6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 】

悪用コードも公開されるいくつかの重要なセキュリティの脆弱性が公開された。主な脆弱性は、WindowsのHTMLヘルプのリモートコード実行の脆弱性、Outlook ExpressのNNTP応答解析機能のバッファオーバーフローの脆弱性、Internet ExplorerのPNGイメージレンダリングのメモリ破損の脆弱性、VERITAS Backup Execの複数の脆弱性である。悪意のあるコードでは、MytobとKelvirワームファミリーの多くの亜種が発見された。VERITASのBackup Execの脆弱性に関連するTCPのポート6101とポート10000への高い攻撃活動がDeepSightのセンサーにより検出され、警告が出された。

ランク	ワールドワイド	日本
1	Tooso.B	Netsky.P
2	Netsky.P	Tooso.B
3	Spybot	Redlof
4	Tooso.F	Mydoom.BU
5	Mytob.CU	Gaobot
6	Gaobot	Tooso.F
7	Lineage	Hybris
8	Lemir	Bugbear.B
9	Tooso.I	Mytob.EE
10	Redlof	Funlove

表1：6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 】

■ Sun Java Web Startとランタイム環境に許可されない権限昇格の脆弱性

信頼されないJavaアプリケーションの権限をリモートから昇格させられる。これにより、悪意のある第三者にローカルのファイルを読み書きされたり、任意のローカルのアプリケーションを実行されたりする可能性がある。

■ Internet ExplorerのPNGイメージレンダリングメモリー破壊の脆弱性

ブラウザーにより使用されているPNGのイメージレンダリングライブラリーに存在する。攻撃者はプログラムの実行フローに影響を与えて、プログラムのコントロール変数を上書きできる。

■ Windowsヘルプのリモートコード実行の脆弱性

HTMLヘルプにリモートでコードが実行される脆弱性が存在し、コンピュータを制御される。

■ Outlook Expressの NNTP応答解析機能のバッファオーバーフローの脆弱性

Outlook Expressがニュースグループリーダーとして使用される場合、リモートでコードが実行される脆弱性が存在する。攻撃者は、悪質なニュースグループサーバーを作成し、ユーザーがサーバーにニュースをクエリーした場合、リモートでコードを実行できる。

■ Windows Web Clientサービスのリモートコード実行の脆弱性

WindowsがWeb Clientリクエストを処理する方法にリモートでコードが実行される脆弱性が存在する。攻撃者がこの脆弱性を悪用した場合、影響を受けるコンピュータが完全に制御される。

■受信SMBパケットの検証にリモートバッファオーバーフローの脆弱性

ユーザーから提供されたデータに対してSMBによる境界チェックが適切に行われないため、容量の不十分なメモリーバッファー上にコピーが行われてしまうことが原因。脆弱なコードを含むカーネルのコンテキストでリモートから任意のマシンコードを実行できる。

■ VERITAS Backup Exec Web管理コンソールリモートバッファオーバーフローの脆弱性

■ VERITAS Backup Execサーバーリモートレジストリアクセスの脆弱性

■ VERITAS Backup Exec Admin Plus Packオプションリモートヒープオーバーフローの脆弱性

■ VERITAS Backup Execリモートエージェントヌルポインター Dereference演算子のDoSの脆弱性

■ VERITAS Backup Execリモートエージェントのバッファオーバーフローの脆弱性

6月22日VERITASのBackup Execに複数の脆弱性が公開された。それらの脆弱性はリモートからのDoS攻撃からリモートでのコードの実行を可能とする多くの影響を持っている。この問題は特にWindowsサーバーとNetWareサーバーのBackup Execのリリース9.0,9.1と10.0に存在する。

■ RealPlayerのRealTextの解析でのヒープオーバーフローの脆弱性

RealPlayerにRealTextファイルの解析を悪用してリモートから悪質なコードを挿入および実行できる脆弱性が発見された。特別なRealTextファイルを作成し、そのファイルを脆弱性があるRealPlayerで開くようにユーザーを誘導し、任意のコードを実行できる。

■ Internet Explorer Javaprxy.DLLというCOMオブジェクトの例示化ヒープオーバーフローの脆弱性

javaprxy.dllというCOMオブジェクトが悪意のあるWebページによってインスタンスされることによって引き起こされる。この問題はクライアントの実行権限で任意のコードを実行させるために悪用される可能性がある。現在、この問題を取り除くパッチは提供されていない。DeepSight脅威分析チームはこの脆弱性に対する悪用コードの公開を確認している。

インターネットマガジン／株式会社インプレスR&D
©1994-2007 Impress R&D

【 新しく発見された主要なウイルス 】

■ Backdoor.Sdbot.ZM
Windows プラットフォーム用のバックドアトロイの木馬機能があるネットワーク感染型ワームである。W32/Sdbot-ZM は事前に設定されたIRCチャンネルに接続し、リモートユーザーからのコマンドをさらに待機する。ワームは下記のようなオペレーティングシステムの脆弱性を悪用し、セキュリティレベルの低いパスワードのあるネットワーク共有フォルダーや SQL サーバーを経由して蔓延する。
Windows LSASS バッファオーバーランの脆弱性／Windows DCOM RPC の脆弱性／SQL Server 2000 解決サービスのヒープオーバーフローの脆弱性

■ SymbOS.Fontal.B
システムファイルを置き換えて、侵入先のデバイスを無効にするトロイの木馬である。このトロイの木馬は Nokia の Series60 の携帯電話で使われている SymbianOS 上で動作する。

■ W32.Kelvir.CB

■ W32.Kelvir.DQ

■ W32.Kelvir.DR

■ W32.Kelvir.DT

■ W32.Kelvir.DU
MSN メッセンジャーを介して拡散するワームである Kelvir ファミリーの亜種がほとんど毎日のように現れた。

■ W32.Mytob.GG@mm

■ W32.Mytob.GJ@mm

■ W32.Mytob.GK@mm

■ W32.Mytob.GM@mm

■ W32.Mytob.GN@mm

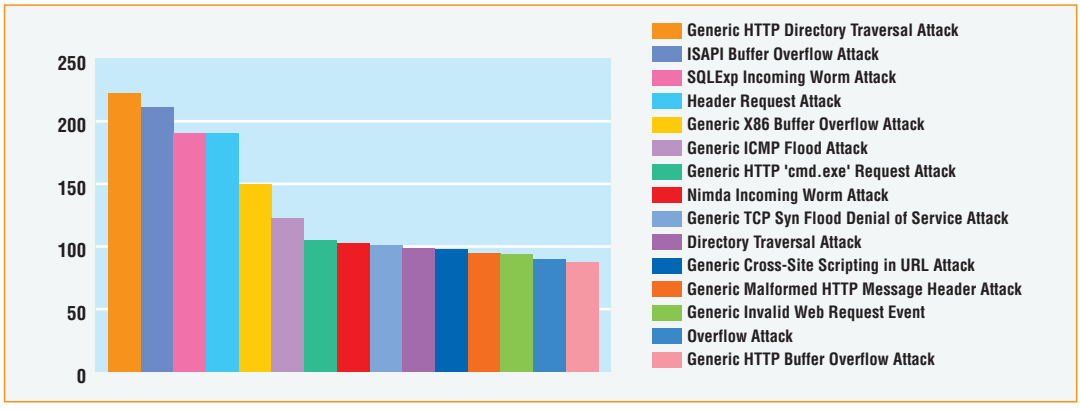
■ W32.Mytob.GP@mmA
別の亜種が多く生まれているワームとして、Mytob がネットワーク上で感染を広げた。Mytob はバックドアを開いたり、侵入先のコンピュータのセキュリティ設定を低下させたりする大量メール送信ワームである。

■ W32.Toxbot.C
VERITAS の Backup Exec リモートエージェントの Windows サーバーの認証のバッファオーバーフローの脆弱性（BID 14022）を悪用して感染を広げるワームである。DeepSight 脅威分析チームは DeepSight のハニーポットにてこのワームを最初に捕らえて分析した。

【 今月のセンサーの状況 】

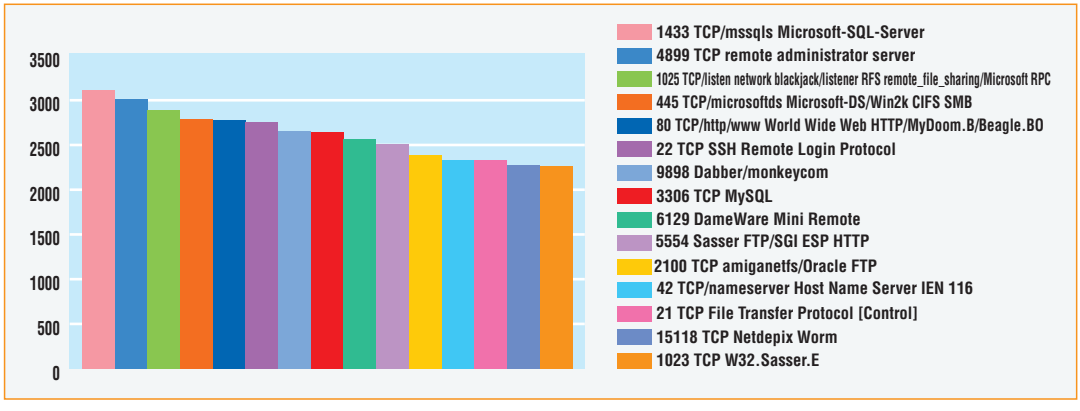
※センサーとは：インターネット上の不正な攻撃などの情報を提供する早期警告システム（Symantec DeepSight Threat Management System）。全世界 180 か国以上、19,000 ものパートナーのもとにあるファイアウォールや侵入検知システムより収集した攻撃のデータを収集、分析することで、最新の攻撃情報や、パッチの情報、その対処法などを素早く提供するもの。

グラフ 1：6 月の攻撃トップ 15（IDS）



6 月の 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。この攻撃は Web サービスで読み込み可能な任意のファイルや Web ルートの外にアクセスしようとするために作成された URL で検知される。そのほかにも攻撃のトップの多くは Web ベースの攻撃である。

グラフ 2：5 月の攻撃を受けたポートトップ 15（ファイアウォール）



ファイアウォールのセンサーではトップ 15 には入っていないが、6 月 22 日に公開された VERITAS の Backup Exec の脆弱性に関連する TCP のポート 10000 に対する攻撃が 6 月 24 日の悪用コードの公開に続き、6 月 25 日から急増したのを観測した。また、この脆弱性を狙ったワーム W32.Toxbot.C も現れた。

インターネットマガジン／株式会社インプレスR&D
©1994-2007 Impress R&D

［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

Copyright © 1994-2007 Impress R&D, an Impress Group company. All rights reserved.