L-021

未利用アドレスブロック監視型モニタリングシステムの開発

Development of an unused IP address block monitoring system

鈴木和也† 馬場俊輔† 田中貴志†
Kazuya Suzuki Shunsuke Baba Takashi Tanaka

1. はじめに

セキュリティインシデントは，年々増加傾向にあり，監視活動の重要性が高くなってきている．これまでの監視技術としてはさまざまなものがあるが，セキュリティ監視には，主に IDS が導入されている．しかし，IDS は基本的には既知の攻撃しか検出することができず，新種のワームなどが流行した場合には問題となってしまう．近年のワームの感染速度を考慮すると，未知の攻撃や新種のワームを早期に発見することは極めて重要になって来ている．

2. 目的

セキュリティインシデント，特に不正侵入を早期に発見するためにはネットワークを監視する必要がある．しかし，全てのトラフィックを検査するには大量のリソースが必要になってくるため，攻撃パケットとそれ以外に分類する工程が必要になってくる．

よって今回の目的は，ネットワークの状況を理解するために攻撃トラフィックを分類し正確に把握することである．パケットそのものを解析することによって既知の攻撃だけでなく，ゼロ day 攻撃や新種のワームを早期に発見することを目標にする．

3. システム

3.1. システム概要

本システムでは，センサをエンドユーザが存在しない未利用アドレスブロック，つまりサーバ，クライアントなどが存在しないネットワークに設置した．これはエンドユーザと同じ環境で監視を行い，実際に攻撃パケットの振舞いを把握するためである．この未利用アドレスブロックに到達するパケットは，基本的にワーム，間違いアクセス，不正アクセスのどれかであり，正常なアクセスのパケットは到達しない．したがってこのブロックに到達するパケットは，通常のアクセスとは考えにくく攻撃パケットみなすことができ，これらを精査すれば良い．

3.2. システム構成

本システムは，インターネットの末端に設置した複数のセンサとその観測データを解析するサーバから構成される．センサは監視アドレスブロックに到達するパケットを全てキャプチャし，そのキャプチャデータの保存を行う．解析サーバは，データ回収モジュール，分類モジュール，分析モジュールの各モジュールから構成される．モジュール単位に分割することによりデータの流れや処理を明確にし，システムにかかる負荷のバランスを分散することができる．回収モジュールは，センサから定期的にデータを回収し，分類モジュールへ引き渡す役割を担う．分類モジュールは，実際にデータの分類を行い，分類済みログとして保存する．分析モジュールは，分析者が解析を開始するとログを解析し，解析結果を提供する．

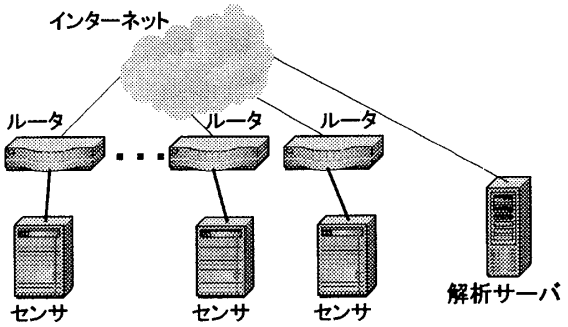

図１ システム概念図

4. 分類手法

未利用アドレスブロックに到達するトラフィックを精査するためには，まず適切に分類しなければならず，分類法もいくつか存在する．一般的には TCP や UDP などのプロトコル別，ディスティネーションポートやソースポート別などがある．この一般的な分類法で実際にトラフィックを分類していくと

・複数のワームが同じポートを用いる事がある
・ポートスキャンなど各種スキャンのノイズが大きい
・恒常的に蔓延しているワームとの区別がつかない

などの問題が発生してしまう．これでは新たな攻撃や微細な準備行為を検出することが難しい．したがってこの問題を解決するために，今回は特に各パケットのソースアドレスを基準とする．このパケットの時刻を t とし，分離するための時間間隔を $\Delta t1$，$\Delta t2$ として，t から $t-\Delta t1$，$t+\Delta t2$ までの間に到達したパケットを解析範囲とする．

ここで
N：送信先ネットワークのアドレスの種類数
H：送信先ホストのアドレスの種類数
SRC：送信元ポート番号の種類数
DST：送信先ポート番号の種類数
と表１のような判定を行うことにより６種類に分類する．

表１ 分類タイプ

判定条件	N = H	N < H
SRC > DST	Port_scan	Network_scan
SRC = DST	Normal	Network_scan2
SRC < DST	Port_scan2	Network_scan3

1. Normal: 送信元ポート種類数＝送信ポート種類数
同じ送信元ポートから，数回のパケットが到達
2. Port_scan : 元種類数＞先種類数

† 横河電機株式会社

観測ホストの複数のポートに対して，複数のポートからのパケットが到達

3. Port_scan2：元種類数＜先種類数

観測ホストの複数のポートに対して，複数のポートからのパケットが到達

4. Network_scan：元種類数＞先種類数

観測ネットワークの複数の IP アドレスの１つまたは複数のポートに対して，複数のポートからのパケットが到達

5. Network_scan2：元種類数＝先種類数

観測ネットワークの複数の IP アドレスの１つまたは複数のポートに対して，一つまたは複数のポートからのパケットが到達

6. Network_scan3：元種類数＜先種類数

観測ネットワークの複数の IP アドレスの複数のポートに対して，一つまたは複数のポートからのパケットが到達

5. 実証実験

今回構築したシステムを実際に運用し，実証実験を行った．実証実験を行ったモニタリング環境は，エンドユーザとして ADSL 契約をし，８個の連続した固定 IP アドレスのブロックを７つ用意した．このブロックにはサーバやクライアントなどは設置せずに未利用アドレスブロックとしてモニタリングポイントとした．モニタリングシステムには以下のものを利用した．また，分類方法における Δt1，Δt2 はともに 60 秒とした．

センサ，解析サーバ：DELL Power Edge 750

OS：FreeBSD 5.2.1

アプリケーション：tcpdump version 3.7.2

ライブラリ：libpcap version 0.7

6. 観測結果

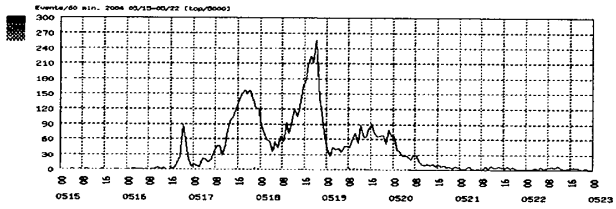

図１　TCP/5000 の全てのアクセス

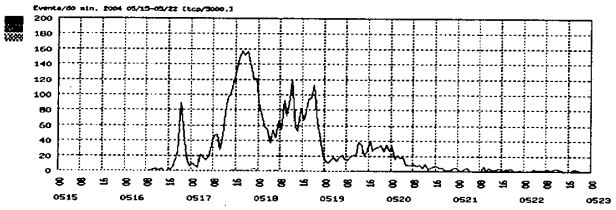

図２　TCP/5000 のみのアクセス

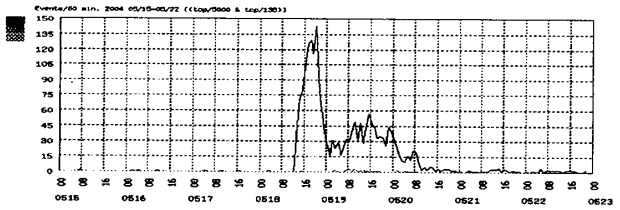

図３　TCP/5000 と TCP/135 のセット

今回構築したシステムを用いて実証実験を行った．実証実験で得られた結果をグラフにしたものを図１～図３に示す．図１のグラフは過去の事例において，TCP/5000 にアクセスしてきた総イベント数のグラフとなっている．図２のグラフは同期間において，TCP/5000 のみにアクセスしてきた総イベント数のグラフとなっている．同様に，図３のグラフは同期間において，TCP/5000 と TCP/135 の組み合わせとしてアクセスしてきた総イベント数のグラフとなっている．図３を見ると 5000 番ポートと 135 番ポートをセットでアクセスするものが 5 月 18 日頃急激に発生し，約２日後には減少して行くのがわかる．

7. 考察

本システムで解析を行った期間には 2 種類のワームの感染が流行しており，今回構築したシステムではこれらのワームを分離することが出来た．シマンテック社などウィルスベンダの報告[1][2]によると，一つ目のワームは LSASS の脆弱性を悪用する Bobax.C であり，二つ目のワームは複数の既知の脆弱性を利用する Kibuv.B である．これらのワームのうち，Kibuv.B に関しては図 2 となっており，Bobax.C に関しては図 3 の通りとなっている．また，Bobax.C に関しては，このワームの発生時期がベンダ発表と同時期となっているため，本システムを用いてモニタリングすることにより 2 種類のワームを分離出来ることが確認できた．また，今回の実験の結果，受信したデータ量としてはモニタリングポイント１ブロックにつき 10～20KB/day 程度の流量となっている．この程度の流量であれば，大量のリソースを必要とせず，モニタリングポイントを増やすことが可能である．

8. おわりに

今回の実験では，エンドポイントの未利用アドレスブロックにセンサを設置し，受信したパケットを６種類に分類した．その結果，攻撃パケットの振る舞いを把握することが可能になり，ワームの分離が可能となった．今後の課題であるが，今回，モニタしたアドレスブロックは 8 個程度の小さいレンジであった．しかし，クラス B のような広大なレンジを観測すると，本来異なるイベントが同一イベントとみなされてしまう可能性があるため，分類方法における Δt の調整を行う必要があると思われる．

なお，本研究は情報通信研究機構(NICT)から「広域モニタリングシステムに関する基盤技術の研究開発」として受託し，実施中である．ここに記して謝辞を表する．

参考文献

[1]http://www.symantec.co.jp/region/jp/sarcj/data/w/w32.bobax.c.html

[2]http://securityresponse.symantec.com/avcenter/venc/data/w32.kibuv.b.html

[3]obin Sommer, Vern Paxson, “Intrusion detection: Enhancing byte-level network intrusion detection signatures with context, Proceedings of the 10th ACM conference on Computer and communication security”, Oct.2003