La cybersécurité

Attaques
Défense et
menaces

Quelques métiers de la sécurité

- Ingénieur cybersécurité
- Pentester
- Red Team
- Analyste SOC/CERT/CSIRT
- Blue Team
- CTI/OSINT/Threat hunting
- Analyste en code malveillant
- Architecte sécurité
- Développeur de solutions de sécurité
- RSSI

Généralités

La sécurité des systèmes informatiques

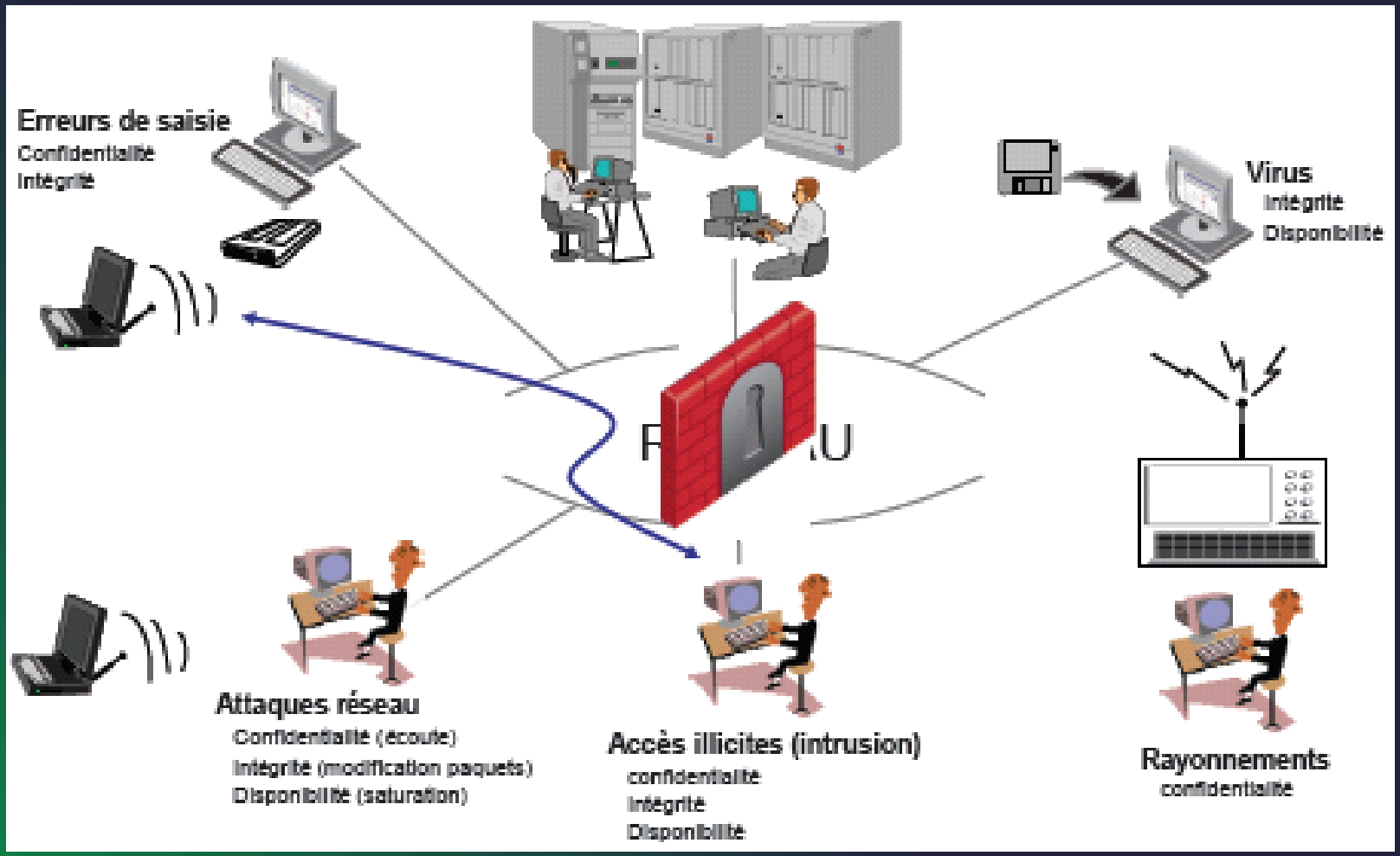
Les systèmes informatiques sont au cœur des systèmes d´information.

Ils sont devenus la cible de ceux qui convoitent l’information.

Assurer la sécurité de l’information implique d’assurer la sécurité des systèmes informatiques.

L'aspect sauvegarde est fondamental dans la sécurité.

La sécurité des systèmes informatiques



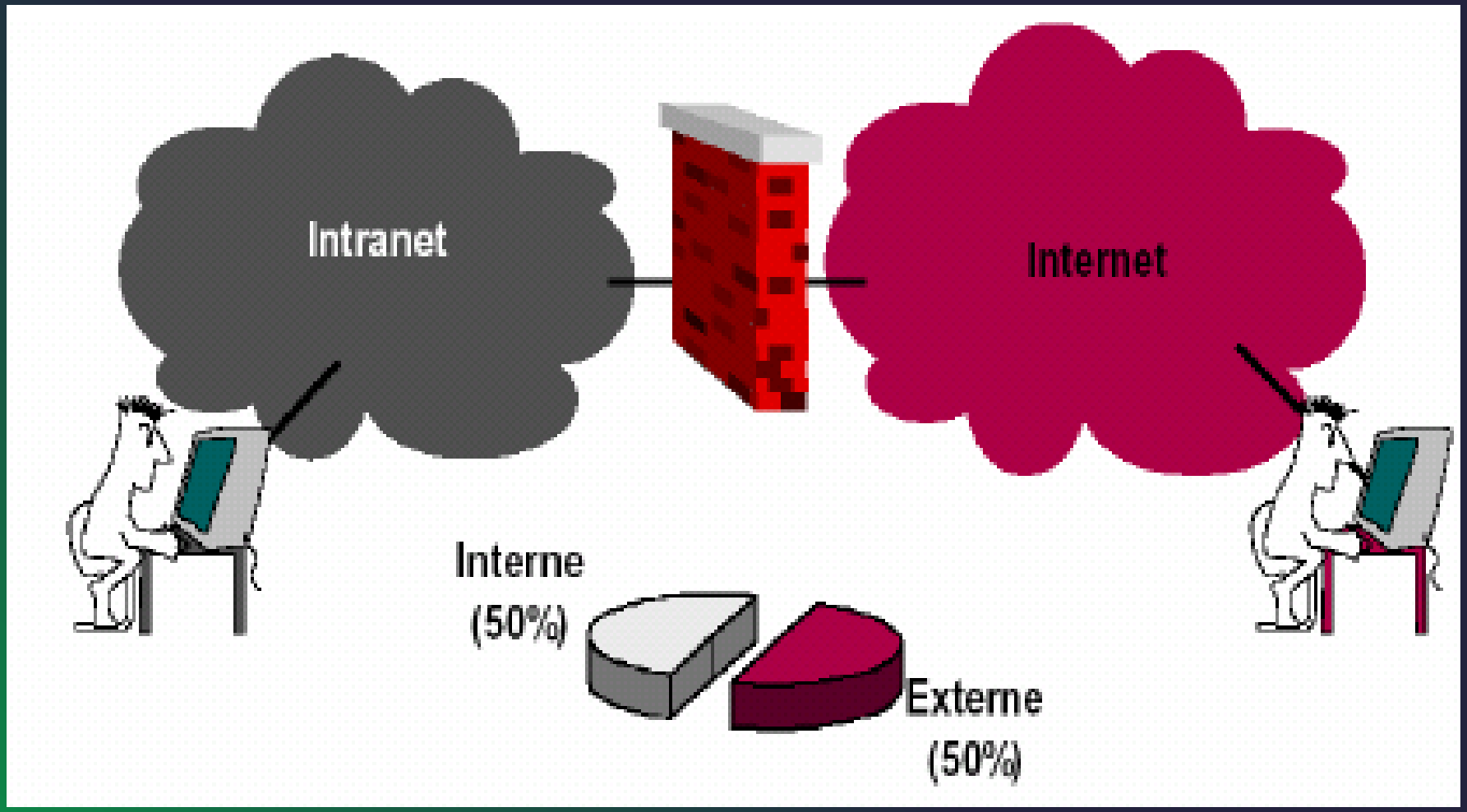
La sécurité des systèmes informatiques

- Rayonnement trouvés dans des câbles VGA (pas dans du HDMI)
- On parle également de rayonnement quand on utilise des claviers sans fil (diffusion sur une dizaine de mêtre touts les infos écrites)
- une attaque consiste à implanter un raspberry pi 0 dans un chargeur de téléphone, une fois le téléphone branché, le rapsberry va "attaquer" tous les wifi à proximité

- Il existe des clés USB(USB killer, remplie de condensateurs) qui peuvent une fois branchée, accumule de l'énergie et la redélivre afin de détruire l'équipement

- sonde x25 (protocole de couche 2 et 3) il est encore utilisé à l'armée et dans des distributeurs de billets / la sonde coûte 130ke

Origine des attaques



Objectifs de la sécurité informatique

Cinq principaux objectifs à garantir:

- intégrité
- confidentialité
- disponibilité
- non-répudiation
- authentification

Evolution des risques

- Croissance de l'Internet
- Croissance des attaques
- Failles des technologies
- Failles des configurations
- Failles des politiques de sécurité
- Changement de profil des pirates

Qui sont les pirates ?

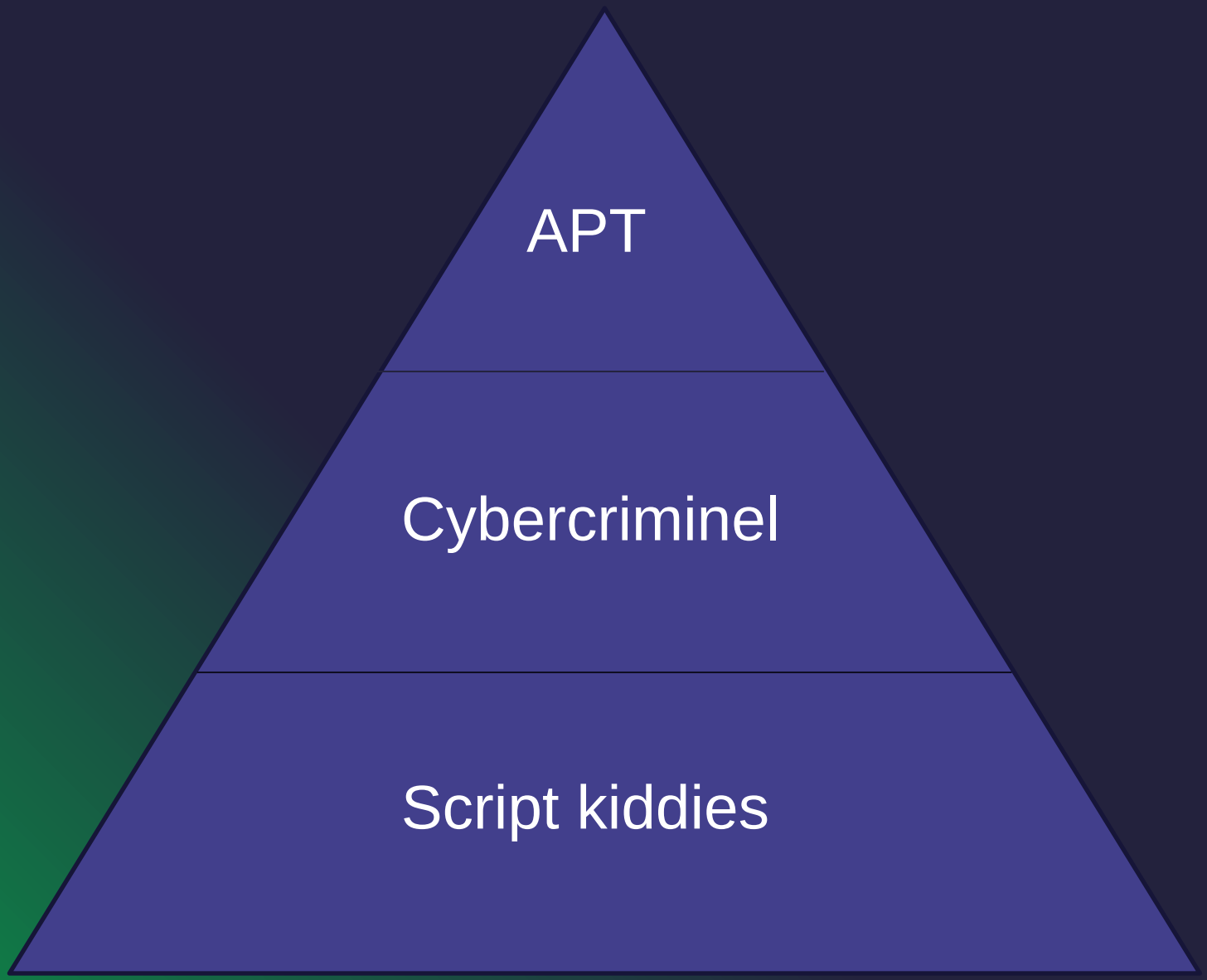
- Peut être n'importe qui avec l'évolution et la vulgarisation des connaissances.

- Beaucoup d'outils sont disponibles sur Internet.

- Vocabulaire:
  - "script kiddies"
  - "hacktiviste« (anonymous)
  - "hackers"
    - white hats, grey hats, black hats,

https://threatmap.checkpoint.com/
https://andreacristaldi.github.io/APTmap/

Qui sont les pirates ?



Phénomènes techniques

- Explosion de la technologie des transferts de données.

- Grande complexité des architectures de systèmes.

- Ouverture (pas toujours maîtrisée) des réseaux de communication

Phénomènes organisationnels

- Besoin de plus en plus d'informations(Big data, GAFAM)
- Grande diversité dans la nature des informations:
  - données financières
  - données techniques
  - données médicales
  - ...
- Ces données constituent les biens de l'entreprise et peuvent être très convoitées.

Objectifs des attaques

- Désinformer
- Empêcher l'accès à une ressource
- Prendre le contrôle d'une ressource
- Récupérer de l'information présente sur le système
- Utiliser le système compromis pour rebondir
- Constituer un réseau de « botnet » (ou réseau de machines zombies)

Les « botnets »

- La notion de botnet date des premiers réseaux irc (début des années 1990).
- Réseau de machines contrôlées par un « botmaster ».
- Contrôlé par:
  - Serveurs irc
  - Serveurs web
  - Requêtes DNS
  - Messageries instantanées
  - Peer to Peer
  - (Process Zombies)

Les « botnets »

- Un botnet peut être utilisé pour:
  - Envoyer du spam
  - Vol d'informations sensibles (avec un keylogger par exemple).
  - Installer des spywares.
  - Paralyser un réseau en déni de services
  - Installer un site web malicieux (phishing)
  - Truquer les statistiques de sites webs (sondage en lignes authentifiés par des adresses IP,
  - rémunération sur des clics de bannières,...)
  - ...

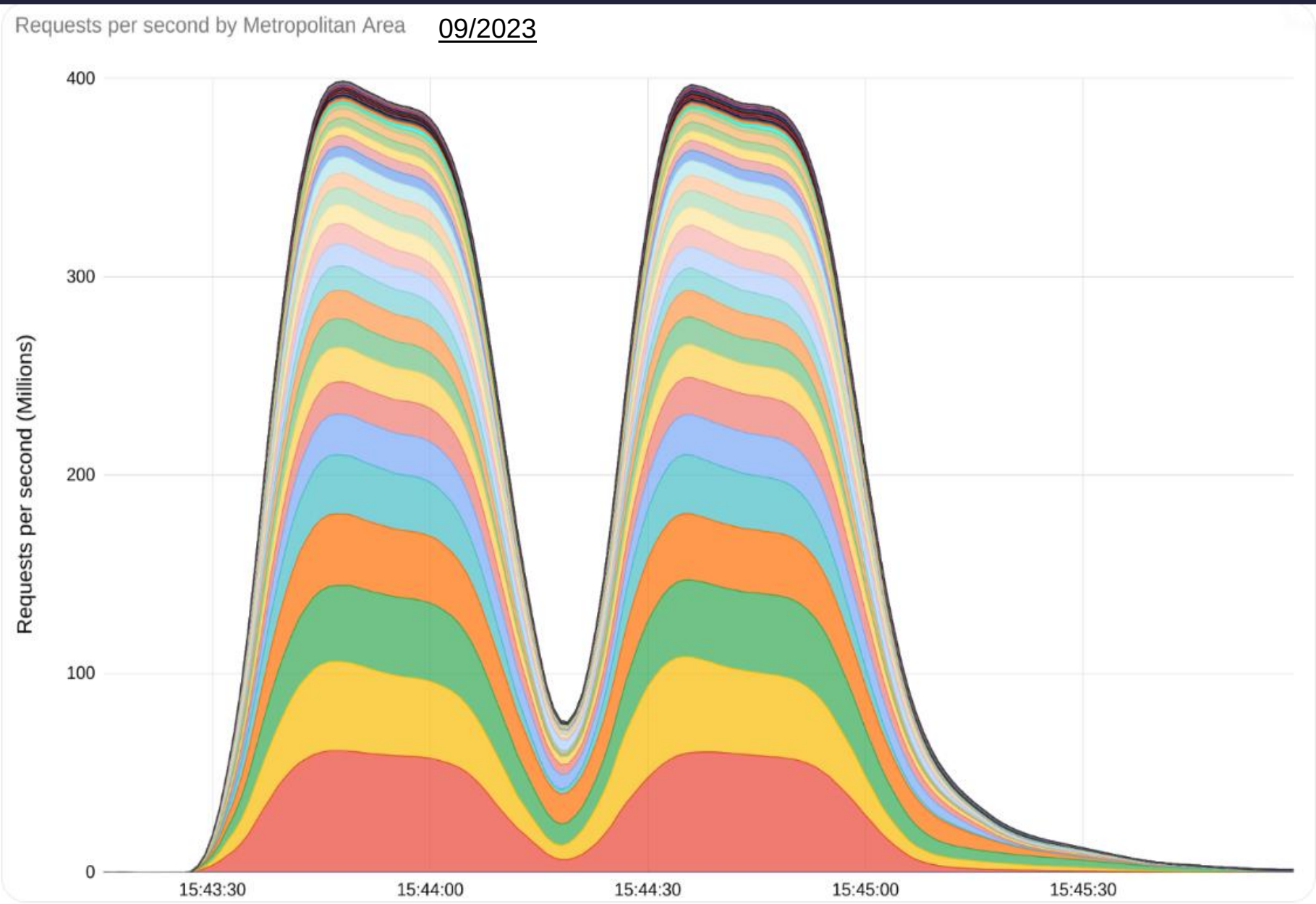
Les « botnets »

Estimation: une machine sur quatre fait partie d’un botnet.

En 2007 est apparu le plus grand botnet jamais enregistré « Zeus », Zeus(Zbot) c’est :

- 13 millions de machines infectées
- Impact financier estimé à 120 millions$
- 196 pays touchés

Les « botnets »


Requests per second by Metropolitan Area
09/2023
Requests per second (Millions)
400
300
200
100
0
15:43:30
15:44:00
15:44:30
15:45:00
15:45:30

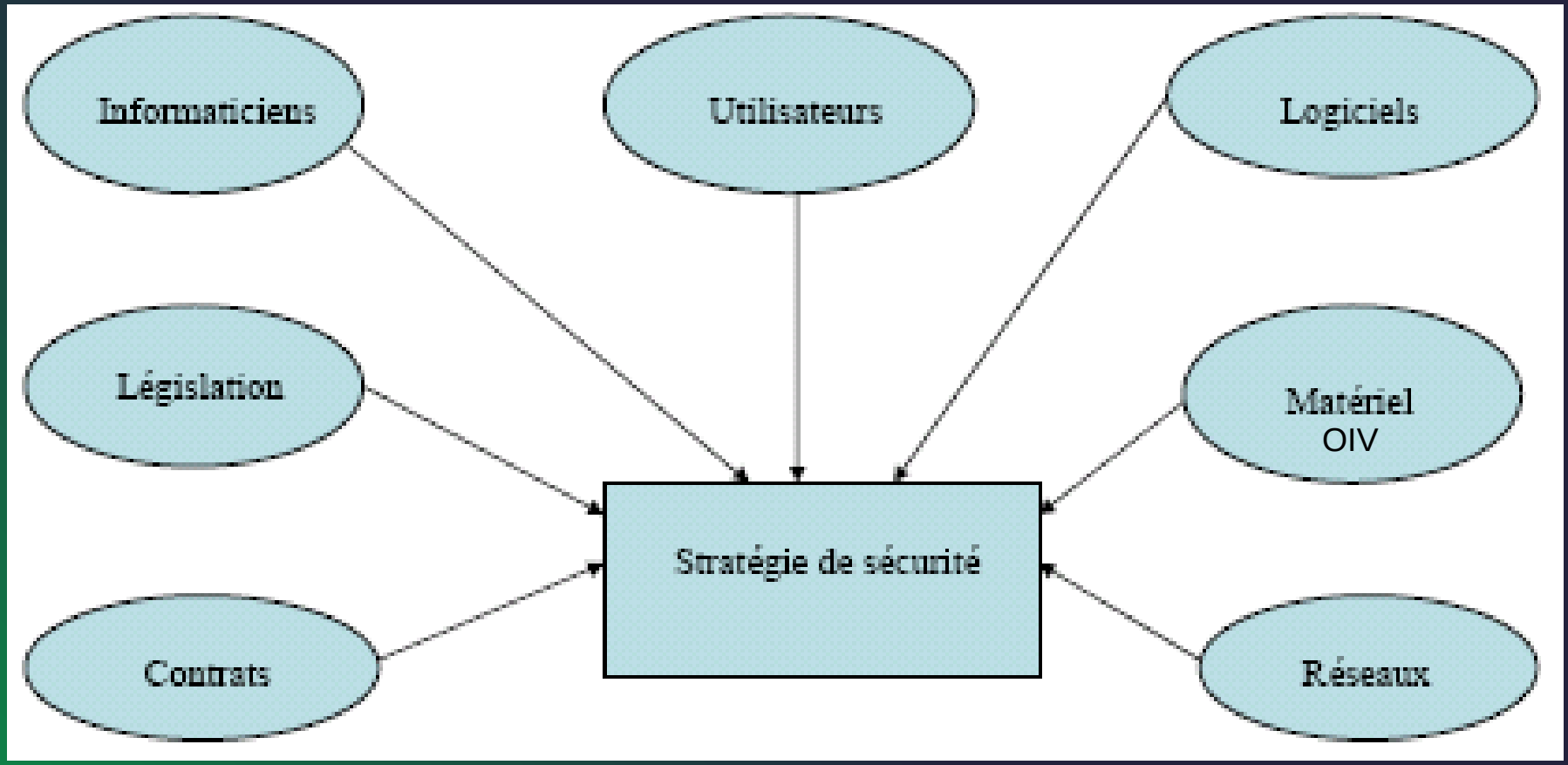
Motivations des attaques

- Vol d’informations (Espionnage industriel)
- Cupidité (Lazarus…)
- Modifications d’informations(scolaire)
- Vengeance/rancune
- Politique/religion
- Défis intellectuels

Cible des pirates

- Les états
- Serveurs militaires
- Banques
- Universités
- Tout le monde

La sécurité : une nécessité



Niveaux de sécurisation

- Sensibilisation des utilisateurs aux problèmes de sécurité.
- Sécurisation des données, des applications, des systèmes d'exploitation.
- Sécurisation des télécommunications.
- Sécurisation physiques du matériel et des accès.

En bref, la **défense en profondeur**

Politique de sécurité

- Compromis sécurité - fonctionnalité.
- Identifier les risques et leurs conséquences.(AMDEC,EBIOS,MEHARI)
- Elaborer des règles et des procédures à mettre en oeuvre pour les risques identifiés.
- Surveillance et veille technologique sur les vulnérabilités découvertes.(CVE,NIST,Mitre ATTACK)
- Actions à entreprendre et personnes à contacter en cas de détection d'un problème.

Mise en place d'une politique de sécurité

- Audit/Pentest (Web,applicatif,code...)

>Lors d'un audit , la note finale retenue sera toujours la note la plus basse obtenue lors de l'audit

- Détection d'incidents(CERT/CSIRT)

>Y compris les failles 0d

- Réactions(CERT/CSIRT)

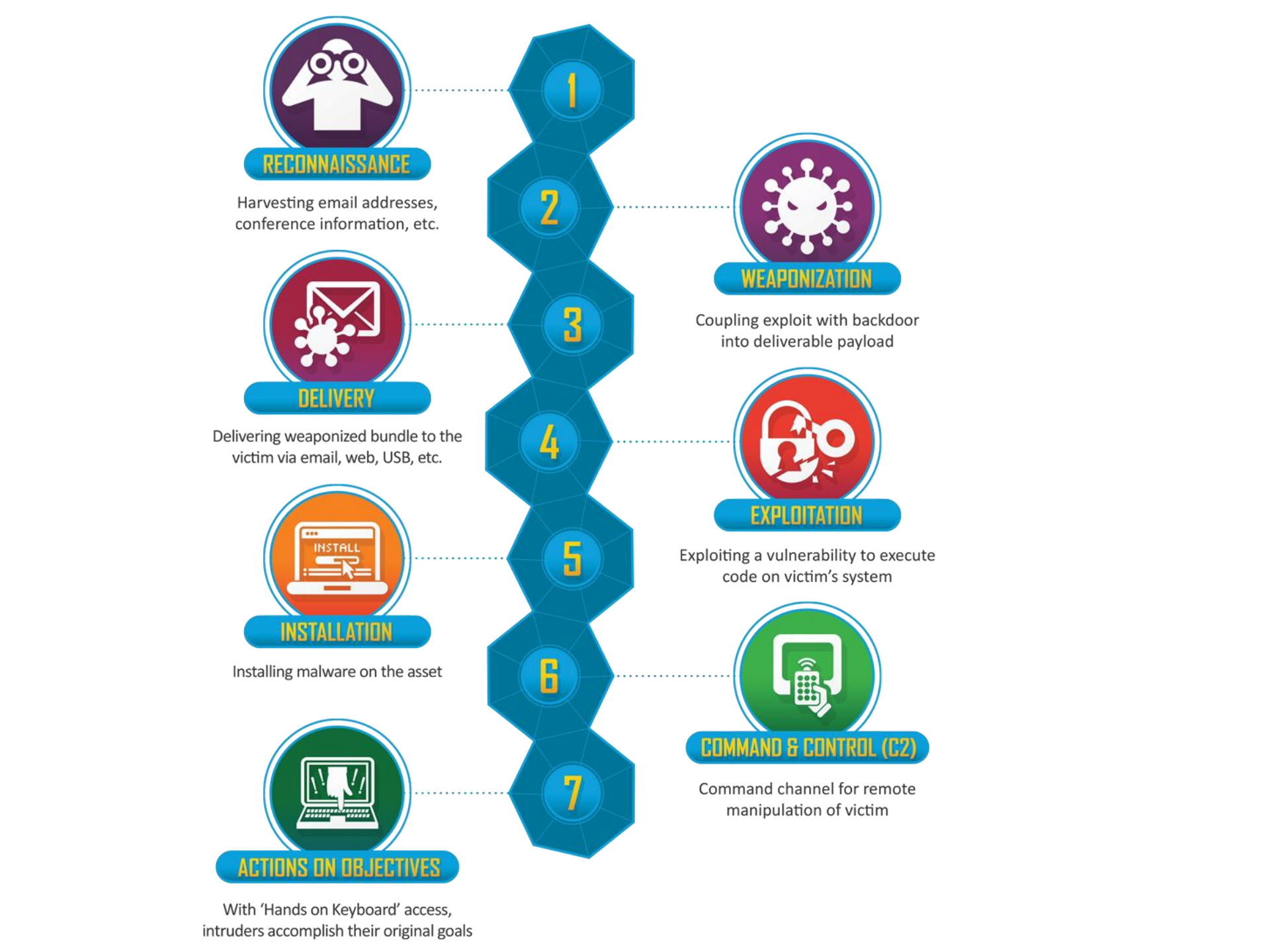
>SOC, Blue Team

- Restauration(PCA/PRA)

Les menaces

Techniques d'attaques

- Social Engineering
- MICE (Money, Ideology, Compromise, Ego)
- Dumpster diving
- Shoulder surfing
- Sniffing
- Scannings
- etc.


1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

Exemple de social engineering

Kevin Mitnick

- 3 livres, 1 film (Cybertraque).
- Piratage des réseaux téléphoniques.
- Attaque des machines de Tsumotu Shimomura au San Diego Supercomputing Center.
- 5 ans de prison et sous interdiction d'utiliser des ordinateurs.

U.S. Department of Justice
United States Marshals Service

WANTED
BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).
United States Marshals Service NCIC entry number: (NIC/ W21460021).

NAME: .....MITNICK, KEVIN DAVID
AKS (S): .....MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

DESCRIPTION:
Sex: .....MALE
Race: .....WHITE
Place of Birth: .....VAN NUYS, CALIFORNIA
Date(s) of Birth: 08/06/63; 10/18/70
Height: .....5'11"
Weight: 190
Eyes: .....BLUE
Hair: .....BROWN
Skintone: .....LIGHT
Scars, Marks, Tattoos: .....NONE KNOWN
Social Security Number (s): 550-39-5695
NCIC Fingerprint Classification: ...DOPM20PM13DIPM19PM09

ADDRESS AND LOCALE: KNOWN TO RESIDE IN THE SAN FERNANDO VALLEY AREA OF CALIFORNIA AND LAS VEGAS, NEVADA

WANTED FOR: VIOLATION OF SUPERVISED RELEASE
ORIGINAL CHARGES: POSSESSION UNAUTHORIZED ACCESS DEVICE; COMPUTER FRAUD
Warrant Issued: CENTRAL DISTRICT OF CALIFORNIA
Warrant Number: 9312-1112-0154-C

DATE WARRANT ISSUED: NOVEMBER 10, 1992

MISCELLANEOUS INFORMATION: SUBJECT SUFFERS FROM A WEIGHT PROBLEM AND MAY HAVE EXPERIENCED WEIGHT GAIN OR WEIGHT LOSS
VEHICLE/TAG INFORMATION: NONE KNOWN OFTEN USES PUBLIC TRANSPORTATION

If arrested or whereabouts known, notify the local United States Marshals Office, (Telephone: 213-894-2485).
If no answer, call United States Marshals Service Communications Center in McLean Virginia.
Telephone (800)336-0102; (24 hour telephone contact) NLETS access code is VAUSM0000.

PRIOR EDITIONS ARE OBSOLETE AND NOT TO BE USED

Form USM-132
(Rev. 3/2/92)

November 1992

Dissimulation d'informations

- L'information peut être dissimulée dans un but de protection (mot de passe, ...) ou dans des buts moins légaux.
- Différentes méthodes pour s'échanger de l'information de manière sûre:
  - chiffrement (symétrique(AES),Diffie hellman(RSA))
  - Stéganographie
- Tout n'est pas autorisé par la loi.(Chiffrement 2048 bits max)

Stéganographie

L'art de cacher l'information dans un autre média

Je suis très émue de vous dire que j'ai bien compris l'autre soir que vous aviez toujours une envie folle de me faire danser. Je garde le souvenir de votre baiser et je voudrais bien que ce soit la une preuve que je puisse être aimée par vous. Je suis prête a montrer mon affection toute desinteressee et sans calcul, et si vous voulez me voir aussi vous dévoiler sans artifice mon âme toute nue, venez me faire une visite. Nous causerons en amis, franchement. Je vous prouverai que je suis la femme sincère, capable de vous offrir l'affection la plus profonde comme la plus étroite en amitié, en un mot la meilleure preuve que vous puissiez rêver, puisque votre âme est libre. Pensez que la solitude où j'habite est bien longue, bien dure et souvent difficile. Ainsi, en y songeant j'ai l'âme grosse. Accourez donc vite et venez me la faire oublier par l'amour ou je veux me mettre.

Stéganographie

- Fichiers graphiques ou sons assez adaptés comme support.
- Permet aux pirates d’extraire les infos sensibles volées en passant inaperçus .

Menaces liées aux réseaux

- Menaces actives
  - Panne, mauvaise utilisation, pertes d'informations
  - Contamination (virus, vers, spyware)
  - Spam, phishing, spear-phishing
  - Chevaux de troie (backdoors)
  - Dénis de services
  - Intrusions

- Menaces passives
  - Écoute des lignes(Wireshark et RTP)
  - Analyse de trafic

Les malwares

Malware

Portion de code inoffensive ou destructrice capable de se reproduire et de se propager.

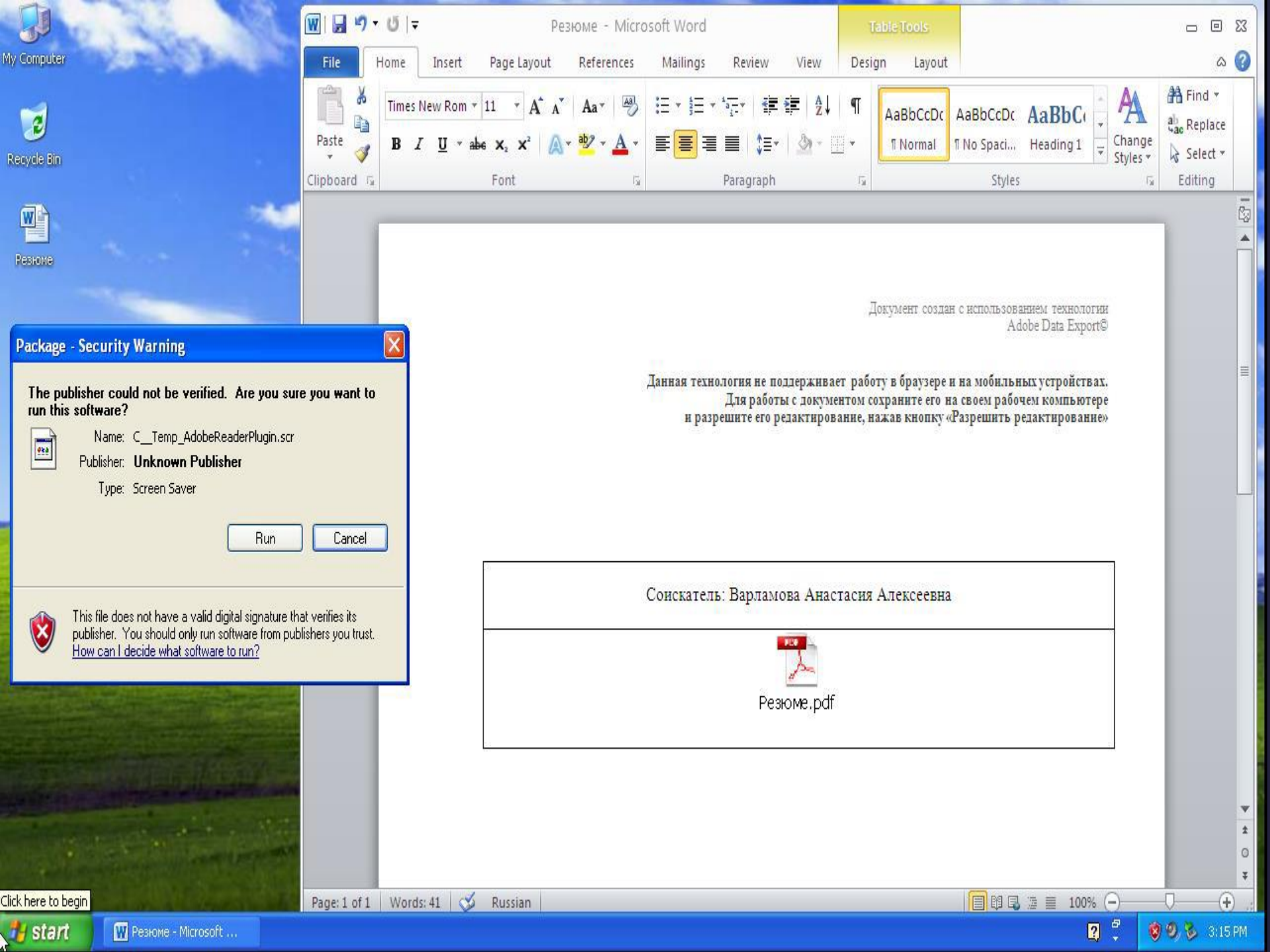
Différentes familles:

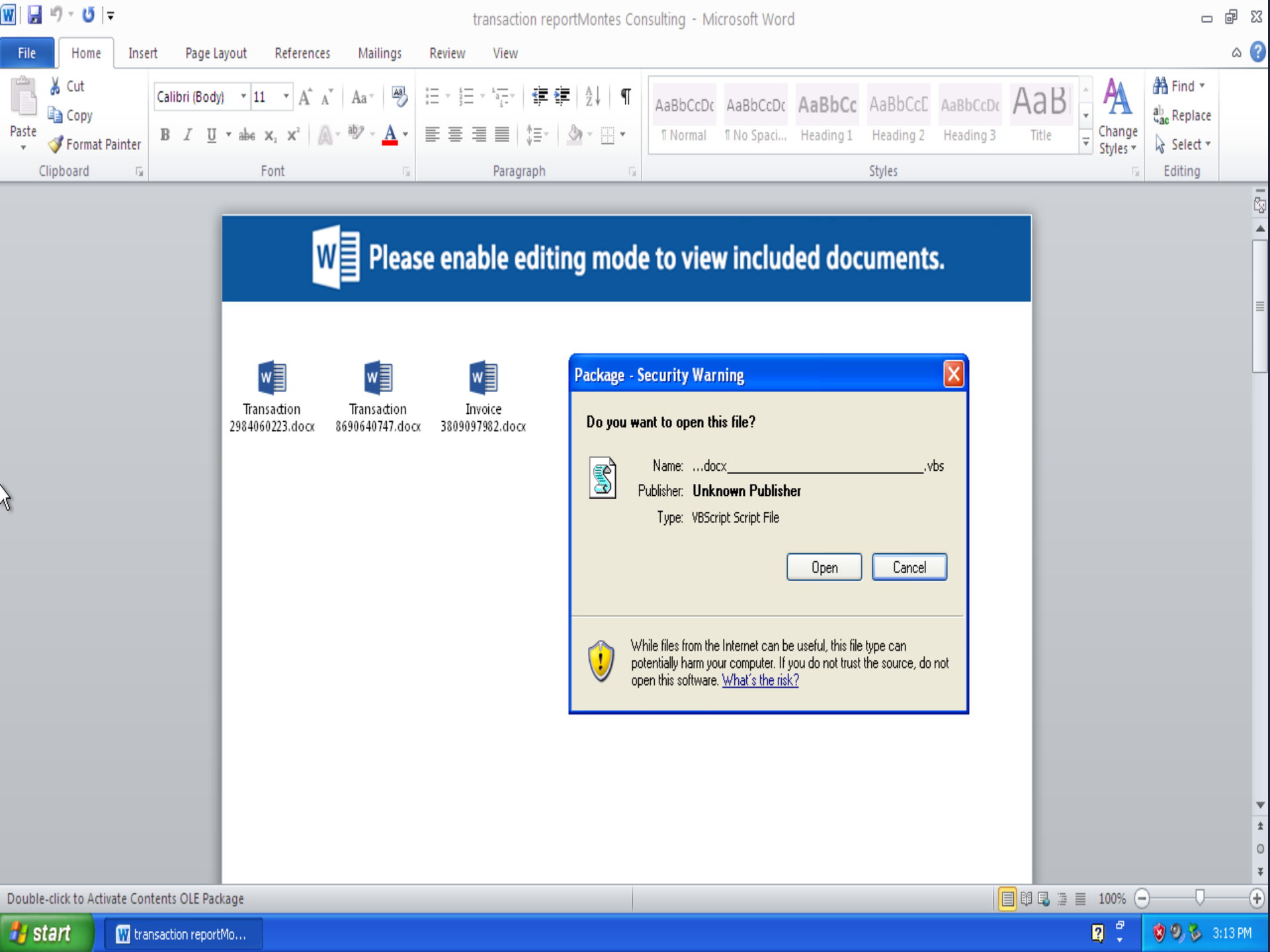
- Backdoor / Trojan / Remote Administration Tool (RAT)
- Ransomware / Locker
- Stealer
- Keylogger (rubber ducky)
- Rootkit

Malware

Déroulement d’une infection:

- Pièces jointes malveillantes
- Attaques “drive-by” via un site infecté(sandbox web)
- Documents piégés (Exploits > PDF et JS/ Macros)
- Clefs USB
- Attaques informatiques


My Computer
Recycle Bin
Резюме
Резюме - Microsoft Word
Table Tools
File
Home
Insert
Page Layout
References
Mailings
Review
View
Design
Layout
Paste
Clipboard
Times New Rom
11
Font
Paragraph
AaBbCcDc
¶ Normal
AaBbCcDc
¶ No Spaci...
AaBbC
Heading 1
Change Styles
Styles
Find
Replace
Select
Editing
Документ создан с использованием технологии
Adobe Data Export©
Данная технология не поддерживает работу в браузере и на мобильных устройствах.
Для работы с документом сохраните его на своем рабочем компьютере
и разрешите его редактирование, нажав кнопку «Разрешить редактирование»
Соискатель: Варламова Анастасия Алексеевна
Резюме.pdf
Package - Security Warning
The publisher could not be verified. Are you sure you want to run this software?
Name: C__Temp_AdobeReaderPlugin.scr
Publisher: Unknown Publisher
Type: Screen Saver
Run
Cancel
This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust.
How can I decide what software to run?
Page: 1 of 1
Words: 41
Russian
100%
Click here to begin
start
Резюме - Microsoft ...
3:15 PM


transaction reportMontes Consulting - Microsoft Word
File
Home
Insert
Page Layout
References
Mailings
Review
View
Cut
Copy
Format Painter
Paste
Clipboard
Calibri (Body)
11
Font
Paragraph
Normal
No Spaci...
Heading 1
Heading 2
Heading 3
Title
Change Styles
Styles
Find
Replace
Select
Editing
Please enable editing mode to view included documents.
Transaction 2984060223.docx
Transaction 8690640747.docx
Invoice 3809097982.docx
Package - Security Warning
Do you want to open this file?
Name: ...docx_____.vbs
Publisher: Unknown Publisher
Type: VBScript Script File
Open
Cancel
While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open this software. What's the risk?
Double-click to Activate Contents OLE Package
100%
start
transaction reportMo...
3:13 PM

Malware

- Les malwares sont très rarement autonomes.

Des instructions doivent être récupérées.

- Nécessité de se connecter à un serveur central qui distribue les ordres.

- Point faible de l'architecture : pas de C&C malware inactif.

- Les auteurs de malwares ont mis au point des contre-mesures(Obfusscassion, VM,clavier,souris…)

Malware

- Comment trouver un virus sur une machine infectée ?

Travailler sur la machine infectée ?

- D'éventuels rootkitspourraient masquer les traces de compromission.
- Débrancher le disque dur et travailler sur une machine saine est le seul moyen.

Certains malwares particulièrement sophistiqués fonctionnent en mémoire de manière non-persistante.

- Redémarrer la machine la désinfecte, aucune trace à trouver sur le disque dur.

- Solution : effectuer un dump mémoire, puis prélever le disque dur.

Malware: Analyse statique

>Analyse statique

Commencer par effectuer un test anti-virus des fichiers inconnus.

- Signatures
- Considérations sur VirusTotal

Empreintes cryptographiques des malwares

- MD5 / SHA1
- `PS> Get-FileHash-Algorithm[MD5/SHA1/SHA256] /path/to/file`
- Recherche Google des hashes pour découvrir les travaux déjà effectués.

Malware:Analyse dynamique

>Analyse dynamique

Analyse *in vivo* d'un code malveillant.En mode «boîte noire».

- Généralement dans une machine virtuelle instrumentée.
- Cuckoo sandbox/Any Run

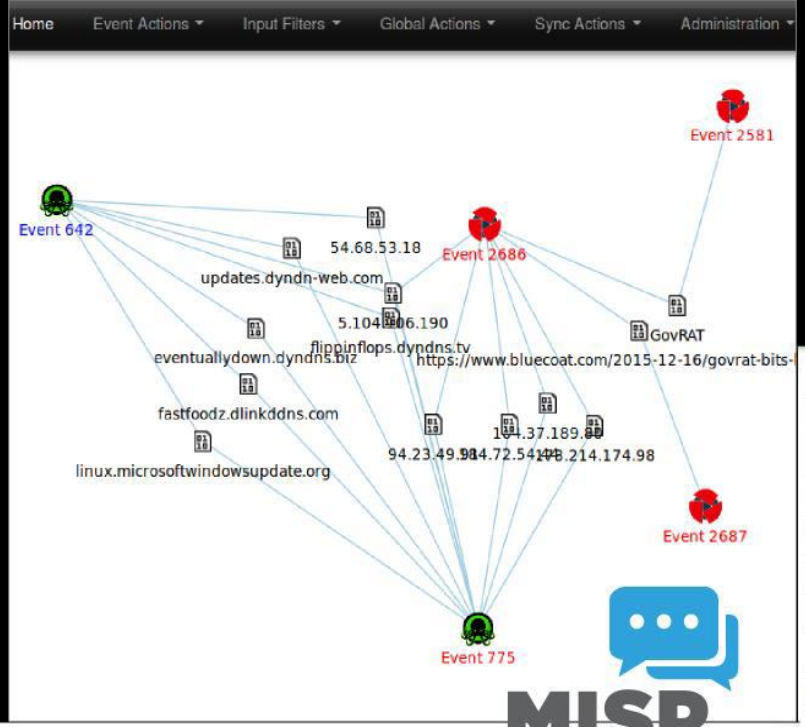
Malware: Analyse dynamique

- Analyse dynamique de code malveillants
- Fournit des informations sur les modifications faites sur le système de fichiers, les clés de registre et le trafic réseau dans un environnement contrôlé et produit un rapport clair et concis.
- L'utilisation d’une sandboxest parfois plus efficace qu’une analyse manuelle.
- Permet de laisser «vivre» le malware.Si la VM ne se fait pas détecter, on peut alors voir toute l’exécution du code malveillant même si celui-ci est chiffré/obfusqué.

Malware

Que sont les IOCs?(Indicatorof Compromise)

- Élément de forensic(«artéfact») permettant une identification ou classification d’un code malveillant.
- Peut être sous forme d’un hash MD5, d’adresse IP, URL, nom de domaine, User-Agent HTTP, etc.
- Utilisé par les antivirus, IDS, et… vous !



TLP Taxonomy Library

Id	3
Namespace	tlp
Description	The Traffic Light Protocol - or short: TLP - was designed with the objective to create a favorable classification scheme for sharing sensitive information while keeping the control over its distribution at the same time.
Version	1
Enabled	Yes (disable)

« previous next »

Filter

Tag	Expanded	Events	Tag	Action
tlp:red	(TLP:RED) Information exclusively and directly given to (a group of) individual recipients. Sharing outside is not legitimate.	3	TLP:RED	
tlp:amber	(TLP:AMBER) Information exclusively given to an organization; sharing limited within the organization to be effectively acted upon.	131	TLP:AMBER	
tlp:green	(TLP:GREEN) Information given to a community or a group of organizations at large. The information cannot be publicly released.	550	TLP:GREEN	
tlp:white	(TLP:WHITE) Information can be shared publicly in accordance with the law.	531	TLP:WHITE	
tlp:ex:chr	(TLP:EX:CHR) Information extended with a specific tag called Chatham House Rule (CHR). When this specific CHR tag is mentioned, the attribution (the source of information) must not be disclosed. This additional rule is at the discretion of the initial sender who can decide to apply or not the CHR tag.	11	TLP:EX:CHR	

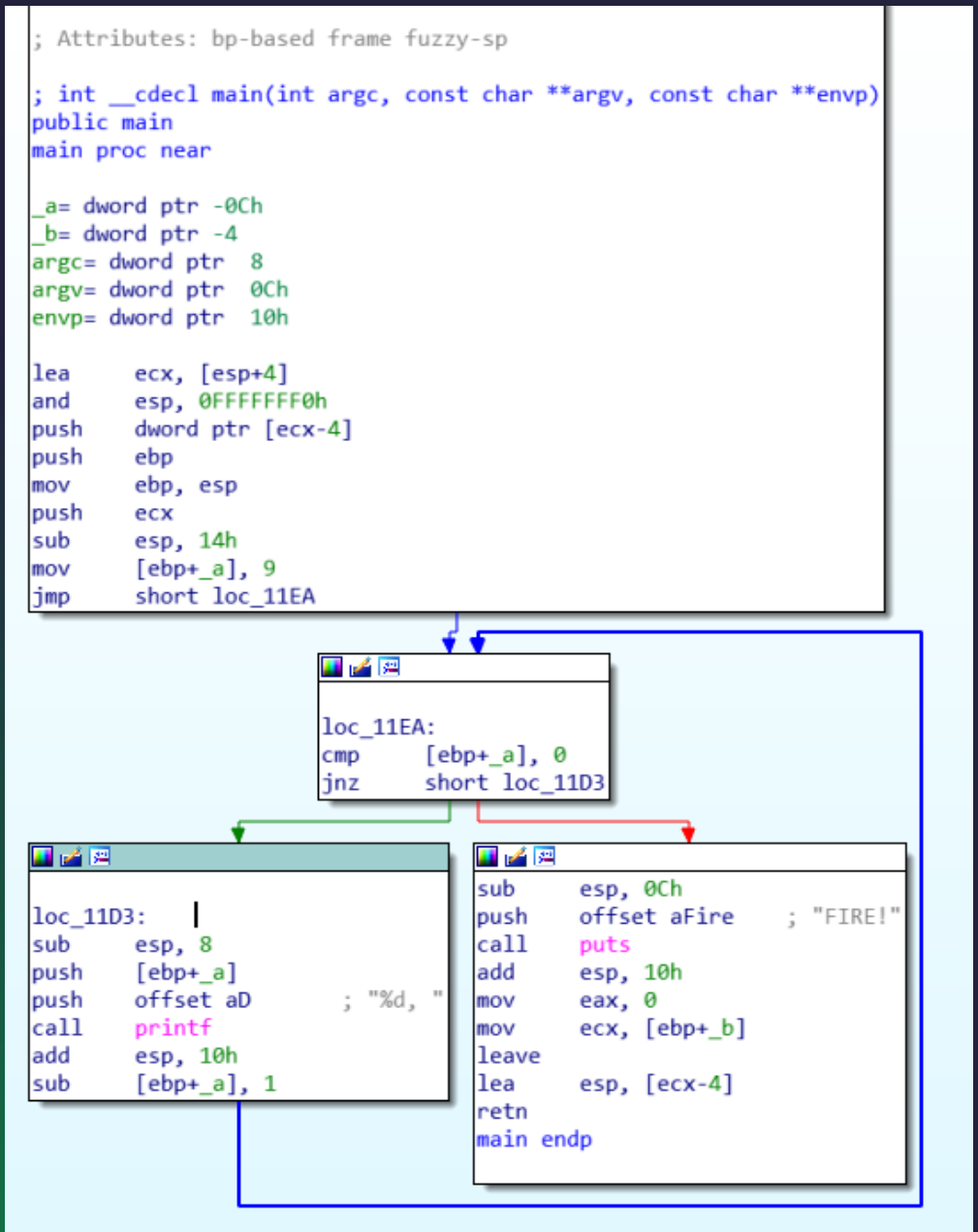
Id	Exportable	Name ↓	Taxonomy	Tagged events	Actions
6	✖	APT		31	
7	✖	Actionable:NO		5	
3	✖	TLP:AMBER	tlp	131	
8	✖	TLP:EX:CHR	tlp	11	
5	✖	TLP:GREEN	tlp	550	
4	✖	TLP:RED	tlp	3	
2	✖	TLP:WHITE	tlp	531	
10	✖	TO:HIDE		2	
9	✖	TODO		9	
11	✖	TODO:VT-ENRICHMENT		8	
1	✖	Type:OSINT		832	
18	✔	admiralty-scale:information-credibility="1"	admiralty-scale	0	
19	✔	admiralty-scale:information-credibility="2"	admiralty-scale	0	
20	✔	admiralty-scale:information-credibility="3"	admiralty-scale	0	
21	✔	admiralty-scale:information-credibility="4"	admiralty-scale	0	
22	✔	admiralty-scale:information-credibility="5"	admiralty-scale	0	
23	✔	admiralty-scale:information-credibility="6"	admiralty-scale	0	

Malware

Quelques exemples de Malware:

- Premiers malware (1970) Creeper > Simple message sur l'écran
- Stuxnet > collaboration des USA et de Israël pour modifier la vitesse de rotation des turbines dans les centrales nucléaires Iraniennes.
- Dridex > stealer, vol de codes d'accès de banque en ligne
- Wannacry et Matsnu > Ransomware , chiffrent les données via des clées de chiffrement inconnues

Malware:Assembleur



Vers

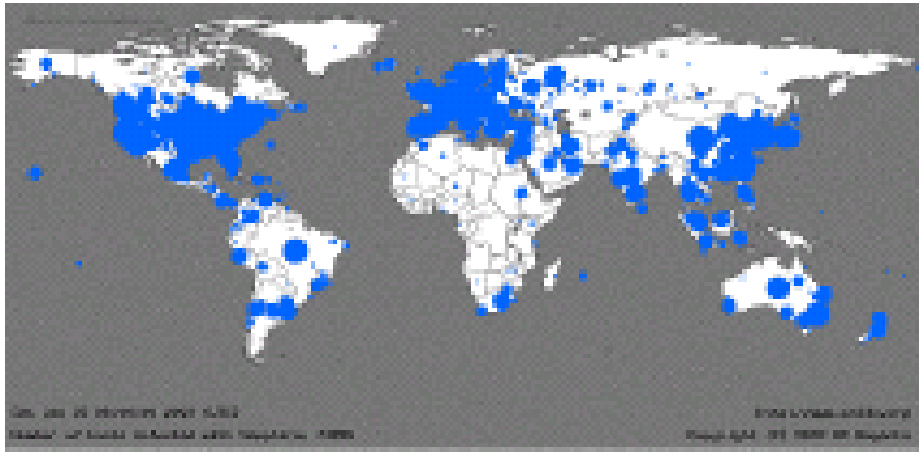
- Proches des virus mais capables de se propager sur d'autres ordinateurs à travers le réseau.
- Un moyen courant de propagation: le carnet d'adresses d'outlook
- Quelques exemples:
  - Code Red (utilisation d'une faille des serveurs IIS et défiguration des sites)
  - Blaster (utilisation d'une faille du protocole windows DCM RPC)

Ver:Sapphire

http://www.caida.org/analysis/security/sapphire/

25 janvier 2003, 05:29 0 victime

25 janvier 2003, 06:00 74 855 victimes



Chevaux de troie

- Très répandu
- Quelques exemples pour Windows
  - Back Orifice
    Permet de la « remote administration ».
  - Eternal blue:
    Maintenue par la NSA

SPAM

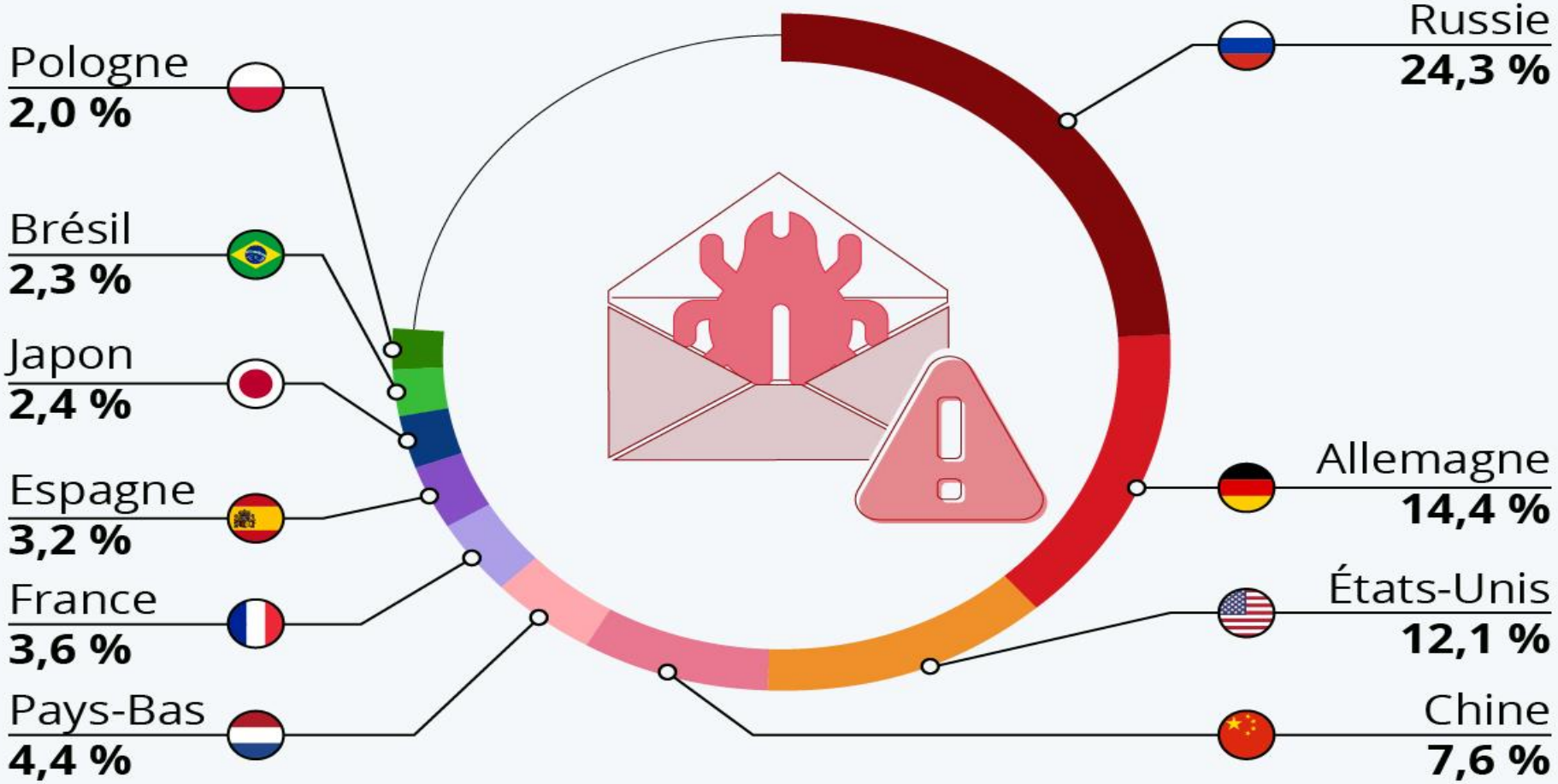
- Définition de la CNIL: Envoi massif et parfois répété de courriers électroniques non sollicités à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact au préalable, et dont il a capté l'adresse électronique façon irrégulière.(pourriel en français).
- SPAM=**Spiced Pork And Meat, popularisé par un sketch des Monty** Python (http://www.dailymotion.com/swf/x3a5yl)
- Un message va être déposé dans une liste de serveurs de courrier; les serveurs abusés vont envoyer une copie à chaque destinataire.
- Courrier basé sur une liste d'adresses collectées de manière déloyale et illicite.
- Messages peu coûteux à l'envoi mais coûteux pour le destinataire.

Le spam en quelques chiffres

- 42 milliards de $: coût global pour les entreprises au niveau mondial en 2004, 200 milliards de $ en 2007
- 600 à 1000 $: coût par an et par salarié
- 49% des 347 milliards de mails envoyés quotidiennement sont des spams

D'où viennent les spams ?

Principaux pays de provenance des courriels indésirables dans le monde, en % du total (2021)



Données issues des rapports trimestriels sur les cyber-menaces de Kaspersky. Moyenne sur le premier semestre 2021.

Protections contre le spam côté utilisateurs

- Ne rien acheter par l'intermédiaire de publicité faite par un spam (des études indiquent que 29% des utilisateurs le font).
- Ne jamais répondre à un spam.
- Ne pas mettre d'adresses électroniques sur les sites webs mais les encoder par un script ou dans une image (exemple: http://www.caspam.org).
- Etre prudent dans le remplissage de formulaires demandant des adresses électroniques; on peut parfois utiliser des adresses « jetables ». Exemple: http://www.jetable.org (adresse valable d'une heure à un mois).
- Protection au niveau du client de messagerie (gestion des "indésirables") .

Protection contre le spam sur les serveurs de messageries

Protection délicate: la frontière entre un courriel et un pourriel n’est pas toujours franche et il ne faut pas rejeter des courriers réels.

- Le SPF est une norme dont l'objectif est d'authentifier le serveur de messagerie émetteur d'un courrier électronique. le serveur de messagerie utilisé pour envoyer l'e-mail est-il autorisé à envoyer des e-mails pour le domaine de question.

- Le DKIM pour DomainKeys Identified Mail, est une méthode d'authentification du courrier électronique basée sur des signatures cryptographiques(vérification via clés publiques avec le server d’authentification)

Phishing

- Contraction de PHreaking et fISHING (Hameçonnage).
- Technique d'ingénierie sociale utilisée par des arnaqueurs (scammers)
- Technique ancienne mais utilisée massivement depuis 2003.
- Par le biais de courrier électronique, messages instantanés, site webs, etc., on tente de duper l'utilisateur en le faisant cliquer sur un lien.
- L'objectif est d'obtenir des adresses de cartes de crédit, des mots de passe, etc.
- Les adresses sont collectées au hasard, mais statistiquement un utilisateur peut avoir l'impression de recevoir un courrier d'un site qui lui est familier (banque,...).

Exemple phishing

Dear valued PayPal® member:

Due to concerns, for the safety and integrity of the paypal account we have issued this warning message.

It has come to our attention that your PayPal® account information needs to be updated as part of our continuing commitment to protect your account and to reduce the instance of fraud on our website. If you could please take 5-10 minutes out of your online experience and update your personal records you will not run into any future problems with the online service.

However, failure to update your records will result in account suspension. Please update your records on or before Oct 04, 2005.

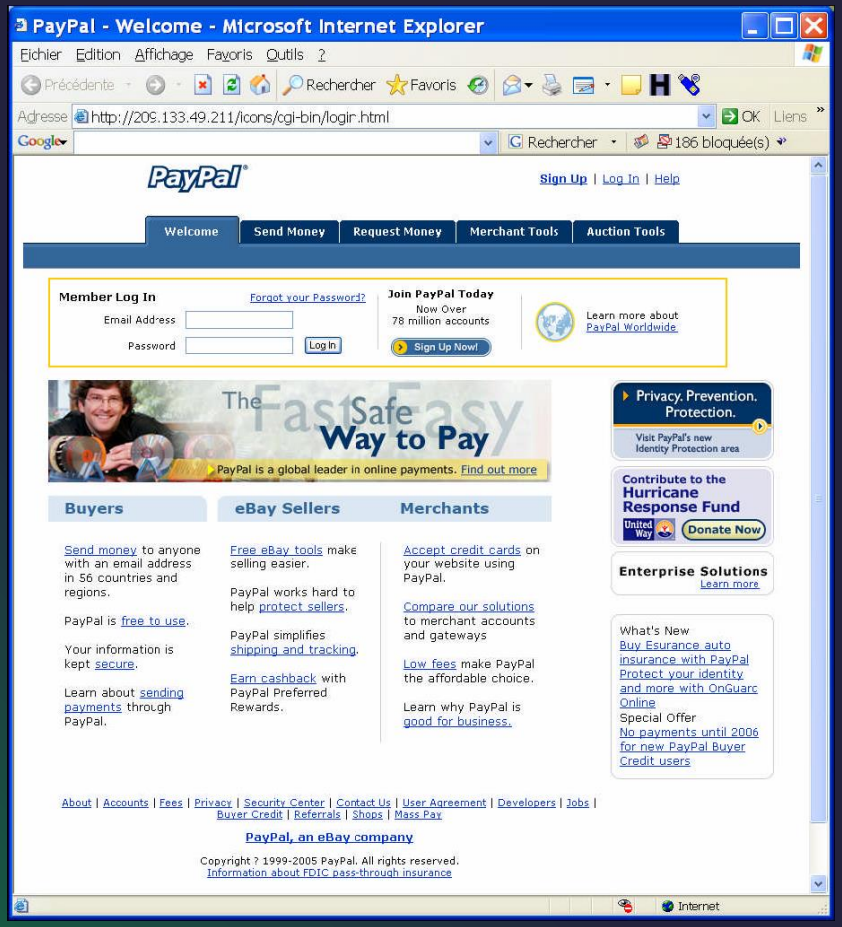
Once you have updated your account records your paypal account service will not be interrupted and will continue as normal.

To update your PayPal® records click on the following link:
http://www.paypal.com/cgi-bin/webscr?cmd=_login-run

Thank You.
PayPal® UPDATE TEAM

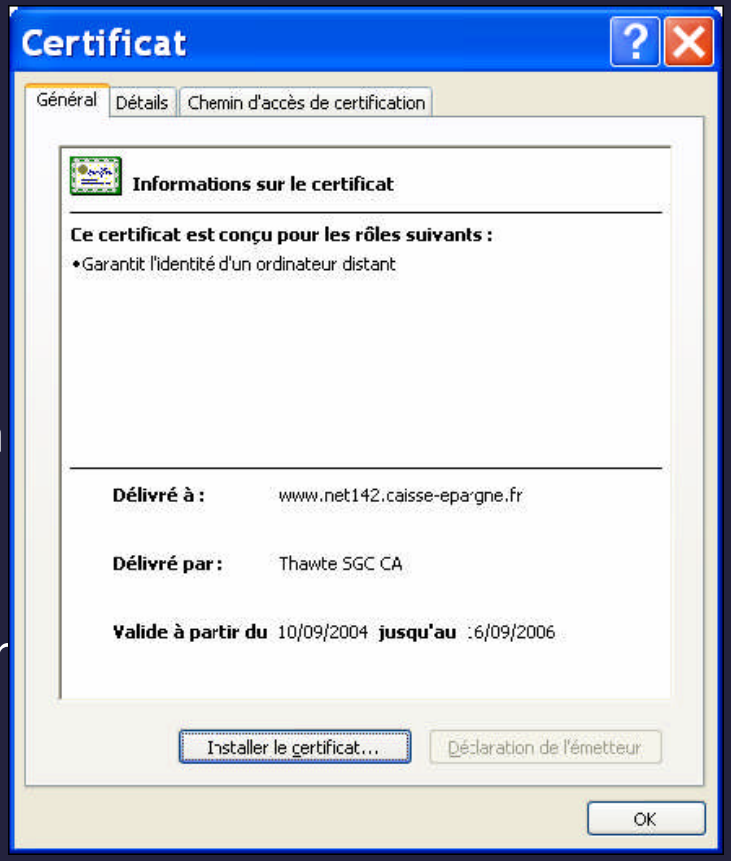
http://209.133.49.211/icons/cgi-bin/login.html

Faux site paypal



Protection contre le phishing

- Vérifier la pertinence des messages.
- Ne pas cliquer sur un lien (mais taper l'adresse dans le navigateur).
- Etre prudent avec les formulaires demandant des informations confidentielles.
- Lors de la saisie d'informations confidentielles, vérifier que l'information est chiffrée et le certificat valide.
- Certains sites commerciaux (ebay, paypal, ...) rappellent le nom d'utilisateur dans les courriers envoyés. Un courrier commençant par quelque chose ressemblant à "Cher utilisateur d'ebay" peut être par conséquent suspect.
- Maintenant inclus dans les navigateur et les antivirus



Exemple de "scam"

Objet: ASSISTANCE
GEORGES TRAORE ABIDJAN,CÔTE D'IVOIRE. AFRIQUE DE L'OUEST.

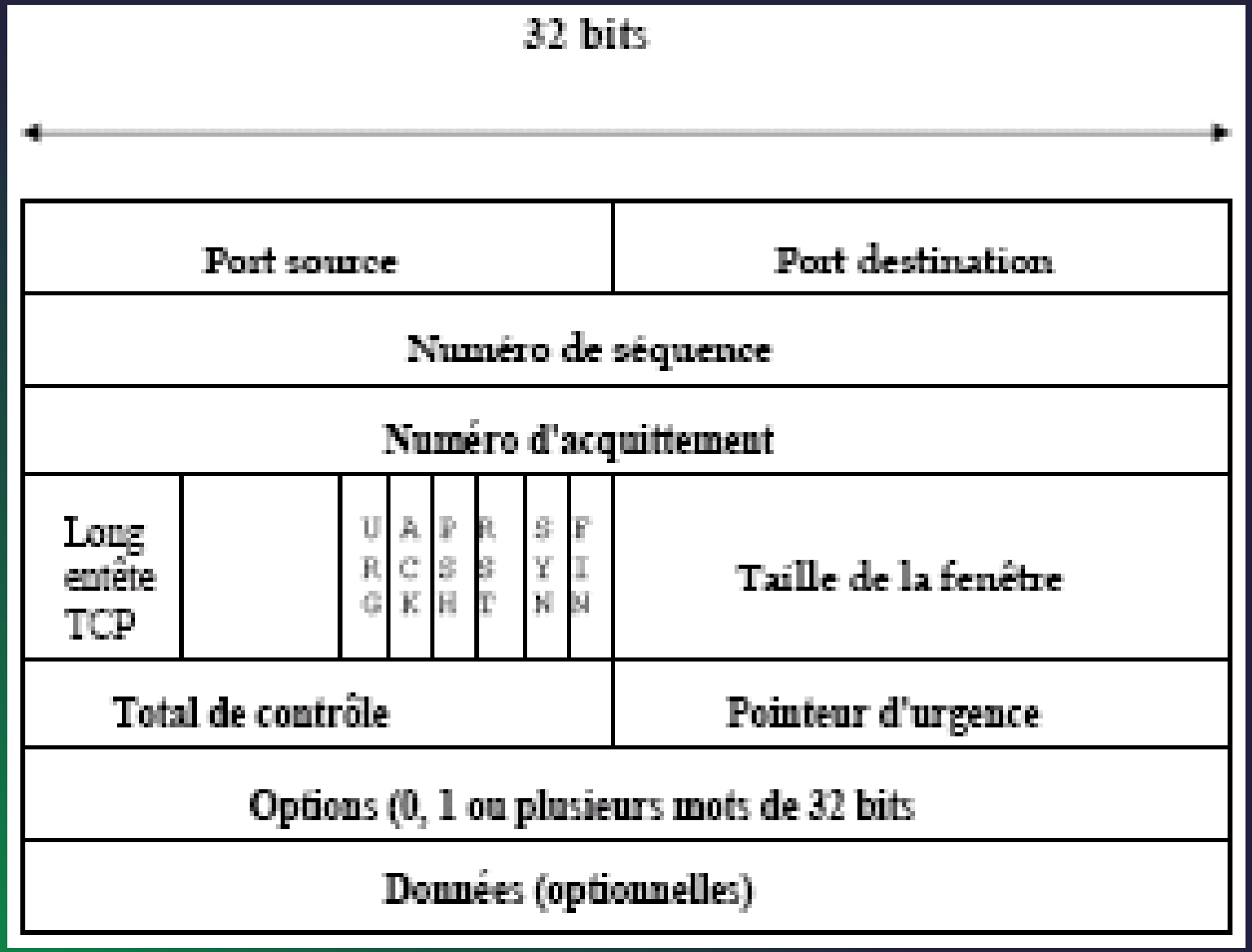
Bonjour,
Je vous prie de bien vouloir excuser cette intrusion qui peut paraître surprenante à première vue d'autant qu'il n'existe aucune relation entre nous.
Je voudrais avec votre accord vous présenter ma situation et vous proposer une affaire qui pourrait vous intéresser.
Je me nomme Georges TRAORE, j'ai 22 ans et le seul fils de mon Père Honorable RICHARD ANDERSON TRAORE qui était un homme très riche, négociant de Café/Cacao basé à Abidjan la Capitale economique de la Côte d'Ivoire, empoisonné récemment par ses associés.
Après la mort de ma mère le 21 Octobre 2000, mon père m'as pris spécialement avec lui. Le 24 Décembre 2003 est survenu le décès de mon père dans une Clinique privée (LAMADONE) à Abidjan. Avant sa mort, secrêtement, il m'a dit qu'il a déposé une somme d'un montant de ($8,500,000) Huit Millions Cinq Cent Mille Dollars Américains dans une valise dans une Compagnie de Sécurité Financière en mon nom comme héritier.
En outre, il m'a dit que c'est par rapport à cette richesse qu'il a été empoisonné par ses associés.
Il me recommande aussi de chercher un associé étranger qui pourrait honnêtement me faire bénéficier de son assistance pour sauver ma vie et assurer mon existence. - Changement de bénéficaire ;
- Servir de gardien ;
- - Fournir un compte pour le transfert de fonds ;
- - M'aider à le rejoindre dans son pays ;
- - Investir dans un domaine profitable.
D'ailleurs, je vous donnerai 25 % et 5% serviront aux dépenses éventuelles qui seront effectuées.
....

Vulnérabilités des réseaux

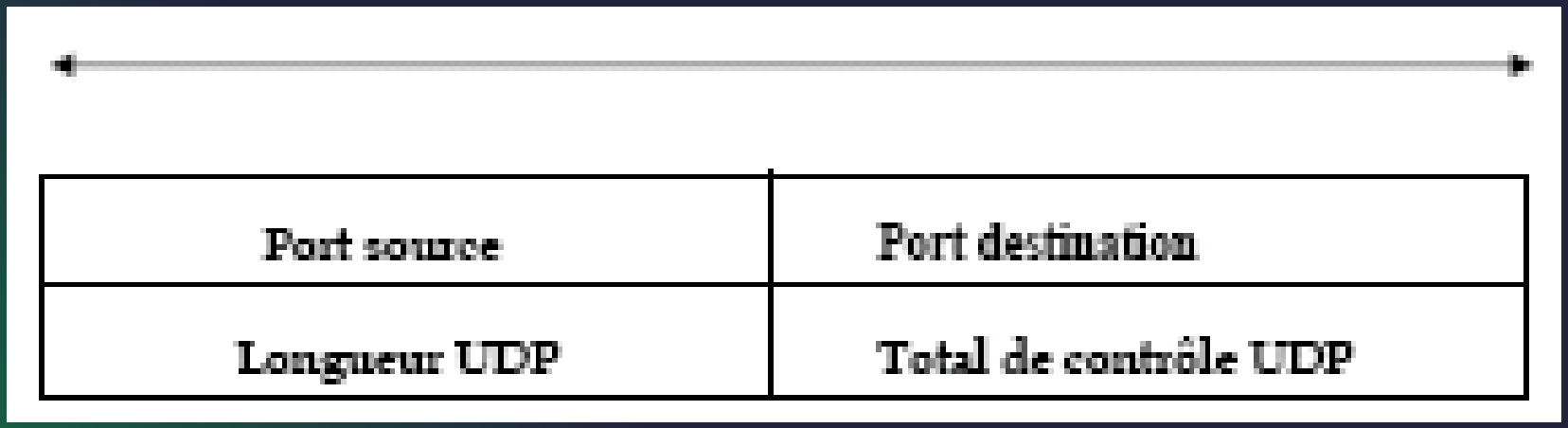
Vulnérabilité des réseaux

- Les réseaux peuvent être vulnérables:
  - par une mauvaise implémentation des piles udp/ip et tcp/ip.
  - par des faiblesses des protocoles
  - Faiblesse des équipements (CVE)

Rappel: Entête TCP

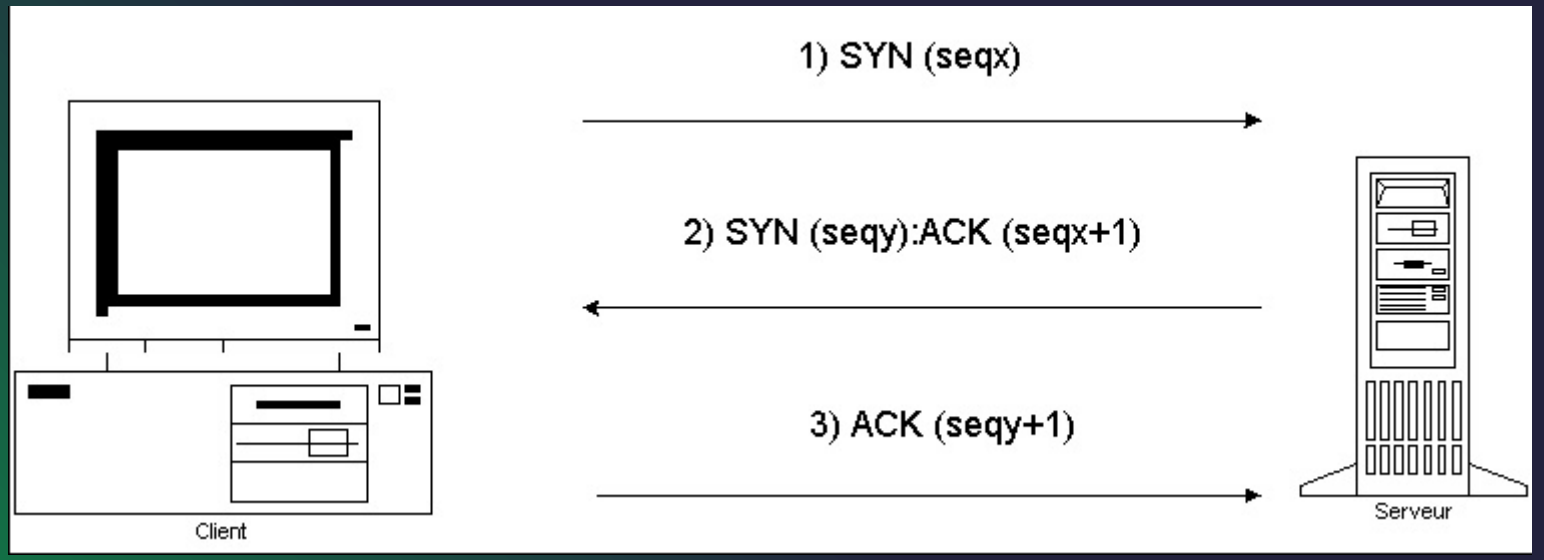


Rappel: Entête UDP



Rappel: établissement d'une connexion TCP

Connexion en 3 temps (Three Way Handshake).



Sniffer

- Permet de visualiser les trames sur un segment de réseau.(TCPDump,Wireshark)
- Attention au problème juridique(demande d’écoute par le n+1)
- Utilise des sockets en mode « promiscuous » socket (AF_INET,SOCK_RAW,IPPROTO_RAW)

IP Spoofing

- Méthode d'attaque qui parodie l'adresse IP d'un autre ordinateur (usurpation).
- Permet de brouiller les pistes ou d'obtenir un accès à des systèmes sur lesquels l'authentification est fondée sur l'adresse IP (rlogin, rsh sur les machines à numéro de séquence TCP prévisible).

Déni de service (DOS)

- Denial Of Service
- Attaque destinée à empêcher l ’utilisation d ’une machine ou d ’un service.
- Type d'attaque utilisée par frustration, par rancune, par nécessité, ...
- Souvent plus facile de paralyser un réseau que d'en obtenir un accès.
- Ce type d ’attaque peut engendrer des pertes très importantes pour une entreprise.
- Attaque relativement simple à mettre en œuvre (outils faciles a trouver).

Différents types de DOS

- DOS local (épuisement des ressources)
  - Saturation de l'espace disque
  - répertoires récursifs
  - boucle infinie
- DOS par le réseau (consommation de bande passante)
  - Réassemblage de fragments (Ex: teardrop, ping of the death)
  - Flags TCP illégaux
  - SYN flood

DOS par « SYN flood »

- Attaque par inondation de SYN avec une adresse source usurpée (spoofée) et inaccessible.
- La machine cible doit gérer une liste de connexions dans l ’état SYN_RECV .
- Une attaque est visible si la commande *netstat –an indique un grand nombre de* connexions dans l'état SYN_RECV.

Parades au SYN Flood

- Allongement de la longueur de la file d'attente.
- Réduction de la durée de temporisation d'établissement d'une connexion.
- OS modernes sont protégés (SYN Cookie, SYN cache, ...).

Connexion par fragments IP

- Une demande de connexion peut être scindée en 2 fragments (tiny fragments):
  - 1er fragment contient un paquet IP de 60 octets + 8 octets TCP (ports + séquence)
  - 2ème fragment contient les flags de connexions.

DOS sur la pile IP

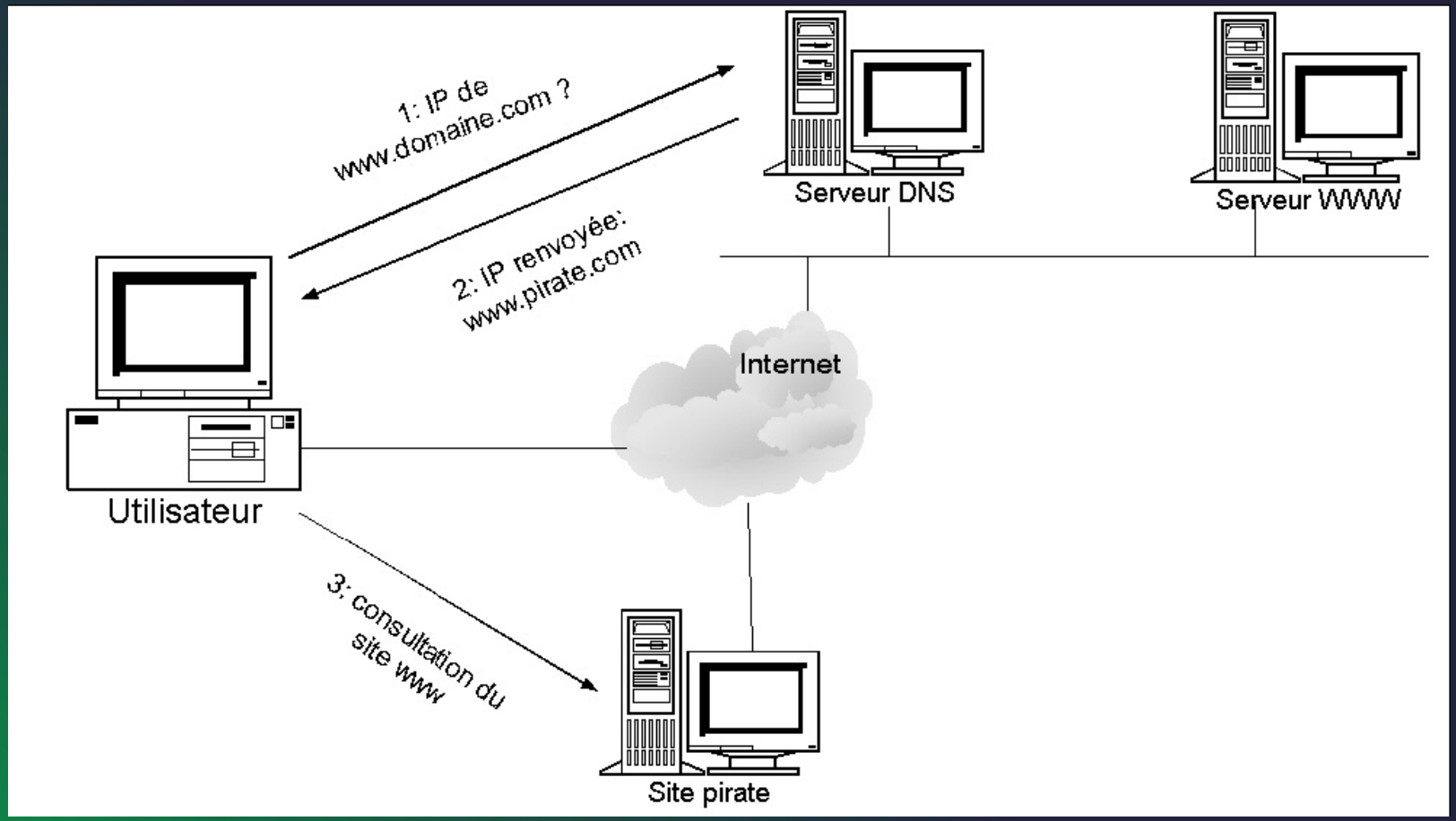
- Teardrop
  - Concerne les anciens noyaux Linux, Windows NT 4.0 inférieur au service pack 3 et Windows 9x non corrigé.
  - Des chevauchements de fragments IP provoquent un arrêt ou un redémarrage de la machine.

DOS sur la pile IP

- Attaque LAND :
  adresse source identique à l'adresse de destination.
- WinNuke :
  paquet OOB envoyé sur le port 139.
- Ping of the Death:
  http://www.insecure.org/sploits/ping-odeath.Html
- Attaque en UDP flooding:
  exemple: echo (UDP 7)/chargen (UDP 19).

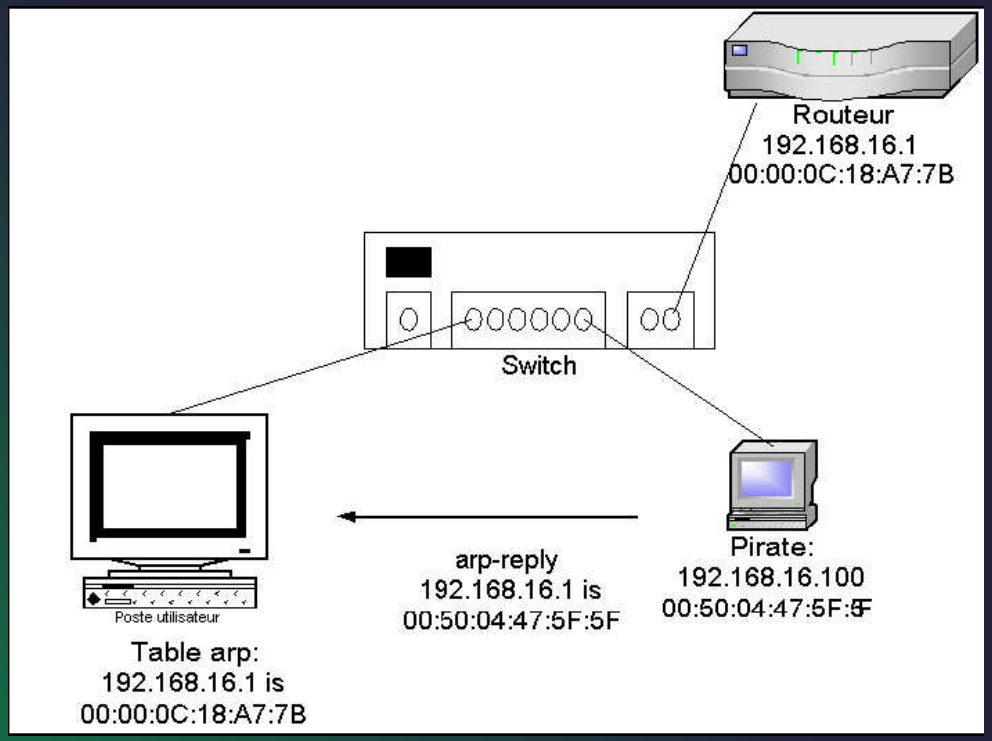
DNS cache poisoning

- Reroutage d'un site sur un site pirate



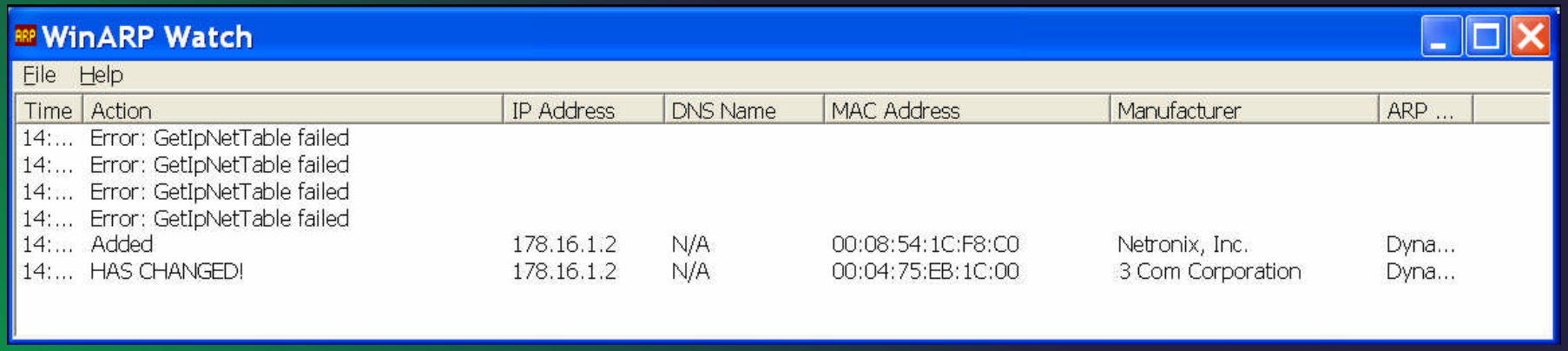
Arp spoofing

- Pollution des caches arp avec de fausses associations adresse mac/adresse IP.(Nmap,EtherCap)
- Permet des attaques de type "man in the middle", DOS, transgression des règles d'un firewall par spoofing.



Parades contre le arp spoofing

- Utiliser des associations statiques
- Surveiller les changements d'association:
  - arpwatch (unix)
    http://www.securityfocus.com/data/tools/arpwatch.tar.Z
  - WinARP Watch (Windows)
    http://www.securityfocus.com/data/tools/warpwatch.zip



tcp hijacking

- Vol d’une session TCP ayant lieu après le « handshake »

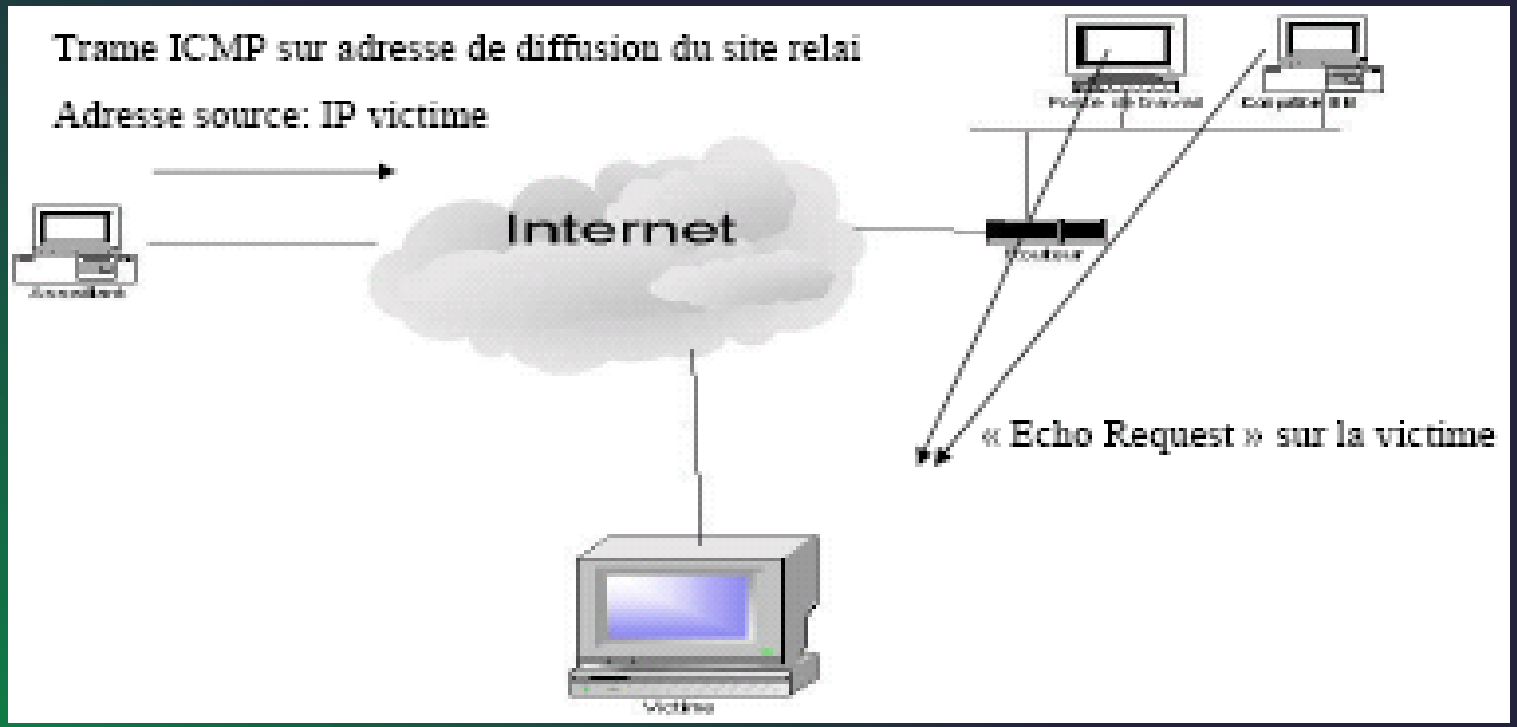
- Exemple d'outil de tcp hijacking: hunt
  http://www.spenneberg.org/TCP-Hijacking//

Smurf

- Envoie d'une trame ICMP "echo request" sur une adresse de diffusion.
- Exemple: *ping 193.49.200.255*
- Méthode utilisée pour déterminer les machines actives sur une plage IP donnée.

Attaque en Smurf

- Objectif: écrouler une machine
- 3 parties: l'attaquant, l'intermédiaire, la victime



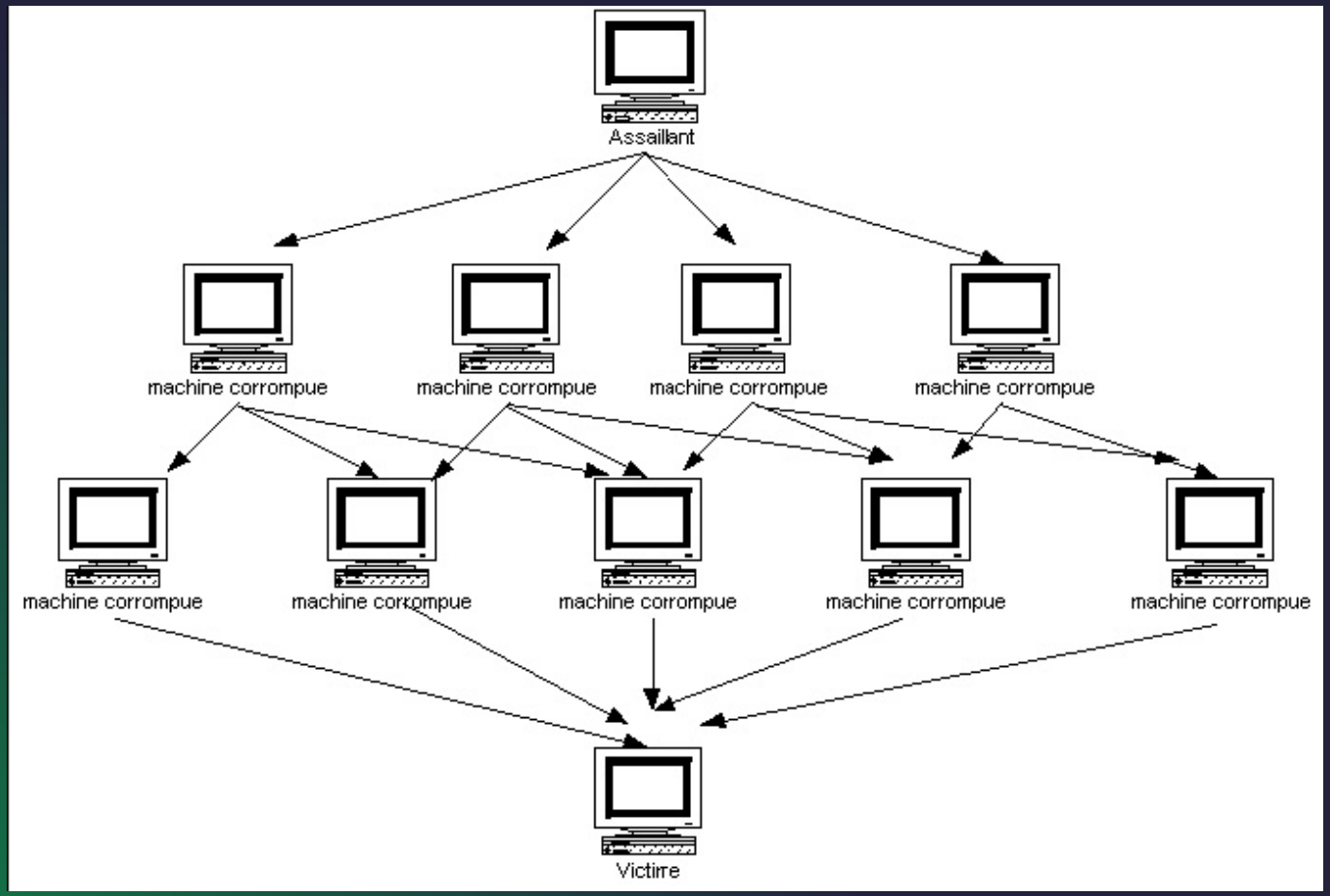
Parades au smurf

- Interdire la réponse aux trames ICMP sur les adresses de diffusion:
  - Au niveau routeur
  - Au niveau machine

DDOS

- Distributed Denial Of Service.
- L ’objectif est d ’écrouler une machine et/ou saturer la bande passante de la victime.
- Nécessite plusieurs machines corrompues.
- Attaque popularisée le 14 février 2000 sur quelques sites .com renommés (ebay, cnn, amazon, microsoft, ...). Le coupable « Mafiaboy », 15 ans, est arrêté au Canada le 15 avril et condamné à 8 mois de détention. Il a causé des pertes estimées à 1,2 milliards de dollars en 24 heures.

Scénario d ’un DDOS



Exemple de ddos

- **Une attaque DDoS paralyse de nombreux sites**
  Date: 16 juin 2004 à 12:07:44 CEST
  Sujet: Sécurité informatique, Virus

  Hier matin, une attaque des serveurs de la compagnie Akamai a rendu certains sites
  inutilisables. De nombreux sites dont ceux de Microsoft, Google, Yahoo, FedEx, Xerox et
  Apple étaient injoignables pendant une courte période. Akamai a déclaré que plusieurs de
  ses clients avaient subit une attaque DDoS, ce qui avait provoqué un crash de leurs
  serveurs DNS. Les serveurs DNS n'étaient alors plus capables de traduire les noms de
  domaines en adresses IP, ce qui rendait les sites inaccessibles.

  Les problèmes ont duré plus de deux heures mais certains sites sont revenus en ligne plus
  rapidement grâce à leurs serveurs DNS de secours. On ne sait pas encore d'ou provenait
  l'attaque, ni quelle était sa cible. Certains virus ont déjà utilisé des techniques similaires,
  notamment Netsky qui ciblait les réseaux d'échange de fichiers Kazaa, eDonkey et eMule.
  En mai dernier, Akamai avait eu des problèmes techniques. Les sites de Symantec et

Vulnérabilités applicatives

Vulnérabilités applicatives

- Beaucoup d'applications sont vulnérables dues à de la mauvaise programmation
  - par manque de temps,
  - par manque de motivation,
  - ou volontairement (backdoor = point d'entrée, ...).

- Toutes les applications ont besoin de sécurité:
  - services réseaux (demons),
  - les applications téléchargées (applet java, ...),
  - les applications web
  - les applications utilisées par l'administrateur ou disposant d'un bit setuid/setgid,

Vulnérabilités les plus courantes

- Les vulnérabilités peuvent être due:
  - "backdoors" laissées volontairement ou involontairement sur un service par le programmeur (Ex: rlogin sous AIX V3)
  - Erreurs de programmation
    - Débordements de tampons (buffer overflow)
    - Entrées utilisateurs mal validées
    - Les problèmes de concurrence
    - etc.

Buffer Overflow

- Appelée aussi "buffer overruns"; c'est une vulnérabilité qui était extrêmement étendue, aujourd’hui moins présentes

- Écriture de données en dehors de la zone allouée (pile ou tas).
- Principalement présent sur du langage C

Buffer Overflow

- Si le buffer est une variable C locale, on pourra essayer de forcer la fonction à exécuter du code pirate ("stack smashing attack").

- Beaucoup d'applications écrites en langage C sont vulnérables car la simplicité et l'efficacité de ce langage ont prévalu sur les contrôles d'intégrité laissés à la responsabilité du programmeur. Mais le problème existe également dans d'autres langages de programmation.

Sécurité des systèmes

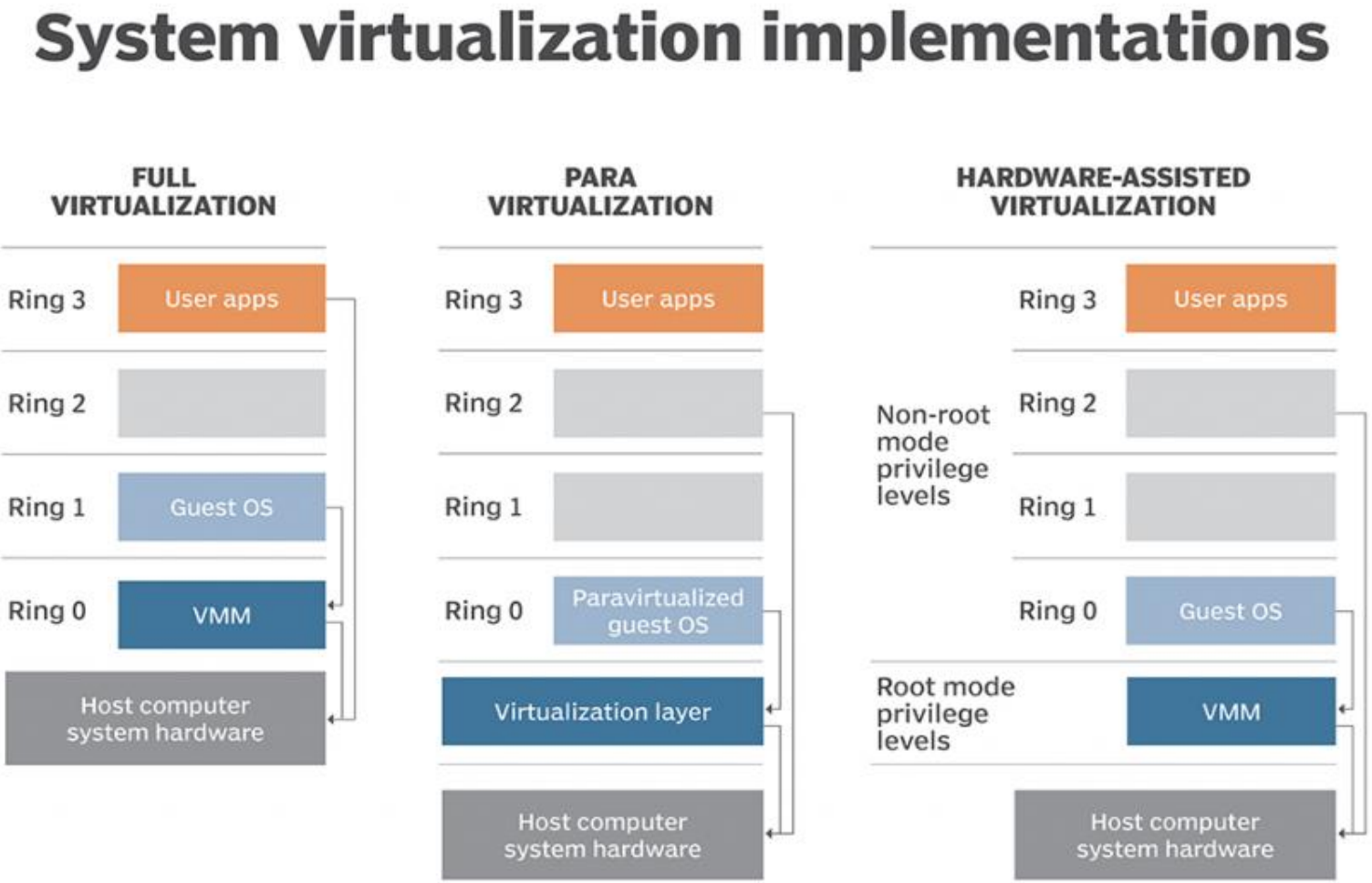
Disponibilité

- Plusieurs ordinateurs peuvent être regroupés en grappe (cluster) pour être visibles comme un seul ordinateur et permettre:
  - D'augmenter la disponibilité
  - De mieux répartir la charge
  - Permettre la montée en charge
  - ...

- Exemples:

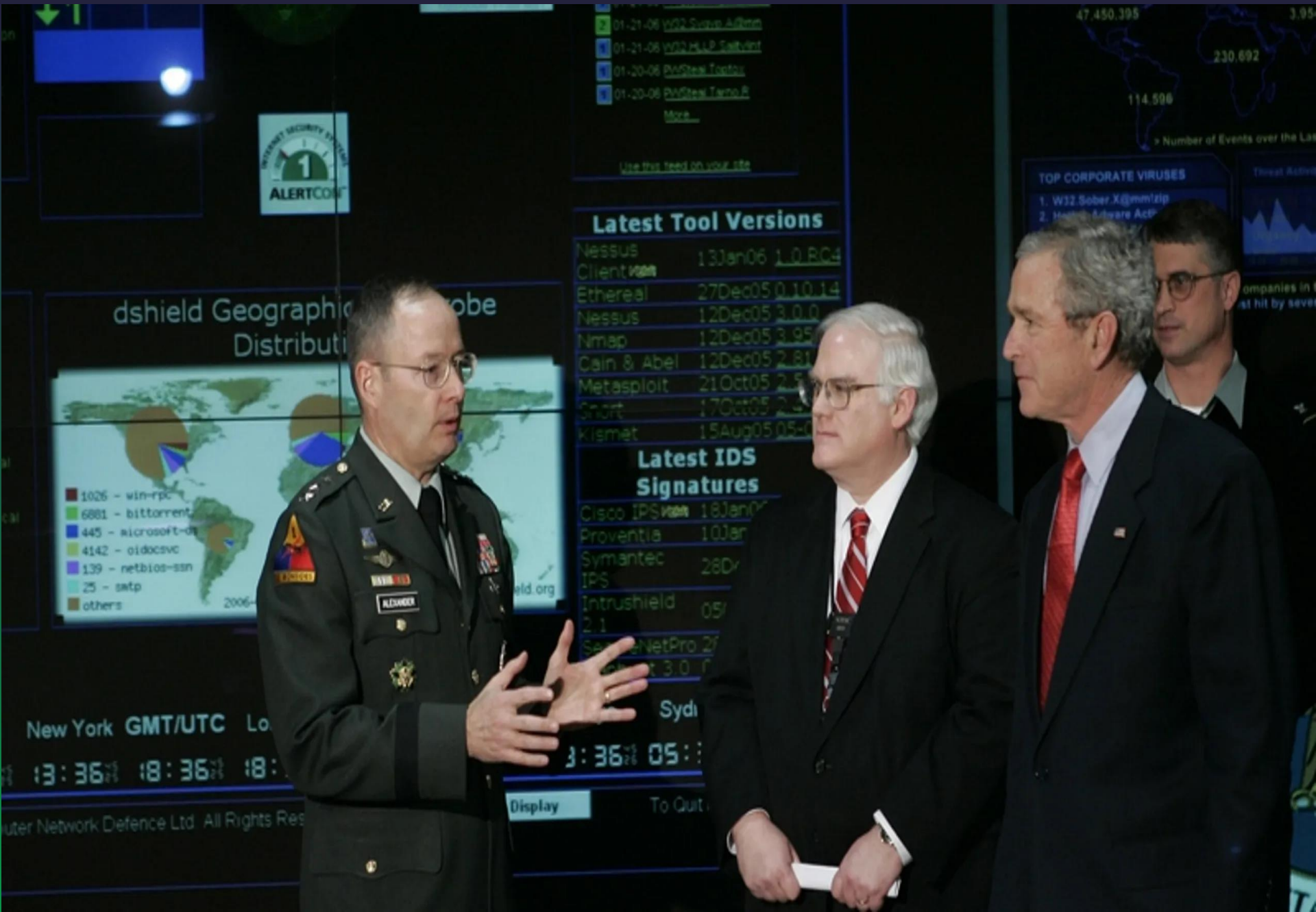
Cluster linux, windows server,...

Virtualisation



Les outils d'attaques/défenses

Beaucoup d'outils disponibles



Cartographie du réseau

- **Méthode standard peu efficace:**
  - ping (Packet Internet Groper).

- **Outils plus sophistiqués:**
  - Pinger *http://www.nmrc.org/files/snt/*
  - fping *http://www.fping.com*
  - Hping3 *http://www.hping.org*
    - *Test firewall rules*
    - *Advanced port scanning*
    - *Test net performance using different protocols, packet size, TOS (type of service) and fragmentation.*
    - *Path MTU discovery*
    - *Transferring files between even really fascist firewall rules.*
    - *Traceroute-like under different protocols.*
    - *Firewalk-like usage.*
    - *Remote OS fingerprinting.*
    - *TCP/IP stack auditing.*
    - *A lot of others.*

Cartographie du réseau

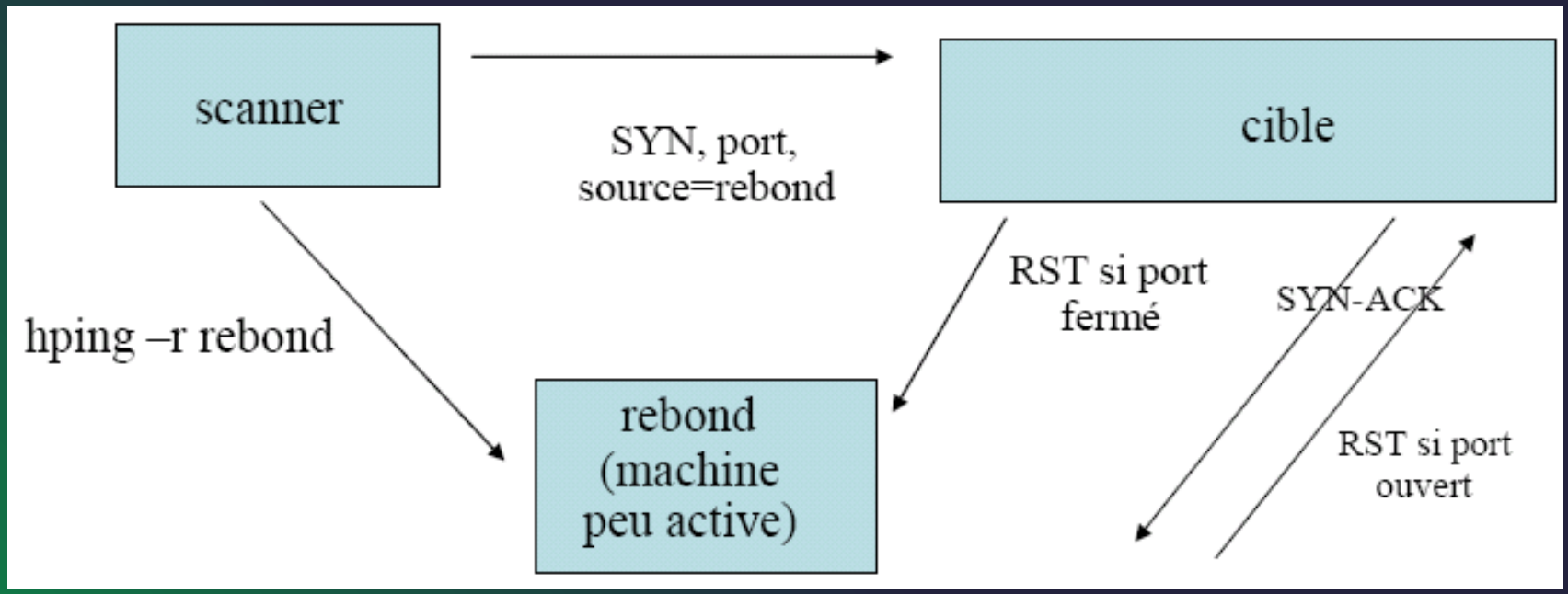
- Le DNS d'un site centralise toutes les machines connectées au réseau.
- Certains DNS incorrectement configurés peuvent autoriser des transferts de zones:
  dig @ns.domaine.com domaine.com axfr

Scan

- Recherche des services ouverts à un instant donné.
- Utilisation d'un scanner de ports
- Envoi d'un paquet (TCP,UDP,ICMP) sur une cible et analyse du résultat; suivant les cas on pourra déterminer l'état d'un port (ouvert,fermé, filtré).
- Beaucoup de logiciels disponibles:
  - Unix: nmap, jakal, IdentTCPscan
  - Windows: ISS,YAPS

Scan Spoofé

- hping permet de scanner une machine en usurpant l'identité d'une autre:



nmap

- Outil de référence.
- nmap sous unix (http://www.nmap.org)
- Scanne une machine ou un réseau à la recherche des services ouverts et de son identité.
- Supporte de nombreuses techniques de scan

nmap: techniques de scan

- vanilla TCP connect () (-sT, défaut)
- TCP SYN (half open) (-sS)
- TCP FIN (stealth) (-sF)
- Xmas scan (-sX)
- Null scan (-sN)
- TCP ftp proxy (bounce attack) (-b server)
- SYN/FIN using IP fragments (-f)
- UDP recvfrom () (-sU)
- RPC scan (-sR)
- Reverse-ident (-I)

Concept de faille

- Une faille est une vulnérabilité permettant à des attaquants d'obtenir un accès non autorisé à un système.(exploit-DB)

- On peut trouver des vulnérabilités à tous les niveaux:
  - routeurs
  - logiciels client/serveur
  - système d'exploitation
  - firewalls

Vulnérabilités

- Un administrateur doit se tenir informé quotidiennement des dernières vulnérabilités et avoir de la réactivité.

- Beaucoup d'information en ligne:
  - Sites officiels
    - CERT (Computer Emergency Response Team)
    - Gouvernement français: CERTA (Centre d'Expertise de Réponse et de Traitement des Attaques), composante du COSSI (Centre Opérationnel de la Sécurité des Systèmes d'Informations) au sein du DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information) dépendant du SGDN (Secrétaire Général de la Défense Nationale) sous l'autorité du Premier Ministre.
    - ...
  - Sites spécialisés
    - Listes de diffusion: BugTraq (http://www.securityfocus.com)
    - et beaucoup d'autres

Nessus:
un outil de test de sécurité

- Modèle client/serveur:
- Utilise des plug-in
- Dispose un langage de programmation (NASL = Nessus Attack Scripting Language)
- Le compte rendu des scanners peut être corrélé avec les bases de données d'incidents pour obtenir l'exploit correspondant.
- Exemples:
  http://www.securityfocus.com (référencement BID)
  http://cve.mitre.org (référencement CVE)

Intrusion Detection System(Snort)

- Basé sur:
  - une approche comportementale:
    - définition de profils type d'utilisateur, ...
  - une approche par scénario:
    - création d'une base de données d'attaques,
    - de signatures,

- Un IDS ne doit pas générer trop de "faux positifs".

Snort: fonctionnalités

- Détection au niveau des protocoles
  IP TCP UDP ICMP
- Détection d'activités anormales
  - Stealth scan,
  - OS Finger Printing,
  - code ICMP invalide
- Préprocesseur pour la gestion des fragments, les sessions http,...

Intrusion Prevention System(Snort)

- Un IPS peut stopper un trafic jugé suspect.
- Un logiciel peut se trouver sur un routeur, sur un firewall ou sur un boîtier spécialisé en rupture du réseau.

- Exemples d'éditeur d'IPS:
  - Cisco,
  - ISS,
  - McAfee, ...

Extrait d'une ACL

ensicaen> show access-lists 112

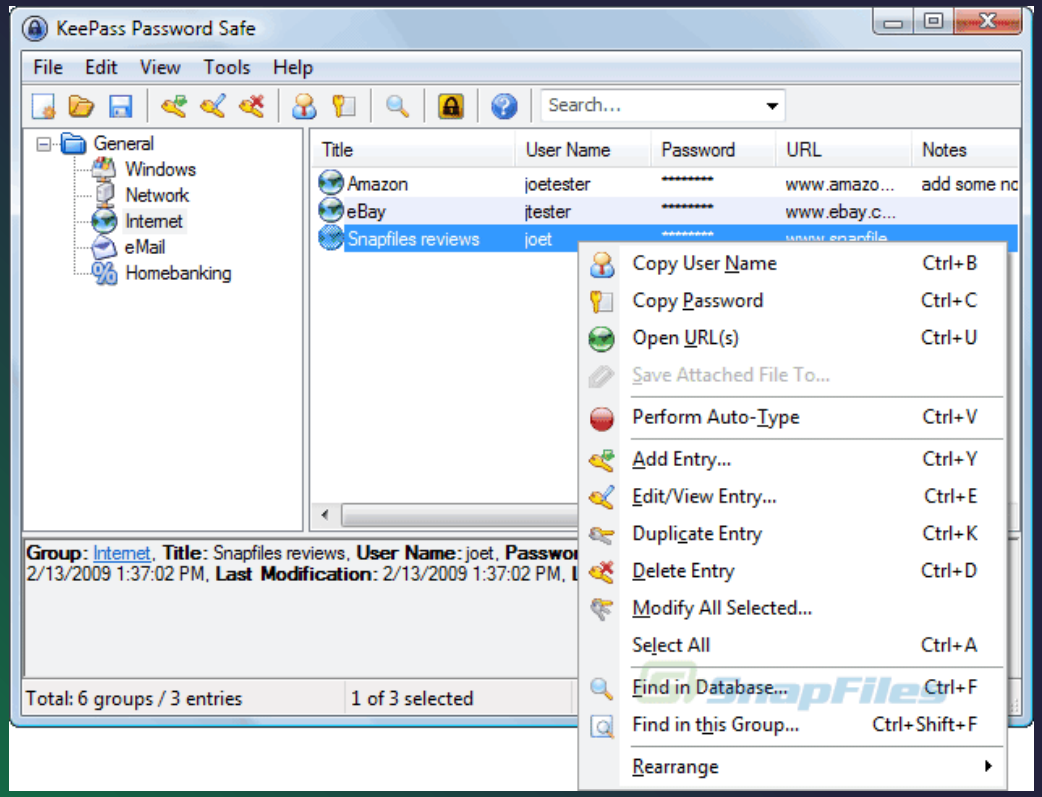
deny tcp any any eq sunrpc log (48501 matches)
deny udp any any eq sunrpc log (54 matches)
deny udp any any eq 135 log (545 matches)
deny tcp any any eq 135 log (8717308 matches)
deny tcp any any eq 136 log (19 matches)
deny udp any any eq 136 log
deny tcp any any eq 139 log (3918461 matches)
deny udp any any eq netbios-ss log
deny tcp any any eq 412 log (13 matches)
deny udp any any eq 412 log
deny tcp any any eq 444 log (4539 matches)
deny udp any any eq 444 log
permit ip any any (330007431 matches)
permit udp any any
permit tcp any any

Craquage de mots de passe

- Les mots de passe sont souvent un maillon faible de la sécurité.
- Le choix d'un mot de passe doit obéir à des règles strictes.
- Des outils existent pour décrypter les mots de passe:
    - Hashcat (utilise le Gpu)
      John The Ripper (utilize le CPU)

Un logiciel de stockage de mot de passes(Keepass)

- De plus en plus de mots de passe à retenir.
- Les mots de passe doivent être robustes.
- Les post-its sont déconseillés pour les mémoriser ;)
- Un exemple de logiciel de stockage de mots de passe:



RootKits

- Souvent utilisé par un intrus pour se dissimuler et garder les accès privilégiés qu'il a obtenu.
- Les premières alertes sur l'utilisation de rootkits datent de février 1994.
- Outil devenu très populaire et qui complique la détection d'intrusion.
- Remplacera des commandes comme ps, netstat, ls
- On pourra trouver également des commandes de nettoyage de logs (/var/log), etc.
- Aujourd’hui le firmware UEFI avec secure boot (vérification des composants et de leurs signatures) protègent contre les rootkit

Détection de rootkits

- Si la machine est infectée, toutes les commandes locales sont suspectes.
- Détection des ports ouverts non officiels (avec nmap sur une machine externe). Par exemple l'inetd de lrk4 ouvre le port 5002.
- Recherche des répertoires spécifiques aux rootkits (par exemple /dev/ptry avec lrk4).
- Utilitaires de détection:

unix:
chkrootkit
windows*:*
rootkitrevealer

Chiffrement, tunnels

SSH

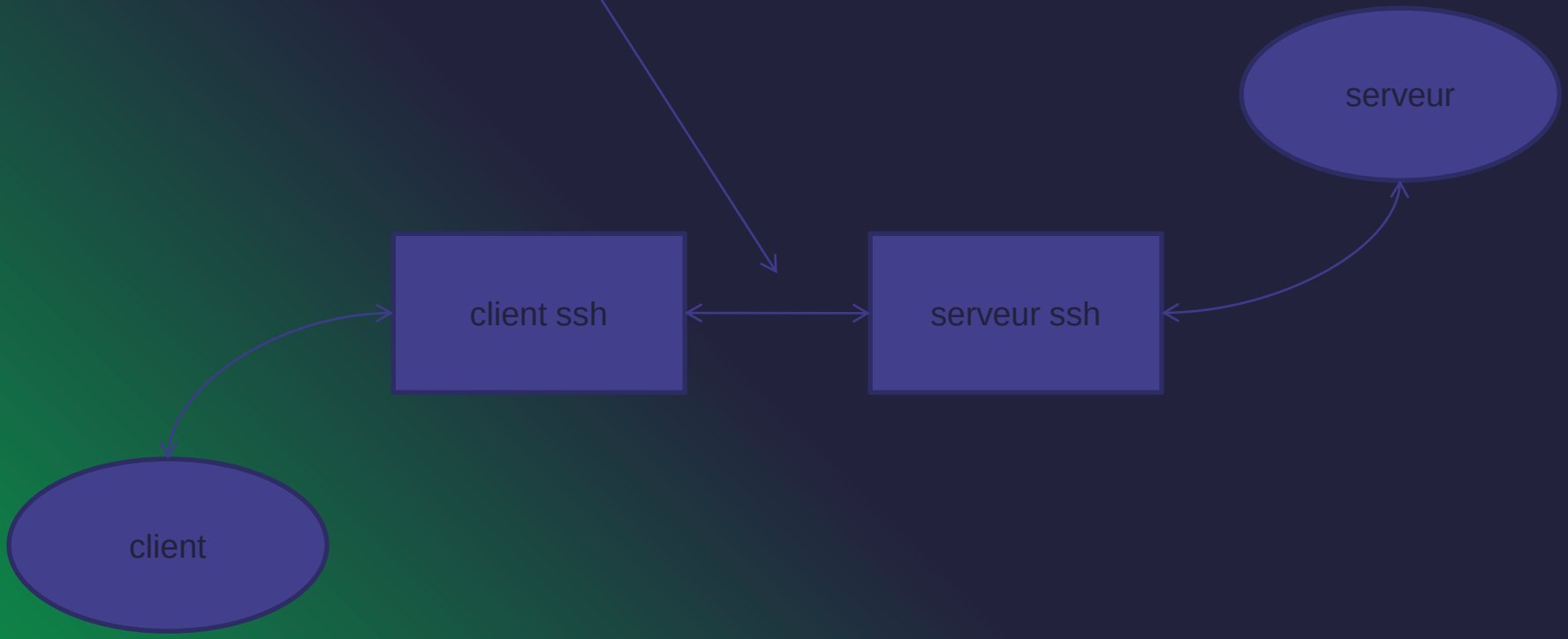
- ssh (Secure Shell) plutôt que telnet,rlogin,rsh,rcp
- Génération d'une paire de clef RSA (toutes les heures) par le serveur.
- Envoi de la clef publique au client qui se connecte.
- Le client génère une clef symétrique, la chiffre avec la clef du serveur et la renvoie au serveur.
- Le reste de la communication est en chiffrement symétrique.

Tunneling

- Un protocole de tunneling est utilisé pour créer un chemin privé (tunnel) à travers une infrastructure éventuellement publique.
- Les données peuvent être encapsulées pour emprunter le tunnel.(possibilité d’encapsuler dans un paquet ou un trame elle-même encapsulée)
- Solution intéressante pour relier deux entités distantes à moindre coût.

Tunneling ssh

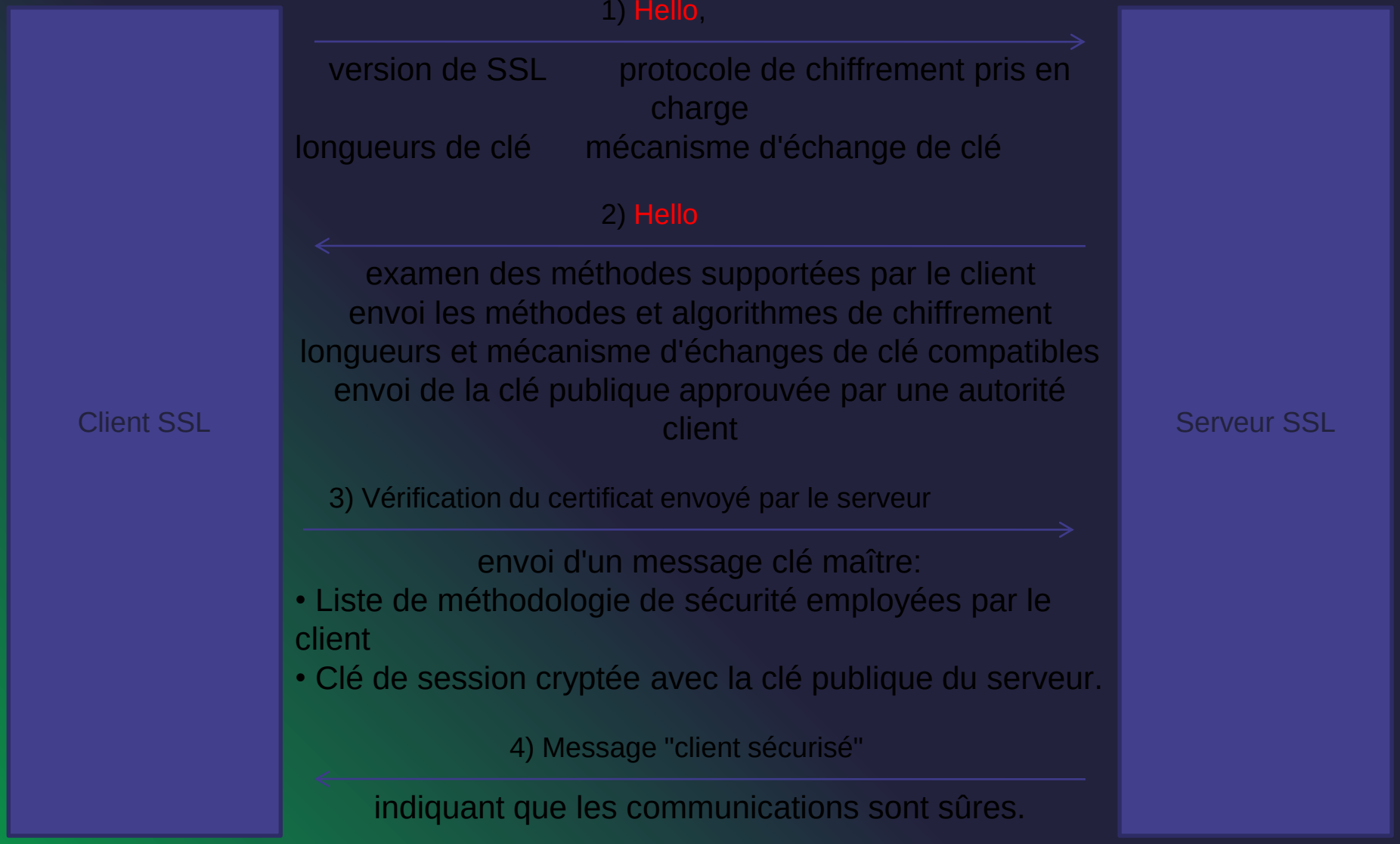
- Un flux tcp quelconque peut être redirigé dans un tunnel ssh



SSL

- SSL (Secure Sockets Layer)
  - Se situe entre la couche application et la couche transport.
  - Garantit :
    - l'authentification
    - l'intégrité
    - la confidentialité.
  - Largement utilisé pour la sécurisation des sites www (https).
  - Popularisé par les révélations de Snowden sur les écoutes de la NSA/CIA,

Fonctionnement SSL



Firewall

Firewall

- Protéger son réseau du monde extérieur (Internet, autres services de l'entreprise).
- Maintenir des utilisateurs à l'intérieur du réseau (employé, enfant, ...)
- Restreindre le nombre de machines à surveiller avec un maximum d'attention.
- Certaines machines doivent rester ouvertes (serveur www, dns, etc).

Firewall

- C'est un outil souvent indispensable mais jamais suffisant:
  - Pas de protection contre le monde intérieur
  - Pas de protection contre les mots de passe faibles
- Nécessite une politique de sécurité:
  - Tout autoriser et interdire progressivement
  - Tout interdire et ouvrir sélectivement

Firewall

STORMSHIELD

SOPHOS

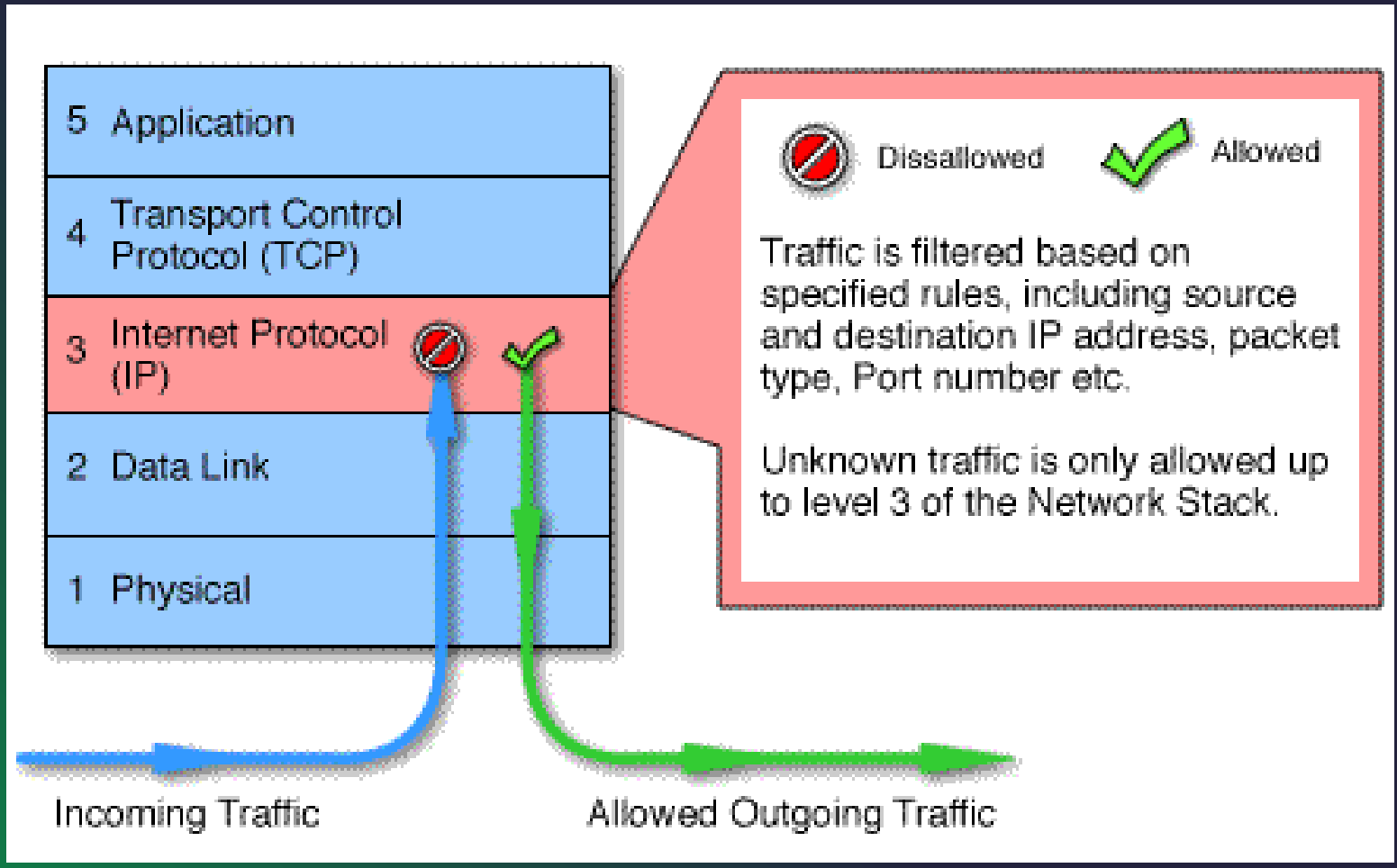
FORTINET

paloalto NETWORKS

Check Point SOFTWARE TECHNOLOGIES LTD

Juniper NETWORKS

Filtrage de paquets



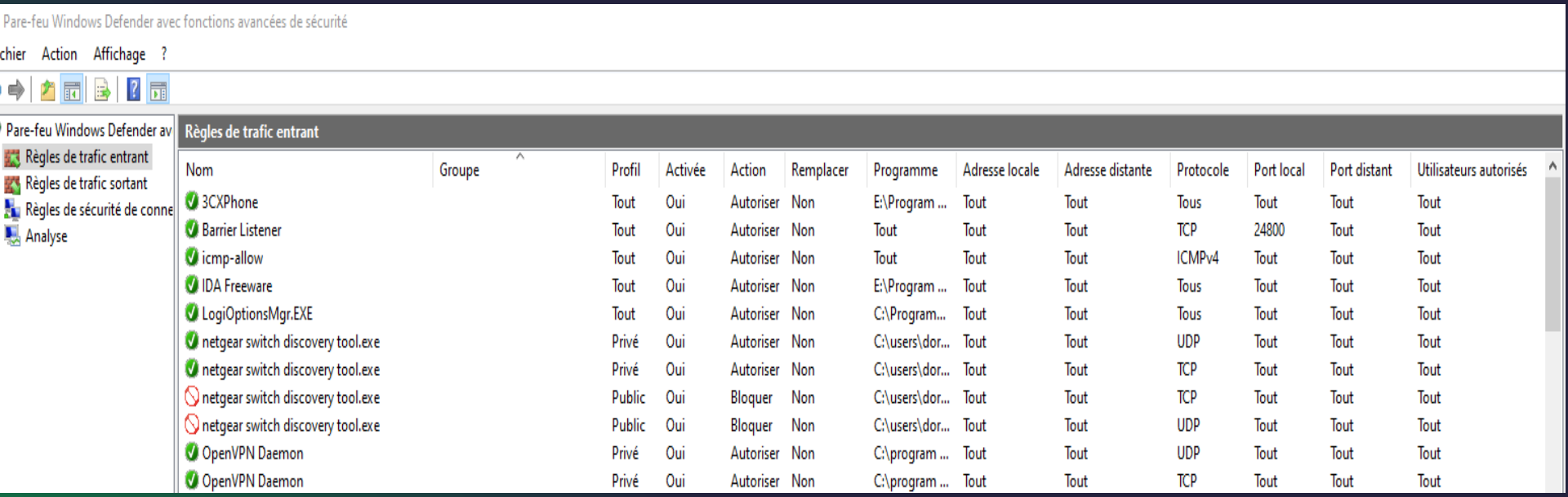
Fonctionnalités actuelles d' un firewall

- Filtrage sur adresses IP/Protocole,
- Inspection stateful et applicative,
- Intelligence artificielle pour détecter le trafic anormal,
- Filtrage applicatif
  - HTTP (restriction des URL accessibles),
  - Anti Spam
  - Antivirus, Anti-Logiciel malveillant
- Translation d'adresses,
- Tunnels IPsec, PPTP, L2TP,
- Identification des connexions,
- Serveur Web pour offrir une interface de configuration agréable,
- Relai applicatif (proxy),
- Détection d'intrusion (IDS)
- Prévention d'intrusion (IPS)
- ...

Protection des endpoints

- Les machines doivent être protégés individuellement; ils sont parties intégrantes de la sécurité d'un site.
  - Antivirus
  - EDR/XDR/SIEM
  - Anti Spywares
  - Firewall personnels
  - Mise à jour de correction des vulnérabilités

Exemples firewalls personnels



Nom	Groupe	Profil	Activée	Action	Remplacer	Programme	Adresse locale	Adresse distante	Protocole	Port local	Port distant	Utilisateurs autorisés
3CXPhone		Tout	Oui	Autoriser	Non	E:\Program ...	Tout	Tout	Tous	Tout	Tout	Tout
Barrier Listener		Tout	Oui	Autoriser	Non	Tout	Tout	Tout	TCP	24800	Tout	Tout
icmp-allow		Tout	Oui	Autoriser	Non	Tout	Tout	Tout	ICMPv4	Tout	Tout	Tout
IDA Freeware		Tout	Oui	Autoriser	Non	E:\Program ...	Tout	Tout	Tous	Tout	Tout	Tout
LogiOptionsMgr.EXE		Tout	Oui	Autoriser	Non	C:\Program...	Tout	Tout	Tous	Tout	Tout	Tout
netgear switch discovery tool.exe		Privé	Oui	Autoriser	Non	C:\users\dor...	Tout	Tout	UDP	Tout	Tout	Tout
netgear switch discovery tool.exe		Privé	Oui	Autoriser	Non	C:\users\dor...	Tout	Tout	TCP	Tout	Tout	Tout
netgear switch discovery tool.exe		Public	Oui	Bloquer	Non	C:\users\dor...	Tout	Tout	TCP	Tout	Tout	Tout
netgear switch discovery tool.exe		Public	Oui	Bloquer	Non	C:\users\dor...	Tout	Tout	UDP	Tout	Tout	Tout
OpenVPN Daemon		Privé	Oui	Autoriser	Non	C:\program ...	Tout	Tout	UDP	Tout	Tout	Tout
OpenVPN Daemon		Privé	Oui	Autoriser	Non	C:\program ...	Tout	Tout	TCP	Tout	Tout	Tout

Les honeypots

Mise en oeuvre d’un « honeypot »

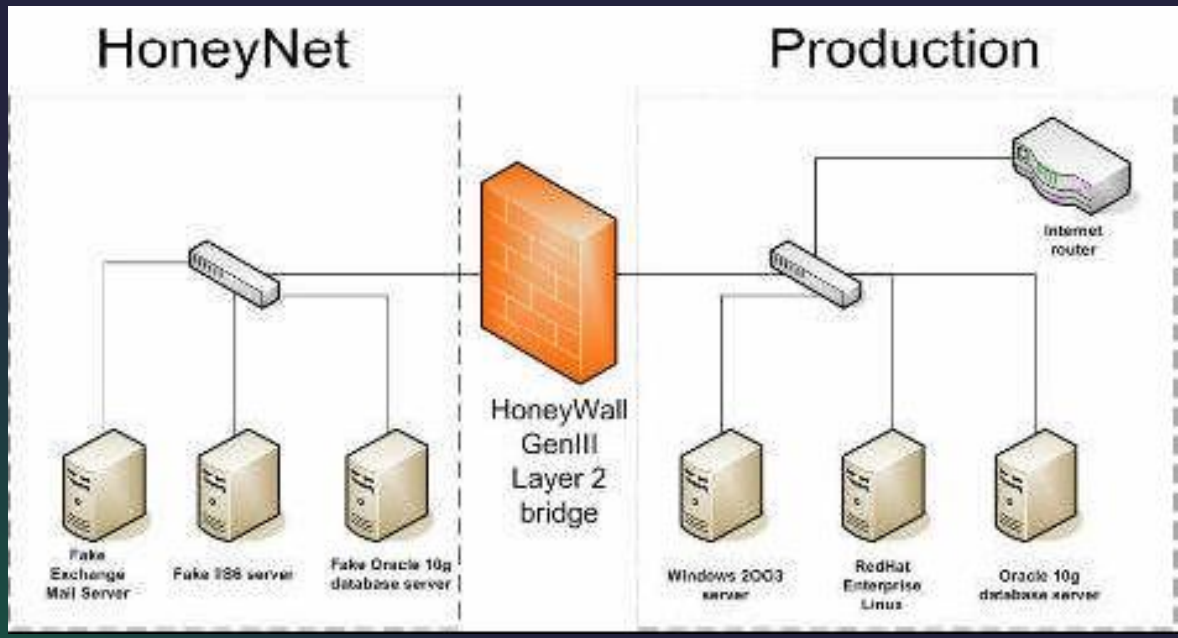
- Un « honeypot » est une machine connectée au réseau et volontairement de sécurité faible.(Honeyd,OSSEC…)

- Objectifs:
  - Distraire un attaquant pour protéger des machines plus sensibles.

  - Découvrir de nouvelles techniques d’attaques, de nouveaux outils, …

Honeypots

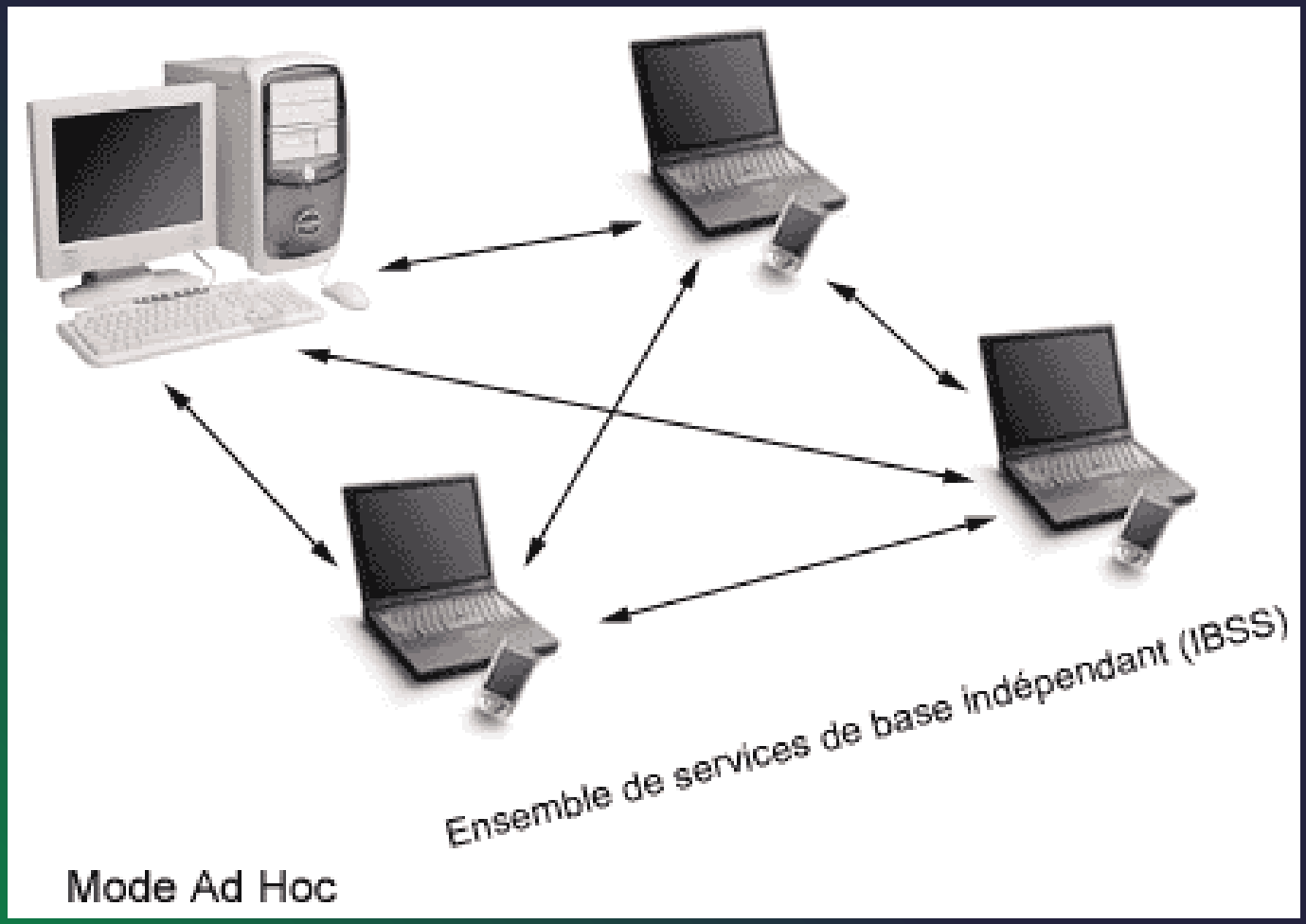
- Donnent de véritables accès à des attaquants.
- Risques beaucoup plus importants impliquant un déploiement prudent.
- Exemple:
  - ROO HoneyWall



Wifi et sécurité

IEEE Standard	802.11a	802.11b	802.11g	802.11n	802.11ac	802.11ax
Year Released	1999	1999	2003	2009	2014	2019
Frequency	5Ghz	2.4GHz	2.4GHz	2.4Ghz & 5GHz	2.4Ghz & 5GHz	2.4Ghz & 5GHz
Maximum Data Rate	54Mbps	11Mbps	54Mbps	600Mbps	1.3Gbps	10-12Gbps

Modes de communication: le mode AD HOC



Les nouveaux risques

- Plus de limite physique au réseau.
- Equivalent à avoir une prise réseau sur le trottoir.
- Possibilité de capter le signal assez loin.
- Déni de services aisé.

Les conséquences

- Ecoute et interception de trafics
- Insertion de trafic
- Introduction d'une station illicite sur le réseau
- Rebonds(imprimante et segmentation par étage)

Sécurisation des points d'accès

- Changer les mots de passe par défaut.
- Désactiver les services inutiles (telnet, snmp, ...)
- Régler la puissance d'émission au minimum nécessaire.
- Mettre à jour le "firmware" au fur et à mesure des mises à jours.
- Sécuriser l'accès physique des points d'accès.

Le chiffrement WPA2

- La norme 802.11i a été ratifiée le 24 juin 2004.
- La certification WPA2 a été créée par la Wi-Fi Alliance.
- WPA2 utilise l'algorithme AES (Advanced Encryption Standard).
- Aujourd’hui c’est le minimum pour lé sécurisation wifi

Conseils et conclusions

Que faire en cas d'intrusion

- Pas de réponse unique:
  - Débrancher ou non la machine (souhaite t'on découvrir les méthodes utilisées par l'intrus ?)
- Sauvegarder la machine en l'état afin de pouvoir l'analyser à posteriori.
- Reformater et réinstaller le système à partir d'une sauvegarde saine.
- Modifier les mots de passe utilisateurs et les éventuelles clés de chiffrement.
- Ne pas donner d'informations sur l'incident à des tiers non directement concernés.
- Être vigilant, l'intrus reviendra probablement.

L'authentification

- Authentification par adresse MAC est peu sécurisée.
- Le protocole 802.1X définit une encapsulation de EAP (Extensible Authentification Protocol) au dessus du protocole IEEE 802.11
- Différentes variantes du protocole EAP:
  - Protocole EAP-MD5 (EAP - Message Digest 5) ;
  - Protocole LEAP (Lightweight EAP) developpé par Cisco ;
  - protocole EAP-TLS (EAP - Transport Layer Security) crée par Microsoft et accepté sous la norme RFC 2716 ;
  - protocole EAP-TTLS (EAP - Tunneled Transport Layer Security) developpé par Funk Software et Certicom ;
  - protocole PEAP (Protected EAP) developpé par Microsoft, Cisco et RSA Security ...

Qui prévenir en cas d'incidents

- La direction (seule habilitée à porter plainte).
- Le responsable sécurité du site.
- Un CERT (Computer Emergency Response Team)
- Une plainte pourra être déposée en fonction de la nature et de la gravité de l'incident.

Installation/Administration

- Protection physique des équipements.
- Intégration des objectifs "sécurité" dans les choix de réseaux et des systèmes d'exploitation.
- Localiser et ne laisser ouvert que les services indispensables.
- Fermer les comptes inutilisés.

Installation/Administration

- Se tenir informer des vulnérabilités.
- Passer régulièrement les correctifs.
- Installer les outils nécessaires (contrôle d'authentification, audits, ...)
- Consulter régulièrement le journal généré par ces outils.
- Informer ses utilisateurs.
- Chiffrement des informations
- etc

Conclusion

- Aucune sécurité n'est parfaite. On définit juste un seuil.
- Des outils sont nécessaires, mais le travail quotidien est indispensable.
- Le niveau de sécurité d'un site est celui de son maillon le plus faible.
- La sécurité n'apporte qu'un gain indirect. Par conséquent, il n'est pas facile de convaincre les décideurs de l'entreprise.

Conclusion

- Le seul système informatique qui est vraiment sûr est un système éteint et débranché, enfermé dans un blockhaus sous terre, entouré par des gaz mortels et des gardiens hautement payés et armés. Même dans ces conditions, je ne parierais pas ma vie dessus.
    - (c) Gene Spafford, fondateur et directeur du "Computer Operations, Audit and Security Technology Laboratory.