Slammer ワーム ウォッチング

奈古屋広昭

1 はじめに

2003 年 1 月 25 日 (土) に発生した Slammer ワーム[1]は、Microsoft SQL サーバの脆弱性を利用して感染するもので、韓国全土のインターネットが一時麻痺するなど全世界的な影響を及ぼしました。一昨年に蔓延した CodeRed / Nimda ワーム以来、久々の「大当たり」だったようです。

幸い学内には Slammer ワームに感染してしまったホストは無かったようで、対外ファイアウォールでこのワームをブロックするまでの 2 時間ほどの間、国立キャンパスのネットワークが不安定になる以外は、直接の被害はありませんでした。

さて、たまたま以前から対外線のトラフィックをモニタしていた関係で、この Slammer ワームの国立キャンパスへの攻撃状況についてのおおざっぱな記録が残りました[2]。というわけで本稿ではその記録のごく簡単な解析結果を紹介します (注記がなければ以下に記載のある日時はすべて JST です)。

2 攻撃状況

グラフ 1 は発生日である 1 月 25 日の攻撃 (ワーム到着) 数と送信元数 (異なるソースアドレスの総数) を分単位で集計したものです。国立キャンパスへ最初に Slammer ワームが到着したのは 1/25 14:29:28 なのですが 2 分後の 14:31 には 1 万回/分以上に攻撃回数が増大し 7 分後の 14:36 には 15000 回/分と攻撃回数がピークに達しています。[1] によると “slightly before 05:30 UTC on Saturday, January 25” に Slammer ワームの拡散が始まったそうなので、ほとんどタイムラグ無しで一橋大学にもワームが届いていたことになります。

なおグラフ中の A~E は、SINET でのフィルタリング実行日時です。これらの日時に各ノードや IX との接続点などで UDP port 1434 のフィルタリングをおこなった旨の通知が SINET から送られてきていたので、グラフに書き込んでみました。目の子で見た印象では、一橋大学ローカルには A,D (某大学ノードでのフィルタリング) と E (IX や ISP との間のフィルタリング) あたりが効果があったのかなあ、というところでしょうか。

グラフ 2 は攻撃回数と送信元数の推移です。1 時間毎の集計で縦軸は対数目盛になっています。1

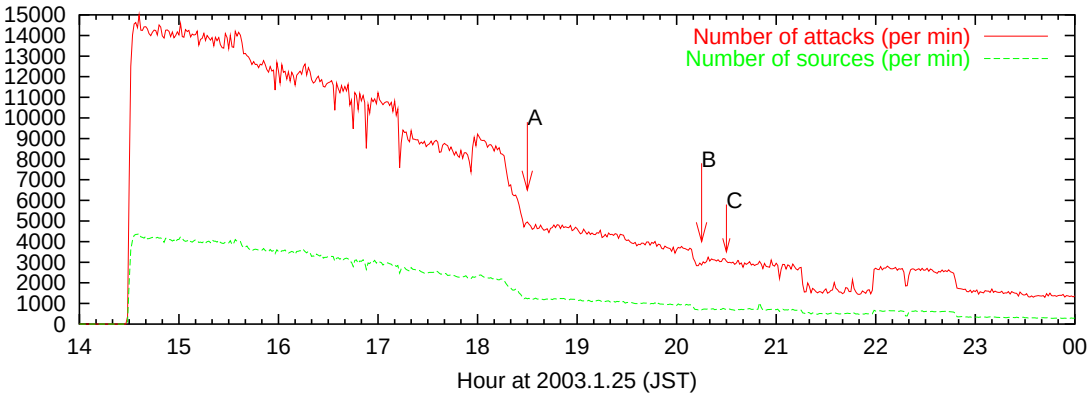
---

[1] CERT Advisory CA-2003-04 MS-SQL Server Worm, `http://www.cert.org/advisories/CA-2003-04.html`

[2] 対外ファイアウォールの外で tcpdump によりパケットをキャプチャしたログから

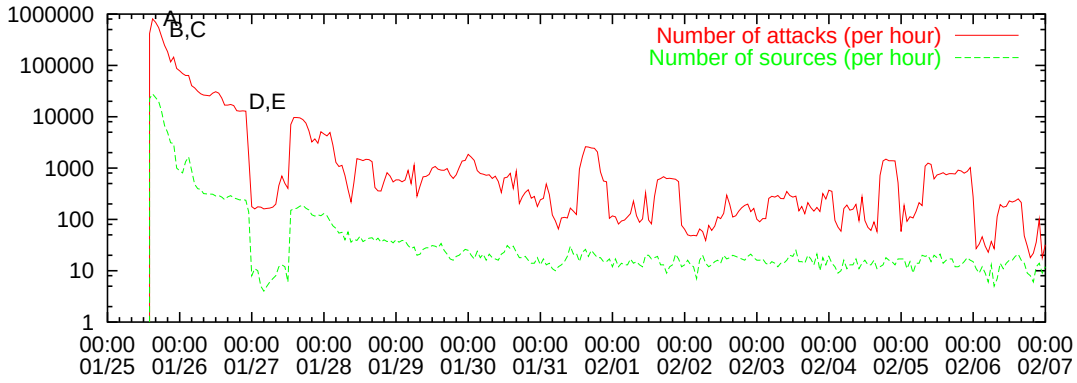
- source address が学外のアドレスブロックに含まれている
- source port が 1024 以上、かつ destination port が 1434
- IP,UDP ヘッダを除いたパケット長 (データサイズ) が 376 バイト

である UDP パケットを Slammer ワームと判定し抽出しました。なおキャプチャシステムの性能的な問題で多少 (最大で 0.1% くらい) のとりこぼしがあります。



グラフ 1: 1 月 25 日の攻撃回数/送信元数

月 27 日にはピーク時の 1/100 程度に収束していますが、その後も延々と、いまだに毎時数十個程度のワームが送られてきていることがわかります。



グラフ 2: 攻撃回数/発信元数の推移

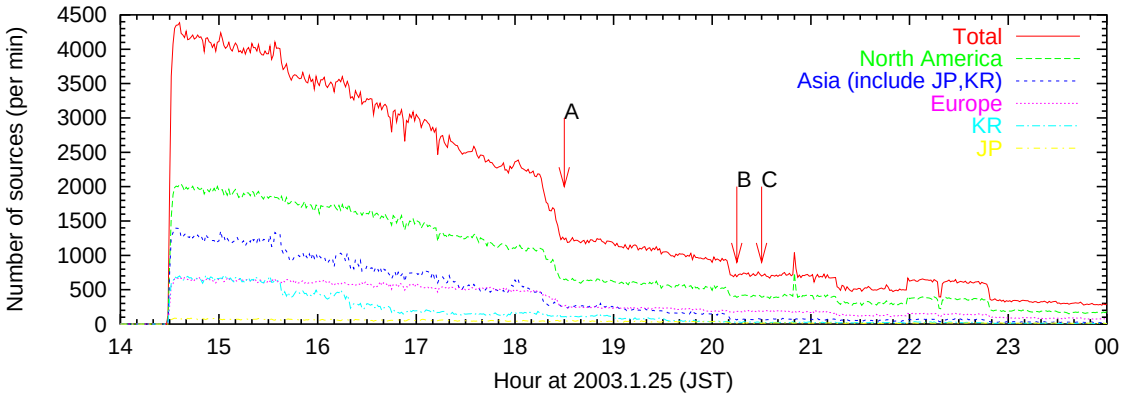
グラフ 3 はワーム発生日である 1 月 25 日の発信元数を分単位で集計したグラフです。一般論としては発信元情報は詐称されている可能性があるため信用できませんが、今回の Slammer ワームは発信元の詐称はおこなわないようです。そこで、国別のアドレスブロック割り当て表[3]を利用して発信元を国・地域別に分類してみました[4]。

発生直後の攻撃元内訳を見ると、北米からの攻撃が半数弱で次いでアジア (とくに韓国)・欧州ということで、(一橋大学にとっては) 火元は国外だったことがわかります。韓国からの攻撃が (他地域と比較して相対的に) 急速に収束していますが、これは韓国では Slammer ワームの影響でネットワークそのものが麻痺してしまった、という事情が反映しているのではないかと推測しています。

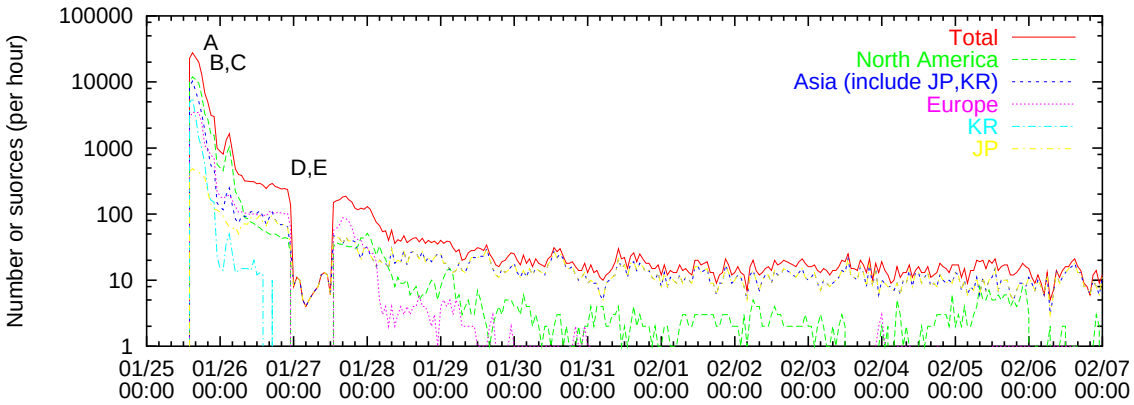
---

[3] ARIN(`http://www.arin.net/`), APNIC(`http://www.apnic.net/`), RIPE(`http://www.ripe.net/`), LACNIC(`http://lacnic.net/`) の anonymous ftp サイトで公開されています。

[4] 本稿では 2003.2.1 現在の下記データを利用しました。
`ftp.arin.net/pub/stats/arin/arin.20030201`, `ftp.apnic.net/apnic/stats/apnic/apnic-2003-02-01`, `ftp.ripe.net/ripe/stats/ripencc.20030206`, `lacnic.net/pub/stats/lacnic/lacnic.20030201`



グラフ 3: 1 月 25 日の地域別発信元数



グラフ 4: 地域別発信元数の推移

グラフ 4 は地域別発信元数の推移です。1 時間毎の集計で縦軸は対数目盛になっています。2 月 7 日までの累計によると 135 の国・地域からの攻撃が届いていますが、海外からの攻撃は数日で収束していて以後はだらだらと国内からの攻撃が継続しているようです。

3 まとめ

このように突如発生し急速に拡散する攻撃に対して、一橋大学のキャンパスネットワークはほぼ無力です。したがって運用体制や技術面などについての、なんらかの改善が必要だと思われます。

参考文献

[1] The Spread of the Sapphire/Slammer Worm, http://www.cs.berkeley.edu/~nweaver/sapphire/

なごやひろあき 情報処理センター
Email: nagoya@cc.hit-u.ac.jp