Computer Emergency Response Team
Industrie Service Tertiaire

Tendances et attaques : Analyse des nouvelles attaques

Philippe Bourgeois

Industrie Services Tertiaire

Juin 2008

Plan de la présentation

- Attaques et vulnérabilités marquantes de 2008
- Analyse des attaques visant les internautes
  - Le "Drive-by download"
  - Infections web massives
  - Le phénomène botnet
- Attaques au travers de panneaux publicitaires
- SPAM : messages NDR (effet "backscatter")
- Evolution des menaces et impacts pour les entreprises

Industrie Service Tertiaire

Plan de la présentation

- Attaques et vulnérabilités marquantes de 2008
- Analyse des attaques visant les internautes
  - Le "Drive-by download"
  - Infections web massives
  - Le phénomène botnet
- Attaques au travers de panneaux publicitaires
- SPAM : messages NDR (effet "backscatter")
- Evolution des menaces et impacts pour les entreprises

Industrie Service Tertiaire

Alertes et Dangers Potentiels émis en 2008

- Pas d'alerte, mais 6 Dangers Potentiels

Référence	Description	Versions
CERT-IST/DG-2008.001	Activités malveillantes autour de vulnérabilités de **RealPlayer**	1.0 - 07 janvier 2008
CERT-IST/DG-2008.002	Nouvelle vulnérabilité RTSP critique dans **QuickTime d'Apple**	1.0 - 11 janvier 2008 1.1 - 07 février 2008
CERT-IST/DG-2008.003	Infections massives de sites web	1.0 - 17 janvier 2008
CERT-IST/DG-2008.004	Propagation de fichiers **PDF malicieux** (CVE-2007-5659)	1.0 - 11 février 2008
CERT-IST/DG-2008.005	Multiples **attaques massive de sites web**	1.0 - 17 mars 2008
CERT-IST/DG-2008.006	Vulnérabilité "0-day" dans **Adobe Flash Player**	1.0 - 28 mai 2008 3.0 - 30 mai 2008

- Ces menaces :
  - Utilisent des vulnérabilités de **logiciels tiers** (Flash, PDF, QuickTime)
  - Visent les internautes lors de leur navigation web (attaques "**Drive-by download** ")
- Autres événements marquants de 2008
  - SPAM : NDR SPAM (Non Delivery Report et effet "backscatter")

Industrie Service Tertiaire

Vulnérabilités des logiciels tiers

- L'intérêt des logiciels tiers pour un attaquant
  - Ils ne bénéficient pas des protections "anti-débordement de pile" de Windows
    - Depuis XP-SP2 et 2003-SP1 la plupart des applications Windows sont protégées contre les "stack overflow"
  - Ils sont exploitables quelque soit le navigateur (IE ou FX) et même parfois quelle que soit la plate-forme (Windows ou Linux).
  - Ils sont plus difficiles à mettre à jour
- Exemple des logiciels tiers visés :
  - Adobe Flash Player (FLASH)
  - Adobe Acrobat Reader (PDF)
  - Apple QuickTime (Streaming)
  - Les "Contrôles ActiveX" !

Industrie Service Tertiaire

Plan de la présentation

- Attaques et vulnérabilités marquantes de 2008
- Analyse des attaques visant les internautes
  - Le "Drive-by download"
  - Infections web massives
  - Le phénomène botnet
- Attaques au travers de panneaux publicitaires
- SPAM : messages NDR (effet "backscatter")
- Evolution des menaces et impacts pour les entreprises

Industrie Service Tertiaire

Attaques "Drive-by download"

- Principe :
  - Infecter l'internaute lorsqu'il passe sur un site web piégé

  Le simple fait de visiter sur une page web piégée provoque l'infection

- Mise en pratique
  - Script (JavaScript) enchainant automatiquement une série d'attaque
    - Exemple : Janvier 2008 – Attaque "uc8010.com"
      - 1 attaque QuickTime (RTSP)
      - 3 attaques de Windows
      - 3 attaques ActiveX
      - 1 attaque AudioFile (NCTSoft) et une attaque "Yahoo Messenger "
  - Serveur web spécialisé dans l'attaque de l'internaute
    - Exemple : Mpack, IcePack, n404

Industrie Service Tertiaire

Infections web massives (1/3)

- Principe
  - Exploiter une vulnérabilité web de façon "industrielle" (à grande échelle)
  - Les sites web vulnérables attaqués sont modifiés de façon invisible …. en y déposant des attaques "Drive-by download"

  Des milliers de sites web "anodins" (infectés) attaquent les internautes qui les visitent

- Mise en pratique
  - Rechercher les sites web vulnérables avec Google
  - Y insérer des redirections vers des sites malicieux (tags "<script>" ou "<iframe>")

Il devient très dangereux de naviguer sur Internet (en utilisant une machine non à jour)

Industrie Service Tertiaire

Attaques web massives (2/3)

- Exemples :
  - Janvier 2008 (CERT-IST/DG-2008.003) : Attaque "uc8010.com"
    - Compromission de 10 000 sites web Linux-Apache (installation d'un rootkit Apache)
  - Mars 2008 (CERT-IST/DG-2008.005) : Attaque "2117966.net"
    - Compromission de 100 000 sites web Windows-ASP (Injection SQL)
  - Avril et mai 2008 (Injection SQL)
    - 200 000 sites le 22 avril (nihao.com)
    - 4 000 sites le 9 mai (winzipices.cn)
    - 20 000 sites le 27 mai (dota11.cn)

Nota : les estimations du nombre de sites infectés sont basés sur Google…

Industrie Service Tertiaire

Infections web massives (3/3)

- La méthode d'estimation du nombre de site infectés : Google

Le phénomène "Botnet"

- Une grande majorité des virus déposent un "bot" (et un keylogger) sur le poste infecté
- Ces "bots" rejoignent des "botnets" pour faire du SPAM (ou du DDOS)

Botnets	Taille (nbre de bots)	Puissance (msg de SPAM par jour)
Srizbi	315 000	60 milliards
Rustock	150 000	30 milliards
Kraken et Bobax	185 000	9 milliards
Storm	85 000 bots	3 milliards
Mega-D	35 000 bots	10 milliards

Source : SecureWorks.com

Industrie Service Tertiaire

Evolution des Botnets

- Les P2P botnets posent de nouveaux problèmes
  - Difficulté d'identification des machines infectées (pas de "pattern réseau" car ports aléatoires)
  - Difficultés de neutralisation du botnet (il faut neutraliser un à un les "bots")
  - Capacité de franchissement des protections périmétriques (utilisation de protocoles difficiles à filtrer : UDP)

Illustration : Botnet conventionel vs Botnet P2P

Industrie Service Tertiaire

Plan de la présentation

- Attaques et vulnérabilités marquantes de 2008
- Analyse des attaques visant les internautes
  - Le "Drive-by download"
  - Infections web massives
  - Le phénomène botnet
- Attaques au travers de panneaux publicitaires
- SPAM : messages NDR (effet "backscatter")
- Evolution des menaces et impacts pour les entreprises

Industrie Service Tertiaire

Bandeaux publicitaires malveillants (1/2)

- Principe
  - Injecter dans une campagne publicitaire un spot publicitaire malveillant
    - Spot publicitaire en Flash
    - Déclenche (de temps en temps) une attaque contre le poste de l'Internaute.
  - L'attaque est ensuite relayée par tous les sites web abonnés à une régie publicitaire donnée
    - Le site web n'est pas lui-même infecté, mais il loue un espace publicitaire et n'a que peu de contrôle sur cet espace.
    - La régie publicitaire ne maitrise pas forcement le contenu publicitaire qu'elle diffuse.
    - Ce contenu peut venir d'associés peu scrupuleux ("réseaux" publicitaires)

Industrie Service Tertiaire

Bandeaux publicitaires malveillants (1/2)

- Exemple de spots publicitaires malveillants
  - Escroquerie de type "Faux antivirus" (octobre 2007)
    (Vu par le Cert-IST sur des sites français)
  - Attaques utilisant une vulnérabilité 0-day dans Flash (janvier 2008)
- La réalisation de ces attaques nécessite
  - Des compétences techniques (spot publicitaire malicieux)
  - Une parfaite connaissance du Business sur Internet (campagne publicitaire)

  Il s'agit d'attaques sophistiquées

  - Et elles sont difficiles à identifier / analyser / tracer

Industrie Service Tertiaire

Plan de la présentation

- Attaques et vulnérabilités marquantes de 2008
- Analyse des attaques visant les internautes
  - Le "Drive-by download"
  - Infections web massives
  - Le phénomène botnet
- Attaques au travers de panneaux publicitaires
- SPAM : messages NDR (effet "backscatter")
- Evolution des menaces et impacts pour les entreprises

Industrie Service Tertiaire

SPAM

- Le volume du SPAM sur Internet ne décroit pas …
  - 81 % à 97 % du trafic email est du SPAM
- En avril 2008 le nombre de messages NDR liés au SPAM est monté en flèche
  - NDR = Non Delivery Receipt (Message de non acheminement)
  - Plusieurs adhérents nous ont signalé un taux anormal de NDR (certains utilisateurs reçoivent des flots de NDR)
- Il s'agit d'un effet "backscatter" lié au SPAM
  - Utilisation de champ "From:" usurpé
  - Certains ont considéré cela comme une technique de SPAM …
  - Depuis, les solutions anti-spam savent détecter ces NDR et les écarter

Industrie Service Tertiaire

SPAM

- [image explicative du NDR]
- [image bsn.borderware.com]

Industrie Service Tertiaire

Plan de la présentation

- Attaques et vulnérabilités marquantes de 2008
- Analyse des attaques visant les internautes
  - Le "Drive-by download"
  - Infections web massives
  - Le phénomène botnet
- Attaques au travers de panneaux publicitaires
- SPAM : messages NDR (effet "backscatter")
- Evolution des menaces et impacts pour les entreprises

Industrie Service Tertiaire

Evolution des menaces et Impacts pour les entreprises (1/2)

- Des attaques de plus en plus sophistiquées
  - Les techniques d'attaques (parfois) très poussées
  - Appliquées à grande échelle
- Et leur emploi quitte le domaine de l'attaque :
  - Cf. les réflexions en cours pour leur usage par la police
  - Cf. les manipulations d'information pour le "ranking Google" (Manipulation, Intelligence Economique, etc...)
- Les attaques contre les internautes ne sont que la partie émergée de l'iceberg :
  - Attaques ciblées (espionnage industriel)
  - Professionnalisation des attaquants
  - L'attaque n'est plus une fin, mais un moyen (Attaques "2.0" ?)

Industrie Service Tertiaire

Evolution des menaces et Impacts pour les entreprises (2/2)

- Malgré un calme apparent (plus de Sasser ou de Codered)
  La menace est réelle et plus pernicieuse (attaque discrète)
- Jusque là tout va bien … ☺
  - Mais la responsabilité du RSSI reste engagée
  - Les moyens de lutte et les bonnes pratiques existent
- Elle nécessite un travail systématique avant la crise
  - Défense en profondeur
  - Analyse des menaces et de l'exposition du SI
  - Surveillance des journaux pour identifier les anomalies
- Recommandations techniques spécifiques
  - Maintenir les plates-formes à jour
  - Filtrer le trafic sortant (TCP et UDP)
  - Surveiller le trafic sortant rejeté (identification de postes infectés)