

株式会社ラック

公開日：2003年 8月 18日 23:55

最終更新日：2003年 8月 22日 20:30

JSOC 緊急レポート (Welchia ワーム (別名：Nachi ワーム) について)

1 . 概要

8/18 (月) 11 時頃より、JSOC の監視ログにて、TCP135 番ポートへの通信の増加および ICMP スキャンの増加を検知しました。また、スキャン活動に合わせて、RPC-DCOM の問題(MS03-026：4 . 関連 URL 参照) を利用した攻撃のほか ntdll.dll に起因する WebDAV の問題(MS03-007：4 . 関連 URL 参照)を利用した攻撃も検知しております。

現在公開されております情報 (4 . 関連 URL 参照) によりますと、この ICMP スキャンの増加は新種のワームであり、現在 Welchia ワーム (別名：Nachi ワーム) と呼ばれているものです。

このワームは Blaster ワームと同様に RPC-DCOM の問題を利用して攻撃を行うほか、ntdll.dll に起因する WebDAV の問題を利用し、IIS5.0 に対する攻撃も行います。WebDAV の問題も利用することから、Blaster ワームに比べ感染範囲がさらに拡大する可能性があります。また、感染が拡大しますと組織内のネットワークで ICMP パケットが溢れることも考えられます。

8/20 (水) 時点では、Blaster ワームに入れ替わる形で Welchia ワーム (別名：Nachi ワーム) が猛威を振っております。Welchia ワーム (別名：Nachi ワーム) は Blaster ワームとは異なり、感染の際に自動的に再起動するなどの動作を起こさないため、一度駆除した後に再び感染していることに気付かないケースもあり、十分な注意が必要です。

尚、WebDAV の問題を利用した攻撃は、日本語環境では現時点で再現しておりません。

今回利用されている可能性がある問題は、以下の問題です。

2003 年 3 月 18 日「Windows コンポーネントの未チェックのバッファにより サーバーが侵害される (815021) (MS03-007) 」

2003 年 7 月 17 日「RPC インターフェイスのバッファ オーバーランによりコードが実行される (823980) (MS03-026) 」

Microsoft 社より修正プログラムがすでに公開されております。RPC-DCOM の問題に対してはすでに Blaster ワームの感染拡大に伴い対策を実施されているところが多いかとは思いますが、対策を実施していないコンピュータは直ちに対策を施すことをお勧めします。また、WebDAV の問題に関しましても対策が実施済みであるかを早急に確認することをお勧めします。

2 . JSOC 統計情報

JSOCで検知したICMP通信とTCP135番ポートでの定点観測状況です。(図1～図4)

図1では、8/18(月)11時頃より急激にICMPの増加が見られます。また、TCP80番ポートの通信も同時刻から増加傾向にあるのは、新種ワームによるWebDAVの問題を利用した攻撃が原因であると考えられます。図2からは、ワームの活動の増加傾向は見られませんが、いまだに感染はおさまっていないことがわかります。

図3は、新種ワームの流行前後のICMPログ件数、およびユニークソースIP数の遷移傾向です。JSOCで検知した攻撃の調査から、感染していると考えられるサイトの数を示しています。(ただし、実際の感染数を示すものではありません)

図4には、国別のICMP件数を示しています。

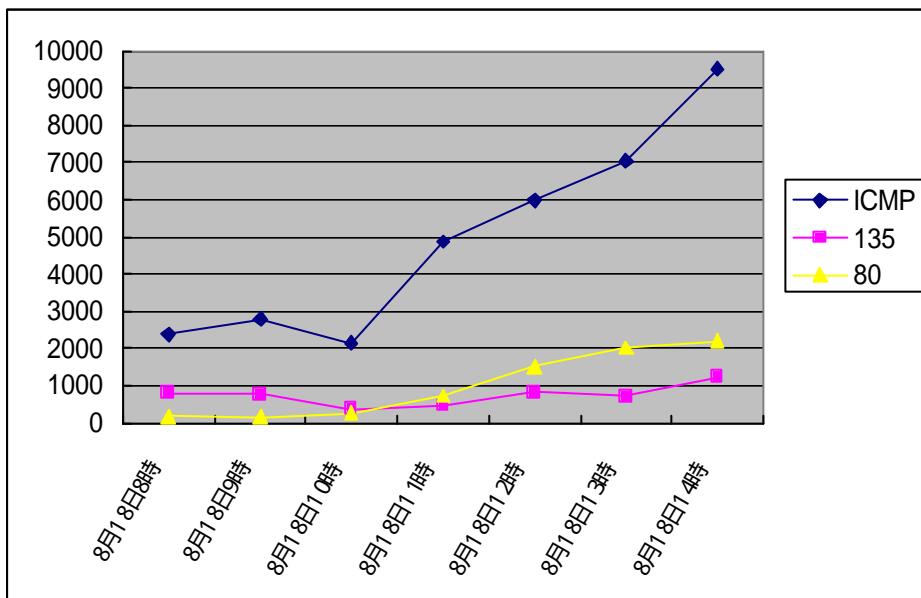


図1 定点観測状況【対象期間：2003年8月18日8:00～14:00】

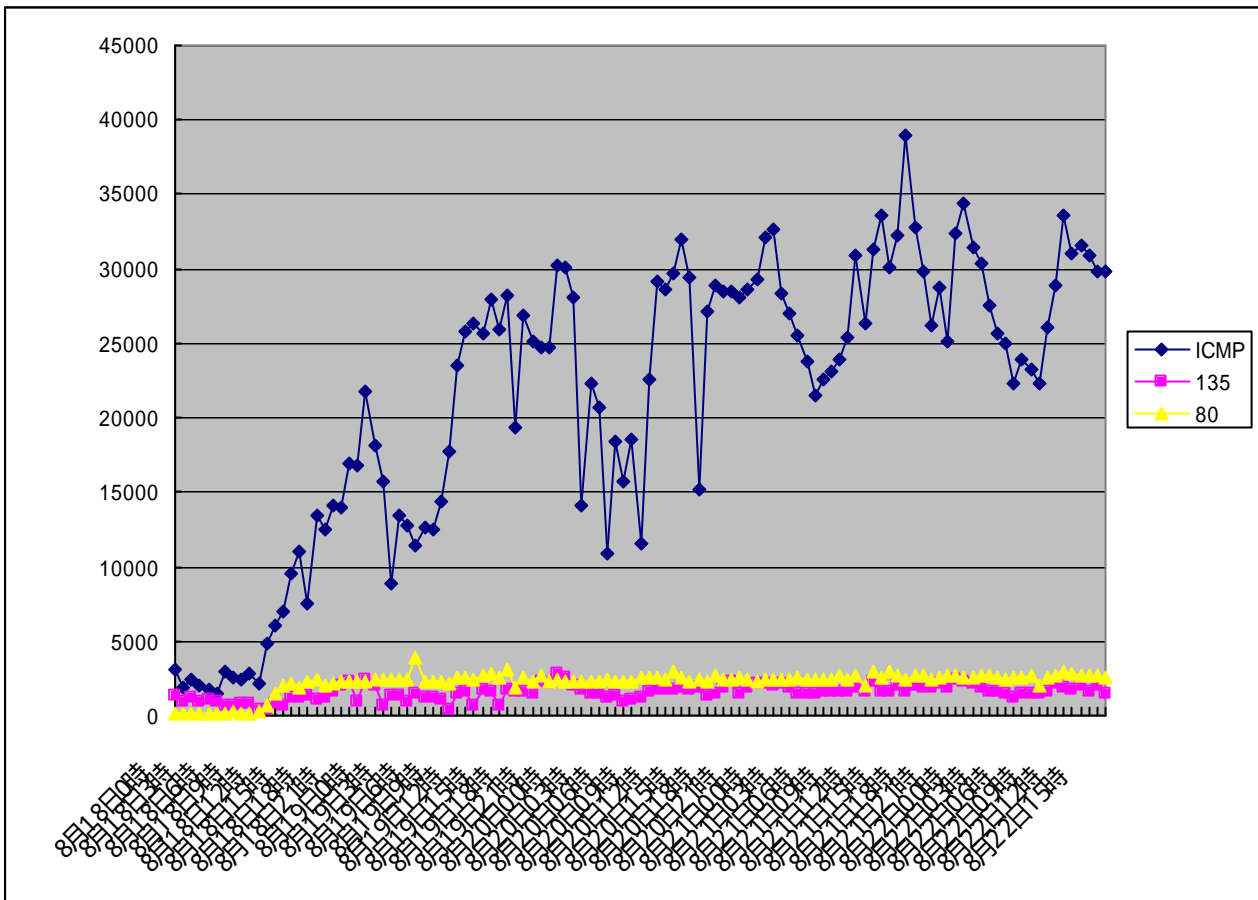


図 2 定点観測状況【対象期間：2003年8月18日0:00～2003年8月22日16:00】

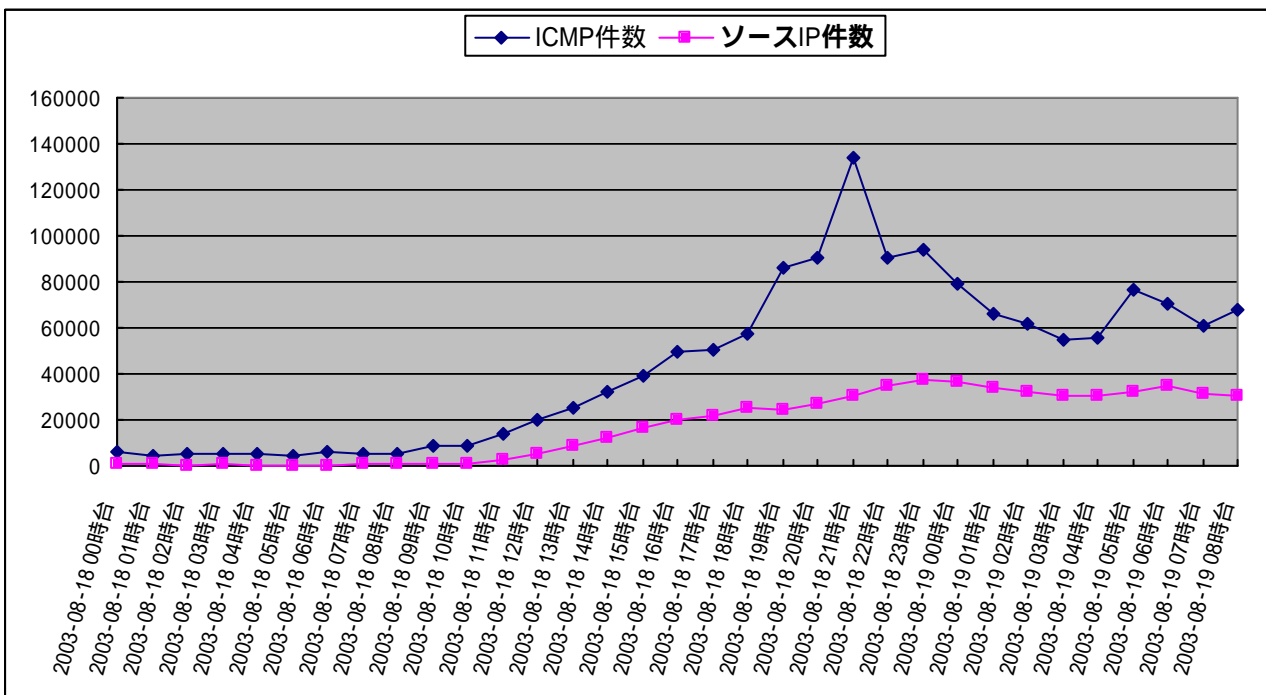


図 3 ユニークソースIPアドレス【対象期間：2003年8月18日0:00～2003年8月19日8:00】

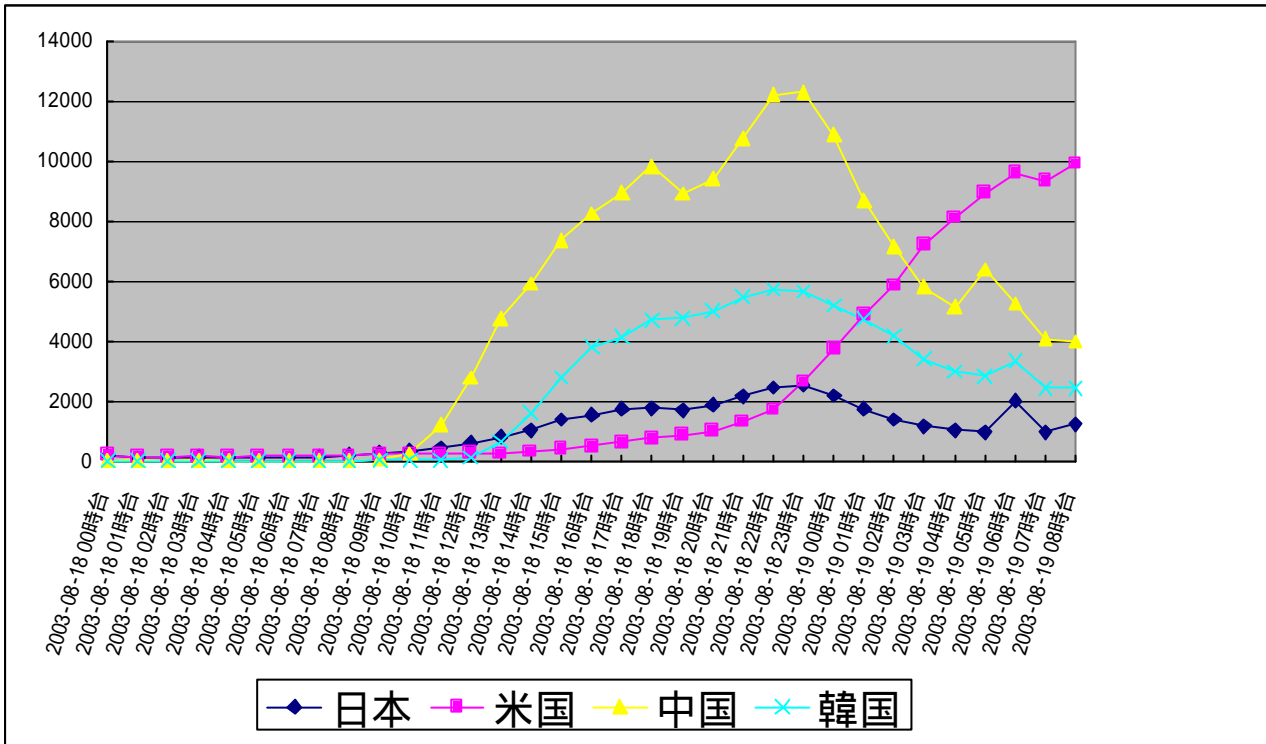


図 4 国別 ICMP 件数【2003 年 8 月 18 日 0:00 ~ 2003 年 8 月 19 日 8:00】

3 . 対策

感染が拡大しますと組織内のネットワークで ICMP パケットが溢れることも考えられます。発信源となっているコンピュータを早期に突き止め、ネットワークから切り離し、対策を実施することをお勧めします。

1) ファイアウォールまたはルータにおける対策

ファイアウォールまたはルータに以下のルールを設定します。

- ・インターネットから内部に対する、TCP 135 番ポート、UDP 135 番ポート、UDP 69 番ポートへのアクセスを許可しない。
また、インターネットから内部への許可する通信は可能な限り、外部に対して公開する必要のあるコンピュータ上の必要最小限のサービスのみに限定することをお勧めします。
- ・内部からインターネットに対する、TCP 135 番ポート、UDP 135 番ポート、UDP 69 番ポートへのアクセスを許可しない。
また、内部からインターネットへ許可する通信は必要最小限のサービスのみに限定することをお勧めします。
- ・内部からインターネットへの ICMP パケットを塞ぐことで、Ping を飛ばすことが出来なくなり、ワームの増殖を最小限に押さえることが可能です。

ネットワークの内部に感染者が存在しないことを確認するため、内部からインターネットに対する不審な痕跡（送信先が TCP135 番ポートの通信が過多、など）がないか確認してください。また、随時ファイアウォールの監視を行い、定期的なログの監査を行うことをお勧めします。

2) コンピュータ上における対策

ウイルスの駆除に関しては各ウイルス対策ベンダの情報を参照ください。なお、駆除しただけでは再度感染する可能性がありますので、以下を参照し修正プログラムを適用して根本的対策を実施してください。

Windows Update を実施し、修正プログラムを適用します。

Windows Update :

<http://windowsupdate.microsoft.com/>

Windows Update を実施できない環境にある場合、以下の URL より修正プログラムをダウンロードし適用してください。

Windows コンポーネントの未チェックのバッファにより サーバーが侵害される (815021) (MS03-007) :

<http://www.microsoft.com/japan/technet/security/bulletin/ms03-007asp>

RPC インターフェイスのバッファ オーバーランによりコードが実行される (823980) (MS03-026) :

<http://www.microsoft.com/japan/technet/security/bulletin/ms03-026.asp>

4 . 関連 URL

WORM_MSBLAST.D :(Trendmicro)

http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM_MSBLAST.D

W32.Welchia.Worm :(Symantec)

<http://www.symantec.co.jp/region/jp/sarcj/data/w/w32.welchia.worm.html>

RPC インターフェイスのバッファ オーバーランによりコードが実行される (823980) (MS03-026) :
(Microsoft)

<http://www.microsoft.com/japan/technet/security/bulletin/MS03-026.asp>

Windows コンポーネントの未チェックのバッファにより サーバーが侵害される (815021) (MS03-007) :
(Microsoft)

<http://www.microsoft.com/japan/technet/security/bulletin/MS03-007.asp>

Blaster に関する情報 :(Microsoft)

<http://www.microsoft.com/japan/technet/security/virus/blaster.asp>

Blaster ワームへの対策 - Windows XP 編 :(Microsoft)

http://www.microsoft.com/japan/technet/security/virus/blasterE_xp.asp

Blaster ワームへの対策 - Windows 2000/Windows NT 4.0 編 :(Microsoft)

http://www.microsoft.com/japan/technet/security/virus/blasterE_nt4w2k.asp

JSOC 緊急レポート (Blaster または Lovsan ワーム) :(LAC)

<http://www.lac.co.jp/security/jsoc/report/index.html>

CERT Advisory CA-2003-20 W32/Blaster worm :

<http://www.cert.org/advisories/CA-2003-20.html>

http://www.lac.co.jp/security/intelligence/CERT/CA-2003_20.html (邦訳)

5 . 補足

【ICMP (Internet Control Message Protocol) とは】

ICMP は ping コマンドなどで利用されており、通信先の機器が状態を調べることができます。通常、ICMP の通信自体は攻撃ではありませんが、ICMP の通信量が過多になることによりネットワークが遅くなる、などの弊害が出てきます。

【RPC (Remote Procedure Call) とは】

RPC はリモートからファイル共有やディレクトリ・アクセスなどを行うときに使用されるサービスで、Windows 環境において最も基本的なサービスのひとつです。サーバ、クライアントを問わず、デフォルトの Windows 環境において有効になっています。

今回利用されているのは RPC に関する以下の問題です。

「RPC インターフェイスのバッファ オーバーランによりコードが実行される (823980) (MS03-026) 」

<http://www.microsoft.com/japan/technet/security/bulletin/ms03-026.asp>

【裏口 (バックドア) とは】

侵入者が一度侵入したコンピュータに対して、仕掛けた別の侵入経路のことです。侵入者は再度、同じコンピュータに侵入しようとする場合、この別経路を使用して侵入してきます。このバックドアは巧妙に隠されていることが多く、仕掛けられたコンピュータ上からは、裏口 (バックドア) を仕掛けられていることをなかなか発見できないことが少なくありません。また最初の侵入経路とは別に作成されるため、管理者が最初の侵入経路に気付いてパッチ適応等の対策を講じた後にも容易にさらなる侵入を可能にします。

裏口の多くは、リモートから利用可能な管理者権限でのコンソールの提供など、より直接的に攻撃を行うことを可能にします。また、裏口を作成する機能を持つワームも多数あります。BUGBEAR や BadTrans と呼ばれるワームはその一例です。

【株式会社ラックについて】

株式会社ラックは、いち早くネットワーク社会の到来を予測して 1986 年 9 月 3 日に設立されました。ネットワークセキュリティ ソリューション分野でのリーディングカンパニーを目指し、コンピュータセキュリティ研究所の先進セキュリティテクノロジーを JSOC 事業本部、セキュアネットサービス事業並びにシステムインテグレーション事業が提供するサービスに付加して、官公庁・企業・団体等の顧客にセキュリティソリューションサービスを提供しています。

【JSOC について】

Japan Security Operation Center は、株式会社ラックの事業部門として運用しているセキュリティオペレーションセンターです。官公庁・企業・団体等の顧客に対して、24 時間 365 日、セキュリティ監視を実施し、種々のセキュリティ事件発生 of 早期検出や攻撃の防御を行い、顧客がセキュリティ事故や予兆に対して、いち早く対応を取れるように支援しています。

同社に関する詳しい情報は Web サイトでご参照頂けます。

< <http://www.lac.co.jp/> >

本ガイドラインに関するお問い合わせ先：

電子メール： jsoc-info@lac.co.jp

【ご注意】

株式会社ラックは、いかなる場合も、この情報の使用や配布により生じる損害について、直接及び間接を問わず責任を負いません。この文書に記載されている情報は予告なしに変更されることがあります。

【改版履歴】

2003 年 8 月 18 日 23:55	初版発行
2003 年 8 月 19 日 15:00	新種のワームの情報に伴い概要、対策を更新。 統計を最新版のデータに更新。 「補足」を追加。
2003 年 8 月 19 日 20:30	統計を最新版のデータに更新。TCP80 番ポートの傾向を追加。
2003 年 8 月 20 日 19:30	新種のワームの情報に伴い概要、対策を更新。
2003 年 8 月 22 日 20:30	統計を最新版のデータに更新。国別 ICMP 件数の統計を追加。