“The Hidden Internet of Iran”

INFO731 – Sécurité et Cryptographie

PERROLLAZ Maverick – IDU4

Résumé :

Cet article est destiné à documenter les manières dont l'Iran a réussi à créer un réseau privé accessible uniquement à l'intérieur du pays. Le but sera donc d'énumérer les services et les ressources disponibles sur ce réseau caché.

Sommaire

Sources :

- *“Evidence Emerges That Iran Is Building Its Own Hiddent Internet”* – ***MIT Tech. Review*** https://www.technologyreview.com/2012/10/02/183482/evidence-emerges-that-iran-is-building-its-own-hidden-internet/

- “The Hidden Internet of Iran, Private Address Allocations on a National Network”, Collin Anderson, 28 Sep 2012 - https://arxiv.org/pdf/1209.6398.pdf

Cet article est destiné à documenter les manières dont l'Iran a réussi à créer un réseau privé accessible uniquement à l'intérieur du pays. Le but sera donc d'énumérer les services et les ressources disponibles sur ce réseau caché.

Si l'on peut situer le contexte, l'ensemble des adresses IP font partie du bloc d'IP **10.0.0.0/8**, ce qui autorise plus de 17 millions d'hôtes différents. Ainsi n'importe qui peut utiliser une de ces adresses et concevoir son propre réseau privé. C'est de ce fait le cas d'un réseau privé à l'échelle nationale. C'est ce qui casse les codes d'un réseau moderne sous lequel l'Iran s'approprie son propre réseau privé qui est accessible seulement à l'intérieur du pays.

Normes sur l'adressage privé

La base du réseau est l'unique attribution d'adresses IP regroupées au sein de sous-réseaux. Aujourd'hui l'espace d'adressage potentiel d'un schéma 32 bits est fini. À l'échelle mondiale, on a besoin de cette unicité afin d'éviter des conflits entre la coordination des différentes adresses IP. Ces responsabilités sont déléguées à un organisme privé, **IANA** : Internet Assigned Numbers Authority où les fournisseurs d'accès Internet obtiennent des blocs d'adresses.
Ainsi des blocs sont réservés pour les réseaux locaux et privés dans le but de laisser libre la gestion de la coordination des adresses.

- Les réseaux privés ne sont pas reliés directement à l'Internet global, ils peuvent être géré par des passerelles intermédiaires
- Les réseaux publics nécessitent un accès vers "l'extérieur" qui maintient une adresse IP qui est globalement non ambiguë et accessible.

La figure suivante montre les allocations des différentes adresses IP pour aider à conserver la réserve limitée d'adresses dans le monde. Cela facilite l'établissement de réseaux plus petits.

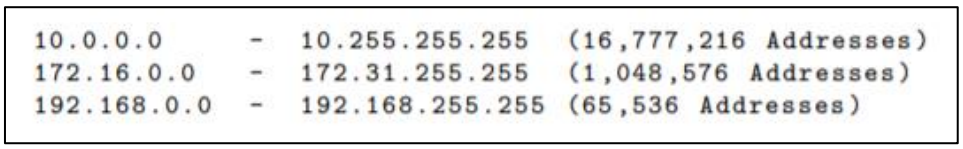

Figure 1 *– Bloc d'adresse privé réservé*

Les réseaux traditionnels utilisent le **NAT** (network address translation) dans le but de permettre à des intermédiaires, d'agir comme des passerelles en envoyant et en recevant de manière transparente du trafic vers Internet au sens large. Mais comme le nombre d'appareils connectés à Internet a considérablement augmenté, le reste d'adresses IP non attribuées a diminué fortement. Nous verrons dans une partie ultérieure les détails de ce service NAT.

Une approche juridique et éthiques

Avant d'avoir une approche sur les résultats de la mise en place de l'expérimentation, il est important d'avoir une approche juridique et éthique sur ce sujet.
L'Iran représente une nation sensible dans la protection ainsi que la gestion de ses données vers l'extérieur, elle couvre des infrastructures ainsi que des données sensibles, qui sont souvent recherchées par les autres pays à travers le monde.

Pour comprendre le réseau privé qui a été créé par l'Iran, l'ensemble des études de ce sujet ont été fait en adéquation avec le respect des règles et des lois. Dans une étude de ce type, il est important de ne pas prendre une place trop importante dans le réseau, il faut rester discret pour éviter d'avoir des problèmes avec les institutions en place.

La collecte des informations dans un projet de ce type est alors forcément limitée, il n'est pas possible d'utiliser l'ensemble des informations toujours dans l'idée d'éviter des problèmes sous-jacents.

Une recherche d'information maximale

Pour comprendre ce qui se passe sur le réseau, il est important de se placer sur différents points du réseau, il est compliqué de faire une généralisation et de tirer des conclusions de manière globale.

L'étude à donc porter sur plusieurs points du réseau, avec une approche sur les différents segments logiques du réseau.
Pour avoir une vision maximale sur l'ensemble du réseau, tout en gardant un comportement non intrusif, les points suivants ont été sélectionnés :

- Un hôte à Téhéran qui sert l'ensemble des agences d'État, comme la radiodiffusion de la république islamique d'Iran.
- Un second hôte à Téhéran pour surveiller les activités autour de plusieurs universités, ministère du Commerce, ou encore des entités liées à la recherche, la science et la technologie.
- L'utilisation d'un HTTP ouverts pour tester des sous-ensembles de réseaux iraniens

Il est tout de même, dans cette étude, très compliqué de faire une analyse sur une grande partie ou un sous-ensemble du réseau sans attirer une attention particulière dans le réseau. Ainsi nous allons voir ce qu'il en est des propriétés internes du réseau.

L'Iran, un filtrage très important

La première analyse de cette étude porte sur la prédominance du filtrage en Iran. En effet, le gouvernement limite énormément l'ensemble des activités sur le pays. L'ensemble des informations pouvant contenir des contenus déterminés à offenser l'ordre politique, moral ou encore religieux, sont complètement radier.

Si un utilisateur souhaite visiter un contenu restreint, une redirection vers un site de l'État prendra place. Ce système de filtrage est placé au niveau du réseau iranien.

Un réseau privé accessible

Une tentative d'envoi de requêtes **HTTP GET** a été établie dans le but d'avoir accès global à un site web à l'intérieur du pays, un domaine qui pointe vers une adresse IP privée ou encore un site web non filtré localisé en dehors du pays. Si la réponse est **200 OK**, alors on arrive au bon titre de page.
L'utilisation d'un réseau privé n'est pas un phénomène nouveau dans la protection des données, en effet l'utilisation d'adresse privée permet la sécurité ainsi qu'une plus grande flexibilité.
Par conséquent on peut se demander à quelle échelle ce type de réseau est utilisé.

Un réseau privé utilisé de manière massive

Si aujourd'hui un plan d'adressage des adresses du réseau public existe, aucun plan n'existe pour les adresses privées. Il est alors compliqué de connaître l'utilisation du réseau privé sans passer par des méthodes parallèles.
Dans cette étude, l'utilisation des chemins d'accès du trafic à permis de faire ce traçage global. De plus, cette méthode à permis de récupérer les identités publiques des hôtes du réseau (voisinages logiques, utilisation ciblée d'espace de réseautage privé, coordination des infrastructures …).
Suite à cette analyse du réseau privé, nous pouvons voir qu'un nombre important de ce qui a été scanné inclut un nom de domaine complet et des adresses publiques comparables à des archives publiques.
Cette première analyse du fonctionnement et de l'utilisation du réseau privé donne une première image de l'utilisation des adresses privées dans le réseau national. Cette utilisation est représentée dans les figures suivantes.

IP Address	Host/Network
10.8.12.18	Iran.ir National Webmail Service
10.8.218.0/24	Pishgaman, ADSL Internet Service Provider
10.10.34.34	Data Communication Affairs's Filtered Site Page
10.10.36.0/24	Telecommunications Company of Iran
10.30.54.0/24	Parsonline, ADSL Internet Service Provider
10.254.50.0/24	Islamic Republic of Iran Broadcasting
10.9.28.0/24	Islamic Republic of Iran Broadcasting
10.143.218.199	Telecommunications Company of Isfahan
10.56.59.198	Khorasgan Islamic Azad University, Isfahan
10.7.234.0/24	Ministry of Agriculture
10.30.170.0/24	Ministry Of Education
10.21.243.37	National Internet Development Agency of Iran

Figure 2 *– Réseaux identifiables et site sur espace IP privé*

lib.atu.ac.ir	10.24.96.14	Allameh Tabatabaie University
www.mdhc.ir	10.30.5.163	Vice Presidency for Management Development and Human Capital
www.iranmardom.ir	10.30.5.148	Vice Presidency for Management Development and Human Capital
erp.msrt.ir	10.30.55.29	Ministry of Science, Research and Technology
ou.imamreza.ac.ir	10.56.51.27	Imam Reza University
www.tehranedu.ir	10.30.95.7	Tehran Education Organization
sanaad.ir	10.30.170.142	Private Individual
ww3.isaco.ir	10.21.201.50	Iran Khodro Spare Parts & After-sales Services Company
iiees.ac.ir	192.168.8.9	International Institute of Earthquake Engineering and Seismology
	169.254.78.139	
	194.227.17.14	
	10.10.3.2	
tci-khorasan.ir	217.219.65.5	Telecommunication Company of Iran, Khorasan
	10.1.2.0	
adsl.yazdtelecom.ir	10.144.0.14	Telecommunications Company of Iran, Yazd
iranhrc.ir	46.36.117.51	Private Individual
	10.30.74.3	
acc4.pishgaman.net	81.12.49.108	Pishgaman, ADSL Access Provider
	10.8.218.4	
lib.uma.ac.ir	10.116.2.5	University of Mohaghegh Ardabili
film.medu.ir	10.30.170.110	Ministry Of Education
www.shirazedc.co.ir	10.175.28.172	Shiraz Electric Distribution Company

Figure 3 *– Nom de domaine et leur responsable*

Bannière de service

Pour évaluer l'étendue du réseau privé, des tests ont été réalisés dans le but d'établir une connexion avec les 17 millions d'adresses privées possibles.
Les résultats présentés sont les suivants : après avoir identifié plus précisément les 16 777 216 adresses IP possibles avec des hôtes, il était alors possible de procéder à l'extraction de données et de mesurer la quantité du contenu web dans l'espace d'adressage privé. En fonction du type de service, un grand nombre de variables peuvent affecter le degré de correspondance entre les résultats et la réalité. Par exemple, beaucoup de routeurs DSL domestiques permettent de configurer le dispositif avec une interface web ou telnet qui serait difficile de faire la différence avec un site Internet normal.
Comme les entreprises hébergent souvent plusieurs sites sur un même serveur, avec une seule connexion, on ne peut pas avoir l'entièreté et la quantité du contenu disponible.

Beaucoup de réponses contenaient des informations qui ont permis d'identifier l'hôte. Différents organismes ressortent, par exemple des organisations impliquées comprennent la diffusion de la République islamique d'Iran ou encore l'agence nationale de développement de l'Internet d'Iran. Par conséquent, cela montre l'utilisation massive d'adresses privées en Iran.

Enregistrements DNS

Lors de l'analyse de la récupération des adresses privées, les études ont montré une forte occurrence de domaine qui conserve des enregistrements DNS pour des adresses IP, privées, valides et accessibles ou plusieurs enregistrements qui incluent des pointeurs publics et privés.
Cependant, l'évaluation des possibles DNS en Iran est compliquée, le fournisseur iranien de domaine de premier niveau .ir, ne partage pas les fichiers qui répertorient les domaines enregistrés. L'étude doit alors se limiter aux ressources publiques ainsi que les bannières de services vues précédemment.

NAT et déviation ICMP

Pour communiquer sur Internet, les machines qui ont une adresse privée, doivent avoir une adresse publique ou alors elles doivent être capable de transiter via une passerelle NAT. Par exemple, si une réponse passe par une passerelle, l'adresse privée de l'hôte sera réécrite avec l'adresse publique.
Des requêtes ICMP ont été envoyées à tous les hôtes en utilisant des données dans le but d'établir une corrélation entre l'adresse privée et la réponse. Il peut y avoir un certain nombre de raisons pour lesquelles un hôte ne pourrait pas répondre, y compris avec des pare-feu. Sur près de 50 000 hôtes interrogés, l'observateur a reçu près de 10 000 réponses parmi lesquelles, un faible pourcentage répondait avec une adresse publique. D'autres ont répondu avec une adresse privée différente de celle interrogée (probablement le fait que la réponse provient d'un intermédiaire).

Données de traçage

Le traçage de l'itinéraire du trafic réseau est trivial et peut fournir des preuves de la participation au système d'adressage privé. On pourrait appliquer cette méthode aux autres destinations du réseau. Par exemple, en traçant les routes allant jusqu'à l'ensemble des adresses IP possibles (commençant par 10. et se terminant par .1). En faisant cela, nous pourrions créer des cartes de chemins, ceci est représenté sur la **figure 4.1 et 4.2**. Ainsi on étend le travail à récupérer les adresses publiques qui sont uniques et déterminer leurs propriétés.

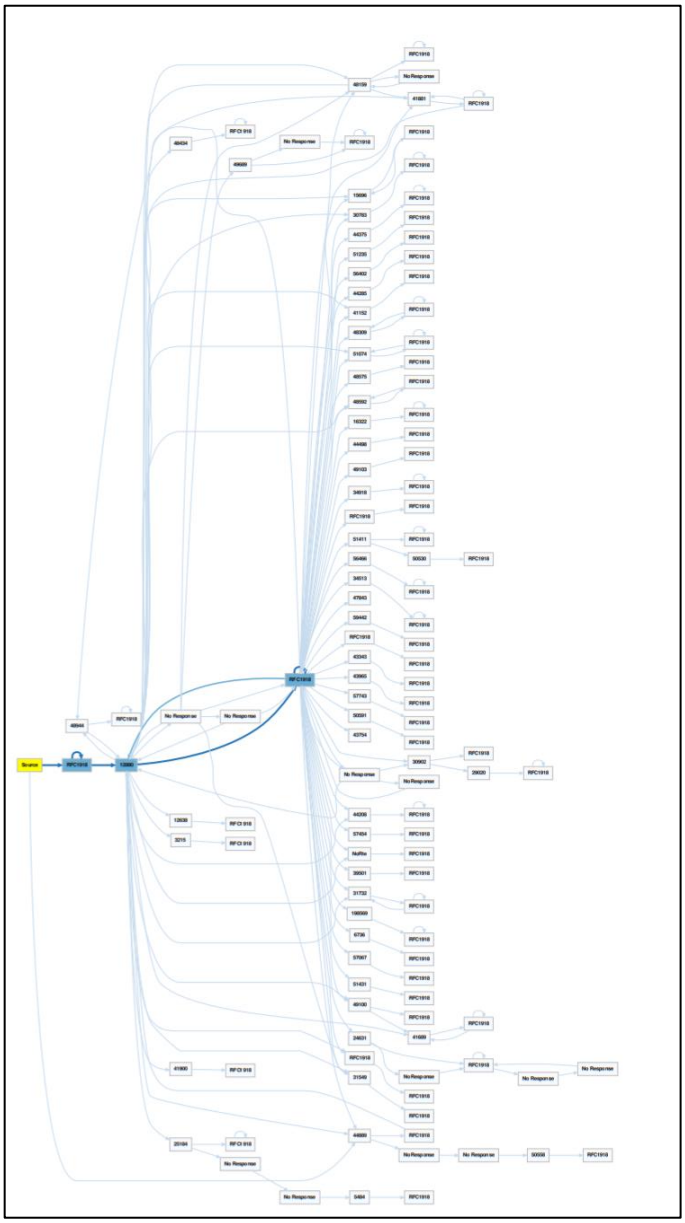

Figure 4.1 *– Chemin depuis l'hôte 1 (traceroute)*

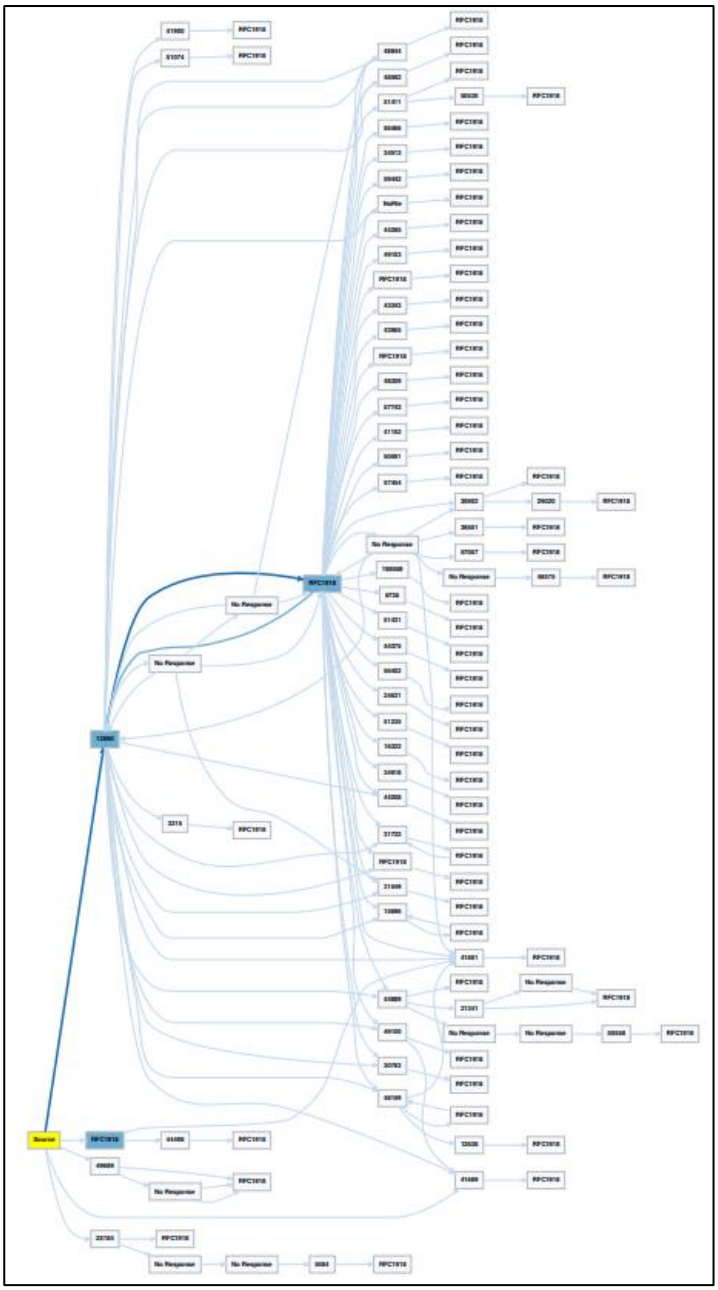

Figure 4.2 *– Chemin depuis l'hôte 1 (traceroute)*

Conclusion

Cet article nous a permis d'éclairer certaines choses concernant les infrastructures de réseaux et d'information de l'Iran. De plus on a pu affirmer que la conception de ce réseau est intentionnelle même si elle peut nous paraître peu usuelle pour des occidentaux. Étant donné les différentes sources et expérimentations que nous avons étudiées, on peut conjecturer du fait que l'Iran possède un réseau interne de plus en plus autonome. Cependant, il reste des questions que nous pouvons explorer dans le but de comprendre pleinement le sujet de l'internet caché en Iran et toutes les stratégies de conception de réseaux.