

LIP6

La lutte contre les botnets Paris, 5 janvier 2012

Lieutenant-colonel Éric FREYSSINET
Chef de la division de lutte contre la cybercriminalité
Pôle judiciaire de la gendarmerie nationale, STRJD/DLCC



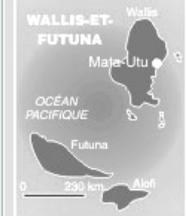


Carte administrative de la France

Collectivités d'outre-mer



POLYNÉSIE FRANÇAISE

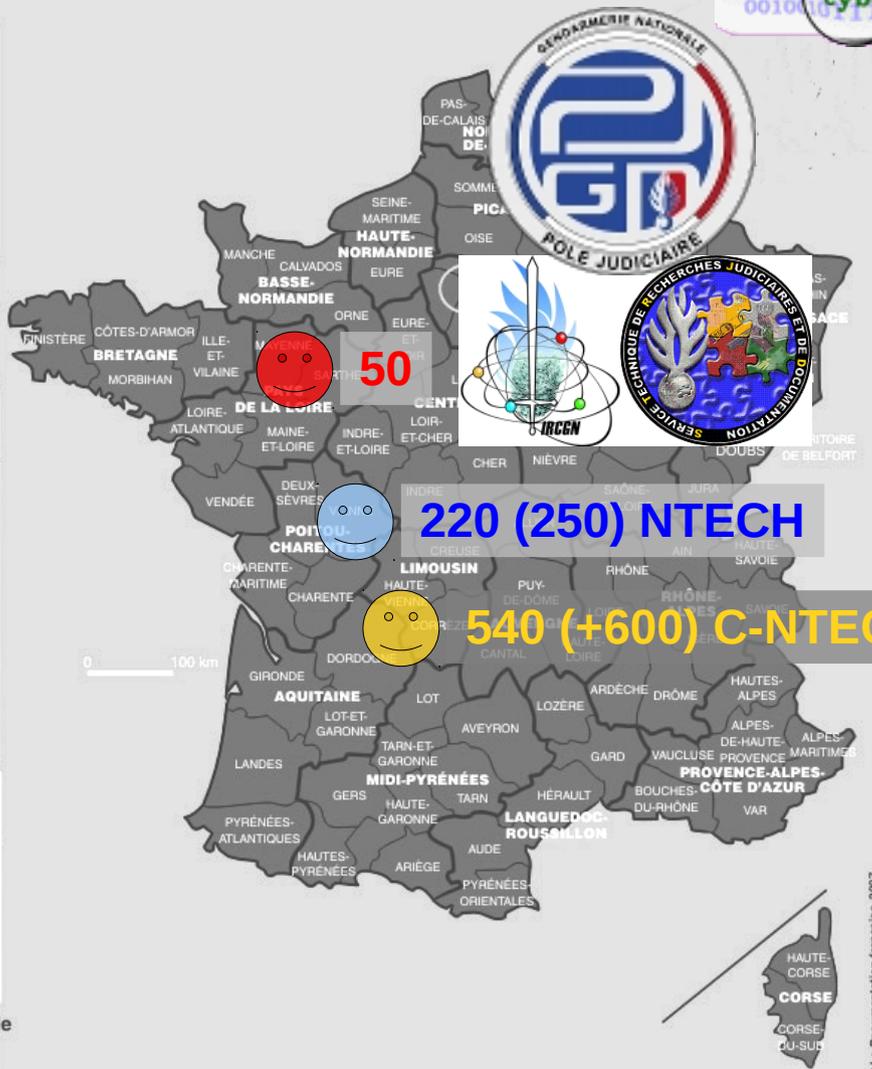


Nouvelle-Calédonie



Terres australes et antarctiques françaises

TAAF



Départements et régions d'outre-mer



Licence pro NTECH Master SSI

- Partenaires:
 - PN: OCLCTIC, BEFTI, DCRI
 - Douanes: SNDJ, DNRED
 - CNIL, HADOPI, ARJEL,...
- AFSIN: enquêteurs, experts, magistrats (www.afsin.org)
- Europe:
 - Services spécialisés
 - Europol, Interpol, Eurojust
 - ENFSI, ECTEG
- Francopol
- Académique, industrie :
 - 2CENTRE (UTT, UCD, UM...)
 - Projets ANR,...

© La Documentation Française, 2007



Division de lutte contre la cybercriminalité

- Première équipe constituée en 1998
- Aujourd'hui, 21 personnels:
 - Commandement
 - D2I: Département investigations Internet
 - RAMI: Département répression des atteintes aux mineurs
 - Centre national d'analyse des images de pédopornographie
 - Département soutien et appui
 - Guichet unique téléphonie et Internet



Quelques outils techniques pour la surveillance

- Surveillance des réseaux pair à pair
- Surveillance du Web
- Cyberpatrouille



Surveillance des réseaux P2P

- Logiciel développé actuellement par une association partenaire: Action Innocence



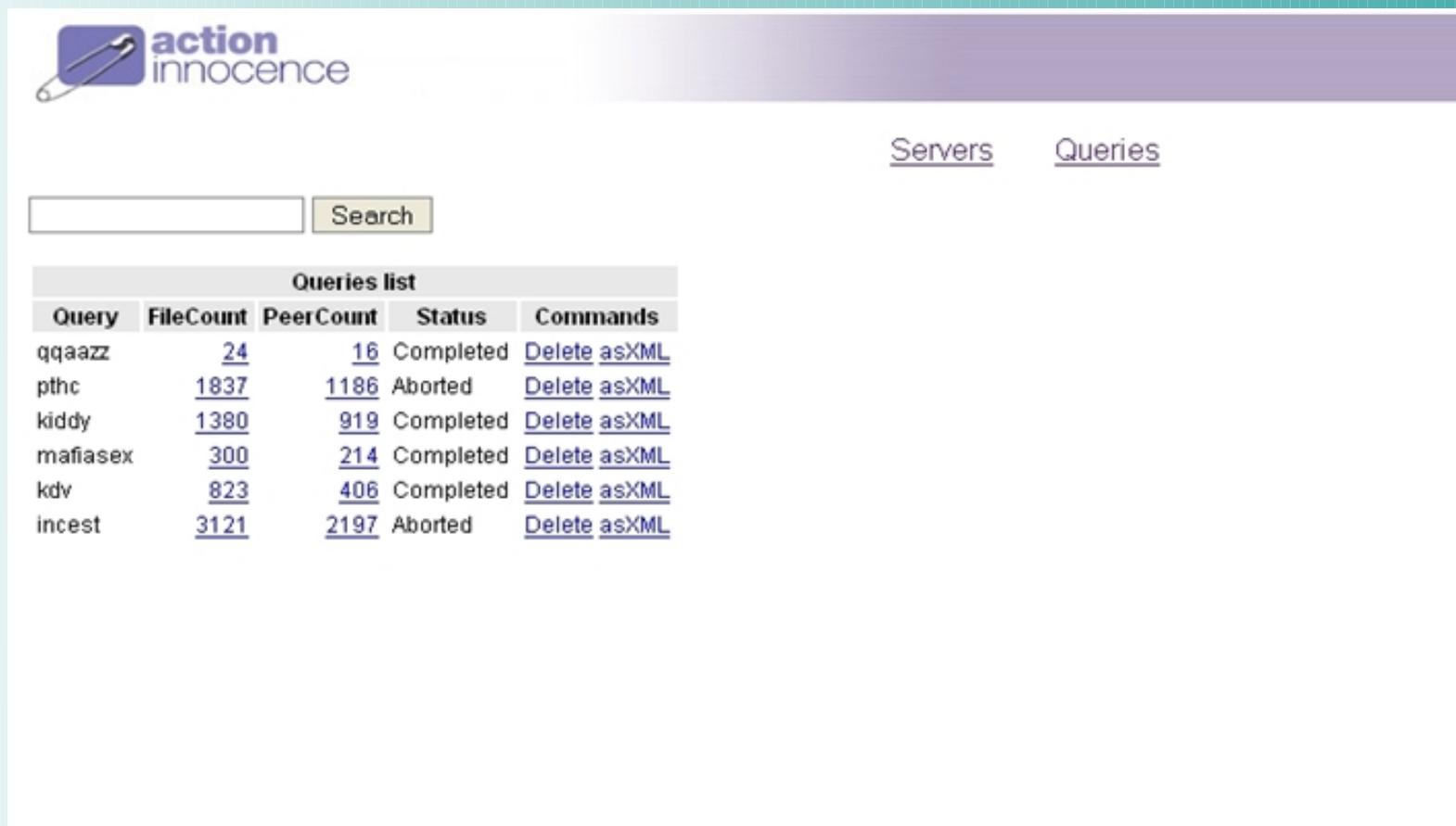
Servers Queries

Server Name	Country	UserCount	FileCount	References	Query	Command
!***HOT SEX***!		18957	5236231	82		
!+++ (Ifreesex.net >> check our servers info +++!		53063	5844111	67		
!+++ (Ifreesex.net >> Sex World wide for free +++!		18235	2080493	65		
!+++ (Fuck For Free) +++!		22577	5838546	77		
!. Much More Sex .!		9648	4290643	76		
!! Saugstube !!		63544	8271175	61		
!- www.FreeOsex.com =-!		43726	6658001	60		
!- www.FreeOsex.com =-!		68903	13248403	58		
!- www.FreeSexBay.com =-!		51145	10880165	57		
!- www.FreeSexBay.com =-!		31845	5322416	61		
!- www.FreeSexBay.com =-! Behemoth		21665	3220227	57		
# eMule Serverlist Nr.1 #		50283	7319373	61		
###BIG KAJUNA###		13439	0	53		
++ FILE FacTORY ++		112906	12871395	32		
-= SexMachine =-		6149	2651988	51		



Surveillance des réseaux P2P (suite)

- 1^{ère} étape: Recherches par mots clés



The screenshot shows the 'action innocence' web interface. At the top left is the logo, which consists of a paperclip icon and the text 'action innocence'. To the right of the logo are two tabs: 'Servers' and 'Queries'. Below the tabs is a search bar with a 'Search' button. Underneath the search bar is a table titled 'Queries list'.

Query	FileCount	PeerCount	Status	Commands
qqaazz	<u>24</u>	<u>16</u>	Completed	Delete asXML
pthc	<u>1837</u>	<u>1186</u>	Aborted	Delete asXML
kiddy	<u>1380</u>	<u>919</u>	Completed	Delete asXML
mafiasex	<u>300</u>	<u>214</u>	Completed	Delete asXML
kdv	<u>823</u>	<u>406</u>	Completed	Delete asXML
incest	<u>3121</u>	<u>2197</u>	Aborted	Delete asXML

Surveillance des réseaux P2P (suite)

- 2^{ème} étape: sélection des résultats nationaux

[Servers](#) [Queries](#)

Results for query 'kiddy' in france

Results by country						38 hosts				
Country	Total	1	2-4	5-9	>=10	IP:Port	Hostname	FileCount	Servers	
	919	633	203	45	38	86.71.1	203.6	61	1	
						90.144	d90-1	43	1	
						80.170	d80-1	33	1	
						83.205	ALyon	adoo.fr	32	1
						81.251	AMont	anadoo.fr	31	1
						84.5.9	84.5.9		28	1
						83.197	AAnne	adoo.fr	28	1
						82.66	bdy93		27	1
						87.231	FR-Lil		27	1
						81.56	Ins-vic	at	26	1
						83.157	dyn-8		25	1
						88.16	88.16		25	1
						83.197	AMont	wanadoo.fr	24	1
						84.7.8	84.7.8		24	1
						87.88	vil93-1		23	1
						81.57	dan75		22	1
						91.91	137.2		22	1
						85.68	abo-1		21	1
						82.224	par69		20	1
						82.254	Ins-bz	i.net	20	1
						84.100	235.2i		17	1
						82.226	lab75		16	1

Surveillance des réseaux P2P (suite)

- 3^{ème} étape: exploitation des résultats d'un

Peer results for query 'kiddy'

Results by country					
Country	Total	1	2-4	5-9	>=10
	919	633	203	45	38

Details of [REDACTED] 03:7229 Print version		
IP	86 [REDACTED]	
Hostname	20 [REDACTED].net	
Port	7229	
Country	france	
First contact	2007-01-03 08:42:22.110343+01:00	
Last contact	2007-01-03 08:43:56.874992+01:00	
Server	BiG BanG 1	
Files	Hash / Size	FileNames
	4eb2acb8d7de25869cc40874a2031219316075	• Little Preteen Boys 8Yo 7Yo Kissing Naked In Shower - Pedo Kdv Pjk Rbv Rizmaster R@Ygold Boys Preteens Kiddy.jpg
	7b5c8151312858362b7de6730f61448a50594	• Collection-Rape Lolita Kiddy Child Incest Xxx Porno Gay Fuck Young Naked Nude Little0156.jpg
	fdf5fa33dca9f19d13bdf32947f806612170454	• Collection2 Play Slave Illegal Preteen Underage Lolita Kiddy Child Incest Xxx Porno Gay Fuck Young Naked Nude Little Girl Cum Face.tif
	360416918c109b73b2b6efed103fcaea114859	• Collection-Rape lolita kiddy child incest xxx porno gay fuck young naked nude littleannette-016.jpg
	392b673aaef6f48fab3466a46ec8a8af38589	• Collection3- dick (illegal preteen underage lolita kiddy child incest xxx porno gay fuck young naked nude little girl 1.jpg
	8ab3486940363fb10ea4d5bf3d60169a46619	• Jeune Sex Fille Garçon Boy Real Teen Porn Illegal Preteen Underage Lolita Kiddy Incest Little Girl Rape Anal Cum Sex Lesbian Blow 064.jpg

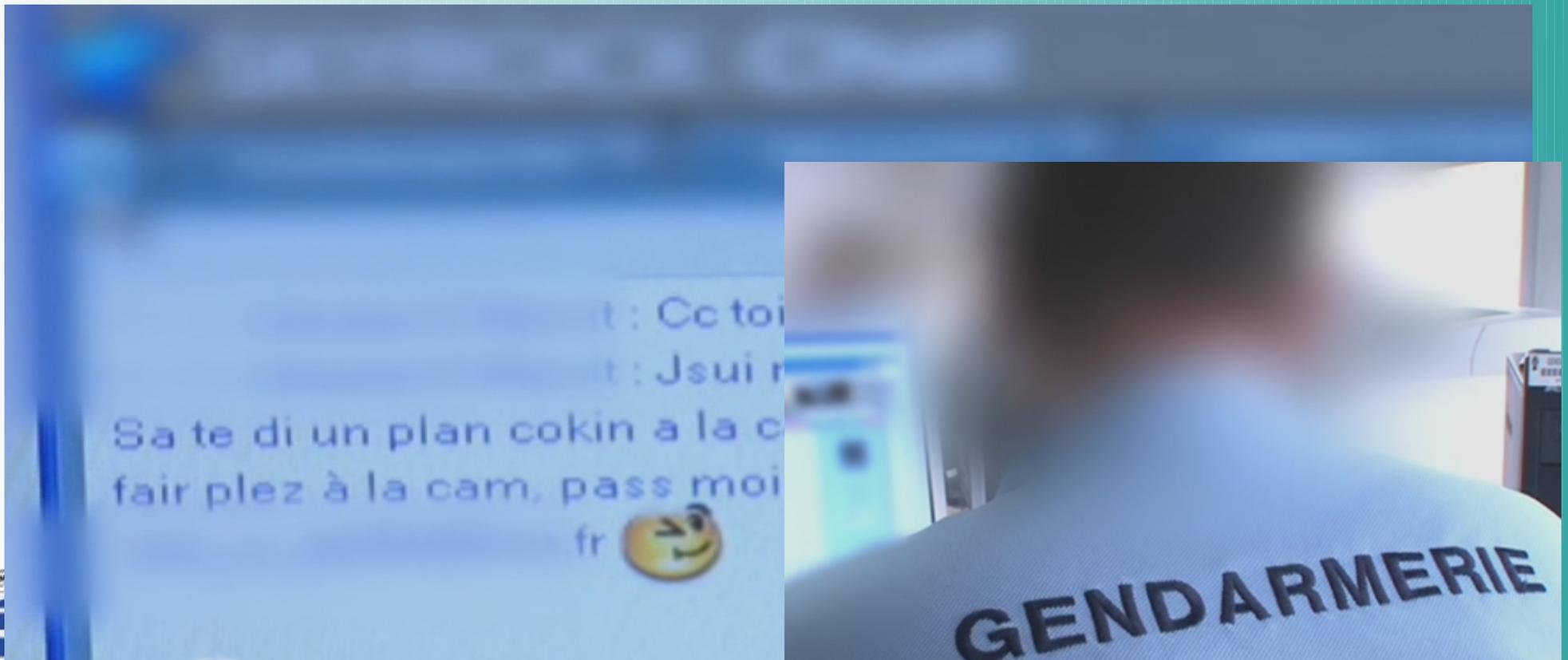
Surveillance Web

- Beaucoup de cette surveillance se fait encore manuellement, avec les moteurs de recherche
- AdvestiSearch nous permet d'automatiser certaines surveillances ciblées:
 - Recherche par mots clés qui permet d'obtenir un grand nombre de document
 - Puis, dans les résultats de la recherche, classification par comparaison avec des textes de référence ou des images de référence
 - Nous permet de détecter diffusion de contenus illicites



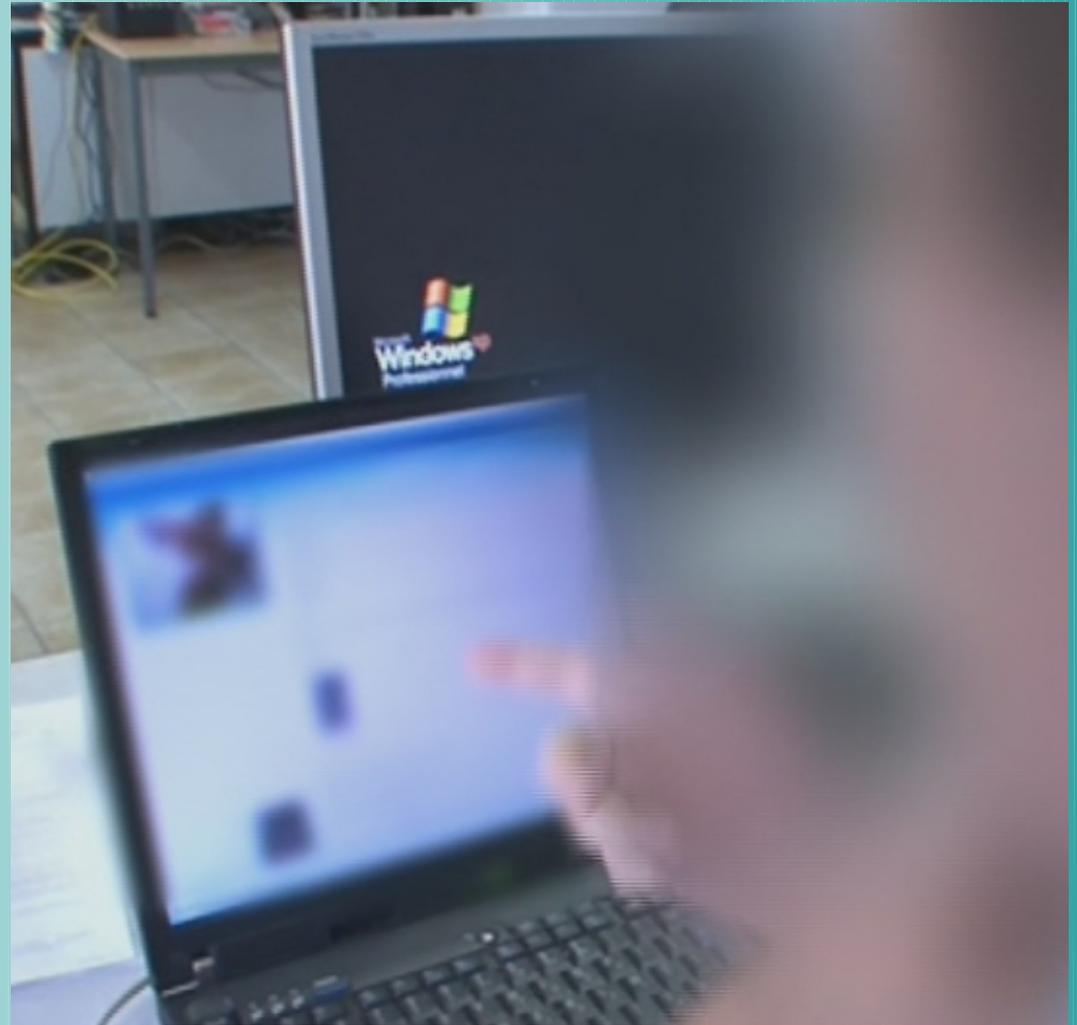
Cyberpatrouille

- Le gendarme se fait passer pour une enfant de 12 ans et se fait rapidement approcher



Cyberpatrouille (suite)

- Parfois le suspect va vouloir s'exhiber devant celle qu'il croit être une très jeune fille
- Ou d'autres fois il va proposer une rencontre physique



Institut de recherche criminelle de la gendarmerie nationale



- Division criminalistique physique-chimie
- Division criminalistique identification humaine
- Division criminalistique ingénierie et numérique
 - Département informatique-électronique
 - Département signal-image-parole
 - Département véhicules
 - Département documents



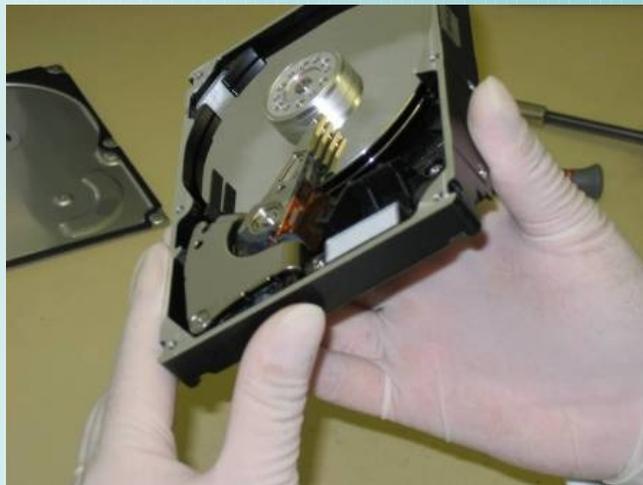
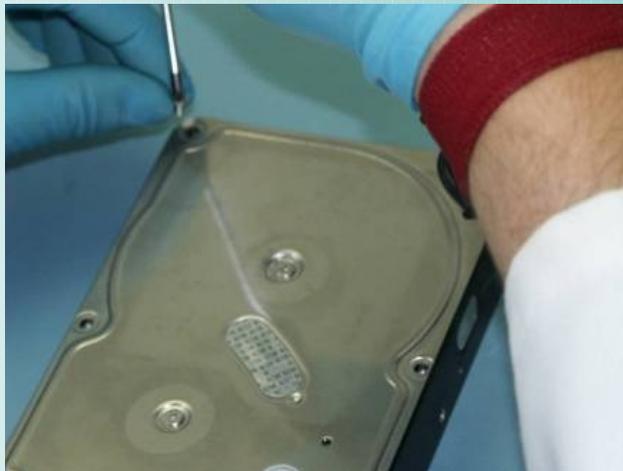
Département informatique- électronique

- Créé en 1992
- Quatre unités d'expertise:
 - Extraction de données numériques (*)
 - Réseaux et télécommunications
 - Traitement de l'information
 - Soutien opérationnel
- (*) Tous les supports de données arrivent d'abord dans l'unité d'extraction de données



Extraction de données

- Réparation de supports endommagés



Extraction de données (suite)

- Séchage



- Nettoyage (ultra-sons)



Extraction de données (suite)

- Dessoudage de composants mémoire



- Puis lecture, décodage, etc.



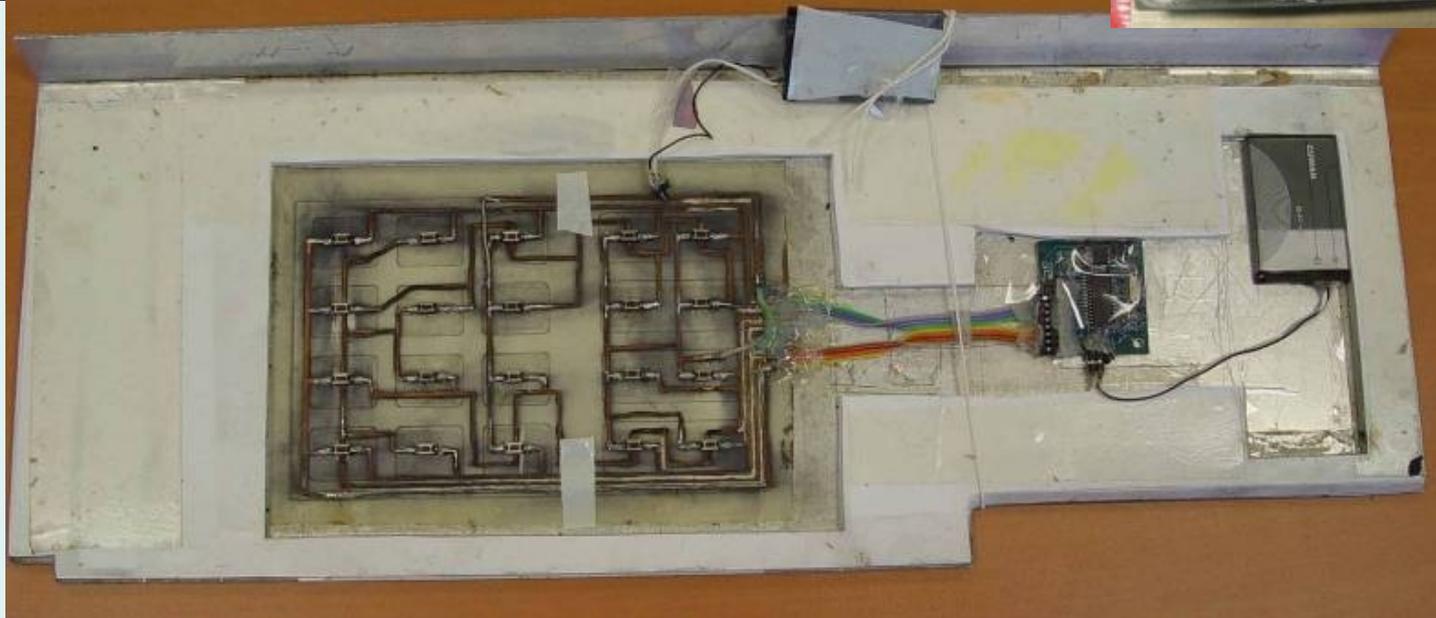
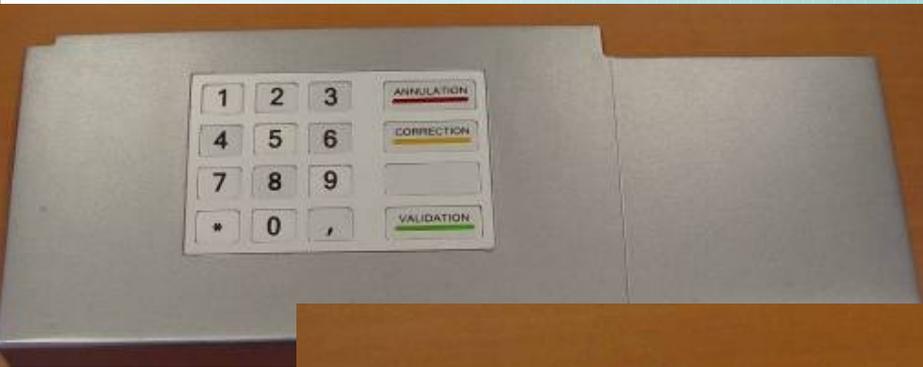
Autres domaines

- Outils classiques pour la téléphonie GSM



Autres domaines

- Skimming



Réseaux et télécommunications

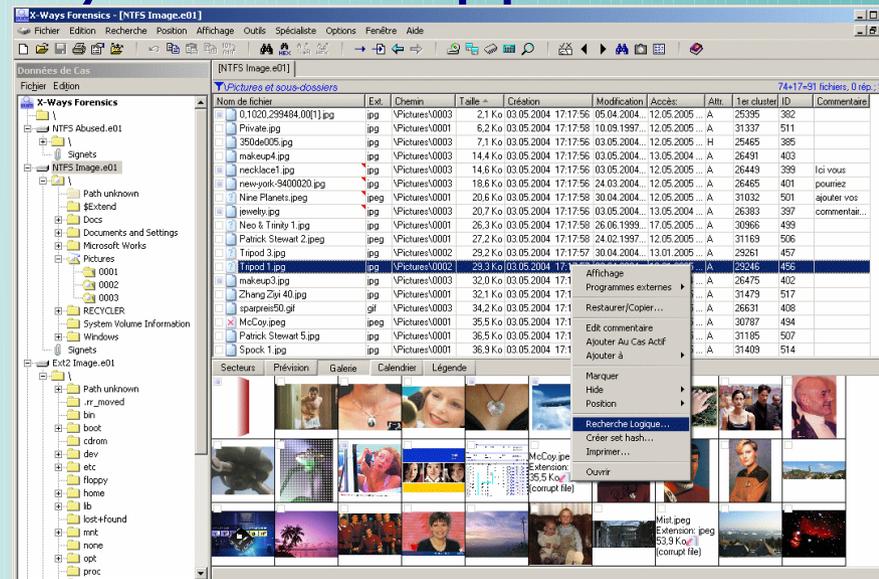
- Aide aux enquêtes sur Internet
- Expertise de systèmes informatiques « piratés »
- Interprétation de résultats d'interception
- Mesures sur les réseaux de téléphonie mobile, réseaux Wifi



Traitement de l'information

- Outils d'analyse des supports

- X-Ways



- Encase (Guidance Software)



- FTK

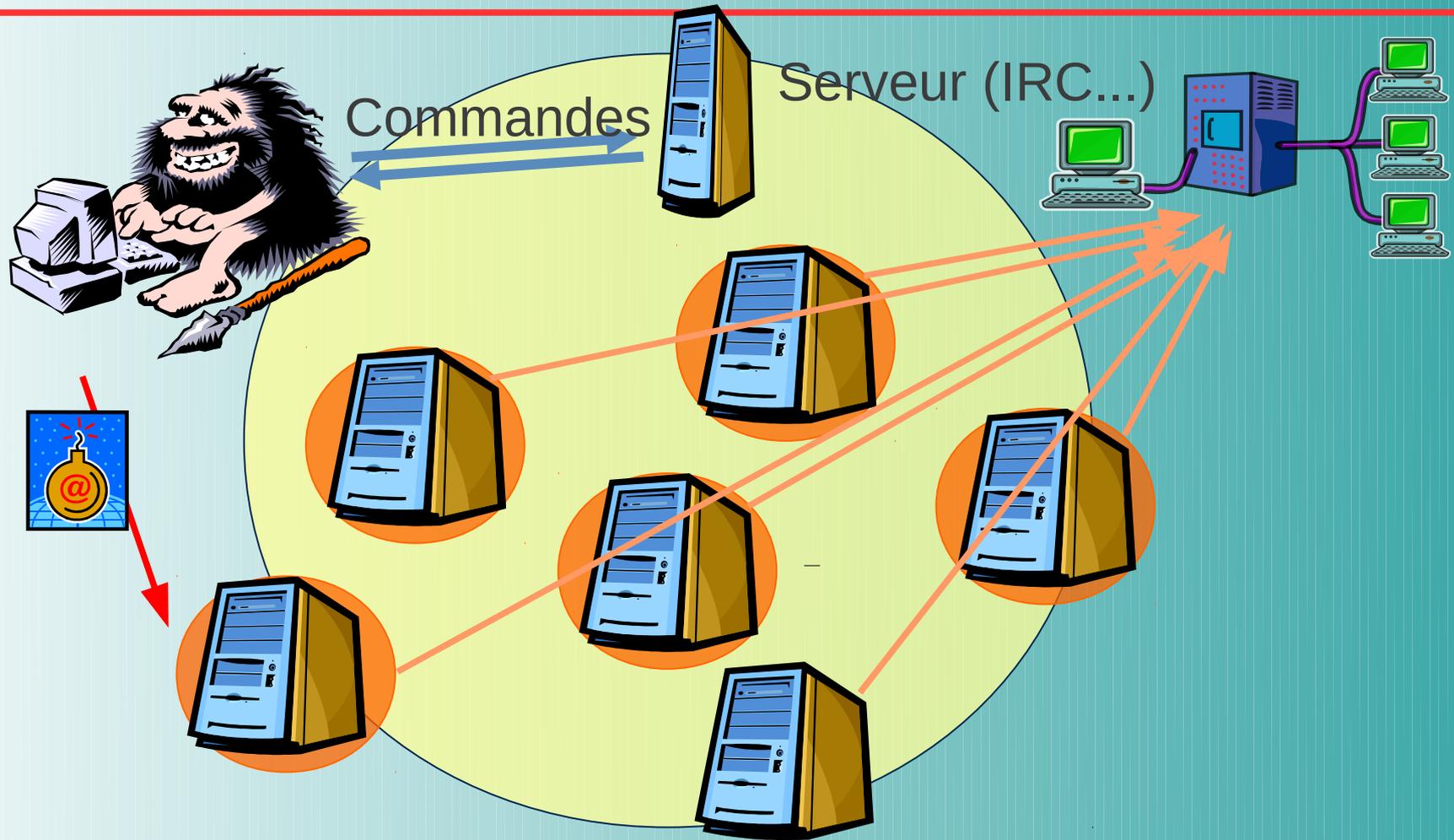


- BlackBag (Mac OS)



Botnet

Victime



Objectif de la thèse

- Décrire une technique de lutte adaptée
 - Comparaison des méthodes employées
 - Test de certaines approches ou expérimentation de certaines étapes
 - Description d'une méthode / de méthodes / d'outils techniques et juridiques utilisables



Première partie

- Mieux connaître les botnets
 - Décrire et documenter, proposer une taxonomie
 - Lancement d'un wiki <https://www.botnets.fr/>
 - Ainsi que les sources d'information et les publications existantes




BOTNETWIKI

Page [Discussion](#) Lire [Voir l](#)

Accueil

Si vous souhaitez contribuer à ce wiki, vous pouvez contacter les chercheurs académiques et indépendants travaillant sur [l'aide spécifique à ce wiki](#).

Language [en]

Although the main language of this Wiki is configured to be French, if you wish to contribute to this wiki, you can have a look at the [terms of use](#) and the work of independent researchers working on **botnets**.

Note: You can switch between French and English interface. If the interface is available in another language, you can also click the [language](#) button.

Accès direct

- [Publications référencées](#)
- [Botnets documentés](#)
- [Logiciels malveillants documentés](#)

Première partie (suite)

- Comprendre le fonctionnement intime des botnets
 - Analyse de malware
 - Analyse de protocoles de commande et de systèmes de commande



Deuxième partie

- Analyse critique des méthodes de lutte existant aujourd'hui
 - Celles qui ont été testées
 - Celles qui sont encore expérimentales
- Quelques exemples ...



Cas Bredolab

Sécurité : avis de tempête Bredolab en Europe

16/07/2009 14:00 par Jérôme G. | 2 commentaire(s) 2 nouveau(x) |    | Partager sur :    

Catégories : Sécurité, Malware

ESET émet une alerte suite à la propagation rapide du cheval de Troie Bredolab dans sa variante AA en Europe. Sous Windows, le troyen exploite une vulnérabilité dans les applications Adobe.

De nouveaux chevaux de Troie font régulièrement leur apparition pour un type de logo_eset malware qui a coutume d'être le plus représenté dans les classements mensuels établis par les sociétés de sécurité. **ESET** pointe aujourd'hui du doigt une menace qui se répand très rapidement, et notamment en Europe.

Selon l'analyse du système ThreatSense.Net de ESET, le **cheval de Troie** baptisé **Bredolab** est déjà la menace la plus fréquemment rencontrée en République Tchèque et en Slovaquie, et dans le Top 5 des menaces en Autriche, Pologne, Turquie. Sa présence est aussi très marquée en Bulgarie, Grande-Bretagne, Allemagne, Suède ou encore Belgique, et la France commence à être contaminée.

Bredolab dans sa variante AA apparemment la plus active, possède la faculté de se copier dans le système de fichiers pour s'exécuter à chaque redémarrage d'une machine Windows. Sa mission est alors d'établir une connexion HTTP avec un serveur distant pour rapatrier d'autres nuisibles.

Diffusé via Internet, Bredolab tire parti pour son infection d'une faille dans les applications **Adobe**. ESET cite ainsi des fichiers .PDF et .SWF spécialement conçus. Ce constat peut paraître étonnant car Adobe ne fait nullement mention pour le moment d'une quelconque exploitation ciblant les utilisateurs de ses

<http://www.youtube.com/watch?v=tWHp8pwif8Y>



Cas Mariposa en Espagne

ELMUNDO edición impresa | Multimedia | Blogs | Especiales | Hemeroteca

ELMUNDO.es | Navegante Tecnología
Líder mundial en español | Miércoles 03/03/2010. Actualizado 12:33h.

Portada España Mundo Europa Opinión Deportes Economía Cultura Toros Ciencia Salud Tec

Edición ESPAÑA Madrid Barcelona Baleares C. Valenciana Castilla y León País Vasco Andalucía

0 50

Twitter J'aime

Enviar a un amigo
 Valorar
 Imprimir
 En tu móvil
 Compartir

SEGURIDAD | Tres españoles detenidos

La Guardia Civil desmantela una red de 12,7 millones de 'ordenadores zombis'

- La red de ordenadores infectados fue desactivada el pasado 23 de diciembre
- Hay tres personas detenidas



Rustock

Belle victoire de Microsoft contre le spam

7 avis

Pierric.Marissal le lundi 21 mars 2011 à 11:47:39



La division anti-criminalité numérique de Microsoft, et quelques partenaires comme Trustworthy Computing ou l'Université de Washington, ont démantelé un vaste réseau de botnets spécialisé dans le spam, nommé Rustock. Derrière ce nom un peu barbare se cache un parc de pas moins d'un million de PC infectés et dédiés à l'envoi de pourriels.

Une opération conjointe s'est déroulée aux Etats-Unis, aux Pays Bas et en Chine. Les hébergeurs ont été identifiés, tous les serveurs stoppés. D'après Microsoft, l'opération est une réussite, « efficace à 100% ». Les

responsables sont en revanche en fuite.

Un monument historique du spam

Pour se rendre compte de l'ampleur de la victoire, il faut savoir qu'un PC infecté peut envoyer 25000 mails par

ECO (Allemagne)

- <http://www.botfrei.de/>



Anti-Botnet
Beratungszentrum

1. INFORMER 2. NETTOYER 3. PRÉSERVER

eco Bundesamt für Sicherheit in der Informationstechnik

Bienvenue !

Au sujet du projet
Les participants au projet
Contact

Bienvenue au Centre de conseil anti-Botnet, un service de l'association de l'économie internet allemande eco qui bénéficie du soutien de l'Office fédéral de la sécurité des technologies de l'informationn (BSI).

Sources d'information privées

- Énormément de sources d'information potentielles (cf. article SSTIC 2010)
 - Sociétés antivirus
 - Groupes de travail sur la sécurité
 - Collecte de données pour d'autres raisons (phishing, spam, vulnérabilités,...)



Questions ?

Lieutenant-colonel Eric Freyssinet

PJGN/STRJD/DLCC

1 bld Théophile Sueur, 93111 ROSNY SOUS BOIS Cedex

eric.freyssinet@gendarmerie.interieur.gouv.fr

+33 1 58 66 54 13 – judiciaire@gendarmerie.interieur.gouv.fr

<http://blog.crimenumerique.fr/>

@ericfreyss

