



“Internet en Iran : Une situation sous tension ”

INFO731 – Sécurité et Cryptographie

MASSIT Clément – CAULLIREAU Dorian – PERROLLAZ
Maverick | IDU4

Résumé :

L'Iran est une puissance nucléaire, un grand nombre de pays souhaite avoir des informations sur les installations. L'ensemble de ces acteurs ont pour objectif de s'infiltrer sur les systèmes internes. Principalement, les attaques sont sur les installations nucléaires, infrastructures économiques ou encore militaire du pays à des fins d'espionnage et de diplomatie coercitive.

Source :

- “Evidence Emerges That Iran Is Building Its Own Hidden 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>
- “Iran and the Soft Ware for Internet Domiance”
<https://www.blackhat.com/docs/us-16/materials/us-16-Guarnieri-Iran-And-The-Soft-War-For-Internet-Dominance-wp.pdf>
- “Iran’s Soft War Get Harder” – **InfoSecurity Magazine**
<https://www.infosecurity-magazine.com/news/iran-soft-war/>
- “ROCKET KITTEN : A campaign with 9 lives” - **CheckPoint**
<https://blog.checkpoint.com/wp-content/uploads/2015/11/rocket-kitten-report.pdf>
- “Rocket Kitten Showing Its Claws: Operation Woolen-GoldFish and the GHOLE campaign” - <https://www.trendmicro.com/vinfo/fr/security/news/cyber-attacks/operation-woolen-goldfish-when-kittens-go-phishing>

Sommaire

1. Des groupes d'acteurs par poignée... des menaces pour l'Iran	4
1.1 Infy, l'attaque aux infrastructures	5
1.1.1. Infy : Une histoire de stratégie	5
1.1.2. Des attaques, des victimes	7
1.1.3. Infy, de la technique à l'attaque	8
1.1.4. Un réseau de personne large et puissant	9
1.1.5. Des régulations pour restreindre les actions d'Infy	10
1.2 Ghambar, beaucoup de cibles et beaucoup d'actions	11
1.2.1. Des cibles, bien précises ...	11
1.2.2. « Ghambar », entre religion et supposition	11
1.2.3. Une force d'attaque unique	12
1.2.4. Une fois infecté, un champ libre pour l'attaquant	13
1.3 Sima, des mails, des mails, des mails	14
1.3.1. Des stratégies, des explications	14
1.3.2. Des organisations importantes pour des systèmes importants	15
2. Rocket Kitten, l'image d'une menace	18
2.1 Différents outils utilisés pour différentes attaques	19
2.2 Plusieurs enquêtes menées	20
2.3 Des analyses démontrant une stratégie préparée	25
3. L'Iran et son "internet caché", un réseau d'adresse privé	27
3.1. La construction d'un réseau réussi	27
3.2. Un réseau privé qui est accessible uniquement au sein du pays	28
3.3. Des tests qui prouvent l'utilisation massive d'adresses privées	29

Depuis la Révolution Islamique de 1979, l'Iran est au ban des nations. En dépit d'une économie exsangue, asphyxiée sous le poids des sanctions internationales, la République Islamique n'a pourtant jamais tiré un trait sur ses ambitions de puissance. Limité dans son accession aux technologies de pointe dans de nombreux domaines par son isolement contraint, l'Iran est passé maître dans l'art de mobiliser des capacités alternatives et subversives lui permettant de défier et déstabiliser ses adversaires les plus avancés technologiquement tels que les États-Unis ou ses rivaux régionaux Israël et l'Arabie Saoudite. Le développement de son programme nucléaire constitue un moyen pour la République Islamique de retrouver une place sur le devant de la scène internationale et de s'imposer comme l'une des puissances incontournables au Moyen-Orient.

Toutefois, les aspirations nucléaires iraniennes suscitent de nombreuses critiques et mettent le feu aux poudres dans cette région déjà explosive et sous haute tension. Depuis plus d'une quinzaine d'années, l'Iran a compris, comme d'autres nations, que le cyberspace représentait un autre levier de puissance, beaucoup plus insidieux, lui permettant de se faire remarquer sans avoir à redouter de potentielles représailles économiques ou diplomatiques. Développé dans un premier temps pour répondre à des problématiques domestiques, le programme cyber iranien s'est ensuite forgé en grande partie en réaction aux attaques dont la République Islamique a été victime. Aujourd'hui, l'Iran considère la stratégie cyber comme un outil offensif tout aussi efficace que des armes conventionnelles, pouvant être mobilisée en cas de montée des tensions dans la région.

Du développement des premières menaces Infy, Ghambar ou encore Sima, en passant par l'analyse de l'omniprésence d'un réseau d'adresse privé, nous allons essayer de mieux comprendre les liens étroits qu'entretiennent la stratégie cyber iranienne et son contexte national et géopolitique actuel.

1. Des groupes d'acteurs par poignée... des menaces pour l'Iran

L'Iran est une puissance nucléaire, un grand nombre de pays souhaite avoir des informations sur les installations. L'ensemble de ces acteurs ont pour objectif de s'infiltrer sur les systèmes internes. Principalement, les attaques sont sur les installations nucléaires, infrastructures économiques ou encore militaire du pays à des fins d'espionnage et de diplomatie coercitive.

C'est uniquement en fin 2009 que des acteurs iraniens ont été inclus à des campagnes d'intrusion, de perturbation d'entreprise privées, d'entités gouvernementales externes à l'Iran et bien d'autres organisations.

Si l'Iran couvre un grand nombre de technologies et d'infrastructures importantes à la sécurité du pays, nous pouvons voir qu'elle garde un retard sur son activité de recherche face. S'il existe un grand nombre d'université de haut niveau en Iran, elle a été lente à développer sa capacité d'espionnage face aux autres pays, qui ont développé de manière exponentielle cette compétence.

Pour contrer les convoitises ainsi que pour compenser le retard dans la recherche, l'Iran élargie ses possibilités avec l'aide d'entreprises externes comme Hacking Team, Finfisher. C'est en partie grâce à l'expertise de ces entreprises externes, que le gouvernement Iranien a pu faire face à un grand nombre d'attaque. Cependant comme nous allons le voir par la suite, l'ensemble des systèmes ne sont pas forcément en adéquation au besoin et aux menaces existantes.

L'Iran étant au centre de plusieurs conflits, sa vulnérabilité est encore plus importante, un grand nombre de pays externe cherche à avoir un maximum de renseignements sur les activités interne du gouvernement. Si les activités iraniennes sont la principale cible des attaques, c'est globalement l'ensemble des civiles et des opposants politiques qui sont pris pour cible.

Par les études de l'article principale **“L'Iran et la guerre douce pour la domination d'Internet”**, ainsi que les articles complémentaires sur les différents sujets, nous allons voir les différents acteurs qui représentent des menaces pour l'État iranien et comprendre les objectifs, les moyens misent en œuvre, ainsi que la finalité de ces projets.

Avant de commencer, il me paraît important de poser les bases sur les théories qui lient le gouvernement et les cerveaux de l'attaque. En effet, si différentes études ont réussi à faire un lien entre le gouvernement Iranien et les cerveaux de l'attaque.

Dans notre contexte pédagogique, nous préférons garder de la distance sur ces analyses, pour éviter les confusions entre réalité et possibilité.

1.1 Infy, l'attaque aux infrastructures

Dans un premier temps, nous allons étudier le cas d'un premier groupe d'acteur, qui ont pour objectif, un angle d'attaque directe vers les infrastructures.

Nous pouvons voir que les premières actions de Infy ainsi que la mise en lumière de ce groupe d'attaque s'est faite durant les élections gouvernementales en Iran, avec un grand nombre d'attaques directement sur la société civile iranienne. La cible ainsi que l'objectif de nuire au bon déroulement des élections a été vérifié : la tendance d'attaque après le déroulement de ces élections a chuté.

Le sujet de Infy ainsi que ses actions, ont été suivi par un grand nombre de personnes à travers le monde. Par exemple, l'entreprise Palo Alto Networks, une grande entreprise américaine de construction de matériel de télécommunication a décrit Infy comme un logiciel malveillant qui fonctionne comme un enregistreur de frappe pour la collecte d'informations des comptes.

Les premières traces d'utilisation de ce logiciel date de 2012, et un grand nombre de versions ont été mises en place, dans le but de toujours avoir une action plus forte et plus précise. L'utilisation ainsi que la mise en service de la première version du logiciel tombe au moment de l'élection présidentielle iranienne en 2013.

Des recherches montrent également que le logiciel est potentiellement plus ancien que les élections, avec des attaques sur la sécurité iranienne dès 2010.

1.1.1. Infy : Une histoire de stratégie

Toute organisation malveillante a des objectifs sur l'ensemble des actions qu'elles réalisent. Pour comprendre le fondement de ces actions, nous allons faire une rétrospective de l'histoire de cette organisation.

Comme nous l'avons évoqué précédemment, l'objectif primaire de l'organisation à tourner sur la sécurité iranienne dans un premier temps, mais rapidement surtout autour des élections de 2013, est la récupération d'informations sur l'opposition politique. Avec ces actions, on cherche à récupérer des informations sur l'ennemi, pour pouvoir le disqualifier.

L'objectif est alors de transmettre un grand flux d'informations continues malveillantes, pour essayer de manipuler les esprits, et manipuler les choix et actions de l'ensemble des civils Iraniens.

C'est donc le souhait de cette transmission d'informations « fake » qui a donné lieu à la diffusion de logiciel malveillant.

La diffusion de ce logiciel devient à alors un jeu d'enfant, en effet les attaquants transmettent des fausses informations pour faire réagir l'utilisateur, pour ensuite l'inviter à télécharger un document (PowerPoint, Fichier texte), avec pour finalité le téléchargement d'un logiciel malveillant.

L'ensemble des acteurs infectés deviennent alors des vecteurs de « contamination », avec une transmission de ce logiciel malveillante en cascade. Plus nous avons de machines infectées, plus la force d'attaque est importante.

Le choix de ce vecteur de transmission est alors stratégique, c'est ainsi que l'organisation s'est tournée vers des personnalités publiques comme des politiques ou des professeurs, pour favoriser cette désinformation.

L'éventail des attaques de Infy est très large et ne se restreint pas uniquement au territoire Iranien. Nous pouvons voir par exemple des attaques sur le ministère des Affaires étrangères danois, rapidement après sa création.

Au cours des différentes années de développement et des différentes versions du logiciel, nous pouvons voir une forte évolution de l'infrastructure et des tactiques du groupe Infy. Avec la présence de nouvelles techniques de surveillance et d'hameçonnage, ainsi que de nouvelles cibles et victimes.

C'est ainsi que nous introduisons la notion de **“Guerre douce”**.

Pour revenir sur l'évolution des moyens de communication, nous pouvons voir une évolution constante sur la précision ainsi que l'importance accordé aux message transmis.

Si au début les messages envoyés par l'organisation étaient très simples, sans corps de mail et uniquement avec des informations pour attirer l'attention, après 2015, l'organisation s'est développée et à commencer à développer ses canaux de communication.

L'objectif de ce développement est de rendre crédible les liens d'hameçonnage, et d'augmenter le taux de conversion entre le nombre d'envoi et le nombre d'infecté. Plus la diffusion de l'information est précise et possible, plus les cibles des attaques peuvent être facilement manipuler.

Au-delà de l'augmentation sur les manières de diffuser l'information, l'organisation à constamment développer ses actions concordant avec des actions politiques, par exemple avec les élections législatives, ou des mails ont été envoyés pour décrédibiliser un opposant politique. La diffusion d'une fausse information avec pour objectif de le décrédibiliser en faisant croire aux civiles de l'utilisation de l'espionnage dans sa famille politique.

Nous pouvons tout de même voir que le facteur de communication peut rapidement devenir limité, en effet une personne qui va subir une première attaque, ne sera pas une future cible potentielle.

C'est ainsi que pouvons voir une diversification des moyens d'attaques, comme la création de site web de scamming, et bien d'autres méthodes sombres. L'évolution de ces méthodes passe également par l'élargissement des technologies comme la présence d'iFrame au cœur de la page web.

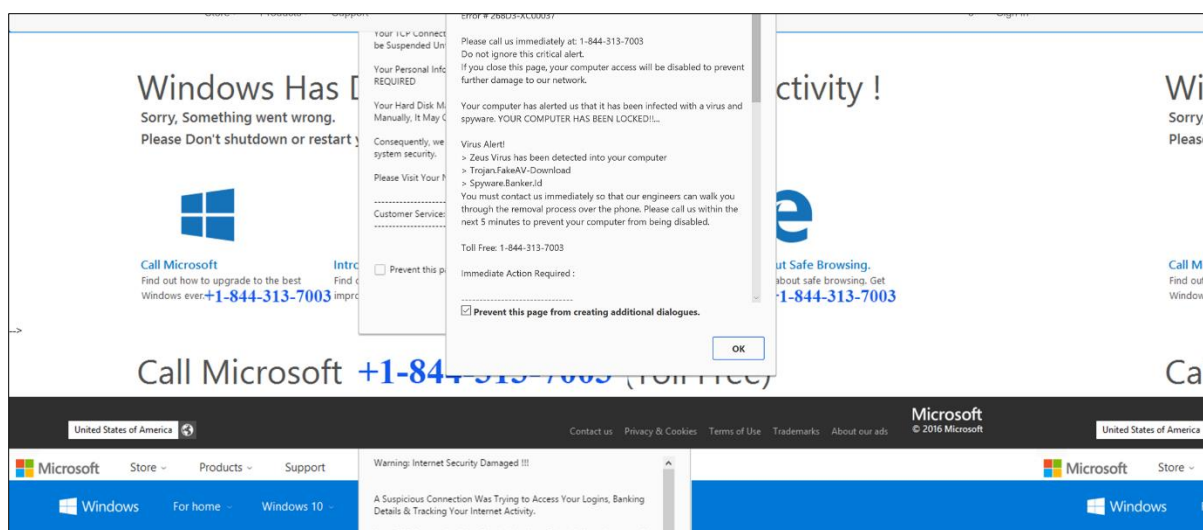


Figure 2 – Exemple d'un site d'arnaque

1.1.2. Des attaques, des victimes

Comme évoqué précédemment, le groupe d'attaque Infy ne porte pas uniquement son vecteur de diffusion sur le territoire Iranien.

Les attaques représentent des menaces internationales, par exemple, sur une courte période, nous pouvons comptabiliser 236 victimes sur 27 pays différents.

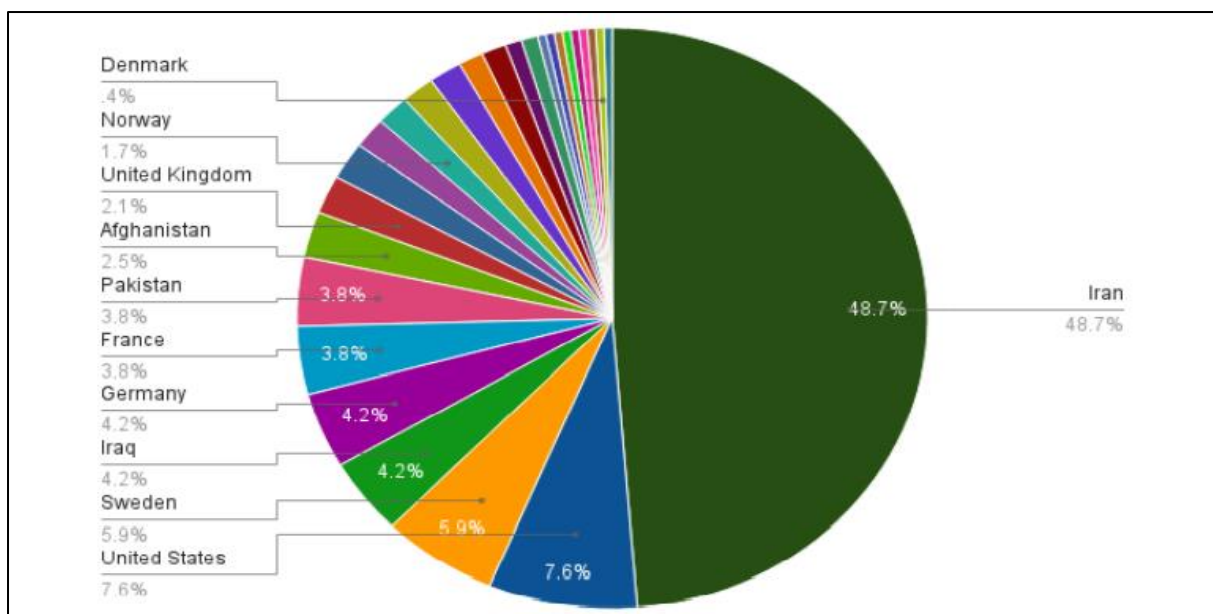


Figure 3 – Répartition des attaques en fonction des pays

Grâce à l'infographie ci-dessus, nous pouvons voir que les attaques portent majoritairement sur l'Iran. En effet 48% des intrusions sont liées à l'Iran. Même si nous pouvons voir la présence d'autres pays, l'utilisation de VPN par exemple peut expliquer le changement de pays. Nous pouvons sans nul doute penser que plus de la moitié des connexions viennent de l'Iran.

Nous pouvons tout de même voir sur les autres pays cibles représente une certaine stratégie. L'espionnage se fait uniquement lorsque la situation représente une importance face au risque encouru. Plusieurs systèmes comme le Soudan, le Pakistan ou encore l'Afghanistan ont été touché pendant de longues périodes.

1.1.3. Infy, de la technique à l'attaque

Technologiquement, la méthode reste simple. Comme nous l'avons aperçu précédemment, pour s'introduire sur les systèmes, ils utilisent des objets qui peuvent s'envoyer par courriel, pour être téléchargé puis rapidement rependu.

La victime reçoit alors un mail avec une information choc sur un sujet d'actualité, et ce mail lui invite à télécharger un document. Lorsqu'il décide de télécharger le document, il doit ensuite juste valider une simple fenêtre Windows et le programme s'installe sur sa machine, il devient alors infecté. Une fois le programme téléchargé, le programme lance de l'enregistreur de frappe et enregistre toutes les données de l'utilisateur petit à petit dans un programme temporaire.

Avec ce programme, l'attaque peut récupérer l'ensemble des données de l'utilisateur et toutes les actions qu'il réalise sur son ordinateur. Cependant, le programme s'attaque majoritairement aux recherches qui sont effectuées sur internet via les différents navigateurs ainsi que sur les messageries pour récupérer les messages qui transitent parmi les différents acteurs.

Le programme permet également l'enregistrement des mots de passes de l'utilisateur, pour pouvoir ensuite utiliser son identité, ou encore surveiller ses activités.

1.1.4. Un réseau de personne large et puissant

Dans le cadre de l'étude sur les différents articles étudiés, des analyses ont été faites pour savoir comment est fixé l'utilisation de l'application malveillante.

Il est alors compliqué de retrouver la tête du réseau, les informations sont souvent masquées et détournées pour rester discrets. L'utilisation de fausses informations comme des données Polonaises ou Indiennes ont eu lieu.

Si les informations du cerveau du projet restent introuvables, des traces des personnes gérant les réseaux sont présentes sur le web, par exemple un commentaire pour défendre des avis négatifs sur les sites de l'organisation ou un commentaire sur un article pour rendre hommage à un commandant.

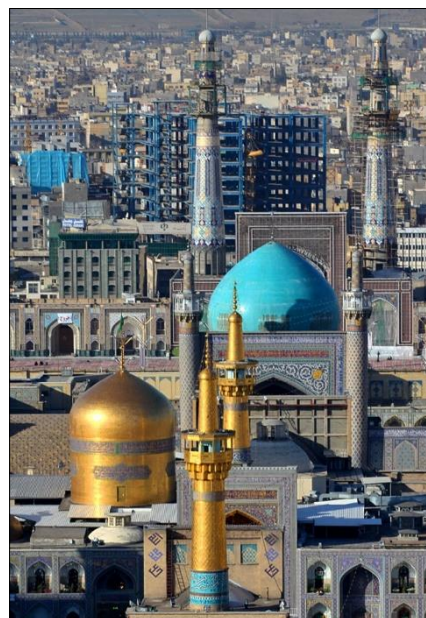


Figure 4 – Photo de Mashad

Si lors d'une action terrestre il est facile de localiser l'ennemie, pour une attaque informatique, la tâche est beaucoup plus complexe, c'est uniquement avec les recherches sur les connexions locales qu'une trace a été découverte sur la province de Khorasan Razavi, potentiellement dans la ville de Mashhad.

Les informations plus précises sur les organisateurs des réseaux restent relativement floues, il est en effet compliqué de retrouver l'ensemble des acteurs, avec les protections qui sont aujourd'hui présentes sur le web.

Nous pouvons tout de même imaginer qu'un grand nombre de personnes se cachent autour de ce réseau et que des stratégies importantes internes aux attaquants sont présentes pour se protéger.

1.1.5. Des régulations pour restreindre les actions d'Infy

Comme nous l'avons vu précédemment, les actions d'Infy représentent de réelles menaces pour la sécurité et la sûreté du pays.

C'est ainsi que différentes mesures ont été prises pour essayer de ralentir le processus et de mettre fin à l'organisation.

Les principales restrictions tournent dans un premier temps autour de la régulation du réseau de télécommunication en Iran. Nous pouvons également voir des mesures plus spécifiques directement pour restreindre Infy, comme la redirection de l'ensemble des solutions Infy, la perte des canaux de communication de l'organisation.

Malgré l'ensemble de mesures prises pour ralentir le programme Infy, nous pouvons toujours voir au moment de l'écriture que le programme est fonctionnel, il continue d'infecter des villes et des cibles sont toujours attaquées.

En effet, l'organisation essaye de contourner les actions mises en place, avec des mises à jour constantes ainsi que des technologies différentes.

Nous pouvons donc voir que le réseau Infy est une source de désinformation et un logiciel malveillant qui a pour but de récupérer un grand nombre d'informations pour ensuite les exploiter. Différentes études ont réussi à faire un lien entre le gouvernement Iranien et les cerveaux de l'attaque.

Dans notre contexte pédagogique, nous préférons garder de la distance sur ces analyses, pour éviter les confusions entre réalité et possibilité.

1.2 Ghambar, beaucoup de cibles et beaucoup d'actions

1.2.1. Des cibles, bien précises ...

Après avoir analysé l'utilisation de Infy, nous allons maintenant faire une rapide entrevue de Ghambar. Dans la même idée que Infy, l'objectif des attaques, tourne autour de l'Iran et des infrastructures qu'elle possède. Ce sont donc les infrastructures économiques, de défense, les entreprises locales ou encore les gouvernements qui sont les principales cibles des attaques ciblées.



Figure 5 – L'Iran, une puissance nucléaire

D'une manière plus restreinte, nous pouvons voir des cibles comme des plaidoyers israéliens, des institutions américaines, des entités saoudiennes, des organisations iraniennes, des bases américaines stratégiques et d'autres institutions à travers le monde.

1.2.2. « Ghambar », entre religion et supposition

Un grand nombre de recherche ont été faite autour de la création de ce groupe d'attaque : question religieuse, variables, ou encore campagnes ... Un grand nombre de théorie tourne autour de ce sujet.

Le nom Ghambar n'est pas une revendication du groupe, mais un nom créer par les chercheurs à ce sujet. En effet, dans le programme, un grand nombre de variables et de fonction utilise ce nom de code. Un indice important sur la revendication.



Figure 6 – Un système en relation avec l'ISLAM

De plus, un second point appuie cette théorie, dans le code un grand nombre de référence tourne autour de dieu et de l'ISLAM. Si cette information semble désuète dans un premier temps, elle exprime les objectifs et les arrières pensées des créateurs du logiciel.

1.2.3. Une force d'attaque unique

Pour se différencier des autres groupes d'attaquants, chaque logiciel utilise des technologies ainsi que des méthodes différentes. Ici, c'est l'utilisation d'un personnage fictif comme appât qui est l'outil mis en place.

L'utilisation de ce logiciel a été prouvée dans l'ouverture d'une université, où la récupération d'informations sensibles a eu lieu avec une vulnérabilité logicielle importante. Ils ont également, et surtout pu utiliser le nom et les informations de l'université pour transmettre des informations.

La technique est simple : on utilise le mail de l'université pour avoir de la crédibilité, on envoie un logiciel qui demande un téléchargement. Si dans un premier temps le fichier semble donner confiance avec par exemple une mise à jour Adobe, le programme est finalement une façade pour cacher un logiciel malveillant. L'ordinateur de la victime devient alors infecté, et peut infecter d'autres personnes (tel un virus chez les humains).

La conception du logiciel permet de laisser le moins d'empreinte possible sur l'ordinateur de la victime. Par exemple, lorsque le logiciel récupère les données de navigation sur l'ordinateur de la victime, nous pouvons voir qu'aucune information n'est stockée directement sur la machine. L'ensemble des informations sont immédiatement envoyées à distance.

Moins de traces sont présentes, moins le risque est présent pour le cerveau du groupe d'attaque.

Pour récupérer un maximum d'information, si les informations ne peuvent pas être directement envoyées à distance, les fichiers sont sauvegardés dans les fichiers de configuration, puis envoyés avant d'être supprimés à jamais.

Pour avoir un champ plus large, le logiciel permet également de télécharger des modules complémentaires, pour avoir encore plus d'information sur la machine. On fait donc des actions différentes en fonction des victimes, pour avoir les bonnes informations sur les bonnes personnes au moment voulu.

1.2.4. Une fois infecté, un champ libre pour l'attaquant

L'étape la plus complexe est d'infecter la machine, une fois que la machine est attaquée est qu'elle à exécuter le fichier malveillant, l'attaquant peut faire l'ensemble des actions qu'il souhaite avec très peu de chance d'être repéré.

Faire le tour de l'ensemble des fonctionnalités possible d'un logiciel malveillant est très compliqué. En effet c'est uniquement lorsque cette fonctionnalité à été mise en place sur plusieurs ordinateurs infectées que nous pouvons la mesure.

Aujourd'hui, les recherches ainsi que les analyses sur les ordinateurs infectées ont montré plusieurs champs d'actions possible : l'autodestruction, exécuter une commande, prendre une capture d'écran, arrêter, démarrer, verrouiller ou encore éteindre l'appareil. Récupérer les données du presse-papiers, désactiver les périphériques, et bien d'autres.

Si d'autres fonctionnalités existent, mais ne sont toujours pas connu, le logiciel permet de tout de même la récupération d'un grand nombre d'informations inquiétantes et dangereuses.

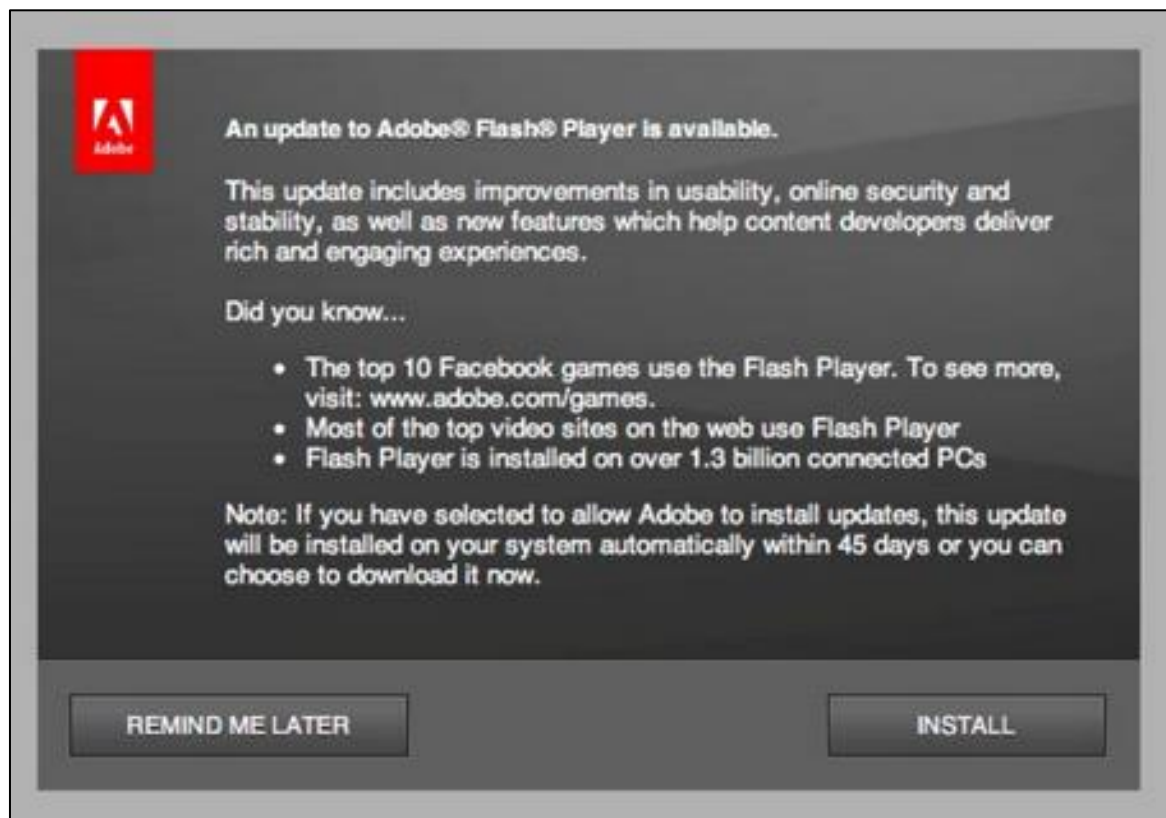


Figure 7 – Exemple d'un exécutable contaminant

1.3 Sima, des mails, des mails, des mails...

1.3.1. Des stratégies, des explications

Si le nom de ce projet n'est qu'un nom donné via la nomenclature des fichiers "PCSimax". Nous pouvons voir dans ces attaques, une nouvelle stratégie, avec des victimes qui recevaient des courriels avec une invitation à lire un article sur l'Iran et l'Afghanistan. Avec pour finalité non pas un lien vers un article, mais un lien vers un questionnaire d'hameçonnage.

Dans ce "projet", nous pouvons tout de même voir une évolution par rapport aux anciennes méthodes. En effet, de réels efforts sur la présentation ainsi que l'écriture du mail sont présents. Un objet intéressant, des données sensibles ce sont l'ensemble de ces points qui on permit un meilleur taux de réussite dans l'attaque.

D'après les études technologiques qui ont été faites sur le logiciel, nous pouvons voir un début d'attaque en février 2016, avec un arrêt dès début mars. Les cibles principales de ce projet ont été des Iraniens de la diaspora qui se concentraient sur la politique étrangère et des questions relatives aux femmes.

Cette attaque à la question des femmes, explique une nouvelle fois le nom du projet "Sima", en effet en persan, il s'agit d'une femme commune, ainsi qu'une expression pour exprimer le visage ou encore l'apparence.

La stratégie de diffusion de l'information en fonction des cibles, tourne autour de différents fichiers. Un fichier pour les politiques, un autre pour les personnes du secteur privé...

Des recherches ont également fait sortir du lot de nombreuses autres tentatives d'usurpation avec les méthodes des fichiers avec une nomenclature précise. Par exemple avec un lien vers un passage télévisé qui invitait à réagir.

Toujours dans ce même groupe d'activiste, nous pouvons voir une autre méthode de diffusion de mauvaise information, avec une usurpation des services de citoyenneté et d'immigration au service de la sécurité. Avec de vraies références ajoutées au mail, mais avec des pièces jointes redirigent vers des logiciels malveillants.

Spearphishing Email - March 2016

From: U.S. Citizenship and Immigration Services <SCOPSSCATA@dhs.gov>
Subject: Alert: Permanent Residence Card

You received this Email because you do not have a Permanent Residence, your Permanent Residence status needs to be adjusted or you need to renew/replace your Permanent Residence Card.

Starting March 9, 2016, customers must fill Form I-485 (can be found at the end of this email), in order to Register Permanent Residence or Adjust Status, and must fill Form I-90 (can be found at the end of this email) in order to Renew/Replace Permanent Residence Card and mail their Form I-485 or I-90 to USCIS local field/International offices. (Offices can be found here: <https://www.uscis.gov/about-us/find-uscis-office>)

USCIS will provide a 30 day grace period from March 9, 2016, for customers who file their Form I-485 or I-90 with one of the USCIS offices. All offices who receive Form I-485 and I-90 during this time will forward the forms to the Chicago Lockbox.

After April 9, 2016, local field/International offices will return all Form I-485 and I-90 they receive and advise customers to file at the Chicago Lockbox.

Download Form I-485, Application to Register Permanent Residence or Adjust Status:

<https://www.uscis.gov/sites/default/files/files/form/i-485.doc>

<<http://148.251.55.114/uscis.gov/sites/default/files/files/form/Form%20I-485,%20Application%20to%20Register%20Permanent%20Residence%20or%20Adjust%20Status%E2%80%AEcod.scr>>

Download Form I-90, Application to Replace Permanent Resident Card: <https://www.uscis.gov/sites/default/files/files/form/i-90.doc>

<<http://148.251.55.114/uscis.gov/sites/default/files/files/form/Form%20I-90,%20Application%20to%20Replace%20Permanent%20Resident%20Card%E2%80%AEcod.scr>>

Contact us: <https://www.uscis.gov/about-us/contact-us>

With Best Regards,

USCIS Service Center.

Figure 8 – Exemple d'un mail diffusé par Sima

1.3.2. Des organisations importantes pour des systèmes importants

Pour comprendre la provenance et les acteurs de ce projet, des analyses d'adresse IP et de serveurs ont montré que le fournisseur principal était Allemand, mais que dans ce groupe de serveur, d'autres site Web étaient en langue persane, ce qui montre un potentiel passage par un revendeur iranien de service.

Si avant la suppression complète de ces services, des archives protégées par mot de passe ont été exfiltrés, les services de renseignements, on réussit à décoder ces archives et récupérer l'ensemble des informations globales.

Nous pouvons voir que sur l'ensemble de ces victimes, la vérification de l'évolution de l'ensemble des techniques d'attaques : ressources, informations supplémentaires, dénomination des fichiers...

Techniquement, les analyses sur cette solution ont été très complexe, en effet les compilations du programme n'ont visiblement qu'été réalisées sur un même serveur et uniquement entre le 29 février et le 1er mars. Soit exclusivement sous 2 jours. Ensuite, les serveurs ont été utilisés de façon discontinue, sur une longue période, pour éviter d'être trop facilement repérable par les services de renseignements et de sécurité.

Sans rentrer dans des considérations techniques avancées, nous pouvons dire que les méthodes d'hameçonnages par le téléchargement d'informations sont très poussées. Elles mènent par exemple au téléchargement de logiciels propres et compliqués à différencier d'une solution sans mauvaises intentions.

Comme nous pouvons le voir avec une solution nommée **"LuminosityLink"** qui ressemble fortement à une interface d'administration, mais avec un but de nuire et de récupérer l'ensemble des informations de la victime



Figure 9 – LuminosityLink, une interface pour tromper.

Les méthodes d'attaques sont de plus en plus larges pour essayer de toucher un maximum de personnes, multiplication des expéditeurs ou encore multiplication des liens et des articles pour éviter qu'il existe un doute chez les victimes.

Nous pouvons voir deux thématiques principales pour l'attaque : **“le droit des femmes”** ainsi que **“le droit de l'homme en Iran”**.

L'ensemble de ces informations, ainsi qu'une analyse des cibles, montrent rapidement que la cible de ces attaques sont dédiées à la surveillance de la société civile ainsi que la diaspora.

Des observations ont également mené à la présence de leur particularité, par exemple des documents copiés des rapports de droit de l'homme, des biographies de personnalité politique.

2. Rocket Kitten, l'image d'une menace

La situation actuelle de l'Iran concernant la cybersécurité s'est développée après une multitude d'attaques dévastatrices. Cela a poussé le gouvernement à développer des capacités cyber dans le but de pouvoir se défendre. Une défense qui on le verra va devenir pour certaines organisations, une force qui leur permettra de concevoir des outils puissants et parfois malveillants.

Nous allons nous intéresser au groupe d'attaquants iraniens : les Rocket Kitten.

Ce groupe de cyber espionnage cible des personnes d'intérêt avec différents outils malveillants. Ce sont les rapports des différentes opérations qu'ils ont effectuées qui nous ont permis de rassembler les preuves vers une origine iranienne.

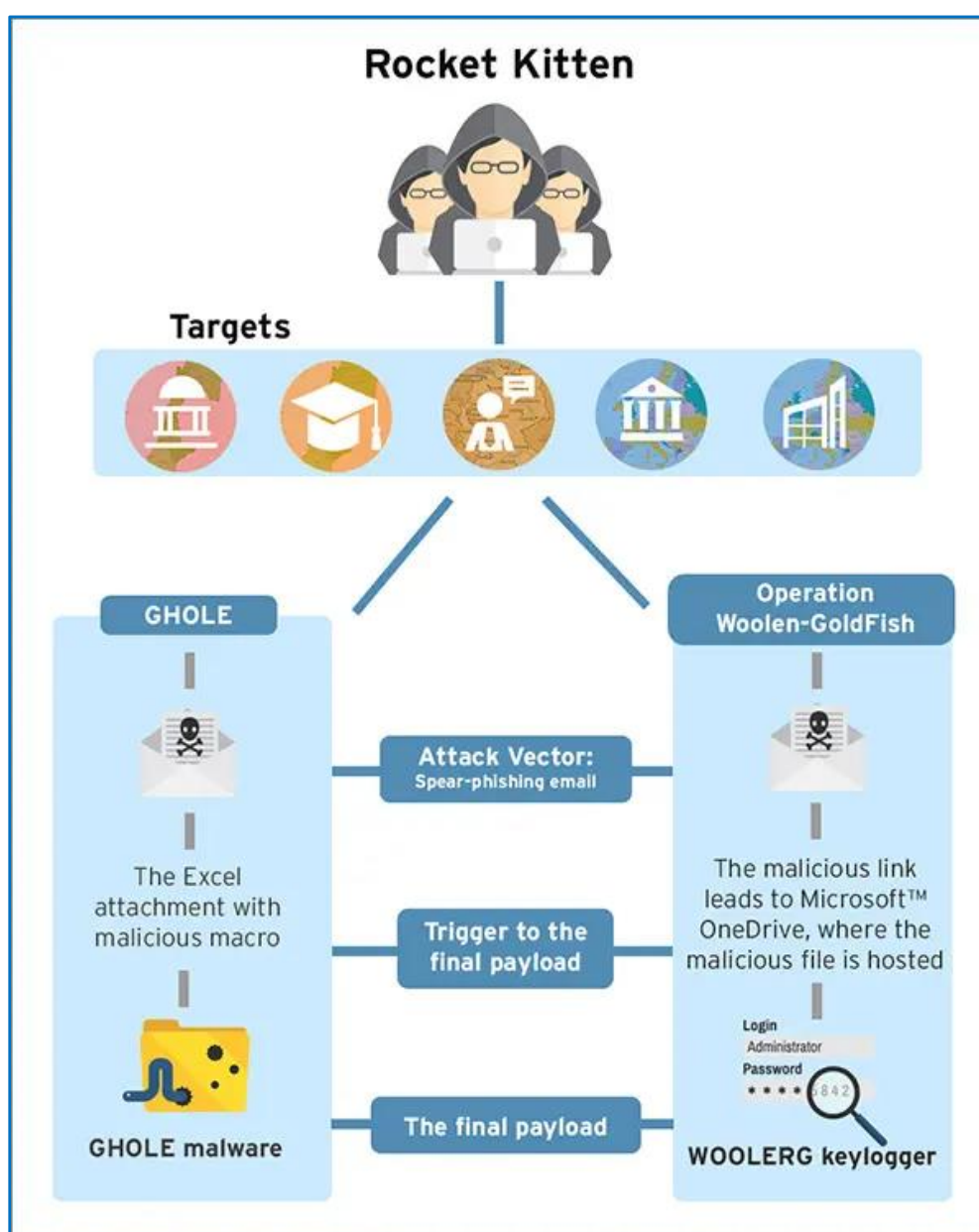


Figure 10 – L'organisation de Rocket Kitten.

Bien que ces rapports datent d'une petite dizaine d'années, les outils que les Rocket Kitten peuvent utiliser sont efficaces sur des systèmes d'exploitation que la plupart des gens utilisent. Cela prouve leur potentiel et l'efficacité de leur campagne.

2.1 Différents outils utilisés pour différentes attaques

Ces rapports montrent une stratégie d'attaque qui revient souvent : le phishing. On sait qu'une campagne de phishing est d'autant plus efficace que la page sur laquelle les victimes sont est bien conçue.

Les outils que les Rocket Kitten utilisent sont variés et pertinents selon leur utilisation.

- **Cwoolger** — un logiciel en C++ (keylogger). Il enregistre toutes les frappes sur le clavier et envoie les données sur un serveur.
- **Wrapper/Gholee** — un outil de pénétration de machine à distance
- **FireMalv** — un outil qui vole les informations d'identification. Il copie des mots de passe stockés dans Firefox.

Les investigations de Check Point ont montré grâce aux attaques, l'utilisation des outils suivants :

- **.NETWoolger**— un keylogger basé sur .NET. Fonctionnement similaire à **CWoolger** . Les attaquants alternent entre les deux outils au cas où l'un est détecté.
- **MPK**— un logiciel qui permet d'enregistrer les clés, l'exécution de commandes, les captures d'écran et la surveillance du trafic.

Il y a en plus d'autres outils que les attaquants utilisent pour cibler les sites Web.

- **Metasploit**— une plateforme d'intrusion open source. Il s'agit d'un exécutable qui permet l'accès à la machine. Cet exécutable est dans les mails de phishing des victimes.
- **Havij & SQLMap**— un outil d'injection SQL. Havij est basé en Iran et SQLMap est un outil open source.
- **Acunetix & Netsparker**— un outil de détection de vulnérabilités des sites Web.
- **WSO Web Shell**— un script PHP qui permet un accès au serveur et réaliser des actions dessus.
- **NIM-Shell**—un outil iranien similaire au **WSO Web Shell**. Il utilise des script Perl sur le serveur.

2.2 Plusieurs enquêtes menées

Beaucoup d'enquêtes ont eu lieu dans le but de déchiffrer le style et la stratégie de ce groupe. CheckPoint est un fournisseur mondial de services de sécurité dans les systèmes d'information. Cette entreprise participe activement à l'enquête concernant un incident d'attaque du groupe sur le réseau d'un client.

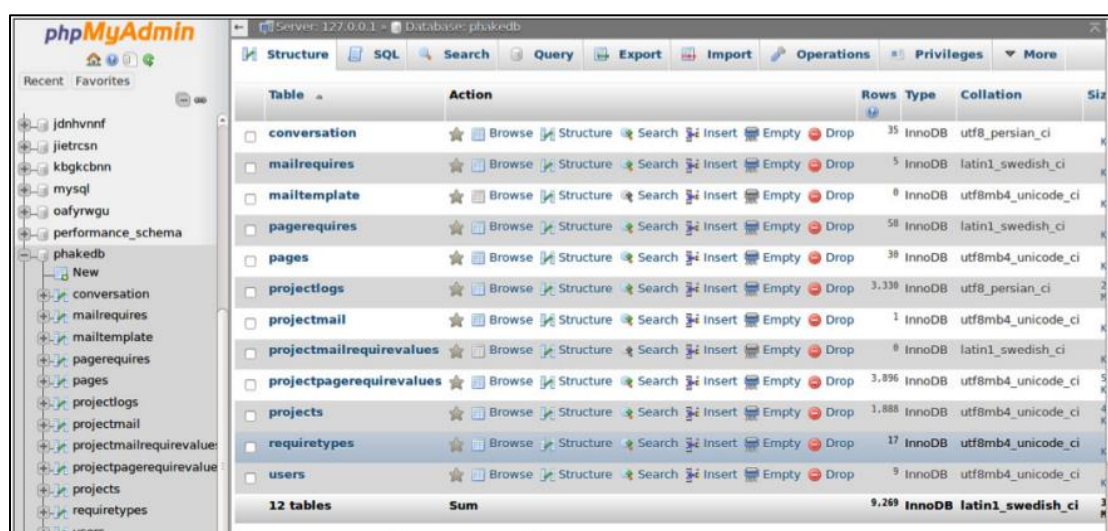
Pour comprendre comment l'attaque a été menée, il a fallu communiquer avec le serveur web de phishing. CheckPoint a appris que l'adresse IP qui a été utilisée revenait plusieurs fois pour pleins de domaines malveillants.

Ils ont donc commencé à effectuer des requêtes GET sur le serveur web pour tenter de naviguer sur des pages connues. Pour quelques réponses, un 200 OK était affiché pour le domaine /xampp.

Ainsi ils sont arrivés sur l'interface de phpMyAdmin et ils ont compris que phpMyAdmin avait été configuré pour permettre un accès root sans mot de passe pour tous les visiteurs. Il se pourrait que cette configuration soit l'image d'un trou si béant. Cela ressemble fortement à un leurre. Pourquoi des attaquants si rusés feraient preuves d'autant d'amateurisme, en laissant la base de données de leur serveur de phishing autant exposée.

La base de donnée avait le nom de '**phakeddb**', il s'agit d'un set de tables et de dataset très croustillants pour les chercheurs de campagnes de lutte contre les logiciels malveillants.

En parcourant les tables, ils ont trouvé l'application web de phishing probablement développée par les attaquants des Rocket Kitten. Cette application génère la page de phishing personnalisée pour la cible pour les services du type Gmail, YouTube... Cette plateforme était nommée '**Oyun Management System**'.



The screenshot shows the phpMyAdmin interface for a database named 'phakeddb'. The left sidebar lists the database and its tables. The main panel displays the 'Structure' tab for the 'phakeddb' database, showing a list of 12 tables with their respective actions, row counts, types, and collations.

Table	Action	Rows	Type	Collation	Size
conversation	Browse Structure Search Insert Empty Drop	35	InnoDB	utf8_persian_ci	
mailrequires	Browse Structure Search Insert Empty Drop	5	InnoDB	latin1_swedish_ci	
mailtemplate	Browse Structure Search Insert Empty Drop	0	InnoDB	utf8mb4_unicode_ci	
pagerequires	Browse Structure Search Insert Empty Drop	58	InnoDB	latin1_swedish_ci	
pages	Browse Structure Search Insert Empty Drop	38	InnoDB	utf8mb4_unicode_ci	
projectlogs	Browse Structure Search Insert Empty Drop	3,330	InnoDB	utf8_persian_ci	
projectmail	Browse Structure Search Insert Empty Drop	1	InnoDB	utf8mb4_unicode_ci	
projectmailrequirevalues	Browse Structure Search Insert Empty Drop	0	InnoDB	latin1_swedish_ci	
projectpagerequirevalues	Browse Structure Search Insert Empty Drop	3,896	InnoDB	utf8mb4_unicode_ci	
projects	Browse Structure Search Insert Empty Drop	1,888	InnoDB	utf8mb4_unicode_ci	
requiretypes	Browse Structure Search Insert Empty Drop	17	InnoDB	utf8mb4_unicode_ci	
users	Browse Structure Search Insert Empty Drop	9	InnoDB	utf8mb4_unicode_ci	
12 tables	Sum	9,269	InnoDB	latin1_swedish_ci	

Figure 11 – L'organisation des données de Rocket Kitten.

Examinons la table des utilisateurs :

user_id	user_name	user_pass	user_nickname	user_created_date	user_lock	isadmin	pcount
49	admin	e10adc3949ba59abbe56e057f20f883e	super admin	2014-08-09	0	UM RT P MT UPL	22
50	anonymous	09d2b6cc9114ed718d9145fa40ed04f8	Anonymous	2014-08-09	0		8
51	merah	c12c563b4584be86a94dcba01aa80d0a	mire	2014-08-17	0		11
52	124	e87aa71e42c7de4780f448c8e92b50cd	razavi	2014-08-17	0	0	18
53	kaveh	46ec41ac0432182829250c0da50f89bb	kaveh	2014-08-17	0	0	10
54	ahzab	7a96925c26ec83a134f2014b77e01211	Ahzab	2014-08-20	0		40
55	attache	827ccb0eea8a706c4c34a16891f84e7b	irakli	2014-08-20	0	0	35
59	amirhosein	e89b359ba9008c1e1fda2bbe3374893e	ParsAAA	2014-08-21	0	0	10
60	john	e10adc3949ba59abbe56e057f20f883e	john	2014-08-24	0		10

Figure 12 – Vision d’ensemble de la table utilisateur.

Sur cette table, on voit que le hash code du mot de passe du super admin est **'e10adc3949ba59abbe56e057f20f883e'**. Les habitués de la cryptographie reconnaîtront la chaîne de caractères : **123456** (cette chaîne n'était pas la seule chaîne de caractère très simple à casser).

En regardant les utilisateurs de la database, on peut voir des noms Persans, tels que merah, kaveh, ahzan, ou amirhosein. Ces personnes étaient les potentiels opérateurs de la campagne chargé de l'ingénierie sociale et de la personnalisation d'une page de phishing pour les différentes cibles.

Cela correspond parfaitement à la stratégie que le groupe adopte, c'est-à-dire créer des pages web de phishing parfaitement corrélées avec l'intérêt des victimes.

msg_id	sndr_id	date	content	viewed
17	51	2014-09-16 03:00:00	http://syntaxmarketing.com.au/wp-content/uploads/2...	1
18	51	2014-09-17 00:00:00	https://www.youtube.com/watch?v=VZmdhwd3axw	1
22	54	2014-09-22 00:00:00	http://profiles.google.com/inc.gs/?_schema=1326&m...	0
24	52	2014-10-01 12:10:25	https://mail.mail2.mod.gov.af/owa/auth/logon.aspx?...	0
25	52	2014-10-05 00:00:00	https://cid-c4351db11d15e77f.users.storage.live.co...	0
26	52	2014-10-05 00:00:00	10/r	0
28	51	2014-10-26 00:00:00	https://accounts.google.com/VA?c=COM3Ijn_2-CSogEQ9...	0
29	51	2014-10-29 00:00:00	Adrese asli: http://outlook.com/owa/biu.ac.il redi...	0
30	51	2014-10-29 00:00:00	http://www.youtube.com/watch?feature=youtu.be&v=-S...	0
31	51	2014-10-29 00:00:00	http://www.youtube.com/watch?feature=youtu.be&v=-S...	0
32	51	2014-10-29 00:00:00	Sign in to continue to YouTube	0
33	55	2014-10-29 00:00:00	please 20 subject for me. tank you attache	0
34	51	2014-11-24 00:00:00	http://profiles.faceboek.in/loginuser/?_schema=198...	0

Figure 13 – Table des conversations

Beaucoup de messages contiennent des liens vers de nombreuses pages de phishing et parfaitement corrélés avec des pages d'attaques signalées. Ce qui prouve que cette base de données est en effet en corrélation directe avec les attaques de Rocket Kitten.

On remarque alors beaucoup de template de codes pour les pages de phishing qui inclus le descriptif de 'Victim Full Name' ou 'Victim User Name'.

req_id	req_exp	req_desc	req_exam
18	%VEA%	Victime Email Address	wool3n.h4t@gmail.com
19	%VFN%	Victim Full Name	John Kerry
20	%VAU%	Victim Avatar Url	http://exam.com/avatar.jpg
21	%DESC_1%	Description (1)	No Example
22	%DESC_2%	Description (2)	No Example
25	%VF%	Victim Family	Kerry
26	%VN%	Victim Name	John
27	%FPLT%	Fake Page Link Text (For email message)	No Example
28	%FPLU%	Fake Page Link Url	No Example
29	%VUN%	Victim User Name	wool3n.h4t
30	%EMAIL_1%	Email Address (1)	No Example
31	%EMAIL_2%	Email Address (2)	No Example
32	%VNN%	Victim Nick Name	Woolen
33	%IMG_1%	Image Url (1)	No Example
34	%IMG_2%	Image Url (2)	No Example
35	%SFE%	Supervisor Email (Fake Mail)	supervisor@ybsoft.com
36	%TMP%	Temp Value	No Example

Figure 13 – Table des requiiretypes

De plus, lorsque la table **'project'** a été étudiée, une découverte importante a été trouvée. Un **'project'** est une simple victime (ciblée via le courriel) avec un lien spécifique pour lequel il serait envoyé à la victime. Ainsi avec toutes les données qu'il a été possible de récolter, il est possible de voir les modèles de pages associées à chaque victime.

proj_id	proj_name	page_id	user_id	proj_date	proj_url	time_stamp
1148	wool3n.h4t@gmail.com	41	54	2014-09-14	http://google-profiles.com/?_schema=1148&md=32331	1432651592
1149	wool3n.h4t@gmail.com	41	54	2014-09-14	http://google-profiles.com/?_schema=1149&md=24266	
1151	wool3n.h4t@gmail.com	48	50	2014-09-14	http://outlook.profile.hmail.us/new/?_schema=1151&md=1410751030	1410751030
1152	wool3n.h4t@gmail.com	48	50	2014-09-14	http://outlook.profile.hmail.us/new/?_schema=1152&md=1410804467	1410804467
1153	wool3n.h4t@gmail.com	48	50	2014-09-14	http://outlook.profile.hmail.us/new/?_schema=1153&md=1410804467	
1154	wool3n.h4t@hotmail.com	48	50	2014-09-14	http://outlook.profile.hmail.us/new/?_schema=1154&md=1410804467	
1155	wool3n.h4t@gmail.com	41	54	2014-09-14	http://google-profiles.com/?_schema=1155&md=31367	1410812432
1156	wool3n.h4t@gmail.com	41	54	2014-09-14	http://google-profiles.com/?_schema=1156&md=17253	1411011128
1157	wool3n.h4t@hotmail.com	48	50	2014-09-14	http://outlook.profile.hmail.us/new/?_schema=1157&md=1410804467	
1158	wool3n.h4t@gmail.com	48	50	2014-09-14	http://outlook.profile.hmail.us/new/?_schema=1158&md=1410804467	
1159	wool3n.h4t@gmail.com	48	50	2014-09-14	http://outlook.profile.hmail.us/new/?_schema=1159&md=1410804467	
1160	wool3n.h4t@gmail.com	41	54	2014-09-14	http://google-profiles.com/?_schema=1160&md=10193	1410810084
1161	wool3n.h4t@gmail.com	48	50	2014-09-14	http://outlook.profile.hmail.us/new/?_schema=1161&md=1410804467	
1162	wool3n.h4t@gmail.com	48	50	2014-09-14	http://outlook.profile.hmail.us/new/?_schema=1162&md=1410804467	1432652579
1163	wool3n.h4t@gmail.com	51	50	2014-09-15	http://members.google-it.info/?_schema=1163&md=1414391670	1414391670
1164	wool3n.h4t@GMAIL.COM	41	54	2014-09-15	http://google-profiles.com/?_schema=1164&md=20601	1411341118
1165	wool3n.h4t@gmail.com	41	54	2014-09-15	http://google-profiles.com/?_schema=1165&md=28997	1410814674
1166	wool3n.h4t@gmail.com	41	54	2014-09-15	http://google-profiles.com/?_schema=1166&md=32180	1432650666
1169	wool3n.h4t@gmail.com	42	49	2014-09-15	http://members.google-it.info/?_schema=1169&md=2410814674	1432650666

Figure 14 – Table des projets

Chaque victime est associée à une page de phishing avec une url spécifique que l’on retrouve dans ‘proj_url’ avec un identifiant.

Ainsi les attaquants connaissent leurs victimes. On peut penser qu’un autre groupe de cyberespionnage aurait pu faire d’autant plus de dégâts qu’ils auraient eu des informations privées de leurs victimes.

Par ailleurs, on a des informations sur les logs dans une table 'projectlogs'. Elle contient des logs pour chaque visite de toute page de phishing. Ainsi avec toutes ces données on a pu récolter les analyses des activités de phishing sur une année d’août 2014 jusqu’à août 2015.

log_id	proj_id	log	date	viewed
50971	2583	</br>Page viewed on Monday 2015-08-17 At 12:19:45<...	2015-08-17	1
50972	2583	</br>Page viewed on Monday 2015-08-17 At 12:21:50<...	2015-08-17	1
50973	2583	</br>Page viewed on Monday 2015-08-17 At 12:23:42<...	2015-08-17	1
50974	2583	</br>Page viewed on Monday 2015-08-17 At 12:23:56<...	2015-08-17	1
50976	2583	</br>Page viewed on Monday 2015-08-17 At 12:27:35<...	2015-08-17	1
50993	2585	</br>Page viewed on Monday 2015-08-17 At 14:11:0</...	2015-08-17	1
50994	2585	</br>Page viewed on Monday 2015-08-17 At 14:11:1</...	2015-08-17	1
50995	2586	</br>Page viewed on Monday 2015-08-17 At 14:17:43<...	2015-08-17	1
50996	2586	</br>Page viewed on Monday 2015-08-17 At 14:17:58<...	2015-08-17	1
50997	2586	</br>Page viewed on Monday 2015-08-17 At 14:18:11<...	2015-08-17	1
51000	2586	</br>Page viewed on Monday 2015-08-17 At 14:49:6</...	2015-08-17	1
51001	2586	</br>Page viewed on Monday 2015-08-17 At 14:51:44<...	2015-08-17	1
51002	2586	</br>Page viewed on Monday 2015-08-17 At 14:51:49<...	2015-08-17	1
51003	2586	</br>Page viewed on Monday 2015-08-17 At 14:52:38<...	2015-08-17	1
51106	2573	</br>Page viewed on Tuesday 2015-08-18 At 9:4:23</...	2015-08-17	0
51107	2588	</br>Page viewed on Tuesday 2015-08-18 At 9:38:39<...	2015-08-17	1
51108	2588	</br>Data sent from victim: </br></br>submitted = 1...	2015-08-17	1
51109	2588	</br>Page viewed on Tuesday 2015-08-18 At 9:39:36<...	2015-08-17	1
51110	2588	</br>Page viewed on Tuesday 2015-08-18 At 9:39:54<...	2015-08-17	1
51111	2588	</br>Page viewed on Tuesday 2015-08-18 At 9:41:22<...	2015-08-17	1
51112	2588	</br>Data sent from victim: </br></br>submitted = 1...	2015-08-17	1
51135	2579	</br>Page viewed on Tuesday 2015-08-18 At 14:4:50<...	2015-08-18	0

Figure 15 – Logs de chaque accès à n’importe quelle page de phishing

En continuant d’analyser le serveur, une interface a été découverte, il s’agit de ‘Webalizer’. Elle fournit des analyses utiles, des statistiques concernant les liens fréquemment consultés. Des analyses ont permis de poursuivre l’enquête notamment avec l’accès de l’attaquant aux sites. Des headers de références ont été trouvés, ce qui mène à un chemin sur un même serveur de connexion :

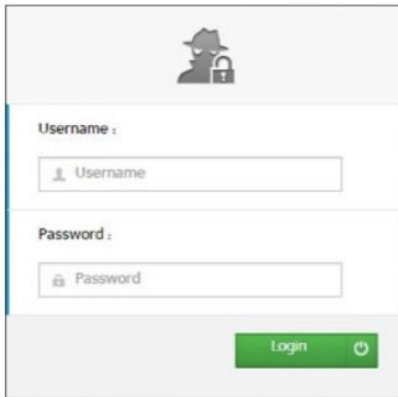


Figure 16 – Ecran de connexion

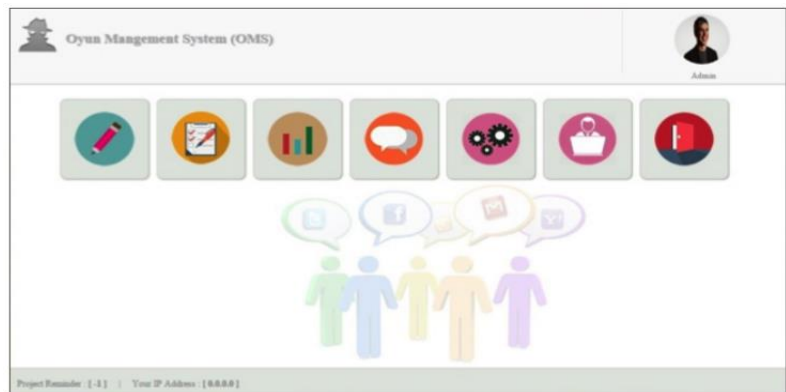


Figure 15 – Le système de management Oyun

C'est ce qui ressemble au portail d'accès secret à la plateforme de phishing. Avec cette page, n'importe qui peut entrer ses propres informations et se faire pirater. C'est le risque le plus invisible pour des individus lambdas.

Ainsi avec l'ensemble des informations obtenues depuis le début de cette enquête il a été possible de se connecter en tant qu'administrateur (figure 15) :

Il s'agit du système '**Oyun**', qui a pour photo de profil Larry Page, l'un des pères fondateurs de Google. Le reste de la page permet un accès vers la base de données 'phakeddb' avec une plateforme de messagerie interne comme nous l'avons vu avec la table 'conversation'.

2.3 Des analyses démontrant une stratégie préparée

Dans cette partie nous allons analyser la stratégie d'attaque. Les attaquants agissent de la manière suivante : courriel, appels téléphoniques avec fausses identités, etc. Ils étudient leur victime avant d'agir, adaptent leur stratégie, et construisent les mails de phishing de manière minutieuse.

Nous allons analyser la base de données des victimes du système 'Oyun'. Cette base de données n'est qu'une vue partielle des attaques, puisqu'elle contient des données allant d'août 2014 à août 2015.

L'analyse de la base de données met en évidence que le volume de cette base de données suggère une opération étendue, ou encore le travail d'un groupe de personnes pendant des mois. Ainsi avec les logs on a les informations concernant l'IP de visite du pays géolocalisé.

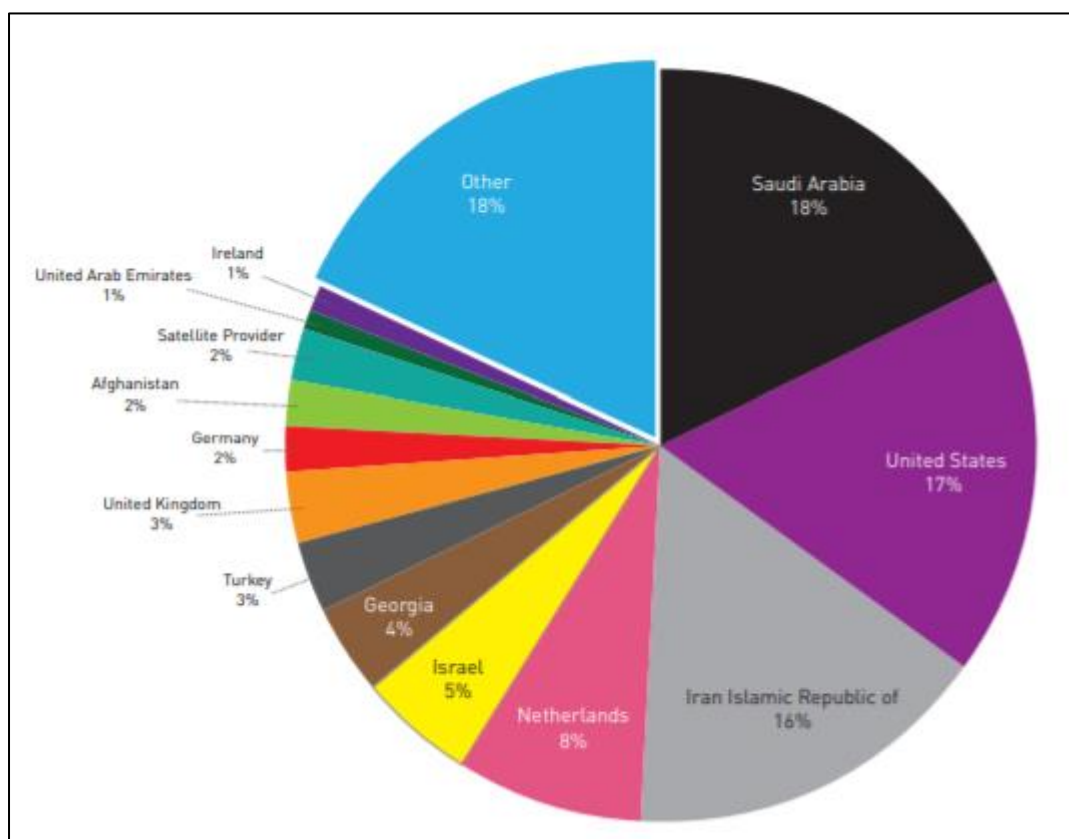


Figure 14 – Distribution des pays en fonction des visites des pages de phishing

De plus, on sait que les attaquants utilisent des adresses venant de l'Iran, mais aussi des VPN depuis les Etats Unis, l'Allemagne, l'Arabie Saoudite et les Pays-Bas. On a alors le diagramme suivant, montrant les logs de phishing avec les succès au fil du temps sur la période d'août 2014 à août 2015.

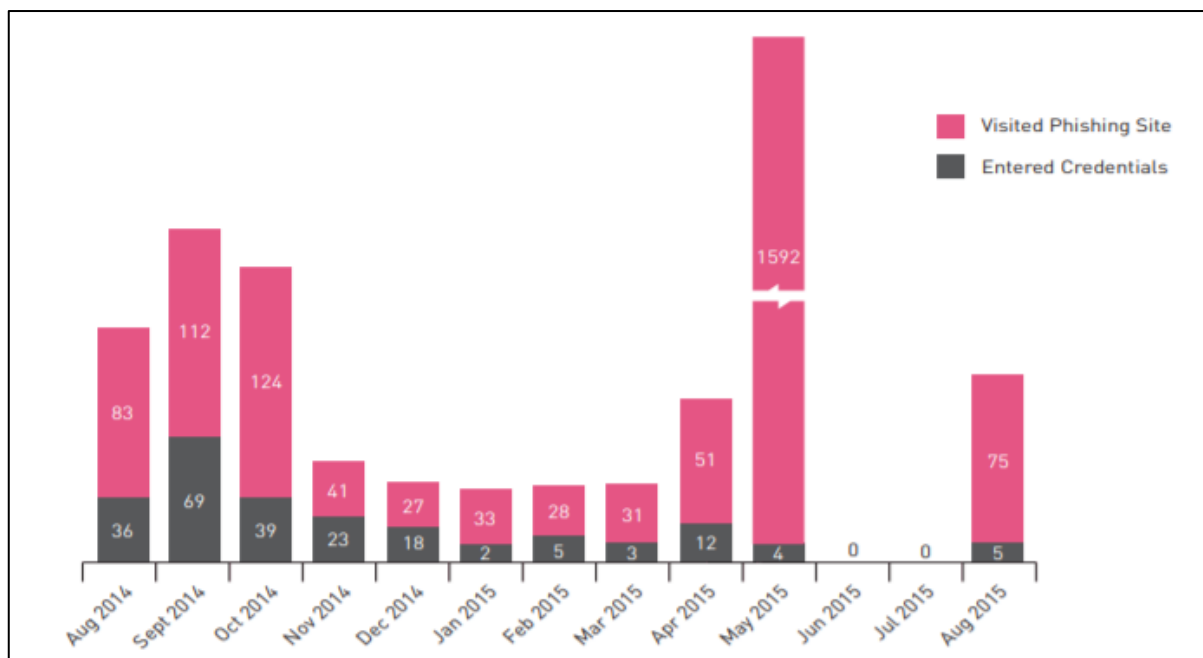


Figure 14 – Logs des pages de phishing avec les succès en fonction du temps

- En moyenne toutes les pages de phishing ont réussi à 26% à tromper les victimes pour qu'elles entrent leurs informations d'identification. On remarque que ces résultats sont plutôt élevés, ce qui prouve la pertinence de leurs cibles et les mails bien adaptés.
- En mai 2015, on observe un pic de visite de sites avec très peu de succès. En effet, ces requêtes proviendraient d'IP Israéliennes où aucune donnée n'est fournie. Il s'agit donc des tentatives de brute-force sur les pages de phishing.
- Les attaquants semblent avoir fermé leur plateforme en juin et juillet 2015 à cause des différentes publications ayant été publiées. Ils ont repris leur activité, avec la particularité que la base de données avait été migrée à partir d'un serveur utilisé précédemment.

Avec toutes les enquêtes, les rapports, les témoignages concernant le groupe d'attaque des Rockets Kitten on peut affirmer que ce groupe a établi une stratégie d'attaque particulièrement bien construite. C'est ce qui peut représenter une menace d'ampleur pour l'Iran, en effet avec l'ensemble des données volées et des différents outils malveillants utilisés. Il se pourrait que des personnes d'intérêt soient ciblés par d'autres groupes de cyberattaques. Il est évident que d'autres groupes émergent avec d'autres intentions, d'autres convictions et d'autres ambitions qui pourront être à l'avenir de réels risques.

3. L'Iran et son “internet caché”, un réseau d'adresse privé

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.

3.1. La construction d'un réseau réussi

Dans un premier temps, il est important d'avoir une approche sur les résultats de la mise en place de l'expérimentation, et par ailleurs 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.

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 a 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.

Ces propriétés internes passent par un filtrage du réseau qui est très important. 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. Il est alors impossible d'accéder à des plateformes en dehors de l'Iran. Ce réseau est donc privé mais quand est-il de l'adressage privé ?

2.2. Un réseau privé qui est accessible uniquement au sein du pays

Comme nous l'avons vu, le filtrage de ce réseau est particulièrement important. Ainsi on peut s'intéresser à l'accessibilité de celui-ci. C'est donc par des tests qu'il faut évaluer toutes les caractéristiques.

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. 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 ...).

Pour donner 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 15 et 16.

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 15 – 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
iees.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	
tc-i-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
iranhr.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 16 – Nom de domaine et leur responsable

3.3. Des tests qui prouvent l'utilisation massive d'adresses privées

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.

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.

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 pares-feux. 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).

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 12 et 13**. Ainsi on étend le travail à récupérer les adresses publiques qui sont uniques et déterminer leurs propriétés.

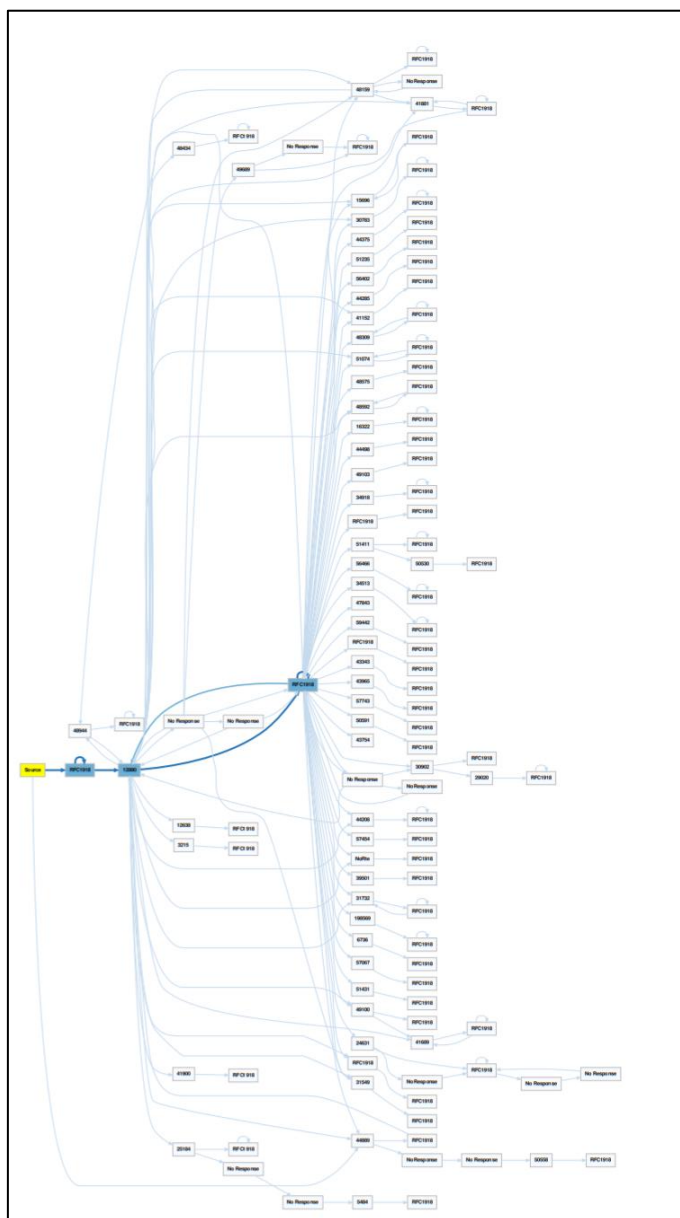


Figure 4.1 – Chemin depuis l'hôte 1 (traceroute)

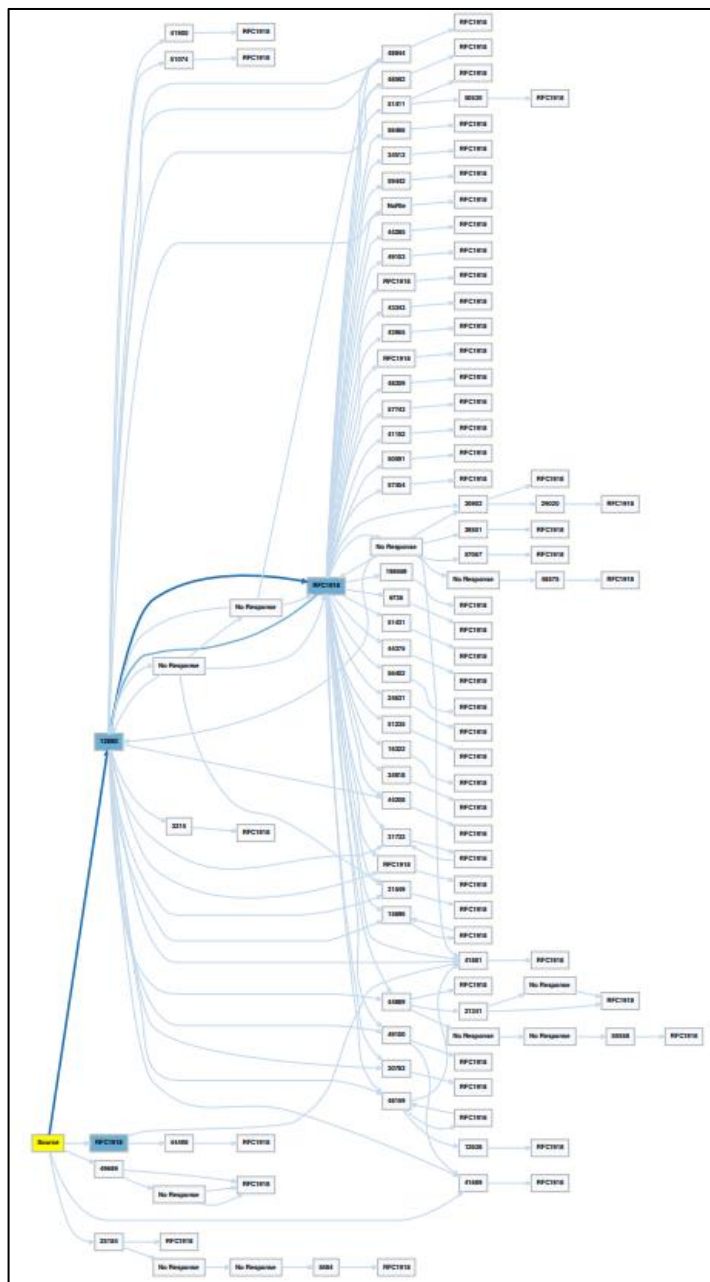


Figure 4.2 – Chemin depuis l'hôte 1 (traceroute)

Cette notion 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.

Conclusion

Pour conclure sur l'ensemble des études que l'on a pu voir, nous avons vu que l'Iran sort la tête de plusieurs événements concernant la sécurité. On connaît aujourd'hui la puissance nucléaire de l'Iran et certaines informations intéressent un grand nombre de pays. Il est inévitable que cette puissance subisse différentes attaques, et en particulier des cyber agressions.

On a vu différents exemples de groupes d'attaque qui sont devenus aujourd'hui des terrains d'entraînement pour les chercheurs en sécurité informatique. Par exemple, Infy qui est friand d'attaquer les infrastructures possède un réseau de personnel large et qui est puissant. Ensuite on peut citer Ghambar, dont la stratégie d'attaque est orientée vers un modèle où le nombre de cibles doit être un point important. Ce groupe attaque un grand nombre de victimes sous la pression d'actions variées. Une fois la victime infectée, il s'agit d'une aubaine pour ce groupe. De plus, une autre stratégie serait d'attaquer l'outil que la plupart de la population utilise, à savoir les mails. C'est ce que fait le groupe Sima. Les mails sont orientés vers le milieu professionnel, ainsi ils peuvent toucher un bon nombre de personnes avec des responsabilités importantes. Enfin, nous pouvons aborder le cas plus précis des Rocket Kitten, dont les attaques ont poussé certaines organisations à effectuer des enquêtes.

Il s'agit d'un groupe originaire d'Iran qui cible des personnes d'intérêt en utilisant des logiciels malveillants. L'outil principal est la conception de pages d'hameçonnage ciblées. C'est-à-dire qu'ils adaptent ces pages dans le but d'attirer les victimes dans un piège invisible. Par exemple, les victimes peuvent faire partie des groupes de responsables de la défense, ambassades, ou alors des chercheurs, et des scientifiques dans les domaines du nucléaire. On comprend ensuite le besoin d'enquêtes afin de démasquer ce genre de groupes et de pouvoir réagir rapidement en cas d'attaque contre des organisations sensibles telles que dans le domaine du nucléaire.

Après avoir étudié les stratégies d'attaques de plusieurs groupes, nous nous sommes intéressés à la structure interne de l'internet de l'Iran. En effet, cette structure est qualifiée de cachée à cause des propriétés du réseau. Il est uniquement accessible au sein de l'Iran. Nous avons abordé le sujet d'un point de vue juridique et éthique. Ensuite, il a fallu comprendre pourquoi l'utilisation d'un réseau privé est adoptée de manière massive. C'est donc une conception volontaire dans le but de se protéger des attaques que l'on a pu voir auparavant.

Ainsi l'Iran a voulu construire son propre réseau privé pour acquérir un certain niveau de défense. Comme le nucléaire est devenu la priorité d'un grand nombre d'attaquants, la sécurité est avant tout le point le plus important sur lequel l'Iran s'est amélioré en quelques décennies. Seulement, cela peut poser des problèmes concernant la population locale, on peut se demander si cette conception du réseau influence le mode de vie de l'Iran. Il s'agirait de faire d'autres études dans le but de voir l'impact de ce réseau d'adresses privées combiné aux attaques de groupes malveillants, sur la vie en Iran.