II月のインターネットセキュリティ脅威情報 ［最終回］

情報提供：株式会社シマンテック

【今月の概況】

今月は影響度の大きな脆弱性としてアンチウイルスのスキャンエンジン、バックアップ製品の脆弱性および、多くのIPSec VPN製品に影響がするIKEの脆弱性を含む6つの脆弱性が公開された。

また、以前DoSの可能性を指摘されたPerlインタープリターのフォーマットストリングにおける脆弱性に新たに任意のコードの実行の可能性が指摘された。

今月、日本ではトロイの木馬であるLodear.B,C,Dが3位、4位、5位に報告された。Loaderは自身での拡散の機能は持っていないが、SPAMによって配布されていることが確認されている。

ランク	ワールドワイド	日本
1	Sober.X	Netsky.P
2	Mytob.KU	Redlof.A
3	Netsky.P	Lodear.B
4	Lodear.B	Lodear.D
5	Netsky.Z	Lodear.C
6	Mytob.DF	Hybris
7	Mytob.DF	Fanbot.A
8	Spybot	Pinfi
9	Vundo	Spybot
10	Lodear	Licum

表1：11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】

■＜Mac OS X Security Update 2005-10-31＞複数のローカルな脆弱性

アップルはMac OS Xの下記の複数のローカルで影響する脆弱性に対するSecurity Update 2005-10-31をリリースした。

・ファイルの所有権情報が不正確な場合がある。
・重要なソフトウェアアップデートがインストールされない場合がある。
・グループメンバーシップへの変更が数時間遅れる。
・「キーチェーンアクセス」がロックのタイムアウト後に、引き続き標準テキストのパスワードを表示する。
・カーネルメモリーがローカルユーザーに漏洩する場合がある。

■＜F-Prot＞アンチウイルスのスキャンニングエンジンのZIPファイルの迂回の脆弱性

F-Prot Anti-Virusのいくつかのバージョンで、ZIP添付ファイルの処理において、アンチウイルスのスキャンニングを迂回できる脆弱性が報告された。

■＜Microsoft Windows＞グラフィックレンダリングエンジンにWMF/EMFフォーマットコード実行の脆弱性

Microsoft WindowsのWMH/EMFグラフィックレンダリングエンジンにリモートでコードが実行される脆弱性が公開された。この問題はユーザーが悪質なWMFやEMF形式のファイルを表示したときに影響を受けるエンジンでファイルの解析が開始された場合に発生する。この問題が発生すると整数オーバーフローが起こり、ヒープメモリーが破壊され、任意のコードが実行される可能性がある。実行されるコードには影響を受けるエンジンの特性に基づきSYSTEM権限が付与される。この脆弱性を悪用した攻撃が成功すると、リモートからのシステム侵害やローカル権限の昇格が発生する場合がある。

■＜VERITAS NetBackup 5.x＞Volume Manager Daemonが使用する共有ライブラリーにバッファオーバーフローの脆弱性

VERITAS NetBackup 5.xサーバーで実行されるVERITAS NetBackup vmd（Volume Manager Daemon）およびクライアントが使用する共有ライブラリーにバッファオーバーフローの脆弱性が公開された。悪質な攻撃者がこのオーバーフローの条件を悪用すると、サービス拒否によるバックアップシステムの障害が発生したり、標的のシステム上で昇格された権限により任意のコードが実行されたりする可能性がある。

■＜Microsoft Internet Explorer＞JavaScript onLoad Handlerリモートコード実行の脆弱性

MicrosoftのInternet Explorerにリモートでコードを実行可能な脆弱性の影響を受けることが報告された。この脆弱性はブラウザーがJavaScriptのonLoadのイベントを処理するときにwindows()JapaScriptの関数を正しく初期化しないことにより引き起こされる。この脆弱性は以前のバージョンのIEで指摘されたが、IE6のSP2においても影響があると報告されている。

■＜PHP＞XML-RPCを使ったリモートコードの挿入の脆弱性

PHPのXML-RPCがリモートでコード挿入の脆弱性の影響を受ける。攻撃者はウェブサーバーの権限で任意のコマンドやコードを実行できる可能性がある。この問題はPHP1.1とそれ以前のバージョンのXML-RPCが影響を受け、このライブラリーを使用するアプリケーションもまたこの脆弱性の影響を受ける。

■＜Sun＞Javaランタイム環境の複数の権限昇格の脆弱性

SunのJREにいくつかの権限昇格の脆弱性が公開された。これらの問題はリモートJavaアプリケーションにローカルなファイルの読み書きや実行環境の権限で任意のアプリケーションを実行が可能。

■＜Perl＞Perl_sv_vcatpvfnのフォーマットストリングの整数の桁あふれの脆弱性

Perlはperl_sv_vcatpvfn ()機能に細工されたフォーマットストリングを送信されることが原因でDoS攻撃を引き起こされるセキュリティホールが存在する。この問題が悪用されるとリモートの攻撃者にシステム上で任意のコードを実行される可能性がある。

【 新しく発見された主要なウイルス 】

■ Trojan.DNSChanger.B
Paypalからの送信を装い感染させようとする。感染するとフィッシングに利用するためDNSを193.227.227.218に振り向ける。

■ Linux.Plupii
下記のウェブサーバー関連の脆弱性を悪用することで拡散するバックドア機能を備えたワーム。
・XML-RPCによるPHPのリモート挿入の脆弱性
・AWStats Rawlog Plugin Logfileパラメーター入力検証の脆弱性
・Darryl Burgdorf Webhintsリモートコマンド実行の脆弱性

■ W32.Mytob.LM@mm、W32.Mytob.FF@mm、W32.Mytob.LO@mm、W32.Mytob.FI1@mm、W32.Mytob.ML@mm、W32.Mytob.MO@mm、W32.Mytob.MQ、W32.Mytob.LZ@mm、W32.Mytob.FR@mm、W32.Mytob.MC@mm、W32.Mytob.ME@mm、W32.Mytob.FO1@mm、W32.Mytob.FV1@mm、W32.Mytob.FX1@mm、W32.Mytob.MX、W32.Mytob.DO1
Mytobの作者のDiabl0の逮捕にもかかわらず、Mytobの新しい亜種が毎日のように報告された。Mytobのソースコードがアンダーグラウンドで出回っているためと思われる。

■ Backdoor.Ryknos、Backdoor.Rayknos.B
標的のコンピューター上で自分自身を隠すために SecurityRisk.First4DRM セキュリティリスクを悪用しようとするトロイの木馬。

■ Trojan.Heoms
IEで訪れられる URL を監視し、この情報をリモートのウェブサイトへ送信するトロイの木馬。

■ W32.Sober.S@mm、W32.Sober.T@mm、W32.Sober.T@mm、W32.Sober.V@mm、W32.Sober.W@mm、W32.Sober.X1@mm、W32.Sober.AE1@mm
大量メール送信型のワームである Soberの亜種の大規模な感染が報告された。

■ SymbOS.Pbstealer.A
Nokia Series 60 携帯電話のOSとして使用される Symbian OS 上で実行されるトロイの木馬。ユーザーのコンタクト情報データベースを他の Bluetooth デバイスへ送信する。

■ SymbOS.Cardtrap.H
Nokia Series 60 の携帯電話のOSに各種の脅威を与えるトロイの木馬。

■ W32.Yimper
AOLメッセンジャーと Yahoo!メッセンジャーで拡散するワーム。有害なウェブサイトへのリンクを含むメッセージを送信して拡散する。

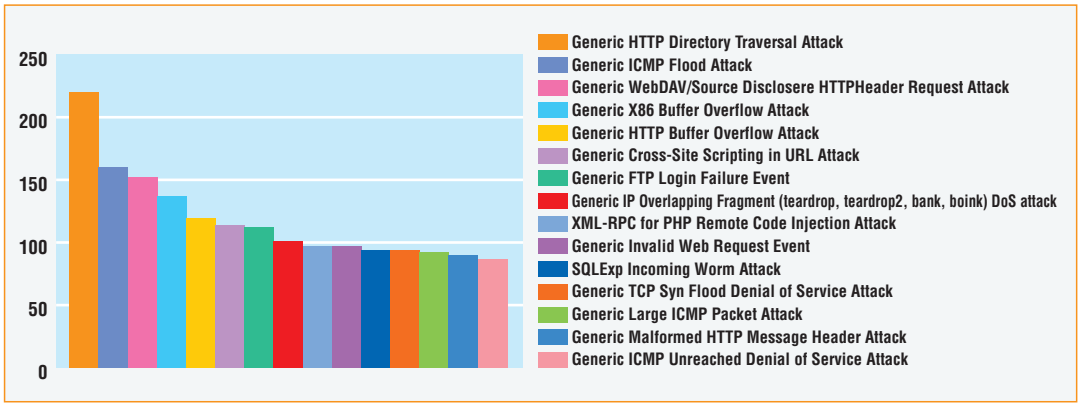
■ W32.Gudeb
標的のコンピューターのセキュリティ設定を低下させ、フォルダを隠すワーム。FTP を介して拡散する。

■ Trojan.Hanmon
複数の Windows プロセス内に有害なコードを挿入するトロイの木馬。

【 今月のセンサーの状況 】

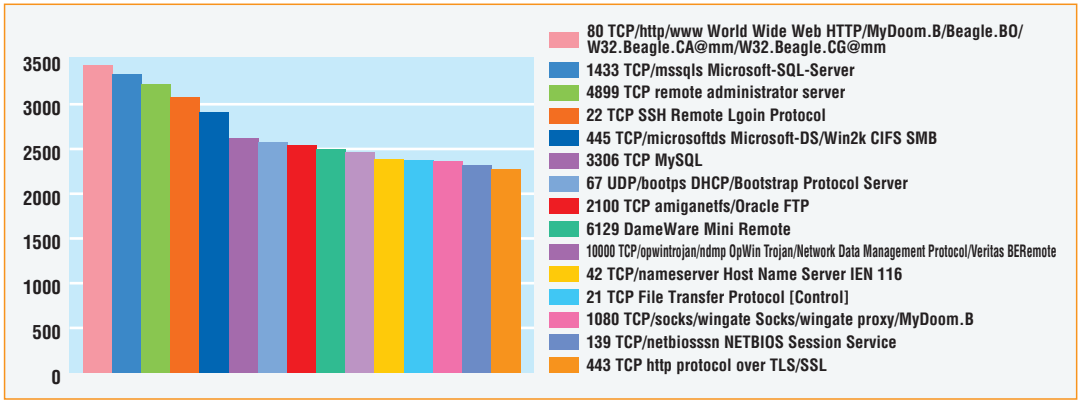
※センサーとは：インターネット上の不正な攻撃などの情報を提供する早期警告システム（Symantec DeepSight Threat Management System）。全世界180か国以上、19,000ものパートナーのもとにあるファイアウォールや侵入検知システムより収集した攻撃のデータを収集、分析することで、最新の攻撃情報や、パッチの情報、その対処法などを素早く提供するもの。

グラフ1：11月の攻撃トップ15（IDS）



11月もIDSのセンサーで検知された攻撃の主なものは古くからのワームであるCodeRed、Nimda、SQLExp（Slammer）による攻撃であった。PHPのXML-RPCの脆弱性を狙うワームLinux.Plupiiによる攻撃と思われる攻撃が第9位に位置した。

グラフ2：11月の攻撃を受けたポートトップ15（Firewall）



HTTP、FTP、SSHのようなインターネット上でよく利用されているサービスを対象にしたトラフィックの他に、自己感染を行うワームのトラフィックの影響が反映されている。たとえばMicrosoft SQL ServerやMySQL、Oracleデータベース、VeritasのBackupExecに関連したトラフィックも含まれている。

［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