メモリ感染型ネットワーク･ワームおよび不正プログラム（ペスト）の脅威とその対策

不正プログラム調査WG
渡部　章

2002 年 6月 3日

1.はじめに

JNSA

- 1.1 不正プログラム調査WGについて
- 1.2 平成14年度成果物について

1.1 不正プログラム調査WGについて

■活動目的

トロイの木馬、スパイウェア、リモートアクセスツールなど、不正アクセスを目的にしたハッキングツールが増加しています。また、ウイルス、ワームも同様に近年では不正アクセスを目的としたものも少なくない。実際の不正アクセス技術ではこれらのツールを組み合わせて利用するケースが多く、不正プログラムとその対策の調査研究を実施し、その成果を普及させる。WGリーダー：渡部　章(アークン)

■活動内容

様々な不正プログラムを分類化し、その利用目的を明らかにし、各分類における代表的な不正プログラムと、昨今話題となっている不正プログラムのメカニズムを説明できるような資料を作成公開します。合わせて具体的な対策方法も示して、この種の技術に関する正しい知識を広めていく。また、既存のセキュリティ技術のこれら不正プログラムによる侵入、攻撃に対する有効性を検証します。

1.2 平成14年度成果物について

- 平成14年は、SQLSlammerワームが発生し、インターネットのインフラに多大な被害を出した。
- 当WGでは平成13年に猛威を振るったCordRedの被害からの教訓を何故生かせなかったのかについて、大きな疑問を抱いた。
- そこでこれらの既存のセキュリティ製品では対策できなかった「メモリ感染型のワーム」について、構造、被害状況、対策について取りまとめることにした。

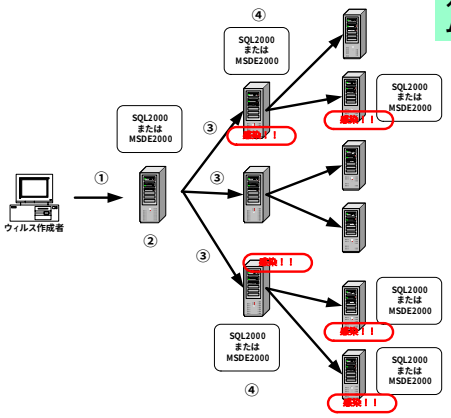
2. SQLSlammerワーム

- 2.1 構造
- 2.2 被害状況
- 2.3 各ワクチンメーカーの対応状況

概要：
平成14年7月にマイクロソフトから報告された脆弱性である、MS02-039を突いて、システムに侵入するワームで、平成13年7月に猛威を振るったCodeRedの数十倍のスピードで感染が広がった。
MS02-039：
SQLサーバが利用するUDP/1434ポートのバッファオーバフローの問題。
綿密に作成されたパケットをUDP/1434ポートが受け取ると、SQLサーバが異常終了してしまう。

2.1 SQLSlammerの構造

Slammerの動作



プログラム自体は376バイトのアセンブラで記述されており、非常にコンパクトになっている。また、ハードディスクへの書き込みは行わず、メモリを介して感染するため、再起動するとワームはクリアされる。

①ワームを送りつけ、メモリに感染させる
②ランダムにIPアドレスを作成
③作成したIPアドレスにワームを送信
④感染したサーバは②と③を繰り返す。

2.2 SQLSlammerの被害状況

- **The Computer Science Division** (http://www.cs.berkeley.edu/~nweaver/sapphire/)
  - わずか30分で7万5千台が感染。トラフィック過多によりネットワークが輻輳、インターネットトラフィックが各所で輻輳するなど被害が拡大した。特に韓国での被害がひどく、DNSサーバがダウンするなど半日インターネット接続ができない状態が続いた。
- 英Mi2g(http://www.mi2g.com/)
  - 最初の5日間で推定9億5000万ドルから12億ドルの被害が発生
- Computer Economics (http://www.computereconomics.com/)
  - 生産性損失額は77億ドル強、後処理にかかったコストは7億5000万ドルから10億ドル
- その他
  - 各調査機関でばらつきがあるが、全世界で数億米ドル（数百億～一千億円弱）
  - Bank of America　1/25 ATM（現金自動預払機）約1万3000台が利用不可
  - Washington Mutual　ATMが1月27日まで利用不可能（2日間にわたって使用不能）
  - Continental Airlines　オンラインチケットおよびチェックインに問題、一部フライトが遅延
  - Microsoft　「Asheron's Call 2」のゲームサーバにアクセス不可
  - シアトル市　緊急通報用ネットワーク(911)が機能不全
  - 韓国
    - 韓国のインターネットユーザの大半が加入しているKTテレコムのDNSサーバがダウン、半日以上国内でのインターネット接続ができなくなった。(注)
    - 実被害、数百億ウォン（数十億円）
    - 韓国保険協会、約860,000ドルの支払い

注意：韓国内SQLServer2000の正規ライセンス52,000台のうち、49,000台がパッチ適用済み、残り3000がパッチをあてていなかった、さらに、不正コピーは正規ライセンスの倍の10万ライセンスであった。(朝鮮日報 より)

2.3 各ワクチンメーカーの対応状況

- シマンテック：(W32.SQLExp.Worm)
  - http://www.symantec.com/region/jp/sarcj/data/w/w32.sqlexp.worm.html
  - 駆除ツールv1.0.4.1を別途配布中。(2003/4/8)
- トレンドマイクロ：(WORM_SQLP1434.A)
  - http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM_SQLP1434.A
  - パターンファイルでの対応ではなく別途トレンドマイクロシステムクリーナにて対応中。(2003/4/8)
- 日本エフセキュア：(Sapphire, Slammer)
  - http://www.f-secure.co.jp/v-descs/v-descs3/slammer.htm
  - パターンファイルにて対応、別途Slammerの専用検知ツールを配布中。(2003/4/8)
- 日本ネットワークアソシエイツ：(W32/SQLSlammer)
  - http://www.nai.com/japan/virusinfo/virS.asp?v=W32/SQLSlammer
  - 無償ウイルス駆除ツール「スティンガー」にて別途SQLSlammerに対応中。(2003/4/8)
- ソフォス：(W32/SQLSlam-A)
  - http://www.sophos.co.jp/virusinfo/analyses/w32sqlslama.html
  - マイクロソフトのMS02-039 でのパッチによるアップデートを推奨。(2003/4/8)

3. CodeRedワーム

- 3.1 構造
- 3.2 被害状況
- 3.3 各ワクチンメーカーの対応状況

3.1 CodeRedの構造

概要：
- マイクロソフトWINDOWS2000のIIS機能の部分に、バッファ・オーバーフローを引き起こす可能性のあるバグ(MS01-033)が存在しており、CodeRedはこれを利用。

構造：
① IIS機能に不正なリクエスト送信、IISにバッファオーバーフローを引き起こす。
② ワームコード本体を送信し、メモリ上にワームコードを上書き格納する。
③ OS内部の命令によって、ワームがそのサーバーマシンで活動状態となる。
④ 他の感染できるサーバーに対して感染活動を開始する。
⑤ IISが英語版の場合は、Webを改ざんする。

感染条件：
- Windows2000或いはWindowsNT4を動作させていて、かつIIS機能を動作させているマシン。

IISの脆弱性 (MS01-033)：正常なサーバープログラムでは、入力されるリクエストのデータ長をチェックしており、入力データがバッファサイズより長ければ、そのデータを受け入れないようにしている。または、バッファが短ければそれに対応した正しい処理を行っている。パッチが提供されるまではIISでは長さチェックが行われていなかった。対策としては、このバグに対するパッチがマイクロソフトから既に公開されているので、これをインストールする。

3.2 CodeRedの被害状況

●CodeRedのアウトブレーク（広範囲にわたる大量の感染被害）は平成12年の夏に2度にわたって起き、各々20万台～40万台（一説によると最大で75万台）のサーバに感染した。
●特に一回目のアウトブレークでは米国ホワイトハウスのWebサイトを攻撃する構造になっていることが分かったため、急遽IPアドレスの変更作業が行われるという事態も発生した。
●二回目のアウトブレークでは、事前にマイクロソフトを始めとする主要ソフトウェアベンダー及び米国政府機関・各種団体等による事前の警告が効を奏して、最初のうちは全てをコントロール下においていると見なされていたが、4日目にバックドアをインストールする亜種(CodeRedII)が発見されるにあたり、状況が一変した。当該亜種は約2ヵ月後に休眠する仕様であったため、必然的にアウトブレークは治まった。
●CodeRedIIの収束以降はユーザサイドの対策が進んだことも有って大規模なアウトブレークは起きていないが、定点観測によるとコンスタントにトラフィックが確認されており、今だ対策が施されていないサーバがインターネット上に存在することを示唆している。
●CodeRedIIが収束した平成14年10月1日現在で被害総額は全世界で26億ドル（約3,000億円）にも上ると言われている。

間接的な被害：このCodeRedの被害は直接的なものに留まらず、CodeRed対策パッチと称してメールの添付ファイルを開かせるようないわゆる「便乗ウィルス」や、CodeBlue、CodeGreen (Anti CodeRed)のような亜種が大量に出現した。また、第一次アウトブレーク初期、及び、第二次アウトブレークのCodeRed II発見直後に起こった不正確な情報や過剰に神経質な対策が引き金となったいわゆる風評被害も統計は出ていないものの決して無視できないものであろう。

3.3 各ワクチンメーカーの対応状況

- トレンドマイクロ
  - 7月18日発見、即日にウィルス定義を更新して供給
  - 7月31日にCodeRed v2に対応
  - 8月4日にCodeRed IIを発見、6日ウィルス定義を更新して供給
- シマンテック
  - 7月17日発見、即日にウィルス定義を更新して供給
  - 8月1日にCodeRed 及びその亜種(CodeRed v2)に対応した脆弱性チェックツールと検知・駆除ツールを供給
  - 8月4日にCodeRed IIを発見、5日ウィルス定義を更新して供給
- ネットワークアソシエーツ
  - 7月18日発見、英語版は即日、また日本語版は20日にエンジン更新という形で供給
  - 8月4日にCodeRed IIを発見、5日にエンジン更新という形で供給

上記の主要ベンダーを比較すると、一時期指摘された英語と日本語の情報提供のタイムラグがほとんどなくなっていることがうかがえる。特に、最初のCodeRedに関しては発見の日に即日対策DB・エンジンをリリースという比較的レベルの高い対応をしていると言える。但し、最初の被害発生から新種のワームと断定されるまで数日間を要しており、その間のリスクはカバーできないという限界をも同時に示している。

4. 対策について

- 4.1 ネットワーク･ワームの脅威
- 4.2 ワクチンで検出できない理由
- 4.3 対策への考察

4.1 ネットワーク･ワームの脅威

- SQLSlammerワームの最大の特徴は活動中にプログラムとしてファイルをつくらず、コンピュータのメモリから、インターネットを介して、他のコンピュータのメモリに感染を広げる「常駐感染型ワーム」だという点で、CordRedも代表的な「常駐感染型ワーム」と言える。
- これらのワームはファイルを作らないため、既存のウイルス対策ソフトではリアルタイムにメモリからワームを検出することが困難である。
- SQLSlammerワームは、ねずみ算式に感染したワームが一斉に感染活動を繰り返したために、インターネット上のトラフィックが急増し、ネットワークが混み、世界的にネットに障害が発生した。
- 特に下層に大量の感染コンピュータを従えているようなインターネットサービスプロバイダーなどのサーバはそのトラフィックに耐えきらずにシステムダウンを起こしたために、一部で完全にネットがつながらない状態になった。
- 現象としては、DNS(ドメインネームサーバ)攻撃やDDoS攻撃のように見えるが、実際にはこのワームは感染活動だけでこれだけの被害を与えた。

4.2 ワクチンで検出できない理由

- ワームが出現してから被害発生までの期間が短過ぎて、定義ファイルがまだ出来ていなかったこと
- インターネットサーバに対して、ネットワーク型のウイルス対策ソフトは導入していても、ホスト型のウイルス対策ソフトを導入していなかったこと
- 例えホスト型であっても、ウイルス対策ソフトのメモリ常駐監視機能がファイルアクセスだけを対象としており、メモリ上で実行中のウイルスを検索対象としていなかったこと

早期発見方法：メモリ常駐監視機能では検出不可能なのだが、通常の手動検索機能では、この種のワームをメモリから検出することができる。対象ワームが定義ファイルに追加されているならば、定期的にサーバに対して手動検索をしていれば、この種のワームについては手動検索プロセス中のメモリ検査で検出可能である。

4.3 対策への考察

社会
- インターネット全体をスローダウンさせる以上、もはや国際的問題と言える。
- 新種ワームは、今後のウイルスに多大な影響を与え、益々強力なものが出現する。
- インフラとしての対策として、根幹となる各国の接続サーバでの対策が必要。
- セキュリティ警告がウイルス作成者にヒントを与えることに対する警告のあり方について検討が必要。
- 専門家達は「一般ユーザの半歩先を歩み、そしてそれを知らしめる」活動が必要。

ユーザ
- 定義ファイルの更新は、最新のウイルスやワームの感染・発病速度に間に合わないと知る。
- 現在開いている未使用ポートを内向き（被害予防）、外向き（加害予防）の両方向について閉じる。
- 各サーバに常駐型のウイルス対策ソフトおよびペスト対策ソフトを導入する。
- 定期的にインタネットサーバに対して手動検索を実施する。
- 復旧のプロセスとして、再起動の前にメモリダンプを取ること。
- 各ベンダーのセキュリティ警告の情報を収集する。
- ベンダーが提供する最新のパッチ（修正プログラム）をあてる。
- 適切なセキュリティ製品を導入する。
- 「風評」によって、あらかじめシステムダウンさせるという過剰防衛が無いようにする。

ベンダー
- 定義ファイルを更新する。
- リアルタイムにメモリ検査を実施する機能を追加する。
- サーバソフトを開発する場合に、期待以外のデータが来ればリジェクトするなどのチェック機能を設ける。

5. おわりに

- 5.1 WG今後の展開について
- 5.2 成果物の取扱いについて
- 5.3 著者
- 5.4 参考資料

5.1 WG今後の展開について

- ウイルスによる被害は、他のセキュリティ被害に比べて圧倒的なもので、これは今後も継続するに間違いないであろう。
- ただし、ウイルス対策ソフトウェアなどの既存セキュリティ技術では対策が十分ではないSQL SlammerやCordRedなどの「メモリ感染型」のワームや、キーロガーなどのトロイの木馬やスパイウェアなどによる情報漏えいは、新しい脅威として既に多大な被害が出ている。
- これらの背景から当WGは、不正プログラムをウイルスだけに留めず、広範囲にその現況と対策について調査研究を実施していく。

5.2 成果物の取扱いについて

- 成果物の著作権、使用等の権利は、著者及びＪＮＳＡとの共有とします。引用した文章、図表についての著作権は各作成者にあります。この成果物の配布、複製、修正についきましては、JNSA事務局までお問い合わせください。

5.3 著者

■高木　みちこ(Michiko Takagi)
株式会社　グローバルエース
システム部

■奈良岡　健太(Kenta Naraoka)
株式会社ディアイティ
製品事業本部　セキュリティビジネスユニット

■濱本　常義 (Tsuneyoshi Hamamoto)
中国情報システムサービス株式会社
ネットワーク事業部

■米澤 一樹 (Yonezawa, Kazuki)
セキュア コンピューティング ジャパン株式会社

■渡部　章 (Akira Watanabe)
株式会社アークン

(敬称略、五十音順)

5.4 参考資料

■SQL Server を標的とした SQL Slammer ワームに関する情報
http://www.microsoft.com/japan/technet/security/virus/sqlslam.asp
■SQLSlammerワームコード
http://www.digitaloffense.net/worms/mssql_udp_worm/
■SQLSlammerワームデバッガの情報
http://www.digitaloffense.net/worms/mssql_udp_worm/windbg_exceptions.jpg
http://www.digitaloffense.net/worms/mssql_udp_worm/windbg_exploit_mem.jpg
■SQLSlammerワーム パケットを出力するperlスクリプト
http://www.digitaloffense.net/worms/mssql_udp_worm/worm.pl
■SQL Serverのセキュリティホールの発見者David Litchfield氏によるサンプルコード
http://archives.neohapsis.com/archives/vuln-dev/平成14-q3/0472.html
（ワームコードがそのサンプルコードと同一であることが注目される）
■CodeRedの正体（ugpop氏による）
http://home.netyou.jp/gg/ugpop/academy001-010.htm
■ IISのセキュリティホールの発見者eEye Digital Security社のホームページ
http://www.eeye.com/
■CordRed解説ページ
http://www.eeye.com/html/Research/Advisories/AL20010717.html
■CordRed II解説ページ
http://www.eeye.com/html/Research/Advisories/AL20010804.html