



Tendances et défenses

Connaissances au profit de l'entreprise

Jean-Francois Gignac

Spécialistes sécurité – TIC – Marchés Affaires

514 870-7846


Agenda

1. Tendances Sécurité

- **Juillet 2009 – Un mois d'attaques cybernétiques**
- **Tendances des cyber crimes**

2. Pourquoi votre SPI (IPS) est probablement vulnérable



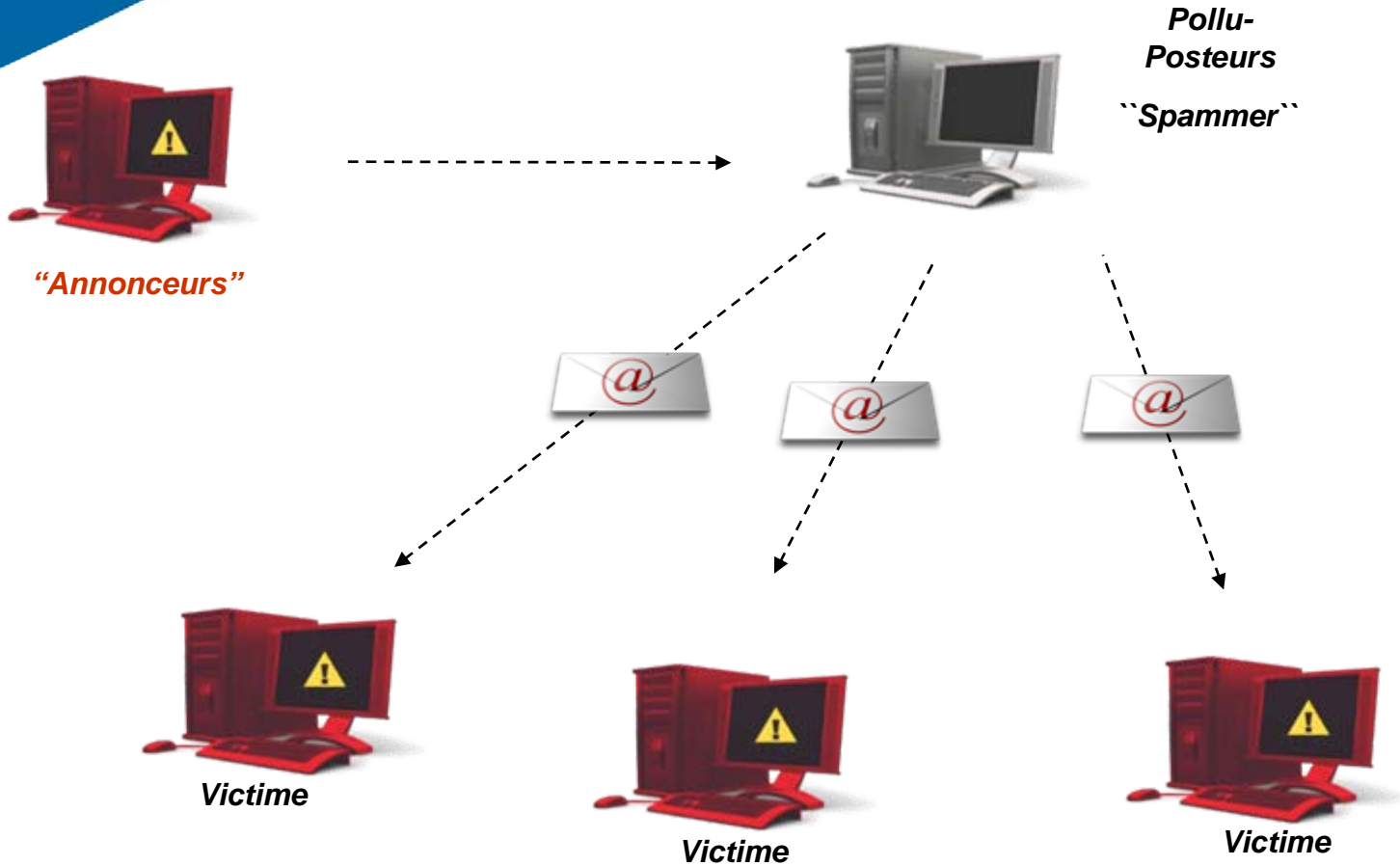


Survol des attaques cybernétiques de Juillet 2009 (Mydoom.EA or Dozer)

CONFIDENTIAL

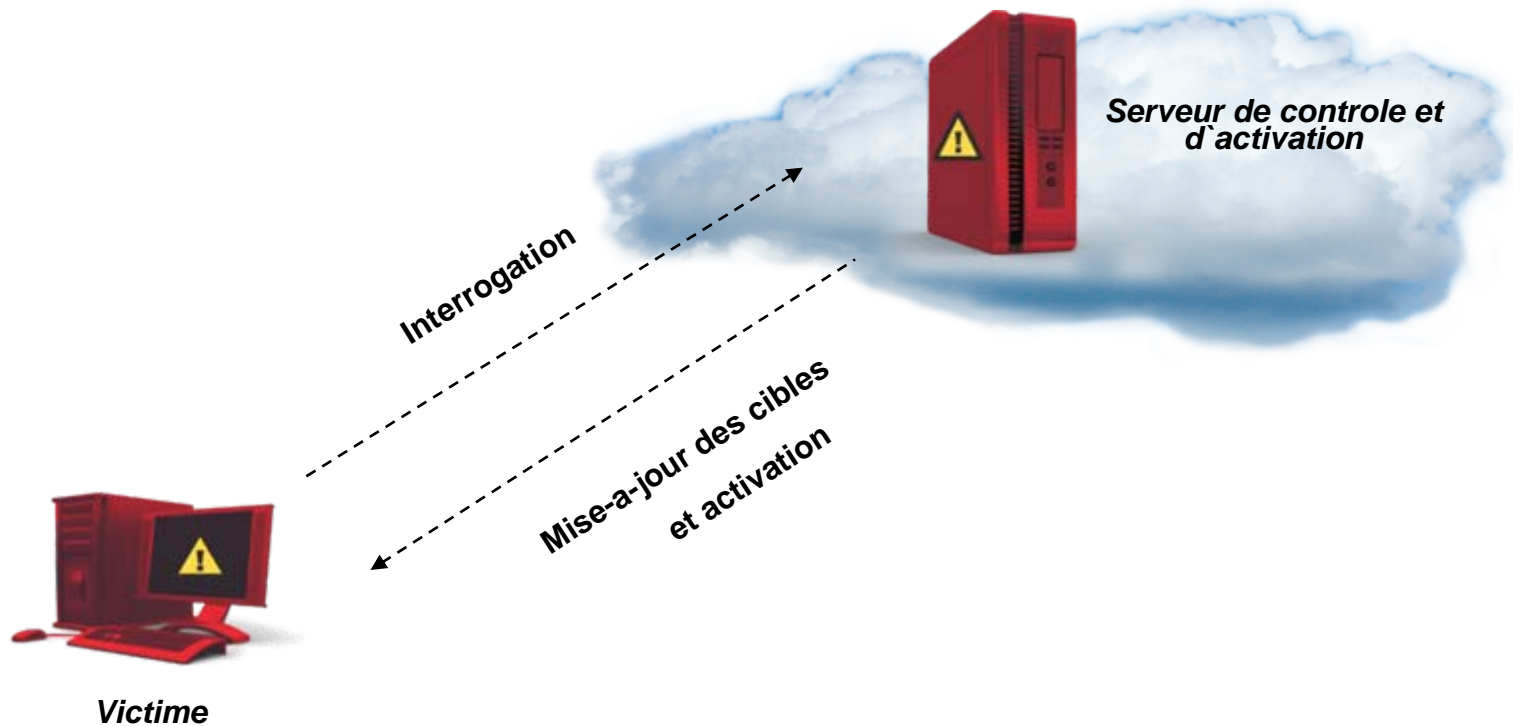
Bell

Répondre les maliciels ``Bot`` par courriel



CONFIDENTIAL

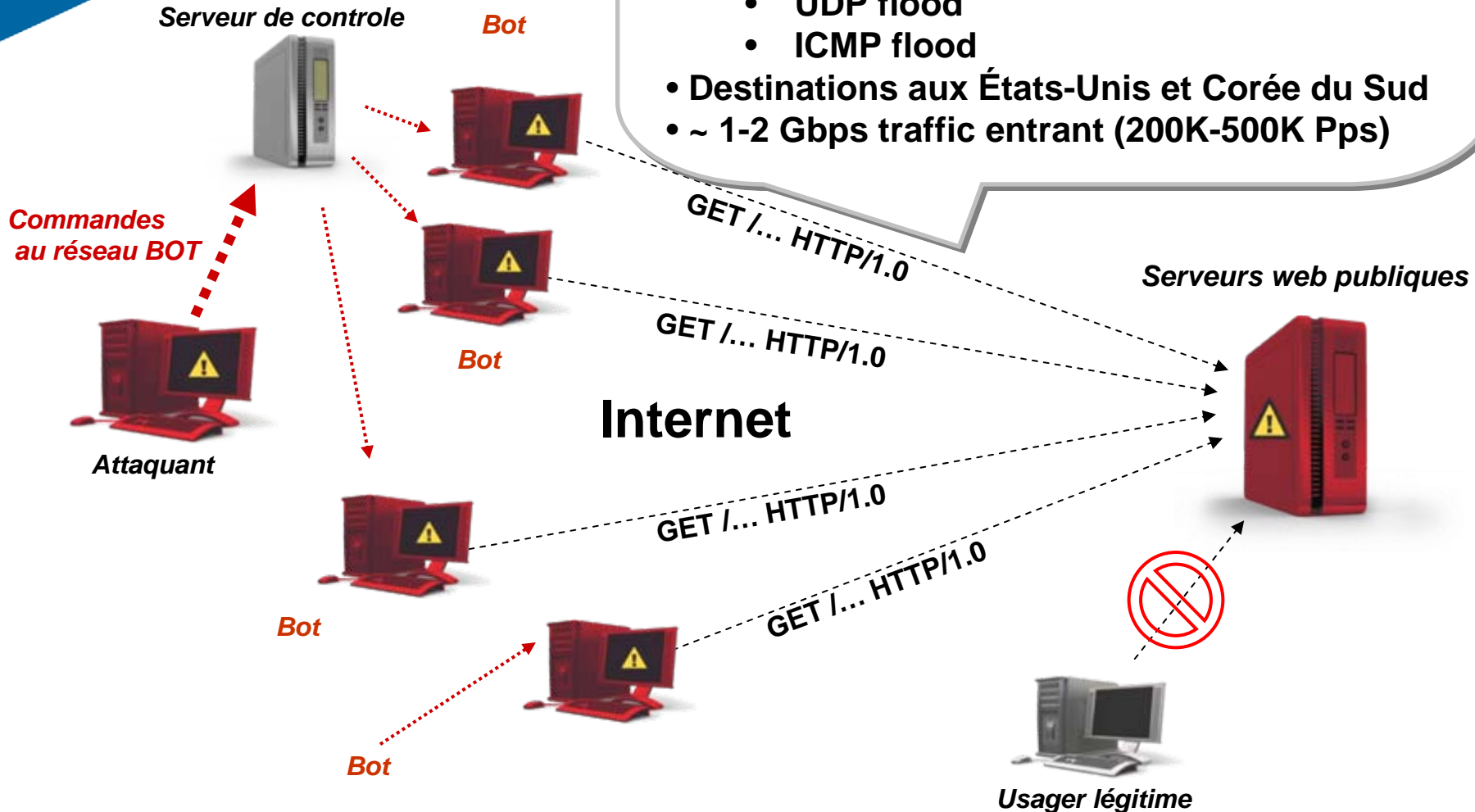
Activation du réseau des maliciels ``Bot``



1ere Attaque : MYDOOM.EA

Caracteristiques des ``Bot``

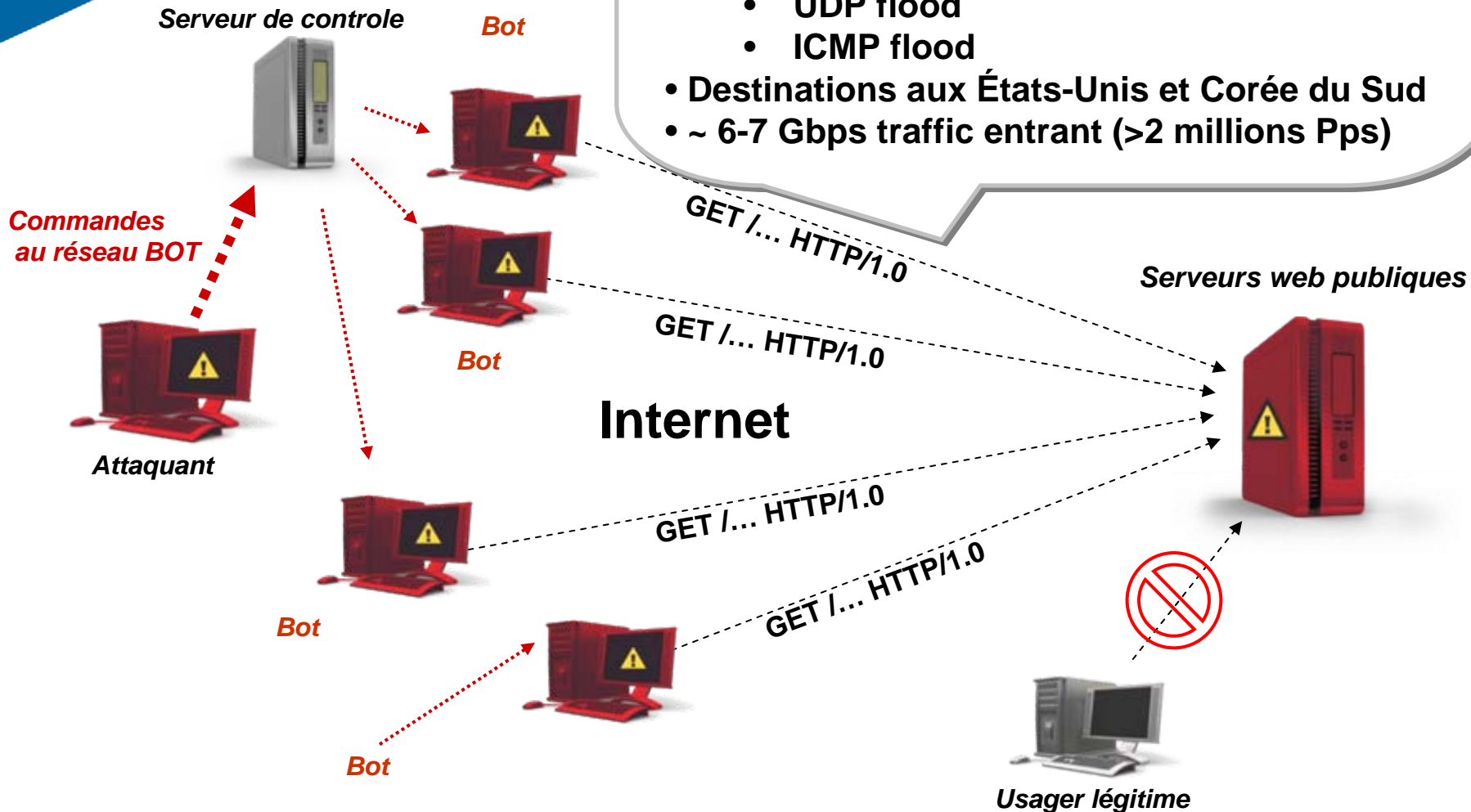
- ~20,000 ordinateurs zombies
- Attaques diversifiées:
 - HTTP page flood
 - SYN flood avec anomalies de paquets
 - UDP flood
 - ICMP flood
- Destinations aux États-Unis et Corée du Sud
- ~ 1-2 Gbps traffic entrant (200K-500K Pps)



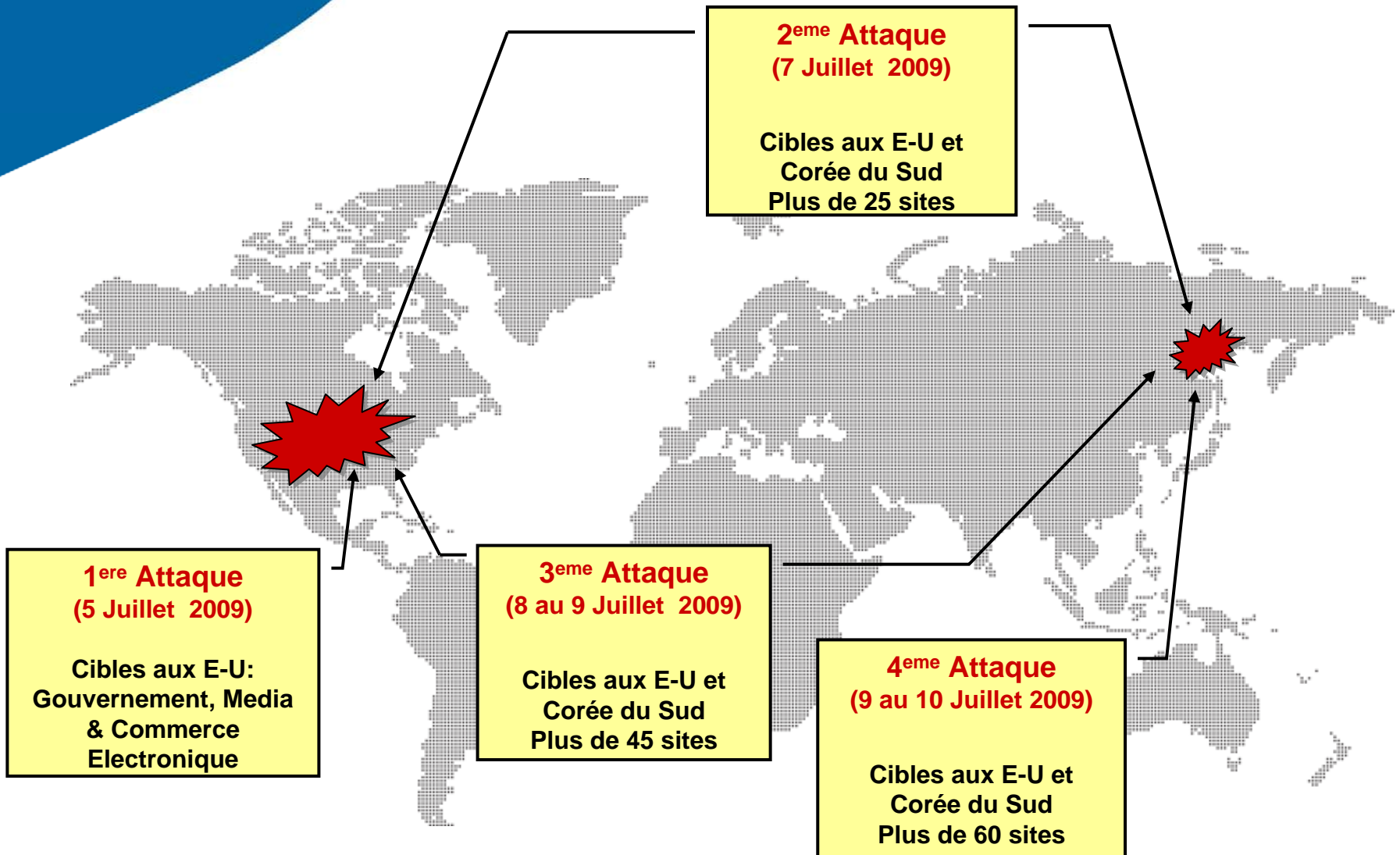
2eme Attaque : MYDOOM.EA

Caracteristiques des ``Bot``

- ~50,000 ordinateurs zombies
- Attaques diversifiées:
 - HTTP page flood
 - SYN flood avec anomalies de paquets
 - UDP flood
 - ICMP flood
- Destinations aux États-Unis et Corée du Sud
- ~ 6-7 Gbps traffic entrant (>2 millions Pps)



Attaques cybernétiques de Juillet 2009



- 1ere attaque – sites aux E-U

- www.whitehouse.gov
- www.nyse.com
- www.nasdaq.com
- finance.yahoo.com
- www.amazon.com
- www.usbank.com
- www.washingtonpost.com
- www.state.gov
- www.usauctionslive.com
- 5 Juillet 2009

- 2eme attaque – sites en Corée du Sud

- www.president.go.kr
- www.mofat.go.kr
- www.assembly.go.kr
- banking.nonghyup.com
- ezbank.shinhan.com
- ebank.keb.co.kr
- www.hannara.or.kr
- www.chosun.com
- www.auction.co.kr
- Activé 7-8 Juillet 2009

- 3eme et 4eme attaques

- Divers sites aux E-U et Corée du Sud
- 8-10 Juillet 2009



Massive Cyber Attack Knocked Out Government Web Sites Starting On July 4

En 2009, les attaques de juillet furent une série de cyber-attaques coordonnées contre des gouvernements majeurs, les médias, et les sites financiers américains et de Corée du Sud. Les attaques ont émis l'activation d'un réseau de botnet constitué de 20,000 à 40,000 ordinateurs infectés par des logiciels malveillants. Mydoom.EA fut une attaque inondant des sites Web causant des surcharges sur les serveurs en raison de l'afflux de trafic - une attaque DDoS. (Distributed Denial of Service)

La liste des cibles inclus aux E-U; la CIA, Département d'Etat américain, NASDAQ, US Bank, US Auctions Live.

Assurément, ces sites ont investi dans la sécurité réseau - cependant ils n'ont toujours pas réussi à atténuer une attaque relativement simple - une variante de Mydoom, connue depuis 2004



Korea
How Did It

ffPost



ich has
against
South
the
ther

g
ould be
tside

n the
ay
uesday
er
of
ea later

ocking, but a recent [series](#)
Korean Web sites was
than one might think.
ing a better understanding
d why it caused so many

Cyber Attaques de Juillet - Comprendre le défi

Outils d'attaque très dynamique

Le ``bot`` télécharge des fichiers “.exe” qui peuvent non seulement ajouter des fonctionnalités mais également fournir de nouvelles cibles

Les attaques sont diversifiées :

HTTP page flood

SYN flood

UDP flood

ICMP flood

Des attaques de natures fausses (spoofed - DDoS) and réels (HTTP flood)

Attaques hautement distribuées: 20,000-40,000 sources

Deni de service due aux HTTP flood targets qui paralysent les pages principales des sites web victimes.

Toutes méthodes de limitation du nombre d'utilisateurs bloquent complètement l'accès au site

Débit d'attaque très élevés

Le débit des attaques ont atteint jusqu'à 5-6 Gbps de trafic HTTP entrant en Corée du Sud



Cybercrime Trends



Hackers motivation change

From vandalism to financially-motivated

Botnets are the main tool against businesses

Organized crime manages cybercrime activities, targeting:

Extortion of online businesses

Financial fraud

Emerging network attacks

Attacks that misuse applications and services: Non-vulnerability based attacks

Uses legitimate application services for malicious activity

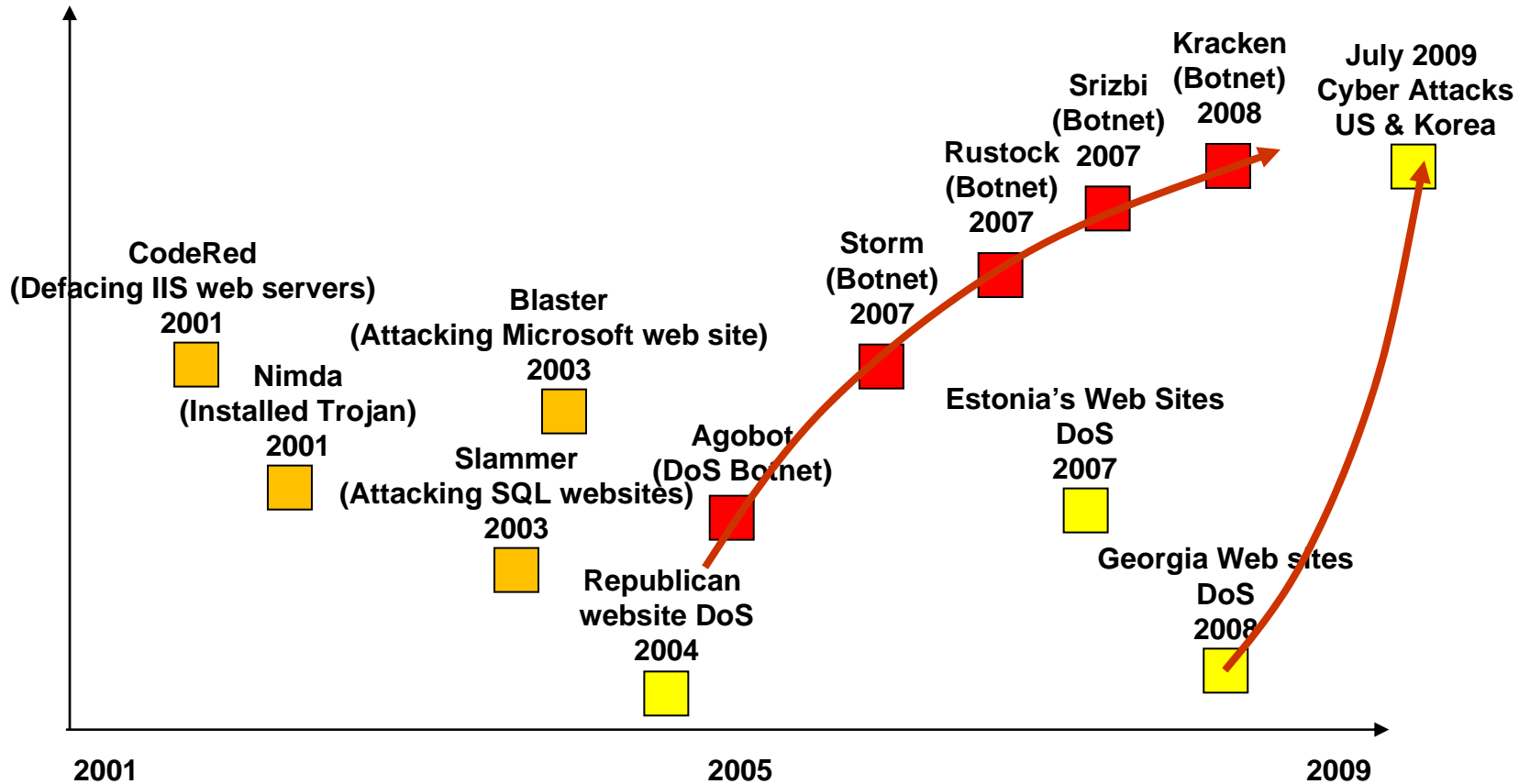
Each attack session behaves like a legitimate user transaction

Cannot be detected through a static signature because the attack does not exploit a vulnerability in the application

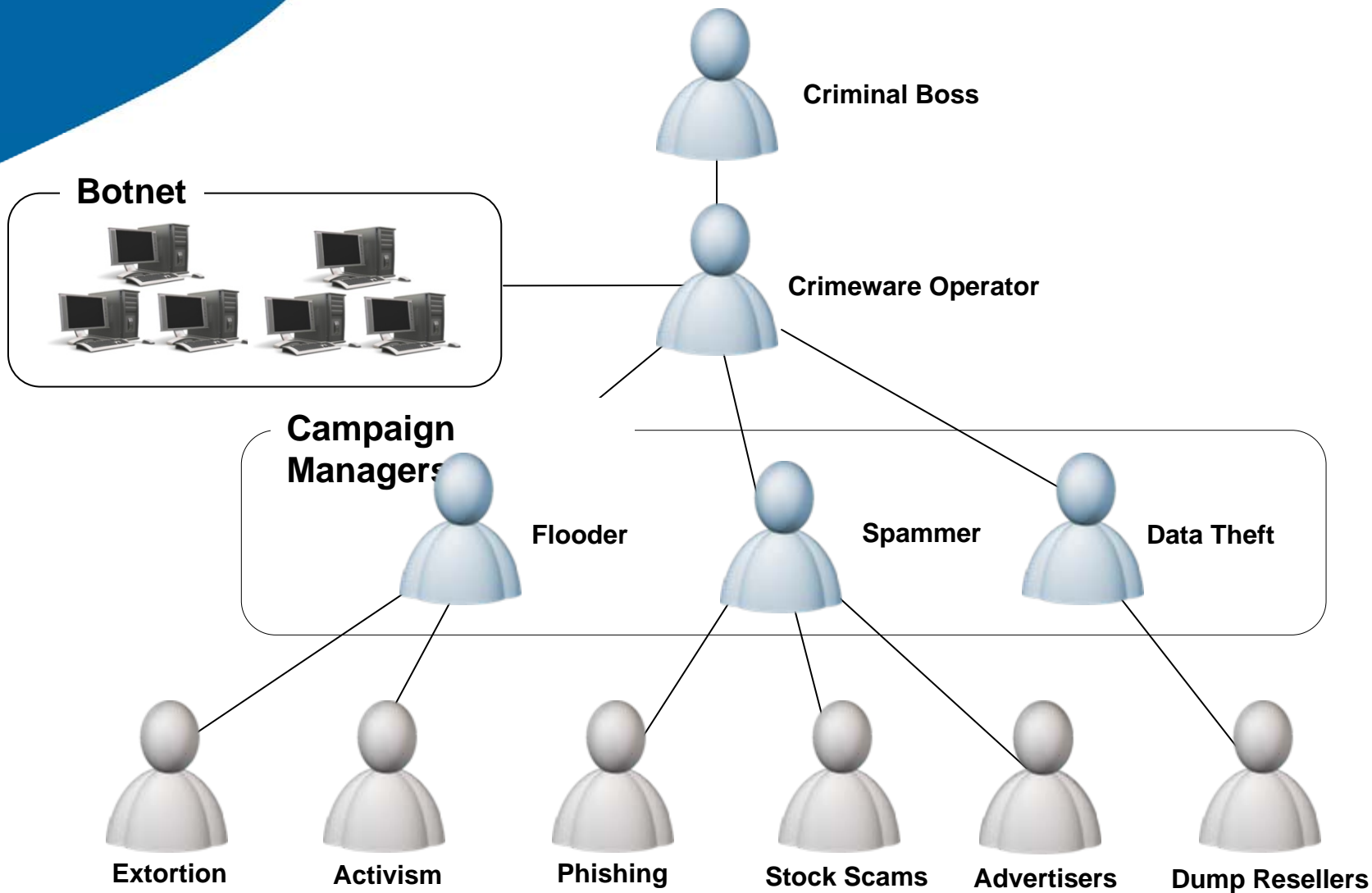
Examples: DDoS, HTTP page floods, brute force, application vulnerability scanning...

Hackers' Change in Motivation

■ Vandalism and publicity ■ "Hacktivism" ■ Financially motivated



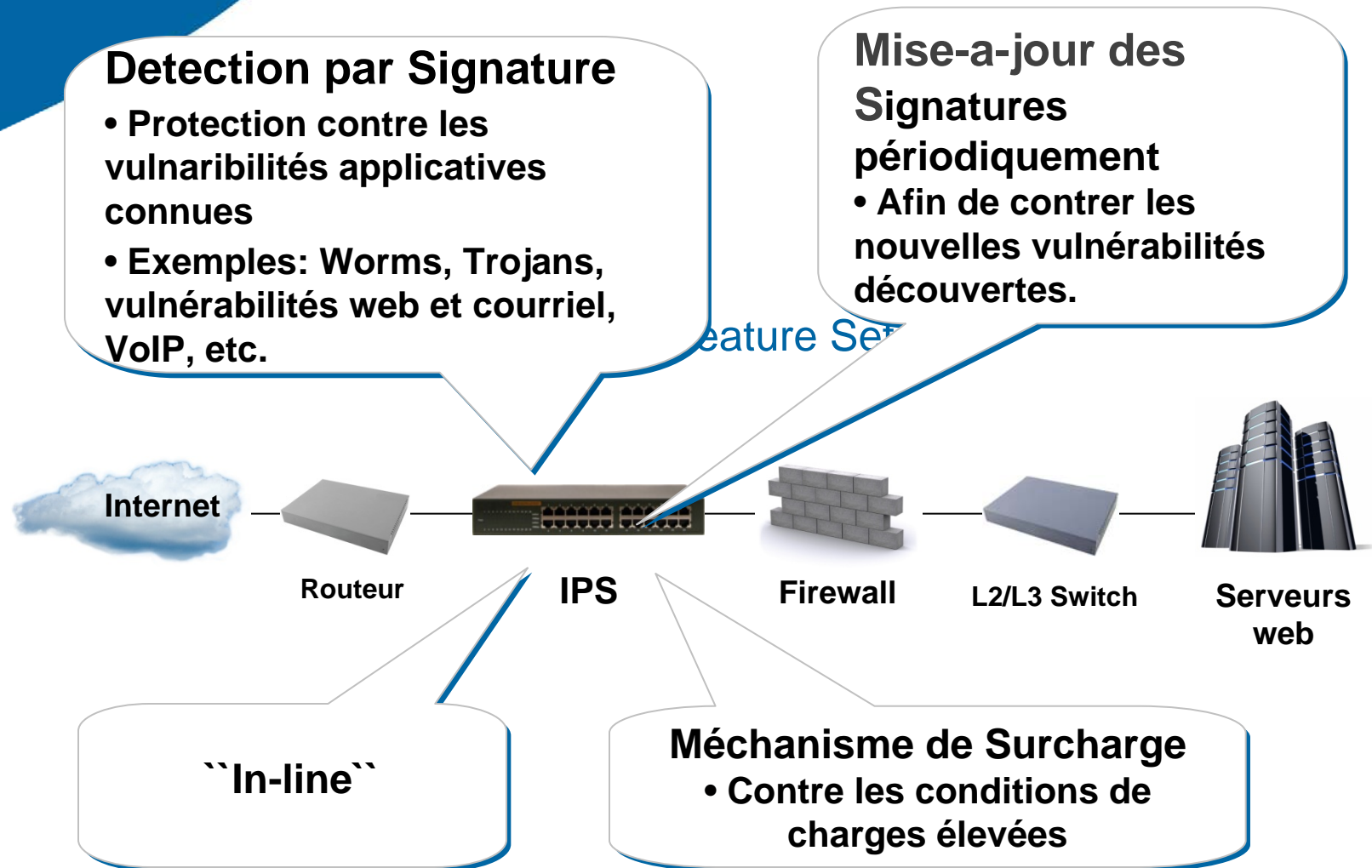
Cyber Crime Organizational Chart



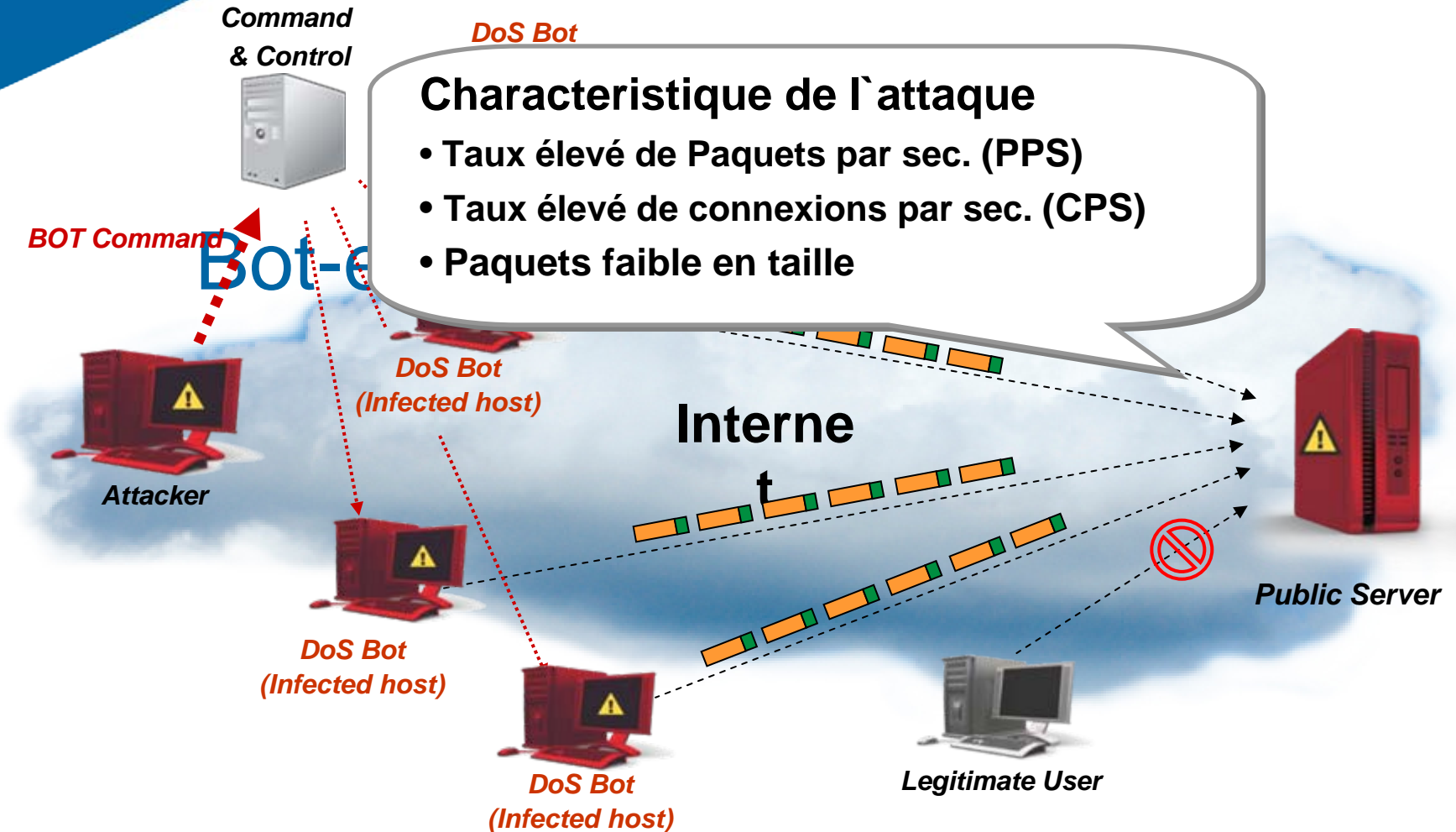
A large, solid blue shape in the top-left corner of the slide, consisting of a thick, curved line that starts from the left edge and curves upwards and to the right.

Your IPS is Vulnerable

Les services d'un "IPS" standard



Attaque de déni distribuée (DDoS) typique



Defenses mal adaptées aux nouvelles attaques

Packet per second dimension



Max PPS
Capacity [PPS]

CPU 100%

Web Servers vulnerable



Your IPS is Vulnerable

Any Botnet can paralyze your network protections!

IPS overload condition:

- Device DROPS packets randomly
- Increased latency
- Sessions blocked

IPS Vulnerability 100% Blocking Users



Your IPS Blocks Users

- “I was told that the IPS overload mechanism will resolve cases of high volume traffic”

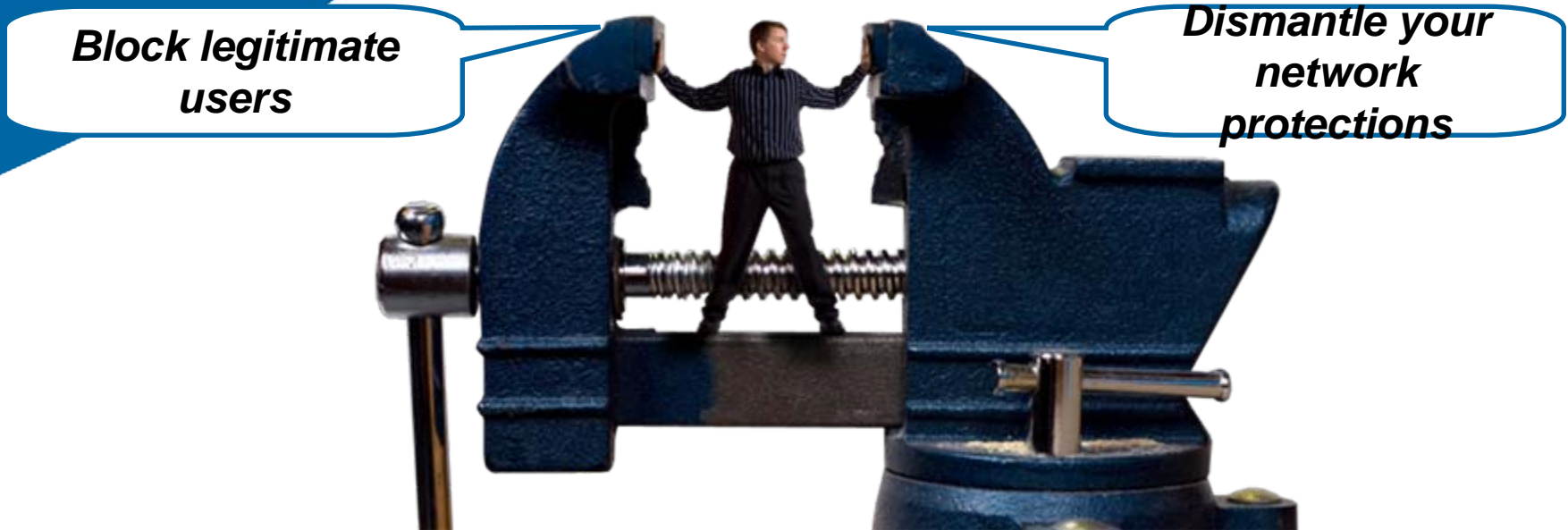


IPS overload condition:

- Device falls into L2 BYPASS mode
- All traffic forwarded!
- Signature engine bypassed

No network protection!
Attacks evade into your network without inspection

IPS Vulnerability Threat: Summary



- DDoS attacks threatens the on-line industry:
 - eCommerce
 - Government
 - Critical infrastructure
- Existing IPS vendors force you to make compromises that are not acceptable
- When your network is under attack you need to choose between:



Conclusion

Questions?