Computer Emergency Response Team
Industrie Services Tertiaire

Bilan 2008 du Cert-IST sur les failles et attaques

www.cert-ist.com

Industrie Services Tertiaire

OSSIR - RéSIST - Avril 2009

Philippe Bourgeois

Plan de la présentation

- **L'année 2008 du Cert-IST en 3 chiffres clés**
- **Les phénomènes majeurs**
  - **Attaques du poste de travail par des sites web compromis**
  - **Compromissions massives et organisées**
  - **La faille DNS : un cas historique**
  - **Conficker (Downadup) : le retour du ver**
- **Autres événements remarquables**
- **Conclusions**

Industrie Services Tertiaire

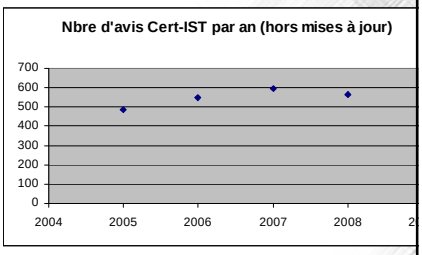
Computer Emergency Response Team
Industrie Services Tertiaire

L'année 2008 du Cert-IST en 3 chiffres clés

Cert IST
Industrie Services Tertiaire

L'année 2008 du Cert-IST

- 563 Avis de sécurité (+1330 mises à jour)
  - Léger retrait par rapport aux années précédentes



- 13 situations à risque
  - Ayant fait l'objet d'un suivi spécifique (Menaces en cours)

- Dont 2 ont donné lieu à des alertes :
  - L'alerte CERT-IST/AL-2008.001 en juillet pour la vulnérabilité DNS
  - L'alerte CERT-IST/AL-2008.002 en novembre pour Conficker

Industrie Services Tertiaire

Computer Emergency Response Team
Industrie Services Tertiaire

Les phénomènes majeurs

Cert IST
Industrie Services Tertiaire

1 : Attaque du poste de travail par des sites web compromis

- Attaque du poste de travail via le navigateur web
  - Ce n'est pas un phénomène nouveau (infection lors de la navigation web)
  - Mais il a pris en 2008 une proportion sans précédent
    - De nombreux sites web relaient involontairement les attaques (ils sont compromis)
    - Les outils d'attaques sont sophistiqués (e.g. IcePack, FastFlux, etc…) et les attaques discrètes (Drive-by download)
    - Les nouvelles vulnérabilités sont intégrées rapidement aux panoplies des attaquants
- Ces attaques visent le plus souvent les logiciels « tiers »
  - Logiciels de type : PDF, Flash, QuickTime RTSP, RealPlayer
  - Plutôt que Windows ou même le navigateur Web
- 5 messages DG émis par le Cert-IST en 2008 sur ces sujets
  - 3 DG sur les logiciels tiers : RealPlayer, QuickTime et PDF
  - 2 DG sur des vagues d'infections massives de sites web
- Constat : Naviguer sur Internet avec un ordinateur non à jour est devenu TRES dangereux.

Industrie Services 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" !

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

2: Compromissions massives et organisées

- Des attaques de plus en plus sophistiquées
  - Intégrer dès que possible les nouvelles vulnérabilités aux outils d'attaques
  - Déployer l'attaque à de larges échelles (par exemple via des sites web compromis)
- Exemples au premier semestre 2008
  - Attaques massives de sites web (failles de type « SQL-injection » sur des CMS sous IIS+SQL-Server)
  - Envoi en masse (spam) de PDF malveillants (CVE-2008_0655)
  - Attaque au travers de bandeaux publicitaires FLASH malveillant (Janvier 2008)

2: Compromissions massives et organisées
Attaques web massives

- 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…

2: Compromissions massives et organisées
Infections web massives (3/3)

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

3: Faille DNS : un cas historique

- Une faille hors-norme : LA faille de l'année 2008 !
  - Par sa gravité : détournement de tout le trafic réseaux pour les utilisateurs d'un DNS vulnérable
  - Par son ampleur : la très grande majorité des serveurs DNS étaient vulnérables. Un déploiement de correctifs à l'échelle mondiale était nécessaire

  Cette faille intéresse les cyber-criminels : de multiples scénarios d'attaques ciblées sont possibles.
- Une gestion controversée en matière de "divulgation responsable"
  - Découverte en février 2008 et maintenue sécrète au sein d'un groupe de travail
  - Annonce des correctifs le 8 juillet. Le détail technique reste secret jusqu'au 8 août.
  - Ce secret excite la curiosité des chercheurs :
    - Le 22 juillet le secret est découvert
    - Le 24 juillet des programmes d'attaque son rendus publics
    - Le 29 juillet des tentatives d'attaques sont signalées
- Des résultats à méditer

  [Voir la planche suivante]

3: Faille DNS : un cas historique

- Des résultats à méditer
  - L'effort de tous a porté ses fruits :
    - La très grande majorité des serveurs DNS ont été corrigés.
    - Les attaques ont été évitées
    - Il ne s'est rien passé !!
  - Mais il reste un sujet de travail (inépuisable ?)
    - Comment déployer un correctif multi-constructeur à l'échelle mondiale ?
    - Comment garder un secret ?
    - Le droit d'en connaître, la curiosité humaine, la raison et l'ego.

4: Conficker : le retour du ver

- Le premier grand ver depuis 2004 (Sasser)
  - Propagation par attaque à distance du service Serveur de Windows (Vulnérabilité MS08-067)
  - Premières attaques le 26/11/2008 (Conficker-A)
  - Véritablement médiatisé à partir de Janvier 2009 (Conficker-B, puis B++, C et E)
- Menace bien anticipée par le Cert-IST
  - Suivi depuis le 24/10/2008 dans le « Hub de Gestion de crise »
  - Emission de 2 dangers potentiels successifs
    - 24/10/2008 : « Nouvelle vulnérabilité critique dans Microsoft Windows (MS08-067) »
    - 06/11/2008 : « Vers utilisant la vulnérabilité MS08-067 de Microsoft Windows » (Welcorl et Kerbot)
  - Puis d'une alerte
    - 27/11/2008 : « Propagation du ver "Conficker" (vulnérabilité MS08-067) »
- Plusieurs cas d'infection reportés au sein de notre communauté
  - Cela parait inévitable du fait des multiples vecteurs de propagation (clés USB, postes nomades, Accès VPN)
  - Il est indispensable de savoir détecter / isoler / traiter les point d'infection ponctuels (parce qu'il y aura des infections ponctuelles)

Computer Emergency Response Team
Industrie Services Tertiaire

Autres événements remarquables

Une année riche en publications

- Des failles préoccupantes mais à l'impact encore limité
  - Faiblesse des clés OpenSSL des systèmes Linux Debian
  - Vulnérabilité TCP-DOS (conférence T2 – octobre 2008)
  - Collisions MD5 et certificats numérique (conférence CCC décembre 2008)
- Une année riche en publications
  - Cold boot attacks (attaque RAM)
  - Ghost in the browser (IE)
  - Token kidnapping (Windows)
  - Clickjacking (DHTML)

Industrie Services Tertiaire

- Des cybercriminels de plus en plus actifs
  - Le retour de GPCode (ransomware – 1er semestre 2008)
  - Botnets : Storm, Kraken (1er semestre 2008)
  - Le marché lucratif des faux antivirus (2eme semestre 2008)
- Une réaction des autorités de plus en plus déterminées
  - Arrêt d'hébergeurs complésants : McColo + Atrivo
  - Levée par l'ICANN de l'accréditation de certains Registrars (ex: EstDomains.com)

Computer Emergency Response Team
Industrie Services Tertiaire

Conclusions

Conclusions 1/2

- Une année 2008 riche en événements
  - Beaucoup d'événements techniques et une forte distorsion de l'information par les média (ou par d'autres sources).
  - L'objectif du Cert-IST est de recentrer l'attention de ses adhérents sur les vraies menaces.
- La professionnalisation des attaques est flagrante (depuis 2007)
  - Avant 2005 : Des attaques gratuites (sans but mercantile) : « **stack overflow for fun** »
  - 2005-2006 : Attaques motivées par la gain d'argent (Spyware, chantage au DDOS, attaques ciblées, ventes de failles 0-day) : « **hack = money** »
  - 2007-2008- etc… : Attaques structurées et professionnalisées
- 2009 sera sans doute l'année « Conficker »
  - La lutte n'est pas finie …

Conclusions 2/2

- 2008 est pour nous une année de durcissement
  - Les attaquants semblent de plus en plus forts
  - La défense a aussi beaucoup progressé :
    - Outils techniques : MSRT, infiltration des réseaux P2P de type StormWorm
    - Une collaboration active (e.g. ShadowServer)
    - Des actions spectaculaires et médiatisées
- Pour les entreprises ce durcissement implique
  - Des défenses solides et étanches
  - Une défense en profondeur (les défenses périmétriques seront contournées)
  - Des procédures rigoureuses (gestion des correctifs, gestion des menaces, réactions en cas de crise)

Q & R ?

Fin de la présentation

Nota : Le bilan 2008 complet du Cert-IST est disponible sur le site web

Industrie Services Tertiaire