Des IDS et des vers...

Détection par l'analyse statistique : de la théorie à la pratique ?

JSSI / OSSIR - 4 mai 2004

Guillaume Arcas <guillaume.arcas@free.fr>

Objet de la présentation

- Au cours de ces dernières années, les vers sont devenus une source bien réelle de nuisances.
- Quelques caractéristiques et tendances :
  - perfectionnement des algorithmes de propagation et des méthodes de pénétration.
- Un terrain favorable :
  - démocratisation des accès à Internet (type ADSL) ;
  - les machines cibles ne sont plus seulement des serveurs et ne sont pas toujours « administrées » ;
  - homogénéité du parc logiciel des systèmes cibles.
- Conséquences : saturation de bande passante, déni de service, etc...
- La nécessité : détecter au plus vite toute activité suspecte.
- Les IDS sont un complément utile aux solutions classiques antivirus mais souffrent des mêmes limites lorsqu'ils fonctionnent à base de signatures.
- La question : l'analyse statistique peut-elle répondre à ces besoins ?
- Début de commencement de réponse à travers un retour d 'expérience.

Contexte

<guillaume.arcas@free.fr>

Contexte (1)

- Fourniture d ’accès Internet à 65.000 professionnels et personnels de la santé (libéraux et établissements)
  - RTC / RNIS / ADSL et LS
- Plate-forme technique « classique »
- Sécurité et Qualité de service présentées comme des valeurs fortes
- Clientèle nomade : un seul poste, plusieurs usages (pro. et perso.).

Etat des lieux

<guillaume.arcas@free.fr>

Etat des lieux (1)

- Nul ne peut contester ni ignorer le pouvoir de nuisance des vers.
- Leur « terrain de jeu » a évolué au cours des dernières années dans un sens très favorable à leur propagation du fait, notamment, des nouveaux moyens d'accès permanent et performant à Internet (ADSL).
- Les utilisateurs sont majoritairement des « non techniciens » : pas d 'administration, encore moins de gestion de parc (mises à jour, correctif).
- L'homogénéité du parc logiciel des cibles potentielles accroît encore la menace.

Etat des lieux (2)

- Perfectionnement des vers
- Algorithmes de propagation améliorés
- Exploitation de failles logicielles multiples mais aussi - et peut-être même avant tout - « ingénierie sociale »
- Propagation « multi-canaux »
- Attaques « tous azimuts » (toute machine connectée - plus seulement les serveurs - est une cible potentielle)

Etat des lieux (3)

- Les méthodes de recherche de cibles évoluent : une certaine et toute relative furtivité semble être préférée à la rapidité :
  - Balayage plus ou moins aléatoire (ex. : plusieurs réseaux traités en parallèle, adresses cibles entremêlées)
  - Balayage lent (à la « nmap mode parano »)
  - Balayage sur des ports très usuels (80)
  - Recherche de la « banalité » dans les traces (balayage d'adresses à l'aide de GET /)
- Mais : caractère « foudroyant » de l 'attaque
- Donc : nécessité de disposer de moyens de détection eux aussi rapides.

Etat des lieux (4)

- Une solution antivirus n'est-elle pas suffisante ?
  - Généralement, les signatures pour un nouveau ver sont mises à disposition sous deux à quatre heures ;
    - Compte-tenu de la « fulgurance » des vers récents, cela peut déjà être trop long.
  - Il faut que les canaux utilisés pour la propagation ou l'attaque puissent être analysés. Les principaux protocoles sont éligibles (SMTP, FTP, HTTP, IMAP, POP3). Mais quid des protocoles Peer-to-peer ? Des flux chiffrés ? Des éventuels protocoles propriétaires ?
- Les antivirus ne traitent pas durant la phase de recherche de cibles.

Etat des lieux (5)

- Pourquoi un FAI devrait-il se soucier des vers ?
  - Après tout, les antivirus personnels existent, de même que les pare-feux du même acabit…
  - Le coût des moyens de détection n ’est généralement pas un bien admis dans les directions informatiques…
  - Brider la liberté des utilisateurs quand ceux-ci sont des clients n ’est pas non plus le meilleur des arguments de vente…
- Oui, mais :
  - l ’indisponibilité d ’un service suite à un DoS (même involontaire) est pire encore que le mal…
  - il y aura peut-être un jour des obligations légales de protection a minima faites aux professionnels
  - il est parfois nécessaire de se protéger de ces propres clients...

Anatomie d ’un ver

(c) 2004 - G. Arcas
<guillaume.arcas@free.fr>

Anatomie d'un ver (1)

- Quelques critères de classification :
  - Méthodes de sélection et de recherche des cibles
    - Utilisation de listes pré-établies
    - Balayage de classes d'adresses et de ports
  - Méthodes de propagation
    - Mono-canal
    - Multi-canaux
  - Attaques
    - Déni de service (parfois involontaire…)
    - Vol de données
    - Installation de portes dérobées
    - Spams

Anatomie d'un ver (2)

- Quelques critères de détection :
  - Sélection et de recherche des cibles
    - Listes pré-établies
      - Détection basée sur des exemplaires (si disponibles) de ces listes
    - Balayage d'adresses et de ports
      - Si balayages séquentiels : utilisation de modules ad hoc
      - Si balayages aléatoires : ?
  - Propagation, attaques
    - Mono-canal
    - Multi-canaux
      - A ce stade, les signatures (tant antivirus que IDS) sont disponibles et souvent suffisamment fiables.

Problématique

Problématique

- Détection par signature :
  - la détection à base de signature peut être efficace (règles Snort pour vers Nimda, Code Red, etc.) … pour autant que la signature existe !
  - généralement, les premières signatures « souffrent » d'une certaine imprécision et produisent beaucoup de fausses alertes ;
  - peu adaptée à une réponse rapide ;
  - inefficace en cas de chiffrement.
- Eléments de résolution :
  - identifier les éléments intangibles (adresses IP, ports, protocoles, taille des paquets…) : existe t-il un profil type associé à un ver ?

Premiers cas

<guillaume.arcas@free.fr>

Blaster, août 2003

- Août 2003
  - Comportements anormaux de certains équipements réseaux « sans raison apparente »
  - Retour à la normale par redémarrage…
  - … avant retour à l'anormal.
  - Après diagnostic : saturation des équipements par balayages de plages d'adresses sur les ports 135/139.
- Cas « classique » et simple
  - Blocage des ports utilisés pour la recherche et la propagation
  - Signature de l'attaque disponible.

« Blaster? », le retour

- Début 2004
  - Comportements anormaux de certains équipements réseaux « sans raison apparente »
  - Retour à la normale par redémarrage…
  - … avant retour à l'anormal.
  - Mais, après première analyse : rien de flagrant.
- Seconde phase d'analyse
  - Traitement des journaux
    - Très nombreuses requêtes HTTP (GET /) d'une adresse « interne » vers des adresses externes. Le post-traitement permet de mettre en évidence le balayage.
  - Blocage des ports utilisés impossible (HTTP !)
  - Signature de l'attaque disponible mais les « dégâts » se produisent lors des actions de recherche.
- Donc : nécessité de mettre en œuvre un dispositif de détection de ces balayages.

Premières pistes

(c) 2004 - G. Arcas
<guillaume.arcas@free.fr>

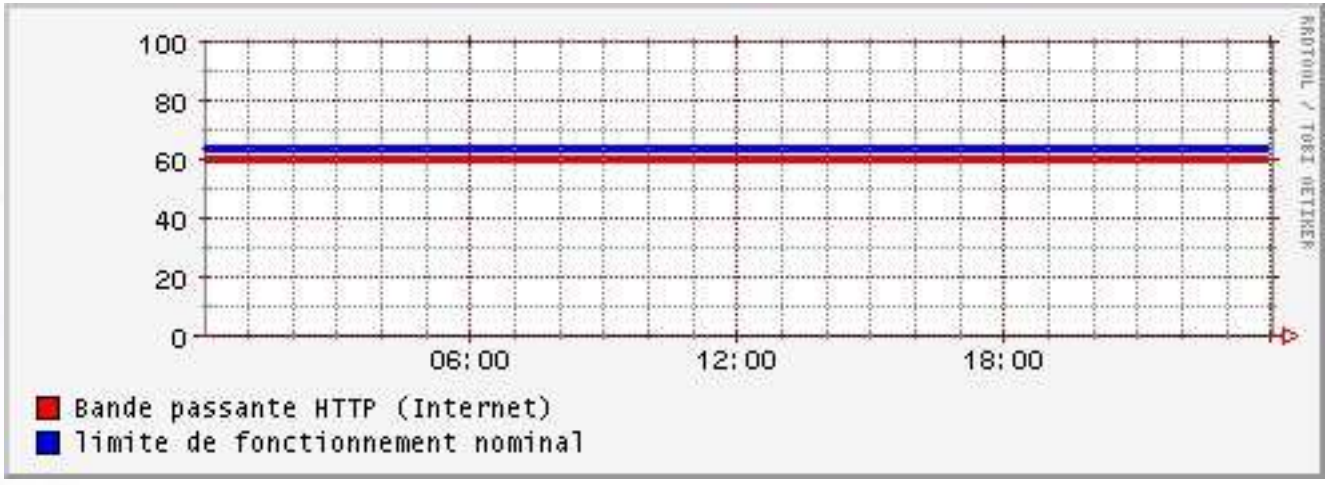
Outils

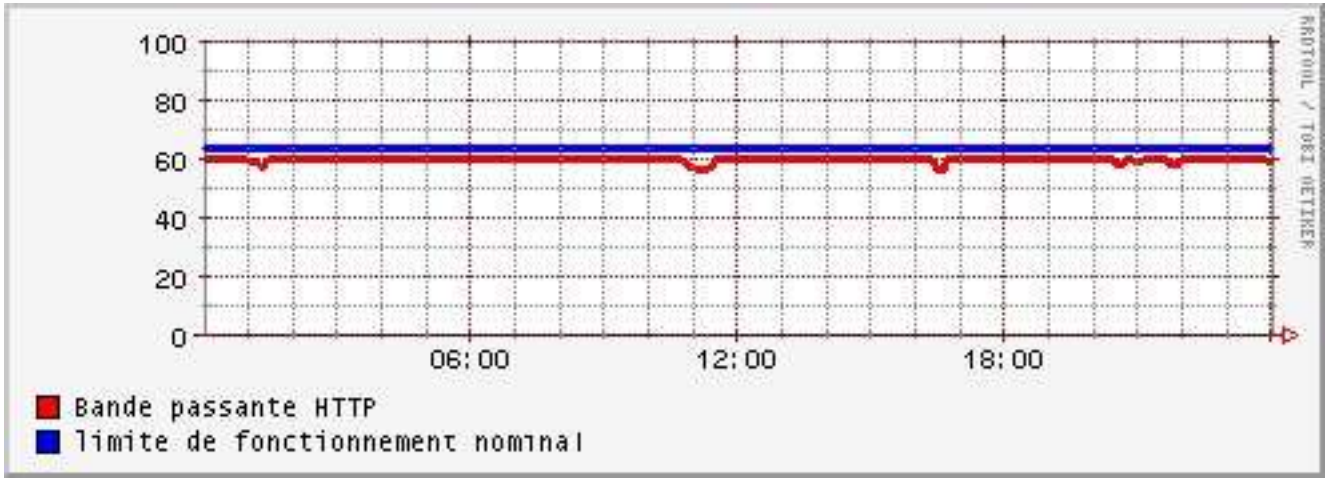
- Analyse réseau
  - tcpdump
  - ntop
- Traitement des journaux
  - grep & awk
  - Expressions régulières PERL
- Mise en forme
  - MRTG / RRDtool
- Détection
  - snort
    - Module flow-portscan
    - Module SPADE

Phase I - 1ère Analyse

- Dans un premier temps : trouver l'origine et la nature des évènements à l'origine des « plantages ».
- Premières actions :
  - Captures réseaux au format tcpdump
  - Traitement des journaux des pare-feux
- Résultats :
  - Traces réseaux
    - Analyse a posteriori avec Snort : RDBM* (*Rien De Bien Méchant*)
    - Passage par la case ipaudit
  - Journaux des pare-feux
    - Nombreuses requêtes de type GET / non suivies d 'autres connexions.
    - Nécessité de retrier les traces pour mettre en évidence un balayage à l 'aide de ces requêtes.
    - Suivi des erreurs 404 peu envisageable (HTTP : 90% du trafic Internet)

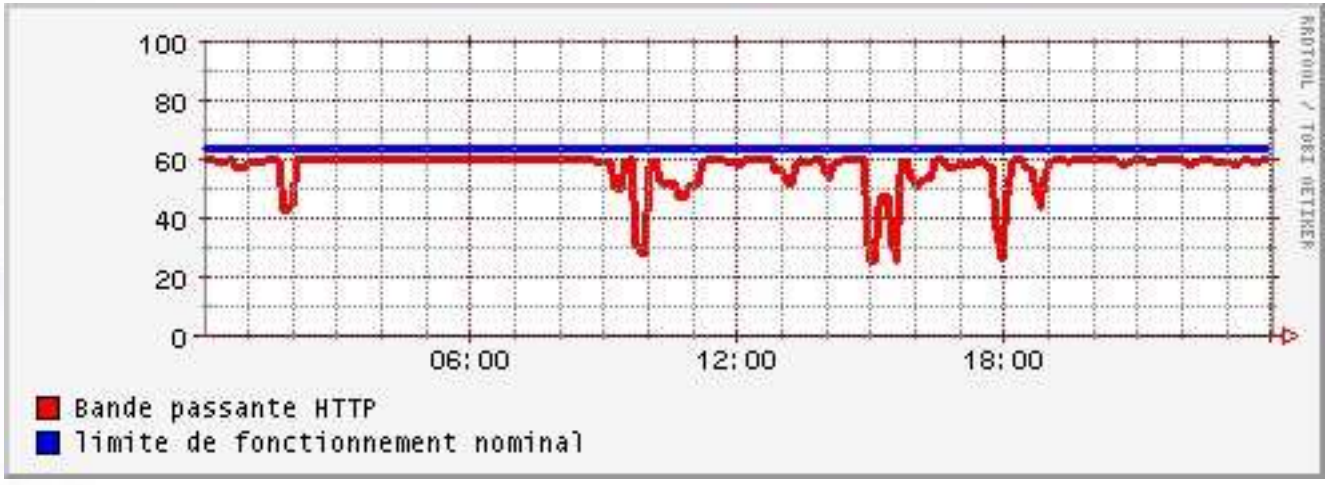
Phase II - Analyse graphique (1)

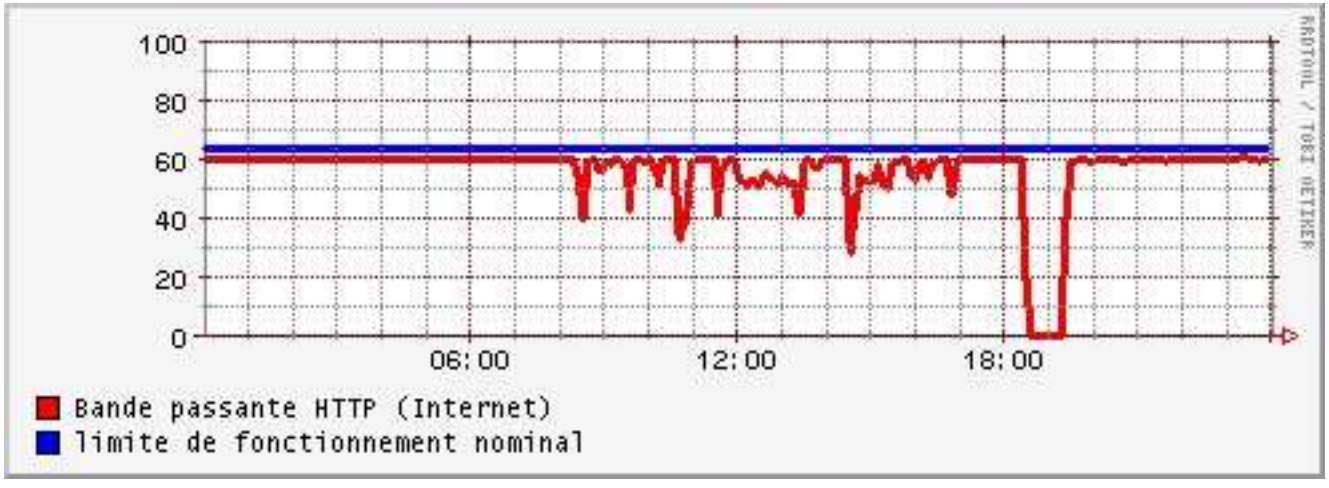




(c) 2004 - G. Arcas
<guillaume.arcas@free.fr>

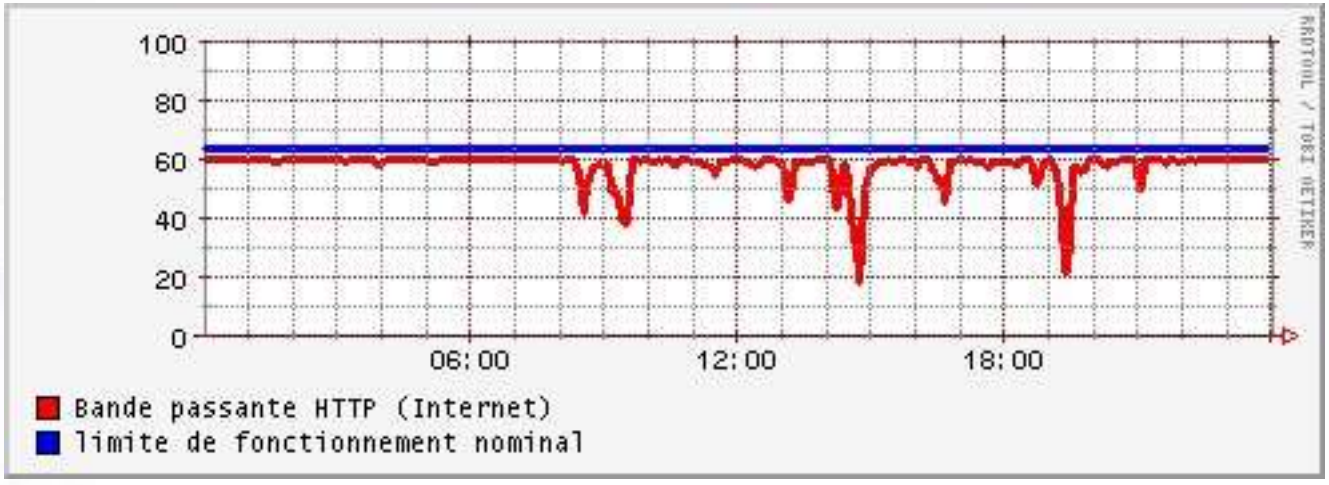
Phase II - Analyse graphique (2)

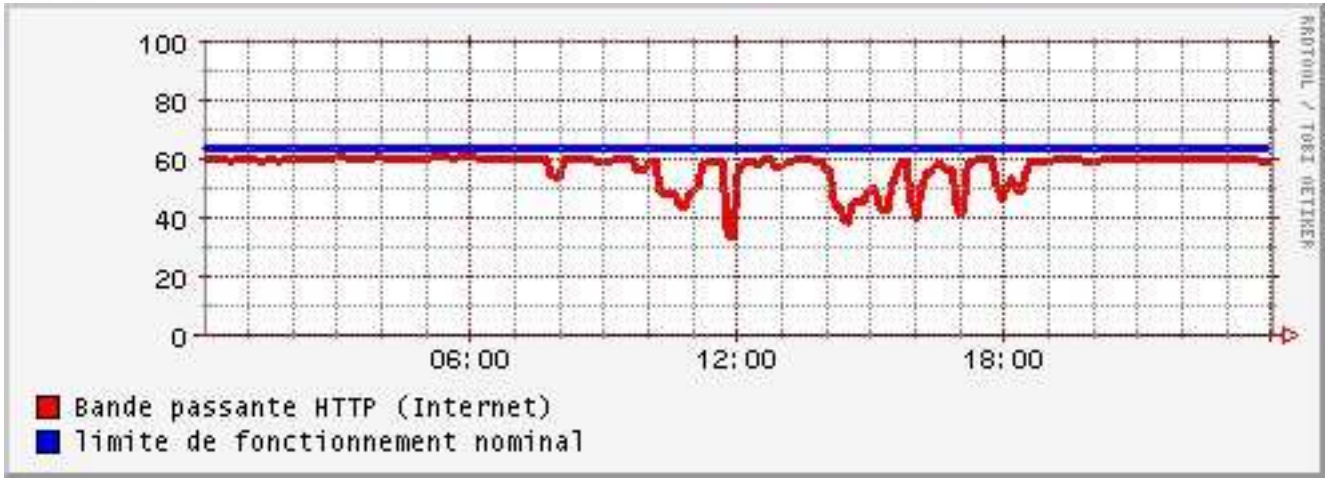




(c) 2004 - G. Arcas
<guillaume.arcas@free.fr>

Phase II - Analyse graphique (3)





(c) 2004 - G. Arcas
<guillaume.arcas@free.fr>

Snort

- Snort (2.1.1 et 2.1.2)
  - Note : Snort a été retenu comme sonde réseau. L ’IDS en tant que tel peut très bien être construit au-dessus d ’une architecture Prelude-IDS.
- Comment traduire - d ’une manière ou d ’une autre - la phrase suivante :
  - si n connexions sont faites en x secondes vers y adresses depuis 1 seule, avec n = 95% y alors : faire quelquechose (alerter, couper la session, etc…)
- Règles Standard
  - Règles standard
    - Event Thresholding
  - Module flow-portscan
    - Module prometteur… dans le README.
      `This is module is designed to detect portscans based off flow creation in the flow preprocessors.` **`The goal is to catch one->many hosts and one->many ports scans.`**
    - Documentation peu claire et réglages pifométriques
  - Module SPADE
    - Adapté à la détection d ’évènements inhabituels.

Nouvelles idées

<guillaume.arcas@free.fr>

D ’abord réfléchir...

- Exemple de quelques « vers » :
  - Code Red I & II ;
  - Nimda ;
  - Slammer ;
  - Blaster.
- Y a t-il des points communs ?
  - algorithmes de recherche de cibles ;
  - vitesse de propagation

… avant d'agir.

- Et si on modélisait le comportement d'un ver ?
- Objectif : trouver les bons réglages pour les modules de détection Snort.
- Quelques outils testés :
  - nmap
  - scripts PERL
  - NetWorm Simulator

Résultats

Conclusion (provisoire)

<guillaume.arcas@free.fr>

Remerciements

<guillaume.arcas@free.fr>