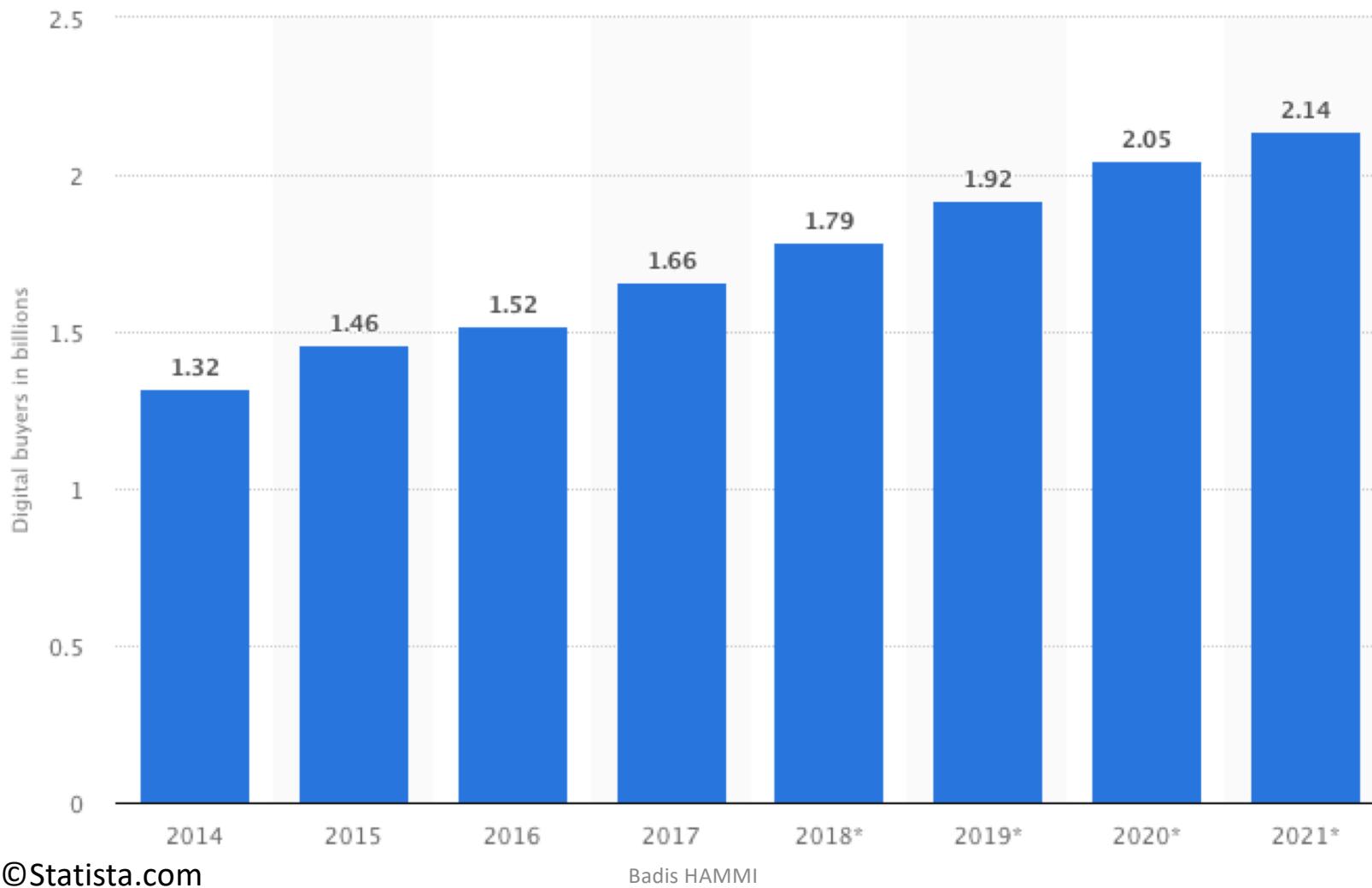


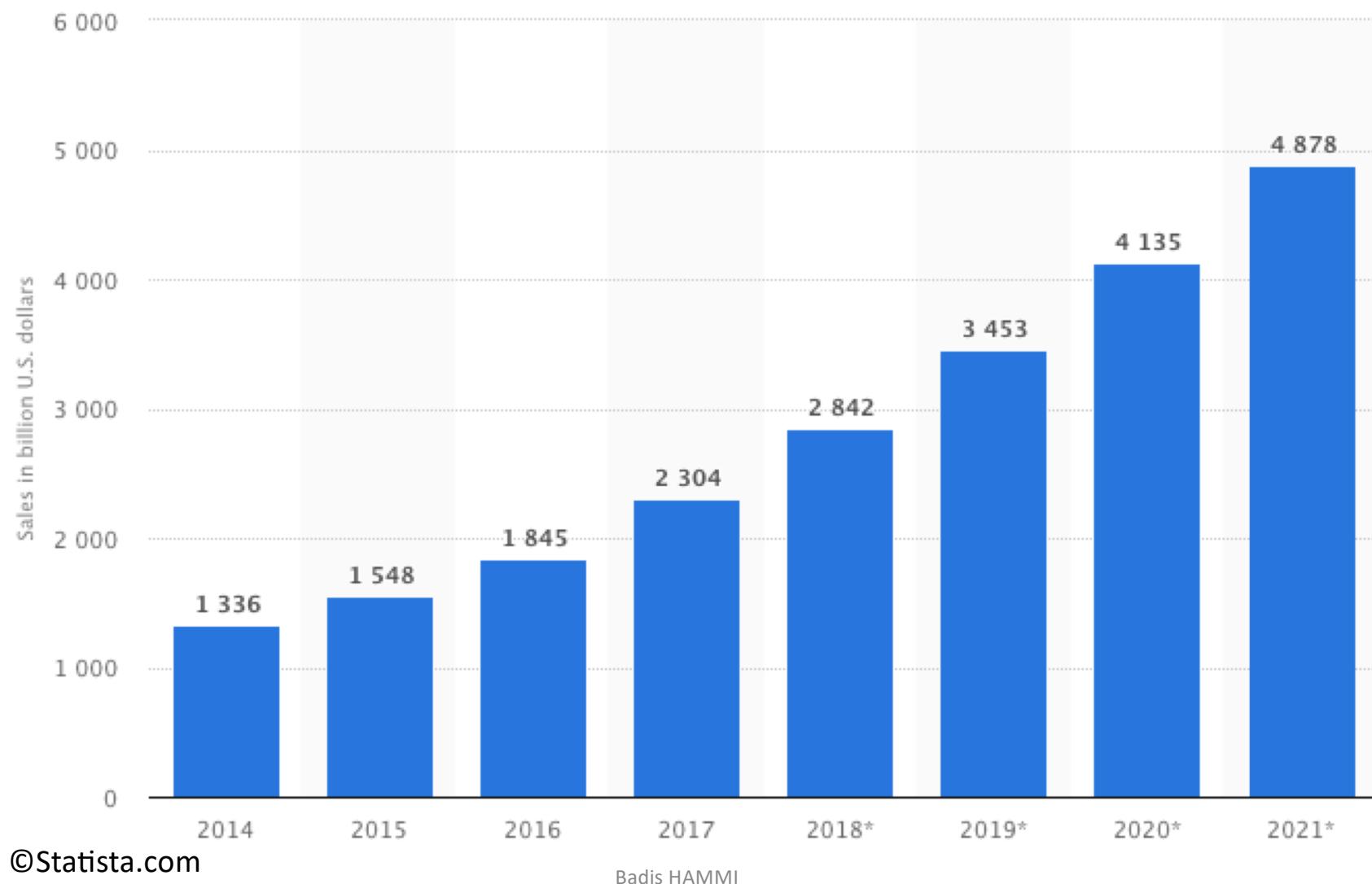
DDoS et Botnets

Badis HAMMI,
Associate Professor (PSB Paris)
b.hammi1@psbedu.paris

Introduction



Introduction



Introduction

January 2018: 115 Cyberattacks

Winner: Health South-East RHF, a large healthcare management organization in southeast Norway — 2.9 million patients

March 2018: 98 Cyberattacks

Winner: MyFitnessPal, Under Armour's food and nutrition app and website — 150 million users affected

May 2018: 117 Cyberattacks

Winner: 50 small Japanese websites — 200+ million Japanese internet users

February 2018: 133 Cyberattacks

Winner: GitHub's successful defense of a massive DDoS attack

April 2018: 99 Cyberattacks

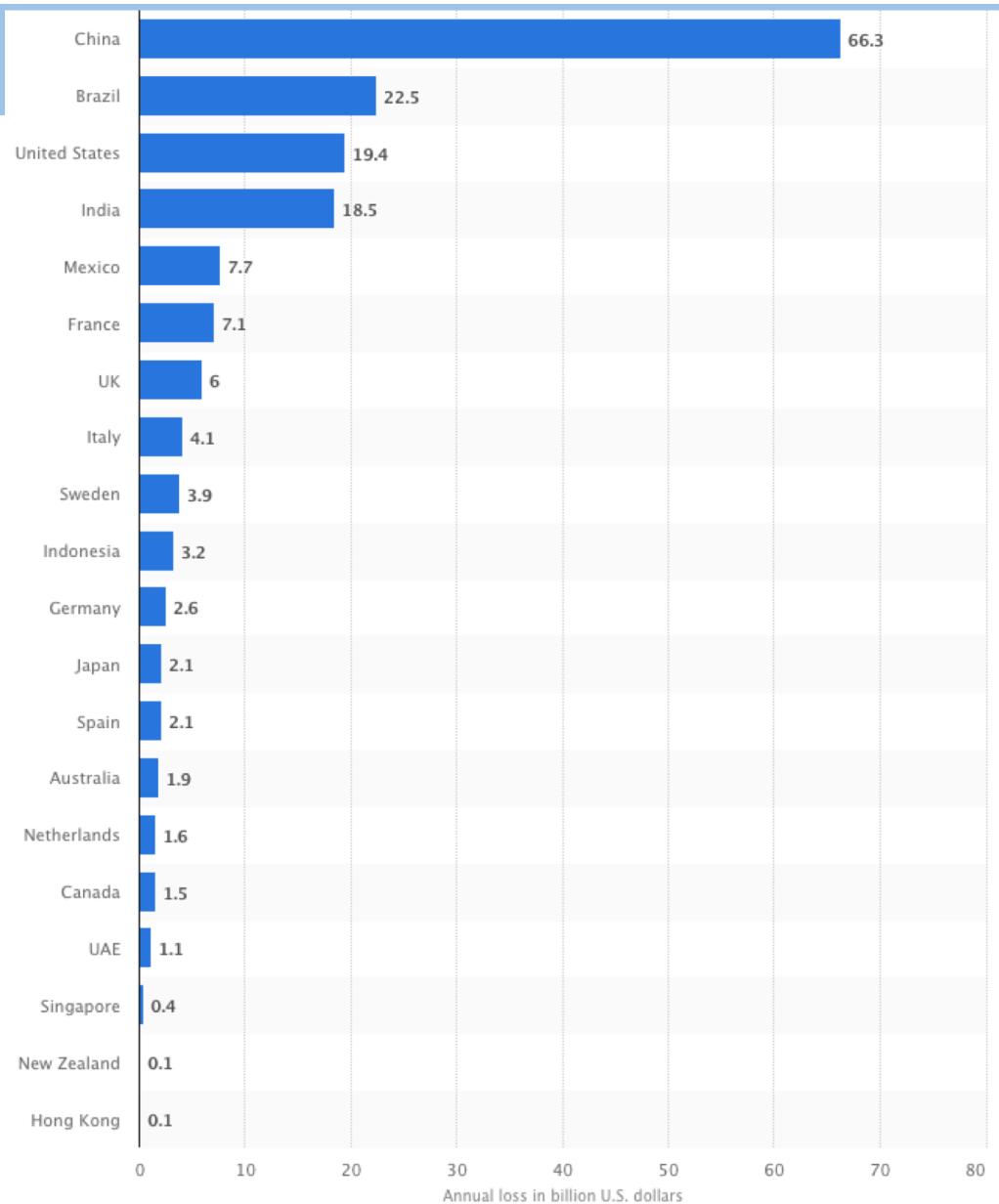
Winner: Saks Fifth Avenue and Lord & Taylor stores — 5 million+ credit card users

June 2018: 96 Cyberattacks

Winner: MyHeritage — 92 million users compromised

Honorable Mention: Bithumb Cryptocurrency Exchange — \$31.5 million of crypto-coins stolen

Introduction



Introduction

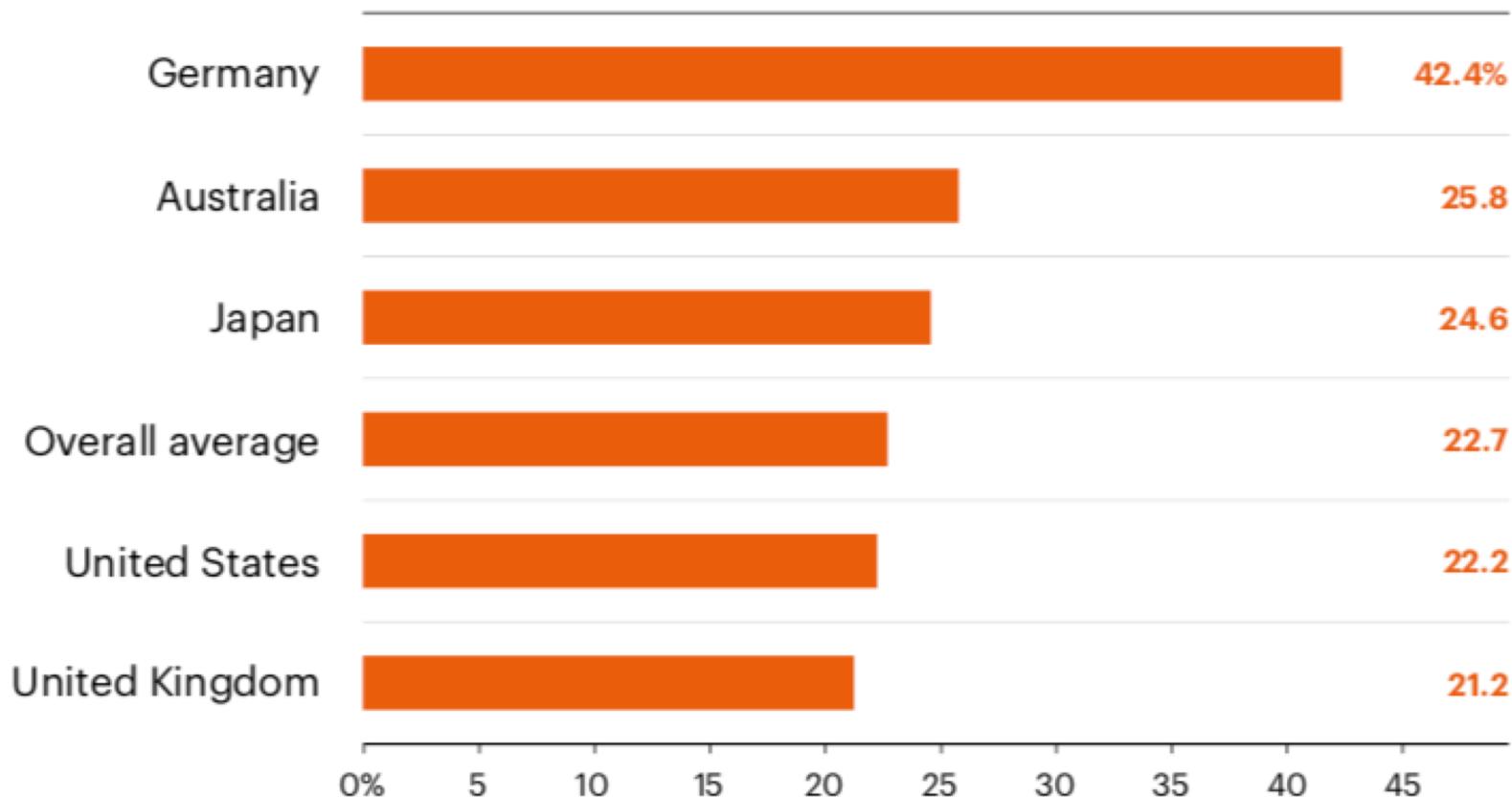


FIGURE 3
One-year percentage increase in cyber crime by country sample

Percentage increase could not be calculated for France and Italy as they were included for the first time in this report

2016 → 2017

Legend

Mean = 20.4%

n = 254 companies

©Accenture.com

Cybersecurity Ventures predicts cybercrime damages will cost the world \$6 trillion annually by 2021, up from \$3 trillion in 2015.

©Cybersecurityventures.com

Badis HAMMI

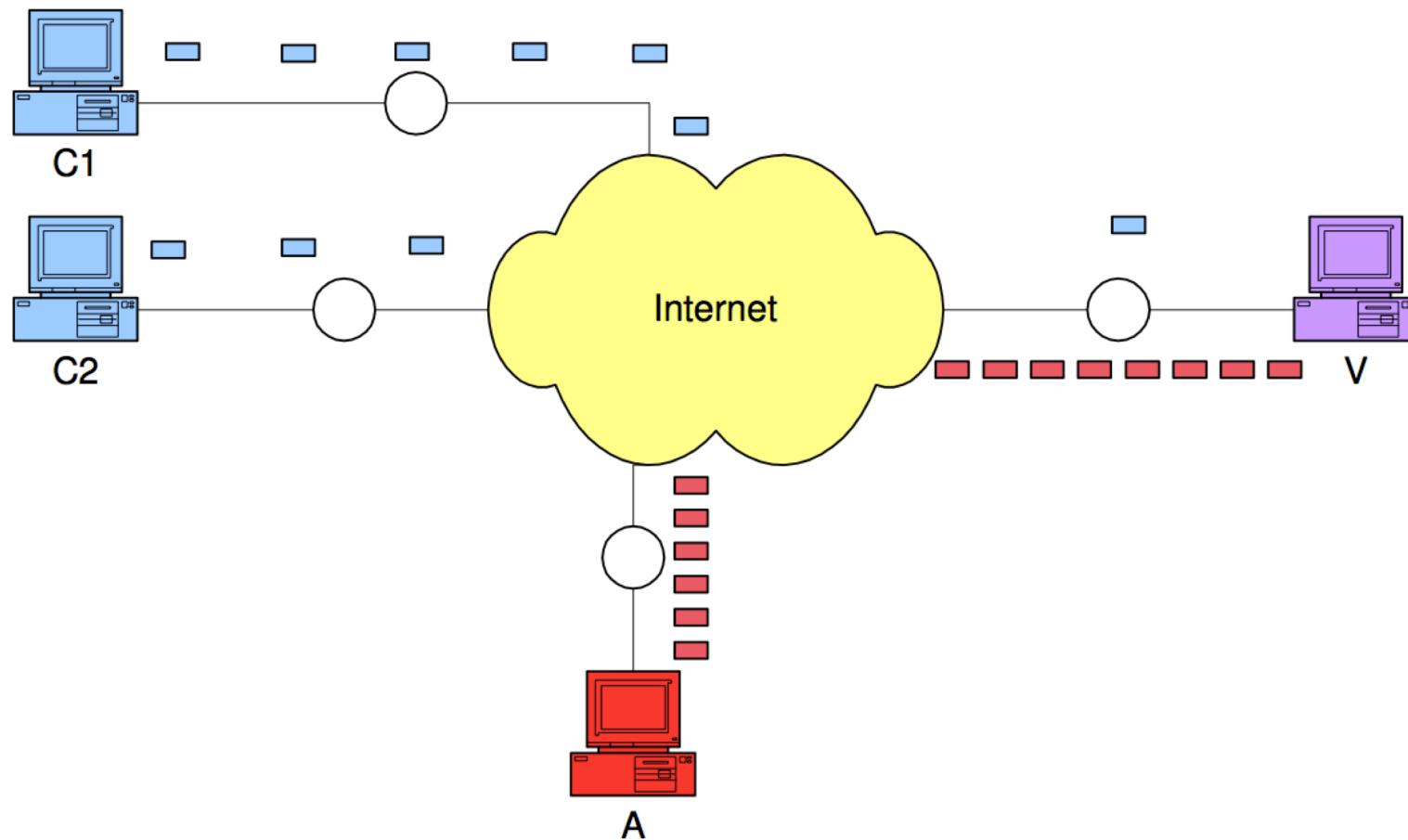
Introduction

- Sécurité informatique
 - Enjeu vital pour l'entreprise
 - Développement de la sécurité dans les réseaux
 - Aujourd'hui une véritable préoccupation pour les différents acteurs de l'économie : entreprises et opérateurs
 - Domaine complexe
 - Pourquoi ?

Attaque DoS

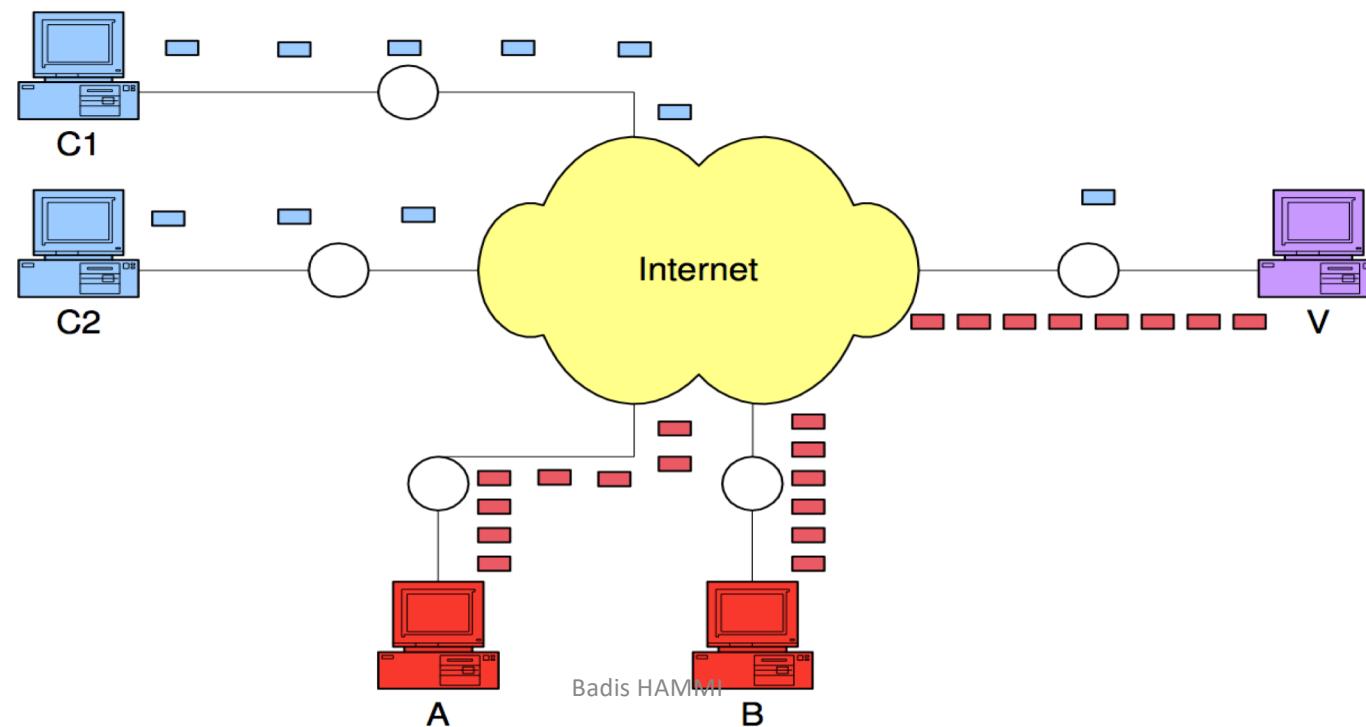
- le déni de service (DoS) représente une attaque où une victime reçoit un flux de paquets malveillants qui épuise une ressource clé. Cet épuisement se traduit par le déni de ce service (la ressource) aux clients légitimes de la victime.
- 2 manière de réaliser un Dos:
 - en exploitant certaines vulnérabilités dans les protocoles ou logiciels utilisés par la victime (attaques de vulnérabilité). EX: Ping of Death, Land attack
 - envoi d'un volume de trafic plus élevé que celui que les ressources de la victime peuvent gérer → Innondation (*Flooding*)

Attaque DoS



Attaque Distributed DoS (DDoS)

- *“An overwhelming quantity of packets being sent from multiple attack sites to a victim site. These packets arrive in such a high quantity that some key resource at the victim (bandwidth, buffers, CPU time to compute responses) is quickly exhausted.” Mirkovic*



Attaque DDoS: Caractéristiques

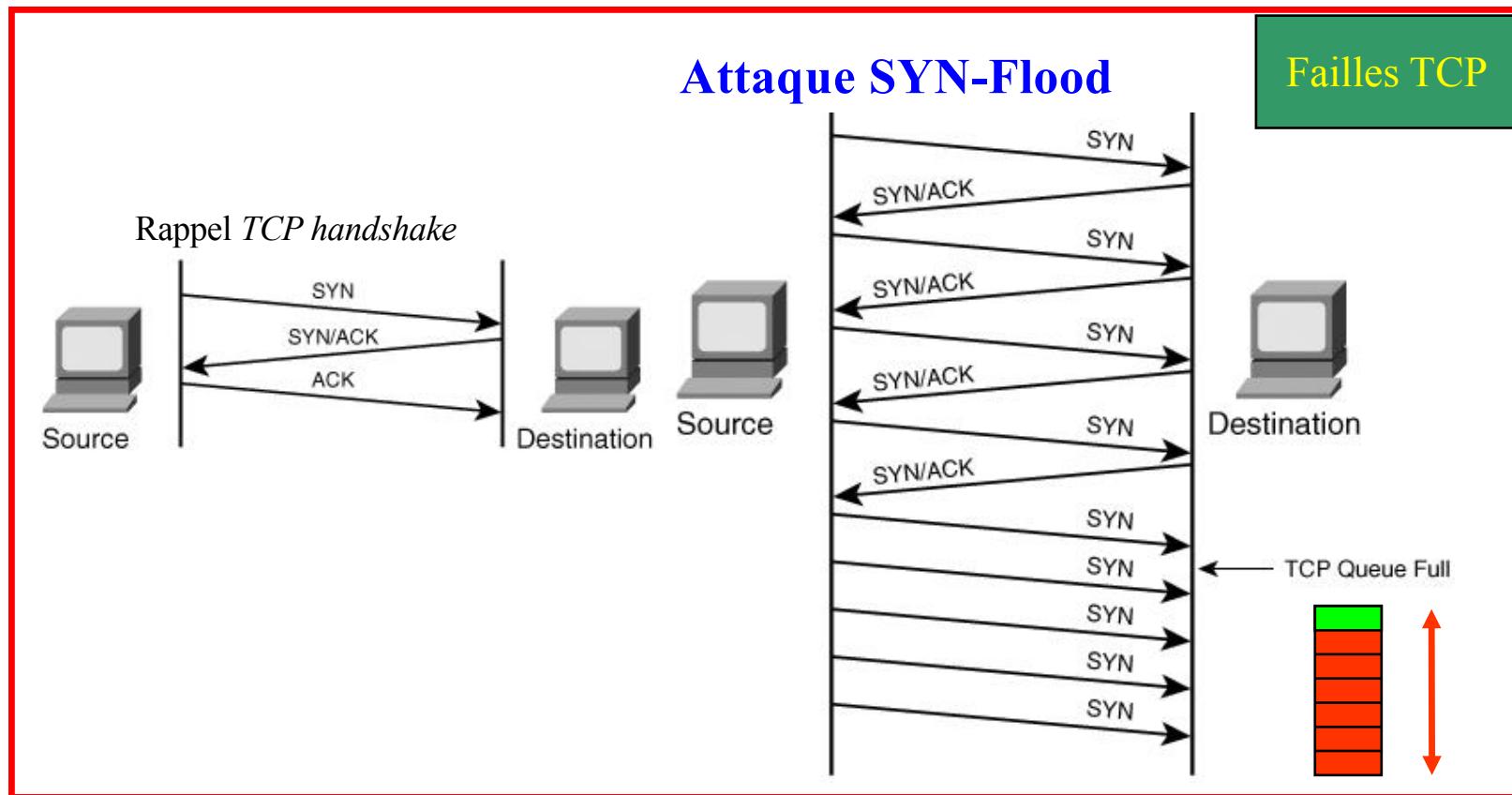
- Usurpation d'adresse IP (*IP Spoofing*)
- Nombre de machine attaquantes
- Similitude entre le trafic d'attaque et le trafic légitime

Attaque DDoS

- Sur la couche transport
 - TCP SYN Flood
 - UDP Flood
 - ICMP Flood
- Sur la couche application
 - HTTP Flood
 - SIP Flood

- Ping of Death
- Land Attack
- Teardrop (fragmentation)

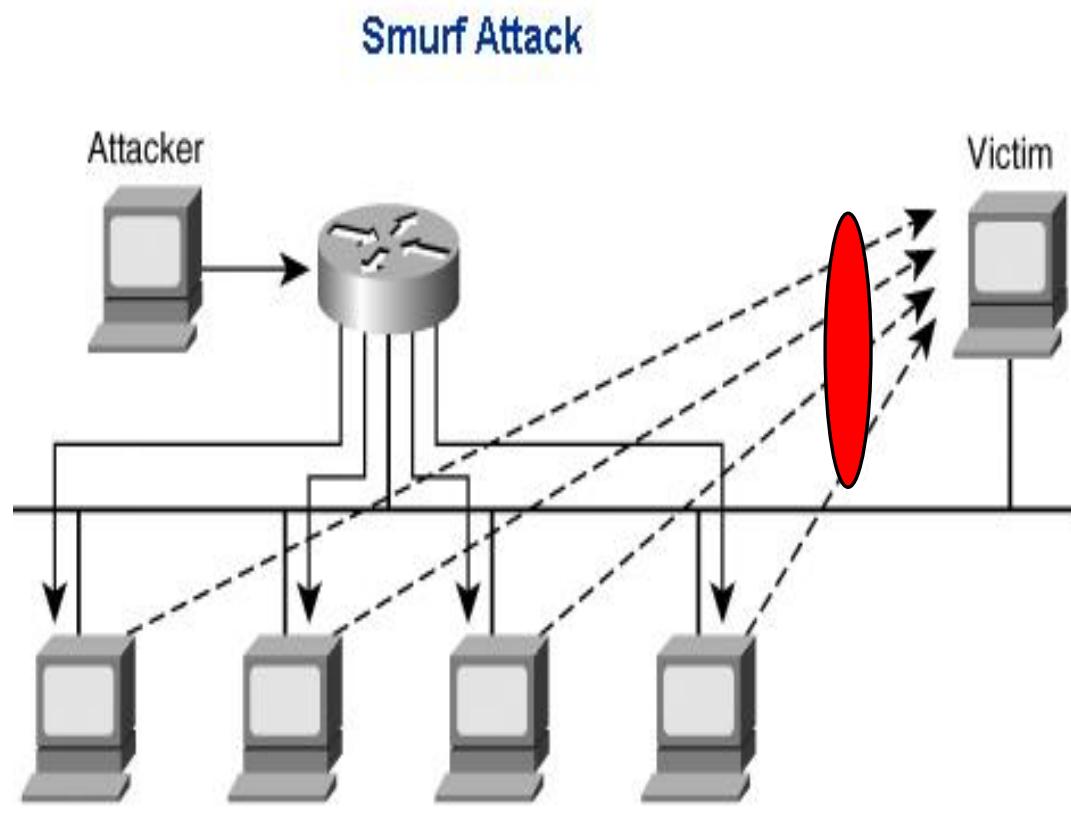
Exemple d'attaque



Exemple d'attaque



Attaque reflective (par rebond)



Badis HAMMI

16

Attaque reflective (par rebond)

DNS Reflection : Durant une attaque DNS reflection/amplification, l'attaquant envoie un flux de requêtes DNS à un ensemble de serveurs DNS ouverts (*open DNS resolvers*), tout en remplaçant l'adresse IP source des requêtes par celle de la victime. Une requête DNS demande généralement un grand jeu d'enregistrements, ce qui engendre une amplification du trafic de l'attaque.

En utilisant plusieurs machines (*bots*) pour envoyer des requêtes à plusieurs serveurs DNS, un attaquant peut provoquer de très gros volumes de trafic d'attaque provenant de sources largement distribuées. L'autre facteur de puissance de ces attaques réside dans le grand nombre de serveurs DNS. En effet, actuellement, on estime qu'il existe plus de 32 millions de serveurs DNS sur Internet, dont 28 millions qui représentent une menace potentielle.

Attaque reflective (par rebond)

NTP Reflection/Amplification: Comme le DNS, NTP représente un outil idéal pour générer des attaques DDoS. Le protocole NTP utilise une commande appelée *monlist* qui peut être envoyée à un serveur NTP à des fins de surveillance. Ce dernier renvoie les adresses des 600 dernières machines avec lesquelles le serveur NTP a interagi, générant ainsi une réponse volumineuse. C'est cette dernière qui est utilisée pour amplifier les attaques. Ainsi, un attaquant, armé d'une liste de serveurs NTP sur Internet, peut facilement réaliser une attaque DDoS puissante, d'autant plus qu'il utilise un grand nombre de *bots*

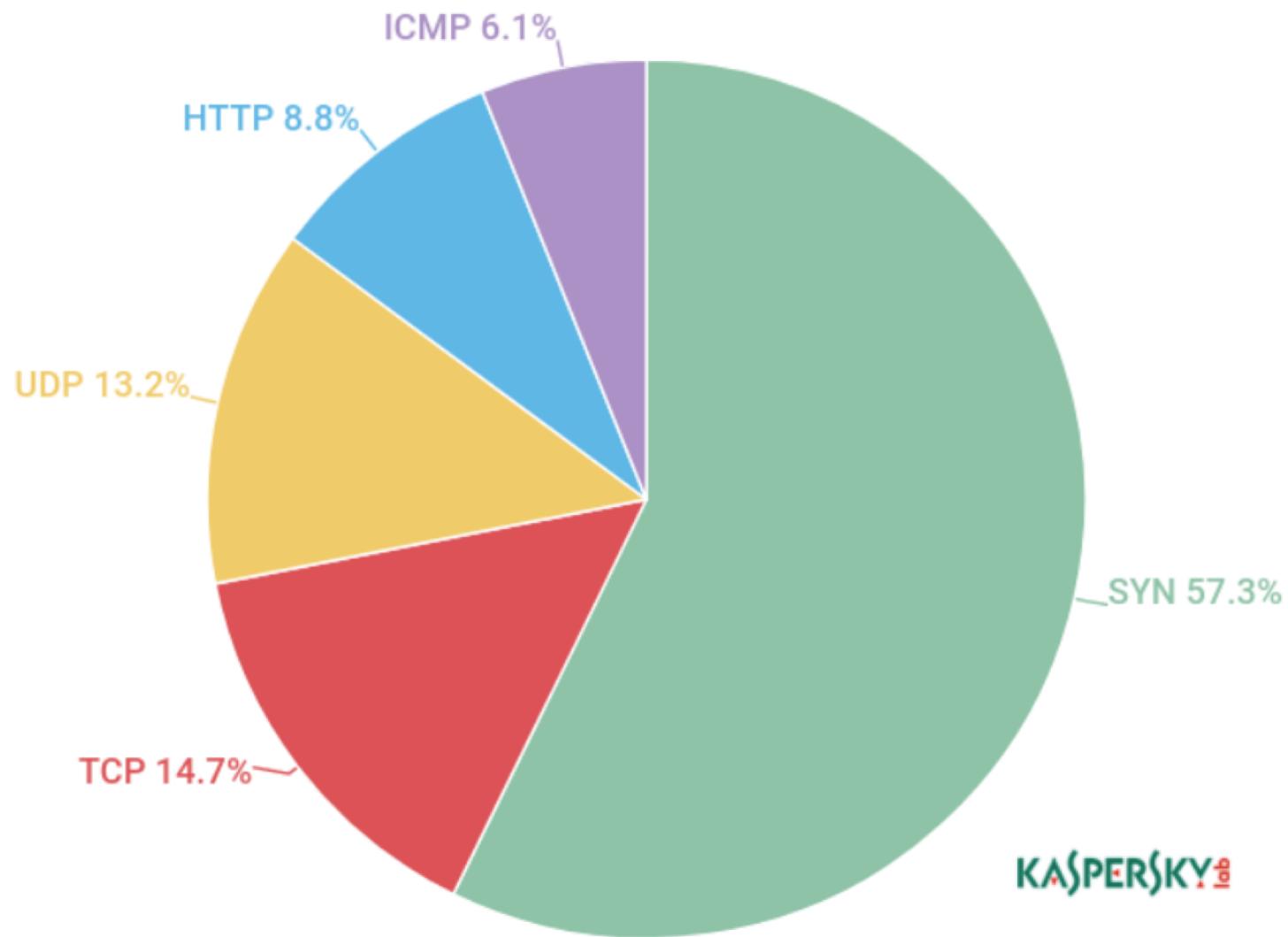
Les serveurs NTP ne sont pas difficiles à solliciter. En effet, les outils communs comme Metasploit et NMAP ont des modules capables d'identifier facilement les serveurs NTP qui supportent la commande *monlist*

DDoS attack evolution

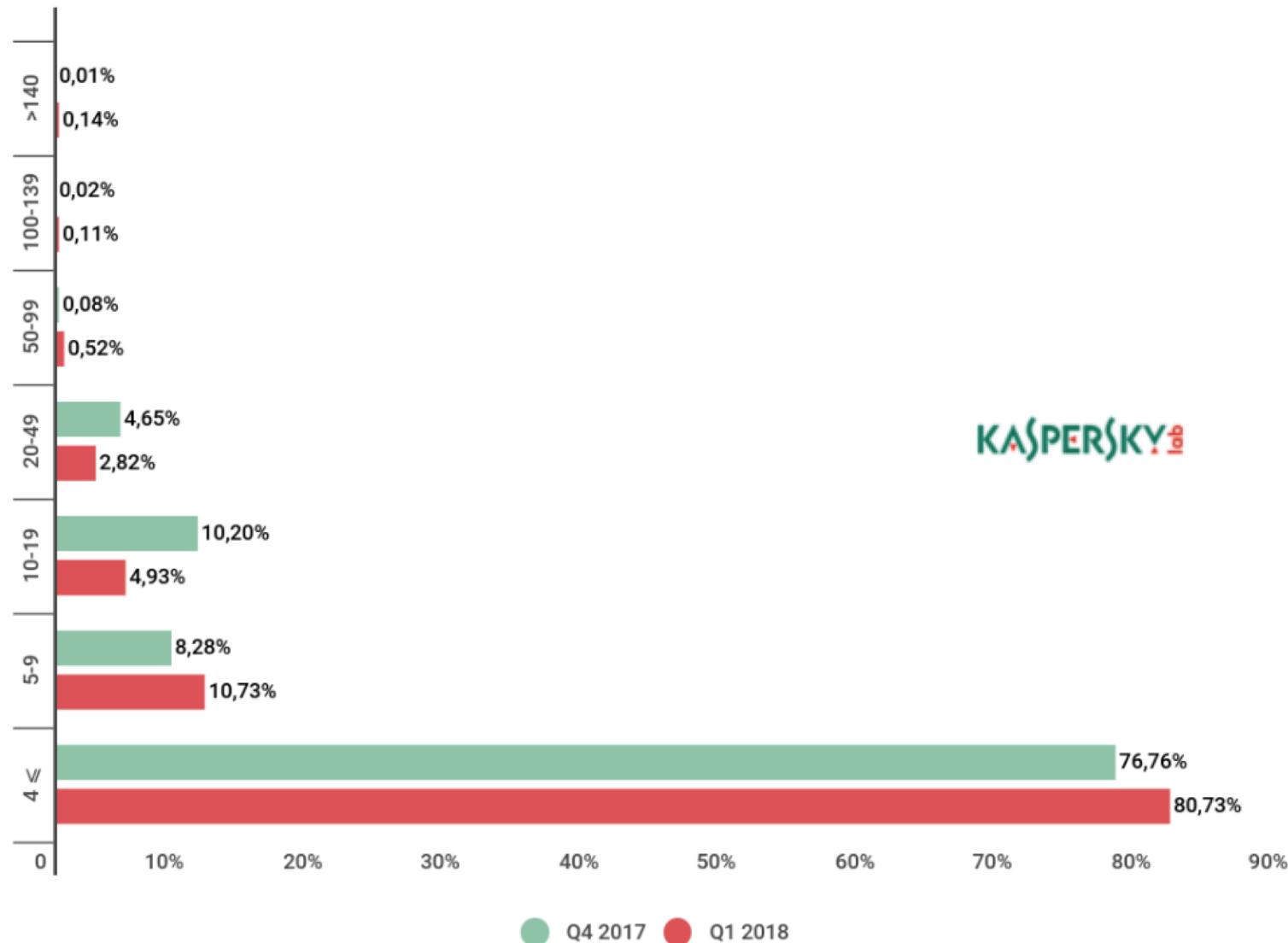
Annual volume peaks



Distribution of DDoS attacks by type, Q1 2018

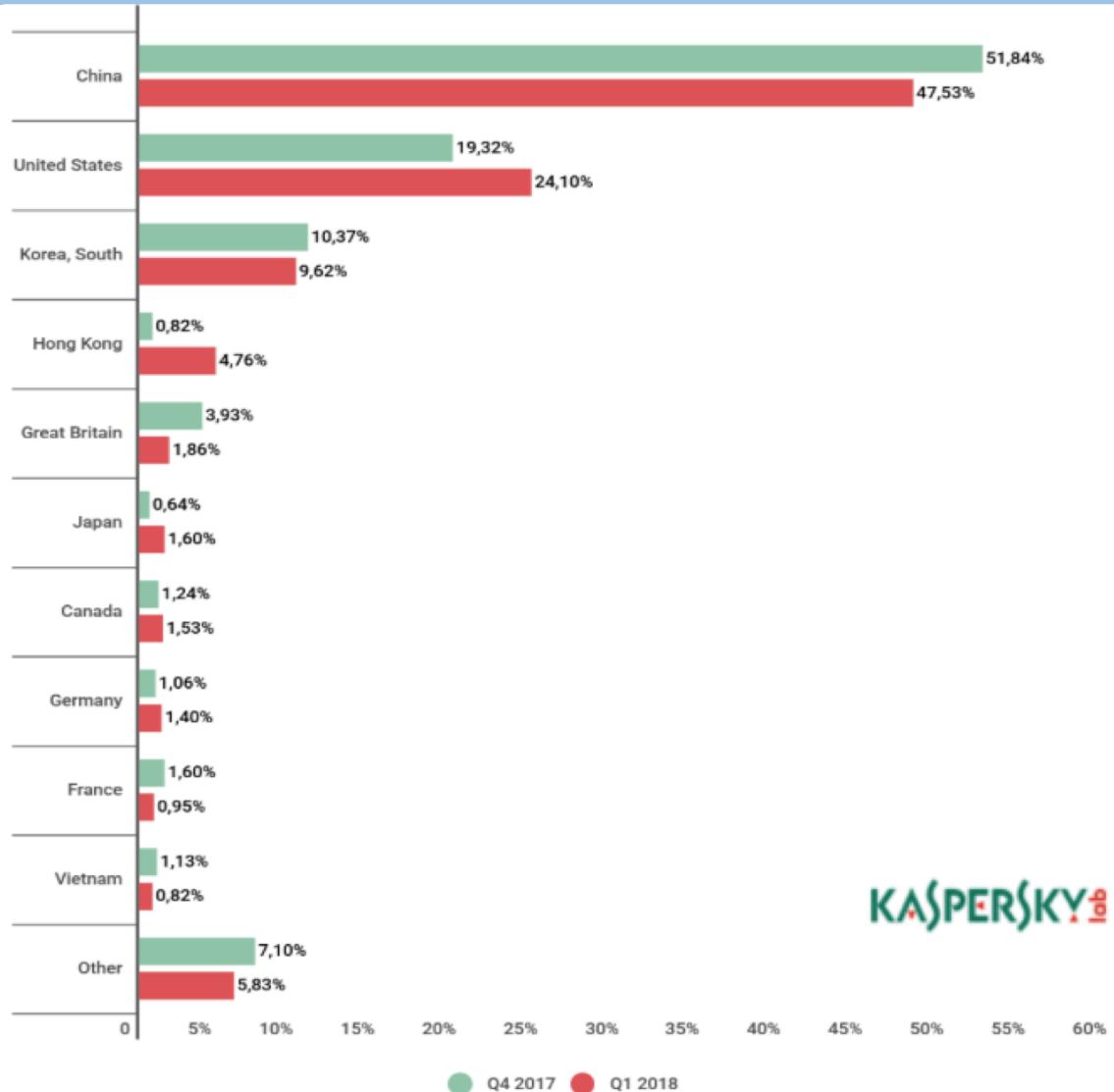


Distribution of DDoS attacks by duration (hours), Q4 2017 and Q1 2018



Most targeted countries

Distribution of unique DDoS-attack targets by country, Q4 2017 and Q1 2018



KASPERSKY

DDoS et Botnets

"DDoS attacks are attempts to make a computer resource (i.e. website, e-mail, VoIP, or a whole network) unavailable to its intended users. Overwhelmed with massive amounts of unsolicited data and/or requests, the target system either responds so slowly as to be unusable or crashes completely. The data volumes required to do this are typically achieved by a network of remotely controlled zombie or botnet (robot network) computers." Prolexic

C'est quoi un Botnet ?????

Botnets

“A botnet is a collection of compromised machines (bots) receiving and responding to commands from a server (the C&C server) that serves as a rendezvous mechanism for commands from a human controller (the botmaster)”. Khattak et al.

“Botnets are networks formed by “enslaving” host computers, called bots (derived from the word robot), that are controlled by one or more attackers, called bot-masters, with the intention of performing malicious activities”. Silva et al.

Botnets: Danger

Les *botnets* sont considérés comme étant la menace la plus importante pour la sécurité et la stabilité d'Internet. Ces réseaux sont créés afin de pouvoir mener des activités illégales à très grande échelle, telles que les attaques DDoS, fraudes au clic, envoi massif de courriers indésirables et vol d'identité

Les *botnets* peuvent infliger de graves dommages et être ainsi nuisibles à la sécurité globale de l'Internet. Environ **80%** du trafic de messagerie électronique est du courrier indésirable (***spam***) et la majeure partie de ces messages est générée par des *botnets*.

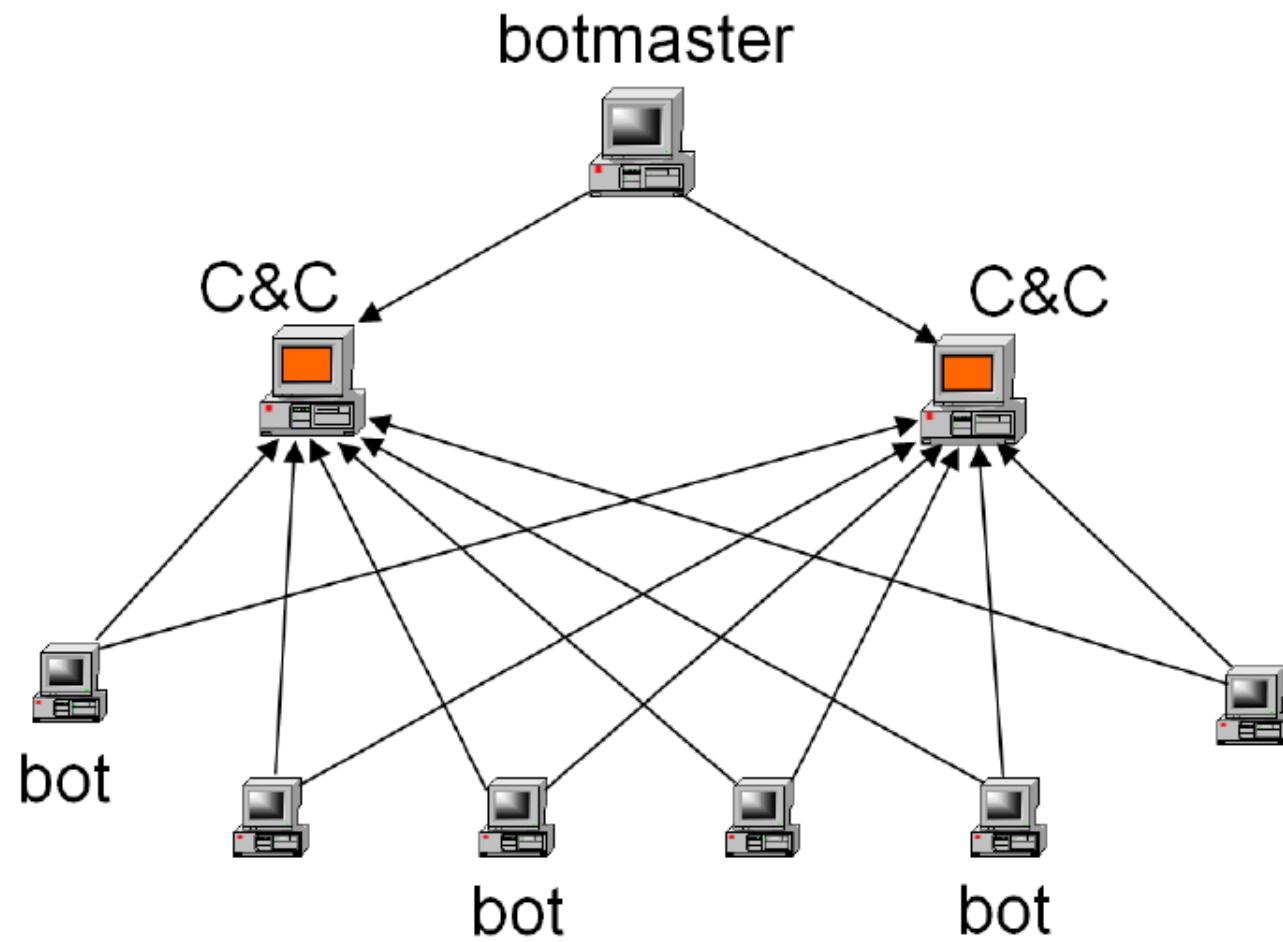
En 2007, l'International Telecommunication Union a estimé que les pertes causées par ce type de courriers reviennent à 100 milliards US\$ dont 35 milliards US\$ uniquement aux Etats Unis.

Botnets: Danger

- DDoS
- Spam
- Vol de données
- Hébergement de BlockChains
- Click Fraud

Botnets: Architectures

Centralisée



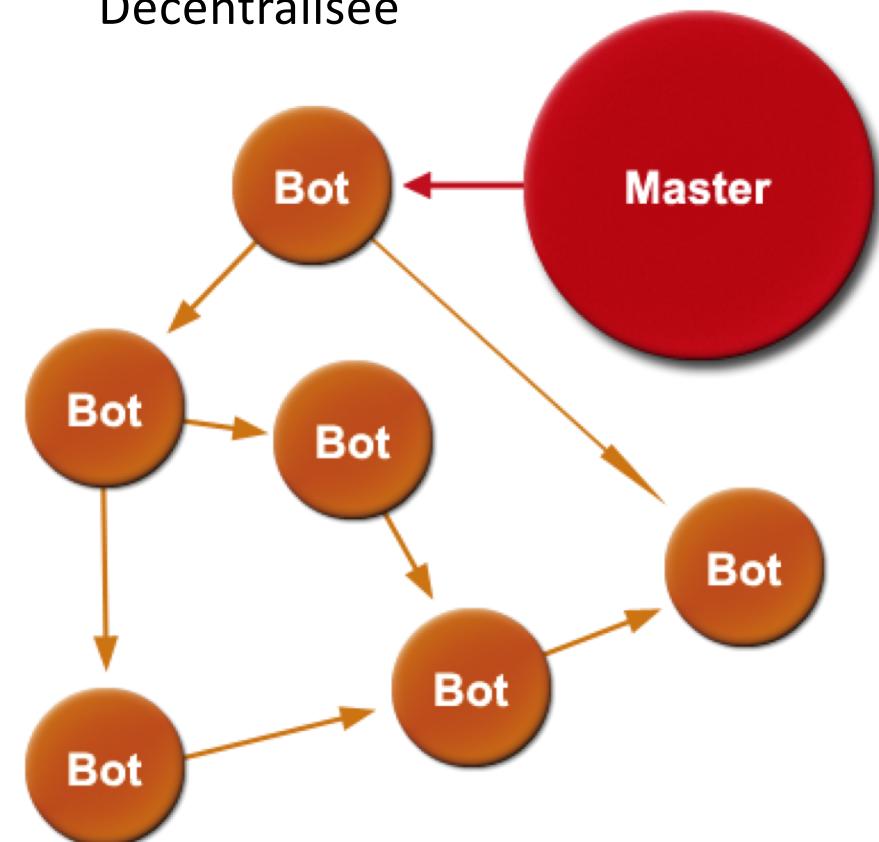
Botnets: Architectures

Les *botnets* décentralisés sont généralement basés sur une variété de protocoles pair à pair (P2P) et fonctionnent tel un réseau *overlay*.

Overlay pair-à-pair structuré : utilise souvent des Tables de Hachage Distribuées (DHT), telle que celles basées sur les protocoles CAN, Chord, Pastry et Tapestry. Ce type d'architecture permet une communication ciblée et optimale entre les différents noeuds du réseau.

Overlay pair-à-pair non-structuré : Ce type de réseaux fait référence aux topologies aléatoires avec différents degrés de distribution. Ainsi, ils n'offrent aucune possibilité de routage.

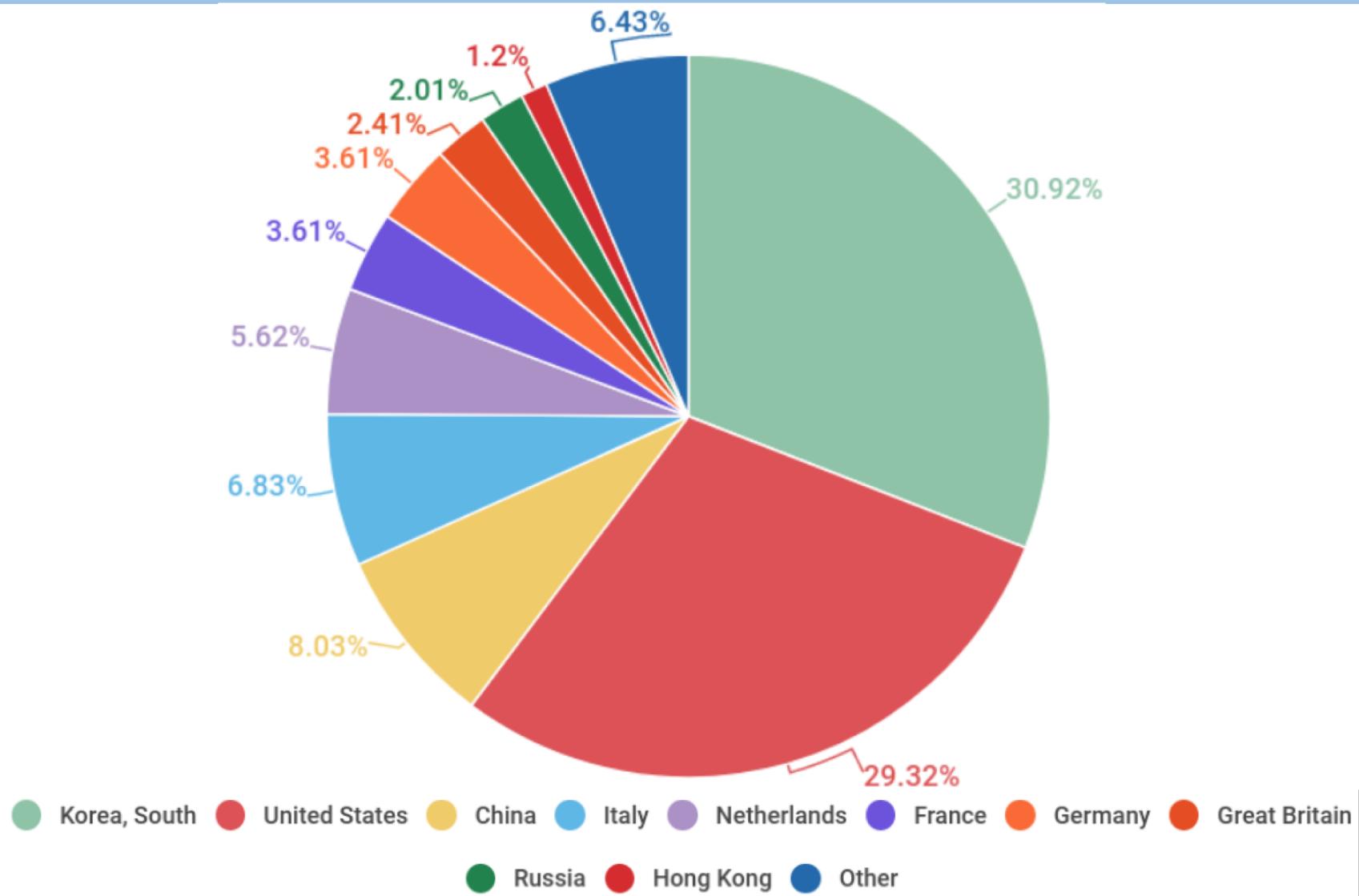
Décentralisée



Botnets: Architectures

Hybride: les *bots* d'un *botnet* hybride peuvent être classifiés en deux groupes : les *bots servants* et les *bots clients*. Les *bots servant* se comportent comme des serveurs et comme des clients. Ils sont configurés avec des adresses IP statiques et routables. Les *bots clients* sont configurés avec des adresses IP dynamiquement et non routables et n'acceptent aucune connexion entrante.

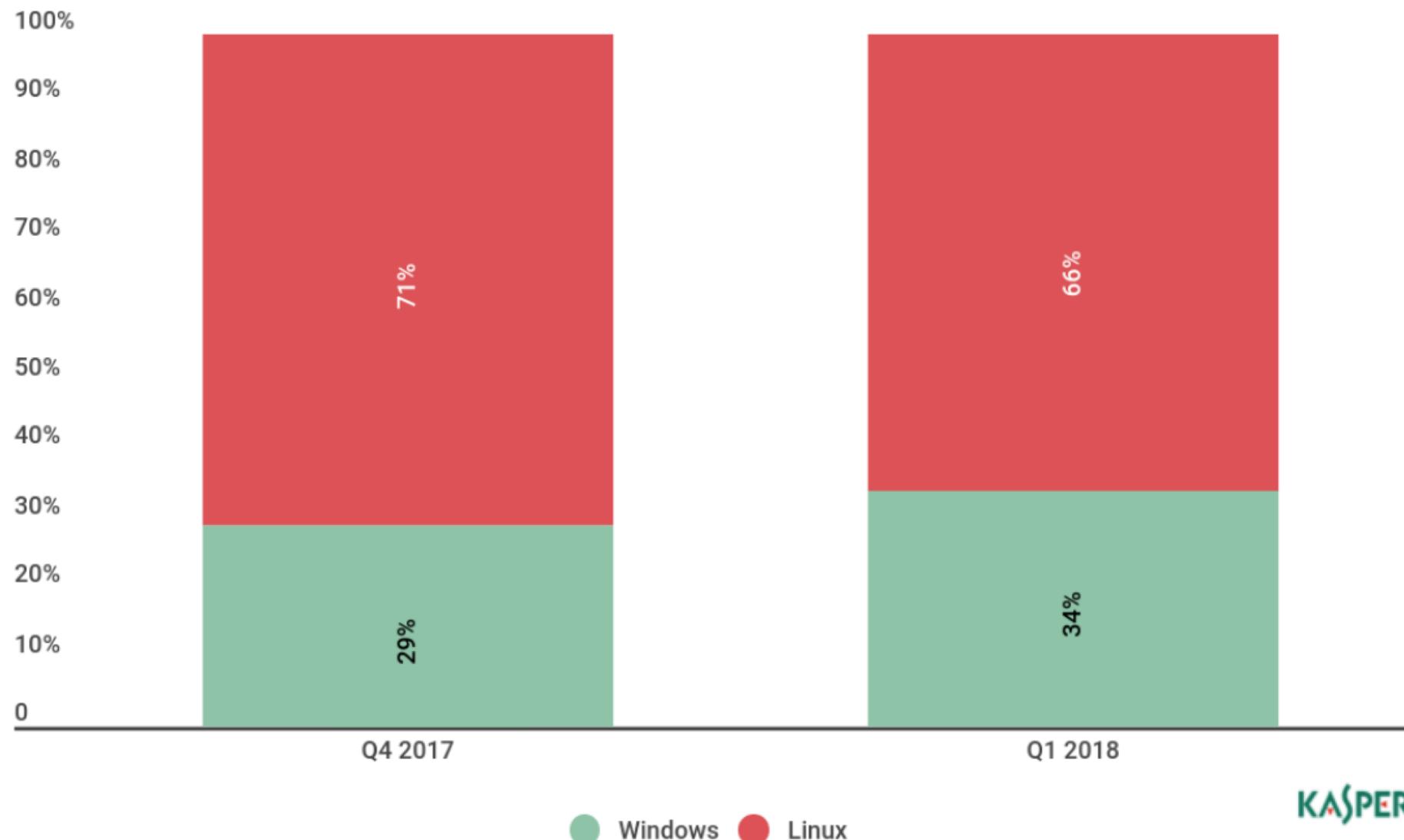
Distribution of botnet C&C servers by country in Q1 2018



Botnets: Protocols de communication

- ***Internet Relay Chat (IRC)*** : le *botmaster* crée des canaux IRC sur les serveurs C&C sur lesquels les *bots* vont se connecter et attendre les commandes. IRC permet la communication à travers des groupes de multicast appelée “canaux de communication” ou à travers des communications unicast privées entre deux membres. Cette caractéristique permet au *botmaster* d'avoir un contrôle flexible sur son *botnet* .
Exemples: Kaiten , Agobot, Rxbot, Sdbot et EggDrop
- ***HyperText Transfer Protocol (HTTP)*** : Face aux inconvénients du protocole IRC, le protocole HTTP a été proposé pour assurer les communications du C&C. Comparativement, son principal avantage réside dans la permissivité du trafic HTTP qui est autorisé dans la plupart des réseaux et qui permet de dissimuler les communications au sein du *botnet*.
Exemple: **Zeus**, Hybrid_V1.0, Festi, Bobax, Asprox, Srizbi

Correlation between Windows and Linux-based botnet attacks, Q1 2018

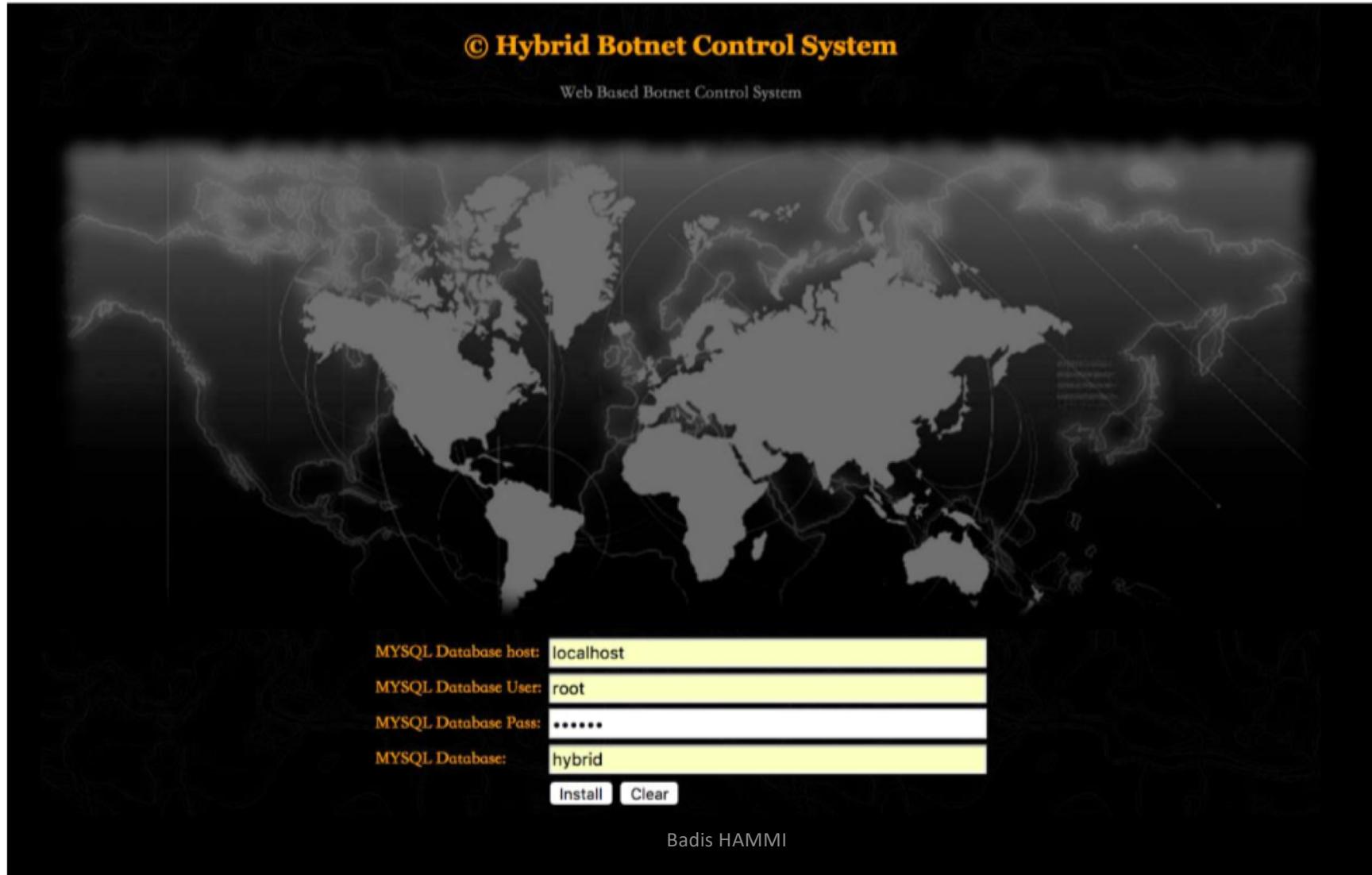


KASPERSKY[®]

Botnets: Cas d'étude

- Composition du Botmaster:
 - Base de données
 - Serveur HTTP
 - IHM

Botnets: Cas d'étude



Botnets: Cas d'étude

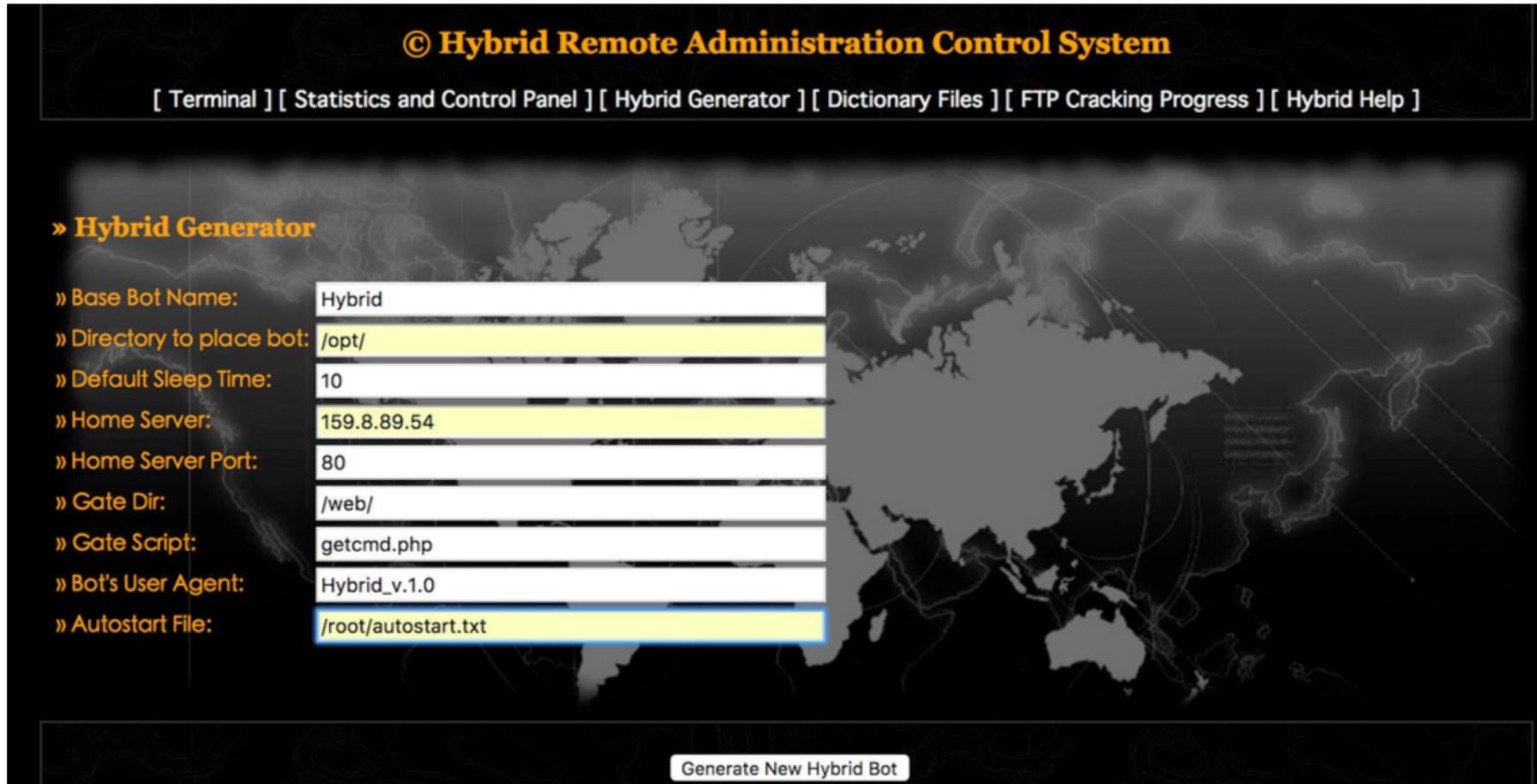
© Hybrid Remote Administration Control System

[Terminal] [Statistics and Control Panel] [Hybrid Generator] [Dictionary Files] [FTP Cracking Progress] [Hybrid Help]

» Hybrid Generator

» Base Bot Name:	Hybrid
» Directory to place bot:	/opt/
» Default Sleep Time:	10
» Home Server:	159.8.89.54
» Home Server Port:	80
» Gate Dir:	/web/
» Gate Script:	getcmd.php
» Bot's User Agent:	Hybrid_v.1.0
» Autostart File:	/root/autostart.txt

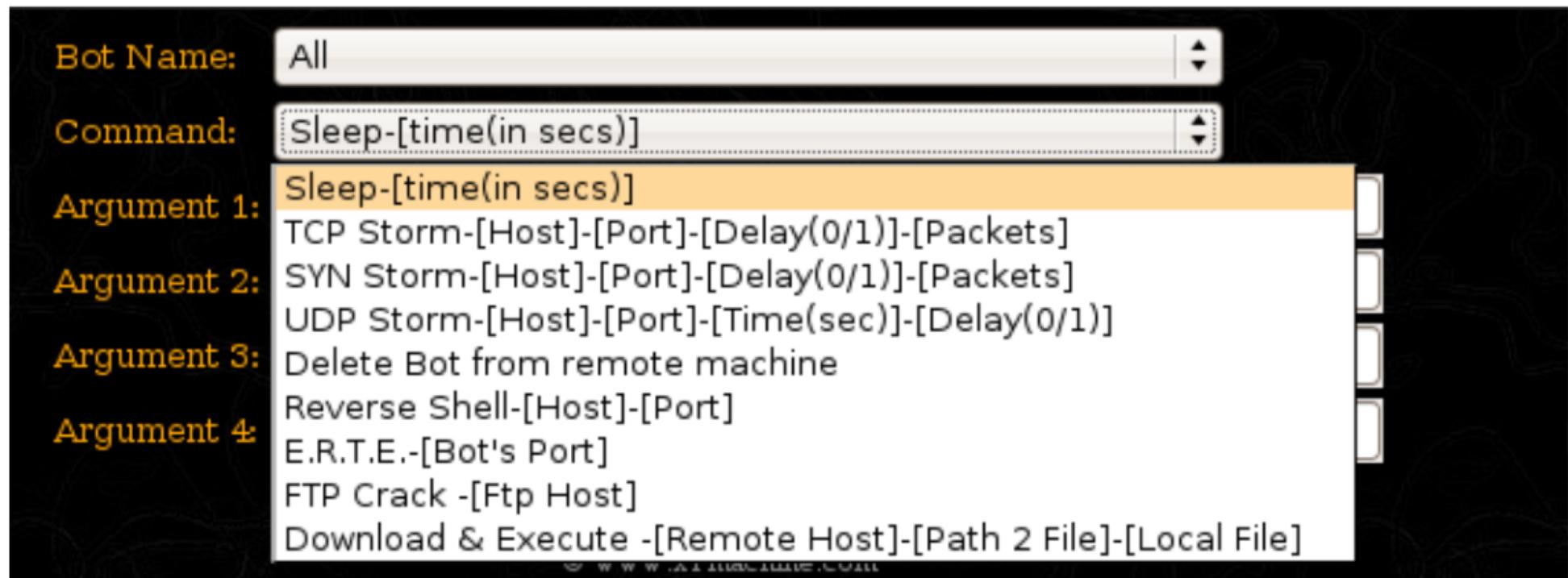
Generate New Hybrid Bot



Botnets: Cas d'étude

» Bot IP «	» Country «	» Current Command «	» Bot Name «	» Bot Message «	» Check «	» Action «
47.89.187.196	Canada		/opt/Hybrid_root_Ouefi	Unknown Command	<input type="checkbox"/>	Delete
173.255.113.41			/opt/Hybrid_pedouard78450_Xi7VW	Unknown Command	<input type="checkbox"/>	Delete
47.89.190.168	Canada		/opt/Hybrid_root_MChG6	Unknown Command	<input type="checkbox"/>	Delete
47.89.178.242	Canada		/opt/Hybrid_root_HjqaU	Unknown Command	<input type="checkbox"/>	Delete
146.148.39.54	United States		/opt/Hybrid_pedouard78450_cJZlu	Unknown Command	<input type="checkbox"/>	Delete
104.197.49.121			/opt/Hybrid_pedouard78450_BysbF	Unknown Command	<input type="checkbox"/>	Delete
104.197.233.90			/opt/Hybrid_pedouard78450_oeEvQ	Unknown Command	<input type="checkbox"/>	Delete
104.197.191.35			/opt/Hybrid_pedouard78450_Fxjyv	Unknown Command	<input type="checkbox"/>	Delete
159.8.96.86	Switzerland		/opt/Hybrid_root_8h2Ni	Unknown Command	<input type="checkbox"/>	Delete
159.8.126.35	Switzerland		/opt/Hybrid_root_ROM1j	Unknown Command	<input type="checkbox"/>	Delete
82.223.67.106	Spain		/opt/Hybrid_root_DgHGM	Unknown Command	<input type="checkbox"/>	Delete
35.167.15.4	United States		/opt/Hybrid_ubuntu_UrfeX	Unknown Command	<input type="checkbox"/>	Delete
35.164.178.68	United States		/opt/Hybrid_ubuntu_QOtoK	Unknown Command	<input type="checkbox"/>	Delete
104.199.5.139			/opt/Hybrid_christophe_ozkur_icBhM	Unknown Command	<input type="checkbox"/>	Delete
104.199.91.145			/opt/Hybrid_christophe_ozkur_rDziw	Unknown Command	<input type="checkbox"/>	Delete
130.211.48.242	United States		/opt/Hybrid_mhaocn1990_ox0ooBTC	Unknown Command	<input type="checkbox"/>	Delete
104.199.81.220			/opt/Hybrid_mhaocn1990_T21Uz Badis HAMMI	Unknown Command	<input type="checkbox"/>	Delete
104.199.72.140			/opt/Hybrid_mhaocn1990_zoo4N	Unknown Command	<input type="checkbox"/>	Delete

Botnets: Cas d'étude



Botnets: Cas d'étude

	104.155.119.59		10000	/opt/Hybrid_mhaocn1990_0x000BTC	TCP Storm	<input type="checkbox"/>	Delete
130.211.48.242	United States	ddos 54.218.105.235 80 0 10000		/opt/Hybrid_mhaocn1990_oxoooBTC	TCP Storm	<input type="checkbox"/>	Delete
146.148.13.176	United States	ddos 54.218.105.235 80 0 10000		/opt/Hybrid_christophe_ozkur_7BoGR	TCP Storm	<input type="checkbox"/>	Delete
104.197.233.90		ddos 54.218.105.235 80 0 10000		/opt/Hybrid_pedouard78450_odEvQ	TCP Storm	<input type="checkbox"/>	Delete
104.155.1.26		ddos 54.218.105.235 80 0 10000		/opt/Hybrid_mhaocn1990_4JhYo	TCP Storm	<input type="checkbox"/>	Delete
173.255.113.41		ddos 54.218.105.235 80 0 10000		/opt/Hybrid_pedouard78450_Xi7VW	TCP Storm	<input type="checkbox"/>	Delete
104.199.81.220		ddos 54.218.105.235 80 0 10000		/opt/Hybrid_mhaocn1990_T21Uz	TCP Storm	<input type="checkbox"/>	Delete
146.148.39.54	United States	ddos 54.218.105.235 80 0 10000		/opt/Hybrid_pedouard78450_eJZlu	TCP Storm	<input type="checkbox"/>	Delete
104.197.191.35		ddos 54.218.105.235 80 0 10000		/opt/Hybrid_pedouard78450_Fxjyv	TCP Storm	<input type="checkbox"/>	Delete
104.199.72.140		ddos 54.218.105.235 80 0 10000		/opt/Hybrid_mhaocn1990_zoo4N	TCP Storm	<input type="checkbox"/>	Delete
104.197.49.121		ddos 54.218.105.235 80 0 10000		/opt/Hybrid_pedouard78450_BysbF	TCP Storm	<input type="checkbox"/>	Delete
104.155.5.98		ddos 54.218.105.235 80 0 10000		/opt/Hybrid_christophe_ozkur_xgvPR	TCP Storm	<input type="checkbox"/>	Delete
104.199.5.139		ddos 54.218.105.235 80 0 10000		/opt/Hybrid_christophe_ozkur_icBhM	TCP Storm	<input type="checkbox"/>	Delete
104.199.91.145		ddos 54.218.105.235 80 0 10000		/opt/Hybrid_christophe_ozkur_rDziw	TCP Storm	<input type="checkbox"/>	Delete

Bot Name:

Command:

Argument 1:

Argument 2:

Argument 3:

Argument 4: Badis HAMMI

Botnets: Cas d'étude

* Bot IP *	* Country *	* Current Command *	* Bot Name *	* Bot Message *	* Check *	* Action *
82.223.67.106	Spain	ddos 54.218.105.235 80 0 10000	/opt/Hybrid_root_DgHGM	TCP Storm	<input type="checkbox"/>	Delete
52.212.1.70	United States	ddos 54.218.105.235 80 0 10000	/opt/Hybrid_ubuntu_ReRXB	TCP Storm	<input type="checkbox"/>	Delete
47.89.187.196	Canada	ddos 54.218.105.235 80 0 10000	/opt/Hybrid_root_Ouefi	TCP Storm	<input type="checkbox"/>	Delete
52.213.240.153	United States	ddos 54.218.105.235 80 0 10000	/opt/Hybrid_ubuntu_XPq6G	TCP Storm	<input type="checkbox"/>	Delete
47.89.178.242	Canada	ddos 54.218.105.235 80 0 10000	/opt/Hybrid_root_HjqaU	TCP Storm	<input type="checkbox"/>	Delete
159.8.126.35	Switzerland	ddos 54.218.105.235 80 0 10000	/opt/Hybrid_root_ROMIj	TCP Storm	<input type="checkbox"/>	Delete
159.8.96.86	Switzerland	ddos 54.218.105.235 80 0 10000	/opt/Hybrid_root_8h2Ni	TCP Storm	<input type="checkbox"/>	Delete
35.167.15.4	United States	sleep 6	/opt/Hybrid_ubuntu_UrfcX	Sleeping...	<input type="checkbox"/>	Delete
47.89.190.168	Canada	ddos 54.218.105.235 80 0 10000	/opt/Hybrid_root_MChG6	TCP Storm	<input type="checkbox"/>	Delete
35.164.178.68	United States	sleep 6	/opt/Hybrid_ubuntu_QOtoK	Done	<input type="checkbox"/>	Delete
104.155.119.59		ddos 54.218.105.235 80 0 10000	/opt/Hybrid_mhaocn1990_UtEij	TCP Storm	<input type="checkbox"/>	Delete
130.211.48.242	United States	ddos 54.218.105.235 80 0 10000	/opt/Hybrid_mhaocn1990_oxoooBTC	TCP Storm	<input type="checkbox"/>	Delete
146.148.13.176	United States	ddos 54.218.105.235 80 0 10000	/opt/Hybrid_christophe_ozkur_7BoGR	TCP Storm	<input type="checkbox"/>	Delete
104.197.233.90		ddos 54.218.105.235 80 0 10000	/opt/Hybrid_pedouard78450_odEvQ	TCP Storm	<input type="checkbox"/>	Delete
104.155.1.26		ddos 54.218.105.235 80 0 10000	/opt/Hybrid_mhaocn1990_4JhYo	TCP Storm	<input type="checkbox"/>	Delete
173.255.113.41		ddos 54.218.105.235 80 0 10000	/opt/Hybrid_pedouard78450_Xi7VW	TCP Storm	<input type="checkbox"/>	Delete
104.199.81.220		ddos 54.218.105.235 80 0 10000	/opt/Hybrid_mhaocn1990_T21Uz	TCP Storm	<input type="checkbox"/>	Delete
146.148.39.54	United States	ddos 54.218.105.235 80 0 10000	Badis.HAMMI /opt/Hybrid_pedouard78450_cJZlu	TCP Storm	<input type="checkbox"/>	Delete

Botnets: Cas d'étude

Voir Code du Bot

Retour vers les DDoS

Quelles sont les motivations du hacker /cracker?

- La rancune
- Le défi !!! un réseau se vante de la sécurité de son système !
- La curiosité ou l'ennui
- L'engagement politique
- La stupidité ! Pour Impressionner les amis...



Rappel : la loi sanctionne ...

- En France, la loi punit cet acte sévèrement
 - L'article 323-2 prévoit des peines de 5 ans de prison ferme et 75000€ d'amende pour "*le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données*"
 - Les mouvements coordonnés sont aussi prévus par la loi française : "*La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée* »
- Les peines prévues au sein des autres pays d'Europe
 - 3 ans en Belgique, 6 ans au Pays-Bas, jusqu'à 10 ans au Royaume-Uni...

- Botnet + DDoS c'est dangereux mais ça peu aller jusq'où ???

Évolution des attaques DDoS

• Types d'attaques

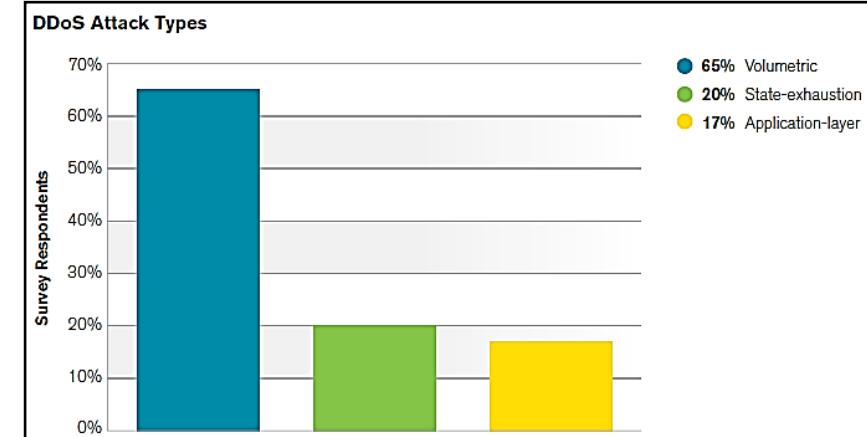
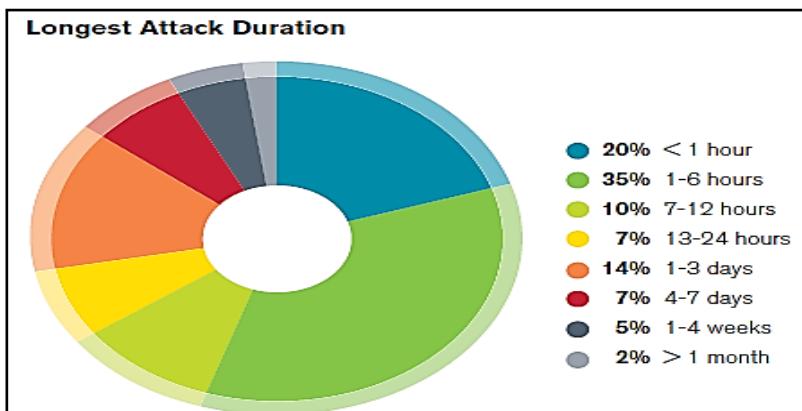
- Attaques volumétriques sont les plus fréquentes
- Attaques de plus en plus puissantes
- Attaques multivecteurs sont de plus en plus fréquentes

• Services Cibles

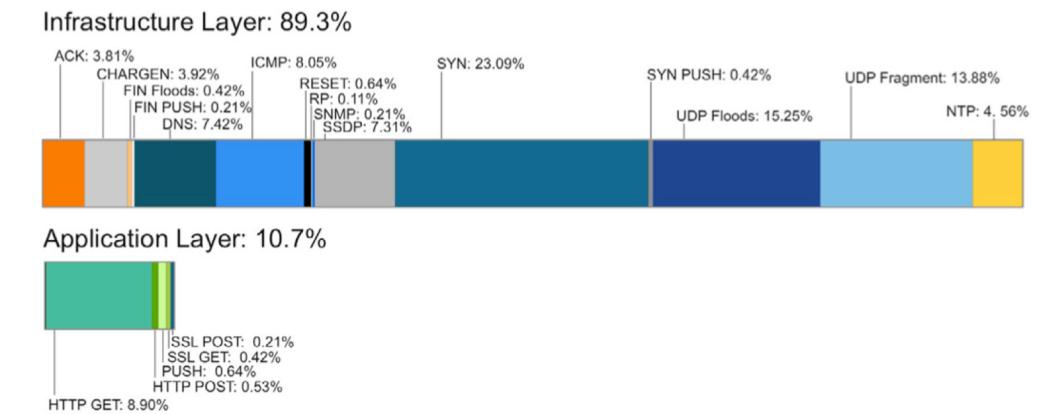
- HTTP devient le service le plus ciblé
- DNS gagne du terrain d'une année à l'autre

• Fréquences des attaques

- Attaques qui durent longtemps sont en baisse
- 2h - 6 h en moyenne / attaque



Q3 2014 attack vectors



Badis HAMMI

Évolution des attaques DDoS

Thread Tools | Display Modes

Yesterday, 08:58 PM #1

 **Citzoothe** ●
Junior Member

Join Date: Jun 2009
Location: Russia
Posts: 1 

 **DDos attack - Kill an enemy or a competitor's site!**

Tired of a competitor's site? Hinder the enemy? Fed pioneers or copywriters? Kill their sites! How? We will help you in this! Obstructions of any site, portal, shop! Different types of attacks: Date-attack, Trash, Attack, Attack, etc. Intellectual You can work on schedule, as well as the simultaneous attack of several sites. On average the data, ordered the site falls within 5 minutes after the start. As a demonstration of our capabilities, allows screening. Our prices 24 hours of attack - \$ 70 12 hours of the attack - \$ 50 1 hour attack - \$ 25 Contact via ICQ: 588 666 582

On average the data, ordered the site falls within 5 minutes after the start

 **Quote**

 **Post Reply**

Prix entre \$9 l'heure et \$67 la journée

Attaques DDoS: Visualisation

**Voir Attack Digital Map of
Arbor Networks**

Un peu d'histoire des attaques DDoS

- Ver de Morris

- 2 novembre 1988 : première bombe électronique
- Proof of concept mettait hors d'état de fonctionner 6.000 systèmes sur Internet (15%)
- Caractéristiques
 - Créé pour se propager en exploitant vulnérabilités et erreurs de configurations
 - Pas de possibilité de détecter sa présence sur un système
 - Se reproduire sur les systèmes distants, mais également en local
- Conséquence évidente
 - Des milliers de petits *process* tournaient sur le système cible et provoquaient le premier *DoS* massif de l'histoire

Un peu d'histoire des attaques DDoS

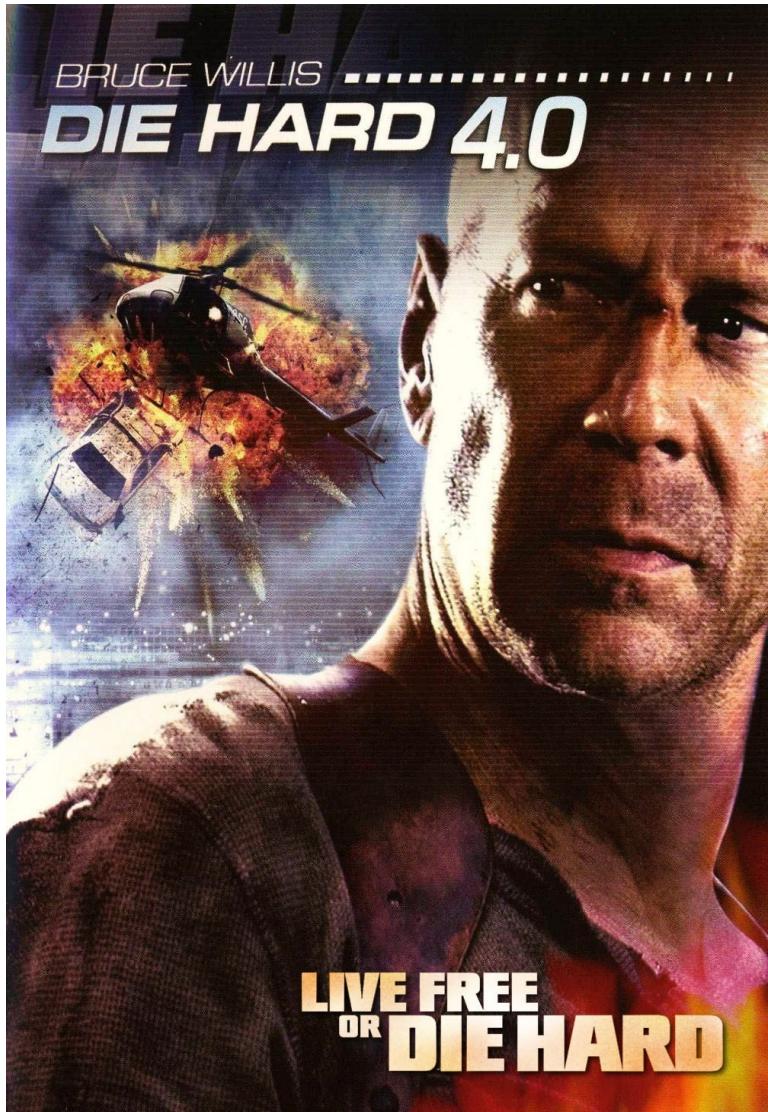
- Ping de la Mort - 1995
 - Premier déni de service fondé sur des anomalies
 - Paquets ICMP *Echo Request* fragmentés de plus de 65.535 octets
 - Caractéristiques
 - Presque aucun *stack* ne résistait à la puissance de l'attaque
 - Simplicité de mise en œuvre
 - Exemple au prompt Windows 95 ou NT4
 - ping www.serveurdoitmourir.com -l 65510



Un peu d'histoire des attaques DDoS

- 2000 :
 - DoS contre un certain nombre de grands sites américains Yahoo (inaccessible pour 3 heures, 500,000 \$ de perte), Buy(disponible que 10%), Stamps, eBay, CNN, Amazon(inaccessible 10 heures et 600,000\$ de perte), MSN et ZDNet
 - Perte de 1.7 milliards \$
 - Combinaison des outils : Trinoo, TFN, TFN2K, Stacheldraht
- 2002 :
 - DDoS contre 7 des 13 serveurs DNS
 - Paralyser le réseau mondial par l'impossibilité d'accéder au web.
 - Attaque par des paquets ICMP, TCP-SYN et UDP.
 - Débit variant entre 50 Mbps et 100 Mbps / serveur
- 2007 :
 - Attaque massive et coordonnée contre l'Estonie
 - 128 attaques en deux semaines
 - 115 en ICMP *floods*, 4 en TCP SYN *floods*, et 9 flux générique
- 2008 :
 - CNN était victime d'une attaque DDoS par un débit de 14 Mo/s
 - Ralentissements sur le site auraient été ressentis par les internautes asiatiques
 - Les contre-mesures qui étaient mises en place n'ont pas protégé le serveur
- 2009 :
 - *Cyber milice* russe met le Kirghizistan hors ligne
 - 3 FAI sont tombés

CyberWar: Estonie 2008



Badis HAMMI

CyberWar: Estonie 2008

Paralysie du système informatique:

- Banque
- Chaine d'infos
- Sites gouvernementaux



CyberWar: Estonie 2008



Badis HAMMI

CyberWar: Estonie 2008

Conséquence : *North Atlantic Treaty Organization (NATO)* intègre la notion de CyberGuerre



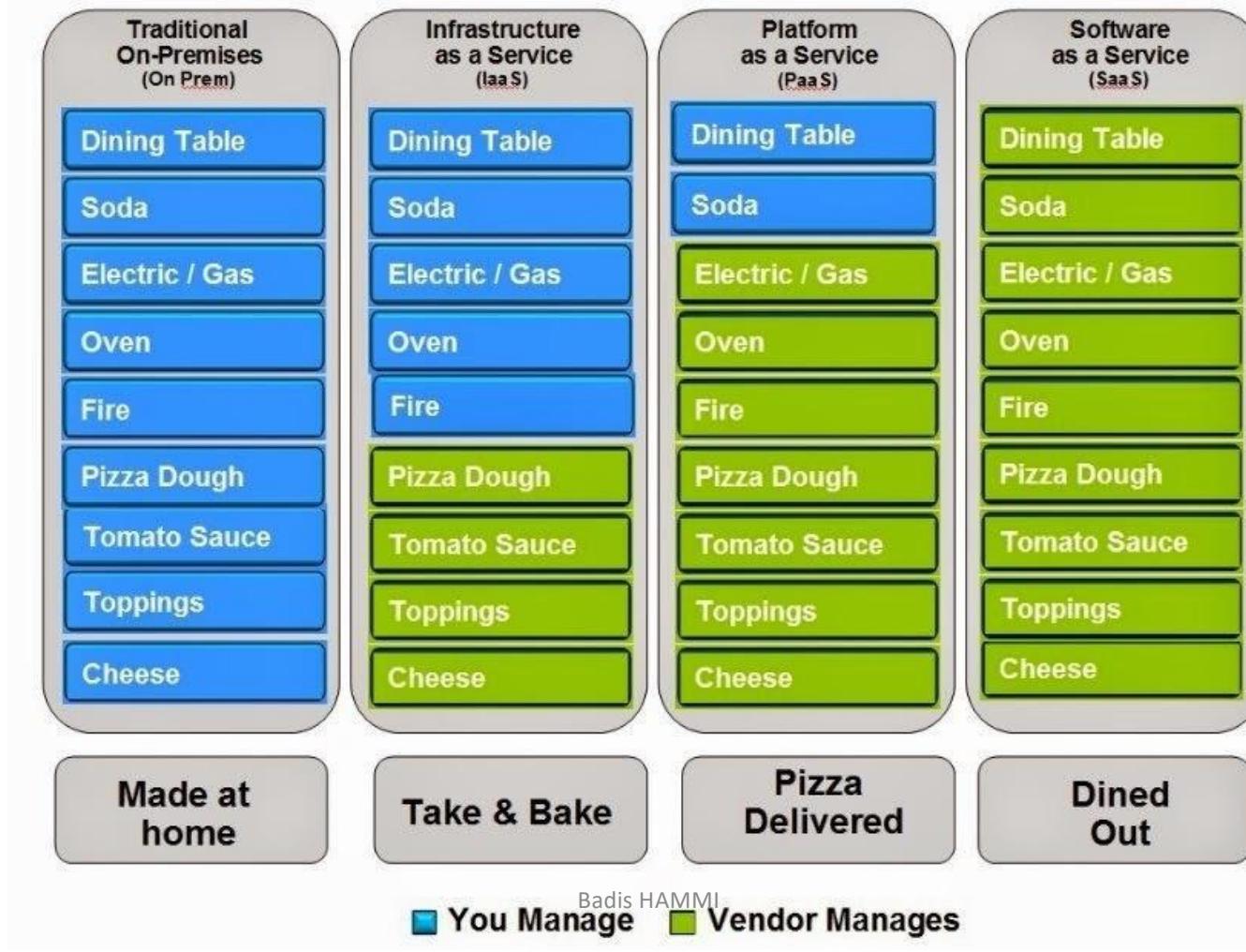
CyberWar

- Iran 2010
 - Guerre électronique contre l'Iran
 - Plusieurs milliers des ordinateurs hors service
 - Contre l'infrastructure de distribution de l'énergie
 - Logiciel malveillant considéré comme arme destinée à porter atteinte à la sécurité du territoire iranien
 - Cyberspace est devenu un théâtre d'un conflit géopolitique
 - Repenser la notion de territoire
- Cyberdefense
 - Ensemble des moyens physiques et virtuels mis en place par un pays dans le cadre de la guerre informatique menée dans le cyberspace
- Cyberspace
 - Une représentation mentale, un territoire virtuel, hors du monde physique dans lequel se déroulent échanges et interactions.

Nouvelle dimension: Botclouds

Cloud Computing services

Pizza as a Service



Nouvelle dimension pour les DDoS

- Attaque sur Spamhaus > 100 GBps 2013 → **cyberBunker**
- Attaque sur Sony playstation Networks :
 - Plus d'un mois de déni de service
 - 77 millions comptes utilisateurs volé
 - milliards de dollars
- 2014 > 300 GBps
- 2015 > 400 GBps



Détection

- HoneyPots
- Détection au niveau de la cible
- Détection au niveau du réseau intermédiaire
- Détection au niveau de la source
- Deux approches de détection
 - Détection comportementale
 - Détection à base de signature
- HIDS vs NIDS

Détection

- Techniques de mitigation utilisées par les entreprises
 - RTBH (Remotely Triggered Black Hole Filtering)
 - On-premises Appliance
- Gartner recommande
 - d'adopter des solutions de protection hybrides
 - de sélectionner une solution de protection anti-DDOS sont selon : la détection, la mitigation et la résilience
- Principaux fournisseurs de solutions de protection anti-DDOS :
 - Arbor Networks
 - Akamai/Prolexic
 - Check Point
 - Corero Network Security
 - F5 Networks
 - Juniper Networks
 - Radware
 - RioRey,
 - A10 Networks.

