L'opération "Carbone 14" : les modalités pratiques et les implications juridiques d'une attaque informatique

David Bénichou[1] and Serge Lefranc[2]

[1] Magistrat
Cour d'appel de Paris
Paris CEDEX F-75000, France
David.Benichou@justice.fr
[2] Ingénieur de l'Armement
Centre d'Électronique de l'Armement
Bruz CEDEX F-35174, France
serge.lefranc@dga.defense.gouv.fr

Résumé Cet article s'inspire d'un cas réel et a pour but de présenter les modalités pratiques et les implications juridiques d'une attaque informatique, que ce soit du point de vue de l'attaquant, comme de celui de la victime.

1 Introduction

Cet article a pour but de présenter les modalités pratiques et les implications juridiques d'une attaque informatique du point de vue de l'attaquant et de celui de la victime. Le scénario retenu est volontairement proche d'un cas réel : un éditeur de jeux vidéo se fait dérober en ligne le code source d'un jeu avant sa sortie sur le marché. Celui-ci sera compilé et mis en ligne sur internet.

Les auteurs se réfèrent à un événement relaté par un responsable d'une entreprise d'édition de jeux vidéo [1]. Les développements imaginés et réalisés n'ont aucun lien avec cette affaire au delà de son cadre général, transposable à tout type d'établissement dont des données constituant son patrimoine seraient susceptibles d'être pillées

Le but est de montrer que, dès les stades précoces de la réalisation et la préparation de l'attaque, des contre-mesures d'ordre techniques ou juridiques pourront être mises en oeuvre, soit pour empêcher la réalisation de l'attaque soit pour obtenir des preuves qui permettront la réparation du dommage subi ou l'identification et la condamnation de l'auteur de l'attaque.

Le scénario est le suivant : un éditeur informatique emploie un "pirate" pour nuire à son concurrent. La mission du pirate est de réussir à s'introduire dans le réseau du concurrent pour dérober les codes source de son prochain jeu et d'en assurer la diffusion, avant commercialisation officielle, sur internet. Les techniques présentées dans cet article, et censées reproduire les actions du pirate, ne sont

pas exhaustives. Son but n'est pas de trouver toutes les failles de sa cible comme pourrait le faire un consultant en sécurité, mais juste celle qui lui permettra de réaliser son objectif. Le lecteur intéressé par plus de détails concernant les tests d'intrusions peut se référer au numéro 11 du magazine MISC [2].

Pour rendre le texte plus vivant nous appellerons ce jeu "demi-vie" et l'opération "carbone 14".

2 Le "pacte des loups"

2.1 Aspects techniques

Un éditeur de jeu vidéo souhaite affaiblir la réputation de son principal concurrent qui est en train de developper la suite d'un jeu à succés. Il decide donc d'engager un pirate informatique dont la mission sera de derober les sources de ce jeu afin de les mettre sur le marché, même si le jeu n'est pas encore finalisé.

Pour ce faire, le pirate doit être d'une compétence technique reconnue, être connu de l'éditeur malhonnête et être vénal. Ces conditions garantissent le succés de l'opération. Dès lors, il existe deux possibilités :

- soit le pirate est recruté en externe, ce qui suppose certains risques importants (notamment au niveau de la fiabilité...),
- soit il est recruté en interne. Il appartient au personnel de l' éditeur malhonnête et ses intérêts sont communs avec ceux de son employeur.

2.2 Aspects juridiques : le délit d'association de malfaiteurs informatiques

Définition Le "pacte des loups" formé par nos agents conspirateurs est susceptible, dès ce stade et sous la réserve d'être matérialisé par au moins un acte préparatoire, de revêtir une qualification pénale.

En effet, l'article 323-4 du code pénal dispose que :

La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Rappelons que les articles 323-1 à 323-3 définissent le noyau dur des infractions portant atteinte aux systèmes de traitement automatisé de données (ci-après STAD). S'il s'agit pour nos agents de s'approprier le code source d'un programme dans un système distant, l'article 323-1, définissant l'accès et le maintient frauduleux dans un STAD, aura vocation à s'appliquer.

Pour reprendre un formalisme familier aux développeurs, il convient de remarquer que les éléments constitutifs du délit pourraient s'articuler en une fonction formée de la manière suivante :

```
Association de malfaiteurs informatiques ($agent) =

Participation ($agent) à
{
 ( [un groupement formé] ou [une entente établie] )
 et
 (
   [la préparation d'au moins une infraction entre 323-1 et 323-3]
   et
   [caractérisée par un ou plusieurs faits matériels ]
  )
}
```

L'important, au-delà de l'analogie entre les deux domaines, est que cette approche formaliste de la loi montre qu'on peut aborder le droit pénal avec la même rigueur qu'une fonction booléenne : le plaideur avisé s'efforcera de démonter un élément essentiel qui fera, par le jeu des opérateurs cumulatifs ("et"), basculer la prévention vers le non lieu. Le juge, s'il se fonde sur son intime conviction, est soumis à un "contrôle de cohérence" par la cour de cassation, qui ne manquerait pas d'annuler une décision en cas de contradiction de motifs.

Il faut souligner l'intérêt d'une telle incrimination : la poursuite pourra être engagée avant même le *commencement d'exécution de l'infraction* (domaine de la tentative, art. 121-5 du cpp), c'est-à-dire dès le stade du premier acte préparatoire. Lorsque l'association de malfaiteurs informatiques est formée et a accompli un premier acte préparatoire (par exemple en mettant en commun des moyens) elle entre dans le champ de la répression.

La frontière entre la préparation, caractérisée par un ou plusieurs faits matériels (323-4 cp) et avec le commencement d'exécution de la tentative punissable est ténue, mais d'importance. A partir de la simple tentative (premier essai infructueux par exemple) ou de la commission d'un délit, les auteurs seront dans un cumul idéal d'infractions : pour l'association de malfaiteurs (323-4) et pour les infractions tentées (323-7 du cp) ou consommées (323-1 à 323-3).

Fondements Un petit retour en 1987, (ou *rétro-conception* de la loi) nous permet de sonder la volonté du législateur de l'époque, d'abord sur l'intérêt de créer une telle incrimination, où l'on constate qu'il peut s'agir réprimer les groupes de pirates informatiques :

Or, ces dernières années ont vu fleurir les clubs de passionnés de l'informatique qui échangent les renseignements dont ils disposent et les techniques qu'ils ont mises au point. En conséquence, il a paru opportun à votre commis-

sion de punir les ententes établies en vue de la préparation du délit de piratage informatique [3].

Ensuite, c'est le garde des sceaux lui-même qui nous éclaire sur la relative mansuétude de la répression, puisque le délit d'association de malfaiteurs informatiques n'est pas plus sévèrement puni que les infractions vers lesquelles ces associations tendent :

M. le président : Quel est l'avis du Gouvernement ? M. le garde des sceaux : Le Gouvernement [..] retient l'initiative du Sénat de créer une incrimination d'association de malfaiteurs. En revanche, il est opposé à l'idée de frapper cette incrimination plus sévèrement que l'infraction elle-même. Avec ce sous-amendement, les principes sont respectés, et la répression n'est pas excessive.[4]

Le délit d'association de malfaiteurs en matière informatique est donc distinct de l'association de malfaiteurs prévue par l'article 450-1 du code pénal [5] . La formule générique de l'association de malfaiteurs concerne les crimes et les délit punissables d'au moins 5 ans d'emprisonnement, ce qui n'est pas le cas des atteintes aux STAD pour lesquels le maximum encouru est 3 ans d'emprisonnement.

Similitude avec la "bande organisée" La rédaction de l'article 323-4 rappelle directement la définition de la circonstance aggravante de bande organisée prévue par l'article 132-71 du Code pénal et reprise par la loi du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité [6] (ci-après " loi Perben II ") :

Constitue une bande organisée au sens de la loi tout groupement formé ou toute entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs infractions.

La définition du délit prévue par l'article 323-4 du code pénal est identique. On pourrait donc parler, s'agissant de 323-4 d'un délit de "bande organisée en matière informatique". C'est que bande organisée et association de malfaiteurs recouvrent une même réalité. Cette identité de situation se traduit par

[3] P. 60, Rapport n°3 de la commission de lois du Sénat, fait par M. le sénateur Jacques THYRAUD, annexé du procès verbal de la séance du 2 octobre 1987.

[4] Compte rendu analytique de l'assemblée nationale, 3e séance du 21 décembre 1987, Journal Officiel, p. 8026.

[5] Art. 450-1 du CP : Constitue une association de malfaiteurs tout groupement formé ou entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'un ou plusieurs crimes ou d'un ou plusieurs délits punis d'au moins cinq ans d'emprisonnement. Lorsque les infractions préparées sont des crimes ou des délits punis de dix ans d'emprisonnement, la participation à une association de malfaiteurs est punie de dix ans d'emprisonnement et de 150000 euros d'amende. Lorsque les infractions préparées sont des délits punis d'au moins cinq ans d'emprisonnement, la participation à une association de malfaiteurs est punie de cinq ans d'emprisonnement et de 75000 euros d'amende.

[6] Loi n° 2004-204 du 9 mars 2004 art. 12 I Journal Officiel du 10 mars 2004.

une définition identique, mais selon que l'on est dans le champ de la bande organisée (132-71) ou de l'association de malfaiteurs (450-1 et 323-4), le but répressif diffère : la première est prévue comme circonstance aggravante de certaines infractions, la seconde est un crime ou un délit autonome en dehors de tout commencement d'exécution de l'infraction principale.

Inapplicabilité des nouveaux moyens d'enquête La loi Perben II permet d'augmenter les pouvoirs d'enquête pour certains crimes ou délits les plus graves, commis en bande organisée et visés limitativement à l'article 706-73 du code de procédure pénale (durée de la garde à vue à 4 jours, détention provisoire plus longue, opérations d'infiltration, de sonorisation ou encore d'interceptions de télécommunications possibles sans passer par le juge d'instruction).

Les infractions commises en bande organisée, visées à l'article 706-74 du Code de procédure pénale (les "moins graves") ne pourront pas bénéficier de ces nouvelles possibilités techniques et juridiques, mais seront susceptibles d'être traitées par les nouveaux pôles interrégionaux de lutte contre la délinquance économique et financière et de lutte contre la criminalité organisée.

Or, le délit *d'association de malfaiteurs informatiques* est, comme l'indiquait la réclame d'une marque de boisson pétillante, le Canada Dry de la bande organisée : il en a la substance (similitude des termes) mais pas l'étiquette (la définition juridique identique par le biais d'une circonstance aggravante distincte).

Cela n'est pas sans implications juridiques puisque au sens de la loi Perben II, le délit d'association de malfaiteurs informatique est insusceptible de bénéficier des moyens nouveaux ni même de ressortir de la compétence des pôles interrégionaux par le biais l'article 706-74, qu'on pourrait qualifier de "procédure balais" des bandes organisées.

On pourrait voir là un oubli ou un paradoxe de la loi : censée adapter la justice aux évolutions de la criminalité, elle ne s'applique pas aux infractions de haute technologie commises en bande organisée (art. 323-4 du cp). Or s'il est un domaine où la criminalité évolue rapidement, est capable de s'organiser et offre des possibilités de gains et d'impunité importantes, c'est bien celui de la cybercriminalité.

Alors qu'on évoque dans les risques liés à un "cyberterrorisme" pour l'instant abstrait, seul ce point d'entrée (l'article 421-1 du code pénal) permettrait de bénéficier des nouveaux moyens légaux offerts par la loi Perben II.

En conclusion, sur le fond, le "pacte des loups" entrera dans l'illégalité dès lors que les agents auront concrétisé leur projet commun, par exemple en mettant à la disposition du pirate une machine, un bureau, un local ou encore des éléments matériels en vue de la commission de l'intrusion.

Sur la procédure, les enquêteurs et magistrats devront se contenter des dispositifs habituels, ceux qu'on réserve à la délinquance de bas niveau, ou inorganisée, ce qui malheureusement n'est pas le cas en l'espèce.

3 La phase préparatoire

3.1 Récupération de l'information publique sur la cible

L'attaquant va réaliser son attaque de façon distante, il se place donc dans le cas ou il n'a pas accès au réseau interne de l'éditeur. Il va donc utiliser Internet et récupérer le maximum d'informations publiques sur sa cible et son contexte. A l'inverse de la prise d'empreinte, le pirate n'aura aucune interaction avec sa cible.

Pour réaliser cet objectif il a plusieurs moyens à sa disposition, nous nous attacherons à présenter ceux concerant les bases Whois, les bases DNS et les moteurs de recherche.

Les bases Whois Les bases Whois permettent de connaître le propriétaire d'une ou plusieurs adresses IP. On les utilise fréquemment pour connaître la ou les adresses IP d'un site Web. Ces bases sont librement consultables via Internet [3]. Elles contiennent également un certain nombre d'informations sur le propriétaire de l'adresse IP (adresse, personne à contacter en cas de problème...).

Il est à noter que la consultation de ces bases se fait de facon complétement furtive du point de vue de la cible, il n'y a acune interaction avec elle.

Dans notre cas, le pirate interroge la base RIPE via le site `network-tools` afin d'obtenir les adresses IP appartenant à sa cible ainsi que toutes les informations légales la concernant et renseignées dans la base.

Domain registry query for sstic.org :

```
Domain ID:D92668917-LROR
Domain Name:BUNKER.COM
Created On:29-Nov-2002 11:02:42 UTC
Last Updated On:24-Jan-2004 12:30:12 UTC
Expiration Date:29-Nov-2004 11:02:42 UTC
Sponsoring Registrar:R42-LROR
Status:OK

Registrant ID:0-674592-Gendi
Registrant Name:John Smith
Registrant Organization:John Smith
Registrant Street1:3rd street
Registrant City:New York
Registrant Postal Code:3492
Registrant Country:US
Registrant Email:john.smith@bunker.com

Admin ID:BP589-GENDI
Admin Name:John Smith
```

```
Admin Street1:4th street
Admin City:New York
Admin Postal Code:3942
Admin Country:US
Admin Phone:564.345623
Admin Email:john.smith@bunker.com

Tech ID:AR41-GENDI
Tech Name:CONTACT NOT AUTHORITATIVE see http://www.gendi.net/whois
Tech Organization:GENDI Corp
Tech Street1:see also whois.gendi.net
Tech City:New York
Tech Postal Code:3942
Tech Country:US
Tech Phone:1
Tech Email:support@gendi.net

Name Server:DNS.BUNKER.COM
```

DNS Records for bunker.com :

```
query from dns.consumer.net to get an authoritative nameserver
NameServer used for query: dns.bunker.com

Answer records
bunker.com 1 NS dns.bunker.com 28705s

Authority records

Additional records
dns.bunker.com 1 A 207.173.176.130 168337s
```

Network IP address lookup :

```
whois whois.ripe.net 207.173.176.142:

inetnum:      207.173.176.0 - 207.173.176.255
netname:      BUNKER
descr:        BUNKER
descr:        10th street
descr:        3942 NY
country:      US
admin-c:      JL644-RIPE
tech-c:       PT316-RIPE
tech-c:       OH251-RIPE
status:       ASSIGNED PA
mnt-by:       OLEANE-NOC
```

```
changed:      hostmaster@oleane.net 19970617
source:       RIPE

route:        62.160.0.0/16
descr:        OLEANE-970501
origin:       AS3215
holes:        62.160.248.0/24
mnt-by:       OLEANE-NOC
changed:      hostmaster@oleane.net 19970502
changed:      hostmaster@oleane.net 20020202
changed:      hostmaster@oleane.net 20021017
source:       RIPE

role:         OLEANE Hostmaster
address:      France Telecom Transpac
address:      20 rue Thomas Edison
address:      92230 Gennevilliers
phone:        +33 1 41 21 78 00
fax-no:       +33 1 41 21 78 99
e-mail:       hostmaster@oleane.net
admin-c:      CP460-RIPE
tech-c:       CW27
nic-hdl:      OH251-RIPE
notify:       hm-dbm-msgs@ripe.net
mnt-by:       OLEANE-NOC
changed:      hostmaster@oleane.net 20000814
changed:      hostmaster@oleane.net 20011105
source:       RIPE


address:      10 Av De Norvege
address:      Bp 742
address:      91962 Les Ulis
address:      France


nic-hdl:      JL644-RIPE
mnt-by:       OLEANE-NOC
changed:      hostmaster@oleane.net 19970617
source:       RIPE


address:      10 Av De Norvege
address:      Bp 742
address:      91962 Les Ulis
```

```
address:      France


nic-hdl:      PT316-RIPE
mnt-by:       OLEANE-NOC
changed:      hostmaster@oleane.net 19970617
source:       RIPE
```

Le pirate obtient donc l'adresse IP de sa victime ainsi que le sous réseau qui lui est attribué. Il récupère également les coordonnées de deux contacts, l'un de nature technique, et l'autre de nature administrative. Il obtient également l'adresse IP du serveur DNS de l'entreprise. Cette donnée est très utile car elle va permettre, nous verrons comment par la suite, de connaître l'ensemble des serveurs présents dans l'entreprise et accessible via Internet (à condition que leur soit associé un nom de domaine).

Les bases DNS Le pirate souhaite recupérer les enregistrements DNS correspondants au domaine de la cible. Cette étape se fait également sans interaction avec la victime.

Pour chaque adresse IP du domaine cible, le pirate va demander au DNS si il existe une entrée dans sa base. Dans la plupart des configurations, seules les adresses des serveurs sont renseignées de cette façon.

Le pirate va ainsi connaître les adresses IP des différents serveurs visibles sur Internet. Le nom associé à ces serveurs peut parfois nous renseigner sur leurs fonctions. Un script pour `bash` automatisant cette tâche pour `bash` se trouve en annexe 1.

```
Nom :    dns.bunker.com
Address:  207.173.176.130
--
Nom :    web.bunker.com
Address:  207.173.176.142
--
Nom :    mail.bunker.com
Address:  207.173.176.202
--
Nom :    ftp.bunker.com
Address:  207.173.176.250
--
Nom :    ssh.bunker.com
Address:  207.173.176.251
```

Il ressort de cette analyse qu'il y a seulement 5 entrées disponibles depuis l'extérieur : les 4 entrées renseignées par le DNS et le serveur DNS lui-même.

Grâce à ces informations, le pirate sait qu'il a potentiellement accés à 5 serveurs appartenant à l'entreprise cible.

Les moteurs de recherche L'utilisation d'un ou plusieurs moteurs de recherche va permetttre d'obtenir beaucoup d'informations sur la cible (informations sur les employés, la structure du réseau, les logiciels utilisés en interne...). Ces données sont rarement exploitables telles quelles, mais elles permettent de se faire une idée sur l'entreprise en général.

Par exemple, il arrive qu'un utilisateur pose ou réponde à des questions dans des forums de discussion. Ce type de comportements permet de renseigner le pirate sur l'environnement qu'il doit attaquer (dans le cas ou cet utilisateur est un administrateur du système cible), d'avoir une meilleure connaissance des compétences des employés, de leurs centres d'intérêt (très pratique au cas où il a besoin de faire de l'ingénérie sociale).

Le moteur de recherche `Google` [6] est un outil très précieux pour obtenir ce type d'informations car il permet, entre autres, de faire une recherche dans les groupes de discussion.

Le pirate reussit à identifier, via des annonces faites lors de salons informatiques, le responsable de la conception du jeu vidéo. Par ailleurs, il reussi, via des forums et l'option `Original Format` de Google, à recupérer un courier électronique et son entête qui lui permet de savoir quel est le serveur mail utilisé par l'entreprise cible.

```
Reply-To: "Bill John" <bill@bunker.com>
From: "Bill John" <bill@bunker.comd>
Newsgroups: comp.dev.microsoft.directx
Subject: Re: directx optimisation problems
Date: Sun, 5 Oct 2003 21:36:28 +0200
Organization: Bunker
MIME-Version: 1.0
Content-Type: text/plain;
charset="iso-8859-1"
Content-Transfer-Encoding: 8bit
X-Priority: 3
X-MSMail-Priority: Normal
X-Newsreader: Microsoft Outlook Express 6.00.2800.1158
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1165
Lines: 124
Message-ID: <3f8074dc$0$27598$626a54ce@news.bunker.fr>
NNTP-Posting-Date: 05 Oct 2003 21:45:32 MEST
NNTP-Posting-Host: 82.65.102.16
X-Trace: 1065383132 news2.bunker.com 27598 207.173.176.202:2504

You could resolve your problems by searching in the MSDN Library.
```

```
Enter your query in the index and follow the answer!

good luck and keep us in touch!

Bill

--
Chief Develloper/Demi-vie
Bunker Software
```

3.2 Cartographie et prise d'empreinte

Les méthodes précédentes n'engendraient aucune interaction avec le système cible, ce n'est plus le cas avec les méthodes de cartographie et de prise d'empreinte que le pirate va maintenant utiliser.

Ces méthodes offrent une granularité de résultats plus importante, mais en contrepartie elles sont beaucoup plus bruyantes en terme d'interactions avec le système cible. Si ce dernier possède un détecteur d'intrusion ou si les fichiers de journalisation sont correctement configurés et analysés, il sera capable de détecter ces interactions.

Le routage La connaissance du chemin emprunté par les paquets réseau permet souvent d'identifier la présence d'un pare-feu. Pour cela, le pirate va utiliser un outil très pratique et présent sur toutes les plate-forme : `traceroute`. Son fonctionnement est relativement simple, il va nous donnner des informations le chemin parcouru par nos paquets avant d'arriver sur la cible.

```
TraceRoute to www.bunker.com (207.173.176.142), 40 byte packets
 1  thing-i.sdsc.edu (198.202.76.40)  1.019 ms
 2  medusa.sdsc.edu (198.202.75.10)  0.759 ms
 3  piranha.sdsc.edu (132.249.30.8)  7.170 ms
 4  sdg-dc1--sdsc-sdsc2-ge.cenic.net (137.164.24.157)  6.171 ms
 5  lax-dc1-sdg-dc1-pos.cenic.net (137.164.22.46)  5.183 ms
 6  dc-sac-dc1--lax-dc1-pos.cenic.net (137.164.22.127)  12.831 ms
 7  dc-oak-dc2--csac-dc1-ge.cenic.net (137.164.22.110)  15.942 ms
 8  dc-oak-dc1--oak-dc2-ge.cenic.net (137.164.22.36)  15.870 ms
 9  dc-paix-px1--oak-dc1-ge.cenic.net (137.164.40.11)  16.017 ms
10  198.32.175.27 (198.32.175.27)  18.212 ms
11  p7-0.cr01.sntd.eli.net (207.173.114.137)  25.384 ms
12  p9-0.cr02.rcrd.eli.net (207.173.114.58)  23.388 ms
13  srp3-0.cr01.rcrd.eli.net (208.186.20.241)  25.533 ms
14  p9-0.cr02.ptld.eli.net (207.173.115.41)  34.162 ms
15  srp3-0.cr01.eli.net (208.186.21.3)  43.713 ms
16  srp0-0-0.gw01.eli.net (208.186.20.38)  43.211 ms
```

```
17  gw0-bunker-COM.eli.net (209.63.173.46)  47.575 ms
18  * * *
19  * * *
```

Cette méthode est sans interactions avec le serveur cible lorsque nous utilisons un `traceroute` disponible sur Internet. Cependant, cela ne permet pas toujours d'avoir la granularité que nous pourrions obtenir en interagissant directement avec les machines cibles.

En effet, le pirate constate qu'il n'arrive pas à atteindre les serveurs cibles (l'opération a été réalisé pour les 4 serveurs figurant dans les entrées DNS, seule celle concernant le serveur Web est présentée ci-dessus).

Ses paquets semblent en effect bloqués par un pare-feu. Etant donné qu'il souhaite connaître précisément l'architecture réseau de sa cible, notamment la présence d'éléments entre le pare-feu et les serveurs, il va être obligé de réaliser certaines actions en interrogant directement les serveurs. Cette méthode laisse des traces, mais c'est la seule qui permettent de faire les tests désirés.

Pour cela, il va utiliser l'utilitaire `Hping2` [5] qui va nous permettre de réaliser un `traceroute` en utilisant le protocole TCP. Le pirate va changer la valeur du champ IP Time To Live (`TTL`) et ainsi joindre exactement la machine souhaitée.

```
[root:/home/lefranc/hping2]# ./hping2 -S -p80 207.173.176.142 -t 19
HPING 207.173.176.142 (eth0 207.173.176.142): S set, 40 headers + 0
data bytes
len=46 ip=207.173.176.142 ttl=53 id=0 sport=80 flags=SA seq=0
win=5840 rtt=36.9ms
```

Le pirate arrive à atteindre le serveur sans problème puiqsu'il répond au paquet que nous lui avons envoyé. Ce serveur se trouve donc bien au hop 19.

```
[root:/home/lefranc/hping2]# ./hping2 -S -p80 207.173.176.142 -t 17
HPING 207.173.176.142 (eth0 207.173.176.142): S set, 40 headers + 0
data bytes
TTL 0 during transit from ip=209.63.173.46 /
name=gw0-bunker-COM.eli.net
```

La valeur donnée par le pirate au TTL ne permet d'atteindre que le routeur Internet. C'est lui qui répond à la requète en indiquant que le TTL a expiré.

```
[root:/home/lefranc/hping2]# ./hping2 -S -p80 207.173.176.142 -t 18
HPING 207.173.176.142 (eth0 207.173.176.142): S set, 40 headers + 0
data bytes
TTL 0 during transit from ip=207.173.176.10 name=UNKNOWN
```

La valeur donnée au TTL par le pirate permet d'atteindre une machine située entre le routeur Internet et le serveur. Selon toute vraissemblance, c'est un pare-feu que le pirate vient d'identifier à l'adresse 207.173.176.10.

Identification système : le balayage de ports Il est possible de déterminer les systèmes qui sont actifs et accessibles à partir d'Internet en utilisant un certain nombre de grandeurs fournies dans les divers champs des protocoles de communications.

En effet, bien que les RFC fournissent un cadre de mise en oeuvre et permettent ainsi une standardisation des protocoles d'échanges. La plupart des implémentations faites par les fabricants de systèmes d'exploitation sont conformes à ces RFC, mais en ont une interprétation différente, et permettent ainsi aux pirates de les identifier.

Dans notre cas, le pirate va utiliser l'outil `Nmap` [4] pour réaliser le balayage de port des différentes machines précédemment identifiées. Cela va lui permettre de vérifier que les services sont bien operationnels et d'être renseigné sur la nature du système d'exploitation utilisé.

Cette technique de prise d'empreinte est relativement fiable, mais elle génère une interaction avec la cible qui peut faire l'objet d'une détection de sa part. C'est pour cette raison que nous allons utiliser le mode furtif (`Stealth Scan`) de `Nmap` afin de ne pas initier complétement la connexion, et ainsi, d'être le plus discret possible.

```
[root:/home/lefranc]# ./nmap -sT -sV -vv -O -P0  207.173.176.142

Starting nmap 3.51-TEST2 ( http://www.insecure.org/nmap/ )
at 2004-04-13 21:37 CEST
Host web.bunker.com (207.173.176.142) appears to be
up ... good.
Initiating Connect() Scan against web.bunker.com
(207.173.176.142) at 21:37
Adding open port 80/tcp
The Connect() Scan took 23 seconds to scan 1660 ports.
Initiating service scan against 1 service on 1 host at 21:38
The service scan took 6 seconds to scan 1 services on 1 host.
Interesting ports on web.bunker.com (207.173.176.142):
(The 1649 ports scanned but not shown below are in state: closed)
PORT     STATE    SERVICE       VERSION
21/tcp   filtered ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
80/tcp   open     http          Microsoft IIS webserver 5.0
135/tcp  filtered msrpc
136/tcp  filtered profile
137/tcp  filtered netbios-ns
138/tcp  filtered netbios-dgm
139/tcp  filtered netbios-ssn
445/tcp  filtered microsoft-ds
```

```
3389/tcp filtered microsoft-rdp Microsoft Terminal Service
(Windows 2000 Server)
Device type: general purpose
Running: IBM AIX 4.X
OS details: IBM AIX 4.3.2.0-4.3.3.0 on an IBM RS/*
OS Fingerprint:
TSeq(Class=TR%TS=0)
T1(Resp=Y%DF=N%W=FFFF%ACK=S++%Flags=AS%Ops=MNWNNT)
T2(Resp=N)
T3(Resp=N)
T4(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)
T5(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)
T7(Resp=N)
PU(Resp=N)

TCP Sequence Prediction: Class=truly random
                         Difficulty=9999999 (Good luck!)
TCP ISN Seq. Numbers: ED8BE3AF 82230B4C D8C1E49E 368DB819
      B5C869F8 14227B78
IPID Sequence Generation: Busy server or unknown class

Nmap run completed -- 1 IP address (1 host up) scanned in
39.508 seconds
```

`Nmap` n'a pas été capable d'identifier le système d'exploitation de façon correctte, le manque de données en est probablement la cause. En effet, plus la machine cible "répond" aux requétes du pirate, plus `Nmap` va être capable de correctement l'identifier.

Dans notre cas, la machine cible n'a pas été suffisamment loquace ! (c'est peut-être le signe d'un pare-feu correctement configuré...). A l'inverse, il a bien reconnu la version du serveur web installé sur la machine `web.bunker.com`.

Etant donné la nature de ses applications, le pirate en conclu que le serveur Web fonctionne sous le système d'exploitation Windows. Cela lui est confirmé par le site Web `Netcraft` [7] qui répertorie, entre autre, les évolutions de configuration des serveurs Web qui sont dans sa base de données. Ce site identifie le serveur Web du système cible comme étant Windows 2000. C'est cohérent par rapport à l'information que le pirate a déjà recueilli.

Identification logiciel : les entêtes Chaque service possède une entête (ou bannière) qui permet de l'identifier. La connaissance de ces entêtes associée aux résultats fournis par `Nmap` permettent de connaître la machine cible de façon très fine.

L'attaquant va donc récupérer les entêtes des différents services précédemment identifiés.

```
[root:/home/lefranc]# telnet 207.173.176.142 80
Trying 207.173.176.142...
Connected to web.bunker.com (207.173.176.142).
Escape character is '^]'.
GET HTTPS
HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/5.0
Date: Tue, 13 Apr 2004 17:40:30 GMT
Content-Type: text/html
Content-Length: 87

<html><head><title>Error</title></head><body>The parameter
is incorrect.
</body></html>Connection closed by foreign host.
```

le pirate recupère la bannière du serveur Web de l'entreprise. Cela confirme ce qu'il avait déjà conclu à l'étape précédente, le serveur Web est basé sur une architecture à base de produits Microsoft.

Toutes les informations que le pirate vient de récupérer, à la fois de façon passive, mais aussi en agissant sur le système, vont lui fournir la connaissance nécessaire à la réalisation de son attaque.

3.3 L'arbre d'attaque

Lors des phases précédentes, le pirate a récolté autant d'informations que possible sur sa cible, à la fois de façon passive, mais aussi en interagissant avec elle. Il a une bonne idée de son architecture matérielle et logicielle (figure 1).

Le but du pirate est de s'introduire sur le réseau de sa cible afin de dérober les sources du futur jeu. Le fait d'identifier un ou plusieurs serveurs vulnérables ne lui est pas d'une grande utilité, même si par "rebond" il lui serait possible d'atteindre son objectif. Le plus simple, compte tenu de ses impératifs de réussite, serait de prendre la main sur la machine d'un développeur du jeu et ensuite d'accéder au serveur ou sont stockées les sources du jeu.

Les informations qu'il a recupérés via `Google` lui indiquent deux choses :
- les employés ont accés à Internet depuis leur poste travail car il existe des traces de leurs discussions dans les forums,
- le serveur de mail est le logiciel `Exchange` de Microsoft, il est donc fort probable que les postes utilisateurs fonctionnent avec le système d'exploitation Windows et utilise le navigateur Internet Explorer.

Ce dernier point est renforcé par le fait que Windows est également la plateforme sur laquelle s'exécutera le futur jeu, il y a donc de fortes chances que ce soit également le type d'OS utilisé par les développeurs.

La mise en corrélation de toutes les informations que le pirate a obtenues lui permet de construire l'arbre d'attaque nécessaire à la réalisation de son objectif.

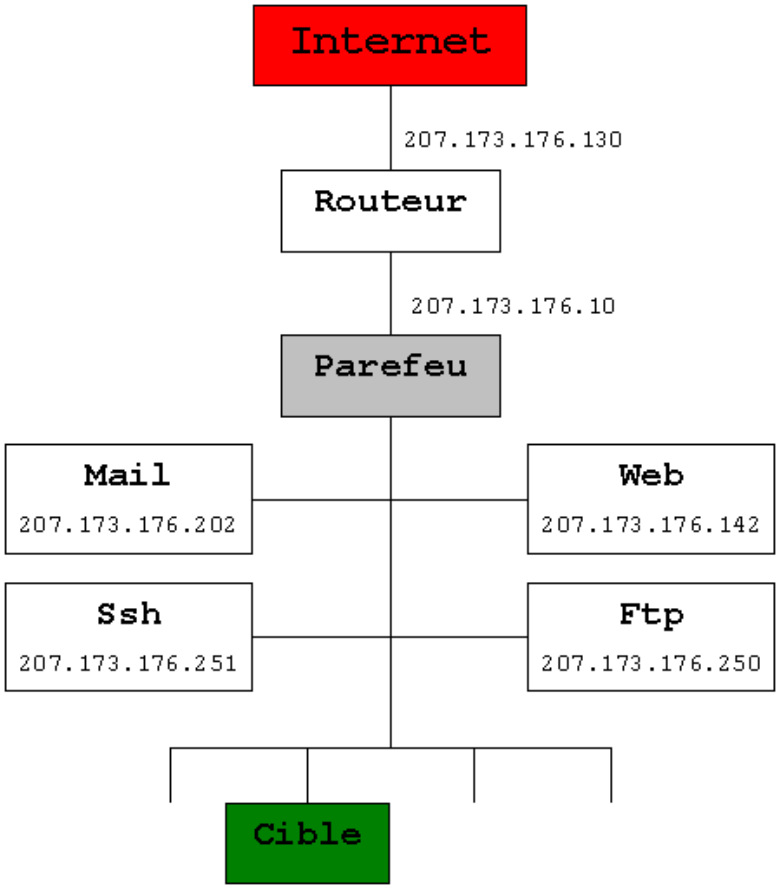

Fig. 1. Architecture de l'entreprise cible

Cette attaque va consister à faire télécharger et exécuter un cheval de Troie par le chef de l'équipe de dévelopement.

Pour cela, il utilise une faille dans Internet Explorer [8] qui permet de faire télecharger un programme et de le faire exécuter lorsque qu'un utilisateur visite une page web, et ce, sans que cette personne en ait conscience. Le pirate va donc forger un mail à l'attention du chef d'équipe, ce mail contient un lien vers la page piégée. L'astuce, pour le pirate, va être de faire en sorte que sa victime aille sur la page incriminée.

Une fois installé, le cheval de Troie va essayer de contacter une machine cliente appartenant au pirate. Ce cheval de Troie n'est rien d'autre que le programme `netcat`. Etant donné que l'entreprise est dotée d'au moins un pare-feu fonctionnant via la méthode `statefull inspection`, le serveur `netcat`ne sera pas accessible de l'extérieur du réseau interne. Pour remédier à ce problème, ce sera le serveur qui initiera la connexion (fonctionnement en mode `reverse connection` vers le client.

Le cheval de Troie permet au pirate d'avoir accés à la machine victime et, notamment, de télécharger et d'installer tout ce qui lui est nécessaire pour atteindre son objectif. Ces composants supplémentaires sont au nombre de trois :

- L'outil Hacker Defender [9] permet de dissimuler une ou plusieurs applications au sein du système d'exploitation. Une fois ce logiciel installé l'utilisateur peut cacher des fichiers, des processus, des services, des drivers système, des clefs de registre, des ports ouverts et enfin modifier l'espace disque disponible.
- un keylogger [10] pour recupérer toutes les touches frappées par l'utilisateur, et notamment les mots de passe de connexions aux autres machines.
- un sniffeur [11] pour analyser les flux auxquels la machine victime a accès, afin de consolider les informations obtenues par les précédents outils..

4 L'opération "Carbone 14"

4.1 La tentative consommée

Le pirate met en pratique l'arbre d'attaque qu'il a élaboré. Il crée une page web sur chez un hébergeur en ligne, en ayant au préalable tout réalisé depuis un "café Internet" afin de minimiser ses traces. Il élabore le contenu du faux site en fonction des centres d'intérêts de la personne qui va aller le visiter.

Il forge un mail dans lequel il se fait passer pour une connaissance de la victime et l'incite à se rendre sur la page en question. Dès que la victime visionne la page, le cheval de Troie s'installe et essaie de se connecter à son client.

4.2 Le vol de sources

Le pirate rapatrie via le réseau les données contenant le code source du jeu "demi-vie". Il est aidé dans cette tâche par le cheval de Troie. En effet, le chef

de projet a, comme l'ensemble des développeurs, un accés direct sur le serveur contenant les sources.

Le cheval de Troie a permis l'installation d'un keylogger qui va pouvoir enregistrer toutes les touches frappées par la victime. Il va notamment permettre de recupérer le mot de passe permettant l'accés au serveur des sources. Lorsque cette opération est réalisée, le pirate prend le contrôle à distance de la machine du chef de projet et se connecte sur un serveur `FTP` afin d'y déposer l'ensemble des fichiers présents sur le serveur.

4.3 La réalisation du préjudice : la dissémination

Le pirate compile les sources et les diffuse ensuite via un service de pair à pair. Rapidement le jeu se dissémine sur le réseau. La presse spécialisée s'empare de cette information et rapidement le tout le microcosme du monde du jeu vidéo est au courant. Les éditeurs cocurrents s'empressent de télécharger le jeu afin d'analyser son potentiel et, eventuellement, de le comparer avec leurs propres productions.

Il y a également une phase 3 bis : c'est celle qui permet au pirate de toucher sa rétribution. Celle ci n'est pas à négliger sur le terrain de la preuve, car tout flux d'argent laisse des traces : au moins un débit au départ et un crédit à l'arrivée.

5 L'enquête

5.1 L'enquête technique post-intrusion réalisée par la victime

L'utilisateur légitime de la machine piratée va remarquer une instabilité de son système. Il décide de faire appel aux administrateurs système afin d'élucider les causes de ces disfonctionnements.

6 Conclusion

La morale de l'histoire : si vous ne voulez pas que le cadavre de votre entreprise doit daté au "Carbone 14", n'attendez pas une "demi-vie" pour protéger simplement votre patrimoine : un tandem juridique et technique sera plus rentable que des logiciels de sécurité seuls ou des contrats d'assurance seuls.

7 Remerciements

Nous souhaitons remercier toutes celles et ceux qui ont pu contribuer à la réalisation de cet article.

Références

1. Valve Software, http://www.halflife2.net/forums/showthread.php?threadid=10692
2. MISC Magazine, http://www.miscmag.com
3. Network Tools, http://www.network-tools.com
4. Nmap, http://www.insecure.org
5. Hping2, http://www.hping.org
6. Google, http://www.google.com
7. Netcraft, http://www.netcraft.com
8. Internet Explorer Unspecified CHM File Arbitrary Code Execution , http://www.k-otik.net/bugtraq/02.18.InternetExplorer.php
9. Hacker Defender, http://rootkit.host.sk/
10. Klogger, http://www.ntsecurity.nu/toolbox/klogger/
11. TCPdump, http://www.tcpdump.org

8 Annexe 1

```
#!/bin/bash

if [ -z "$1" ]; then
    echo
    echo "USAGE : ./lookup addr_ip_range bit_inf bit_sup string_match"
    echo "   ex : ./lookup 10.11.12 1 255 coco"
    echo
    exit
fi

base_ip="$1"
inf="$2"
sup="$3"
string="$4"

for i in ‘seq $inf $sup‘;
do
nslookup $base_ip.$i >> nslookup_res.txt
done

grep -A 1 -i $string nslookup_res.txt > addr_ip_res.txt

exit 0
```