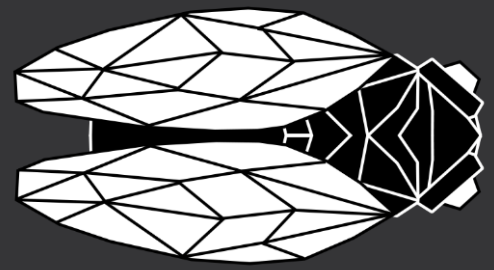
HackInProvence



Internationalized Domain Names…

…and its possible bad uses

fladnaG – Independent Trainer/Pentester
Hack in Provence staff – chiffrer.info – Twitter: @fladna9

Rule 1: don't say "crypter".
Rule 2: If you say "crypter" in front of me you owe me a beer.
Rule 3: When in doubt see Rule 1

Disclaimer

Does not exist IRL

- Don't have the dumbs.
- Please think twice about something you want to test.
- Jails are not that comfy.
- Remember that Justice don't care about motives or morale. It condamns for facts. And fact is that... it might be considered illegal in your country.
- So be smart 'bout this.
- This is NOT a point-and-shame presentation.
  - This technique is not prevalent yet, but seen a bit more each year.
  - The goal here is to demonstrate it can happen to anybody and see how we can protect ourselves from these attacks.

Plan

- Domain names
  - A bit of history
- What is IDN?
  - Punycode?
  - Let’s play a game :)
- In the wild
  - Some historical examples of IDN squatting in the wild
  - What about bad guys?
  - A bad idea later… my funny IDN squatting
  - Consequences
- How to patch/protec/prevent?

Domain names

A bit of history

Domain names – a bit of history

- Host names syntax (what was used before DNS, and still used today) can be traced back to January 1974, RFC 608: ***HOST NAMES ON-LINE.*** (feeling old yet ?)
  - <basic-part>.<attibute-item><eol>
    - <basic-part> is up to 48 chars, [A-Z0-9\-]+, no space and no blank chars. No case.
      - First char is a letter
      - Last char is not a –
  - <attribute-item>
    - SERVER, USER, TIP, UNKNOWN
  - <eol>
    - Well, End Of Line.
  - Shared via FTP, not very efficient…

Domain names – a bit of history

- Domain names syntax itself can be traced back to March 1982, RFC 810: ***DoD INTERNET HOST TABLE SPECIFICATION***
  - A « name » (Net, Host, Gateway, or **Domain name**) is a text string up to 24 chars, [A-Z0-9\-\.]+
    - No blank or space chars allowed.
    - No case.
    - First char must be a letter
    - Last char must not be a – or .

Domain names – a bit of history

- Domain Name Systems themselves dates back to November 1987, RFCs 1034 & 1035, **Domain names – concepts and facilities** and **Domain names – implementation and specifications.**
  - The domain name space is **a tree structure**. Each node and leaf on the tree corresponds to a resource set (which may be empty). The domain system makes no distinctions between the uses of the interior nodes and leaves, and this memo uses the term "node" to refer to both.
  - **Each node has a label, which is zero to 63 octets in length**. Brother nodes may not have the same label, although the same label can be used for nodes which are not brothers. One label is reserved, and that is the null (i.e., zero length) label used for the root.
  - **The domain name of a node is the list of the labels on the path from the node to the root of the tree**. By convention, the labels that compose a domain name are printed or read left to right, from the most specific (lowest, farthest from the root) to the least specific (highest, closest to the root).
  - By convention, **domain names can be stored with arbitrary case, but domain name comparisons for all present domain functions are done in a case-insensitive manner, assuming an ASCII character set**, and a high order zero bit. This means that you are free to create a node with label "A" or a node with label "a", but not both as brothers; you could refer to either using "a" or "A".
  - To simplify implementations, the total number of octets that represent a **domain name (i.e., the sum of all label octets and label lengths) is limited to 255**.

Domain names – TL;DR

- Domain names syntax is very old, and is a very restricted char set.
  - A-Z
  - 0-9
  - - and .
  - No case
  - And few more constraints (cannot start with . or -).

- With the current usage of technology, including Internet, many people from many countries with plenty of languages and alphabets made it through the Internet.
- So how to satisfy everybody and every language, allowing regional chars in domain names without breaking everything ?

What is IDN?

I DONUT NORMALIZE?
I DISTRUST NSA?

What is IDN?

- Since March 1998, researchers at Sigapore University was aware of the « all-ASCII » problem, and were looking for a solution.
- In July 1998, APNIC (Asia Pacific) creates a working group, iDNS.
- In 1999, some tests are done on asia pacific ccTLDs.
- Then IETF and ICANN get to work on this as well, on an planetary level.
- In 2000, An IDN working group is created.
- On March 2003 RFC 3454, 3490, 3491, 3492 are published.
- On June 2003, ICANN publishes its IDN guidelines.

What is IDN?

- Main pitch is:
- Without changing current Domain Names syntax, is there a way to add, encode some non-ASCII chars in current encoding?
- UNICODE seems a very good place for a start…

Punycode

It has UNYCODE in it, right?

Punycode (« code chétif » in french)

- Standardized in RFC 3492, ***Punycode: A Bootstring encoding of Unicode for Internationalized Domain Names in Application (IDNA)***
- Thanks to ***bootstring***, an algorithm design to encore Unicode characters in ASCII, we ***can*** name a domain with extended charsets.
  - Bootstrap properties:
    - Simple : algorithm is easy to implement.
    - Unique : there is only one way to encode Unicode to ASCII
    - Efficient : use as little space as possible.
    - Reversible : ASCII <- bootstring -> Unicode
    - Quick : quick to do, not power consuming
    - Readable : non Unicode ASCII chars must stay readable without Punycode

Punycode in IDNs

- Domain name **must** start with ***xn--*** to be registered as an IDN.
- Followed by ASCII chars part of the domain name, if any. Ended with a -, except if not any ASCII chars.
- Ending with ***<code>.tld***
- This ***<code>*** is about where to insert which char in the previous ASCII text, if any.

Punycode in IDNs - samples

Input in Unicode	Output in Punycode (missing xn--)
Lloyd-Atkinson	Lloyd-Atkinson-
This has spaces	This has spaces-
Bahnhof München-Ost	Bahnhof Mnchen-Ost-u6b
ドメイン名例	eckwd4c7cu47r2wf
MajiでKoiする5秒前	MajiKoi5-783gue6qz075azm5e
правда	80aafi6cg

Punycode

- Each TLD registry can choose to support all Unicode chars, or a subset of it.

- Example: .com registry: Verisign, inc.
  - Many Unicode sub-charsets allowed: latin, japanese, vietnamese, chinese, cyrillic, etc.

- Example: .fr registry: AFNIC
  - a, à, á, â, ã, ä, å, æ, b, c, ç, d, e, è, é, ê, ë, f, g, h, i, ì, í, î, ï, j, k, l, m, n, ñ, o, ò, ó, ô, õ, ö, œ, p, q, r, s, t, u, ù, ú, û, ü, v, w, x, y, ý, ÿ, z, ß, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, -
  - Restricted charset, but why ß? Or ü?

Punycode

- Each TLD registry can choose to support all Unicode chars, or a subset of it.

- Example: .com registry: Verisign, inc.
  - Many Unicode sub-charsets allowed: latin, japanese, vietnamese, chinese, cyrillic, etc.

- Example: .fr registry: AFNIC
  - a, à, á, â, ã, ä, å, æ, b, c, ç, d, e, è, é, ê, ë, f, g, h, i, ì, í, î, ï, j, k, l, m, n, ñ, o, ò, ó, ô, õ, ö, œ, p, q, r, s, t, u, ù, ú, û, ü, v, w, x, y, ý, ÿ, z, ß, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, -
  - Restricted charset, but why ß? Or ü?
    - Because of historical local languages (breton, alsacien, lorrain, basque, corse, gascon, provençal, etc.)

Punycode TL;DR

- Punycode: necessary for Unicode in domain names (as they were created for and by English speaking people) without breaking anything...
- ... it's a nice hack of an encoding problem!
- But what can be the problem about IDNs and Punycode encoding?
  - Best way to talk about this is by playing a game...

Let’s play a game

I have nothing to offer you if you win, FYI.

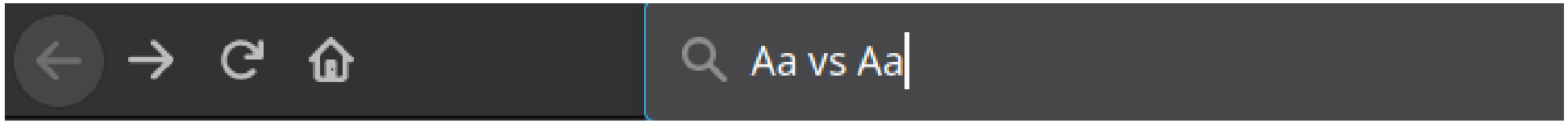
Rules

- Guess game
- 2 chars. 2 types. Guess which is which.
- Ready?

Round 1/5

- One is cyrillic, other is latin ASCII.
- Which is which?

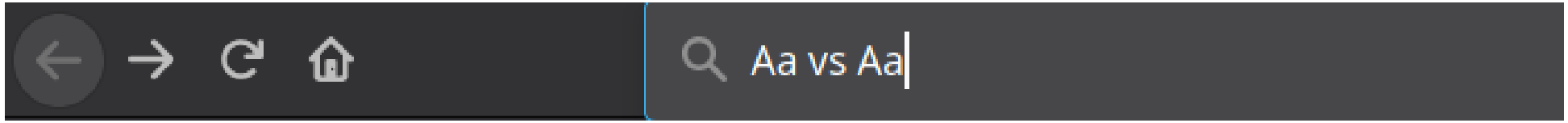
Aa vs Aa



Round 1/5

- One is cyrillic, other is latin ASCII.
- Which is which?

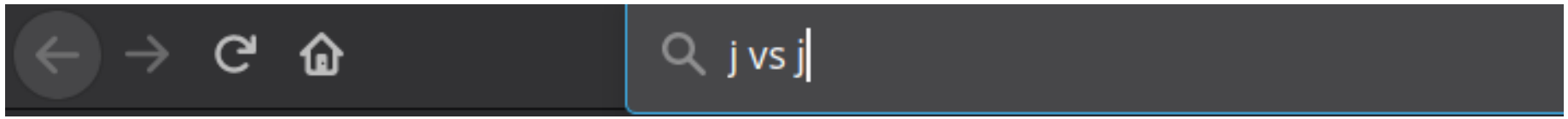
Aa (cyrillic) vs Aa scii



Round 2/5

- One is greek, other is latin ASCII.
- Which is which?

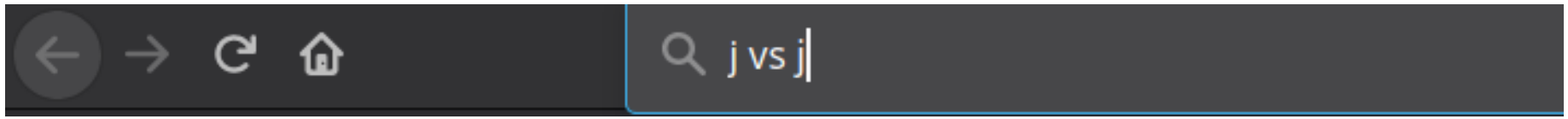
j vs j



Round 2/5

- One is greek, other is latin ASCII.
- Which is which?

j (greek) VS j (ASCII)



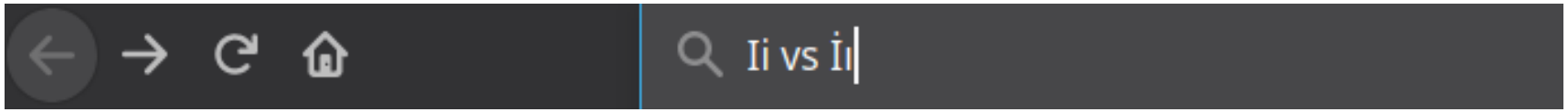
Round 3/5

- One is latin extended, other is latin ASCII.
- Which is which?

Round 3/5

- One is latin extended, other is latin ASCII.
- Which is which?

Ii (ASCII) vs İı (latin ext. A)



Round 4/5

- One is ASCII, other is thai.
- Which is which?

. VS .

Round 4/5

- One is ASCII, other is thai.
- Which is which?

. (thai) VS . (ASCII)

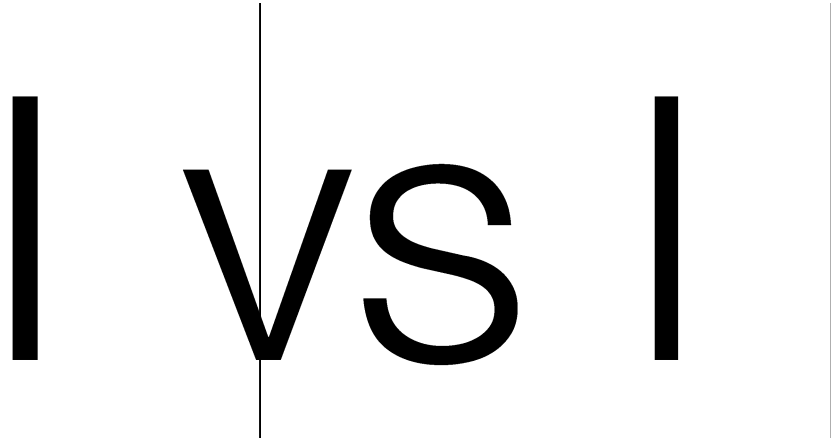
Round 4/5 - Bonus

- ฺ is Thai caracter ***phinthu***, and is a dead key and thus combinable with other chars.

j (thai) vs j (ASCII)

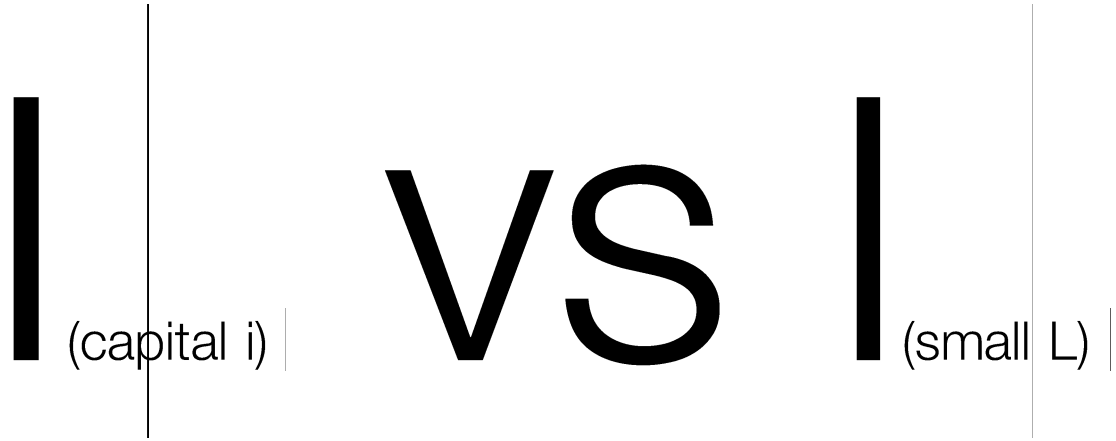
Round 5/5

- Easy folks, no help
- Which is what?



Round 5/5

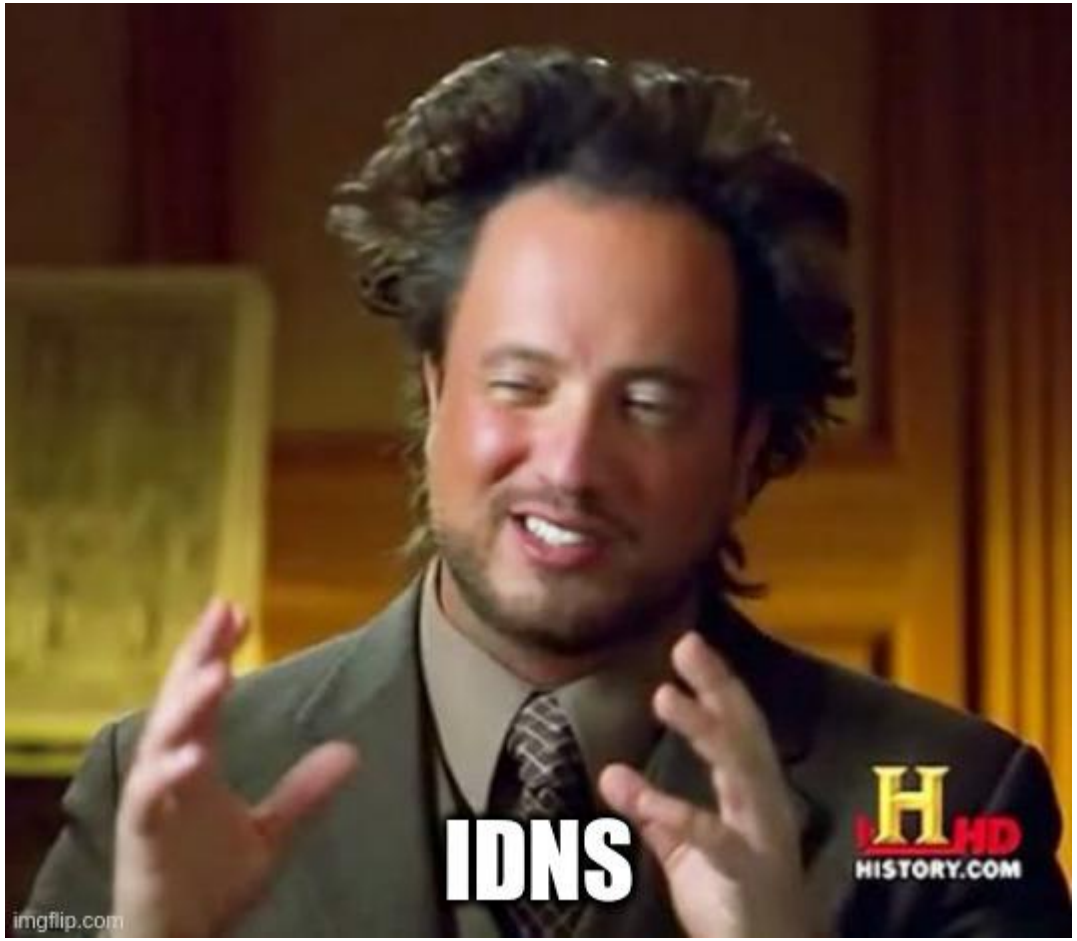
- Easy folks, no help
- Which is what?



Game TL; Didn’t play

- Sometimes hard/impossible to recognize one charset to the other.
- So, attacks possible? People know, watch and monitor this, right?

- And all users know that u and ü are differents...

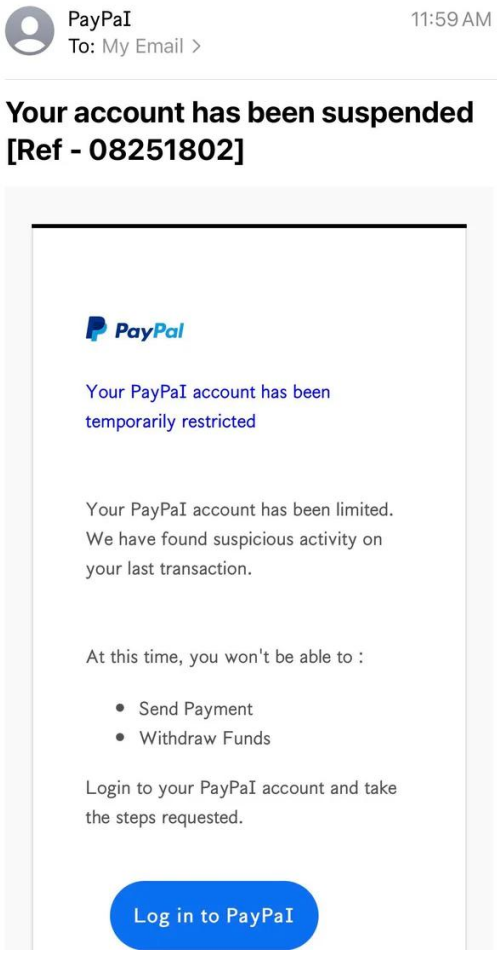


Some historical homograph attacks

What can go wrong?

PayPaI – not IDNs, but still homograph

- Look again ^ above ^, it is paypai (capital i)
- Created about mid-2000, then reused in 2011, 2012, 2017 and 2020.
- Phishing to get credentials.
- Website registered by Network Solutions, to a « Birykov » in Russia.



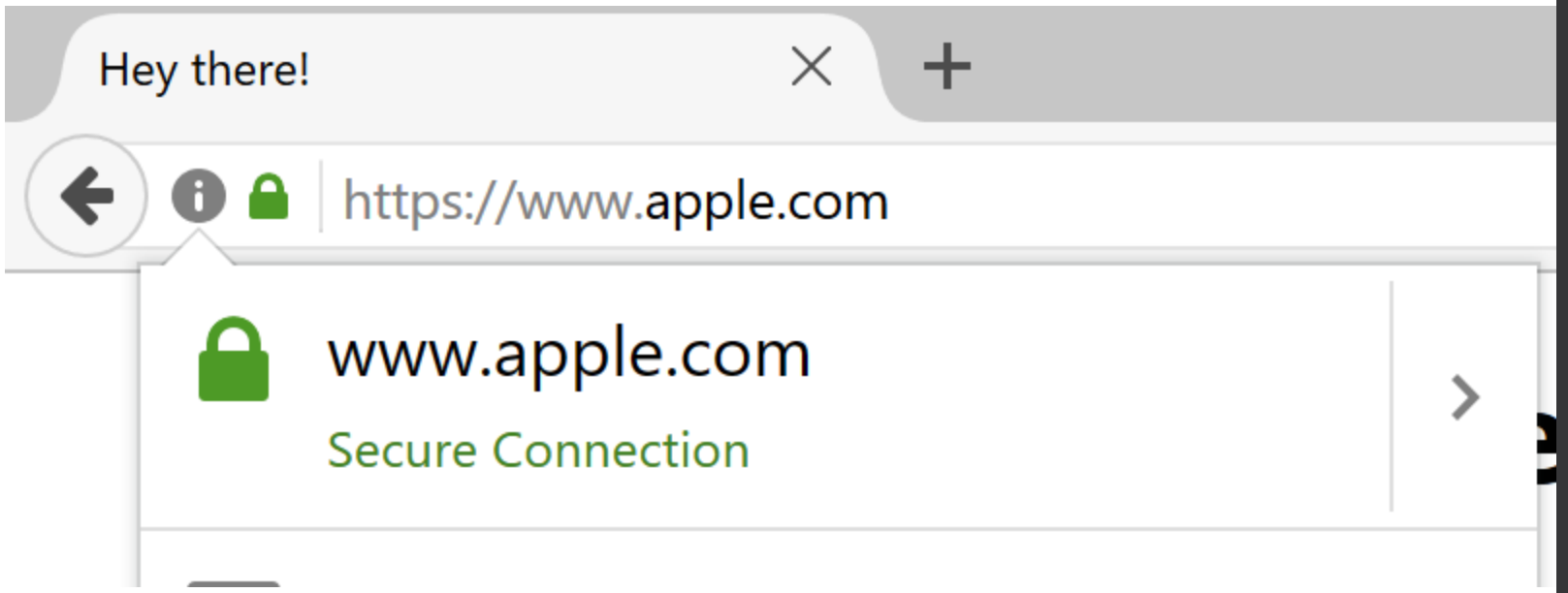
u/xellos30 on Reddit

Paper: « The homograph attack » - 2001

- Evgeniy Gabrilovich and Alex Gontmakher – Israel.
- Describe attacks using Unicode URLS to spoof a website URL.
- Microsoft.com reserved by researchers, cyrillic chars.

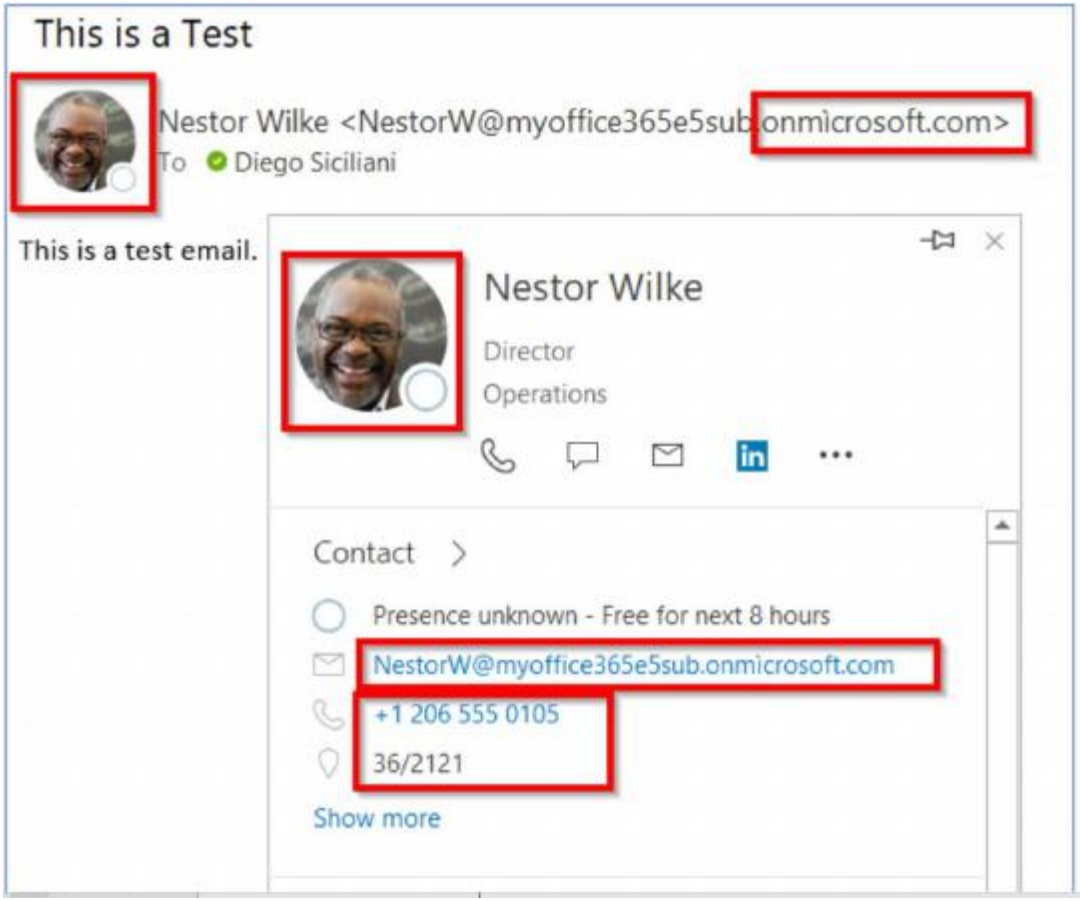
apple.com

- Xudong Zheng, April 14 2017



M1cr0$0ft Outlook vulnerability

- DobbyWanKenobi, 2021.
- Imagine you have your good friend, Jean Bon,email jean.bon@mycompany.onmicrosoft.com in your address book.
- The code thingy linking an address book's contact to a mail 'simplifies' some accentuated chars.
- Meaning that if you receive a phishing email from jean.bon@mycompany.onmìcrosoft.com, it will link it to your good friend in your address book, Jean Bon, which it is not.



What about bad guys?

Is this exploited in the wild by bad actors?

What about bad guys?

- APWG – Anti Phishing Working Group – is studying among all phishing techniques the homograph attacks.
- Up to now, phishers don't seem to be interested a lot in these, even though they point out some IDNs used sometimes.
  - Phishers don't care about domain names, the email+landing page just needs to be convincing.
- From 2007 to 2014: only 9 real homograph attacks.
- In 2015:
  - xn--paypl-680b.com paypạl.com
- In 2016:
  - About 185 IDNs used for phishing. Only these 2 are homograp attacks:
    - xn--fcbook-wta9d.com fâcêbook.com
    - xn--arbnb-b4a.com aịrbnb.com

What about bad guys?

- Funny, they use IDNs for « local » attacks:
  - xn--apple-uj8l559d.com　apple客服.com = “Apple customer service.com”
  - xn--iphone-gj7k537u.com　iphone官网.com = "iphone official website.com"
  - xn--wfrr5djviml2ak75a.cc　商家办理部.cc = “merchant processing department.cc”

- In case you’re interested, more information in APWG Global Phishing Report 2015-2016. ;-)

A bad idea later…

Hack: 1) an article or project without constructive end; **2) work undertaken on bad self-advice**; 3) an entropy booster; 4) to produce, or attempt to produce, a hack (3).

In a cold December night, in 2019…

- During a phone call with a friend, we wanted to use stoopid homograph attacks to make a demo website for our students/trainees to learn about this kind of attacks, as it may be powerful for spear-phishing attacks and is not well known/not a lot used for now.

- What could be a good and impacting demo for our french participants?
- Must be a domain name everybody knows.

Looking at AFNIC's naming policy at the time

- Version 25052018
- I was reading through it and then...

Article 2.5 - L'extension « .gouv.fr »

34. L'extension « .gouv.fr » est réservée au gouvernement français.

35. Les justificatifs nécessaires à l'obtention du code d'autorisation sont :

- ✓ Un identifiant au répertoire SIRENE ou tout autre document officiel permettant d'identifier l'entité et,
- ✓ La validation du Service d'Information du Gouvernement (SIG).

- Nothing here about IDNs, right ?

Looking at AFNIC's naming policy at the time

- Gouv was not a « restricted » term.
- A « restricted » terms (extermism, rascism, administration etc.) must follow some rules and are subject to approval:

  - ✓ n'est pas susceptible de porter atteinte à l'ordre public ou aux bonnes mœurs ou à des droits garantis par la Constitution ou par la loi ;
  - ✓ n'est pas susceptible de porter atteinte à des droits de propriété intellectuelle ou de la personnalité ou n'est pas identique ou apparenté au nom de la République Française ou d'une collectivité territoriale ou d'un groupement de collectivités territoriales ou d'une institution ou service public national ou local sauf si le demandeur justifie d'un intérêt légitime et agit de bonne foi.

- Cannot have a name too close to administration, except if:
  - Good will: *white hat sec engineer*,
  - Legitimate interest: *trainings/demos in cybersecurity*.
- So, at the time, i thought about making a static webpage explaining it is a demo site, with explanations and a way to contact me. It HAD to be clear that this was a copy, not the original, to prove good will.

Göuv.fr and Göüv.fr

Introducing the bad idea.

What i tried:

- Göuv.fr
  - Xn--guv-sna.fr
- Göüv.fr
  - Xn--gv-fkay.fr

- Secretly, i was kind of hoping this attempt will be detected/stopped somewhere.
- I was not.
- But now, it'll likely be.
- Let's see.

Cher client,

Ceci est un message automatique de confirmation de l'enregistrement du ou des

göuv.fr (https://www.gandi.net/whois/details/?search=xn--guv-sna.fr)

La création a bien été effectuée. Il sera pleinement disponible (éventuelle re
heures maximum.

Si votre commande comportait d'autres domaines et qu'ils ne figurent pas dans
Dans tous les cas, vous pouvez vous rendre dans votre panneau de contrôle pour

https://admin.gandi.net/domain/

Cher client,

Ceci est un message automatique de confirmation de l'enregistrement du ou des

göüv.fr (https://www.gandi.net/whois/details/?search=xn--gv-fkay.fr)

La création a bien été effectuée. Il sera pleinement disponible (éventuelle re
heures maximum.

Si votre commande comportait d'autres domaines et qu'ils ne figurent pas dans
Dans tous les cas, vous pouvez vous rendre dans votre panneau de contrôle pour

https://admin.gandi.net/domain/

Si vous utilisez les serveurs de nom de Gandi (DNS), vous pouvez également ajo
ce panneau de contrôle.

Cher client,

Ceci est un message automatique de confirmation de l'enregistrement du ou des

göuv.fr (https://www.gandi.net/whois/details/?search=xn--guv-sna.fr)

La création a bien été effectuée. Il sera pleinement disponible (éventuelle re
heures maximum.

Si votre commande comportait d'autres domaines et qu'ils ne figurent pas
Dans tous les cas, vous pouvez vous rendre dans votre panneau de cont

https://admin.gandi.net/domain/

Cher client,

Ceci est un message automatique de confirmati ement du ou des

göüv.fr (https://www.gandi.net/whois/d .n--gv-fkay.fr)

La création a bien été effectué ement disponible (éventuelle re
heures maximum.

Si votre commande c es domaines et qu'ils ne figurent pas dans
Dans tous les c vous rendre dans votre panneau de contrôle pour

https:// domain/

s les serveurs de nom de Gandi (DNS), vous pouvez également ajo
c contrôle.

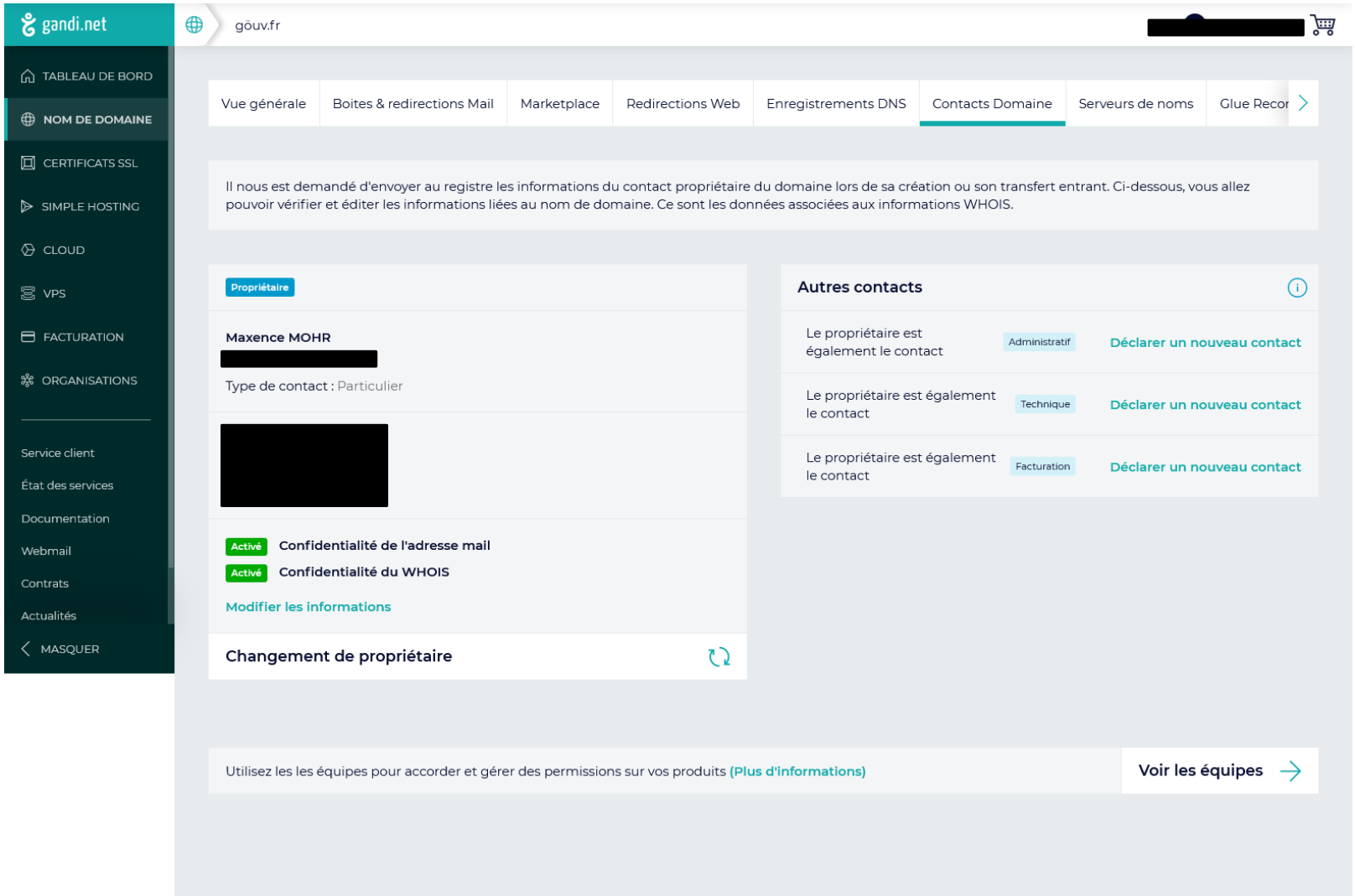
"[Q_328831] AFNIC – Avis de gel de vos noms de domaine" pour xn--gv-fkay.fr
"[Q_328832] AFNIC – Avis de gel de vos noms de domaine" pour xn--guv-sna.fr

Bonjour Maxence,

Merci d'avoir patienté.

L'Afnic nous communique que la vérification a bien été prise en compte et que les domaines xn--gv-fkay.fr et xn--guv-sna.fr ne seront pas gelés.

Nous restons à votre disposition pour toute demande d'information complémentaire.



MERCI DE LIRE CET ENCADRÉ - IMPORTANT
Ce site est réservé à titre de démonstration. Ce site n'est pas et n'a aucune relation avec le gouvernement Français et le nom de domaine 'gouv.fr'.

Ce site est encore en travaux et en cours de rédaction. Cette page sera mise à jour régulièrement.

>>> Foire Aux Questions <<<

Avez-vous cliqué sur un lien dans un email pour arriver sur ce site ?

Si c'est le cas, regardez bien la barre d'adresse de votre navigateur. Le nom de domaine n'est pas 'gouv.fr' comme vous pourriez vous y attendre, mais 'göuv.fr' (ou 'göüv.fr') avec la lettre 'O tréma' aussi appelée 'O umlaut' (et possiblement 'U tréma' aussi appelé 'U umlaut').

Comment est-ce possible ?

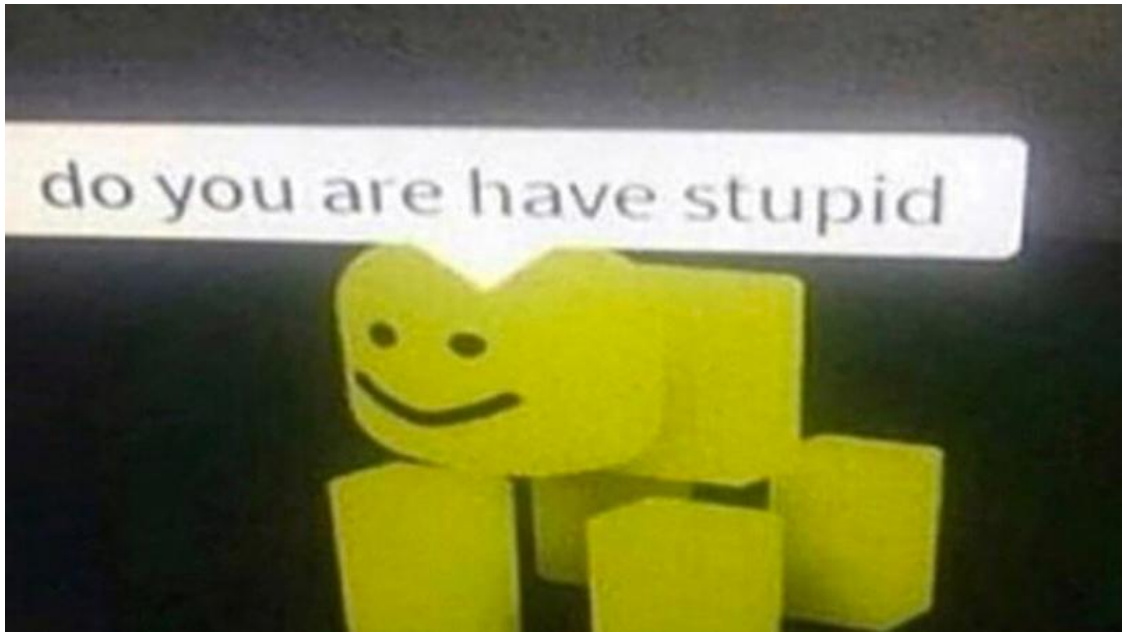
Depuis 2012, l'AFNIC (qui est en charge des extensions en .fr) autorise les noms de domaine internationalisés (IDN) avec des caractères spéciaux. Ces caractères sont des caractères de la langue française ou de langues régionales.

En soit, cela ne pose pas de problèmes, et c'est même très bien que l'on puisse utiliser les caractères accentués dans des domaines français (limité à quelques caractères seulement), ou des systèmes d'écriture/alphabets entiers correspondant à celui du site visité (N'ko, cyrillique, grec, arabe, hébreu, katakana, thaï, etc.), mais il est parfois possible de réserver des noms de domaines proches de sites existants. Parfois, c'est visible et parfois, c'est subtil.

En réalité, le nom de domaine de ce site est xn--guv-sna.fr (ou xn--gv-fkay.fr). Il s'agit d'un encodage (c'est à dire une façon d'écrire) pour avoir des caractères spéciaux. Il est probable que votre navigateur interprète ces caractères et vous affiche dans la barre d'adresse l'encodage interprété (en replaçant le 'xn--' et les codes (ici 'sna' ou 'fkay') par les caractères spéciaux (ici 'ö' ou 'ü')).

Y no HTTPs?

- ssi.göuv.fr
- impots.göuv.fr
- amendes.göuv.fr
- defense.göuv.fr
- interieur.göuv.fr
- Etc.
  - You get the idea.



Consequences

What can/could have gone wrong?
Sometimes fun things are in fact stupid.

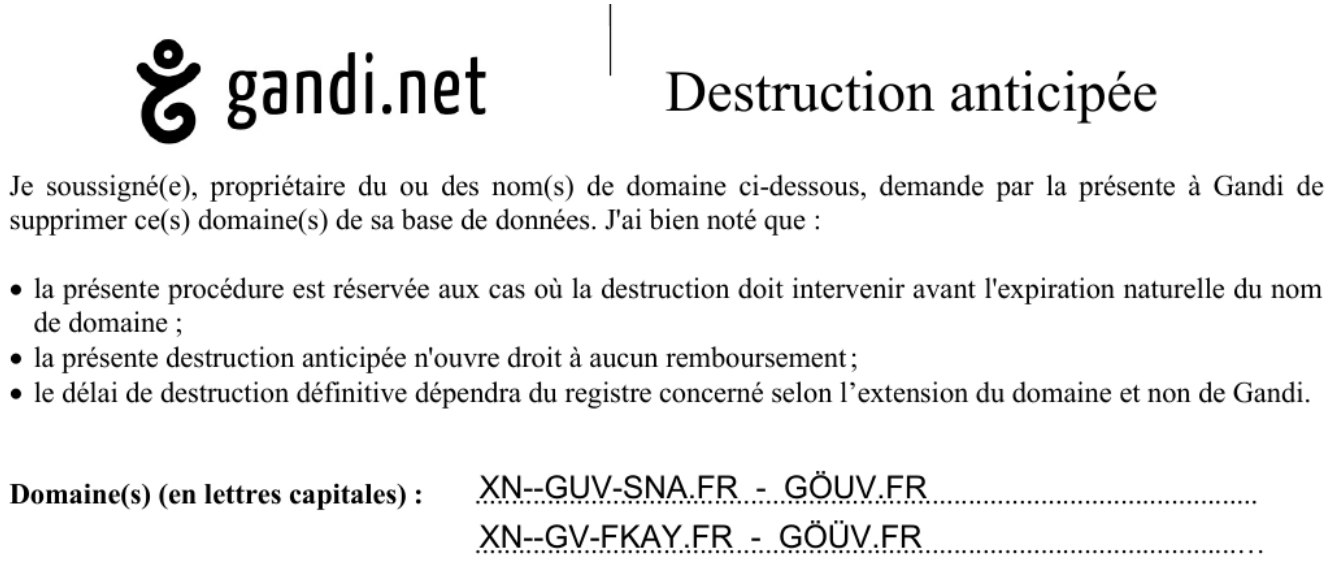
March 31 2021 (about 1 year and a half in)

- Anonymous Twitter account warns me.
- Says he is from Gvt, and they found my homographs, in a meeting about domain names homograph attacks.
- Sometimes says i'll be fine, sometimes seems to try to pressure me.
- Says police, gendarmerie, customs, french IRS (impots) are aware, and a bit angry that a dumbass like me did this (and i can understand that).
- Says people in this meeting are angry about the certificate containing A LOT of French gov subdomains homographs.
- Wanted me to tranfer domain names to them... but what if not from French authorities? He gave me no proof whatsoever.

- What to do?
- VERY STRESSED OUT, called a friend, then contacted ANSSI.

March 31 2021

- I submitted them a mail, declining my identity, explaining the situation and asked them what to do.
- They told me to « forcely delete the domain names in question and everything will be fine », which I did.



gandi.net | Destruction anticipée

Je soussigné(e), propriétaire du ou des nom(s) de domaine ci-dessous, demande par la présente à Gandi de supprimer ce(s) domaine(s) de sa base de données. J'ai bien noté que :

- la présente procédure est réservée aux cas où la destruction doit intervenir avant l'expiration naturelle du nom de domaine ;
- la présente destruction anticipée n'ouvre droit à aucun remboursement ;
- le délai de destruction définitive dépendra du registre concerné selon l'extension du domaine et non de Gandi.

Domaine(s) (en lettres capitales) : XN--GUV-SNA.FR - GÖUV.FR
XN--GV-FKAY.FR - GÖÜV.FR

- Kudos to Gandi, it was being worked on VEEERY fast. The destruction order was forwarded to AFNIC within 8 hours. \o/

Things learned

- Never thought so much about consequences at the time.
- This is why I couldn't recommend you to play with this.
- This might be illegal in your country.
- This might bring to you « les amis du petit-déjeuner » (breakfast friends, cops that is). It already happened to a guy in France, for the same reason.
- This might even end up in court, or in jail (and remember, in our field, not so good to find work).
- I forgot, and maybe you should think about it too if you're in my position in the future: make dumb DKIM/DMARC/SPF entries, as it will prevent bad guys sending phishing through it. Even though, nearly all email operators today drops or flag as spam emails from domains not having them.
- So. Will I do this again ? Maybe, but not in the same way. (And not the same target). What I see as « fun » might be seen as « moquery » by the people concerned. And I nover really thought about it.

Out of curiosity – after all this – checked some things

- In my VPS logs for the machine behind göuv.fr and göüv.fr, found IP addresses from the French Gov, seemd that Anonymous was not lying.
- The AFNIC's Domain naming policy has changed, as follow (subtle change, can you spot it?)

Article 2.5 - L'extension « .gouv.fr »

34. L'extension « .gouv.fr » est réservée au gouvernement français.

35. Les justificatifs nécessaires à l'obtention du code d'autorisation sont :

- ✓ Un identifiant au répertoire SIRENE ou tout autre document officiel permettant d'identifier l'entité et,
- ✓ La validation du Service d'Information du Gouvernement (SIG).

Article 2.5 - L'extension « gouv.fr »

34. L'extension «.gouv.fr » ainsi que ses versions IDN sont réservées au gouvernement français.

35. Les justificatifs nécessaires à l'obtention du code d'autorisation sont :

- ✓ Un identifiant au répertoire SIRENE ou tout autre document officiel permettant d'identifier l'entité et,
- ✓ La validation du Service d'Information du Gouvernement (SIG).

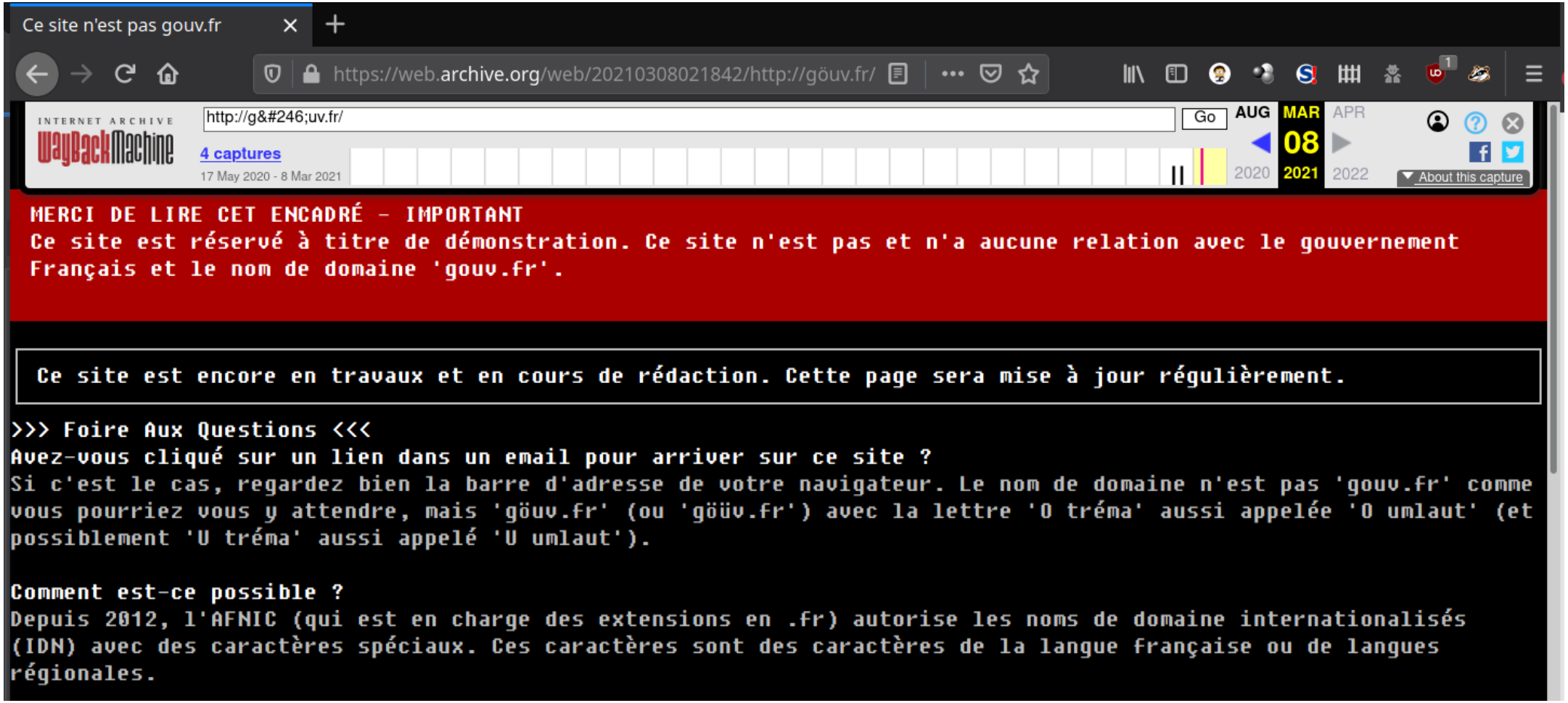
Out of curiosity – after all this – checked some things

- It seems they can no longer be reserved. Even WHOIS is bad on Gandi.


```
looping@laptop:~$ whois göuv.fr
%%
%% This is the AFNIC Whois server.
%%
%% complete date format : YYYY-MM-DDThh:mm:ssZ
%% short date format    : DD/MM
%% version              : FRNIC-2.5
%%
%% Rights restricted by copyright.
%% See https://www.afnic.fr/en/products-and-services/services/whois/whois-special-notice/
%%
%% Use '-h' option to obtain more information about this service.
%%
%% [109.190.212.55 REQUEST] >> -V Md5.5.10 xn--guv-sna.fr
%%
%% RL Net [##########] - RL IP [#########.]
%%

%% No entries found in the AFNIC Database.
```

Still on archive.org :)



Je soussignée Marianne Georgelin, directrice juridique de l'Afnic, certifie et atteste que Maxence MOHR est bien le titulaire déclaré du nom de domaine suivant :

- **göuv.fr (xn--guv-sna.fr)** créé le 5 décembre 2019

Vous trouverez ci-après les informations contenues dans la base concernant ce nom de domaine.

Bureau d'enregistrement actuel : GANDI

Titulaire :	nic-hdl :	MM47499-FRNIC
	type :	PERSON
	contact :	Maxence MOHR
	adresse :	[redacted]
	pays :	
	téléphone :	
	e-mail :	

Fait à Montigny-le-Bretonneux-le-Bretonneux, le 27 avril 2021.

How to patch/protec/prevent

Too many memes? Deal with it.

The solution has 3 parts

- Client (user) side:
  - In browsers
    - Firefox, Chrome, Safari, Internet Explorer all have **some kind of protection. For some domains or for some alphabets that should not be mixed, they show the raw URI, not the Unicode one.** It is not perfect, and with my trick it worked everywhere, except for impots.göuv.fr on Chrome. (some FQDNs listed in a base are shown as
    - Browsers extensions, such as « No Homo Graphs » for Firefox will show you phishing attempts with homograph attacks if the domain name is well known.
  - In mail clients
    - A lot of mail clients don’t care about punycode. Or does stupid things (hello |\/|1cr0$0f7)
- Problem
  - Depends on the user…

The solution has 3 parts

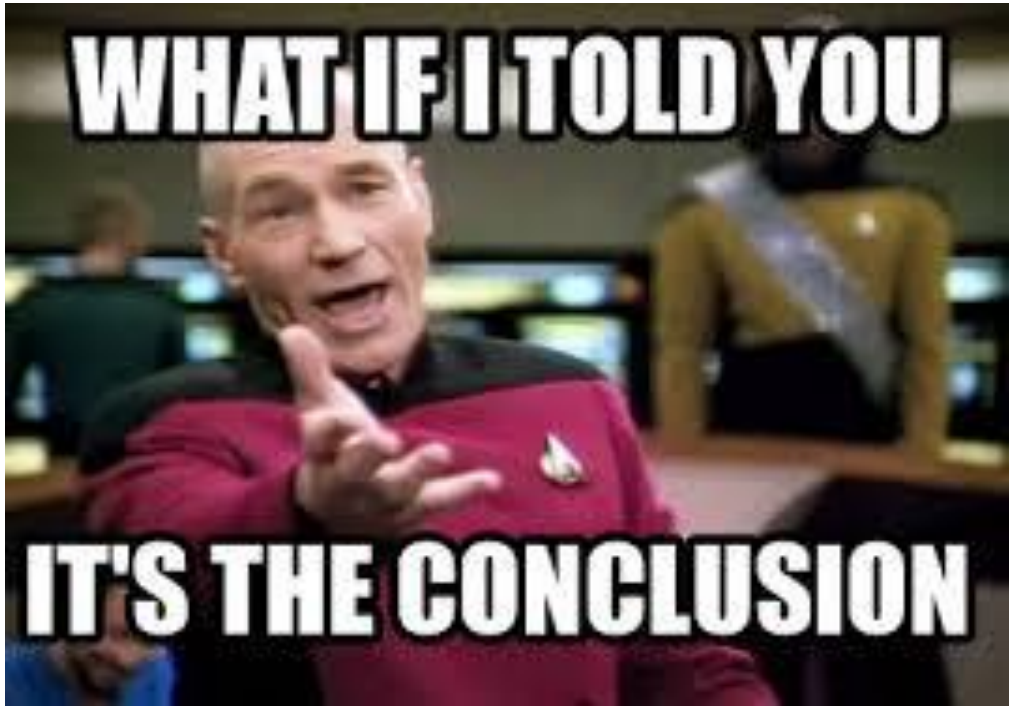
- Registry side:
  - ccTLDs should only accept correct alphabets for the country, not more than that.
    - Just like .рф only allowing cyrillic alphabet, not more.
    - AFNIC is doing a good job for that, it is really limiting the possibilities for attackers.
  - Maybe some alphabets mixing cloud be banned, as not compatible with each other.
- Problem:
  - For some gTLDs, like .com, it’s a bit late.

The solution has 3 parts

- Domain owner side:
  - Monitoring, monitoring, monitoring.
    - Some python scripts try to search for known domain names close to yours
      - Github.com/elceef/dnstwist
      - Github.com/urbanadventurer/urlcrazy
      - …
  - You can also pay a private company for this service
    - Like Nameshield (not linked or affiliated)
    - Or OVH (not linked or affiliated)
- Problem:
  - Everybody monitors, right?

For Frenchies

- Anonymous said a new law is being redacted, to prevent homograph attacks.
- This kind of attacks on gouv.fr should not be possible again, as the naming policy now prohibits it.
- Attacks are limited on .fr due to AFNIC's allowed chars in the Domain name's policy.

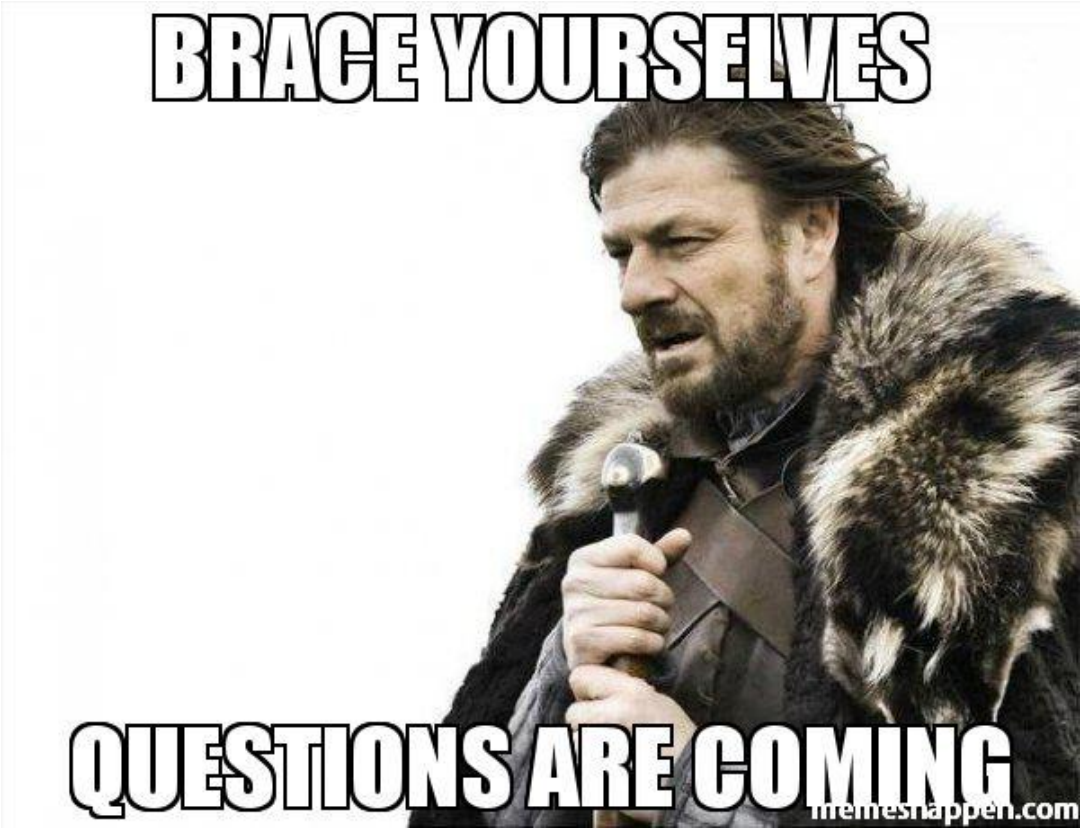


Conclusion

I need to drink something, sore throat. I talk too much.

Special thanks to…

- … *Fred Crypto*, in the role of the good friend pushing a bad idea to the Max :3
- … *Jusk* for the support :D
- … *Anonymous* that was nice with me, even though I didn't know at that time (I still don't know (and will not know) who he/she/it is) :x
- … *ANSSI/Cert-FR/COSSI* email team :)
- … *French Gov officials* for the understanding (and for not sending me (yet) into GàV)
- … *Gandi*, my registrar, with great support and wonderful team <3
- … *SecSea CfP team* for accepting my submission :o
- … *you* for listening to this with my not-so-great French accent and supporting my bad jokes and memes %)



Questions?

Everybody is so SecSea today. <3