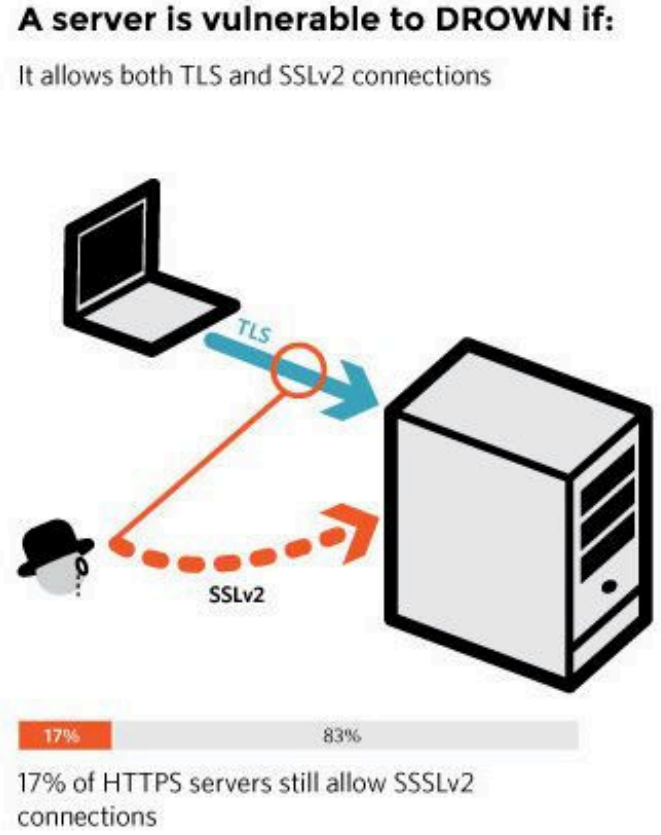
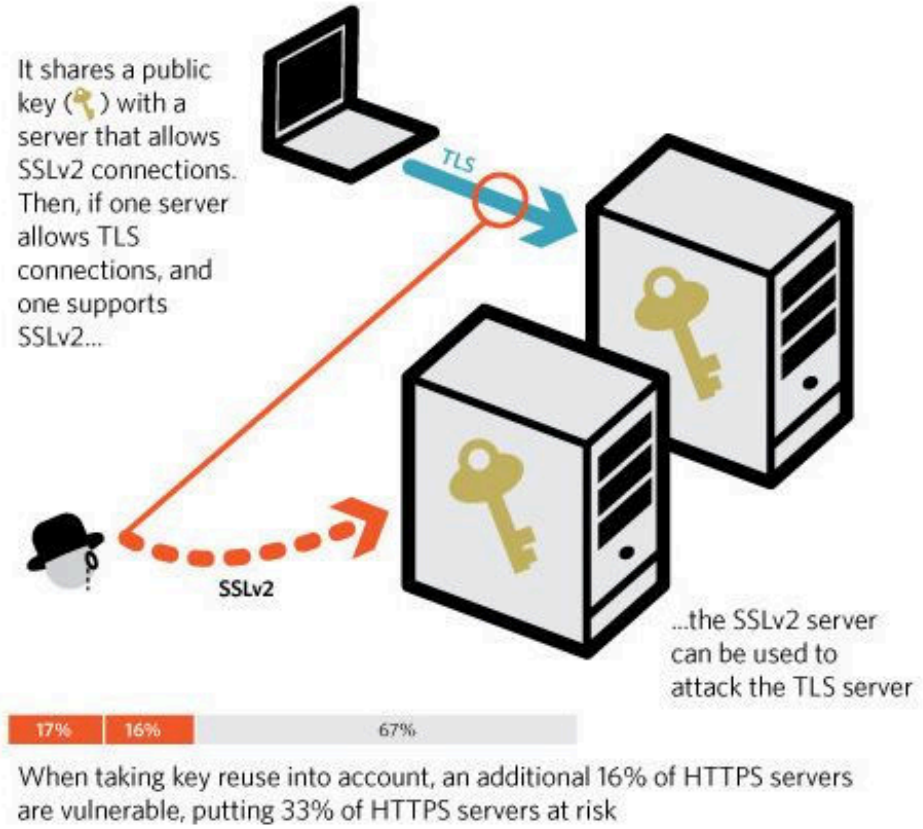
Faille HTTPS des serveurs (3 mars 16)

1. observer plusieurs centaines de connexions TLS entre une victime et un serveur vulnérable (période de monitoring)
2. connexion serveur via SSL v2, envoyer des msg de connexion spécifiques sur la base des cryptogrammes RSA
3. la réponse du serveur à ces tentatives d'accès permet à l'assaillant de déduire la clef privée employée par le client lors de ses connexions TLS.





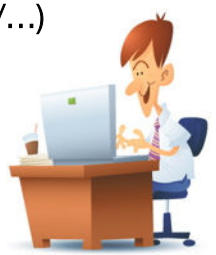
Injection de code – côté client

- XSS dépendant de la technologie de script mais la vulnérabilité concerne toutes les technologies usuelles :
  - JavaScript,
  - ActiveX,
  - Flash,
  - VBscript, ..
- Les conséquences sont importantes
  - Désagrément à l'utilisateur
  - Compromission complète de son compte
    - Vol d'informations, usurpation d'identité, détournement de session
  - Installation de Cheval de Troie
  - Modification d'informations importantes par la modification de l'interprétation d.une page web
    - Communiqué de presse influant le cours de l'action
    - Diffusion de rumeurs sur l'entreprise X

Scénario par XSS

Vol de cookie par Cross-site scripting

(1) Envoi d'un e-mail/message sur un forum/… contenant un code JavaScript malicieux (image/lien/…)



(4) Le code malicieux s'exécute (récupération du cookie envoyé par mail)

(3) Le serveur attribue un cookie au client

(5) Le pirate récupère le cookie et accède au serveur de manière authentifiée avec les droits de l'utilisateur

(2) La victime s'authentifie sur le serveur HTTP/webmail/… et accède au mail/message/…

Scénario par XREF

Exécution à distance par Cross-site request forgery [CSRF]

Scénario par PDF

PDF Attack

(1) Création du fichier PDF malicieux

(3) Envoie d'un e-mail

(phishing ou en pièce jointe)

(5) Ouverture et exécution du code malicieux

(6) Création d'un reverse shell

(2) Stockage sur un serveur public

(7) Rebond

persistence

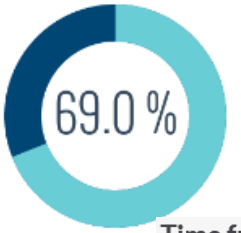
exfiltration

(4) récupération

JavaScript (Java, C#, VB.NET, Vala, Objective C, Eiffel, Python, Ruby, C++, Ada, PHP, Smalltalk, LOGO, AS3…)

APT et défis de la sécurité

- **Signification :** Au sens large, une APT est une catégorie d'attaques mettant en oeuvre de nombreuses techniques d'attaques (injection SQL, XSS, PDF, virus, phishing etc ...).
- **Advanced** : Attaque dite "avancée" au sens où elle utilise tout un arsenal de techniques d'attaques et d'outils pour atteindre son objectif.
- **Persistent :** Attaque basée sur une stratégie dont l'objectif est de rester le plus longtemps possible sans éveiller les soupçons (furtivité), par opposition une attaque "opportuniste".
- **Threat :** C'est bien sûr une menace, elle implique une coordination de moyens techniques et humains.



Des victimes découvrent l'attaque par une source externe

70-90%

Des échantillons de malware
- sont uniques
- ciblés par entreprise

- **Des effets importants et finalement peu visibles**
  - ✓ Une atteinte directe à la confidentialité
  - ✓ Rarement à la disponibilité et à l'intégrité, ce qui diffère des crises traditionnelles
  - ✓ Une détection bien après le démarrage de l'attaque et souvent par des tiers

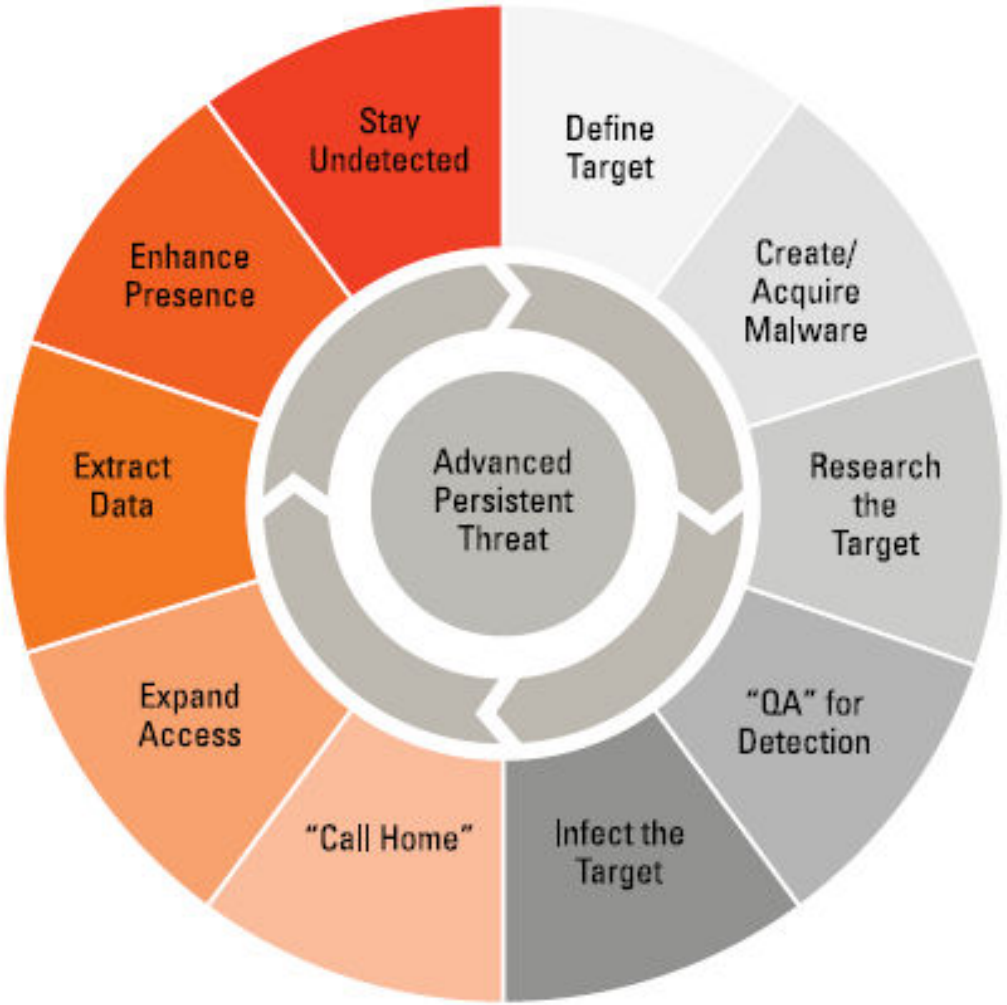
Target

TV5 Monde

RSA

APT : cycle de vie

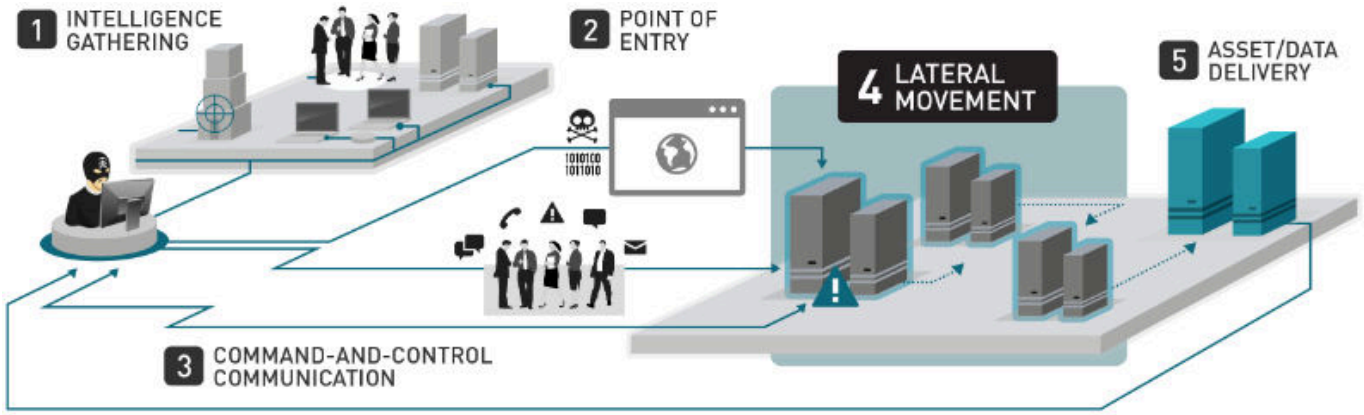
- Préparation de l'attaque et des objectifs
- Elaboration de la stratégie d'attaque
- Intrusion furtive dans l'infrastructure de la cible
- Repérage et état des lieux de l'écosystème cible (scan, capture réseau, etc.)
- Compromission de systèmes, récupération d'identifiant, de comptes,d'adresse
- Exécution de code (backdoors, chevaux de Troie, proxy, etc.) et déploiement d'outils (ex. RAT, kits etc.)
- Recherche de nouvelles cibles & développement de codes malveillants ciblés
- Utilisation de privilèges obtenus pour accéder aux données
- Exfiltration des données (protocoles légitimes, emails, covert-channels)



Mouvement Latéral

- **Reconnaissances** « dans le réseau » pour se déplacer latéralement au sein du réseau corrompu et maintenir une présence persistante sans être détecté, les attaquants obtiennent des informations : hiérarchie du réseau, des services utilisés dans les serveurs et les type de systèmes d'exploitation ce qui précise les actifs à cibler.
- Ils peuvent utiliser ces informations « à la carte » et acquérir des renseignements au sujet de leur prochain mouvement afin d'éviter le repérage.
- Les attaquants peuvent également recueillir des informations d'**authentifications** pour se connecter dans les systèmes, les serveurs et les commutateurs.
- Les outils de contrôle à distance permettent aux pirates d'accéder à d'autres postes de travail dans le réseau et **effectuer des actions** comme l'exécution de programmes, la planification des tâches, et la gestion des collections de données sur d'autres systèmes.

HIGH LATERAL MOVEMENT	LOW LATERAL MOVEMENT
CVE-2015-0117: IBM Domino CVE-2015-0117 Arbitrary Code Execution Vulnerability	CVE-2015-1155: Apple Safari CVE-2015-1155 Information Disclosure Vulnerability
CVE-2015-2545: Microsoft Office CVE-2015-2545 Remote Code Execution Vulnerability	CVE-2015-5737: FortiClient CVE-2015-5737 Multiple Local Information Disclosure Vulnerabilities



source : trendmicro

contrôlée

Evolution ?

OWASP
The Open Web Application Security Project

OWASP Top 10 – 2010 (Previous)	OWASP Top 10 – 2013 (New)
A1 – Injection	A1 – Injection
A3 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A2 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References	A4 – Insecure Direct Object References
A6 – Security Misconfiguration	A5 – Security Misconfiguration
A7 – Insecure Cryptographic Stora	e
A8 – Failure to Restrict URL Access	Access Control
A5 – Cross-Site Request Forgery (C	gery (CSRF)
<buried in A6: Security Misconfigu	le Components
A10 – Unvalidated Redirects and F	s and Forwards
A9 – Insufficient Transport Layer P	new 2013-A6

OWASP Top 10 - 2016 Data Call Announcement

Public Notice: The OWASP Top 10 project is launching its effort to update the Top 10 again. The current version was released in 2013, so this update is expected to be the 2016 or more likely 2017 release. This time around, we are making an open data call so any organization with a broad set of application vulnerability statistics can contribute their data to the project. To make it easier for the project to consume this contributed data, we are requesting it be provided via a Google form.

DEADLINE: Data must be submitted by July 20, 2016 (Extended to July 31).

OWASP Top 10 2017

Release Candidate 2

TELECOM Evolution

OWASP Top 10 2013	±	OWASP Top 10 2017
A1 – Injection	→	A1:2017 – Injection
A2 – Broken Authentication and Session Management	→	A2:2017 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)	↘	A3:2013 – Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017 – XML External Entity (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017 – Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017 – Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017 – Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017 – Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017 – Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017 – Insufficient Logging & Monitoring [NEW, Comm.]

- Le Top 10 de l'OWASP a dû changer.
- OWASP Top 10 a complètement été refaçonné, la méthodologie réorganisé, un nouveau processus sur les données, un grand travaille avec la communauté
- Nos risques ont été réorganisés, chaque risque réécrit à partir de zéro et des références ajouté aux cadres et langages qui sont maintenant couramment utilisés.

Un web defacement

Defacement : archives…

zone-h unrestricted information

Home | News | Events | Archive | Archive ★ | Onhold | Notify | Stats | Register | Login | search...

NOTIFIER DOMAIN .fr

Special defacements only ☑ Fulltext/Wildcard ☑ Onhold (Unpublished) only ☑

Date : ALL Apply filter

Total notifications: **157** of which **157** single ip and **0** mass defacements

Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
L - IP address location
★ - Special defacement (special defacements are important websites)

We don't accept notifications through email, IP address notifications, notifications with fake and/or created subdomains by notifier or with wrong attack methods selected.

Time	Notifier	H	M	R	L	★	Domain	OS	View
2014/01/07	SultanHaikal			R		★	ville-lempdes.fr/images/s.txt	Unknown	mirror
2013/12/19	UTEPA					★	www.math.univ-toulouse.fr/cere...	Linux	mirror
2013/12/15	G4eL			R		★	ville-montivilliers.fr/library...	Unknown	mirror
2013/12/14	HighTech			R		★	www.cc-sauxillanges.fr/ck.htm	Unknown	mirror
2013/12/12	Over-X					★	www.polynesie-francaise.biep.g...	Linux	mirror
2013/12/12	Over-X					★	www.corse.biep.fonction-publiq...	Linux	mirror
2013/12/12	Over-X					★	www.auvergne.biep.fonction-pub...	Linux	mirror
2013/12/12	Over-X					★	www.antilles-guyane.biep.fonct...	Linux	mirror
2013/12/12	Over-X					★	www.picardie.biep.fonction-pub...	Linux	mirror
2013/12/12	Over-X					★	www.polynesie-francaise.biep.f...	Linux	mirror
2013/12/12	Over-X					★	www.limousin.biep.fonction-pub...	Linux	mirror
2013/12/12	Over-X					★	www.rhone-alpes.biep.fonction-...	Linux	mirror
2013/12/12	Over-X					★	www.alsace.biep.fonction-publi...	Linux	mirror
2013/12/12	Over-X					★	www.midi-pyrenees.biep.fonctio...	Linux	mirror
2013/12/12	Over-X					★	www.centre.biep.fonction-publi...	Linux	mirror
2013/12/12	Over-X					★	www.centre.biep.gouv.fr/common...	Linux	mirror
2013/12/12	Over-X					★	www.ile-de-france.biep.gouv.fr...	Linux	mirror

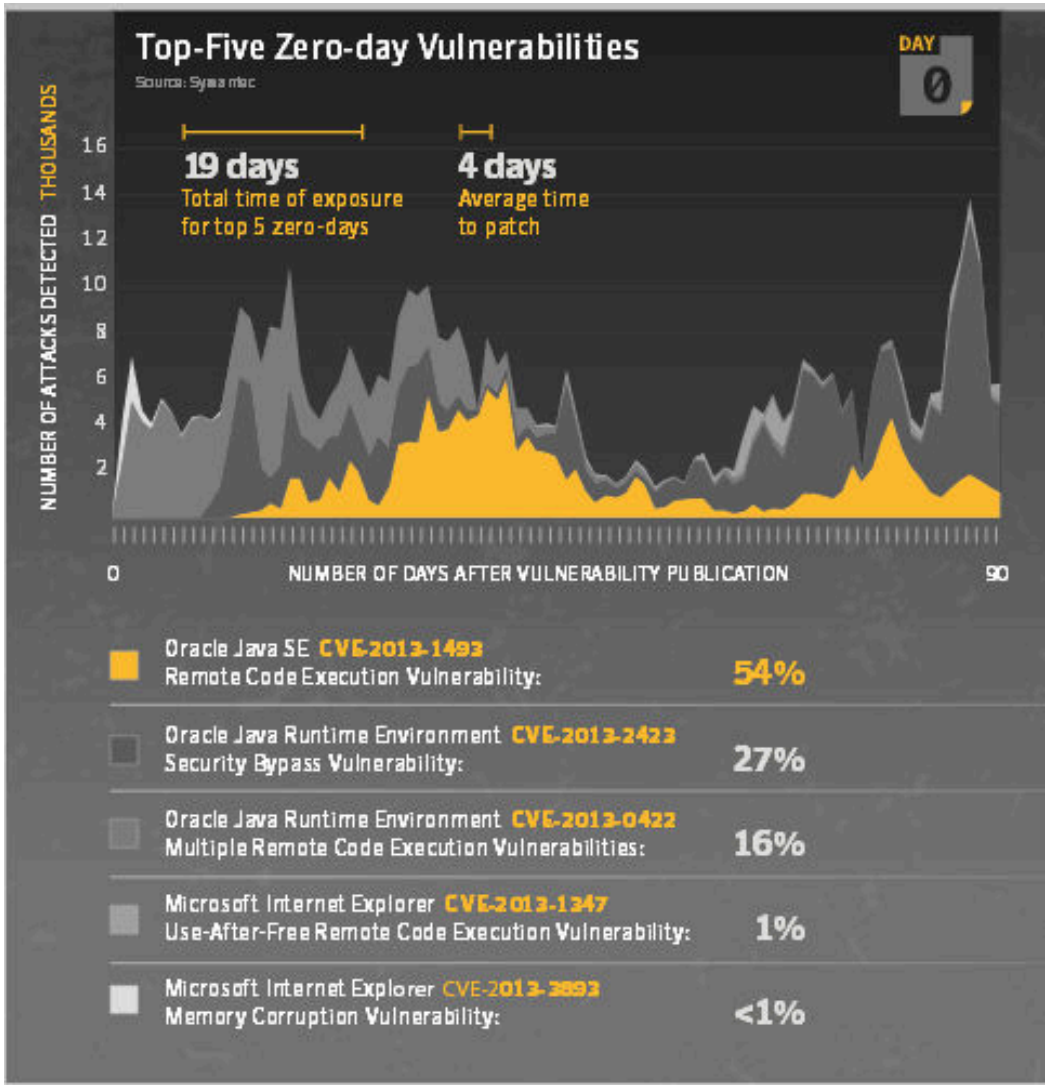
- Source : zone-h.org

0-days : les navigateurs en danger

- Multiplication des attaques 0-Days
  - Non détectées pendant une durée moyenne d'une année !
  - Attaques discrètes pour ne pas être découvertes
  - Dès la publication, les attaques se multiplient par un facteur 100 au mieux ou 100.000 dans le pire des cas
- Faille Google Chrome
  - Ucha Gobejishvili, pirate géorgien, indique avoir trouver une faille critique dans Chrome en juillet 2012. Google demande la preuve, qui n'est pas fournie malgré une prime de 60.000 $
- Microsoft confirme une faille 0-day sur Internet Explorer
  - Les version 6,7 et 8 sont concernées
  - Permet de prendre le contrôle de la mémoire

0 Days : Vulnérabilités

- vulnérabilités qui ont été identifiés comme zéro-jour en 2013 et fréquemment exploitées.
- Pour réduire la «surface d'attaque», les entreprises doivent s'assurer qu'elles fonctionnent avec les dernières versions logicielles
- Utilisation d'un scanner de vulnérabilité pour identifier les applications non patchées
- Pour certaines vulnérabilités zero-day, il y avait une plus grande quantité d'activité malveillante très tôt après publication, une indication d'exploits étant disponibles avant que la vulnérabilité soit documenté.



Source : http://www.symantec.com

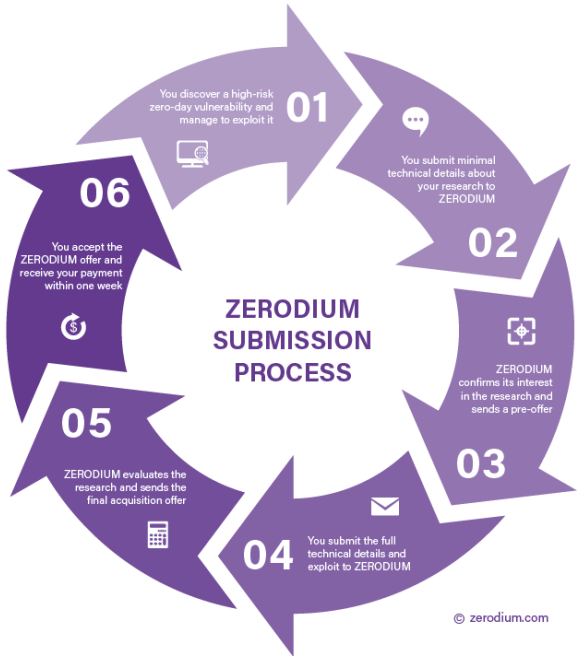
Tarification des 0-Days logiciel et systèmes

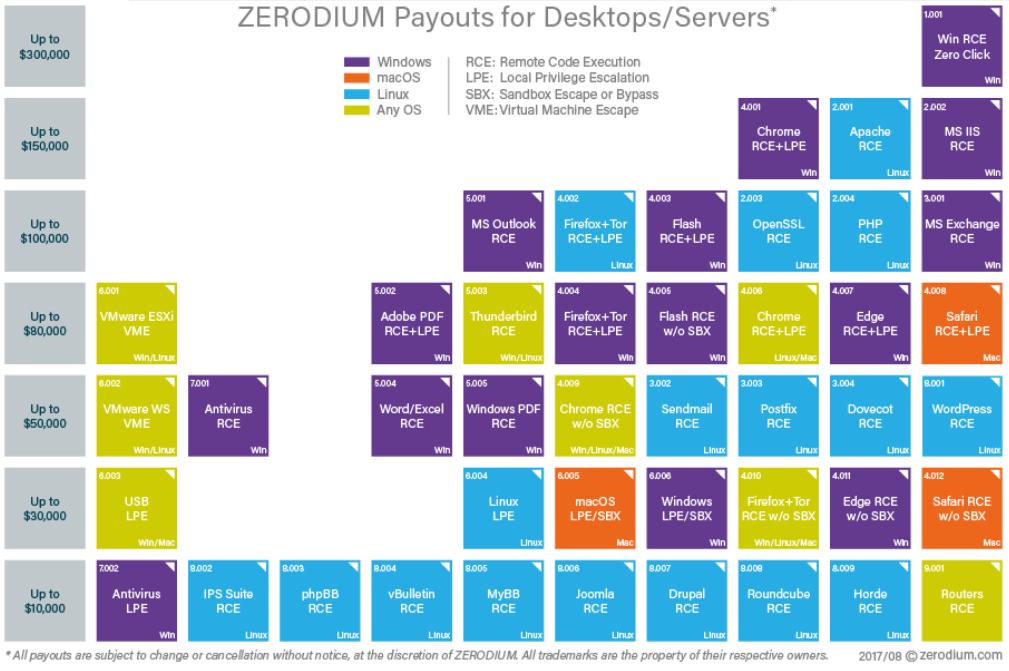
- Tarifs qui dépendent
  - de la complexité de la cible et de sa surface d'attaque
  - de l'acheteur
- Prix des vulnérabilités :
- Plus le nombre de vulnérabilités est faible, plus le prix augmente…
- Entre 500 et 40,000 $ en moyenne pour les failles 0-day
- Exemple :
  - OS Commerce : 2,000 $
  - Microsoft Office: 15,000 $
  - Piratage de compte iCloud: 17,000 $
  - Record de l'année 2015 avec Zerodium et une faille i0S 9.1/9.2b à 1,000,000 $
  - Janvier 2016 : prime de 100,000 $ pour un exploit Flash devant contourner la sandbox de Flash Player et prendre à défaut une protection (heapisolation), récemment implémentée
- Un service de plus en plus professionnel : TheRealDeal / DeepDotWeb

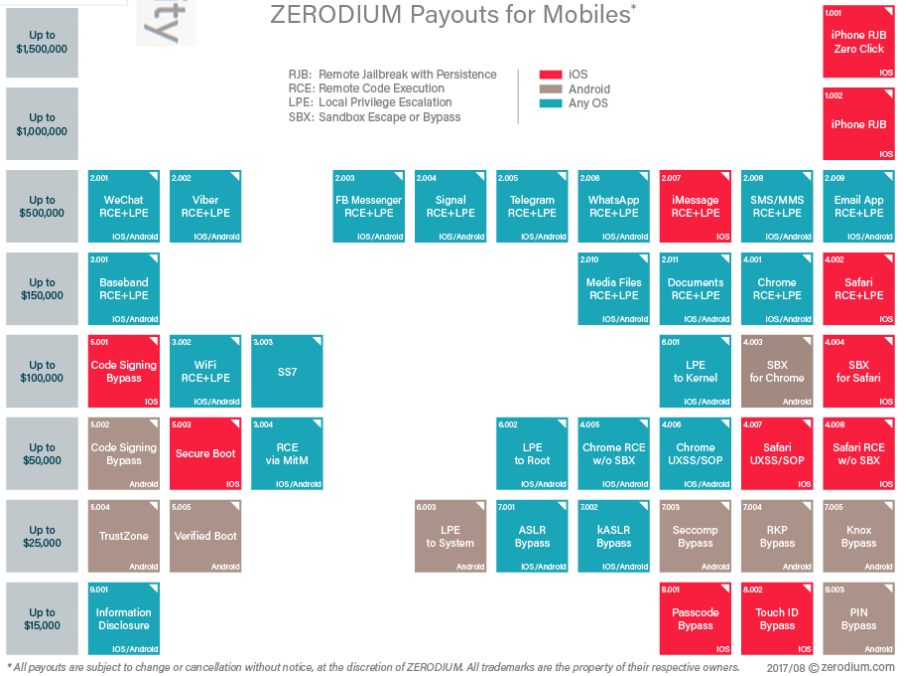
0-Day : Une Tarification officielle

Category	Examples	Applications that permit taking over a Google account [1]	Other highly sensitive applications [2]	Normal Google applications	Non-integrated acquisitions and other sandboxed or lower priority applications [3]
Vulnerabilities giving direct access to Google servers					
Remote code execution	*Command injection, deserialization bugs, sandbox escapes*	$31,337	$31,337	$31,337	$1,337 - $5,000
Unrestricted file system or database access	*Unsandboxed XXE, SQL injection*	$13,337	$13,337	$13,337	$1,337 - $5,000
Logic flaw bugs leaking or bypassing significant security controls	*Direct object reference, remote user impersonation*	$13,337	$7,500	$5,000	$500
Vulnerabilities giving access to client or authenticated session of the logged-in victim					
Execute code on the client	Web: *Cross-site scripting* Mobile / Hardware: *Code execution*	$7,500	$5,000	$3,133.7	$100
Other valid security vulnerabilities	Web: *CSRF, Clickjacking* Mobile / Hardware: *Information leak, privilege escalation*	$500 - $7,500	$500 - $5,000	$500 - $3,133.7	$100

Google Application Security







Evolution du marché des 0-day : Bug Bounty

Category	Examples	Applications that permit taking over a Google account [1]	Other highly sensitive applications [2]	Normal Google applications	Non-integrated acquisitions and other sandboxed or lower priority applications [3]
Vulnerabilities giving direct access to Google servers					
Remote code execution	*Command injection,*	$20,000	$20,000	$20,000	$1,337 - $5,000

- Bug bounty, un métier qui évolue **Des plateformes professionnelles de plus en plus reconnues**

- **Des primes qui explosent**
  - Mozilla => la prime maximale est passée de 3,000 à 10,000 $
  - Microsoft => jusqu'à 15,000 $ de prime pour une faille sur son nouveau navigateur Edge(programme de 3 mois avant son lancement)
  - United Airlines => jusqu'à 1,000,000 de points Miles sur ses vols comme primes
- **Et des sociétés de plus en plus hétérogènes**

Comprendre la Sécurité – dec 2018 - © Xa - diffusion contrôlée

Origine de failles de sécurité

- Défaut dans la conception de protocoles et applications
  - Pas de prise en compte de la sécurité lors de la conception…
- Défaut dans l'implémentation de ces protocoles
  - Erreurs de programmation (Dr. Wietse Venema : 1 bug / 1000 lignes de code)
  - Solaris 7 : 12 M° de ligne de code, 10% de code nouveau
  - Windows 2K : 40 M° de ligne de code, 50% de code nouveau (+100 M / W8)
  - Plus de complexité > Plus de code > plus d'erreurs > plus de vulnérabilités
- Défaut dans la configuration des systèmes et équipement réseaux
  - Peu ou pas de systèmes audités régulièrement
  - Un ensemble d'erreurs mineures peuvent entraîner un risque majeur

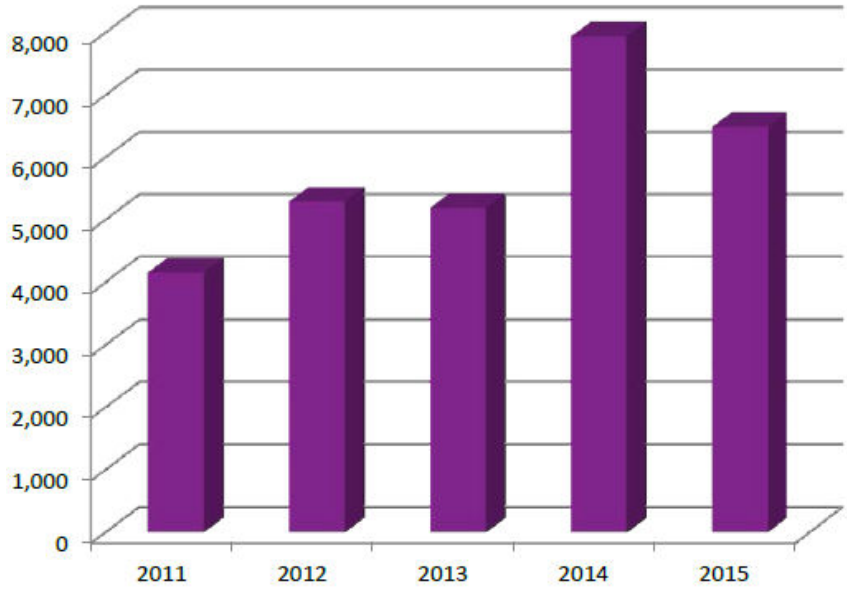
Year	Operating System	SLOC (Million)
1993	Windows NT 3.1	4-5[1]
1994	Windows NT 3.5	7-8[1]
1996	Windows NT 4.0	11-12[1]
2000	Windows 2000	more than 29[1]
2001	Windows XP	45[2][3]
2003	Windows Server 2003	50[1]

Operating System	SLOC (Million)
Debian 2.2	55-59[4][5]
Debian 3.0	104[5]
Debian 3.1	215[5]
Debian 4.0	283[5]
Debian 5.0	324[5]
OpenSolaris	9.7
FreeBSD	8.8
Mac OS X 10.4	86[6][n 1]
Linux kernel 2.6.0	5.2
Linux kernel 2.6.29	11.0
Linux kernel 2.6.32	12.6[7]
Linux kernel 2.6.35	13.5[8]
Linux kernel 3.6	15.9[9]

en.wikipedia.org/wiki/Source_lines_of_code

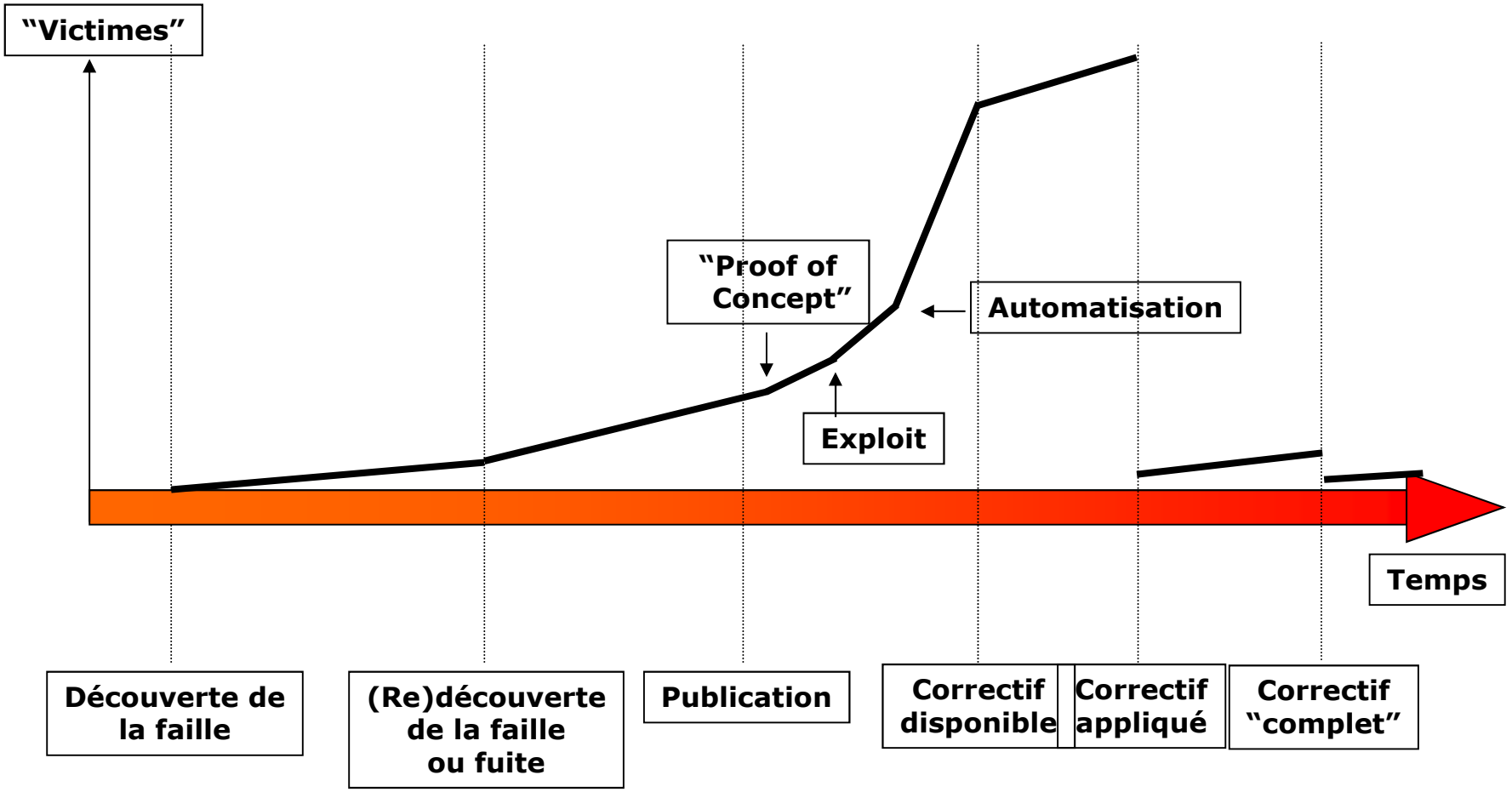
Vulnérabilités (Sécurité Informatique)

- En sécurité informatique, une vulnérabilité est une faiblesse qui permet à un attaquant de réduire l' « assurance d'un système » . La vulnérabilité est l'intersection de trois éléments:
  - ✓ Une susceptibilité ou un défaut du système,
  - ✓ l'accès de l'attaquant à la faille,
  - ✓ la capacité de l'attaquant d'exploiter la faille
- Pour exploiter une vulnérabilité, un attaquant doit disposer d'au moins un outil ou une technique applicable qui peut se connecter à la faiblesse du système. Dans ce cadre, la vulnérabilité est également connue comme la surface d'attaque.
- Vulnérabilités sans risque: par exemple, lorsque l'actif concerné n'a pas de valeur.
- Une vulnérabilité avec un ou plusieurs cas de travail connus et des attaques pleinement mis en œuvre est classée comme une vulnérabilité exploitable - une vulnérabilité pour laquelle un exploit existe



Cycle de vie d'une vulnérabilité

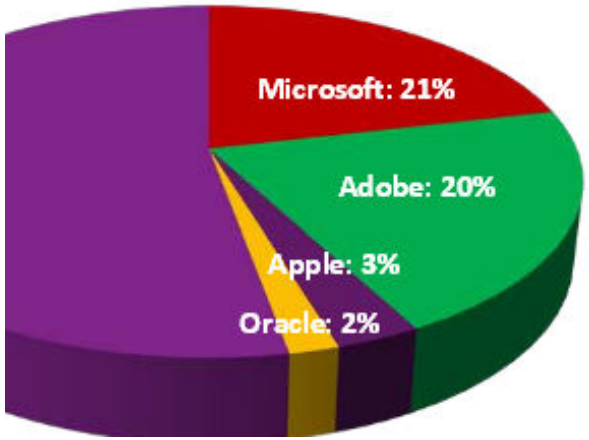
Source : www.securite.org

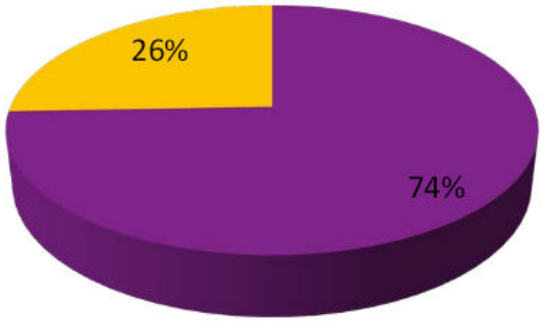


Les meilleurs vulnérabilités en kits du moment

- Populaire en raison de la compatibilité entre les différents navigateurs et systèmes d'exploitation

Source : RSA Conference



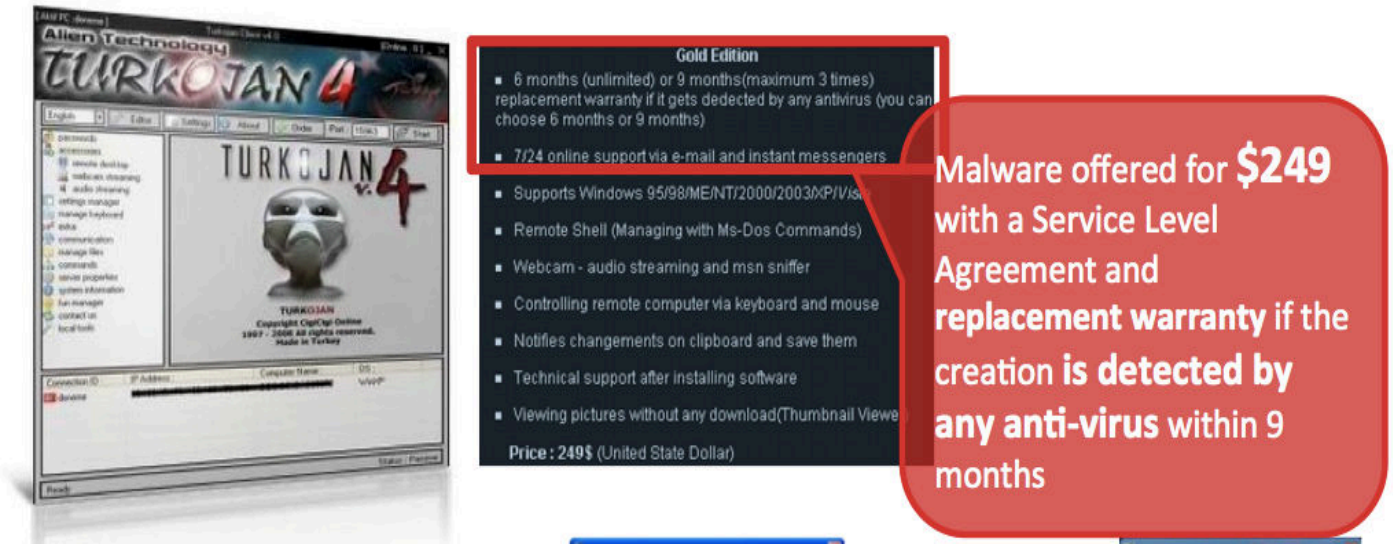


Exemples de « Exploit Framework »

- Les « Exploit kits » boîtes à outils qui sont utilisés dans le but de propager des logiciels malveillants.
  Ils automatisent l'exploitation de la plupart des vulnérabilités côté client, ils viennent avec un code d'exploitation pré-écrit et l'utilisateur du kit n'a pas besoin d'avoir une expérience / compétences sur les Vulnérabilités ou Exploits.
- Un exploit, d'autre part, tente de transformer une vulnérabilité (une faiblesse) en une réelle façon de corrompre un système.

Le Malware : le logiciel traditionnel

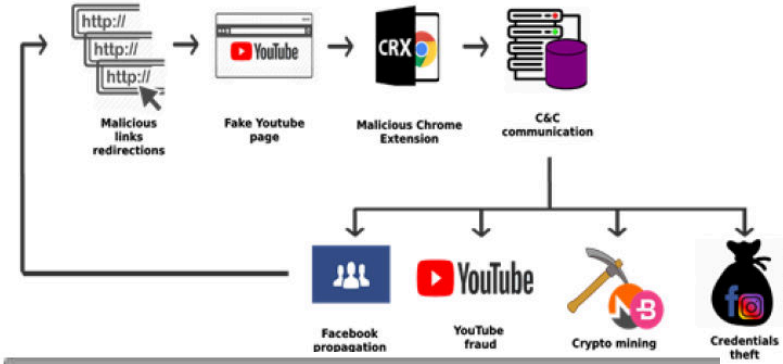
- Malware, abréviation de logiciels malveillants, est un logiciel utilisé pour perturber les opérations informatiques, collecter des informations sensibles, avoir accès à des systèmes informatiques privés,
- La première catégorie de la propagation de logiciels malveillants concerne des fragments de logiciels parasites qui se fixent à un contenu exécutable existant. Le fragment peut être un code machine qui infecte une application, utilitaire existant, ou d'un programme de système, ou même le code utilisé pour démarrer un système informatique.
- Les logiciels malveillants peuvent être furtif, destiné à voler des informations ou espionner les utilisateurs d'ordinateurs pour une période prolongée à leur insu, comme par exemple le Regin, ou il peut être conçu pour causer des dommages, souvent comme le sabotage (par exemple, Stuxnet), ou pour extorquer de l'argent (cryptolocker).

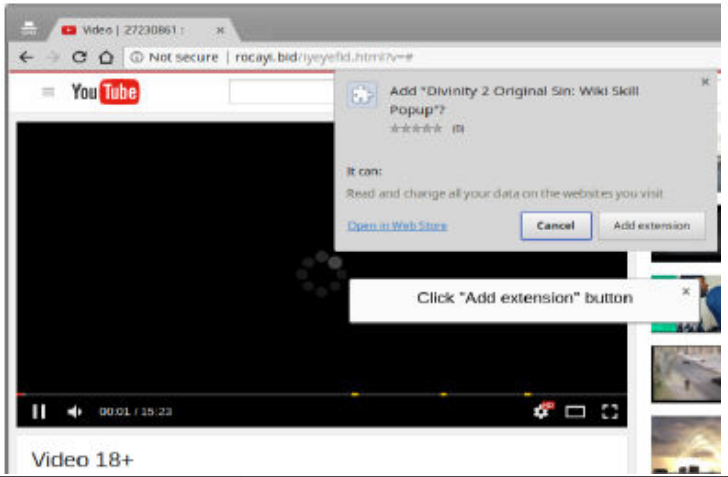


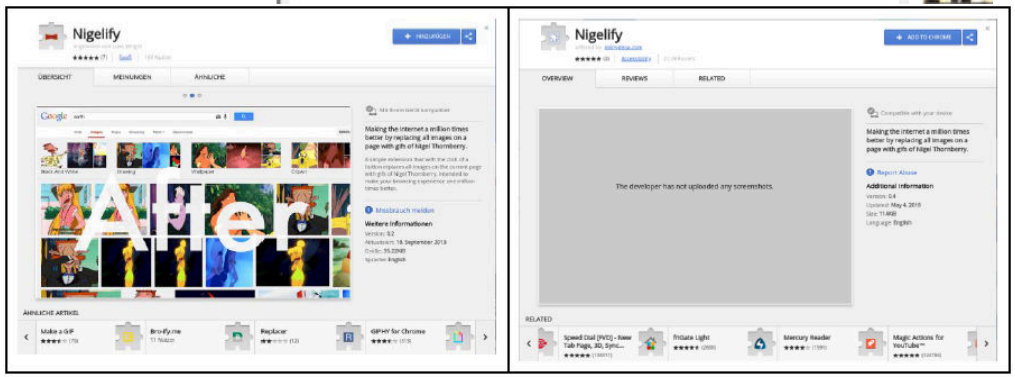
usion contrôlée

Exploit NigelThorn malware – mai 2018

- Campagne malveillante se propage via des liens socialement conçus sur Facebook et infecte les utilisateurs en abusant d'une extension Google Chrome (l'application 'Nigelify') qui effectue des vols d'informations d'identification, cryptomining, fraude aux clics et plus encore.
- Le groupe est actif depuis au moins mars 2018 et qu'il a déjà infecté plus de 100 000 utilisateurs dans plus de 100 pays
- Le logiciel malveillant redirige les victimes vers une fausse page YouTube et demande à l'utilisateur d'installer une extension Chrome pour lire la vidéo.
- l'extension malveillante installée la machine fait partie du botnet. Le logiciel malveillant dépend de Chrome Windows et Linux, les autres navigateurs ne sont pas exposés.
- Pour contourner les outils de validation des applications Google les opérateurs de campagne ont créé des copies d'extensions légitimes et injecté un script malveillant dissimulé pour lancer et gérer l'opération de détection de logiciels malveillants.
- La version légitime à gauche, version malveillante à droite, l'extension installe un JavaScript malveillant est exécuté et télécharge la configuration initiale - un ensemble de demandes est déployé, chacune avec son propre but et ses propres déclencheurs.
- Le malware est axé sur le vol des identifiants de connexion Facebook et des cookies Instagram
- Les jetons d'accès Facebook des utilisateurs authentifiés sont générés et la phase de propagation commence. Le logiciel malveillant collecte des informations de compte pertinentes dans le but de diffuser le lien malveillant sur le réseau de l'utilisateur.







Source : https://security.radware.com/malware/nigelthorn-malware/

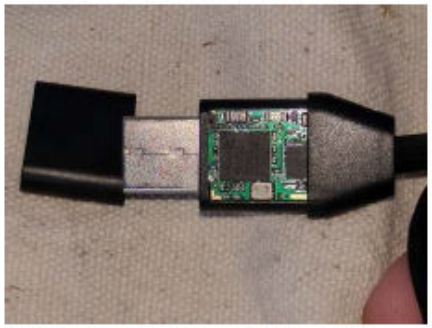
Virus & Ver

- Un virus est un logiciel qui à pour principales caractéristiques de se propager localement en ce recopiant sur le poste infecté : disque, mémoire, clé USB, …
- L'infection est déclenché par une action volontaire de l'utilisateur, il est présenté comme un programme « légitime » : utilitaire, ludique, …
- Une fois installé sur la machine, un virus met en œuvre une charge finale : action pour lesquelles il a été développé :
  - Envoi de SPAM
  - Attaque par Dénie de Service
  - Effacement de fichiers
  - Blocage de la machine
- Un ver est un programme autoreproducteur qui se propage sur un réseau.
- Contrairement au virus, l'infection de la machine ne nécessite pas d'action de la part de l'utilisateur. Le vers exploite une vulnérabilité ou une faille sur les logiciels présents sur la machine
- Une fois installé le ver se comporte très souvent comme un virus

Cheveaux de Troie & Keylogger

- Un cheval de Troie
- logiciel d'apparence légitime, conçu pour exécuter des actions à l'insu de l'utilisateur. En général, il utilise les droits appartenant à son environnement pour détourner, diffuser ou détruire des informations, ou encore pour ouvrir une porte dérobée
- La principale différence entre les virus, les vers et les chevaux de Troie est que ces derniers ne se répliquent pas.
- keylogger est un un logiciel espion ou un périphérique qui espionne électroniquement l'utilisateur d'un ordinateur. Le but de cet outil est varié, et peut se présenter sous des airs de légitimité, mais il ne peut être assuré qu'en espionnant l'intimité informatique de l'utilisateur.
- Le terme *keylogger* est parfois utilisé pour parler de l'espionnage des périphériques d'entrée/sortie, bien que ces espions puissent être nommés spécifiquement en fonction du périphérique visé, comme les *mouseloggers* pour la souris.

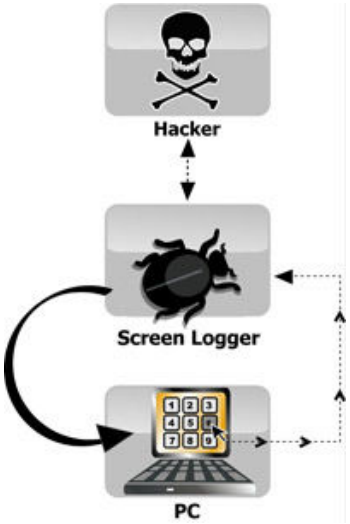





Comprendre la Sécurité – dec 2018 - © Xa - diffusion contrôlée

Screenlogger / AdWare et SpyWare

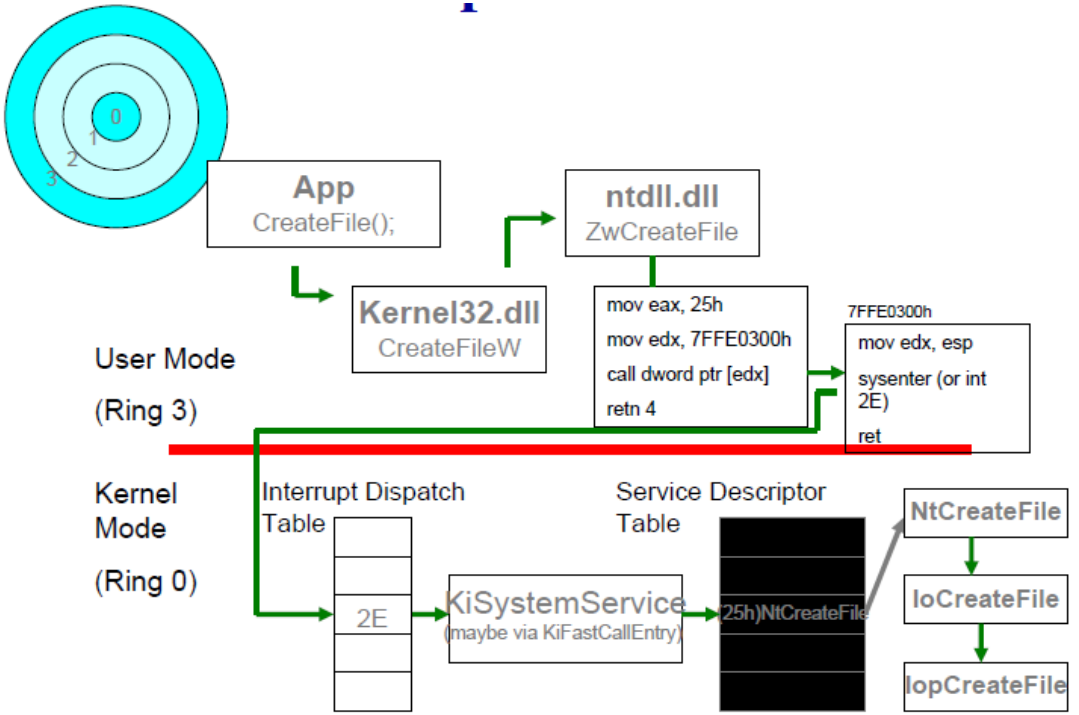
- Un screenlogger est un logiciel qui surveille les entrées et les portions de l'écran de l'utilisateur
  - Pour lutter contre les keyloggers, les sites bancaires notamment utilisent des claviers virtuels. L'utilisateur n'utilise plus sont clavier, mais sa souris pour saisir les paramètres de connexion.
  - Pour contourner ces « contre-mesures » les pirates disposent de screenloggers qui sont capables de capturer ce qui s'affiche à l'écran lorsque l'internaute est sur le site « sécurisé ».
  - Les captures d'écran sont ensuite envoyées sur un site contrôlé par le pirate.
- Un AdWare (Advertising Software) est un logiciel qui affiche des publicités en échange d'un service / fct
  - Un AdWare est considéré comme nuisible dès lors qu'il s'installe à l'insu de l'utilisateur ou qu'il permet le téléchargement de contenus non sollicités ou non souhaités.
- Un SpyWare (Spying Software) est un logiciel espion qui recueille à l'insu de l'utilisateur, des informations sur sa navigation Internet. Ces informations sont envoyées à des régies publicitaires pour des opérations de mailing ciblés ou des affichages de bandeaux publicitaires en fonction du profil de l'utilisateur.



Comprendre la Sécurité – dec 2018 - © Xa - diffusion contrôlée

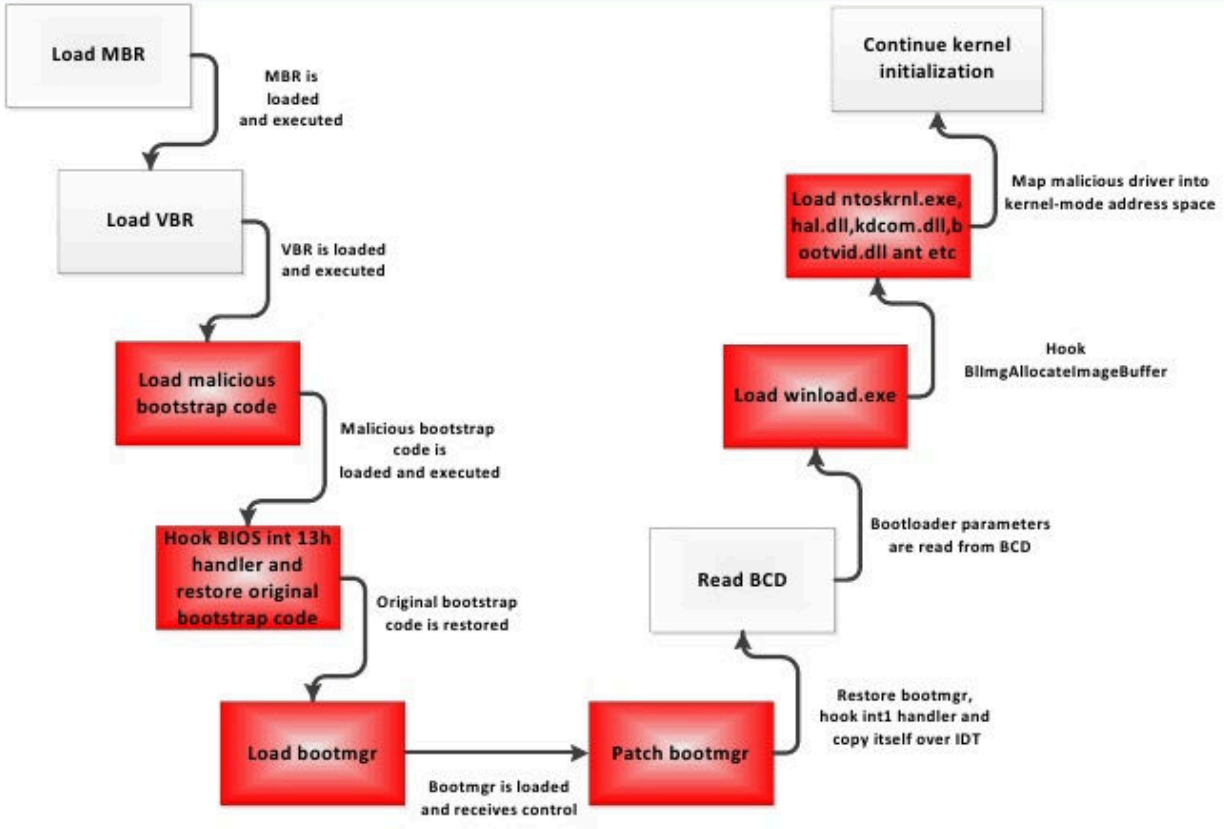
Rootkit

- La « boite à outil » du pirate
- Installation automatique sur la cible
- Un rootkit peut s'installer dans un autre logiciel, une bibliothèque ou dans le noyau d'un système d'exploitation. Certains peuvent modifier l'hyperviseur fonctionnant au-dessus des systèmes ou le micrologiciel intégré dans un matériel.
- Fonctions
  - Masque les activités du pirates
  - Mets en place des backdoors
  - Sécurise le système (!)
  - Maintenir la présence malveillante sur un système compromis
  - Fonctionnement possible en « machine virtuelle »



Bootkit

- Un bootkit est similaire à un rootkit, il sert à activer et maintenir un accès privilégié à un ordinateur tout en cachant activement sa présence d'administrateurs en renversant la fonctionnalité du système d'exploitation standard ou une autre application (Wiki)
- La principale différence est qu'une bootkit infecte la séquence de démarrage de l'ordinateur.

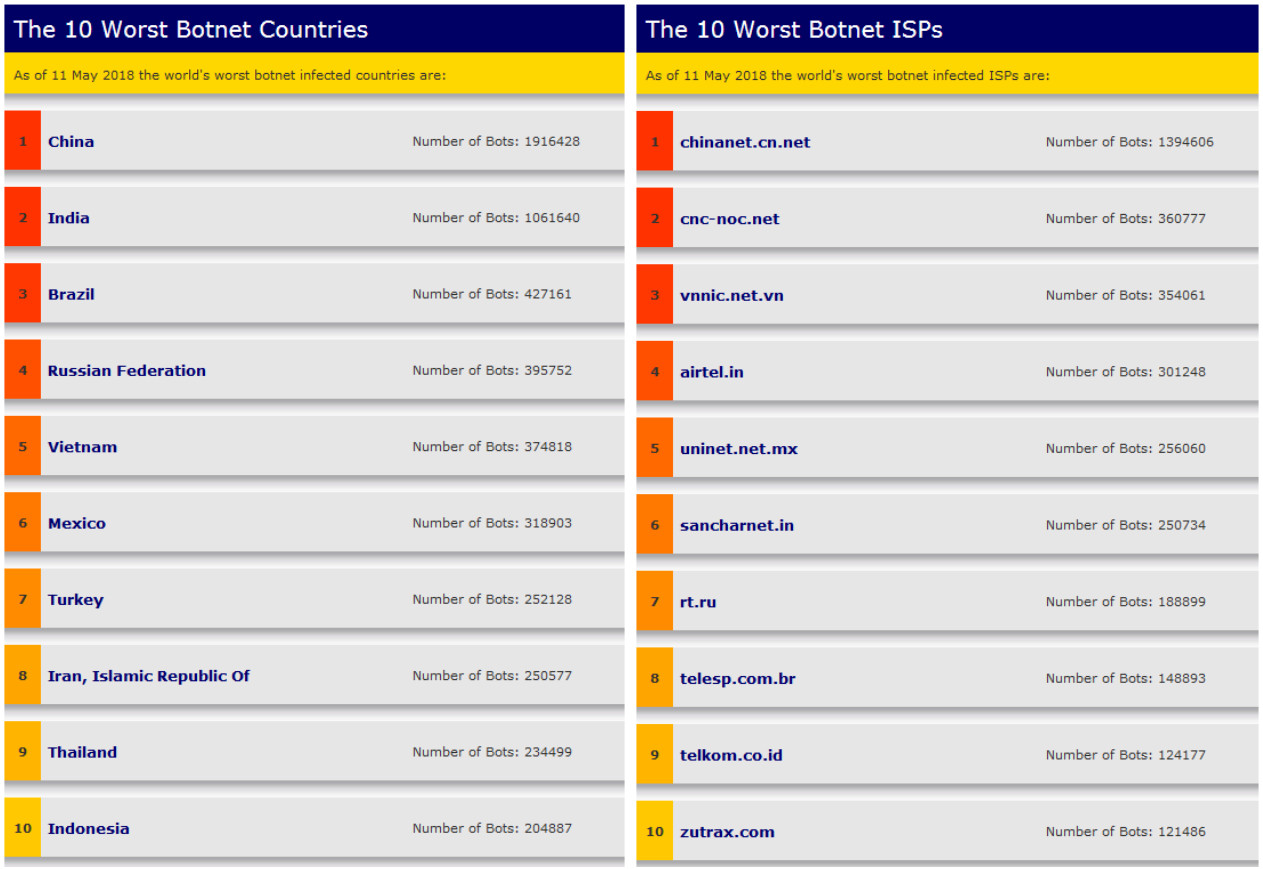


- Cela signifie qu'au lieu d'un rootkit commun qui représente un pilote dans le système, le code du bootkit est injecté dans le master boot record du disque dur, de sorte que le bootkit est plus difficile à détecter car il est exécuté avant le système d'exploitation et peut tout contrôler.
- La seule façon d'obtenir une véritable sécurité est d'avoir une solution matérielle qui est en mesure de prouver que la séquence de démarrage n'a pas être modifié.

Comprendre la Sécurité – dec 2018 - © Xa - diffusion contrôlée

Les Botnet

- Un botnet (de l'anglais, contraction de « robot » et « réseau ») est un réseau de bots informatiques, des programmes connectés à Internet qui communiquent avec d'autres programmes similaires pour l'exécution de certaines tâches.
- Le sens de botnet s'est étendu aux réseaux de machines zombies, utilisés pour des usages malveillants.
- Evolutions des menaces : du ver au Botnet
- Outil de frappe massive, nombreuses possibilités
  - SPAM
  - DoS/DDoS
  - Keylogger
  - Serials
  - Fake AV
  - Vol d'identité
  - …



The 10 Worst Botnet Countries

As of 11 May 2018 the world's worst botnet infected countries are:

1	China	Number of Bots: 1916428
2	India	Number of Bots: 1061640
3	Brazil	Number of Bots: 427161
4	Russian Federation	Number of Bots: 395752
5	Vietnam	Number of Bots: 374818
6	Mexico	Number of Bots: 318903
7	Turkey	Number of Bots: 252128
8	Iran, Islamic Republic Of	Number of Bots: 250577
9	Thailand	Number of Bots: 234499
10	Indonesia	Number of Bots: 204887

The 10 Worst Botnet ISPs

As of 11 May 2018 the world's worst botnet infected ISPs are:

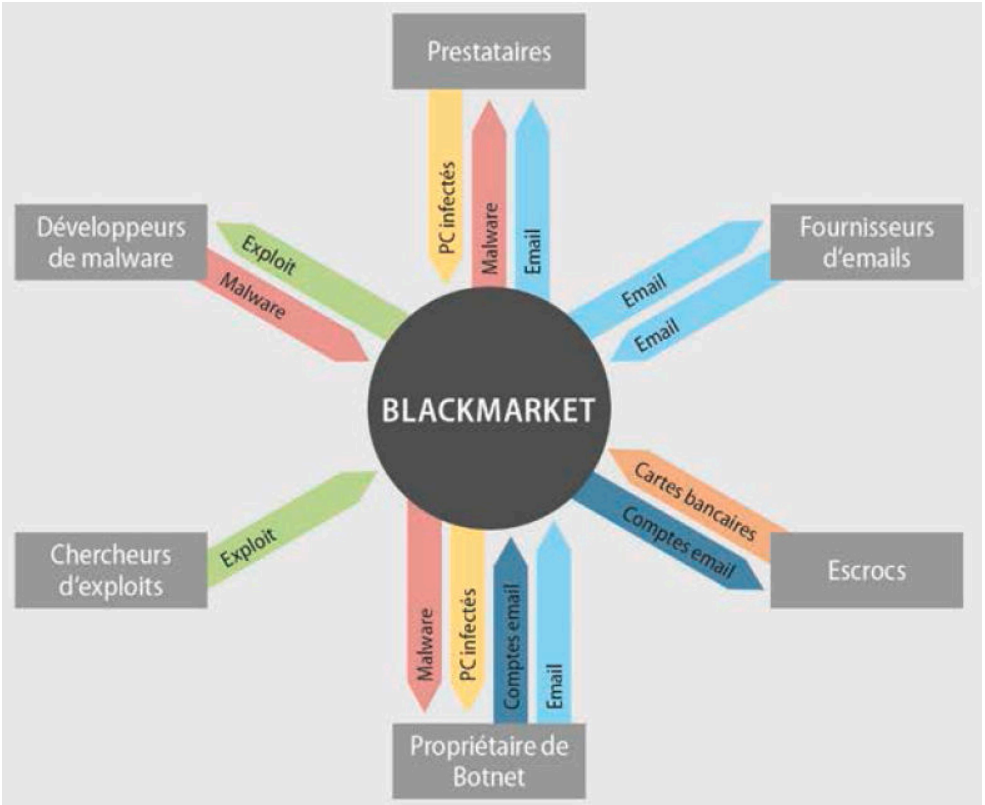
1	chinanet.cn.net	Number of Bots: 1394606
2	cnc-noc.net	Number of Bots: 360777
3	vnnic.net.vn	Number of Bots: 354061
4	airtel.in	Number of Bots: 301248
5	uninet.net.mx	Number of Bots: 256060
6	sancharnet.in	Number of Bots: 250734
7	rt.ru	Number of Bots: 188899
8	telesp.com.br	Number of Bots: 148893
9	telkom.co.id	Number of Bots: 124177
10	zutrax.com	Number of Bots: 121486

https://www.spamhaus.org/statistics/botnet-cc/

Écosystème du botnet

- En tant que système complexe, le botnet requiert **différentes compétences** et implique l'interaction de plusieurs intervenants qui commercent sur les places de marchés parallèles
- Les codes malveillants nécessaires à l'infection et au contrôle, c'est à ce niveau qu'interviennent les **programmeurs**.
- Des milliers de codes malveillants de tout type sont disponibles à l'achat sur les forums spécialisés
- **Diffuser** le code au plus grand nombre, sans compétence interne,faire appel à des services dédiés 20 et 100 € pour l'infection de 1000 ordinateurs
- Son propriétaire va alors pouvoir compter sur les données qu'ils renferment, en fonction de la qualité des internautes infectés, il va récupérer sur les machines **infectées les identifiants d'emails, de réseaux sociaux voire de comptes bancaires**

une vision limitée de l'écosystème cybercriminel global

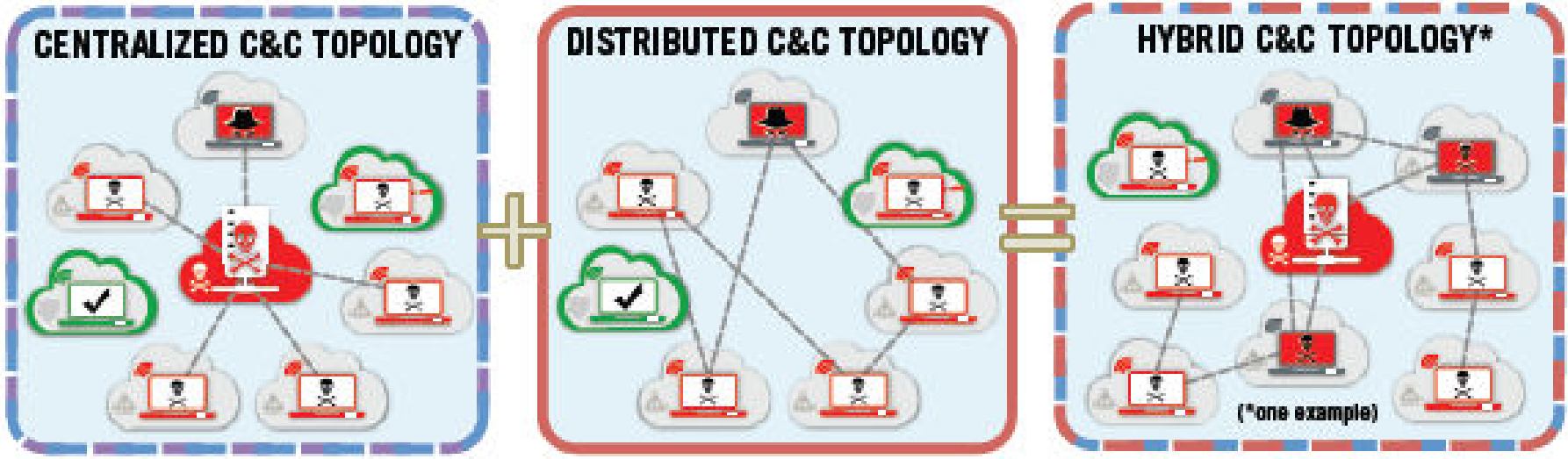


source : GDATA software AG

Botnet : protocoles de communication

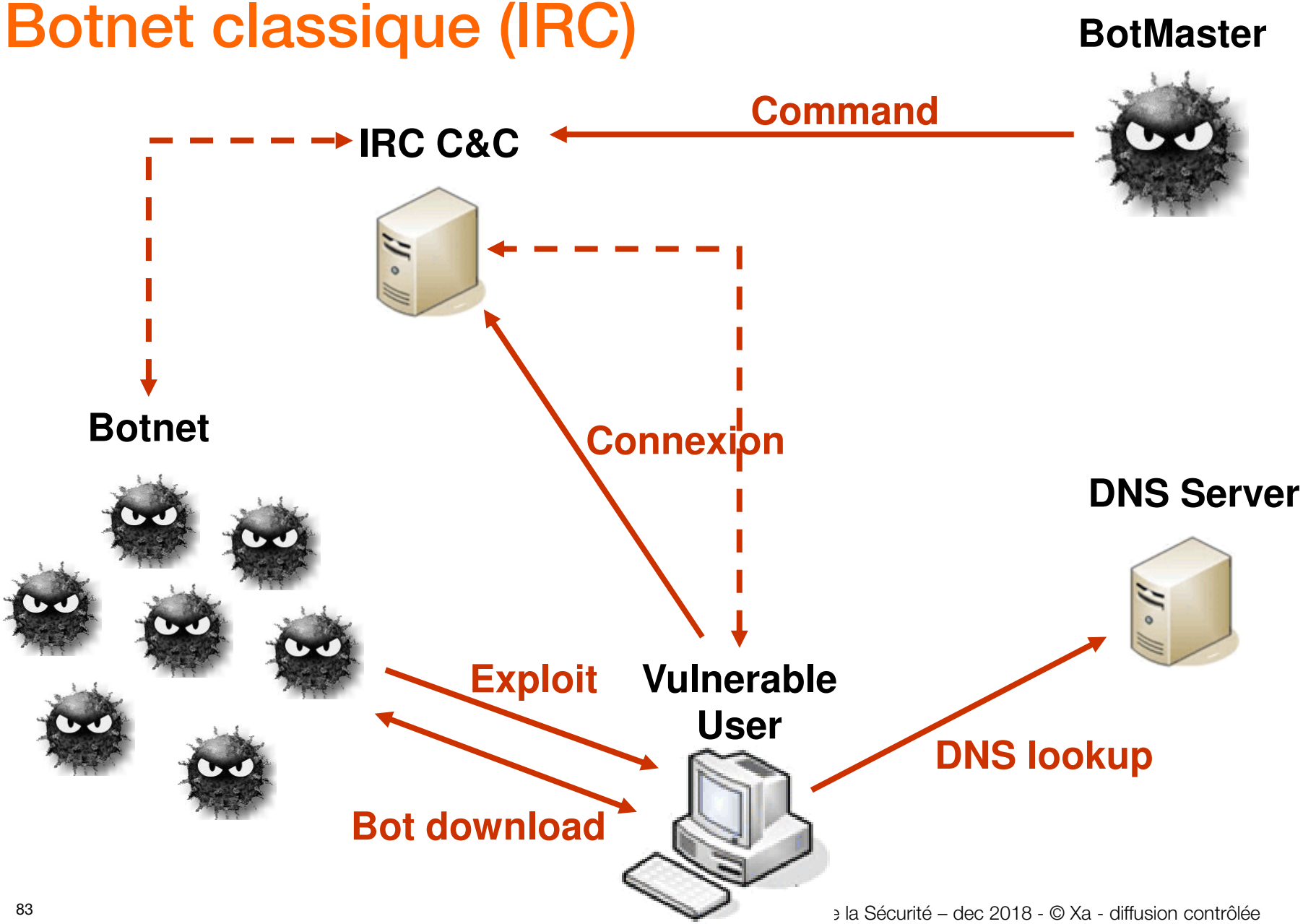
- IRC ("chat") ou HTTP ("Web") pour un topologie centralisée,
- P2P ("de partage de fichiers») pour une topologie distribuée,
- ou une combinaison des topologies hybrides.

Communication	Past	Present
Topology	Centralized	Distributed or hybrid, yet many are still centralized
Protocols	IRC or HTTP	P2P
Setup	Easy	Hard
Detection	Easy	Hard
Communication	Small delays	Small to medium delays
Resiliency	Bad	Good
Anonymity	Bad	Good

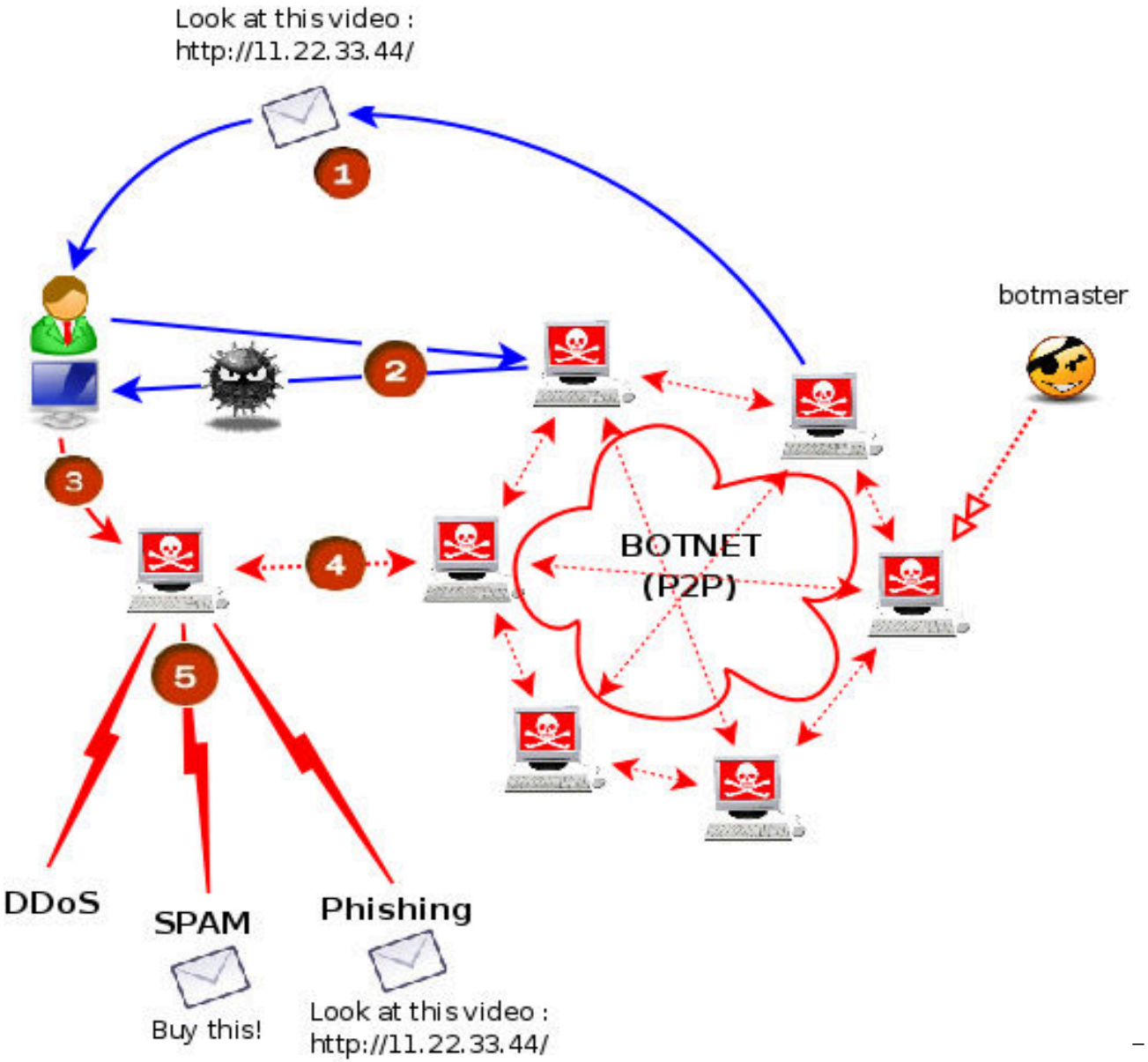


Source : www.umbrella.com

Botnet classique (IRC)



… au Botnet : StormWorm – canal de commande P2P



1: Sollicitation d'un utilisateur Internet

2: Infection / propagation du bot

3: le PC de l'utilisateur Internet fait partie du botnet

4: Il reçoit des ordres d'autres membres du bot.

5: Il effectue les actions illégales demandées, à l'insu de l'utilisateur.

Botnets : points à retenir

- Les concepteurs du botnet font de plus en plus preuve de professionnalisme
  - Conception modulaire: pouvoir utiliser des vulnérabilités différentes selon le contexte, mise à jour des codes d'exploitation utilisés, mise à jour des modules d'attaques…
  - Canal de contrôle distribué et résistant, confondu avec un réseau légitime.
    - Utilise éventuellement des techniques cryptographiques standards.
  - Partition du botnet : possibilité de vendre ou de louer un sous ensemble du botnet grâce aux clefs de chiffrement des *hash*, identifiant chaque bot.
  - Possibilité de fournir un service clefs en main pour le spam en vendant ou louant l'accès aux serveurs de contrôle.
  - Grande variété de binaires: binaires obfusqués, analyse longue et répétitive, difficulté de créer des signatures.

Services à la demande

- Attaques DDoS : une attaque sur une ou plusieurs cibles sans disposer nécessairement du savoir-faire ou des outils
- Spam : inonder le web d'un message publicitaire ou subversif
- Installation de Bot : prestation facturé entre 20 et 100 € pour du bot sur 1000 ordinateurs situés en Europe. Un tarif aussi bas démontre que la procédure est rapide.
- Attaques d'hameçonnage : kits clés en main, inutile d'être un spécialiste. Il est possible de créer une page Internet falsifiée en quelques minutes sans connaissances particulières.
- Chiffrement à la demande (FUD) : La création d'un code malveillant passe par une étape incontournable qui consiste à masquer (obfuscation) le programme
- Multi Scanner : vérification de sa non-détection par les logiciels antivirus.

20 – 200 €

5 €

50 €

20 €

10 €

30 €

GDATA

Déni de service

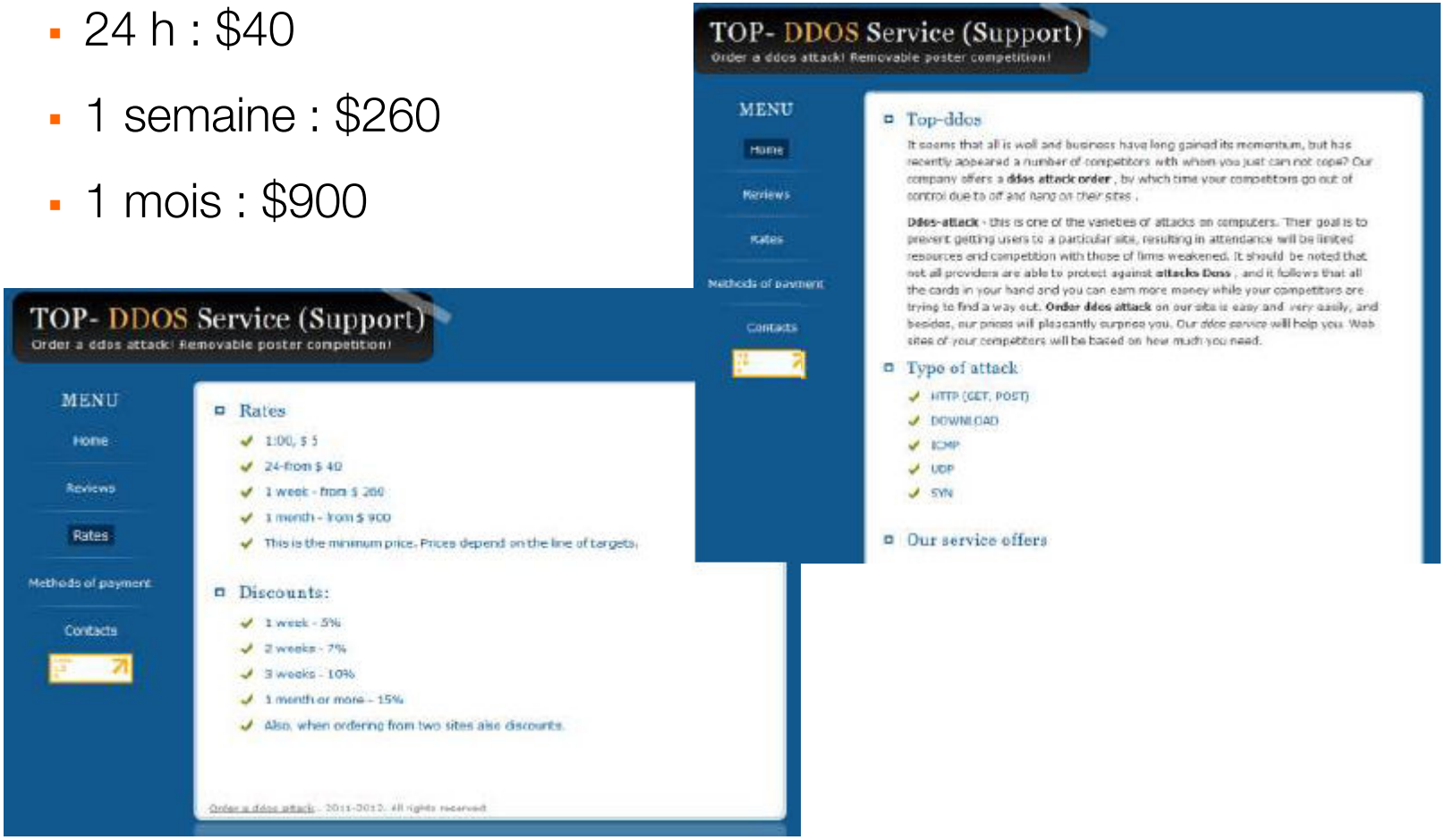
- Applications Web particulièrement sensibles aux attaques par déni de service
  - Visibilité en première ligne sur Internet
  - Encapsulation protocolaire multiple
  - Difficile de filtrer le trafic
    - Les adresses IP ne signifient pas grand-chose
- Attaques par inondation de paquets
  - IP, TCP, UDP, ICMP flood
  - Attaques applicatives
    - demandes de pages
    - demande de ressources trop importantes
    - injection de commandes exécutant des fonctions gourmandes en ressources (benchmark mysql ; forkbomb, XML « laugh bomb », requêtes récursives ou faisant boucler la logique de l'application, …)
    - saturation des ressources du serveur
      - upload de fichiers saturant le disque du
      - requêtes BDD gourmandes, …

DDoS : problématiques

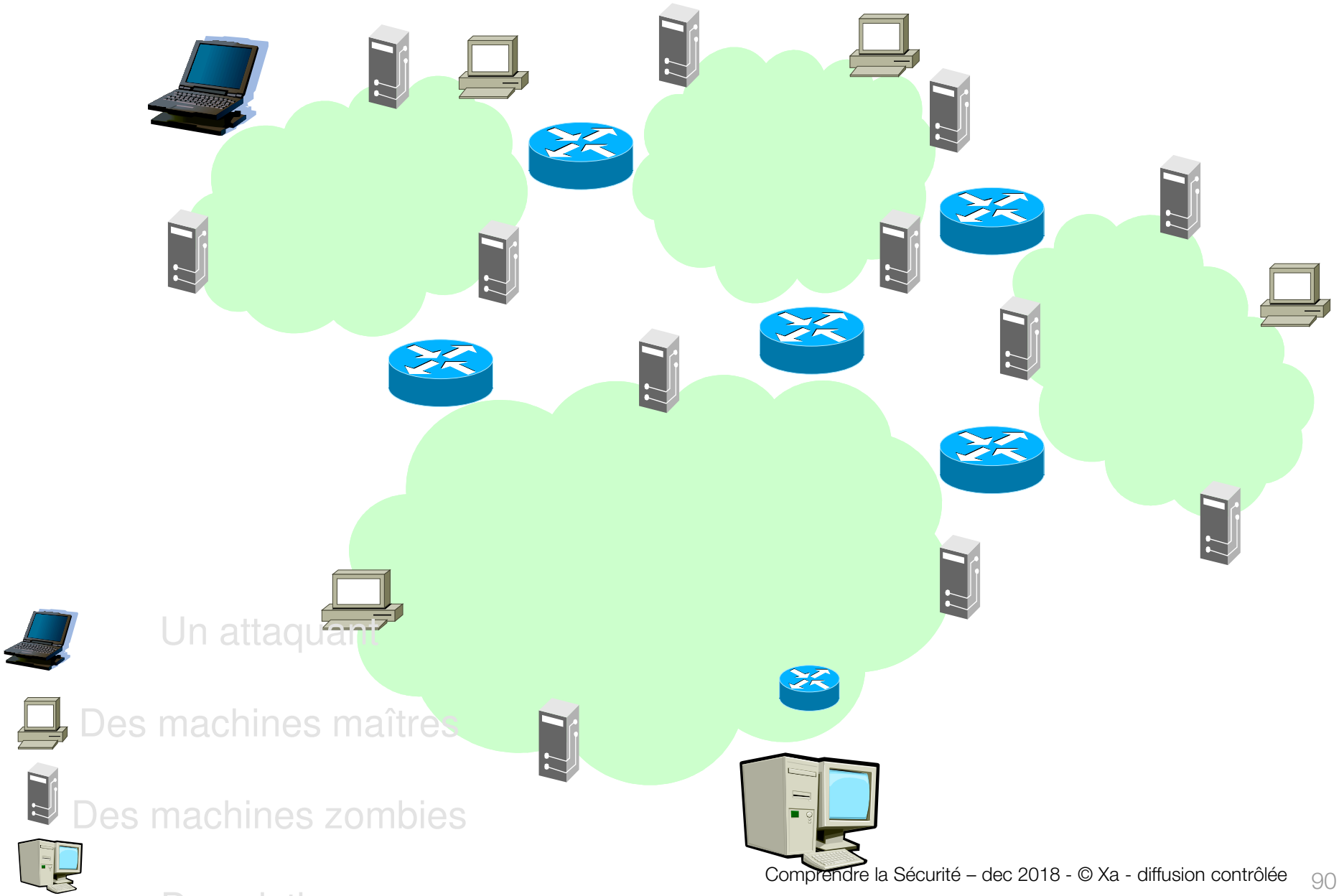
- Des « botnets » de tailles variés…
  - Réseau > 10k machines…
  - Réseau de quelques centaines de système (cloisonnement)
- Des flux d'attaques difficile à tracer
  - spoofing d'adresse source par exemple, ICMP, UDP
  - Trafic légitime (simple requêtes HTTP, ICMP, DNS…)
- Des méthodes de saturation classique (utilisation de toute la bande passante)
  - 10000 bots sur ADSL 512/128 → 2.5 Gb
  - Exemple : Attaque des roots DNS en 10/2002, par saturation ICMP
- Vers un nouveau business
  - Chantage sur services en lignes…
- Cas d'attaque : Spamhaus
  - ✓ DDos à 300 Gbits/s : débit max des routeurs du cœur de réseaux opérateurs
  - ✓ Faille DNS, usurpation IP, requête 36 octets -> réponse de 3000 (facteur 100)
  - ✓ Config DNS ouverte => (DNSSec)

Des offres DDOS pour tous

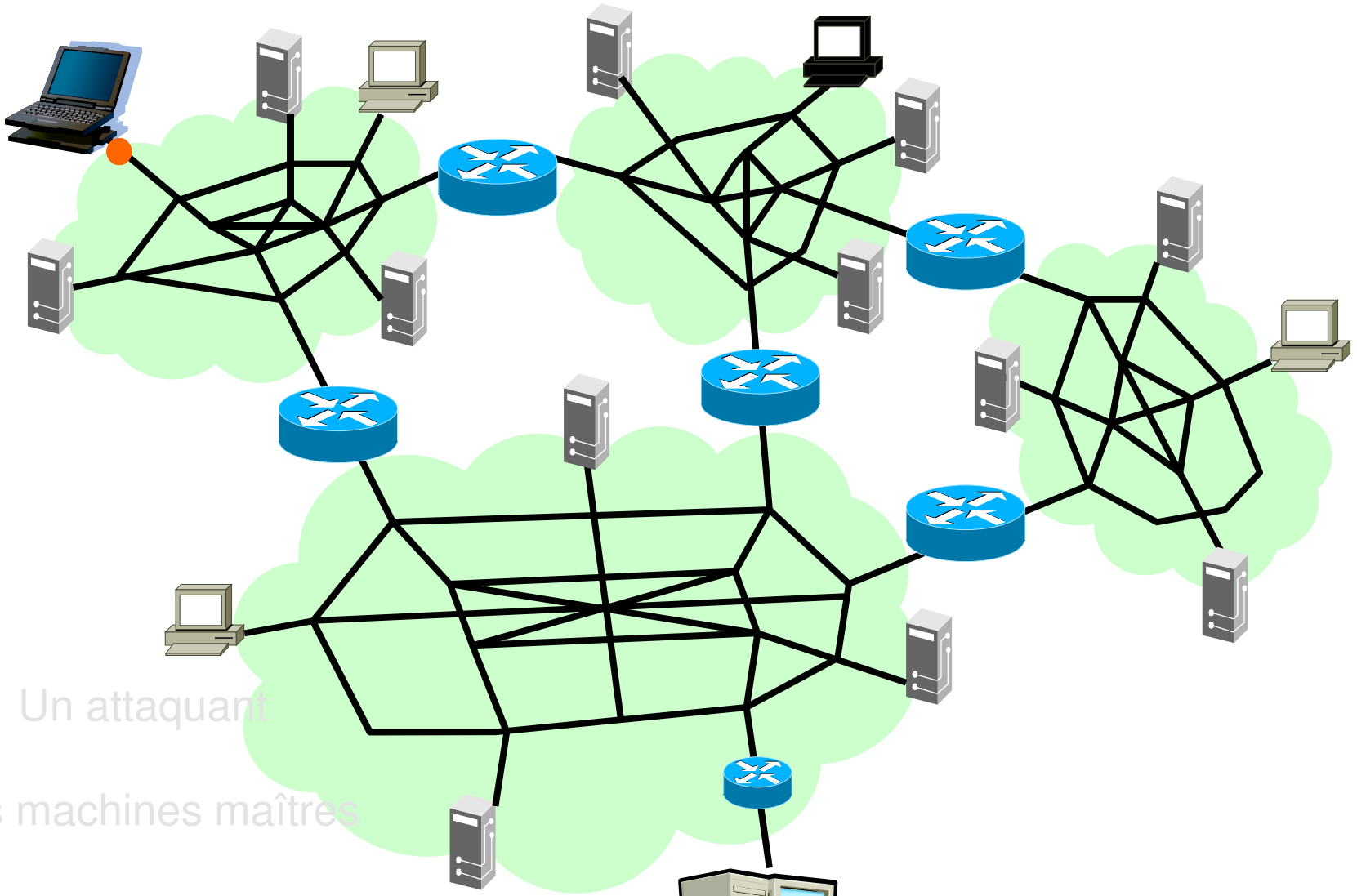
- 1h : $5
- 24 h : $40
- 1 semaine : $260
- 1 mois : $900



Un exemple d'attaque : le DDoS (1/4)



DDoS : Prise de contrôle des maîtres (2/4)



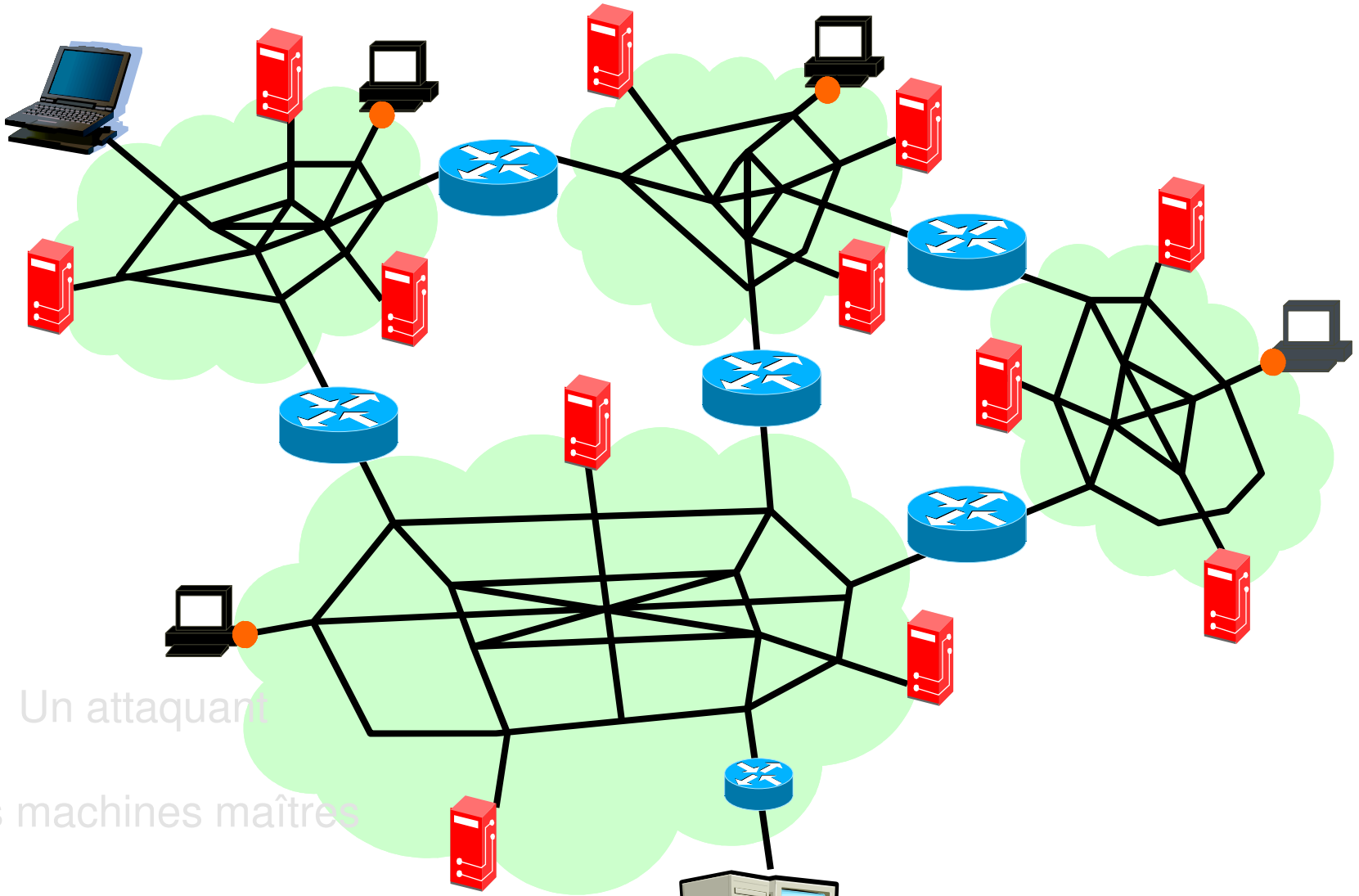
Un attaquant

Des machines maîtres

Des machines zombies

Des victimes

DDoS : Prises de contrôle des zombies (3/4)



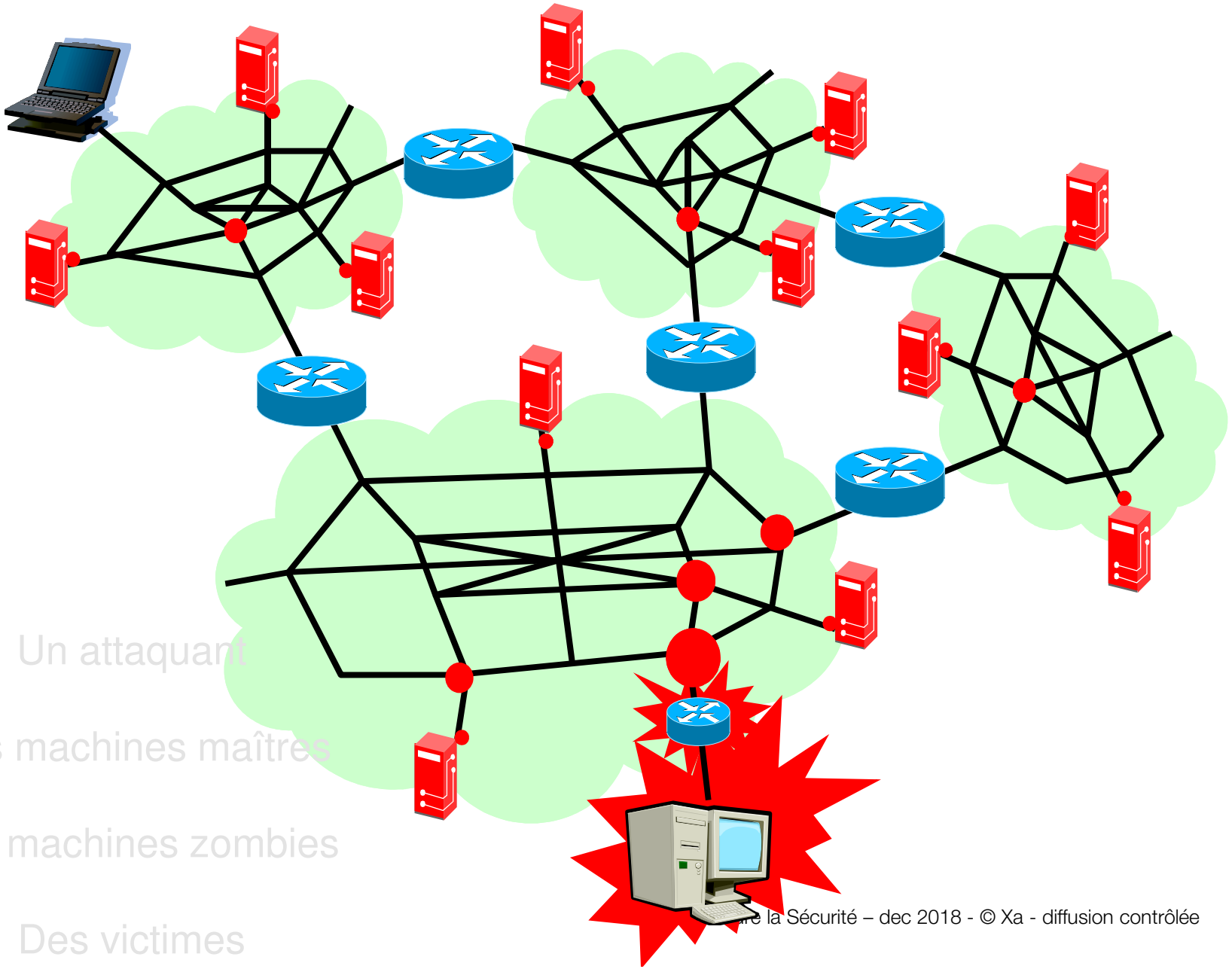
Un attaquant

Des machines maîtres

Des machines zombies

Des victimes

DDoS : Attaque par inondation (4/4)



Un attaquant

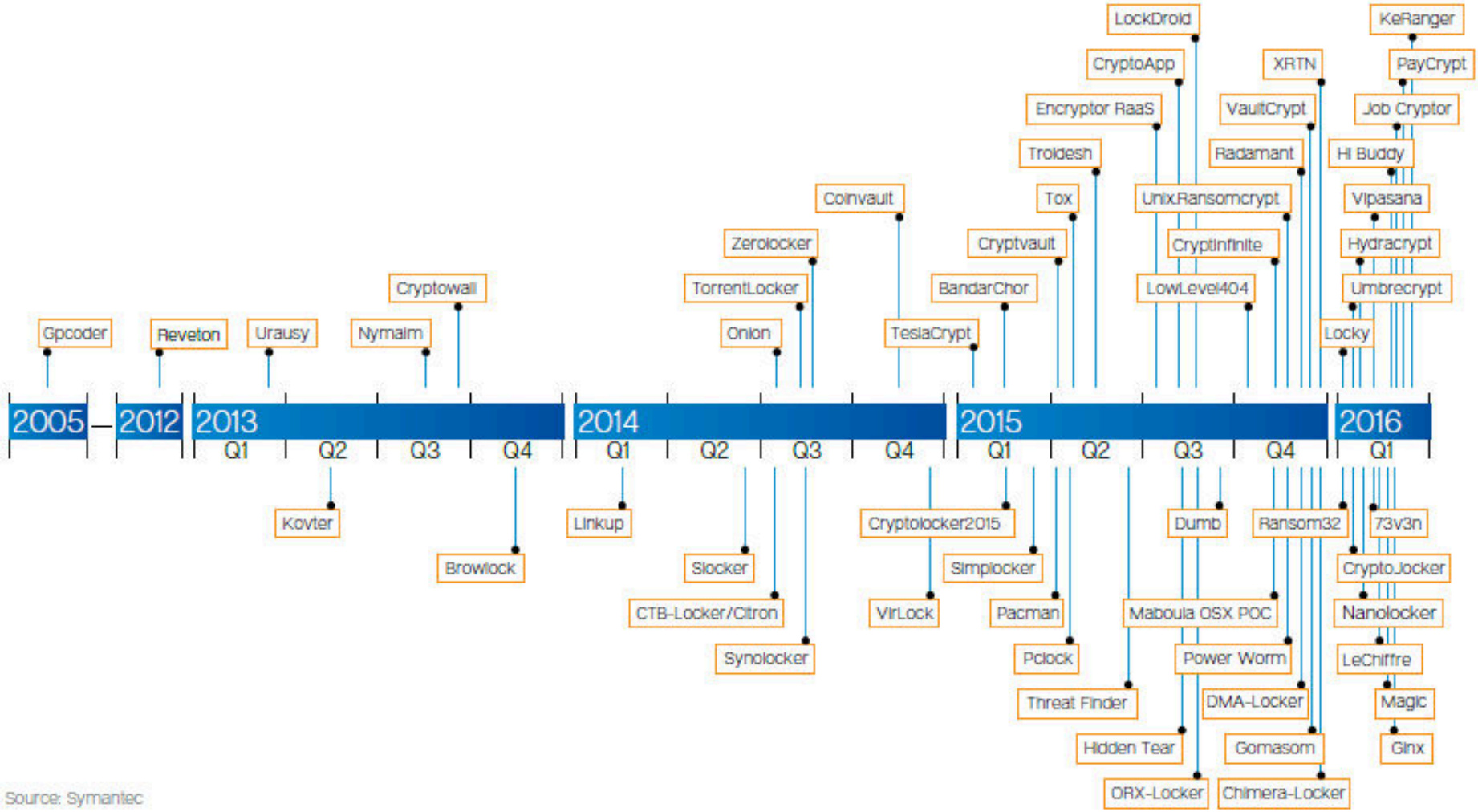
Des machines maîtres

Des machines zombies

Des victimes

Ransomware : CaaS

- kit à partir de 250 $ / semaine et 500 $ / mois
- licence 700 $ / 3 mois ou 1,500 $ / an

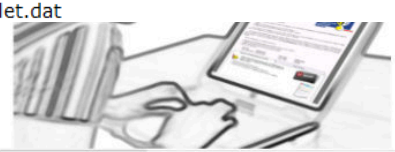


Source: Symantec

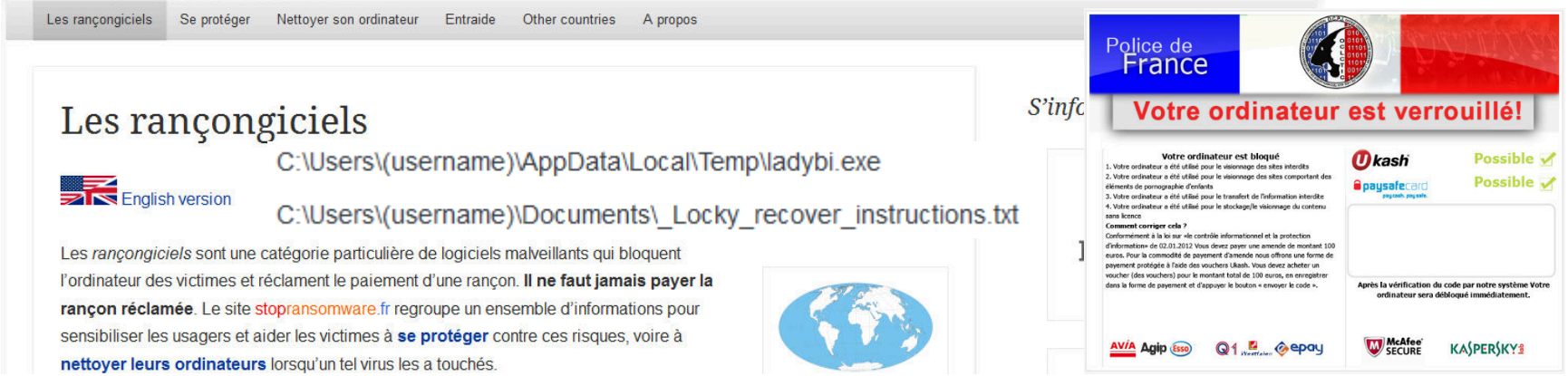
Les rançonciels

- Logiciel malveillants qui bloquent l'ordinateur
- Réclament le paiement d'une rançon
- **Policier, Chiffreur, Bloqueur** (Pub)
- 5 millions de $/an (Symantec)
- Smarphone et tablettes depuis 2013
- Prévention : http://stopransomware.fr

, .tif, .tiff, .NEF, .psd, .cmd, .bat, .class, .jar, .java, .asp, .brd, .sch, .dch, .dip, .vbs, .asm, .pas, .cpp, .php, .ldf, .mdf, .ibd, .MYI, .MYD, .frm, .odb, .dbf, .mdb, .sql, .SQLITEDB, .SQLITE3, .asc, .lay6, .lay, .ms11 (Security copy), .sldm, .sldx, .ppsm, .ppsx, .ppam, .docb, .mml, .sxm, .otg, .odg, .uop, .potx, .potm, .pptx, .pptm, .std, .sxd, .pot, .pps, .sti, .sxi, .otp, .odp, .wks, .xltx, .xltm, .xlsx, .xlsm, .xlsb, .slk, .xlw, .xlt, .xlm, .xlc, .dif, .stc, .sxc, .ots, .ods, .hwp, .dotm, .dotx, .docm, .docx, .DOT, .max, .xml, .txt, .CSV, .uot, .RTF, .pdf, .XLS, .PPT, .stw, .sxw, .ott, .odt, .DOC, .pem, .csr, .crt, .key, wallet.dat

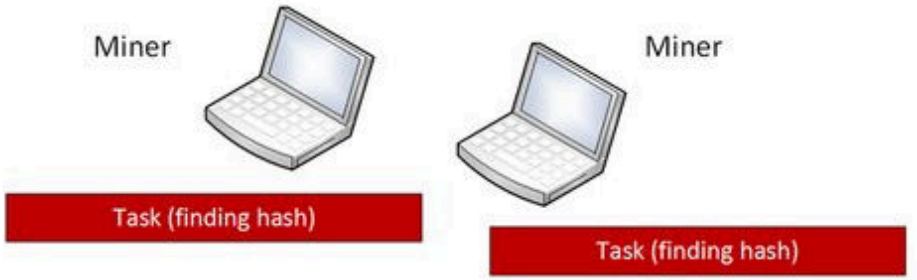


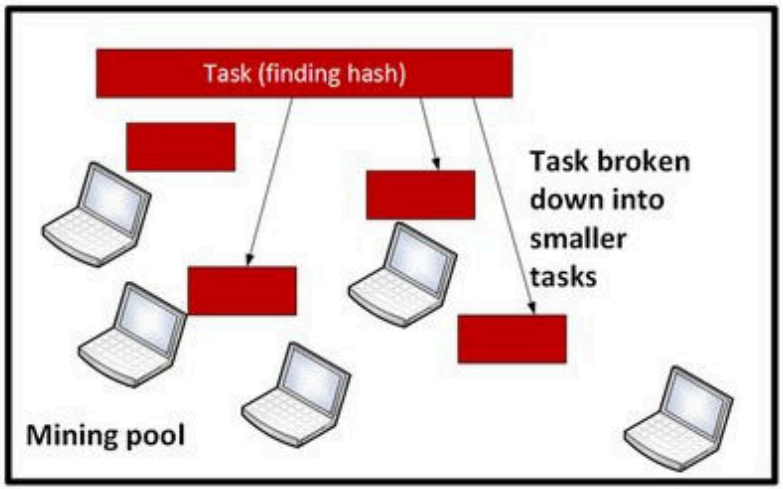
stop ransomware



Cryptojacking

- Votre ordinateur fabrique des bitcoins à votre insu Lorsque vous visitez certains sites et utilisez leurs services, soi-disant gratuits, ils peuvent utiliser votre ordinateur pour fabriquer de la monnaie virtuelle.
- 500 millions d'utilisateurs dans le monde en auraient été victimes en minant des cryptomonnaies sans le savoir.
- Miner devient souvent une compétition entre ordinateurs. Le plus rapide est récompensé par de l'argent.
- Cela signifie que le site Web ou le fournisseur d'accès Internet qui effectue le cryptojacking peut exploiter la cryptomonnaie à peu de frais. Selon certaines estimations, 220 des 1 000 sites Web les plus visités au monde font du cryptojacking, cela représente un total de 57 000 $ par mois.





Ransomware et Domotique

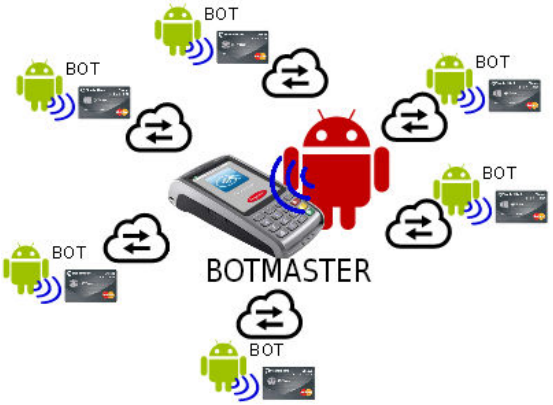
DEFCON

- Avec la multiplication des terminaux connectés au sein des foyers et la démocratisation de la domotique, les pirates informatiques pourraient mettre au point de nouvelles méthodes en vue d'extirper de l'argent à leurs victimes
- Thermostat pirater par des cybercriminelles qui verrouillent avec les logiciels malveillants
- Une rançon pour obtenir ce retour à la normale, vous laissant littéralement dans le froid jusqu'à ce que vous payez quelques centaines de dollars.

- Avec une carte SD, laquelle sert normalement à ajouter des fonds d'écran et à transférer des fichiers de configuration dans le thermostat
- Une fois implanté sur l'appareil, permet aux pirates de contrôler le dispositif à distance.
- la méthode utilisée nécessite obligatoirement un accès physique à l'appareil, et même une action spéciale de la part de l'utilisateur

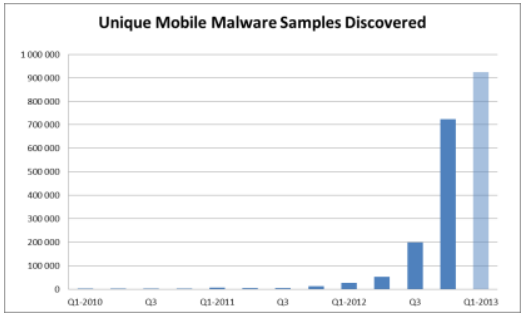
Attaques par relais EMV sur cartes NFC

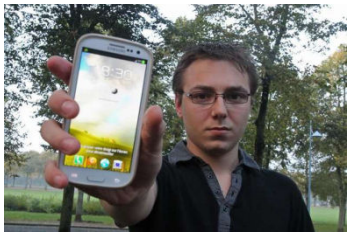
- Application malveillante sur Android KitKat
- Carte de crédit est détecté sur le réseau
- Approcher le terminal « relais » du TPE
- Transaction illégale



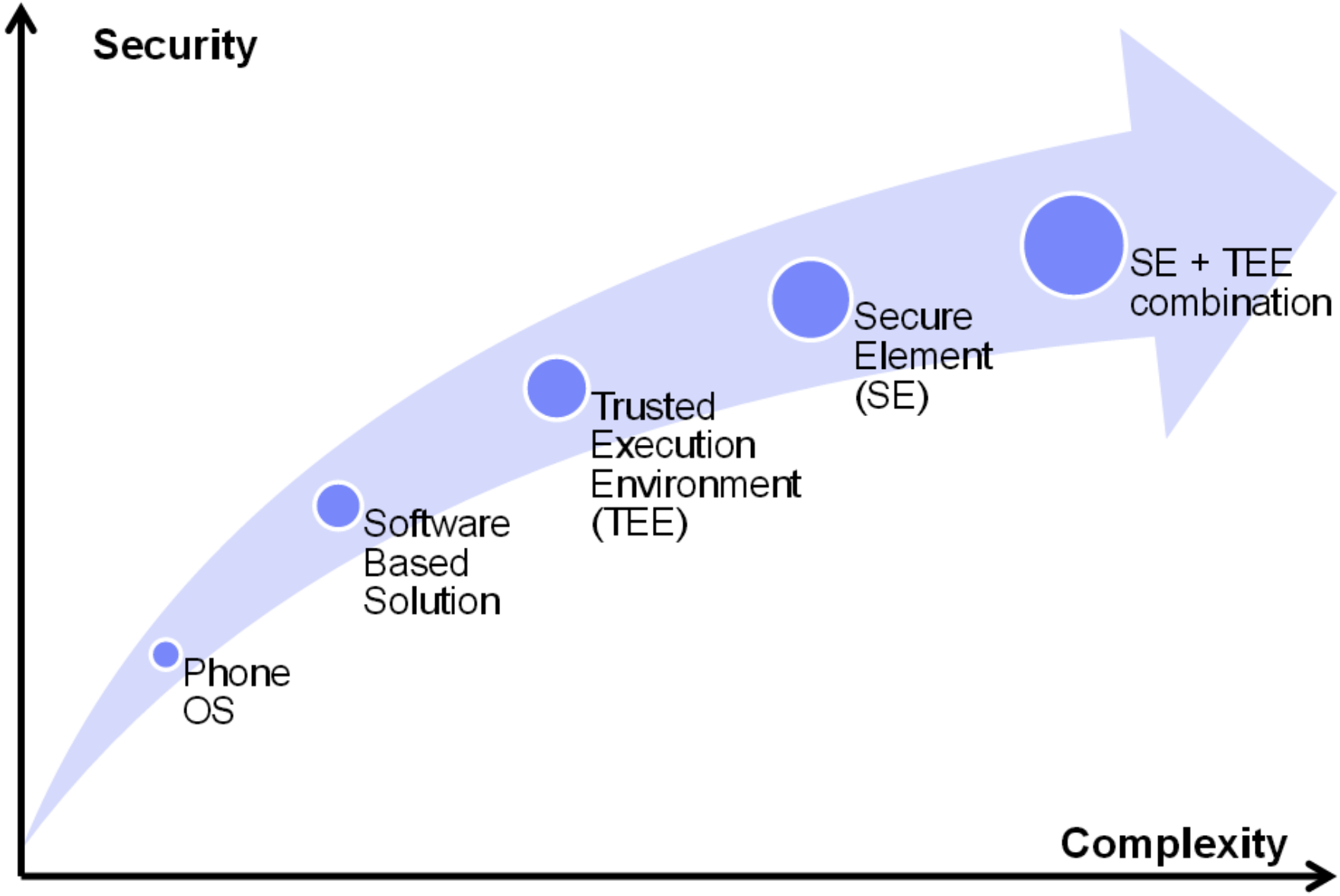
Evolution des attaques

- Les attaquants sont préparés et organisés
- Les attaques sont de plus en plus faciles à mener, et de plus en plus difficiles à tracer
- Outils d'attaque en évolution constante
  - Sophistication augmente
  - Faciles à utiliser, surtout pour des attaquants novices (script kiddies)
  - Conçus pour des attaques à grande échelle (distribuées)
- La programmation n'est plus requise pour trouver des vulnérabilités
- Paradoxe : Facilité accrue à mener des attaques de plus en plus complexes
  - Disparité des législations
  - Multiplication des acteurs
  - Multiplication des cibles
  - … des enquêtes complexes





Modulation de la sécurité



Questions / Réponses