“Iran and the Soft War for Internet Dominance”

INFO731 – Sécurité et Cryptographie

CAULLIREAU Dorian – 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 :

- *“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 and the Soft Ware for Internet Domiance”* **- PowerPoint Presentation** https://iranthreats.github.io/us-16-Guarnieri-Anderson-Iran-And-The-Soft-War-For-Internet-Dominance-presentation.pdf

- *“Iran’s Soft War Get Harder”* – **InfoSecurity Magazine** https://www.infosecurity-magazine.com/news/iran-soft-war/

Sommaire

Introduction

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 parait 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. Infy, le désir de s'attaquer 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 élection 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 personne à travers le monde. Par exemple, l'entreprise Palo Alto Networks, une grande entreprise américaine de construction de matériel de télécommunication à décris 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.

Figure 1 *– Revendication et échange sous forme de tweet*

1.1. Infy : Une histoire de stratégie

Toute organisation malveillante à 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 continue malveillantes, pour essayer de manipuler les esprits, et manipuler les choix et actions de l'ensemble des civiles 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 et 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.

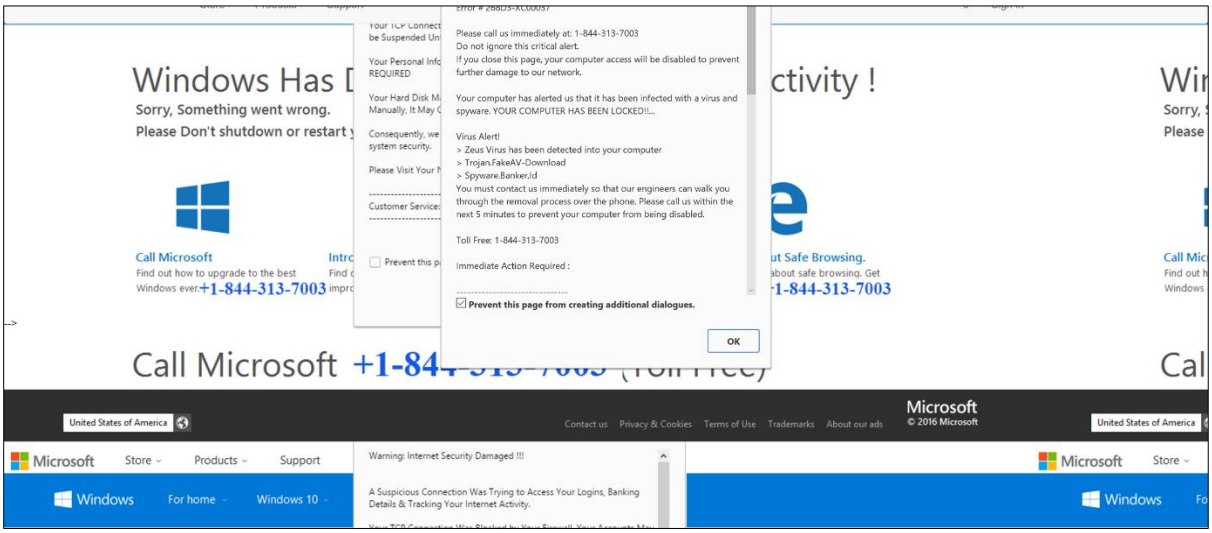


Figure 2 *– Exemple d'un site d'arnaque*

1.2. 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.

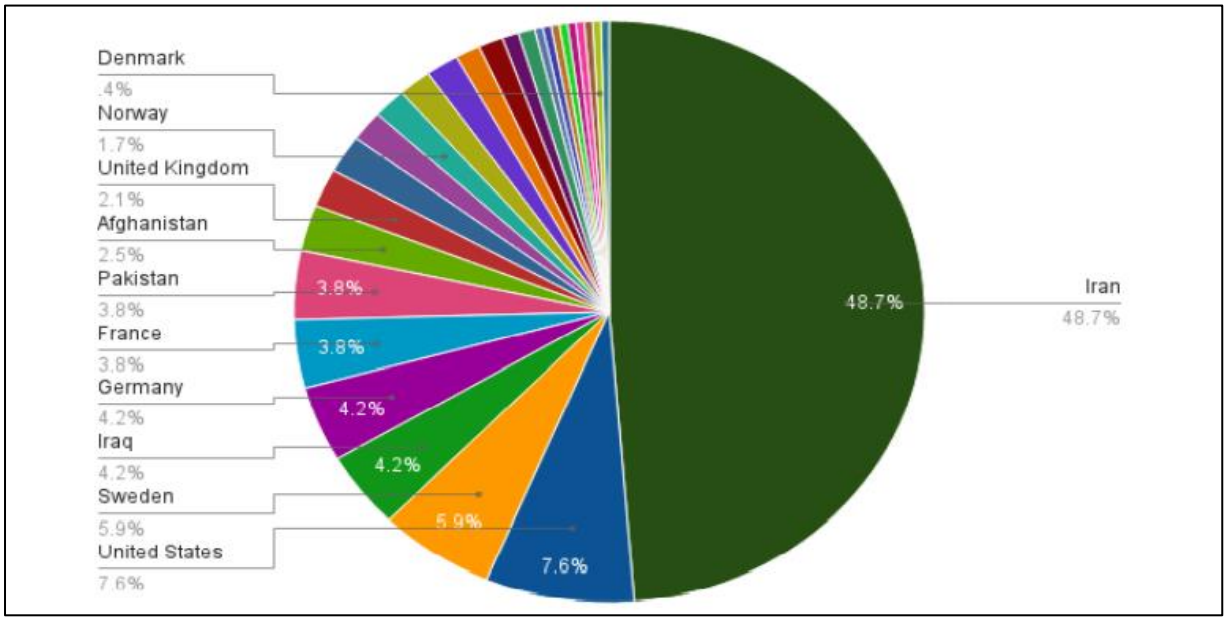


Figure 3 *– Répartition des attaques en fonction des pays*

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.

1.3. Infy, de la technique dans 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 télécharger, 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'utilisateurs et toutes les actions qu'il réalisent 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.

1.4. Un réseau de personnes large et puissant

Dans le cadre de l'étude sur les différents articles étudiées, 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 détourner 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 présente 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.

1.5. Des régulations pour restreindre les actions de Infy

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

C'est ainsi que différentes mesures ont été prisent 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 prisent pour ralentir le programme Infy, nous pouvons toujours voir au moment de l'article 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 missent 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.

2. Ghambar, beaucoup de cibles et beaucoup d'actions

2.1. Des cibles bien précises …

Après avoir analyser 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.

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.

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.

Figure 6 *– Un système en relation avec l'ISLAM*

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'outils mise en place.

L'utilisation de ce logiciel a été prouvé dans l'ouverture dans une université, ou la récupération d'informations sensibles à 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 stocké directement sur la machine. L'ensemble des informations sont immédiatement envoyés 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 envoyé à distance, les fichiers sont sauvegardés dans les fichiers de configuration, puis envoyé avant d'être supprimé à jamais.

Pour avoir un champ plus large, le logiciel permet également de télécharger de 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.

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.

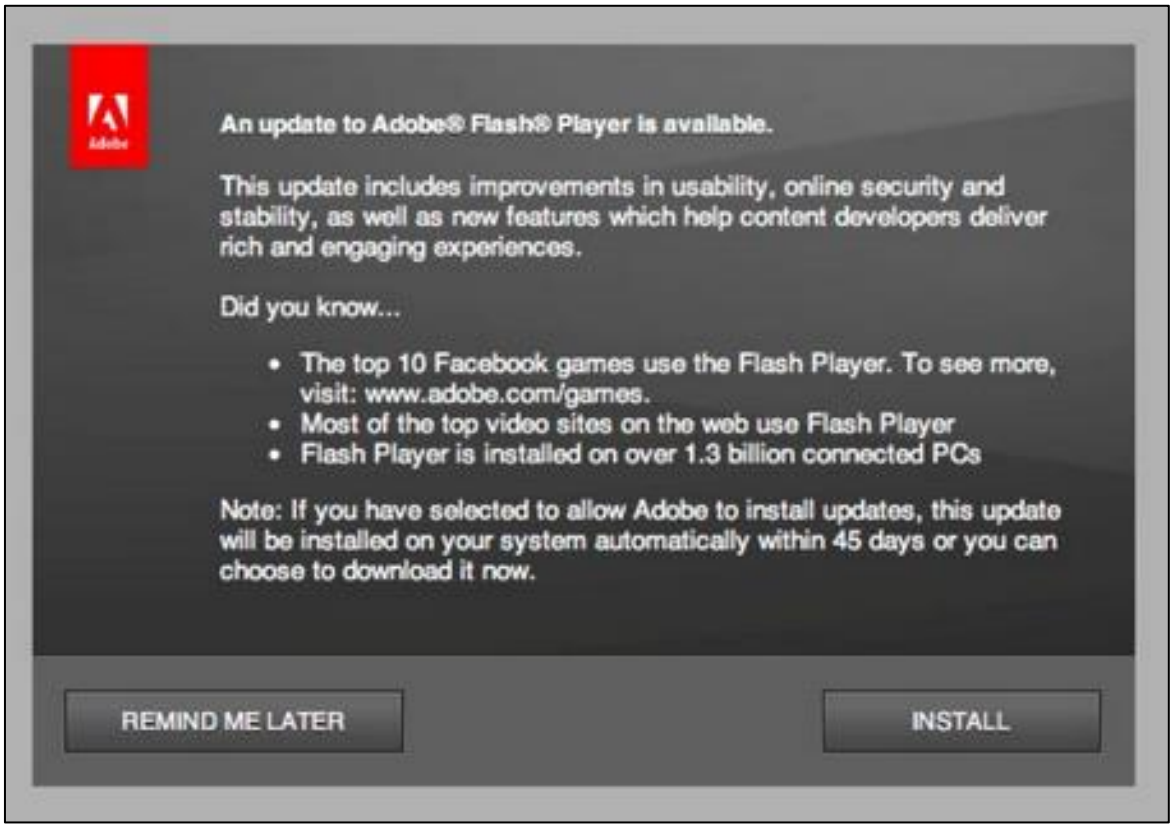


Figure 7 *– Exemple d'un exécutable contaminant*

3. Rocket Kitten, encore et toujours des attaques

Nous allons maintenant étudier un troisième organisme « Rocket Kitten », nous allons dans la même idée que la présentation des précédent voire les modes d'actions, les objectifs ainsi que les cibles.

3.1. Quoi ? Par qui ? Pourquoi ?

Le premier cas d'utilisation de ce programme nous vient de 2014. Avec une utilisation dans des institutions et entreprises israéliennes via des courriels avec des documents Microsoft Office. Les cibles restent les mêmes, avec un premier cas d'infiltration ayant pour cible les universités israéliennes ou encore des défenseurs internationaux des droits humains.

Rapidement, le logiciel a été détecté comme ayant pour but de mener des compagnes d'hameçonnage et d'utiliser des logiciels malveillants.

L'étude de la racine de ce logiciel a été plus rapidement que les précédents, en effet 'écriture du logiciel avec l'utilisation du persan a permis de rapidement faire le lien avec le lieu d'écriture du programme. De plus, des traces des pseudonymes du concepteur du projet a permis d'être retrouvé. C'est donc un certain **Yaser Balaghi** qui semble être à la tête du projet.

Figure 8 *– Yaser Balaghi*

Si les opérations du groupe d'attaque ont un moment été limité, elles se sont remises en route rapidement, avec des nouvelles techniques d'hameçonnage. Pour résumé, les victimes recevaient un lien vers une copie de Google, pour les inciter à modifier leur mot de passe, et par conséquent récupérer l'ensemble de leurs informations.
Globalement, et dans un premier temps, les principales cibles étaient alors les locaux.

3.2. Telegram, un réseau facilitant ?

Au-delà de l'utilisation de Microsoft Office et de la copie de Google, nous pouvons également voir l'émergence d'un nouveau moyen d'attaque, avec l'utilisation de l'application de communication « **Telegram** ». L'objectif était de rentrer en communication avec des victimes, et de récupérer leurs informations de connexion, pour ensuite pouvoir utiliser leur propre compte.

Un terrain d'attaque parfait, en effet Telegram s'est développé comme une application sécuritaire avec le cryptage des informations, ce qui n'est finalement pas totalement le cas, l'utilisateur finit toujours par être trompé par l'attaquant, avec pour cause une baisse de vigilance importante.

Via l'utilisation des techniques d'attaque par l'utilisation d'une copie de Google ainsi que l'utilisation de Telegram, le groupe d'activiste a pu récupérer plus de 15 millions de numéros de téléphone, et donc parallèlement, énormément d'informations.
De plus, l'utilisation de l'authentification à Telegram via un SMS a posé beaucoup de problème d'un point de vue sécuritaire. En effet, la vérification par messages permet dans une certaine mesure un espionnage. Si l'application fait transiter des codes de vérification via le réseau mobile, ces informations peuvent être interceptées et utilisé par des personnes tierces. Si ces techniques ont déjà été utilisé et observé en Égypte et en Russie, un grand nombre de personnalités Iranienne, ont été prisent pour cibles. Par exemple, des personnalités politiques, des militants, ou encore des acteurs de la surveillance.

3.3. Des techniques bien ciblées

L'objectif de ce groupe d'activiste s'est donc tourné autour des techniques de récupération des informations et les moyens misent en œuvre pour accéder à ses informations. Comme la récupération d'un compte Facebook pour récupérer l'ensemble des informations et rentrer en communication avec les contacts et véhiculer des informations pour prendre en traite leur compte Facebook à nouveau. Globalement un cercle vicieux pour contaminer le plus de monde possible.

Nous pouvons également voir que la technique passe par la transmission d'images ciblées pour faire réagir des futures victimes, avec un lien vers un hameçonnage pour les contaminer à nouveau.

Nous pouvons alors voir une multiplication des moyens de communication : Images ciblées avec lien de téléchargement, logiciels cachés dans des documents envoyés par mail, création de fausses ressources Facebook et bien d'autres.

Nous pouvons par exemple, voire une mise en place d'une technique d'hameçonnage avec une invitation à télécharger des images, pour faire télécharger un logiciel malveillant.

Figure 9.1 *– Exemple d'une invitation à mettre à jour une application sur Flash Player*

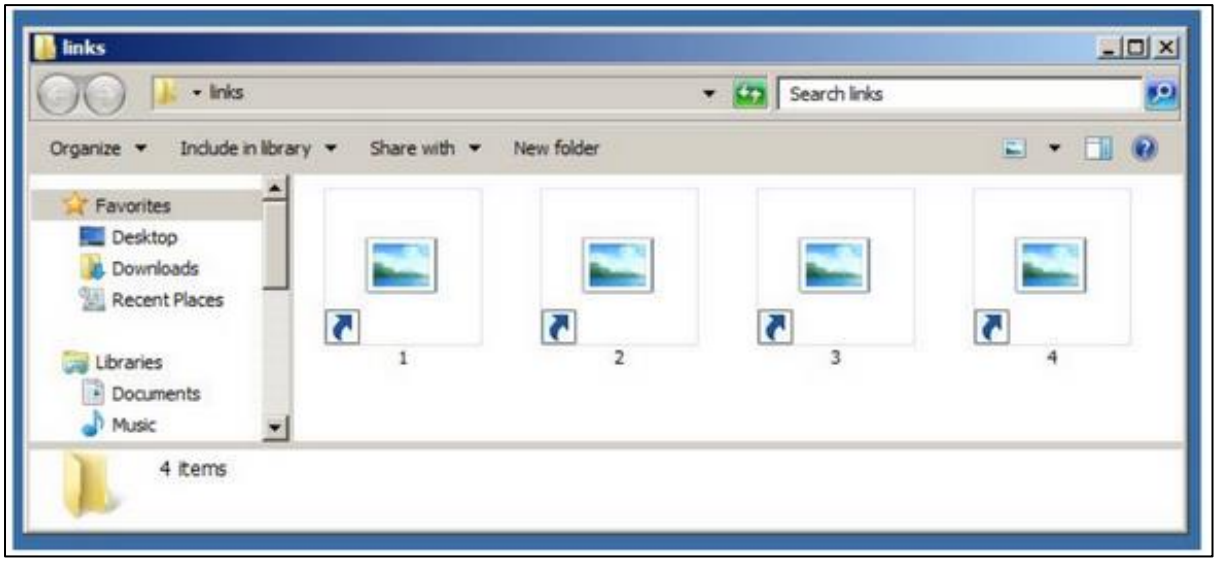


Figure 9.2 *– Exemple d'un fichier contaminé*

Si dans un premier temps l'utilisateur voit des images, des fichiers LNK sont présents. Ces fichiers téléchargent via une exécution PowerShell. Il permet d'ouvrir une nouvelle page web, qui fait télécharger à nouveau des images et un nouveau fichier LNK qui exécute un fichier binaire sur la machine.

Comme évoqué précédemment, un grand nombre de techniques ont été misent en œuvre pour avoir un taux de réussite plus important. Plus le nombre de techniques est important, plus il y a de chance de récupérer les informations d'un grand nombre de victimes.

4. Sima, des mails, des mails des mails…

4.1. 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.

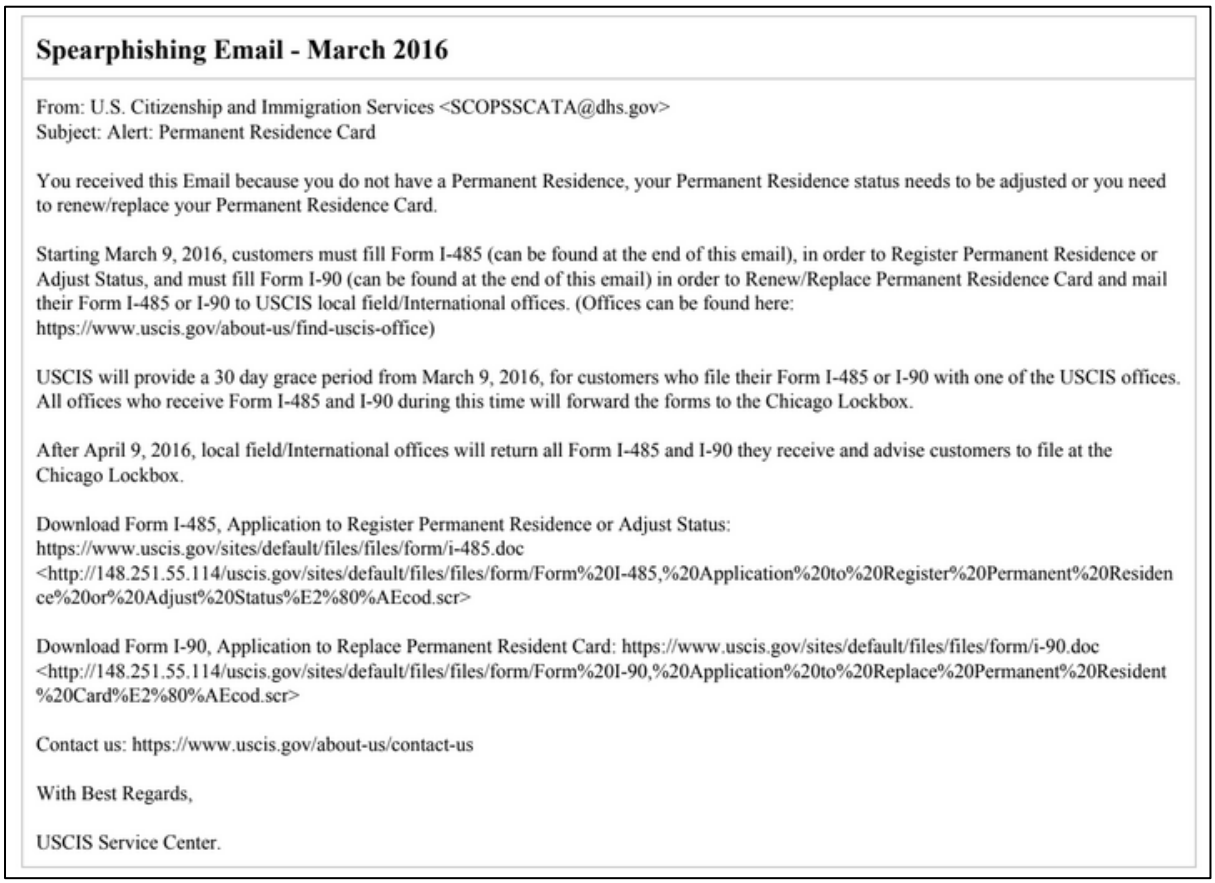
D'après les études technologies qui ont été faites sur le logiciel, nous pouvons voir un début d'attaque en février 2016, avec un arrêt dès début mars. Les cibles principales de ce projet ont été des Iraniens de la diaspora qui se concentraient sur la politique étrangère et des questions relatives aux 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 10 *– Exemple d'un mail diffusé par Sima*

4.2. 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 réalisé 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 rentrée dans des considérations technique avancée, nous pouvons que les méthodes d'hameçonnages par le téléchargement d'informations soient très poussées. Elles mènent par exemple au téléchargement de solution propre et compliqué 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 11 *– LumiosityLink, 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.