Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTERE DE L'INTERIEUR
DE L'OUTRE MER
ET DES COLLECTIVITES LOCALES

Direction Générale
de La Police Nationale
Direction Centrale
du Renseignement Intérieur

PN/RI/N°

Levallois Perret, le 25/01/2012

Le Commandant de Police [redacted]
En fonction à la Direction Centrale du Renseignement Intérieur

à

Monsieur le Procureur de la République
près le Tribunal de Grande Instance de Paris

O B J E T : Compte-rendu d'enquête concernant des faits d'entrave au fonctionnement d'un Système de Traitement Automatisé de Données (S.T.A.D.) commis entre les 21 et 23 avril 2011 ainsi que le 02 juin 2011.

AFFAIRE : C / X...

REFERENCES : Votre soit-transmis N° **11.132.9101/8** en date du 12 mai 2011.
Saisine de la Juridiction Inter Régionale Spécialisée / Section S2.

P. JOINTES : Une procédure établie par le service comprenant cent-soixante quatre procès-verbaux numérotés 2011/101/01 à 2011/101/164 et leurs annexes , sa copie conforme ainsi que deux Cotes et vingt-trois scellés.

J'ai l'honneur de vous rendre compte du déroulement ainsi que des résultats de l'enquête diligentée par le service, conformément à vos instructions, dans le cadre préliminaire et pour laquelle vous avez été régulièrement informé.

LES FAITS

Le 21 avril 2012, la D.C.R.I. était avisée par l'Agence Nationale pour la Sécurité des Systèmes d'Information (A.N.S.S.I.) du déroulement d'une attaque informatique visant le portail Internet de l'Opérateur d'Importance Vitale (O .I.V.) EDF. Ayant débutée la veille, cette attaque dite par « **déni de service distribué**[1] » aurait été lancée contre le site Internet institutionnel d'EDF dans le cadre d'une offensive d'envergure menée par la nébuleuse « ***Anonymous*** » et dénommée « **opération Greenrights** ».

Cette opération, initiée à la suite du mouvement d'opinion lié à l'incident de la centrale nucléaire Japonaise de Fukushima, visait en premier lieu le groupe américain GENERAL ELECTRIC, l'opérateur français EDF ainsi que l'opérateur Italien ENEL.

Les premiers éléments communiqués indiquaient un haut degré de sophistication dans la méthode utilisée pour cette attaque : les équipements ou services visés variant au fil des heures en fonction des protections mises en place par les équipes d'EDF.

La plainte déposée par les représentants d'EDF le 2 mai 2011 permettait de préciser les points suivants :

- l'attaque, qui s'est déroulée entre les 20 et 23 avril 2011, a été caractérisée par plusieurs vagues successives visant le portail « **www.edf.com** » et a eu pour effet de rendre inaccessibles les sites Internet commerciaux « **edfpro.edf.com** », « **bleuciel.edf.com** », « **entreprises.edf.com** » et « **collectivites.edf.com** », atteignables à partir de ce portail, sur une durée cumulée d'environ **quatorze heures**.

- un premier préjudice cumulé estimé à **162 000 €** était communiqué par le représentant d'EDF : celui-ci prenait en compte l'indisponibilité des sites du groupe, les mesures d'urgence prises au niveau technique ainsi que les nombreux recours d'internautes effectués auprès du Centre de Relation Clients d'EDF du fait de l'absence des sites d'Internet.

Les équipements attaqués étant localisés sur le département de Seine-saint-Denis, un premier avis était effectué auprès d'un représentant de Monsieur le Procureur de la République près le Tribunal de Grande Instance de Bobigny en la personne de M. Rémi CHAISE. Le 9 mai 2011, cette juridiction était dessaisie au profit de la Juridiction Inter Régionale Spécialisée (JIRS) de Paris, Section S2 du Parquet de Paris.

L'ENQUETE

Les premières recherches menées en milieu ouvert sur les revendications déclarées pour cette « **opération Greenrights** » indiquaient rapidement que celle-ci aurait pour origine des membres de la nébuleuse dénommée « ***Anonymous*** » en réaction à l'utilisation du nucléaire comme énergie « dangereuse et non contrôlée ».

L'exploitation d'un « micro-message » émis sur le réseau social « *Twitter* » appelant au déclenchement de l'opération « Greenrights » permettait de localiser le manifeste de cette

---

[1] un déni de service distribué (DDoS) est un type d'attaque consistant à « noyer » un serveur sous un afflux massif de requêtes (légitimes) lui étant adressées par de très nombreux ordinateurs, en même temps, à partir d'Internet.

opération, document librement consultable sur le serveur du fameux parti pirate Allemand[2] localisé en Allemagne et atteignable à l'adresse « **http://piratenpad.de/greenrights** ». Ce document collaboratif était imprimé par nos soins ; une Demande d'Entraide Judiciaire Internationale étant rendue nécessaire afin d'obtenir les adresses IP des internautes l'ayant établi (cf procès-verbal 101/2011/2 du 22/04/2011).

Ces mêmes recherches, menées sur la sphère « *Anonymous* » permettaient d'apprendre que cette dénomination englobait un groupement fluctuant d'Internautes au sein duquel aucune hiérarchie n'existerait et qui interviennent régulièrement sur l'Internet afin de défendre ou d'en punir les différents acteurs, ceci en fonction des circonstances : le déni de service distribué étant l'arme de prédilection de ce mouvement (cf procès-verbal 101/2011/4 du 27/04/2011). Ces éléments plaidaient ainsi en faveur d'une participation volontaire de chaque ordinateur à l'attaque ; contrairement aux « botnet » usuellement utilisés pour ce type d'opération.

Rapidement, une demande de « gel de données » via le réseau G8/24-7 dédié à la Cybercriminalité était adressée aux autorités Allemandes : Celles-ci nous demandaient, vu la popularité du parti pirate Allemand, l'envoi dans les meilleurs délais de la demande judiciaire officielle. L'opération dans les locaux du parti allemand était réalisée le 19 mai 2011 par les policiers du BKA.

Parallèlement, les constatations techniques réalisées sur les différents journaux de connexion remis par EDF confirmait la présence de très nombreuses adresses IP à l'origine de l'attaque, mais permettaient également d'isoler des adresses françaises ayant utilisé une part importante de la bande passante lors des faits. Celles ci étaient identifiée comme suit :

- adresse IP FREE attribuée à un particulier, Monsieur [redacted] demeurant dans le Finistère (29),
- adresse IP d'un serveur OVH loué par Monsieur [redacted] demeurant à SANTRY (IRLANDE), [redacted] (cette société fournit des solutions de VPS[3],
- adresse IP NEUF/SFR attribuée à Monsieur [redacted] demeurant dans les Ardennes (08),
- adresse IP France Telecom attribuée à Madame [redacted] demeurant dans les Hauts-de-Seine (92).

Les adresses IP précédemment énoncées figurant directement « en frontal » dans les traces d'attaques, il apparaissait pertinent de tenter d'identifier un « second niveau » de responsabilité pour ces faits ; plus particulièrement concernant des internautes étant plus liés à l'organisation et à l'incitation / provocation pour cette « opération Greenrights ».

A cette fin, les investigations suivantes étaient diligentées à partir des différents médias utilisés par la nébuleuse « Anonymous » pour diriger les attaques dans le cadre de l'opération « Greenrights » :

* envoi d'une réquisition à « Google » afin d'identifier le titulaire et animateur du « blog » hébergé à l'adresse « **http://operationgreenrights.blogspot.com** », blog sur lequel les différentes actions sur cette opération sont annoncées à grand renfort de tracts et vidéos.

---

[2] Le parti pirate allemand est le 6ème parti allemand en terme d'effectifs et compte environ 12000 adhérents.

[3] VPS pour Virtual Private Server, serveur privé virtuel permettant notamment de se rendre anonyme sur Internet.

* recherches et envoi d'une réquisition judiciaire au site Internet de vidéo en ligne « Youtube » afin d'identifier le titulaire de la « chaîne Youtube » « ***Kloudization*** » sur laquelle plusieurs vidéos officielles des « Anonymous » avaient été déposées, dont certaines prônaient la participation active à « **#opération Greenrights** ».

En outre, le 31 mai 2011, un nouveau tract virtuel (ou « flyer ») était déposé sur la tribune **http://operationgreenrights.blogspot.com** appelant à de nouvelles attaques contre le site d'EDF le 02 juin à partir de 13h00. Sur ce tract était mentionnée une adresse de WebIrc, « **irc.lc/anonops/operationgreenrights**[4] ».

L'identification de ce nom de domaine permettait d'apprendre que celui ci appartenait à un dénommé **Pierrick GOUJON** demeurant à Lanneran (22), titulaire d'un espace d'hébergement chez OVH. L'intéressé, connu des services de Police pour des délits mineurs, se révélait être le promoteur en France du mouvement « déchétarien »[5].

Cet espace d'hébergement loué par M. GOUJON correspondait à un « serveur dédié » supportant **68** sites Internet. Une majeure partie des noms de ces sites a été déposée au nom de l'intéressé, les autres l'étant visiblement sous des identités fictives et farfelues. Une réquisition adressée à OVH permettait d'apprendre que le serveur était essentiellement géré depuis une adresse IP attribuée à l'opérateur FREE et correspondant au client final Pierrick GOUJON. Une copie de cet espace était placée sous scellé provisoire aux fins d'exploitation ultérieure.

Le 08 juin 2011, les responsables techniques d'EDF confirmaient que la seconde attaque s'étant déroulée le 02 juin avait bien été suivie d'effets et avait entraîné une interruption cumulée de 20 minutes. Les journaux d'évènements des équipements et systèmes attaqués étaient remis pour constatations.

La poursuite des investigations révélaient que, derrière le masque d' « Anonymous » apparaissant dans les vidéos du profil « Kloudization », se dissimulait vraisemblablement un jeune homme, fan de nouvelles technologies et de musique métal en la personne de [redacted] demeurant près de Nîmes (cf procès-verbaux des 24/06/2011 et 05/07/2011). Les constatations et recherches ultérieures semblaient indiquer que l'intéressé, réalisant ses propres vidéos invitant à une participation aux attaques des « Anonymous », les mettaient ensuite en ligne sur sa chaîne « Youtube » ; celles-ci allant jusqu'à apparaître sur le site Internet « www.rezocitoyen.fr », la vitrine officielle du mouvement « Anonymous » en France.

Les dernières constatations menées sur les éléments communiqués par EDF permettaient de relever la présence d'une adresse IP particulièrement active caractérisée par l'utilisation d'un outil utilisé par la nébuleuse « Anonymous » pour commettre des attaques en déni de service (outil « webLOIC »). L'identification de cette adresse IP désignait la connexion de [redacted] demeurant près de Brest. Les recherches menée à partir de cette identité indiquaient que cette personne participait activement à des forums de discussion de la nébuleuse « Anonymous » sous le pseudonyme « ***nahliflor*** » : sur l'un

---

[4] Les canaux IRC (Internet Relay Chat, protocole de communication instantané sur Internet) sont utilisés par la nébuleuse « Anonymous » pour coordonner et organiser les attaques. La mise en place d'un web IRC permet d'accéder à ces canaux sans installation et paramétrage préalables d'un logiciel « dédié » à l'IRC. L'accès se fait alors par le navigateur Internet, comme pour n'importe quel site.

[5] Le « *Freeganisme* » ou mouvement « *déchétarien* » consiste à trouver sa nourriture dans les poubelles. Ce mouvement est basé sur une idéologie contestant les gaspillages engendrés par les sociétés industrielles et les régimes capitalistes...

d'entre eux elle allait jusqu'à déclarer « *Pour ce que j'en fais du DdoS, c'est un devoir ! Le devoir de faire respecter mes droits et ma liberté comme il est écrit dans notre constitution* »

Sous vos instructions, il était, dans un premier temps, procédé aux auditions des titulaires des connexions apparues « en frontal » sur les deux vagues d'attaque ayant ciblé le portail web d'EDF.

Entre les 17 et 18 janvier 2012, messieurs [redacted] (utilisant la connexion Internet attribuée à Madame [redacted], son ancienne compagne) étaient concomitamment entendus. Affirmant être complètement étrangers à la sphère « Anonymous », les intéressés consentaient à ce que des copies des ordinateurs présents à leurs domiciles respectifs soient effectuées.

A l'image de [redacted], embarqué sur un navire à la date des faits et indiquant avoir volontairement déconnecté le Wi-fi de sa « freebox », ces trois personnes ne correspondaient au « profil » du militant « Anonymous » et n'en possédaient pas non plus la « culture » informatique.

Les premières constatations techniques menées sur les différentes copies réalisées lors de ces opérations ont dors et déjà permis de confirmer que les intéressés *ne sont pas liés* aux opérations ni à la mouvance « Anonymous ». Les systèmes concernés ont donc manifestement été « piratés » ou utilisés à l'insu de leurs propriétaires légitimes. La poursuite des analyses devra démontrer la nature, et si possible l'origine de chaque piratage.

l'analyse de la copie du serveur mutualisé OVH loué à la **société IT EXPERTS** permettait uniquement de constater que le serveur virtuel utilisé pour l'attaque avait été irréversiblement effacé. Les « logs » systèmes, paramétrés pour ne conserver qu'un court historique, n'étaient pas plus exploitables.

Après compte-rendu de l'état de nos investigations le 20 janvier dans les locaux du pôle financier du T.G.I. de Paris, des déplacements étaient effectués aux domiciles des nommés [redacted] qui étaient tous les trois entendus sous le régime de la garde à vue.

* Etudiant en dernière année de B.T.S. « technicien du son » à Montpellier, [redacted] se définit lui-même comme un « utilisateur classique d'Internet », mais tout en précisant qu'il connaît et utilise des logiciels dédiés à la sécurité informatique. Il reconnaissait utiliser le pseudonyme de « ***Kloud*** » ou « ***Kloudization*** » et fréquenter régulièrement les salons de discussion IRC de la nébuleuse « *Anonymous* » dont il adhère aux valeurs. Passionné de montage vidéo, M. [redacted] précisait être le gestionnaire de la chaîne « Youtube » associée à son pseudonyme.

Revendiquant son appartenance aux « *Anonymous* », l'intéressé reconnaissait rapidement être à l'origine des nombreuses vidéos défendant les actions de ce mouvement et annonçant, menaces à l'appui, les différentes attaques ayant jalonnées l'année 2011. Il indiquait en outre participer aux attaques par déni de service distribué. Mathieu ORTET expliquait en substance que ces actions « offensives » matérialisaient son droit de ne pas être d'accord en résumant « ... c'est la démocratie ».

Il définissait son action comme de la « propagande » afin de supporter ce qu'il défini comme une « guerre de communication ». Ayant appris l'existence de l'opération « Greenrights » sur l'un des nombreux salons de discussion IRC qu'il fréquente, [redacted] confirmait n'avoir participé qu'à la seconde vague du 02 juin ; attaque pour laquelle il confectionnait et publiait une vidéo.

Le jeune homme reconnaissait avoir offert une publicité considérable aux différentes actions intentées par les « *Anonymous* » mais précisait également avoir été quelque peu « effrayé » par le retentissement de ces attaques et surtout de leurs conséquences financières pour la victime. Il finissait par considérer sa participation comme une erreur et un acte grave .

[redacted] désignait un internaute utilisant le pseudonyme de « MACKEN » et s'exprimant en anglais comme le « commanditaire » de ses différentes vidéos. A contrario, il niait avoir contribué à la constitution du « manifeste » sur le serveur du parti pirate allemand.

* Inversement, **Pierrick GOUJON** précisait ne pas adhérer à la philosophie du mouvement « Anonymous » même si il suivait les évolutions de cette nébuleuse.

Partageant son temps entre de la récupération dans les poubelles, de l'informatique et de la guitare, l'intéressé montrait une bonne connaissance du domaine des nouvelles technologies et confirmait être le locataire-gestionnaire de l'espace d'hébergement loué auprès d'OVH, serveur contenant -entre autres- le site Internet intéressant l'enquête « **irc.lc/anonops/operationgreenrights** ».

C'est en veine de fréquentation sur son serveur, et conscient du potentiel représenté par le mouvement « Anonymous » qu'il mettait en place **une passerelle** permettant très facilement à un simple internaute d'accéder aux multiples salons tenus par la nébuleuse sur IRC... protocole peu convivial nécessitant l'installation de logiciels spécifiques.

Contestataire dans l'âme, il reconnaissait avoir précédemment hébergé un miroir du site « *Wikileaks* », Pierrick GOUJON indiquait qu'il condamnait les actions « barbares » menées par les « Anonymous » : ce qui ne l'a pas empêché de proposer ses services de passerelle vers le canal IRC dédié à l'opération « Greenrights » et sur lequel il avait lui-même constaté qu'EDF figurait parmi les cibles. Ce brillant dilettante, tout en reconnaissant que son site offrait une ampleur supplémentaire à l'attaque, limitait sa responsabilité à la « mise en relation » et non au contenu....

La copie et le début d'exploitation du serveur de M. GOUJON menés durant le temps de la garde à vue confirmaient ces éléments et plus particulièrement le pic de fréquentation vers le salon « ***#operationgreenrights*** » atteint le 23/05/2011.

Estimant « *ne pas avoir apporté d'apport logistique au mouvement anonymous* », Pierrick GOUJON reconnaissait néanmoins s'être connecté sur le site d'EDF lors de la première vague d'attaque, ceci « pour voir ». Connaissant parfaitement les outils collaboratifs proposé par le Parti pirate Allemand, il reconnaissait les utiliser ponctuellement afin d'y glisser l'adresse de sa passerelle vers le monde IRC... et d'y gagner ainsi en fréquentation !

* actuellement sans emploi, [redacted] reconnaissait immédiatement sa participation active aux attaques par déni de service distribué menée contre le site Internet d'EDF en avril et juin 2011.

Séduite par la liberté apparente et le discours alternatif du mouvement « Anonymous », cette quadragénaire isolée et mère de deux enfants reconnaissait avoir vivement adhéré aux actions « offensives » prônées sur les canaux de discussion.

[redacted] précisait en outre avoir été réellement bouleversée par la catastrophe japonaise au printemps 2011; évènement-clé l'ayant fait basculer dans l'action « en vue de faire entendre » son point de vue. Devenant militante, elle affirmait avoir fréquenté d'une manière intensive l'ensemble des canaux de diffusion utilisés par la sphère « Anonymous » et avoir finalement entendu parler de l'opération « Greenrights »... à laquelle elle participait en utilisant un outil fourni par cette communauté pour augmenter l'effet de saturation (L.O.I.C.).

Réfutant sa participation à l'établissement du « manifeste » présent pour cette opération sur le site du Parti pirate Allemand, l'intéressée nous précisait que celle-ci visait à l'origine la seule entité italienne ENEL et que l'internaute nommé « MACKEN » semblait en être à l'origine sur les canaux IRC des « *Anonymous* ».

C'est suite à une mission d'intérim de deux mois qu'elle reprenait contact avec la nébuleuse courant septembre 2011. Elle notait alors ce qu'elle désigne comme « une dérive » au sein de ce mouvement où des membres, vraisemblablement de confession musulmane, prônent des opérations « anti-occidentales »..pervertissant ainsi l'esprit initial du mouvement. Elle coupait définitivement les ponts à la fin de l'année 2011.

Conformément à vos instructions, il a été mis fin à la mesure de garde à vue s'appliquant à [redacted] qui a été laissée libre.

Vous nous faisiez part de votre souhait de vous voir présentés les nommés [redacted] et Pierrick GOUJON au terme de leurs garde à vue.

Ainsi, à ce stade des investigations menées en cadre préliminaire sur les deux vagues d'attaques par déni de service distribué ayant ciblé le portail Internet « **www.edf.com** » entre avril et juin 2001, il apparaît que les responsabilités respectives des nommés [redacted] **Pierrick GOUJON** et dans une moindre mesure, [redacted] ,sont susceptible, d'être établies.

- Mettant ses talents de jeune cinéaste au profit de ce qu'il qualifie lui même de « propagande », [redacted] **fabrique** et **diffuse** ses vidéo prônant une participation directe à l'attaque contre le site d'EDF. Ces supports relaient les menaces édictées par les initiateurs de l'attaques et invitent clairement à y participer. La fréquentation de la chaîne « Youtube » de l'intéressé ajoutée à la reprise de cette vidéo par les canaux de la nébuleuse laissent imaginer l'engouement provoqué face à une population éprise d'effets visuels.

- Technicien talentueux conservant en apparence une « *prudente distance* » avec les thèses « Anonymous », **Pierrick GOUJON** est pourtant omniprésent dans chacune de leurs actions et s'intéresse aux « manifestes » publiés pour chaque attaques. C'est en toute connaissance de cause qu'il procure à cette communauté une « passerelle Web » permettant à celle-ci de mieux

communiquer et facilitant la participation des nouveaux venus - trop néophytes pour s'initier à l'IRC- aux différentes actions déclenchées. C'est cette fourniture de moyen, dont M. GOUJON semble se féliciter, que l'on retrouve dans l'accès ainsi procuré vers le canal IRC « ***#operationgreenrights*** » et qui permet à une attaque -dont l'efficacité repose sur le nombre de participants- de gagner en ampleur... et qui n'aurait peut pas été rendue possible sans cette accès facilité par le lien « **irc.lc/anonops/operationgreenrights** ».

- Militante « piégée » par l'image volontairement transportée sur la sphère « Anonymous », [redacted] a manifestement conçu le déni de service distribué comme arme de contestation politique et comme un moyen d'expression face à des problèmes de société comme l'utilisation de l'énergie nucléaire. C'est dans cette optique qu'elle a participé à l'attaque contre EDF. Renouant avec les « Anonymous » après quelques mois de coupure, elle découvrait des mouvances aux objectifs plus subversifs, ce qui lui permettait de « décrocher » définitivement de ce mouvement. Reconnaissant sa participation, Mme [redacted] en regrette l'aspect illégal.

Des investigations restent néanmoins à poursuivre, qui sont susceptibles de mettre en lumières de nouvelles responsabilités, notamment sur **l'origine de la conception** de l'opération « Greenrights » ainsi que sur **l'identité** du fameux « MACKEN ». Elles peuvent se décliner comme suit :

* remise et exploitation des données de connexion au site « **http://operationgreenrights.blogspot.com** » (D.E.P.I. en cours auprès des autorités judiciaires américaines),

* remise et exploitation des traces de connexions sur le manifeste de l'opération présent sur le site « **http://piratenpad.de/greenrights** » (D.E.P.I exécutée par les autorités judiciaires allemandes).

* poursuite des constatations techniques sur les copies des systèmes informatiques de messieurs [redacted] afin de déterminer leur degré de piratage et l'origine compromission

Conformément à vos instructions, la présente procédure vous est transmise à toutes fins que vous jugerez utiles.

Le Commandant de Police [redacted]

Identités des personnes vous étant présentées :

Monsieur [redacted]

Monsieur [redacted]

Destinataire :
- Madame Frédérique DALLE, Substitut de Monsieur le Procureur de la République près le Tribunal de Grande Instance de Paris, Section S2.