Panne du domaine national russe

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 30 janvier 2024. Dernière mise à jour le 8 février 2024

https://www.bortzmeyer.org/ru-dnssec.html

Aujourd'hui, une panne a affecté le domaine de premier niveau russe, .ru. Que sait-on ? (Quand cet article a été initialement publié, on ne savait pas exactement ce qui s'était passé. Voir à la fin pour des explications vraisemblables.)

La panne a duré à peu près de 15 :20 UTC à 19 :00 UTC (avec une réparation partielle à 17 :50 UTC). Pour l'instant, il semble certain que le problème <https://t.me/news_sirena/23858> était lié à DNSSEC et qu'il s'agissait probablement d'une panne, pas d'une action volontaire de la Russie ou de ses ennemis (hypothèse parfois citée, vu le contexte de guerre). Un petit rappel : DNSSEC est une technique de sécurité visant à garantir l'intégrité des noms de domaine. DNSSEC, comme toutes les techniques de sécurité, peut, en cas de fausse manœuvre, aboutir à un déni de service ; si vous perdez les clés de votre maison, vous ne pourrez plus rentrer chez vous. Ici, les signatures des domaines de .ru étaient invalides, menant les résolveurs DNS <https://www.bortzmeyer.org/resolveur-dns.html> à les rejeter et donc à ne pas réussir à résoudre les noms de domaine sous .ru. Deux points sont notamment à noter :

— Du fait du caractère arborescent du DNS, une panne de .ru affecte **tous** les noms situés sous .ru. La gestion d'un TLD est quelque chose de critique ! Il est donc faux de dire que tel ou tel site Web russe était en panne ; en fait, son nom de domaine ne fonctionnait plus.
— Comme tous les résolveurs DNS <https://www.bortzmeyer.org/resolveur-dns.html> ne valident pas les signatures DNSSEC, la résolution marchait encore pour certains.

Compte-tenu des observations faites sur le moment, il semble bien que le communiqué du ministère russe <https://t.me/mintsifry/2114> était correct (à un point près, détaillé plus loin). Le problème était bien dans le registre du .ru et était sans doute le résultat d'une erreur de leur côté. La traduction du communiqué par DeepL : « Ministère russe de la numérisation \ L'accès aux sites de la zone .RU sera bientôt rétabli \ La zone .RU a été affectée par un problème technique lié à l'infrastructure DNSSEC* mondiale. Des spécialistes du Centre technique de l'internet et de MSC-IX travaillent à son élimination. \ Actuellement, le problème a été résolu pour les abonnés du système national de noms de domaine. Les travaux de restauration sont en cours. Nous vous tiendrons au courant de l'évolution de la situation. \ *DNSSEC est un ensemble d'extensions du protocole DNS, grâce auxquelles l'intégrité et la fiabilité des données sont garanties. » Et le communiqué original <https://t.me/mintsifry/2114> sur Telegram :

Notons que les TLD `.su` et `.[Caractère Unicode non montré [1] ][Caractère Unicode non montré ]` ne semblent pas avoir été affectés, alors qu'ils sont gérés par le même registre.

Un peu plus de technique, maintenant. Avec dig, voyons la résolution DNS, via un résolveur validant :

```
% date -u ; dig ru. NS
Tue 30 Jan 17:12:05 UTC 2024

; <<>> DiG 9.18.18-0ubuntu0.22.04.1-Ubuntu <<>> ru. NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 32950
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1232
; EDE: 6 (DNSSEC Bogus): (NXJA)
;; QUESTION SECTION:
;ru. IN NS

;; Query time: 2384 msec
;; SERVER: 192.168.2.254#53(192.168.2.254) (UDP)
;; WHEN: Tue Jan 30 18:12:07 CET 2024
;; MSG SIZE  rcvd: 41
```

Le SERVFAIL indique un échec. Notez l'EDE ("*Extended DNS Error*", RFC 8914 [2]), qui indique que l'échec est lié à DNSSEC.

Ensuite, vérifions que tout marchait, à part DNSSEC. En coupant la validation DNSSEC (option `+cd`, "*Checking Disabled*"), on avait bien une réponse :

```
% date -u ; dig +cd ru. NS
Tue 30 Jan 17:15:06 UTC 2024

; <<>> DiG 9.18.18-0ubuntu0.22.04.1-Ubuntu <<>> +cd ru. NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5673
;; flags: qr rd ra cd; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1232
;; QUESTION SECTION:
;ru. IN NS

;; ANSWER SECTION:
ru. 344162 IN NS b.dns.ripn.net.
ru. 344162 IN NS d.dns.ripn.net.
ru. 344162 IN NS e.dns.ripn.net.
ru. 344162 IN NS f.dns.ripn.net.
```

1. Car trop difficile à faire afficher par LaTeX
2. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc8914.txt`

```
ru. 344162 IN NS a.dns.ripn.net.
ru. 344162 IN RRSIG NS 8 1 345600 (
20240305102631 20240130141847 52263 ru.
kw9oqgvi/l0MZp/6FY0Ha+VZDWRR3+iDUCYqAY5W7D2w
CfIXXdOOvdd58nNY7z/3b4fRK6tlTF3wQpCDSpeKrmkW
mric4kcUptaj1rp71lC0GHXHmGwDsx8Zi/lvo6sJEk0g
uBbJYBJkzKqeseD4u1Pw29jkRHhQEJKk2seP+Zk= )

;; Query time: 8 msec
;; SERVER: 192.168.2.254#53(192.168.2.254) (UDP)
;; WHEN: Tue Jan 30 18:15:06 CET 2024
;; MSG SIZE  rcvd: 285
```

Les serveurs de nom faisant autorité <https://www.bortzmeyer.org/serveur-dns-faisant-autorite.html> répondaient bien :

```
% dig @b.dns.ripn.net. ru NS

; <<>> DiG 9.18.18-0ubuntu0.22.04.1-Ubuntu <<>> @b.dns.ripn.net. ru NS
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37230
;; flags: qr aa rd; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 11
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;ru. IN NS

;; ANSWER SECTION:
RU. 345600 IN NS a.dns.ripn.net.
RU. 345600 IN NS e.dns.ripn.net.
RU. 345600 IN NS b.dns.ripn.net.
RU. 345600 IN NS f.dns.ripn.net.
RU. 345600 IN NS d.dns.ripn.net.
ru. 345600 IN RRSIG NS 8 1 345600 (
20240305102631 20240130141847 52263 ru.
kw9oqgvi/l0MZp/6FY0Ha+VZDWRR3+iDUCYqAY5W7D2w
CfIXXdOOvdd58nNY7z/3b4fRK6tlTF3wQpCDSpeKrmkW
mric4kcUptaj1rp71lC0GHXHmGwDsx8Zi/lvo6sJEk0g
uBbJYBJkzKqeseD4u1Pw29jkRHhQEJKk2seP+Zk= )

;; ADDITIONAL SECTION:
a.dns.RIPN.net. 1800 IN AAAA 2001:678:17:0:193:232:128:6
b.dns.RIPN.net. 1800 IN AAAA 2001:678:16:0:194:85:252:62
d.dns.RIPN.net. 1800 IN AAAA 2001:678:18:0:194:190:124:17
e.dns.RIPN.net. 1800 IN AAAA 2001:678:15:0:193:232:142:17
f.dns.RIPN.net. 1800 IN AAAA 2001:678:14:0:193:232:156:17
a.dns.RIPN.net. 1800 IN A 193.232.128.6
b.dns.RIPN.net. 1800 IN A 194.85.252.62
d.dns.RIPN.net. 1800 IN A 194.190.124.17
e.dns.RIPN.net. 1800 IN A 193.232.142.17
f.dns.RIPN.net. 1800 IN A 193.232.156.17

;; Query time: 268 msec
;; SERVER: 2001:678:16:0:194:85:252:62#53(b.dns.ripn.net.) (UDP)
;; WHEN: Tue Jan 30 17:56:45 CET 2024
;; MSG SIZE  rcvd: 526
```

Et DNSviz <https://dnsviz.net/> confirme le diagnostic <https://dnsviz.net/d/ru/Zbko4g/dnssec/> :

Comme le note DNSviz, les signatures étaient invalides :

Il ne s'agissait pas de problèmes locaux. En demandant aux sondes RIPE Atlas <https://atlas.ripe.net>, on voit beaucoup d'échecs de résolution (SERVFAIL, "*SERVer FAILure*") :

```
% blaeu-resolve -r 200 --type NS ru
[ERROR: SERVFAIL] : 79 occurrences
[a.dns.ripn.net. b.dns.ripn.net. d.dns.ripn.net. e.dns.ripn.net. f.dns.ripn.net.] : 66 occurrences
[ERROR: NXDOMAIN] : 13 occurrences
Test #66905129 done at 2024-01-30T16:59:57Z
```

(Notez les NXDOMAIN - "*No Such Domain*", qui sont des mensonges de résolveurs qui censurent la Russie, en raison de son agression de l'Ukraine.)

Une fois que tout était réparé, la validation se passait bien :

```
% blaeu-resolve -r 200 --type DNSKEY --displayvalidation --ednssize 1450 ru
...
[ERROR: NXDOMAIN] : 19 occurrences
[ (Authentic Data flag)  256 3 8 awea...] : 93 occurrences
[256 3 8 aweaa...] : 64 occurrences
[ERROR: SERVFAIL] : 9 occurrences
[] : 1 occurrences
[ (TRUNCATED - EDNS buffer size was 1450 ) ] : 1 occurrences
Test #66910201 done at 2024-01-30T18:20:56Z
```

Notez que la phrase du ministre « le problème a été résolu pour les abonnés du système national de noms de domaine » était fausse. Le problème a été résolu pour tout le monde (ce « système national de noms de domaine » est l'objet de beaucoup de propagande et de fantasme et il n'est pas du tout sûr qu'il ait une existence réelle). La situation actuelle :

```
% dig ru DNSKEY

; <<>> DiG 9.18.18-0ubuntu0.22.04.1-Ubuntu <<>> ru DNSKEY
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6401
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1232
;; QUESTION SECTION:
;ru. IN DNSKEY

;; ANSWER SECTION:
ru. 39023 IN DNSKEY 256 3 8 (
AwEAAcBtr/w2hP6OQjiCacPFzK6xh0pR7QsHV9lxprIX
G9WBoBB5XWPVc5q17F3yt3wpJ7xmedt80gxVMaicPYNY
Aa8YUFyMxTGVBDVQlz5gCmXQKlr0yImI78sdwzWNmgKH
ap0BLypTBVxAKxpcvuwTmqXQUSONkjq9werHvogrvkUb
) ; ZSK; alg = RSASHA256 ; key id = 44301
ru. 39023 IN DNSKEY 257 3 8 (
AwEAAfcMZekGvFYkmt18Q8KIS+XX/7UBbpmIJ4hK3FNz
ErkJmiNPxq+sbM00NYJwY725QxoDwHPeK0JIybKW6s+U
2+I7aBGJus/bvDklw0CMTDsG7HoJG+4sjq/jRPUQNwkO
A/cNoiYjroqw7/GnB8DEAGE03gyxdZcxxU3BJKPZfds8
```

```
DJYPBaDUO35g9I6+dLPXxHK6LFUFprkBtpqj13tJ/ptL
yMSaivvi3xrvJMqu/FWN6piMzu7uYmrSdv6s01y+0x62
29sZ7ufSQ6E66gdTmXebDx8S8q70B4BmMZosrsHlf3uX
VMMY72LnrQzbere2ecd95q+1VDMDXcXB/pT1/C0=
) ; KSK; alg = RSASHA256 ; key id = 43786
ru. 39023 IN DNSKEY 256 3 8 (
AwEAAbjj3GP0TUwaNI7BIIw/fvwKTmdR+oZsEPk64pl8
VYn4dfdbGHWpYIooxcgEbuBEYrnC/oqnKhad38nTxrZ9
SAK3qV5qShntFdgozS5IKs5m1ebNmg2sotlhXRhJ4vqg
H+BQh/lw6T4vdB8FE5tHGE1vwPs9Vhj0vLTBhX8TwB6/
) ; ZSK; alg = RSASHA256 ; key id = 52263
ru. 39023 IN RRSIG DNSKEY 8 1 345600 (
20240213000000 20240124000000 43786 ru.
rgqGAFvlWoGzSGrKaaMUqpNkOGyKQS+MOwvrwy3+A4nh
FiioZ610H9GlN/fh3kUjiFrRJ7T1sKiW9AVekkpdZk/Q
T5vRGqWi+PLyuRtfL7ZtJKVgUPV+jGVOc0A9AZA0dVgx
qX54L+mbMY6OGCcMeTHwUpg6J2UR0MmB3TCyHPhg0Z/L
VHWf/E9hHO4dqdePwKvlVeA7txcXemiJE6C1/mgFvtQl
uQsot9eDOqKZt9oUpqzi63gsw835+h6fiKNbMJf4SEPw
5enbdQqcubSWwwY/SbeoW74qgPgPgJrmiP8UxT6DEAZc
W5UO9CsMcyfgifsL0zy5SMba4kS0izp4rQ== )

;; Query time: 4 msec
;; SERVER: 192.168.2.254#53(192.168.2.254) (UDP)
;; WHEN: Tue Jan 30 21:04:05 CET 2024
;; MSG SIZE  rcvd: 893
```

Plusieurs personnes ont noté une lenteur, ou même parfois une absence de réponse, de la part de certains des serveurs faisant autorité <https://www.bortzmeyer.org/serveur-dns-faisant-autorite.html> pour `.ru`. Il s'agit probablement d'un effet dû aux efforts des résolveurs DNS <https://www.bortzmeyer.org/resolveur-dns.html> qui, recevant des signatures invalides, réessayaient (éventuellement vers d'autres serveurs faisant autorité) dans l'espoir de récupérer enfin des signatures correctes. En tout cas, rien n'indique qu'il y ait eu une attaque externe contre `.ru`.

Mais peut-on savoir ce qui s'est passé ? Pas exactement, mais on peut toujours poursuivre l'analyse. DNSviz <https://dnsviz.net/> nous donne également accès aux numéros de série, stockés dans l'enregistrement SOA de la zone `.ru`. On peut donc reconstituer une chronologie (elle a été faite par Phil Kulin <https://lists.dns-oarc.net/pipermail/dns-operations/2024-January/022408.html> et vérifiée par moi) :

- 2024-01-30 12 :29 :44 UTC <https://dnsviz.net/d/ru/ZbjruA/dnssec/> : dernier test où tout était correct. Le numéro de série était 4058855, la clé signant les enregistrements (ZSK, "*Zone Signing Key*") était la 44301, la ZSK 52263 était déjà publiée (remplacement de ZSK en cours).
- 2024-01-30 15 :27 :27 UTC <https://dnsviz.net/d/ru/ZbkVXw/dnssec/> : premier test avec la panne, qui a donc dû commencer quelques minutes plus tôt (en cas de problème DNSSEC, il y a toujours quelqu'un qui se précipite pour faire un test DNSviz). Le numéro de série est le 4058857. La clé signante est désormais la 52263, et les signatures sont invalides.
- Il y aura une zone de numéro 4058858, mais le problème continue.
- 2024-01-30 17 :59 :46 UTC <https://dnsviz.net/d/ru/Zbk5Eg/dnssec/> : la réparation commence. L'ancienne zone de numéro 4058856 est republiée, signée par l'ancienne clé 44301. Notez que, pendant plus d'une heure, plusieurs versions de la zone coexisteront (avec trois numéros de série différents, 4058856, 4058857 et 4058858).
- 2024-01-30 19 :07 :29 UTC <https://dnsviz.net/d/ru/ZblI8Q/dnssec/> : réparation terminée, on est revenu à la situation d'avant la panne.
- À un moment dans la journée du 31 janvier : la zone bouge à nouveau (le numéro de série augmente, la zone est signée par la clé 52263).

Il est important de noter que la chaine des clés depuis la racine a toujours été correcte. La plupart des problèmes DNSSEC sont dûs à une chaine incorrecte (du genre d'un enregistrement DS qui pointe vers une clé inexistante) mais ce n'est pas le cas ici. La KSK ("*Key Signing Key*", introduite deux semaines

auparavant <https://mastodns.net/@diffroot/111772960703242665>. Elle est bien pointée par un enregistrement DS de la racine, et signe bien les ZSK 44301 et 52263.

Enfin, on notera que le numéro de série ne bougeait plus (il changeait toutes les deux heures environ auparavant), ce qui fait penser que le problème n'était pas tant dans la clé 52263 que dans un système de signature désormais cassé.

```
% dig ru SOA

; <<>> DiG 9.18.19-1~deb12u1-Debian <<>> ru SOA
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44285
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 6, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;ru. IN SOA

;; ANSWER SECTION:
ru. 86400 IN SOA a.dns.ripn.net. hostmaster.ripn.net. (
4058856    ; serial
86400      ; refresh (1 day)
14400      ; retry (4 hours)
2592000    ; expire (4 weeks 2 days)
3600       ; minimum (1 hour)
)
ru. 86400 IN RRSIG SOA 8 1 345600 (
20240313163045 20240130121923 44301 ru.
dAGkfXQSmGCwwUuzxIfNeIgd+/BbAYt0whh3JcqvKi6x
z6N8a7KGBHkfBCbg19xzx6b+LQBJgK4yVtvTQLqLNo8P
fxg5J8S/JUw2EHgPUMJw0CjsrqH85biJqkv+5TVoN9dG
PFnFIjaTPLP0DRscR3ps5NP8lJstDwBYQmg/i68= )

;; AUTHORITY SECTION:
ru. 86400 IN NS e.dns.ripn.net.
ru. 86400 IN NS d.dns.ripn.net.
ru. 86400 IN NS a.dns.ripn.net.
ru. 86400 IN NS f.dns.ripn.net.
ru. 86400 IN NS b.dns.ripn.net.
ru. 86400 IN RRSIG NS 8 1 345600 (
20240304113906 20240126101933 44301 ru.
KthCG9ahQ3UyFl1aakpJRiXI0GXH6TNB6i+uY+920a93
DQgCgkokpsYAHCCzqJl0VXiAmcaEK1yLFHxfJzDbjsel
0xz8IJi3CIuzEtBfBbedXUfBzE/64HmJ9xHVgc5fdLDA
6AfIAmw0oeHCgssUTdZ67IlZO90nzeEHu6PHj2k= )

;; Query time: 32 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Wed Jan 31 10:45:15 CET 2024
;; MSG SIZE  rcvd: 580
```

Il n'a repris sa progression que dans la journée du 31 janvier, et la clé 52263 était à nouveau utilisée :

```
% dig ru SOA

; <<>> DiG 9.18.19-1~deb12u1-Debian <<>> ru SOA
```

```
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37102
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 6, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;ru. IN SOA

;; ANSWER SECTION:
ru. 86397 IN SOA a.dns.ripn.net. hostmaster.ripn.net. (
4058871    ; serial
86400      ; refresh (1 day)
14400      ; retry (4 hours)
2592000    ; expire (4 weeks 2 days)
3600       ; minimum (1 hour)
)
ru. 86397 IN RRSIG SOA 8 1 345600 (
20240306211526 20240201082001 52263 ru.
trZgMG6foXNX+ZotfA11sPGSCJwVpdSzobvrPbMfagIj
pToI2+W9fa3HIW5L3GSliQHbWDnaTp0+dhMs/v3UFnFs
UtCoTy00F/d1FysBtQP2uPZLwPTI3rXJSE2U5/Xxout/
2hSCsIxQE5CxksPzb9bazp63Py0AfbWY56b1/FE= )

;; AUTHORITY SECTION:
ru. 86397 IN NS e.dns.ripn.net.
ru. 86397 IN NS f.dns.ripn.net.
ru. 86397 IN NS a.dns.ripn.net.
ru. 86397 IN NS b.dns.ripn.net.
ru. 86397 IN NS d.dns.ripn.net.
ru. 86397 IN RRSIG NS 8 1 345600 (
20240303133621 20240131134337 52263 ru.
MD8EOMQtjhr08qt3I890qHE+E0HBvhdbtUkasjez+1zd
8zsxH0GCPz5zD0db/HQr9o0hDUMd3xZLHaDvlS/PjLti
6dEVOT7SYHHC2yF7Ypu97alFpEHpGEcchEhMx3rSUBZF
Jik3JVG9yqOxF4m0r+QgVotU4PMIejFGjPdvZ0w= )

;; Query time: 16 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Thu Feb 01 11:27:06 CET 2024
;; MSG SIZE  rcvd: 580
```

Merci à John Shaft, et Paul [Caractère Unicode non montré] Du[Caractère Unicode non montré][Caractère Unicode non montré]ai[Caractère Unicode non montré] <https://twitter.com/du_dot_ie/status/1752451916804616364> pour les analyses expertes et les discussions. J'ai fait à la réunion FOSDEM du 3 février 2024 un exposé rapide sur la question <https://fosdem.org/2024/schedule/event/fosdem-2024-3740-observations-on-a-dnssec-incident-the-russian-tld/> (supports et vidéo sont en ligne).

Vous pouvez lire le premier communiqué officiel du registre <https://cctld.ru/media/news/kc/35566/> (dont les affirmations sont conformes aux observations). Contrairement à ce qui a été affirmé sans preuves <https://www.numerama.com/cyberguerre/1622286-lenorme-panne-dinternet-en-rus
html>, il n'y a aucune indication que cette panne soit liée aux projets russes de renforcement du contrôle étatique sur la partie russe de l'Internet.

L'explication technique officielle et détaillée a finalement été donnée le 7 février dans un message <https://www.rbc.ru/technology_and_media/07/02/2024/65c38fea9a794752176bd3a0> aux BE. Il s'agirait donc bien d'une bogue logicielle dans le système de signature, qui se déclenchait lorsque deux clés avaient le même "*key tag*" (ce qui est possible, vu la taille de ce "*key tag*", mais n'aurait

pas dû provoquer de faille.) Cette explication officielle colle très bien aux observations qui ont été faites au moment de la panne. Notez aussi que cette explication confirme bien que `.[Caractère Unicode non montré ][Caractère Unicode non montré ]` et `.su` n'ont pas été affectés (conformément à ce qui a été observé, et au contraire de ce qu'ont affirmé plusieurs articles écrits sans vérifier) alors que deux TLD peu connus, `.[Caractère Unicode non montré ][Caractère Unicode non montré ][Caractère Unicode non montré ][Caractère Unicode non montré ]` et `.tatar` l'ont été.