5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 】

重大な脆弱性がMozillaベースのブラウザとGDB、OllyDbgデバッガー、およびいくつかのウイルススキャナーで利用されているコンピュータアソシエイツ社のVetライブラリーに発見された。また、特定の状況下でリモートでのコードの実行を許すQmailの脆弱性が複数発見された。

悪意のあるコードの報告件数のトップ10についてはワールドワイドではSober.Oが一位だが、日本では流行しなかった。

新規に発見されたウイルス、ワームとしては感染すると重要なファイルを暗号化して人質にとり、金銭をゆすり取る目的で作成されたTrojan.Gpcoderというトロイの木馬プログラムが注目を集めた。

ランク	ワールドワイド	日本
1	Sober.O	Netsky.P
2	Tooso.F	Redlof.A
3	Netsky.P	Gaobot
4	Vundo.B	Mydoom.BO
5	Gaobot	Tooso.F
6	Spybot	Pinfi
7	Lemir	Jasbom
8	Redlof.A	Spybot
9	KillAV	Bugbear.B
10	Linege	Hybris

表1：5月の悪意のあるコードのトップ10と新たに発見された主要な悪意のあるコードの情報トップ10

【 新しく発見された主要な脆弱性 】

■Apple社のMac OS X NetInfoセットアップツールのローカルバッファオーバーフローの脆弱性
http://online.securityfocus.com/bid/13486

NeSTツールは、コマンドライン引数の処理において、ローカルバッファオーバーフローの脆弱性を持っている。これは、攻撃者が任意のコードを実行するのを許す可能性がある。

■Apple社Mac OS X VPNDローカルバッファオーバーフローの脆弱性
http://online.securityfocus.com/bid/13488

vpndはコマンドラインの“－iオプション”に任意のコードの実行を許す脆弱性を持っている。攻撃者はこの脆弱性を利用して、ルート特権を取得できる。

■Etherealの複数のリモートプロトコルディセクターへの脆弱性
http://online.securityfocus.com/bid/13504

Etherealの複数のリモートプロトコルディセクターに下記のような脆弱性が発見された。
・バッファオーバーフローの脆弱性
・フォーマット文字列の脆弱性
・ヌルポインタ参照値読み出しのDoSの脆弱性
・セグメンテーション違反のDoSの脆弱性
・無限ループのDoSの脆弱性
・メモリー枯渇のDoSの脆弱性
・メモリーの2度の開放の脆弱性
・予期せぬDoSの脆弱性

攻撃者はEtherealの実行権限で任意のコードを実行またはクラッシュさせられる。

■Oracle 10d DBMS_Scheduler権限昇格の脆弱性
http://online.securityfocus.com/bid/13509

■Oracle9i/10gデータベースのファイングレイン監査ロギング失敗の脆弱性
http://online.securityfocus.com/bid/13510

2005年5月5日にAlexander KornbrustがOracleのデータベースの複数のバージョンに影響する2つの脆弱性の詳細を公開した。最初の脆弱性はファイングレイン監査機能を意図せずに無効にできるものだ。2番目の脆弱性は攻撃者が権限を昇格できる脆弱性で、“creat job”権限のユーザーが“session_user”を“SYS”へ変更できる。

■Qmail Alloc()関数リモート整数オーバーフローの脆弱性
http://online.securityfocus.com/bid/13528

■Qmail Commands()関数リモート整数オーバーフローの脆弱性
http://online.securityfocus.com/bid/13535

■Mozilla Firefoxインストールメソッドにおけるリモートでの任意のコード実行の脆弱性
http://online.securityfocus.com/bid/13544

2005年5月7日にBugtraqのメーリングリストにFirefoxの新しい脆弱性がアナウンスされた。攻撃者はこの脆弱性を利用して、Firefoxが動作している権限で任意のコードを実行が可能。

■マイクロソフトSQL Server 2000の複数の脆弱性
http://online.securityfocus.com/bid/13564

マイクロソフト社が複数の脆弱性に対応したSQL Server 2000のSP4を提供を開始した。攻撃者はこの脆弱性を利用して、DoS攻撃、データベースのポリシーをバイパス、重要な情報の盗み出し、任意のコードの実行が可能である。

■複数のベンダーのTCPのPAWSのtimestampにリモートのDoSの脆弱性
http://online.securityfocus.com/bid/13676

TCPのtime-stampオプションは、高速な通信のためにパケットごとのタイムスタンプを提供する機能で、広く利用されている。このTCPの一部の実装において、DoS攻撃が可能となる脆弱性が確認されている。

この脆弱性により、リモートの第三者がTCPコネクションの内部タイマーの値を任意に設定でき、Protect Against Wrapped Sequences（PAWS）機能を利用している場合にDoSが発生する可能性がある。

【 新しく発見された主要なウイルス 】

■ W32.Sober.O@mm

http://www.symantec.co.jp/region/jp/avcenter/venc/data/jp-w32.sober.o@mm.html

W32.Sober.O@mmは、侵入先のコンピュータから収集したメールアドレスに対して、自分自身を添付ファイルとして送信する大量メール送信型ワームである。このワームは拡散するため独自のSMTPエンジンを使用する。メールは英語、またはドイツ語で記述される可能性がある。W32.Sober.O@mmはシマンテックセキュリティレスポンスに危険度3として警告された。

■ PWSteal.Bancos.U

http://www.symantec.co.jp/region/jp/avcenter/venc/data/jp-pwsteal.bancos.u.html

PWSteal.Bancos.Uはキーストロークを記録して、特定の銀行のウェブサイトに入力された情報を盗み取るパスワード盗用型のトロイの木馬である。また、特定の銀行のウェブページのスクリーンショットを撮影することにより、パスワード等の機密情報を収集しようとする。

■ W32.Drivus.A

http://www.symantec.co.jp/region/jp/avcenter/venc/data/jp-w32.drivus.a.html

W32.Drivus.Aは共有フォルダを介して拡散し、Trojan.Drivusの亜種を投下するワームである。%Windir%フォルダにSharedDocsという共有フォルダを作成し、自身とTrojan.Drivusをコピーする。このフォルダは“MyShare”として共有され、ネットワーク共有のコメント行には“Share Dir”というコメントが表示される。Trojan.Drivusはルートキットの機能を備えたバックドアトロイの木馬である。

■ W32.Yami.A

W32.Yami.AはWindows XPのWindows Portable Executable(PE)ファイルに感染するファイル感染型ウイルスである。カーネルメモリーに自分自身を挿入し、ファイルアクティビティを監視する。このウイルスはスラックスペースを使用して、実行可能ファイルに感染する。そのため、感染したファイルのサイズは増加しない。

■ Trojan.Gpcoder

http://www.symantec.co.jp/region/jp/avcenter/venc/data/jp-trojan.gpcoder.html

2005年5月22日に発見され、感染したユーザーから金銭をゆする目的で作成されている。Trojan.Gpcoderは様々な拡張子が付いているファイルを探し出して、暗号化するトロイの木馬である。その後、オリジナルファイルは削除される。暗号化されたファイルは判読できない。

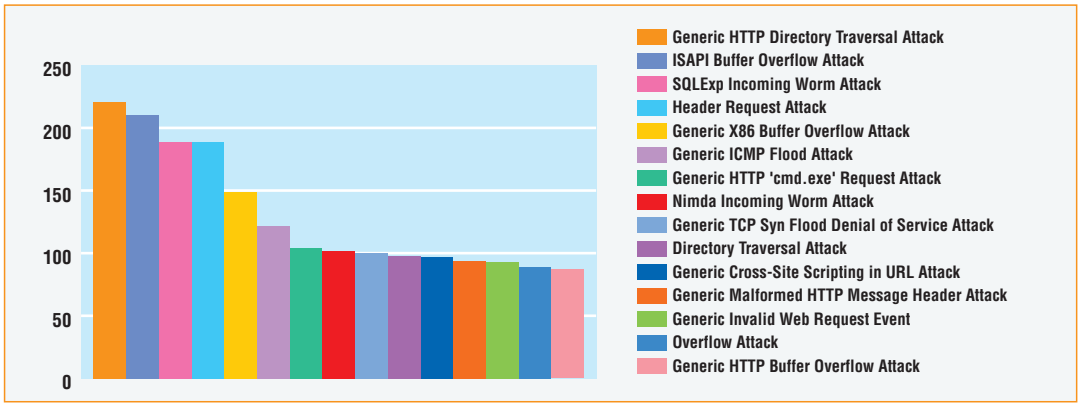
■ Java.Nastybrew.A

Java.Nastybrew.AはJava.Nastybrew.Aはインターネットからファイルをダウンロードしようと試み、Java .class ファイルに感染するウイルスだ。

【 今月のセンサーの状況 】

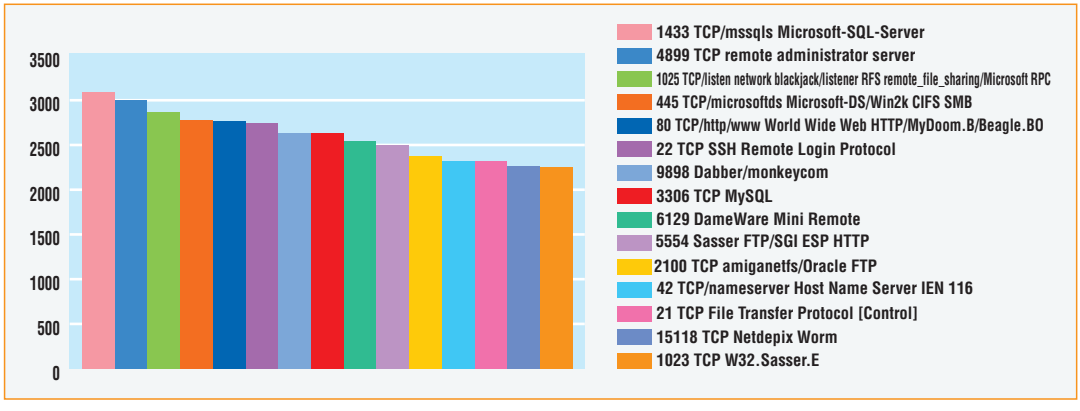
※センサーとは：インターネット上の不正な攻撃などの情報を提供する早期警告システム（Symantec DeepSight Threat Management System）。全世界180か国以上、19,000ものパートナーのもとにあるファイアウォールや侵入検知システムより収集した攻撃のデータを収集、分析することで、最新の攻撃情報や、パッチの情報、その対処法などを素早く提供するもの。

グラフ1：5月の攻撃トップ15（IDS）



5月の攻撃トップ15としては、ウェブサーバーのWebのルートディレクトリーを飛び越えて、不正にファイルにアクセスするための汎用HTTPディレクトリートラバーサル攻撃がトップとなった。

グラフ2：5月の攻撃を受けたポートトップ15（Firewall）



5月の攻撃を受けたポートトップ15からは、ボット感染PCのボットネットワーク拡大のための攻撃が行われていることが推測される。

［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