statistics

- Most webmasters' real addresses... @gmail.com
- Guessing name from email... about 50%
- Name couldn't be found on the website... about 66%
- Email wouldn't otherwise appear in a Google search...

Some statistics

- Most webmasters' real addresses... @gmail.com
- Guessing name from email... about 50%
- Name couldn't be found on the website... about 66%
- Email wouldn't otherwise appear in a Google search... about 45%

Some statistics

- Most webmasters' real addresses... @gmail.com
- Guessing name from email... about 50%
- Name couldn't be found on the website... about 66%
- Email wouldn't otherwise appear in a Google search... about 45%
- Identify business connections/conflict of interest/fake competitors...

Some statistics

- Most webmasters' real addresses... @gmail.com
- Guessing name from email... about 50%
- Name couldn't be found on the website... about 66%
- Email wouldn't otherwise appear in a Google search... about 45%
- Identify business connections/conflict of interest/fake competitors... about 23%

Some statistics

- Most webmasters' real addresses... @gmail.com
- Guessing name from email... about 50%
- Name couldn't be found on the website... about 66%
- Email wouldn't otherwise appear in a Google search... about 45%
- Identify business connections/conflict of interest/fake competitors... about 23%

Homework: how many of these email addresses have an entry in `haveibeenpwned.com`?

Can we use this power for "good"?

Try doxxing scam (and adult) websites!

Can we use this power for "good"?

Try doxxing scam (and adult) websites!

- Don’t tell my wife

Can we use this power for "good"?

Try doxxing scam (and adult) websites!

- Don’t tell my wife
- Fail: their email doesn’t disclose their names
- (but we still have the emails, who’s the scammer and who’s the scammee now!)

Anything... serious?

- Some famous peoples' emails (mentioned on Wikipedia)

Anything... serious?

- Some famous peoples' emails (mentioned on Wikipedia)
- A few personal emails of activists

Anything... serious?

- Some famous peoples' emails (mentioned on Wikipedia)
- A few personal emails of activists

- On a lighter note, a lawyer website with a redirect to...

Anything... serious?

- Some famous peoples' emails (mentioned on Wikipedia)
- A few personal emails of activists

- On a lighter note, a lawyer website with a redirect to...

my.little.pony.1xxx@gmail.com

Anything... serious?

- Some famous peoples' emails (mentioned on Wikipedia)
- A few personal emails of activists
- On a lighter note, a lawyer website with a redirect to...
  my.little.pony.1xxx@gmail.com
- ~50 redirects for `noreply@`. Really?

Caveat! Manual analysis

- We manually went through hundreds of websites, fishing for names and emails
  - Contact pages
  - Googling names and email addresses
  - Deal with obscene stuff such as Adobe Flash websites
  - ...
- This is all ‘best-effort’: aka we might have missed public data

Disclosure with OVHcloud

- We called the hotline

Disclosure with OVHcloud

- We called the hotline they said "send a mail to abuse@"

Disclosure with OVHcloud

- We called the hotline they said "send a mail to abuse@"
- First email, including technical details...

Disclosure with OVHcloud

- We called the hotline they said "send a mail to abuse@"
- First email, including technical details... no reply

Disclosure with OVHcloud

- We called the hotline they said "send a mail to abuse@"
- First email, including technical details... no reply
- Call the hotline again to confirm the process, which they do

Disclosure with OVHcloud

- We called the hotline they said "send a mail to abuse@"
- First email, including technical details... no reply
- Call the hotline again to confirm the process, which they do
- Second email...

Disclosure with OVHcloud

- We called the hotline they said "send a mail to abuse@"
- First email, including technical details... no reply
- Call the hotline again to confirm the process, which they do
- Second email... no reply

Disclosure with OVHcloud

- We called the hotline they said "send a mail to abuse@"
- First email, including technical details... no reply
- Call the hotline again to confirm the process, which they do
- Second email... no reply
- Get someone working there to ping the right person and forward...

Disclosure with OVHcloud

- We called the hotline they said "send a mail to abuse@"
- First email, including technical details... no reply
- Call the hotline again to confirm the process, which they do
- Second email... no reply
- Get someone working there to ping the right person and forward...

We're still waiting for a response :)

Fixing DNSSEC

- Use public-key cryptography (“DNSSEC white lies”, RFC 4470, 4471)
- Either NSEC5? (2014)
  - Initial draft had issues, met with skepticism, not final, not standardised...
  - Latency...
  - Bad track record for the NSEC family
- Or NSEC3 with digital signatures?
  - Today most DNS servers would use Algorithm13 i.e. ECDSA because of fast signing and wide support
  - Verification is slow... so there’s a burden on resolvers
  - Also requires proper management of keys and algorithms...

... experience shows that DNS servers are bad at it

→ `https://eprint.iacr.org/2015/1000.pdf`

Fixing my redirections

If you are an OVHCloud customer and use their redirections...

How do you protect yourself?

Fixing my redirections

If you are an OVHCloud customer and use their redirections...

How do you protect yourself?

- Protecting the target email is quite easy

Fixing my redirections

If you are an OVHCloud customer and use their redirections...

How do you protect yourself?

- Protecting the target email is quite easy
- Protecting the domain email list is more difficult...

666. Conclusion

Conclusion

- Do not store private info in your DNS Zone
- DNSSEC NSEC3 attacks are practical
- Push for NSEC5 or ECDSA-alg13 adoption!

That's all folks

Proof of concept on:

https://dnssection.ovh

Your friendly neighbourhood hackers

contact@dnssection.ovh