インターネット早期広域攻撃警戒システム WCLSCAN

鈴木 裕信
鈴木裕信事務所
hironobu@h2np.net

石黒正輝
三菱総合研究所
masa@mri.co.jp

村瀬一郎
三菱総合研究所
murase@mri.co.jp

大野 浩之
通信総合研究所
hohno@ohnolab.org

1. 要旨

インターネット上に設置されたセンサーに到着する IP パケットを計測・集計し，ベイズ推定に基づき広域的なネットワーク攻撃の活発化によるインターネットの危険状態を検知するシステム (以下 WCLSCAN)を作成し運用実験を行っている．本発表ではそのシステム概要，評価，実際のケース紹介，一般ユーザの利用方法を報告する．

2. はじめに

近年においてはシステムの脆弱性の発見から exploit コードや攻撃コードの出現までの期間は非常に短くなっており，0-day Attack のように脆弱性情報が公開される前に，その脆弱性を狙った攻撃も行われている[1]．一方でベンダー等による脆弱性対応も進んでいるため，攻撃側は脆弱性が有効である短期間に広域に攻撃する傾向が見られる．また Slammer や MSblaster のように極めて短時間で一気に広がるようなワームが発生するため 24 時間 365 日体制の監視を続ける必要がある．本研究では，広域に影響するインシデントでは不特定の IP アドレスにたいしても攻撃 IP パケットが増えることに着目し[1][2]，その到着を計測しベイズ推定をもちいて危険度を計算し[3]，危険レベルを報告するシステムを作成した．

3. システム概要

3.1. WCLSCAN の処理ステップ

Step1: インターネット上に設置した複数センサーボックスで IP パケットの到着を記録し，暗号化した後，集積システムへ送る．**Step 2:** 集積システムはそれを復号化しデータベースへ記録する．**Step 3:** 計算システムは一定時間毎(現在 30 分間隔)で，データベースから情報を取り出し危険度を計算する．**Step 4:** 表示作成システムは計算結果を受け取り，グラフや見やすい表を作成し，公開用 Web サイトへ転送する．作成するために必要な情報はデータベースから取り出す．

3.2. 危険度の通知

Web サイト上に情報を転送し，PC などで参照が可能である．また簡易 HTML(I モード用)，HDML (EZWeb 用)を用意している[4]．筆者の場合は携帯電話からの確認回数の方が多い．危険度が高まったときメールで通知する機能もある．

3.3. ベイズ推定による攻撃検知手法

インターネット上の危険度は，時間とともに変化するため，観測に対してベイズ推定に基づき危険度推定値を繰り返し更新することにより，危険度の動的な変動に対応した推定を行う必要がある．本システムでは，ポートスキャン頻度をそのトレンド(移動平均)からの差として観測することにより危険状態を推定する．尚，ここでの危険状態とは“ネット上の広域的な攻撃活動の活発化により自サイトへの攻撃による被害が発生する可能性の高い状態”と定義とする

4. まとめ

ベイズ推定の手法が有効であるかどうかの評価実験を行った結果，有効であることがわかった．また Doomjuice[5]が発生した際では，ウィルスベンダらが警告を出す前に異常を検知し，すばやく危険な状態であることが認知できた．一般にも公開しているので、広く利用されインターネットセキュリティ向上に役立てば幸いである．

参考文献

[1] 鈴木裕信，ポートスキャンログ分析からみたインターネットセキュリティの一考察，SEA ソフトウェアシンポジューム 2001 予稿集, 2001

[2] http://isc.incidents.org/

[3] 石黒正輝ほか,ベイズ推定に基づくインターネット攻撃検知システムの開発，SCIS2004 予稿集, 2004

[4] http://www.clscan.org

[5] http://www.f-secure.co.jp/v-descs/v-descs3/doomjuice.html