7月のインターネットセキュリティ脅威情報

情報提供：株式会社シマンテック

【 今月の概況 】

今月も注意すべき脆弱性がいくつも公開され、DeepSightの脅威警告が発行された。特にBlack-HatというイベントでCiscoのIOSの脆弱性についてはメディアでも大きく取り上げられて話題となった。先月に引き続きMytobワームファミリーの亜種が数多く発見され、日本ではトップ10に3つの亜種が報告された。また、今月の注目すべき悪意のあるコードとしてW32.Toxbot.C、および日本で作成されたと考えられるTorojan.Sacrepが発見された。さらに、今月はTPCのポート2100番と4321番への攻撃が活発であることがDeep-Sightで捕らえられた。このポートはともにOracle XDB FTPサーバーの悪用に関連している。

ランク	ワールドワイド	日本
1	Netsky.P	Netsky.P
2	Tooso.J	Mytob
3	Lineage	Rants.A
4	Desktophijack	Mytob.AW
5	Spybot	Redlof.A
6	Mytob.EE	Gaobot
7	Tooso.B	Webus.G
8	Gaobot	Sacrep
9	Fugif	Ahker.D
10	Bancos	Mytob.EE

表1：7月の悪意のあるコードのトップ10

【 新しく発見された主要な脆弱性 】

■ Cisco IOSでのIPv6の処理における任意のコード実行の脆弱性

Cisco IOSのIPv6の処理の機能にリモートから任意のコードを実行できる脆弱性が存在する。この問題の原因は現在不明。脆弱なバージョンのIOSを実行する装置が論理的・物理的なインターフェース上の同一セグメント上で捏造されたIPv6パケットを処理する場合にこの問題が発生する。

■複数のOracle製品の脆弱性に対するセキュリティアップデート

Oracle製品およびそのコンポーネントに複数の脆弱性が公開された。複数の脆弱性によりOracle Database Server、Oracle Enterprise Manager、Oracle Application Server、Oracle Collaboration Suite、Oracle E-Business SuiteとApplication、Oracle Workflow、Oracle FormsとReports、Oracle JInitiator、Oracle Developer Suite、Oracle Express Serverが影響を受けた。

■ Zlib圧縮ライブラリーのバッファオーバーフローの脆弱性

データ圧縮ライブラリーとして広く利用されているzlibにおいて、バッファオーバーフローを引き起こす可能性のある脆弱性が発見された。同ライブラリーの実装方法により影響は異なるが、リモートから任意のコードを実行されたり、DoS状態を引き起こされたりする可能性がある。

■ Windowsのカラー管理モジュールICCプロファイルにバッファオーバーフローの脆弱性

Windowsのカラー管理モジュールにバッファオーバーフローの脆弱性があることが報告されている。サポート対象となっているさまざまな画像およびドキュメント形式のICC（International Color Consortium）プロファイルタグを解析する際に、境界条件のエラーが原因で発生する。

■ Sophosアンチウイルスライブラリーの予期しないヒープオーバーフローの脆弱性

Sophosのアンチウイルスライブラリーに予期しないリモートヒープオーバーフローの脆弱性が存在する。この問題は内部メモリーバッファへデータをコピーする前にユーザーが入力したデータの適切な境界チェックを行わないために発生する。

■ MIT Kerberos 5 KRB5_Recvauthにおけるメモリー二重解放の脆弱性

MIT Kerberos5に含まれるkrb5_recvauth()関数はエラー処理のなかで、メモリーの二重解放をする可能性が存在する。結果として、リモートから任意のコードが実行される可能性がある。

■ Microsoft Wordのフォント処理におけるバッファオーバーフローの脆弱性

Microsoft Wordのフォント解析処理部分に未チェックバッファの脆弱性が存在する。異常に大きなフォント情報がWord文書に追加されていると、Wordがそれを解析する際にバッファオーバーフローを発生し、スタック領域が破壊される。この際、破壊されるスタックの値を適当に調整することで、任意のコードを実行できる可能性がある。

■ Mozilla Suite、FirefoxとThunderbirdに複数の脆弱性

Mozilla FoundationがMozilla Suite、FirefoxとThunderbirdに影響する12の脆弱性セキュリティアドバイザリーを公開した。この脆弱性を利用することで、リモートからMozilla, Firefox, Thunderbirdを実行しているユーザーの権限を取得される可能性がある。

■インターネットエクスプローラのJPEGイメージレンダリング処理にバッファオーバーフローの脆弱性

インターネットエクスプローラのJPEGイメージのレンダリング処理に脆弱性が発見された。この問題は固定サイズのメモリーバッファに入力データをコピーする前に適切な境界チェックを行っていないために引き起こされる。

【 新しく発見された主要なウイルス 】

■ W32.Toxbot.C

W32.Toxbot.C は侵入先のコンピュータに IRC バックドアを開いたり、脆弱性を悪用して拡散したりするワームで、以下の脆弱性を悪用する。

- UDP ポート 1433 を使用して、Microsoft SQL Server 2000 または MSDE 2000 audit の脆弱性（マイクロソフトセキュリティ情報 MS02-061 参照）
- Microsoft Windows DCOM RPC インターフェースバッファオーバーランの脆弱性（マイクロソフトセキュリティ情報 MS03-026 参照）
- Microsoft Windows Local Security Authority Service のリモートバッファオーバーフローの脆弱性（マイクロソフト セキュリティ情報 MS04-011 参照）
- VERITAS Backup Exec エージェントブラウザのリモートバッファオーバーフローの脆弱性

■ Trojan.Abwiz.C

Trojan.Abwiz.C はリモートファイルをダウンロードして実行したり、機密のシステム情報をリモートの攻撃者に送信したりするトロイの木馬である。この新しい亜種は短い間隔で自身を配布するサーバー上でポリモーフィック圧縮ユーティリティを使い、Abwiz.C を置き換えることにより、アンチウイルスのシグネチャによる検知を逃れるための比較的斬新な方法を使っている。

■ Trojan.Sacrep

Trojan.Sacrep はキーストロークを記録して盗んだ情報を前もって決められた電子メールアドレスへ送信するトロイの木馬で、日本ではトップ 10 の中にレポートされたが、他の国では報告されなかった。このトロイの木馬は日本語をファイル名に使用し、日本で作成されたと思われる。

■ W32.Mytob ファミリー

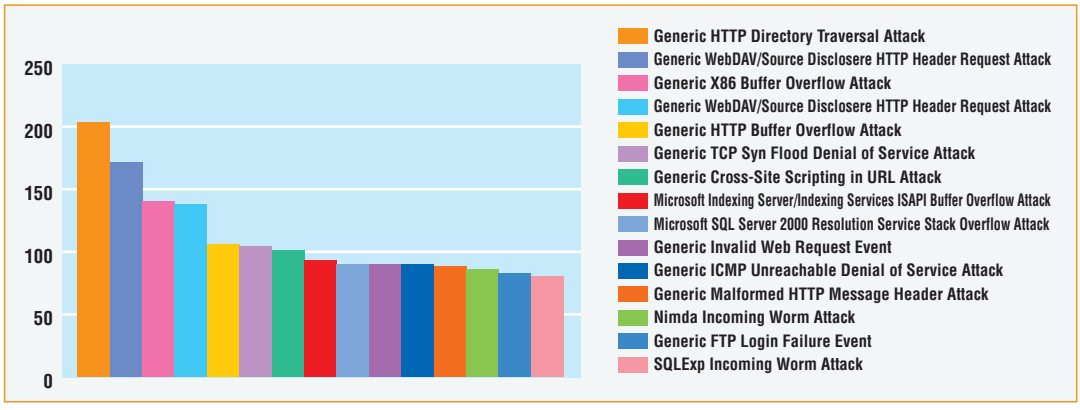
今月は非常に多くの Mytob の亜種が発見された。この Mytob ファミリーは現在、TMS によって非常に高い割合で検知されている。Mytob はマスメールワームで感染したコンピュータ上にバックドアを作成する。また、亜種のいくつかはターゲットコンピュータ上に存在するリモート攻撃可能な脆弱性によって感染する機能も持っている。

W32.Mytob.IM@mm、W32.Mytob.JF@mm、W32.Mytob.IK@mm、W32.Mytob.HU@mm、W32.Mytob.IH@mm、W32.Mytob.IG@mm、W32.Mytob.IV@mm、W32.Mytob.HM1@mm、W32.Mytob.HO@mm、W32.Mytob.IE@mm、W32.Mytob.DU@mm、W32.Mytob.ET1@mm、W32.Mytob.IM1@mm、W32.Mytob.IC@mm、W32.Mytob.IA@mm、W32.Mytob.HM@mm、W32.Mytob.ID@mm、W32.Mytob.IB@mm、W32.Mytob.HY@mm、W32.Mytob.DM@mm、W32.Mytob.DK@mm、W32.Mytob.HI@mm、W32.Mytob.HH@mm、W32.Mytob.HG@mm、W32.Mytob.HS@mm、W32.Mytob.GU@mm、W32.Mytob.GT@mm、W32.Mytob.GX@mm

【 今月のセンサーの状況 】

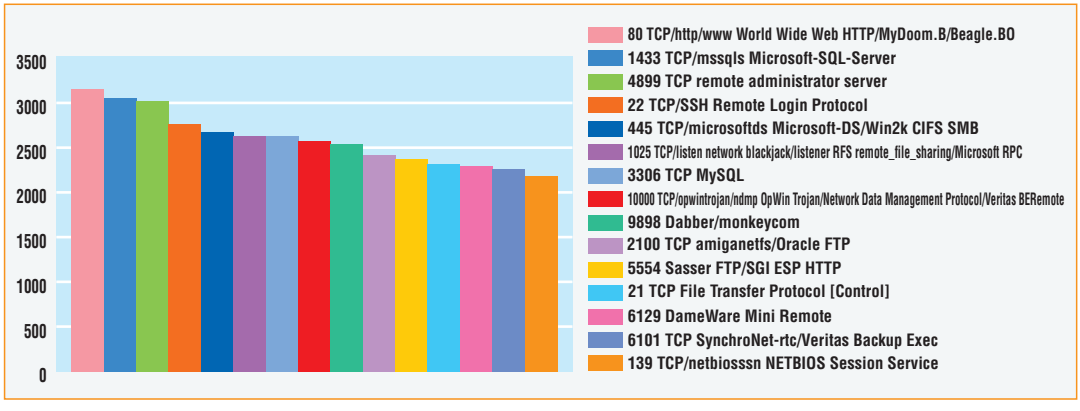
※センサーとは：インターネット上の不正な攻撃などの情報を提供する早期警告システム（Symantec DeepSight Threat Management System）。全世界 180 か国以上、19,000 ものパートナーのもとにあるファイアウォールや侵入検知システムより収集した攻撃のデータを収集、分析することで、最新の攻撃情報や、パッチの情報、その対処法などを素早く提供するもの。

グラフ 1：7 月の攻撃トップ 15（IDS）



7 月も IDS のセンサーでは多くのワームや攻撃で利用される Generic HTTP Directory Traversal Attack がトップに報告された。トップイベントに上がってくる攻撃の多くが、Web に関連する 80 番のポートに対する攻撃である。

グラフ 2：7 月の攻撃を受けたポートトップ 15（ファイアウォール）



Bot ネットワークが感染ホストを増やすための活発な活動が今月の Firewall センサーのトップ 15 に見られる。以前公開された悪用可能な脆弱性に対するサービスおよび以前のワームの感染により開けられたバックドアが頻繁に狙われている。これは攻撃者が可能な限り多くの感染したホストを集めようとしているためと思われる。

［インターネットマガジン　バックナンバーアーカイブ］ ご利用上の注意

このPDFファイルは、株式会社インプレスR&D（株式会社インプレスから分割）が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン　バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

http://i.impressRD.jp/bn

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真の撮影者、イラストの作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元（株式会社インプレスR&D）、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D（当時は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先
株式会社インプレスR&D
All-in-One INTERNET magazine 編集部
im-info@impress.co.jp