Computer Emergency Response Team
Industrie Services Tertiaire

Réponse sur incident : Processus de gestion et analyses techniques

Forum 2010

Philippe BOURGEOIS
et David TRESGOTS
Cert-IST

Sommaire

- Processus type de gestion d'incident
  - Présentation du processus en 6 phases
  - Analyse de chaque phase
- Analyse technique
  - Analyse de logs
  - Analyse de malwares
  - Analyse d'un incidents de type phishing

Computer Emergency Response Team
Industrie Services Tertiaire

Processus de gestion d'incident

CertIST
Industrie Services Tertiaire

Vue d'ensemble du processus

- Phase 1 : Préparation à l'arrivée d'un incident
- Phase 2 : Identification / qualification de l'incident
- Phase 3 : Limiter l'extension possible de l'incident
- Phase 4 : Investigation et suppression de la vulnérabilité
- Phase 5 : Restaurer un système sain
- Phase 6 : Post-incident – Archiver & Tirer les leçons de l'incident

☝ Gestion d'incident ≠ Investigation sur incident

Industrie Services Tertiaire

Phase 1 : Préparation avant l'incident

- Préparation d'un plan de réponse sur incident
  - Inclure le traitement des incidents dans la politique sécurité de l'entreprise
  - Définir des personnes impliquées
    - Experts techniques, Architectes du S.I., Manager, Juristes
  - Définir des procédures pour structurer et guider la gestion d'incident
    - Préserver les traces
    - Documenter les actions
  - Mettre en place les infrastructures nécessaires
    - Backup, Plan de reprise
    - Gestion des traces
- Quelques éléments importants dans la gestion d'incident
  - Isoler l'équipe de traitement d'incident, définir clairement les rôles, limiter le stress
  - Effectuer des réunions fréquentes : points d avancement, ajustement du plan d'actions

Phase 2 : Identification / qualification de l'incident

- Il n'est pas toujours sûr qu'un incident (de sécurité) a eu lieu
  - A défaut : renforcer la surveillance et attendre confirmation
- Pour confirmer l'incident
  - Interview minutieuse (écouter et laisser s'exprimer)
  - Vérifier les anomalies signalées (demander des éléments matériels)
  - Rechercher d'autres traces suspectes (attention à ne pas effacer les traces ou à ne pas brouiller les pistes)
- Si l'incident est confirmé
  - Déclencher le processus de réponse sur incident
  - Fixer les objectifs et les priorités
  - Préserver les données (indices)
    - Ex : copie intégrale de disque, limiter l'accès au système, etc…

Phase 3 : Limiter l'extension possible de l'incident

- Retirer ou sauvegarder certaines données critiques
- Protéger les machines saines ou isoler les machines infectées.
  Exemple :
  - Evaluer si d'autres machines proches présentent les mêmes symptômes
  - Supprimer les partages entre machines,
    Changer les mots de passe sur les machines périphériques
  - Interdire (par filtre réseau) certaines communications
- Faut-il arrêter la machine ? / Faut-il la débrancher du réseau ?
  - Cette décision doit être analysée au cas par cas sur chaque incident.
  - Dans tous les cas, une collecte de données doit être réalisée avant l'arrêt.

Industrie Services Tertiaire

Phase 4 : Investigation et suppression de la vulnérabilité

- Comprendre la nature du problème (investigation du problème) :
  - Le niveau de compréhension à atteindre dépend des objectifs fixés
    - Trouver la cause de l'incident (vulnérabilité du système ou faiblesse à pallier)
    - Savoir ce qui a été fait sur le système,
      l'étendue exacte du sinistre (impact effectif de l'incident)
    - Poursuivre judiciairement
  - Les moyens à mettre en œuvre sont d'autant plus lourds que l'objectif est ambitieux

⇨ C'est le cœur de l'investigation.

- Trouver une solution au problème

Industrie Services Tertiaire

Phase 4 : Investigation et suppression de la vulnérabilité (suite)

- Démarche générale d'investigation
  - Collecter le maximum d'information sur l'incident (collecter les indices)
  - Elaborer un scénario expliquant ces informations (analyser/corréler les indices)
  - Evaluer la vraisemblance de ce scénario (vérifier et démonter)

Industrie Services Tertiaire

Phase 5 : Restaurer un système sain (et non vulnérable)

- Ré-installer **complètement** le système :
  - Reformater ou changer les disques (pour conserver des pièces à conviction)
  - Ré-installer le système à partir des supports constructeurs
  - Renforcer le niveau de sécurité (niveaux de patch, palliatif de la vulnérabilité identifiée)
  - Changer tous les mots de passe
  - Ne reconnecter la machine au réseau que lorsqu'elle est prête
- Utilisation de sauvegardes ou de données provenant de la machine infectée :
  - A utiliser toujours en dernier recours
  - Démontrer que les données sont saines
  - Utiliser le moins de données possibles et en les validant une à une

Industrie Services Tertiaire

Phase 6 : Post-incident - Tirer les leçons de l'incident

- Maintenir une surveillance sur le système qui a été attaqué
  - L'incident peut se reproduire
- Rédiger un rapport global décrivant l'incident
  - synthèse que l'on pourra ré-utiliser
  - identifier les améliorations à apporter :
    - à la procédure de gestion d'incident
    - au système d'information lui-même
  - identifier les outils manquants
- Identifier les problèmes globaux à traiter au niveau organisation
- Communiquer (O/N) : utilisateurs, partenaires, autres (presse)…

Industrie Services Tertiaire

Computer Emergency Response Team
Industrie Services Tertiaire

Réponse sur incident : Analyses techniques

Industrie Services Tertiaire

David TRESGOTS
Cert-IST

Sommaire

- Réponse sur incident : Analyses techniques

1. Analyse de logs
2. Analyse de malwares
3. Analyse d'un incidents de type phishing

Industrie Services Tertiaire

1. Analyse de logs

- Techniques d'analyse
- Outils de visualisation

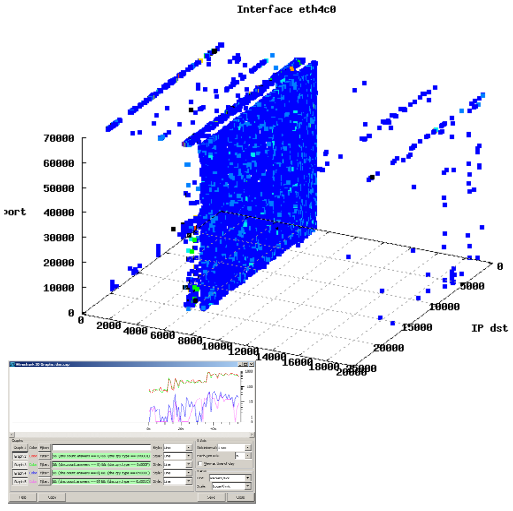
Industrie Services Tertiaire

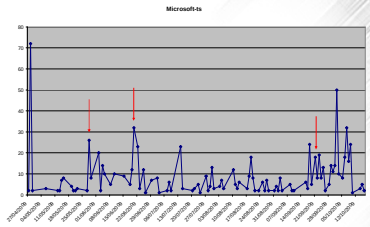
Analyse de logs

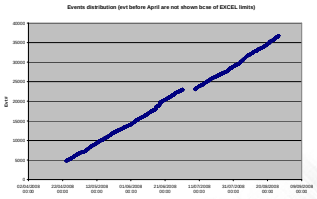
- Les problèmes techniques
  - Le format des fichiers à traiter
    - Il faut souvent développer de nouveaux « parsers »
  - Le volume des données à traiter
    - Excel ne sait tracer que 65000 points !
    - Le stockage en base de données est vite indispensable
- Les problèmes de fond
  - Les données peuvent être corrompues/falsifiées
    - Très courant pour un incident interne de type « malveillance »
    - Des vérifications de vraisemblance sont indispensables
  - Quoi chercher dans les logs ?
    - Les logs « métiers » sont souvent plus parlants
    - Le log du « permit » est plus important que le « deny »
    - Il est indispensable de prendre du recul, vérifier si l'anomalie suspecte n'est pas en fait habituelle

Industrie Services Tertiaire

Visualisation des données







Industrie Services Tertiaire

2. Analyse de malwares

- Un besoin croissant
- Problématiques de ce type d'analyse
- Approches Techniques

Industrie Services Tertiaire

Pourquoi ce besoin d'analyse ?

- Les attaques ciblées via des malwares visant certains SI sont en nette augmentation.
- Des kits de création de malwares avec des fonctionnalités avancées sont disponibles sur Internet
  - Chiffrement, shell, shell inversé, création de comptes, etc… (Illustration)
- Les signatures anti-virus ne les détectent pas immédiatement, voire pas du tout.
  - Certaines formes génériques sont détectées, mais pas toutes (souches polymorphes, auto-chiffrante, etc).

Industrie Services Tertiaire

Problématiques de ce type d'analyse

- L'analyse de malware est un processus chronophage
  - Cette activité doit être bornée dans le temps.
  - Il faut trouver un bon compromis objectifs d'analyse/temps d'analyse
    -> adapter l'analyse en fonction des objectifs
  - Elle requiert souvent :
    - un niveau d'expertise élevé (développeur)
    - parfois de gros moyens techniques (environnement dédié)
      (ex. machine virtuelle dédiée, ou réseau virtualisé, outil de virtualisation applicative)
    - Nécessite des outils adaptés (debugger, outils de reverse engineering, etc.)
- Les techniques utilisées sont de plus en plus complexes.
  - Les malwares intègrent des contre-mesures complexes pour éviter toute analyse
    - Certains se désactivent, voire s'autodétruisent dans certains environnements

    (Illustration)
- Le binaire seul n'est pas suffisant
  - L'information contextuelle est importante (poste compromis, environnement, logs d'équipements filtrants, logs DNS, etc.)

Industrie Services Tertiaire

Différents approches techniques (1/3)

- Analyse statique
  - A priori simple sur le papier
    - Nécessite des outils simples (parser, désassembleurs, anti-virus, éditeur hexadécimal, etc.)
  - Mais parfois complexe dans l'interprétation
    - Difficultés liées au binaire (OS impactés, format du binaire)
      - Est-ce un exécutable, une DLL, un service, un processus ?
    - Difficultés liées aux protections du malware
      - Routines d'obfuscation, utilisation de Packers, etc.
      - Injection de code
      - Masquage des points d'entrées des appels de fonctions
      - Camouflage de codes dans les zones DATA
    - Etc.
  - Peut nécessiter un désassemblage / débogage du code (selon le temps imparti)
    - Pour analyser des points particuliers (Illustration)
    - Nécessite des compétences pointues
    - Les ramifications du code sont souvent très nombreuses pour rendre toute rétro-analyse difficile.

    (Illustration)

⇨Permet :

- De mieux comprendre le fonctionnement du binaire
- D'identifier des chaînes de caractères utilisées (compte / mot de passe utilisés, etc.)
- D'isoler des shells embarqués, ou des code d'exploitation, etc.
- De comprendre le déroulement du code et les actions menées

Industrie Services Tertiaire

Différents approches techniques (2/3)

- Analyse dynamique (dite comportementale ou « runtime »)
  - Nécessite un environnement dédié et confiné (sandbox / sandnet)
    Ex. connexion Internet, réseaux virtualisés, serveurs DNS, serveurs DHCP, loggers, IPS, base de données, etc...
  - Mise en place de moyen de journalisation et de capture réseau
  - Ne nécessite pas la compréhension des techniques utilisées par le code malveillant
    - Il n'est pas utile de comprendre les protections, packers, ou les techniques d'obfuscation utilisées.
  - Dangereuse car le malware est exécuté
  - Fonctionne sur le modèle d'analyse par clichés (état du système avant et après exécution du code)
    - Nécessite des outils spécifiques permettant de comparer les états de la base de registres, des systèmes de fichiers, des processus, etc. (Regshot, RegMon, TDIMon, PSlist, ProcView, Fport, …)
    - Effort d'analyse important pour interpréter les résultats

⇨Permet :

- D'être dans une situation proche d'une attaque réelle (Illustration)
- D'identifier les actions du binaire (dépôt d'autres malwares, d'outils, etc.) (Illustration)
- De détecter :
  - La Création / Modification / Effacement de fichiers
  - Les altération de la base de registre
  - La Création de comptes (privilégiés / non privilégiés)
- D'accéder aux processus,
- De détecter le détournement de processus existant
- De capturer les tentatives de connexions réseau (requêtes DNS, connexions HTTP/HTTPS, etc.)

Industrie Services Tertiaire

Différents approches techniques (3/3)

- Analyse hybride
  - Statique + dynamique du code (Illustration)
  - Débogage et désassemblage des binaires avec exécution pas à pas

⇨Permet :

- De comprendre le fonctionnement du binaire en profondeur
- Une analyse pointue (haut niveau d'expertise en développement)
- De suivre le graphe d'exécution du binaire
- Extrêmement consommatrice de temps

Industrie Services Tertiaire

3. Analyse d'un incident de Phishing

- Augmentation de ce type d'attaque
- Processus d'analyse

Industrie Services Tertiaire

Augmentation de ce type d'attaques

- La professionnalisation des attaques de phishing et leur « industrialisation » sous forme de kits « prêt à l'emploi » engendre une recrudescence d'incidents.
- Un marché parallèle de revente d'informations (N°CB, identifiants, etc.) s'est créé dans le milieu underground.
- Les « *kits de phishing* » sont devenus :
  - Faciles d'accès pour des pirates en herbe
  - Construits pour être déployés rapidement et pour permettre de récupérer rapidement les informations volées (de façon plus ou moins triviales).
  - Composés du code d'un site contrefait (banques, FAI, etc.), avec des graphismes et logos adaptés aux sites ciblés
  - Accompagnés d'une campagne d'emails destinés à abuser les utilisateurs

Industrie Services Tertiaire

Processus d'analyse d'un incident de phishing

- Partie technique
  - Récupérer les emails de spams conduisant vers le site contrefaisant
  - Analyser les entêtes (header) pour « essayer » de déterminer les sources
    - Pas forcément fiable pour les campagnes sophistiquées
  - Identifier l'hébergeur, le responsable du site
  - Récupération des données volées si elles sont accessibles

- Partie non-technique
  - Il faut s'adapter au spécificités et au contexte de l'incident de phishing
    - Chaque cas a ses spécificités ;
      - Métier visé (bancaire, FAI, autres), localisation géographique du site contrefaisant, présence de kits, etc.)
  - Prise de contact avec l'hébergeur, le responsable du site (ex. cellules abuse)
    - Attention ! le responsable du site hébergeant un phishing, peut être lui-même une victime (c'est souvent le cas).
  - Demande de mesure conservatoire des données utilisées dans le phishing ; des données collectées, kits utilisés, etc. (nécessaire si une plainte est envisagée)
    - Dépend de la compétence du service concerné (pas toujours possible lorsque le phishing est hébergé à l'étranger)
    - Peut permettre de récupérer légalement les données volées aux victimes crédules du phishing.
  - Faire fermer le site
    - Le succès d'une fermeture est fortement dépendant du relationnel et de l'esprit de coopération des parties impliquées (parfois difficile avec certains pays).
    - La coopération entre Certs peut être déterminante dans l'aboutissement de la fermeture d'un site de phishing

Industrie Services Tertiaire

Q & R ?

Fin de la présentation

Industrie Services Tertiaire