Computer Emergency Response Team
Industrie Services Tertiaire

Failles de sécurité et lutte informatique
Bilan 2005

Industrie Services Tertiaire

Yvon KLEIN
Mars 2006

Rappel : Top 20 des vulnérabilités 2004
Les Vers en environnement Windows

- Lors de son Forum 2005, et en collaboration avec le magazine CSO, le Cert-IST procédait à la désignation par le public des « 10 vulnérabilités 2004 »

40 nominées pour le vote

Vote du Public

10

11	CERT-ISTAV-2004.132		20[ER]	40[Elect]	Ver "Sasser" sur les systèmes Microsoft Windows 2000 et XP
1	CERT-ISTAV-2004.369		20[ER]	40[Elect]	Vulnérabilité dans le service WINS sur les systèmes Microsoft Windows NT4, 2000 et 2003
12	CERT-ISTAV-2004.119		20[ER]	40[Elect]	Multiples vulnérabilités dans les systèmes d'exploitation Microsoft Windows
14	CERT-ISTAV-2004.054		20[ER]	40[Elect]	Ver "Netsky" sur les systèmes Microsoft Windows
16	CERT-ISTAV-2004.024		20[ER]	40[Elect]	Ver "MyDoom" sur les systèmes Microsoft Windows
3	CERT-ISTAV-2004.321		20[ER]	40[Elect]	Deux vulnérabilités dans le navigateur web Microsoft Internet Explorer 5.x et 6
19	CERT-ISTAV-2004.015		20[ER]	40[Elect]	Ver "Bagle" sur les systèmes Microsoft Windows
5	CERT-ISTAV-2004.306		20[ER]	40[Elect]	Multiples vulnérabilités sous les systèmes Microsoft Windows
6	CERT-ISTAV-2004.305		20[ER]	40[Elect]	Multiples vulnérabilités dans le navigateur Microsoft Internet Explorer 5.x et 6
7	CERT-ISTAV-2004.273		20[ER]	40[Elect]	Vulnérabilité dans la gestion du format d'image JPEG sous les produits Microsoft

20 « commentées" par l'équipe technique

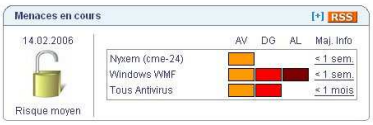
- Les critères : la spécificité, l'impact …
- Le résultat : Sasser, Netsky, Mydoom, Bagle, et les failles associées …

Industrie Services Tertiaire

Quel besoin pour l'identification et l'évaluation des menaces ?

- Exemple : « Kama Soutra » (CME-24)
  - 3 février 2006 xx : « Kama Sutra » : un dangereux virus qui détruit des documents
  - 3 février 2006 zz : *Virus CME-24 dit Kama Sutra, plus de peur que de mal ?*
  - 2 février 2006 xx met gratuitement à disposition un outil de désinfection pour [..] Nyxem
  - 2 février 2006 yy appelle à éviter la panique face à l'attaque du ver Nyxem
  - 1er février 2006 tt : Le vendredi noir approche pour les ordinateurs infectés par Nyxem
  - 31 janvier 2006 Top Ten yy Janvier 2006
    - Nyxem-D, le ver Kama Sutra, […] directement en quatrième place du classement
  - 27 janvier 2006 ww : Alerte rouge sur le ver W32/Small KI@MM
  - 25 janvier 2006 Alerte uu : Blackworm est de retour et s'active le "3" de chaque mois
  - 24 janvier 2006 Alerte : le virus Nyxem efface les documents Word et Excel le 3 fevrier
  - 23 janvier 2006 yy : Le ver Nyxem-D se répand à grande vitesse sur les réseaux

Un dangereux virus
Se répand à grande vitesse
Alerte rouge
Le vendredi noir
Éviter la panique



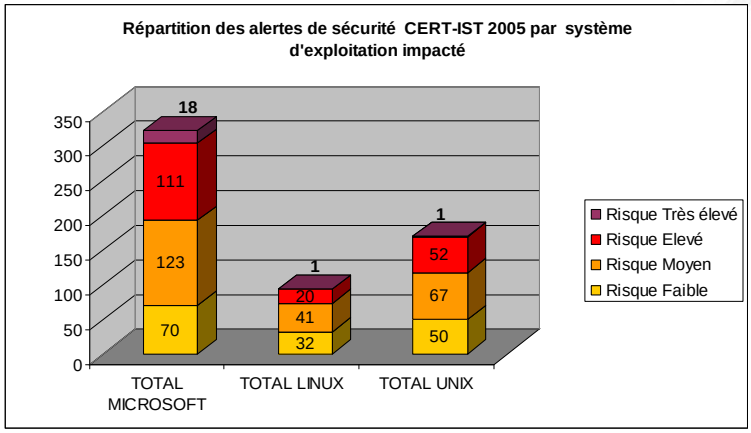
- Et pourtant …
  - « CME-24 ne comporte aucun dispositif de furtivité, […] Le dernier programme à déclenchement retardé, Sober, est apparu en novembre 2005. Sa mise à feu, […] "Bien que très surveillée, elle a été un non-événement.«
  - « Malgré les fonctions de destruction de CME-24, le CERT-IST rappelle que la plus importante alerte de ces dernières semaines n'était pas le fait d'un virus mais d'une faille de sécurité découverte sur les systèmes Windows (Le Monde du 4 janvier) et corrigée le 6 janvier. »

Le Monde

- Il est nécessaire de se référer à des sources neutres et fiables pour évaluer la gravité des attaques : CME, CVSS etc …

Industrie Services Tertiaire

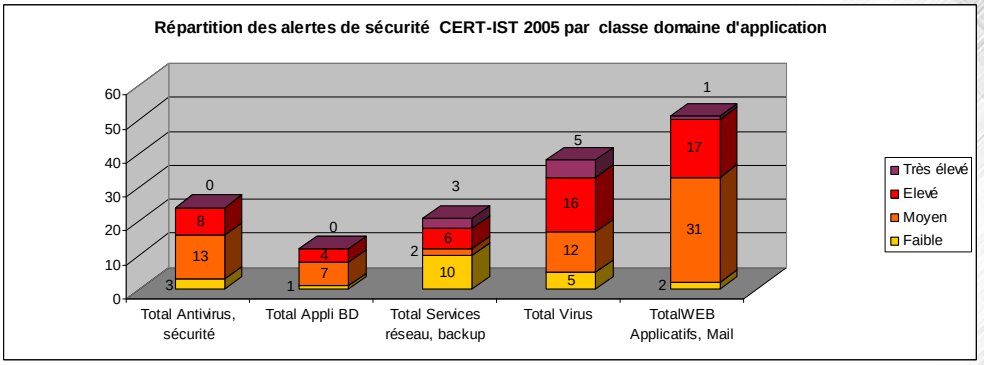
le Cert-IST fait une analyse objective par rapport aux éditeurs : le résultat 2005



- En 2005, la situation de vulnérabilité s'est rééquilibrée entre
  - Firefox et Internet Explorer
  - UNIX et Windows

Industrie Services Tertiaire

le Cert-IST surveille toutes les principales menaces : le résultat 2005

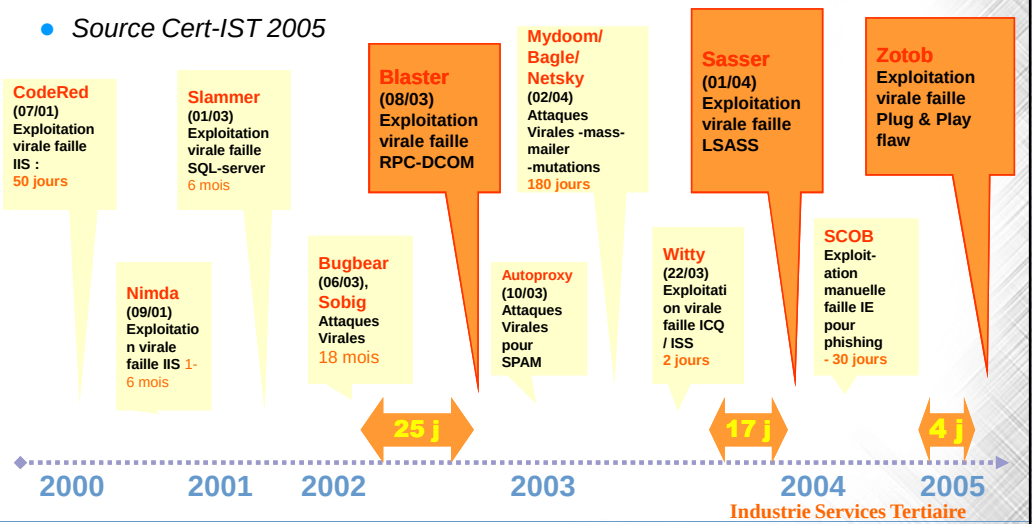


- Les virus et les failles Windows ne doivent pas occulter des menaces plus discrètes mais très dangereuses pour les entreprises

Industrie Services Tertiaire

Evolution
Des attaques de plus en plus rapides

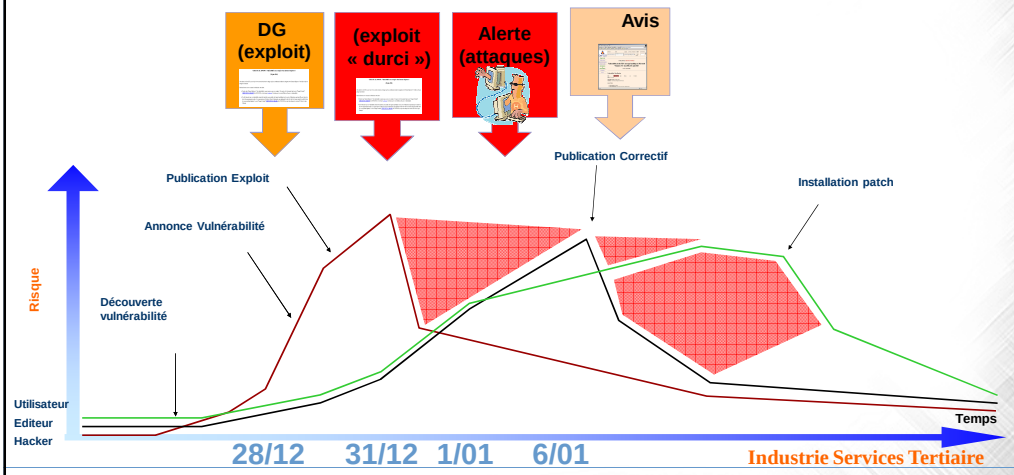
- L'attaque suit de plus en plus souvent et vite l'identification d'une faille
- *Source Cert-IST 2005*



Industrie Services Tertiaire

Evolution des attaques de plus en plus rapides

- L'attaque suit de plus en plus souvent et vite l'identification d'une faille
- Quand elle ne la précède pas … (faille WMF)



Industrie Services Tertiaire

Evolution de la Cybercriminalité

- Virus, Failles et cybercriminalité
  - Le virus est devenu un « outil », un vecteur d'attaque
    - pour déposer une backdoor, constituer un botnet ou préparer une attaque de masse:
  - Le délai de grâce entre la divulgation d'une faille (et d'un « exploit ») et l'attaque associée est de plus en plus court
    - 6 mois pour Slammer (2003), 2 semaines pour Sasser (2004), 4 jours pour Zotob (2005), 4jours (sans correctif …) pour WMF
- Etre victime d'une attaque est dévastateur
  - Les attaques massives via virus sont les plus visibles en terme de perturbations (encore que de nombreuses entreprises ont réussi à dissimuler qu'elles avaient été impactées)
  - Des attaques ciblées via cheval de troie ou phishing peuvent avoir des effets encore plus graves sur l'activité et la confiance en l'entreprise
- L'organisation de la SSI en entreprise doit s'adapter à l'évolution des menaces.


Le Monde

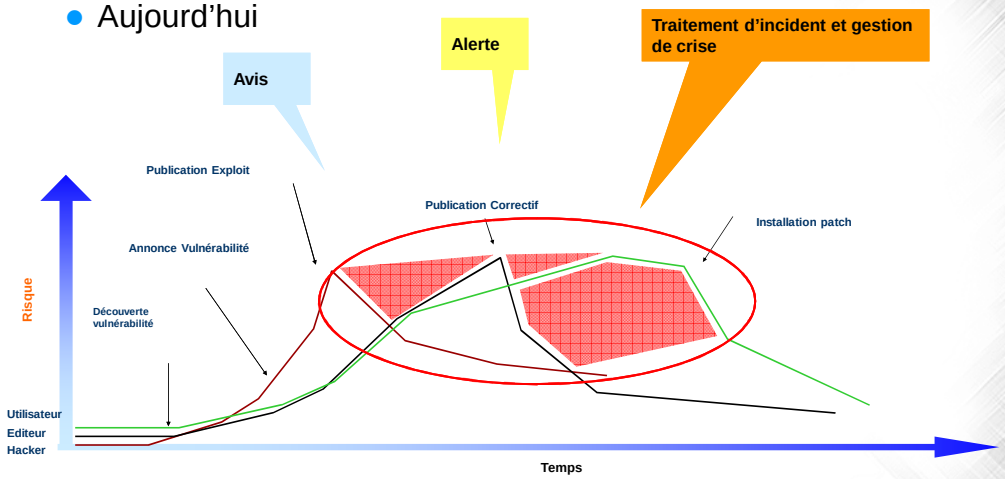
Les créateurs de virus informatiques deviennent des mercenaires


Several vulnerabilities in the H.323 message handling on Cisco equipments and the Microsoft ISA firewall

Industrie Services Tertiaire

Le Cert-IST aujourd'hui
Modélisation de la menace : La zone de danger maximum

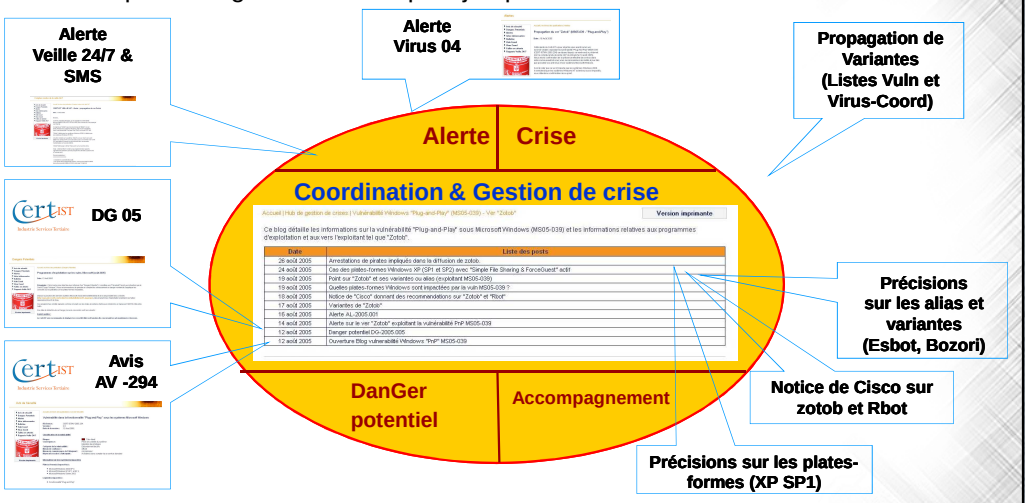
- Aujourd'hui



Industrie Services Tertiaire

Veille de sécurité et gestion de crise
Accompagnement tout au long de la crise

- Anticipation et gestion des risques jusqu'à la clôture des crises



Industrie Services Tertiaire

Face à la cybercriminalité : l'intérêt d'un réseau d'experts

Intervenants Externes (Mutualisation)

Un équilibre délicat entre gestion des ressources et responsabilité

Maîtrise Interne (Entreprise)

PREVENTION / VEILLE

ACCOMPAGNEMENT

ALERTE ET REACTION

Une solution :

Le transfert de compétence permanent

GESTION VULNERABILITES

SURVEILLANCE

TRAITEMENT

Industrie Services Tertiaire

Conclusion

- Prospective 2006
  - L'année des attaques sur VoIP et Mobiles ?
  - Encore une année difficile pour Microsoft ?
    - (le leader du marché en butte à une hostilité illustrée par la progression des « zéro-day », hostilité qui sera exacerbée par l'entrée de Microsoft sur le marché de la sécurité)
  - L'année du ~~spyware~~ comportement intrusif ?
    - Entre les éditeurs qui veulent protéger leurs contenus (DRM), les opérateurs qui les financent par des publicitées amenées à être de plus en plus ciblées, les éditeurs d'architectures « désintéressées » (skype, google), les adware, spyware, et comportements plus ou moins intrusifs vont se multiplier.

Industrie Services Tertiaire