L'opération Carbone 14 :

Les modalités pratiques et les implications juridiques d'une attaque informatique

Serge LEFRANC

David BENICHOU

MINISTÈRE DE LA DÉFENSE

DGA

L'opération « Carbone 14 »

Introduction

Introduction

Scénario

- Un éditeur informatique emploie un pirate pour nuire à son concurrent, mais également pour essayer de connaître les progrès des dernières techniques de programmation qu'il ne maîtrise pas encore.

- Le pirate doit s'introduire dans le réseau concurrent et récupérer le code source du jeu en cours de réalisation et d'en assurer la diffusion via Internet.

- Afin de minimiser les risques, l'opération doit se dérouler à distance, rien ne doit être réalisé en local.

- Le but du pirate n'est pas d'être exhaustif dans sa façon de procéder, il ne souhaite pas trouver toutes les failles du système. Son objectif est d'en trouver une et de l'exploiter afin d'atteindre son objectif.

Plan de l'exposé

- **Introduction**
- **Le « pacte des loups »**
  - Aspects techniques et juridiques.
- **La phase préparatoire**
  - Collecte statique et dynamique de l'information.
  - Réalisation de l'arbre d'attaque
  - Moyens logistiques.
- **L'opération « Carbone 14 »**
  - Tentative consommée et réalisation du préjudice.
- **L'enquête**
  - Aspects techniques et juridiques.
- **Conclusion**

L'opération « Carbone 14 »

Le « pacte des loups »

L'opération « Carbone 14 »

Le « pacte des loups »

- **Afin de réaliser son objectif, l'éditeur concurrent a besoin d'un pirate dont les compétences techniques sont reconnues, il doit le connaître et ce dernier doit être vénal.**

- **2 possibilités existent:**
  - Le pirate est recruté en **externe**. C'est risqué au niveau de la fiabilité, mais il est plus difficile de remonter jusqu'au commanditaire.
  - Le pirate est recruté en **interne**, il appartient au personnel. Ses intérêts sont communs avec ceux de son employeur, mais cela comporte des risques pour le commanditaire.

L'opération « Carbone 14 »

Le « pacte des loups »: une association de malfaiteurs






Art. 323-4 du code pénal:

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

323-4 pour les développeurs

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

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

L'opération « Carbone 14 »

323-4: les fondements (1987)

*« Or, ces dernières années ont vu fleurir **des 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 commission de **punir les ententes établies en vue de la préparation du délit de piratage informatique.** »*

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.

323-4: la répression

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

- ***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.***

L'opération « Carbone 14 »

323-4: similitude avec la bande organisée

Art. 132-71 du code pénal (bande organisée)

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.

Art. 323-4 du code pénal (association de malfaiteurs)

La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisé 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.

L'opération « Carbone 14 »

Finalité répressive différence

Art. 132-71 du code pénal (bande organisée)

- Circonstance aggravante d'une infraction principale.
  - Ex: le vol en bande organisée.

Art. 323-4 du code pénal (association de malfaiteurs)

- Infraction autonome: intérêt d'une répression précoce.
  - Ex: la bande de braqueurs est une association de malfaiteurs.

L'opération « Carbone 14 »

Association de malfaiteurs & Perben II

- **La loi du 9 mars 2004, portant adaptation de la justice aux évolutions de la criminalité, prévoit des nouveaux moyens d'enquête pour des situations relevant de la criminalité organisée (infiltration, sonorisation…).**

- **Le critère d'application des nouveaux moyens repose une liste limitative d'infractions, les plus graves, commises en bande organisée (art. 706-73 du CPP).**

- **Pour les autres infractions commises en bande organisée, un dispositif « balai » permet le traitement par les juridictions interrégionales spécialisées (art. 706-74 du CPP).**

L'opération « Carbone 14 »

Le paradoxe de Perben II et 323-4

- **L'association de malfaiteurs informatiques (art. 323-4 du CP), *Canada Dry de la bande organisée et version minimale de l'association de malfaiteurs générique* (même définition, mais effet différent) échappe aux nouvelles dispositions de la loi Perben II.**

- **Ceci est paradoxal: l'association de la malfaiteurs informatiques incarne typiquement le haut niveau d'organisation et de sophistication que peut revêtir une activité criminelle, pourtant, les nouveaux moyens d'enquête ne lui bénéficieront pas, ni même les juridictions interrégionales spécialisées !**

L'opération « Carbone 14 »

La phase préparatoire

1. **Collecte PASSIVE d'informations sur la cible**
2. **Collecte ACTIVE d'informations sur la cible**
3. **Réalisation de l'arbre d'attaque**
4. **Préparation logistique**

La phase préparatoire

- **Cette phase est nécessaire au pirate afin de récupérer et d'assembler tous les éléments dont il a besoin pour mener à bien son objectif.**

- **Collecte d'informations sur la cible.**
  - Le pirate doit récupérer le maximum d'informations concernant la cible afin de construire l'arbre d'attaque.

- **Ces informations peuvent être obtenues de façon passives ou dynamiques.**
  - Dans le 1er cas, les actions de l'attaquant se font sans interaction avec la cible, dans le 2ème, l'attaquant exerce une stimulation et observe le résultat.
  - Cela va avoir un impact sur les traces potentielles qu'il peut laisser. Plus la collecte se fait de façon dynamique, moins le pirate est discret, mais plus les informations recueillies peuvent être pertinentes…
  - Certaines actions ne seront pas sans conséquences au niveau juridique.

La phase préparatoire

- **Par recoupement, ces informations vont permettre au pirate d'établir le chemin maximisant son potentiel de réussite.**
- **Il va être pouvoir élaborer une stratégie dont il déduira l'arbre d'attaque.**
- **La dernière partie de la phase préparatoire va consister à mettre en place les moyens logistiques nécessaires à la réussite de l'objectif.**
  - Ils peuvent être de nature logicielle et opérationnelle.
  - Ils garantissent la confidentialité des opérations menées par le pirate, ainsi que la non-imputabilité des actions aux commanditaires.

L'opération « Carbone 14 »

La phase préparatoire

1. **Collecte PASSIVE d'informations sur la cible**
2. Collecte ACTIVE d'informations sur la cible
3. Réalisation de l'arbre d'attaque
4. Préparation logistique

Les bases WHOIS

- **Elles permettent de connaître le propriétaire d'une ou plusieurs adresses IP et sont librement consultables via Internet.**
- **Dans notre cas, le pirate va utiliser un outil se trouvant sur Internet et réalisant cette tache pour lui (`www.network-tools.com`). Il interroge la base RIPE concernant le site web de la victime, `www.bunker.com`.**
  - Il obtient l'adresse IP de la victime ainsi que le sous réseau qui lui est attribuée. Il récupère les coordonnées de 2 contacts, l'un de nature administrative et l'autre de nature technique.
  - Il récupère également l'adresse du serveur DNS qui va lui permettre d'interroger la base DNS.
- **Tous ces éléments vont permettre de délimiter le périmètre d'attaque.**

Les bases DNS

- **Ce sont des tables qui font la correspondance entre un nom de machine et une adresse IP.**
- **Le pirate veut identifier quelles sont les machines renseignées dans le serveur DNS de la victime. Le nom de ces serveurs peut nous indiquer leur fonction.**
  - Pour cela, il utilise la technique du `reverse lookup`: il interroge le serveur en lui demandant, pour chaque adresse IP appartenant à l'entreprise, quelle est le nom de la machine… Si il n'y a pas de nom de machine associée à cette adresse IP, le serveur DNS renvoi une erreur, sinon il renvoi le nom de la machine.
  - Cette technique va permettre d'identifier toutes les machines nommées et accessibles depuis Internet!
- **L'analyse montre qu'il y a 5 entrées disponibles depuis l'extérieur (DNS, Web, mail, FTP et SSH).**

Les moteurs de recherche

- **Leurs utilisation va permettre d'obtenir des informations sur la cible, que ce soit techniques, professionnelles ou personnelles.**
  - Ils archivent systématiquement les messages des groupes de discussions et cela peut se révéler très utile pour connaître les goûts de certains utilisateurs ou les problèmes techniques non résolus...
- **Dans notre cas, le pirate identifie le responsable du développement du jeu qu'il doit pirater via les annonces faites dans un salon sur le jeu vidéo.**
  - En possession du nom et de l'adresse email de sa victime, il utilise le moteur de recherche `www.google.com` et l'option `Original Format` afin de récupérer les entêtes des mails émis par le responsable du jeu « Demi-vie ».
- **Cela va lui permettre d'identifier que l'entreprise utilise le client de messagerie `Outlook Express` de Microsoft.**

L'opération « Carbone 14 »

La phase préparatoire

1. Collecte PASSIVE d'informations sur la cible
2. **Collecte ACTIVE d'informations sur la cible**
3. Réalisation de l'arbre d'attaque
4. Préparation logistique

Le routage

- **La connaissance du chemin emprunté par les paquets réseau permet souvent d'identifier l'architecture du SI.**
  - Et notamment la présence d'un pare-feu…
- **Le pirate va utiliser le logiciel `traceroute`.**
  - Ce logiciel utilise l'option « durée de vie » du protocole IP (champ TTL) pour émettre un message `ICMP TIME_EXCEEDED` pour chaque routeur. A chaque fois qu'un routeur manipule le paquets, il décrémente le champ TTL. Ce champ ayant une valeur déterminé au départ, il devient possible d'en déduire le nombre de routeur emprunté par le paquet.
- **Cela va permettre au pirate de connaître le chemin parcouru par ses paquets avant d'arriver à la cible.**

Le routage

- **Cette méthode n'a pas nécessairement d'interactions avec la cible.**
  - Il est possible d'utiliser des outils disponibles sur Internet, mais cela ne permet pas d'avoir une granularité aussi fine que lors d'une interrogation directe (notamment via l'utilisation d'option spécifique).
- **Le pirate constate qu'il n'arrive pas à atteindre les serveurs cibles.**
  - Les paquets semblent bloqués par un pare-feu.

Le routage (exemple)

```
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  * * *
```

Le routage

- **Il souhaite connaître l'architecture du réseau entre le pare-feu et les serveurs cibles, il va donc utiliser l'outil `Hping2` qui permet de réaliser un `traceroute` en utilisant le protocole `TCP`.**
  - En changeant la durée de vie du paquet, il va être capable de joindre exactement le serveur cible. Il obtient ainsi la confirmation de la présence du pare-feu et son adresse IP (207.173.176.10).

[serveur Web]

```
[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
```

[routeur]

```
[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
```

[pare-feu]

```
[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
```

Le balayage de ports

- **Il est possible de déterminer les systèmes qui sont actifs et accessibles à partir d'Internet.**
- **Les RFC fournissent un cadre de mise en œuvre et permettent une standardisation des protocoles d'échanges.**
  - Les implémentations faites par les constructeurs d'OS sont conformes à ces RFC, mais en ont parfois une interprétation différente, ce qui va permettre d'identifier ces systèmes d'exploitation.
- **L'outil `Nmap` va permettre de réaliser cette tâche.**
  - Cette technique est relativement fiable, mais elle génère un trafic important qui peut faire l'objet d'une détection.
  - Nous allons utiliser le mode furtif qui permet de laisser moins de traces.

Le balayage de ports (exemple)

```
[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
[…]
(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/*
```

Le balayage de ports

- **Le pirate considère que `Nmap` n'a pas été capable de correctement identifier l'OS.**
  - Compte tenu des services en fonctionnement, il ne semble pas possible que l'OS soit de type `Unix AIX`.

- **Grâce à l'identification des services tournant sur la machine, le pirate en déduit que le serveur fonctionne sous l'OS Microsoft Windows NT.**
  - C'est confirmé par le site `www.netcraft.com` qui répertorie les évolutions de configuration des serveurs Webs présents dans sa base.
  - D'après ce site, l'OS utilisé est `Windows 2000`.
  - C'est déjà plus cohérent compte tenu de ce qui a précédemment été trouvé.

Les entêtes logiciels

- **Chaque service possède un entête (ou bannière) permettant de l'identifier.**
  - Leur connaissance, associée aux précédents résultats, permet de connaître avec plus de précisions la configuration du système cible.
- **Le pirate va donc « interroger » les différents services pour récupérer leurs bannières.**
  - Ces requêtes peuvent être légitimes ou non.
- **Les informations que le pirate récupère confirment ce qu'il avait déjà découvert.**
  - L'environnement de l'entreprise est fortement orientée vers des solutions Microsoft.

L'opération « Carbone 14 »

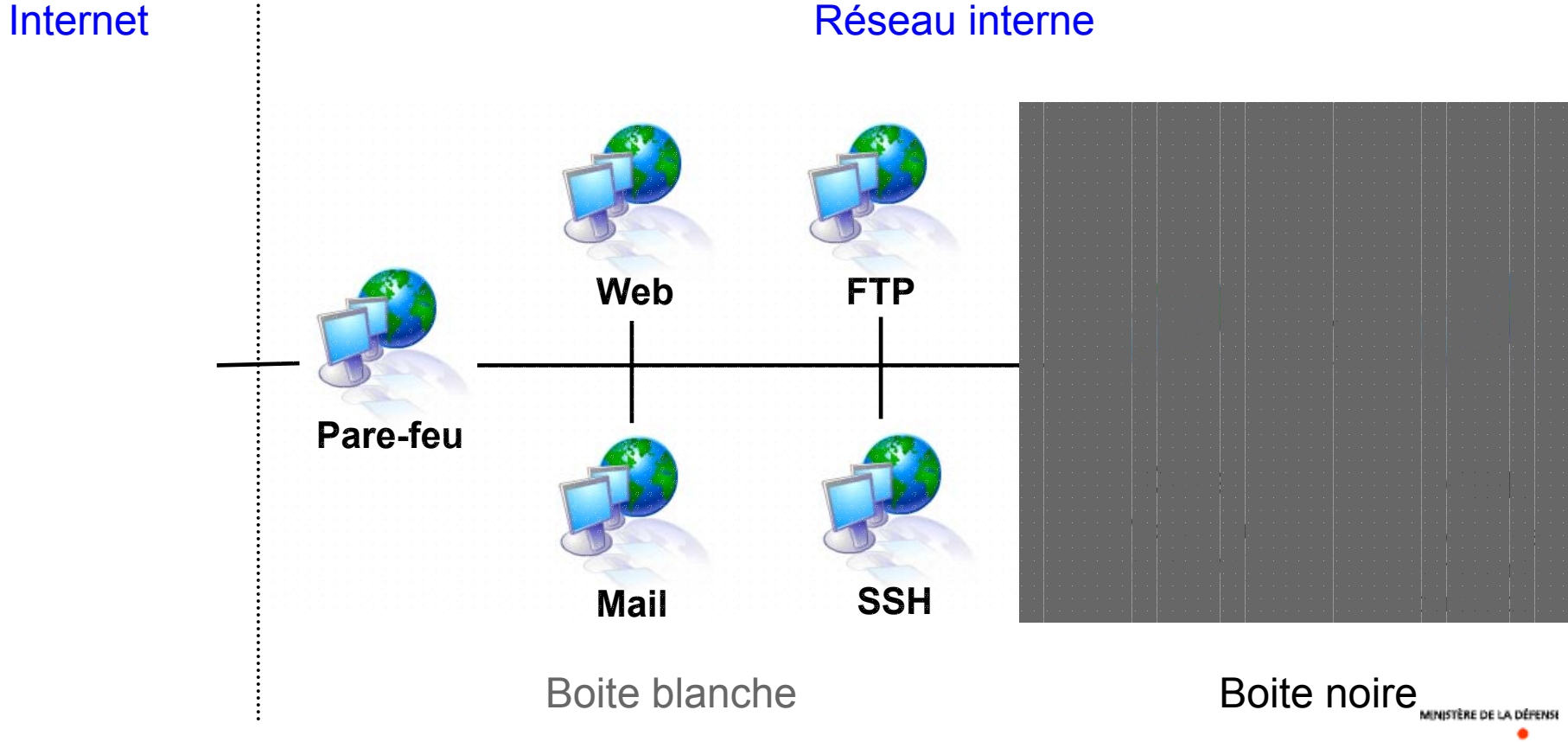
La phase préparatoire

1. Collecte PASSIVE d'informations sur la cible
2. Collecte ACTIVE d'informations sur la cible
3. **Réalisation de l'arbre d'attaque**
4. Préparation logistique

L'arbre d'attaque

- **Avec les éléments que le pirate a précédemment récupérés, il en déduit une partie de l'architecture du réseau cible.**
  - Elle sera affinée une fois qu'il aura atteint l'intérieur du système.
- **Il est maintenant capable de mettre au point le scénario de son attaque.**

L'arbre d'attaque (architecture)



L'arbre d'attaque

- **Le but du pirate est de s'introduire sur le réseau de sa cible et de dérober les source du jeu « demi-vie ».**
  - Le fait d'identifier un ou plusieurs serveurs vulnérables ne lui est pas d'une grande utilité.
  - Compte tenu de ses objectifs, le plus simple est d'essayer de prendre la main sur la machine d'un développeur du jeu pour ensuite pouvoir accéder par rebond au serveur de stockage des sources.
- **L'attaque va donc consister à faire télécharger et exécuter un cheval de Troie par le chef du développement.**
- **Le pirate est particulièrement intéressé par 2 informations qu'il a précédemment récupérées:**
  - Les employés ont accès à Internet depuis leur poste de travail.
  - L'environnement logiciel semble fortement orienté vers les produits de Microsoft, il en déduit que le client de navigation a de bonnes chances d'être `Internet Explorer`.

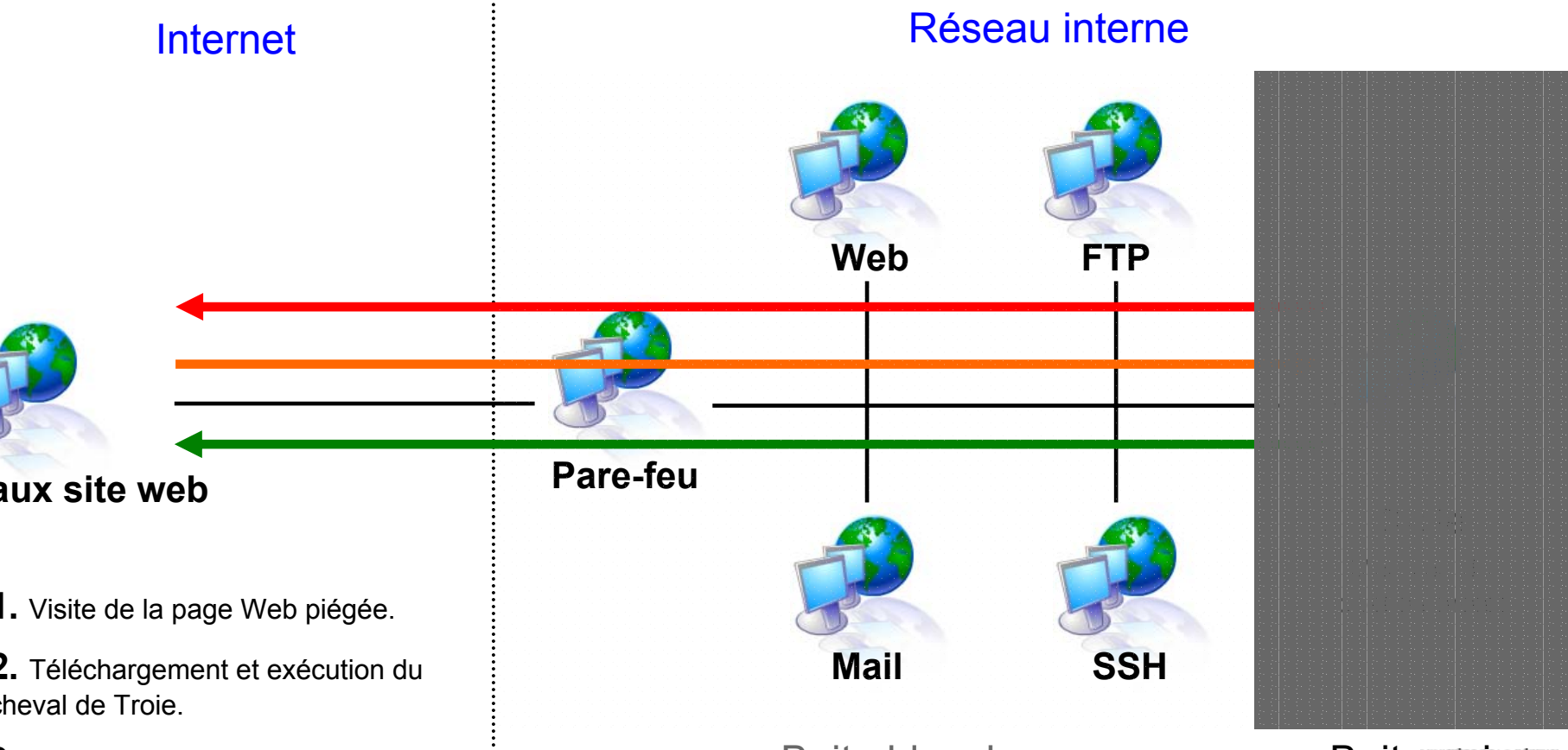
L'opération « Carbone 14 »

L'arbre d'attaque (modus operandi) 4/5

- **Le pirate utilise une faille d'`Internet Explorer` qui permet, lors de la visualisation d'une page Web, de faire télécharger et d'exécuter un programme sans que l'utilisateur n'en soit averti.**
  - La faille étant récente (mars 2004), le pirate compte sur le fait que le système informatique n'est pas encore été mis à jour.
- **Le pirate va donc forger un mail contenant un lien vers une page Web qu'il aura créée et contenant le programme malveillant.**
- **Afin d'être sûr que sa victime va se rendre sur ce site, il va utiliser des techniques d'ingénierie sociale.**
  - Le mail sera, par exemple, en rapport avec les centres d'intérêts personnels du développeur et émis par une de ses connaissances afin de maximiser les chances que la victime « visite » la page…

L'opération « Carbone 14 »

L'arbre d'attaque



1. Visite de la page Web piégée.
2. Téléchargement et exécution du cheval de Troie.
3. Le cheval de Troie se connecte chez le pirate.

L'opération « Carbone 14 »

La phase préparatoire

1. Collecte PASSIVE d'informations sur la cible
2. Collecte ACTIVE d'informations sur la cible
3. Réalisation de l'arbre d'attaque
4. **Préparation logistique**

Préparation logistique

- **Le pirate doit se procurer les moyens logiciels nécessaires:**
  - **au maintien de son accès sur la machine cible;**
  - **au rapatriement des données**
    - par exemple: un cheval de Troie, un keylogger, un analyseur de paquets…
- **Il doit également confectionner:**
  - **un faux site web;**
  - **un courriel qui servira à attirer la victime vers le site piégé.**

Préparation logistique

- **Le pirate doit aussi mettre en place des moyens opérationnels pour garantir sa clandestinité:**
  - Il doit faire héberger son faux site web à partir d'une machine piratée ou de confiance.
  - Ses actions pourront être menées à partir de cafés Internet, il doit donc repérer ceux où il pourra officier en toute tranquillité…
  - D'autres moyens sont possibles mais ne seront pas détaillés

L'opération « Carbone 14 »

Analyse juridique des actes préparatoires

323-4 CP 323-3-1 CP

1

Renseignement ouvert

(bases de données publiques, moteurs de recherche)

323-4 CP 323-3-1 CP

2

Collecte dynamique
(balayage de ports, traceroute, en-têtes logiciels)

a. Un balayage de ports peut-il caractériser une tentative d'accès frauduleux ?

3

Arbre d'attaque
(Elaboration du mode opératoire)

b. Quid de la légalité des outils utilisés ? (art. 323-3-1 du CP)

4

Logistique

(outils d'attaque, moyens matériels et lieux d'action)

MINISTÈRE DE LA DÉFENSE DGA

L’opération « carbone 14 »

La réalisation de l'attaque

- **Le pirate met en pratique l'arbre d'attaque qu'il a élaboré.**
  - La page piégée est créée chez un hébergeur en ligne et l'intégralité du processus est réalisé depuis un café Internet afin de minimiser les traces.

- **Lorsque la page est visitée, le cheval de Troie est téléchargé puis exécuté par la victime.**
  - Le pirate fait l'hypothèse que le pare-feu de l'entreprise fonctionne en mode `statefull inspection` et que le cheval de Troie n'est pas joignable directement depuis l'extérieur.
  - Le pirate le configure donc pour qu'il fonctionne en mode `reverse connection` et contacte une machine précise dont il a le contrôle (c'est le serveur qui va initier la connexion et non pas le client).

La prise de contrôle

- **Une fois le cheval de Troie installé, le pirate transfère vers la machine compromise 3 composants lui permettant de réaliser ses objectifs, tout en conservant un accès frauduleux à la machine:**
  - L'outil `Hacker Defender` qui va lui permettre de dissimuler ses fichiers au sein de l'OS;
  - Le keylogger `Klogger` pour récupérer toutes les touches frappées par l'utilisateur, et notamment les mots de passe d'accès aux autres machines;
  - Le sniffeur réseau `TCPdump` pour analyser le trafic de et à destination de la machine piratée.

Une cascade de délits

Article 323-1

ACCES, MAINTIEN, MODIFICATIONS: 2 ANS

Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'un an d'emprisonnement et de 15000 euros d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de deux ans d'emprisonnement et de 30000 euros d'amende.

Article 323-3

INJECTION DE DONNEES: 3 ANS

Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de trois ans d'emprisonnement et de 45000 euros d'amende.

Le vol de sources

- **Le pirate a maintenant un accès au réseau interne de l'entreprise.**
  - Il attend que la victime se connecte au serveur contenant les sources.
  - Il récupère les informations enregistrées par le keylogger afin d'obtenir le mot de passe permettant la connexion sur ce serveur.
- **Il rapatrie, via le réseau, le code source du jeu « demi-vie ».**
  - Il transfère les sources vers un serveur FTP qu'il contrôle.

L'opération « Carbone 14 »

Peut-on voler un fichier ?

VOL = soustraction FRAUDULEUSE de la chose d'AUTRUI

L112-2, 14° du CPI: les logiciels, ainsi que le matériel de conception sont des **œuvres de l'esprit**

L335-3: la violation d'un des droit d'auteur de logiciel est une **contrefaçon**

L335-2: **Contrefaçon** = **3 ANS + 300.000 €**

si **bande organisée** = **5 ANS + 500.000 €**

Bonus: L335-5: **Fermeture de l'établissement pour 5 ANS**

L'opération « Carbone 14 »

La dissémination

- **Après avoir récupéré le code source sur son serveur FTP, le pirate les compile et le met à disposition du publique via un service de pair à pair.**
  - L'opération de dissémination est réalisée à partir d'un café Internet.
- **Rapidement le jeu se propage sur le réseau et la presse spécialisée s'empare de l'information.**
  - Le microcosme du jeu vidéo est rapidement au courant et les éditeurs concurrents s'empressent de télécharger le jeu afin de le comparer avec leurs propres productions.

L'opération « Carbone 14 »

L'enquête technique post intrusion

L'opération « Carbone 14 »

L'enquête technique post intrusion 1/2

- **L'utilisateur légitime de la machine va remarquer une dégradation des performances de fonctionnement, ce qui se manifeste notamment par une instabilité du système.**
  - C'est dû aux logiciels installés par le pirate.
- **Par ailleurs, les administrateurs systèmes remarquent une augmentation du trafic sortant de leur réseau et identifient sa provenance après enquête.**
  - Ils mettent en évidence que la machine du chef de projet a été compromise et qu'elle est à l'origine de la fuite du code source disponible sur Internet.
- **Une plainte va être déposée et l'enquête judiciaire et technique va pouvoir commencer…**

L'enquête technique post intrusion 2/2

- **L'identification de l'auteur va dépendre de son degré de compétence dans les domaines suivants:**
  - Technique (quelles sont les traces logiques qu'il a laissé ?).
  - Juridique (quelle est sa connaissance du principe de fonctionnement d'une enquête judiciaire et des moyens légaux mis en œuvre pour récupérer l'information suite au délit ?).
  - Organisationnel (gestion de la clandestinité faisant suite à l'action).

L'opération « Carbone 14 »

Conclusion

Conclusion

- **Si vous ne voulez pas que le cadavre de votre entreprise soit daté au « carbone 14 », n'attendez pas une « demi-vie » pour protéger votre patrimoine.**

- **Bien qu'indispensables, les outils de sécurité ne sont pas suffisants.**

- **En matière d'attaque et de défense, seule une approche à la fois technique et juridique permet d'envisager tous les aspects du théâtre des opérations: d'abord dans la sphère technique, puis sociétale.**
  - ➔ Les informaticiens ont tendance à oublier que tout ne se situe pas au plan technique et que bien des choses sont possibles après l'action…

Conclusion (Principes fondamentaux de sécurité) 2/2

- **Il faut séparer physiquement le réseau qui supporte le patrimoine informationnel de la société et les réseaux interconnectés.**
- **Il est nécessaire d'avoir une politique stricte de la gestion des informations disponibles sur la société.**
  - Cela permet d'éviter les actions de renseignements comme les actes préparatoires.
- **Souscription de contrat d'assurance réaliste portant sur des attaques vraisemblables.**
  - Analogie avec une serrure 3 points qui permet seulement de garantir un laps de temps (quelques dizaines de secondes) avant que la serrure puisse être ouverte. De la même façon, il est possible de compartimenter les réseaux afin de garantir une meilleure sécurité.

L'opération « Carbone 14 »

Merci

Serge LEFRANC

Ingénieur de l'armement

serge.lefranc@dga.defense.gouv.fr

David BENICHOU

Magistrat

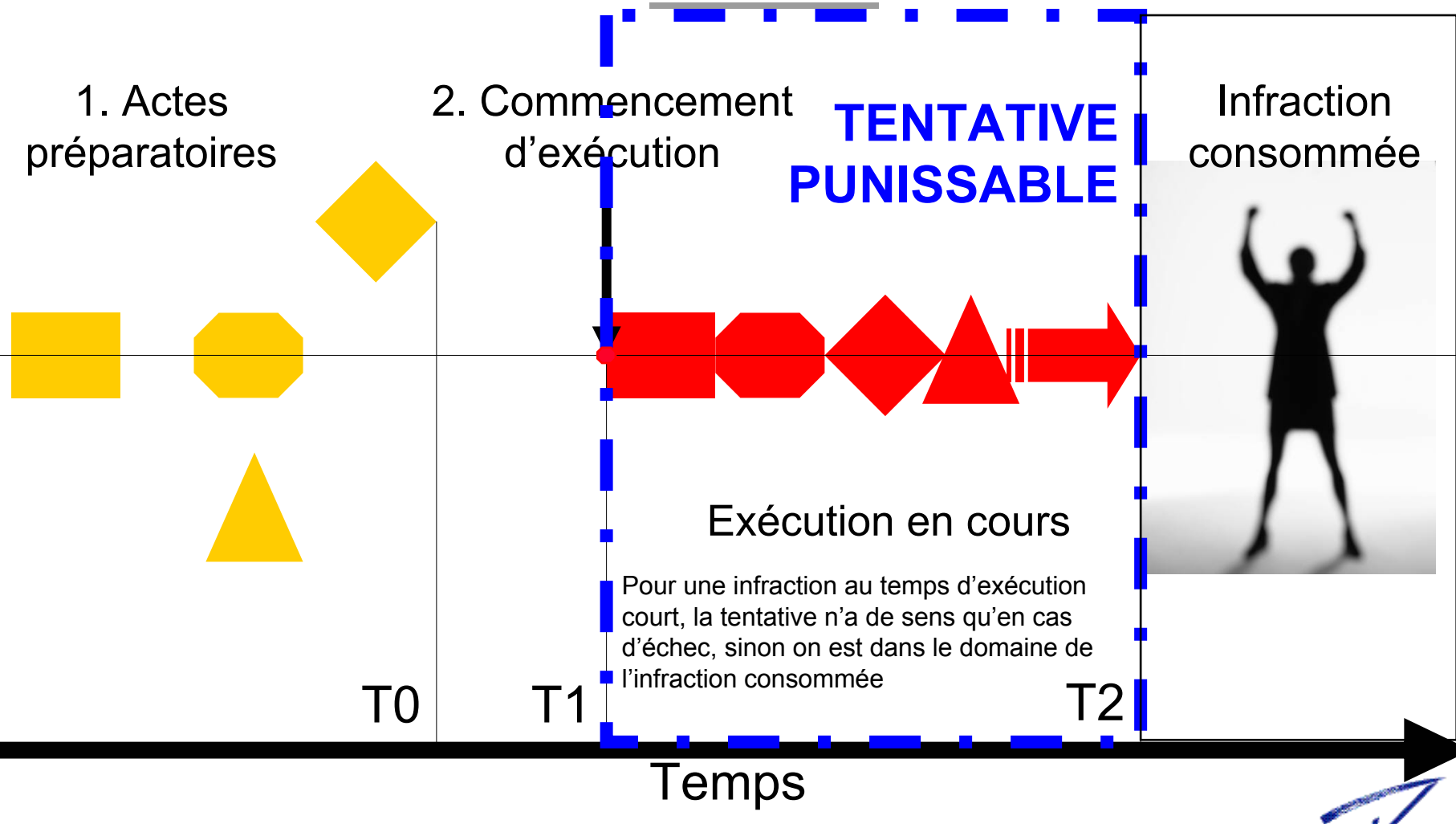
David.Benichou@justice.fr

MINISTÈRE DE LA DÉFENSE

DGA

L'opération « Carbone 14 »

Fonctionnement de la tentative



Balayer n'est pas fauter !

Si un balayage de port a eu lieu entre T1 et T2, cela peut caractériser, non sans ambiguïté (tout dépend de l'outil utilisé pour le balayage, simple scanner ou outil d'attaque ?).

- 1. une prise d'information en vue d'un accès légitime.
- 2. un acte préparatoire en vue d'une intrusion.
- 3. ou une tentative ayant manqué son effet.

retour

Définition de la tentative

- **art. 121- 5 du code pénal:**

La tentative est constituée dès lors que manifestée par un commencement d'exécution, elle n'a été suspendue ou n'a manqué son effet qu'en raisons de circonstances indépendantes de la volonté de son auteur.

retour

Détention d'outils d'attaque: 323-3-1 CP

Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un ***programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues*** *par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.*

Les dispositions du présent article ne sont pas applicables lorsque l'importation, la détention, l'offre, la cession ou la mise à disposition de l'équipement, de l'instrument, du programme informatique ou de toute donnée n'est pas intentionnelle.

retour