2005年上半期

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

今回のインターネットセキュリティ脅威レポートでは2005年1月から6月までのセキュリティ情報をまとめ、脅威の傾向を分析する。毎月のレポートだけでは分からない脅威の傾向を知ることができるだろう。

【2005年上半期の傾向】

この半年で、これまでと違う脅威の傾向が見られた。攻撃者はネットワーク境界部に対する大規模な多目的攻撃から離れ、より小規模で対象を絞り込んだクライアントサイドへの攻撃にシフトしてきている。

今後の脅威環境はボットネットワーク、カスタマイズ可能なモジュール式の悪意のあるコード、Webアプリケーションや Webブラウザーを狙った攻撃など、新種の脅威が大半を占めるようになるだろう。また従来の攻撃は好奇心や自分の技能を見せたいという顕示欲を動機としていたのに対し、現在の脅威は金銭を得ることを動機としたものやID盗用、恐喝、詐欺などといった犯罪行為が多くなっている。

悪意のあるコードについて、報告件数トップ50のうち64%はスパムの中継を行うものだった。また新種のトロイの木馬で、ユーザーのWebブラウザー内にポップアップ広告を表示するアドウェアをダウンロードして、インストールするものも発見された。さらに、ボットネットワークやカスタムボットコードが販売されたり、レンタルで提供されたりしている。2005年上半期、前期に比べて100%の増加となる1日平均10,352台の有効なボットネットワークコンピュータを観察した。これはセキュリティ上、重大な脅威だ。金銭的な利得が大きくなるにつれて、さらに高度で発見されにくく、ウィルス対策や、ファイアウォールなどのセキュリティ手段を停止させる悪意のあるコードが開発されると考えておくべきだろう。

金銭目的の悪意のあるコードのほか、悪意のあるコードの亜種、および秘密情報を公開する悪意のあるコードの増加がみられる。2005年上半期に記録した新種のWin32対応ウィルス／ワームの亜種は10,866種を超えた。これは2004年下半期の7,360種に比べて48%の増加、2004年上半期の4,496種から142%の増加である。Win32対応ウィルス／ワームの亜種が増えている理由の1つはボットの亜種が増加しているためで、危険度3や4（深刻度が中から高）の脅威が大きく減り、その分、危険度1や2（深刻度が非常に小、あるいは小）の脅威が増えている。

攻撃者が小型でモジュール式構造の悪意のあるコード（ダウンロードによってさらに危険な機能を追加するコード）にシフトしていくにつれて、重大な侵入の危険性が高まっている。今期、悪意のあるコードの報告件数上位50のうち、秘密情報を暴いてしまう能力のあるものは74%を占めており、その暴かれた情報はID盗用、クレジットカード詐欺など違法な金銭的活動に利用できる。

この6か月間、フィッシング攻撃の増加が続いているが、より小規模で、特定地域を標的にする傾向が強まっている。フィッシングメールの数は1日平均299万通から570万通まで増加した。またSymantec Brightmail AntiSpamソ

2005年上半期の順位	2004年下半期の順位	攻撃	2005年上半期の攻撃の中の割合	2004年下半期の攻撃の中の割合
1	1	Microsoft SQL Server Resolution Service Stack Overflow Attack	0.33	0.22
2	14	Muhammad A. Muquit Count.cgi Attack	0.07	0.01
3	41	Generic HTTP Chunked Encoding Overflow Attack	0.04	<1%
4	11	Generic HTTP Directory Traversal Attack	0.04	0.02
5	44	Debian Linux HTTPD Attack	0.04	<1%
6	8	Generic WebDAV/Source Disclosure HTTP Header Request Attack	0.03	0.02
7	12	Generic X86 Buffer Overflow (TCP NOPS) Attack	0.03	0.02
8	16	Generic SMTP Pipe Attack	0.03	0.01
9	3	Microsoft Windows DCOM RPC Interface Buffer Overrun Attack	0.03	0.07
10	101	Microsoft RPCSS DCOM Interface	0.02	<1%

表1　攻撃のトップ10（2005年1月～6月）

順位	名称	タイプ	感染手段
1	Netsky.P	Worm	SMTP, P2P
2	Gaobot	Bot	CIFS, Remotely Exploitable Vulnerability, Back doors
3	Spybot	Bot	CIFS, Remotely Exploitable Vulnerability, Back doors
4	Tooso.F	Trojan	NA
5	Tooso.B	Trojan	NA
6	Redlof.A	Virus	Email
7	Lemir	Trojan	NA
8	Lineage	Trojan	NA
9	Sober.O	Worm	SMTP
10	KillAV	Trojan	NA

表2　2005年上半期、世界の悪意のあるコード報告件数トップ10

リューションがスキャンしたメールのうち、フィッシングの試みは125通に1通の割合で、前期に比べ100%増加している。

2005年上半期に記録した新たな脆弱性は1,862件あった。これは週72件、つまり1日あたり10件強の新しい脆弱性が発見されたということになる。そのうち97%が深刻度「中」または「高」、つまり悪用が成功した場合、システムの全部または一部に侵入される可能性があるものである。また、73%が脆弱性の悪用が容易なもの、つまり悪用に特別なコードが不要、もしくはコードが公表されているものだった。さらに問題を複雑にしているのは記録された脆弱性の84%がリモートからの悪用が可能なため、被害を与えうる攻撃者の数を増加させる可能性がある。

2005年上半期に記録された脆弱性のうち、約59%がWebアプリケーションに関連する脆弱性で、前期から59%、前々期から109%の増加だった。

新たに発見される脆弱性に対して企業のパッチ適用状況について、いくつかの傾向を観察した。2005年上半期の間、脆弱性の公表からその脆弱性に関連する悪用コードの出現までの期間は平均6日だった。これに対して、ベンダーが確認した脆弱性の公表から対応パッチのリリースまでの期間は平均54日だった。つまり、法人／個人ユーザーが攻撃の可能性にさらされている期間が約48日間あるということである。つまり、パッチはできる限り早く施すべきだということだ。

今回のインターネットセキュリティ脅威レポートの内容をいち早くお知らせするために、以下に一部の内容を抜粋しました。詳細については、インターネットセキュリティ脅威レポートVolume 8内で説明されています。

http://ses.symantec.com/WP000I

【攻撃の傾向】

- 4期連続で最も攻撃回数が多かったのは攻撃者の33%が使用していたMicrosoft SQL Server Resolution Service Stack Overflow Attack（Slammer Attackとしても知られている）だった。
- ファイアウォールと侵入検知のデータを合わせて、1日平均の攻撃回数は57回、前年同期に比べて21回減っている。
- 既知のボットネットワークコンピュータの数は1日平均10,352台で、前年同期の4,348台から増加した。
- DoS攻撃は2005年1月1日から6月30日までの期間に、1日119回から927回まで増加した。これは前年同期に比べて680%の増加である。
- ボット感染コンピュータの割合が一番高いのは前期と同じくイギリスで32%だった。前年同期の25%から増加している。
- 攻撃発信元国の第1位はアメリカで33%、前期の30%から増加している。続いて、ドイツとイギリスがいずれも7%となっている。
- 攻撃が最も多かった業界は教育機関で、続いて小規模企業、金融サービスの順だった。

【脆弱性の傾向】

- 脆弱性の公表からそれを悪用するコード出現までの間隔は前期の6.4日から、平均6.0日と短くなっている。
- また、脆弱性の出現からベンダーが対応パッチをリリースするまでの日数は平均54日だった。
- 2005年上半期に1,862種の脆弱性を新たに記録した。これは前期に比べて31%の増加である。
- 2005年上半期に記録された脆弱性のうち、Webアプリケーションに関連する脆弱性は約59%だった。前期から59%の増加、前々期からは109%の増加である。
- 脆弱性の97%が、深刻度「中」または「高」だった。
- 2005年上半期、Mozilla系ブラウザーに関連して記録された脆弱性は25種、そのうち72%にあたる18種が深刻度「高」だった。Microsoft Internet Explorerについてはベンダーで確認した脆弱性が13種、うち62%にあたる8種が深刻度「高」だった。
- 発見された脆弱性のうち73%は悪用が容易なものだった。

【悪意のあるコードの傾向】

- 2005年上半期、悪意のあるコードの報告件数トップ10のうち、5種までがトロイの木馬だった。第1位は世界、日本共にNetsky.Pだった。
- 新たに記録されたWin32向けウィルス／ワームの亜種は10,868種、前期より48%、前々期よ142%増加している。ただし、ファミリー単位でのウィルス数は安定しており、過去2期と同じ170だった。
- 悪意のあるコードの報告件数上位50のうち、秘密情報を公開する種類のコードは74%を占めており、前期の54%、前年同期の44%よりも増加している。
- ボット関連の悪意のあるコードが増え続けている。報告された悪意のあるコード上位50のうち、GaobotとSpybotが14%を占めていた。前期は3位と4位だったが、今期は2位と3位に順位を上げている。
- スパイボットは亜種を含めて新たに6,361種が報告された。前期の2004年下半期の4,288種から48%増加している。

【その他のセキュリティリスクの傾向】

- 2005年上半期、報告を受けた上位50種のなかで、アドウェアは8%を占め、前回のレポートの5%から増加している。
- 2005年上半期、アドウェアの報告件数上位10種のうち8種までがWebブラウザー経由でインストールされるものだった。
- 2005年上半期、スパイウェアの報告件数上位10種のうち6種までが他のプログラムにバンドルされていたもの、6種がWebブラウザー経由でインストールされるものだった。
- スパムはシマンテックの詐欺対策センサーが監視しているメールトラフィックの61%を占めていた。最大の発信国はアメリカで、世界のスパムの51%を占めている。
- フィッシングにあたるメールは2005年1月に1日平均299万件だったのが、6月には570万件まで増加した。

【今後の傾向】

- モジュール式構造の悪意のあるコード（ダウンロードによって機能を追加する種類のコード）が今後も増えていくと予想される。
- ボットネットワークは数、種類、複雑性とも高まっていくと予想される。
- 攻撃者がさらに巧妙な方法で検知を避けるため、フィッシングの対象が広がると予測される。
- アドウェア、スパイウェアがモバイル機器を狙うことが増え、検知を避ける方法も巧みになり、発見しにくくなるテクノロジーを導入すると予測している。
- ワイヤレスネットワークを対象とした攻撃／脅威の数が増えると予想される。
- 企業におけるデータネットワークと音声ネットワークの統合が進むにつれて、Voice Over Internet Protocol（VoIP）に対する脅威が出現すると予想される。

［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