鉄壁のファイアーウォールでも通用しない

Blasterの教訓を活かすセキュリティーの新常識

8月12日に発見され、お盆明けから各企業、政府機関などで大流行した「Blaster」。はたして、このウイルスはインターネットにおけるセキュリティーの概念をどのように変えたのか。具体的な事象と実際にこのウイルスと戦った人たちのコメントから検証する。

“ウイルス”への認識を一変させたBlaster騒動

2002年7月
SQLスラマーの脆弱性発見。

2003年1月
SQLスラマーが猛威を振るい、韓国全土のネットが麻痺して「インターネット大乱」に。

7月17日
「RPCインターフェイスのバッファオーバーランによりコードが実行される」（MS03-026）という脆弱性がポーランドの研究者グループによって発見され、マイクロソフトが公表。修正パッチをリリースする。

7月25日
MS03-026を使ったエクスプロイトコードを中国人ハッカーグループが完成させる。

8月4日
セキュリティー企業ラックのオペレーションセンターであるJSOCがMS03-026を悪用したポート135経由の攻撃を検知。

8月12日
Blasterが出現。

8月12～16日
この時期にかけて、感染する企業などが続出。お盆明けに、家に持ち帰ったパソコンを企業のLANにつなぐことで爆発的な感染をするのではないかという懸念が広がる。

新常識 1

脆弱性発見からウイルス発生までの期間はわずか数週間に縮んだ！

MS03-026――つまり2003年に入って26番目となるウィンドウズの脆弱性がマイクロソフトから報告されたのは、7月16日だった。そして1週間後の7月25日には、中国のハッカーグループがこの脆弱性を利用したエクスプロイトコードをネット上で公表してしまう。今までの常識から考えると驚くべき早さだった。

エクスプロイト（攻略）コードというのは、脆弱性を利用してコンピュータを攻撃するための具体的な手順のことだ。このコードが公にされれば、ウイルスの出現までは、時間の問題となる。そして人々の恐れたとおり、わずか2週間あまり後の8月12日にはBlaster（別名、MSBlast、Lovsan）という強力なワームの出現を迎えるのだ。

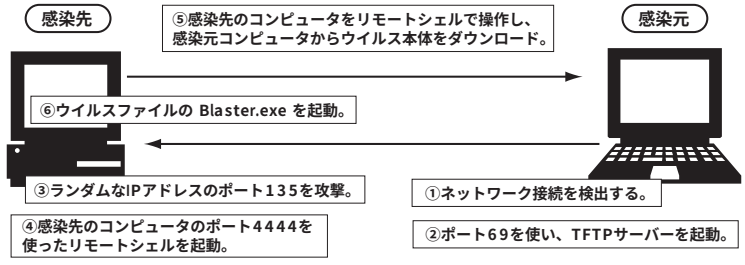
これまでは、脆弱性が発見されてから、ウイルスが出現するまでには半年ぐらいのタイムラグがあるというのが常識だった。実際、今年1月に出現したSQLスラマーの脆弱性が発見されたのは、昨年7月。半年以上の時間が流れている。

そしてこの「脆弱性発見―ウイルス出現」というタイムスパンが縮まっていくと――。最終的には、恐怖のゼロデーを迎える日がやってくるかもしれない。ゼロデーという言葉をご存じだろうか。それは悪意のあるハッカーが未知の脆弱性情報を入手し、マイクロソフトがその修正パッチをリリースするよりも前に、その脆弱性を使ったウイルスをインターネットに放ってしまう日のことだ。それは悪夢のような光景に違いない。インターネットは完全に麻痺し、ネットワークケーブルをルーターから物理的に切断するしか手だてはなくなるだろう。

新常識2 TFTPを使って感染力を大幅に上げたBlasterタイプのウイルス

Blasterが特徴的なのは、ファイル転送に使われるプロトコルのFTPよりもコネクション回数が少なくてすむTFTPというプロトコルを利用する点。通常、Blasterのようなタイプのウイルスは、複雑な手順が必要なためにメールで送られてくるウイルスなどよりも感染力が弱いと言われている。ただし、BlasterはTFTPを使うことでその感染力を高めているのだ。

Blasterが感染するまでの手順



8月16日
Blasterがマイクロソフトのwindowsupdate.comへのDDOS攻撃を宣言した日。しかし実際には大規模な被害は生じなかった。

8月18日
Ping(ICPM ECHO)のトラフィックが急激に増加。Nachiが出現する。

8月下旬
一時期沈静化すると思われたものの、亜種の発生などによりあたらな感染企業などが現れ続ける。

8月29日
亜種のBlaster・Bを作成した容疑で、米ミネアポリスに住む18歳の少年が米連邦捜査局(FBI)に逮捕される。

9月3日
亜種のBlaster・Fの作成容疑でルーマニアの大学院生(24歳)が捜査当局に摘発される。

9月11日
ウィンドウズに新たに三つの脆弱性(MS03-039)が発見された。Blasterが悪用することになった脆弱性と非常に似通っている。

2004年
システムの日付が2004年を迎えると、Nachiは自分自身のサービス登録を削除する。

新常識3 ウイルスの被害は1か月以上経っても消えない!

Blasterの本当の恐怖は、その亜種であるNachi(別名Blaster.D、Welchi)が出現した時に始まった。このウイルスは亜種とはいえ、その挙動は原種のBlasterとはまったく異なる。

①感染先を探すため、Ping(ICPM ECHO)を大量に送信。
②攻撃対象を決定し、MS03-026を突いて侵入。
③Blasterを発見し、強制終了。
④download.microsoft.comからMS03-026の修正パッチを入手し、実行。

やっていることはこれだけだ。当初、Blasterを終了させて修正パッチを当ててくれることから、「善玉のウイルスなのではないか」と考える人もいたほどだ。

しかし、Nachiは感染すると外に向かって大量のPingを打ち続ける。出現から1か月近くが経った9月中旬現在でも、NachiによるICPM(ネットワークにエラーが生じた場合、そのことを送信者に通知するプロトコル)のトラフィック増はまったく衰えを見せていない。パソコンが安定したことに安心して、ネットワークに負荷をかけていることにユーザーが気づかないからだ。ウイルスの被害は1か月以上経っても消えない。これまでは考えられなかったことだ。

新常識4 ウイルスを仕掛けるのは外部ではなく内部の人間

「インターネット大乱」。今年1月のSQLスラマー騒動を、韓国国民が名づけた言葉だ。翻って日本。なぜか被害はほとんど生ぜず、中央省庁を中心に「日本企業のセキュリティー意識は高かった」などという自画自賛の大合唱が起きた。

しかし、SQLスラマーが感染するのはサーバーマシン。日本ではこうしたマシンを使っているのは企業が大半で、防御態勢が整っているところが多かった。だがSQLスラマーは、Microsoft SQL Server 2000 Desktop Engine(MSDE 2000)というデータベースエンジンをインストールしてあるパソコンにも感染する。韓国では偶然MSDEを導入したパソコンが多かった……そのあたりが、結果的に彼我の被害の差となった可能性は大きい。

今回のBlasterではファイアーウォールを突破して感染した例は、実は少ない。ほとんどが内部からの感染、つまり家庭などで感染したノートPCを企業内LANに接続してしまったことによるものだった。多くの企業ではファイアーウォールは設定していたが、こうした人的被害への対応はが行われているケースは少ない。日本のセキュリティーは、諸外国に比べても決して高くはないのだ。

Blaster騒動に直面した人間が見るセキュリティーの新常識

新常識5

「個人ユーザーが本格的にウイルスのターゲットになる時代が来た」

ラック取締役本部長 西本逸郎氏

契約した企業のネットワークを監視し、攻撃がないか、また攻撃があればどのように対処すればいいかなどを通知するJSOCを運営するのが、株式会社ラックだ。今回のBlasterの猛威はセキュリティーのプロである同社本部長西本氏の予測をも上回っていたようだ。

「7月17日にMS03-026の脆弱性が発見され、そして同月25日にはエクスプロイトコードが作られた。われわれはネットで流れる情報をずっと監視していて、エクスプロイトコードがどんどん進化し、さまざまなOSのバージョンや言語に対応していく様子が観測できた。8月5日にはMS03-026を悪用したポート135経由の攻撃を初めて観測し、この段階で新たなウイルスの出現は秒読み段階に入っていた。その意味で、今回のBlasterは事前にある程度は予測できていたと言いえる。だが結果的にはその想像を超えて、大きな影響をインターネットに与えることになった」と西本氏は説明する。

この予想を超えた被害の拡大は、ウイルスのために業務がストップしてしまった場合、社員への連絡はどうするのかなど、さまざまな意味で企業の対応が問われる事態を引き起こしている。なかでも根本的に対応を変えなければいけない大きなポイントが1つあると西本氏は言う。

「今年1～3月期のわが社の統計によると、セキュリティーインシデントの原因として外部からの攻撃は47パーセントしかない。しかもそうした攻撃を受けているのは大半が研究所や学術機関だ。残りの53パーセントは内部からのウイルス感染などで、企業における事故の大半がこうしたケースだと見られている。つまり、ノートパソコンなどの持ち込みによってウイルスに感染してしまうということだ。今回のBlasterは、はからずもその実態を浮き彫りにしてしまったと言える。Blasterはファイアーウォールを設定してポート135を塞いであれば、侵入されるはずはなかった。だがこれほどまでに多くの企業が被害に遭ったのは、ポート135経由ではなく、自宅や外出先から持ち込んで企業内LANに接続したノートパソコンが最大の原因になっていたのだ」(西本氏)。

日本企業はどこもまじめにセキュリティー対策に取り組んでいるから、米国の企業などと比べても高いセキュリティー水準を誇っている。だがそれはあくまで外部からの攻撃への対処であって、内部からの感染に関しては非常に弱かったのだ。企業はこの内部からの感染に関して根本的な対応をはかるべきなのである。

「Blasterでもう1つ注目すべきなのは、クライアントへのリモート攻撃を仕掛ける最初の大規模なワームだったという点だ。一昨年、世界中で猛威を振るったNimdaやCodeRedの攻撃対象はサーバーだった。一方、クライアントに攻撃を行うワームとしてはKlezや、古くはILoveYouなどのウイルスがある。だがこれらはあくまでメールなどを使ったローカル攻撃で、クライアントOSの脆弱性を突いたリモート攻撃を大規模に展開したのは、今回のBlasterが初めてだったと言える。

これはきわめて重要な問題をはらんでいる。ブロードバンド時代に入って、個人ユーザーが本格的に狙われる時代になってきたということだ。これに対処するにはインターネットに対する考え方自体を、変えていかなければいけない。

ラック取締役本部長、西本逸郎氏

もっとも影響が大きいのは、ISPだろう。会員の間に感染者が増えていき、そしてNachiのようにトラフィックが消滅しないでネットに負荷をかけ続けるワームが蔓延するとどうなるだろうか。ISP外部からの感染を防ぐだけでなく、会員による内部から生じるトラフィックにもISPは対処しなければならなくなってくる。こうした状態が続けば、ISPの基幹ネットワークに与える影響は無視できなくなってくる。ISPが単なるプロバイダーとしてではなく“社会インフラ”として、ウイルス対策に本腰を入れて取り組まなければならない時代になってきたと言えるだろう」(西本氏)。

新常識6「メール型ではなくハッカー的手法のウイルスが主流になる」

トレンドマイクロ・ウイルスエキスパート 岡本勝之氏

Blasterを契機に、脆弱性を突いて侵入するというハッカー的手法のウイルスが今後は主流を占めていくようになる可能性は高いだろう。こうした侵入方法がこれまで一般的でなかったのは、コンピュータ内部に入り込むまでの手順が多く、感染に時間がかかったからだ。だがMS03-026の脆弱性を突いた今回のBlasterの場合、FTPよりもコネクションの回数が少なくてすむTFTPプロトコルを利用し、さらに受信確認応答などを受け取る必要のないプロトコルである、UDPだけで送り込むなどの工夫をしている。また通常のウイルスがネット経由で感染先を探す際、ランダムなIPアドレスにパケットを送り続けるのに対し、Blasterは自分の所属するサブネットの周囲を中心に探すといったアルゴリズムも同時に持っている。これによって遠くのコンピュータにも近くのコンピュータにも、同時に感染する能力を持つに至っているのだ。

こうした高度な侵入能力を持つワームが流行してくると、セキュリティー対策自体を抜本的に見直さなくてはならなくなる。特にセキュリティポリシーを持っていない家庭ユーザーにとっては深刻な問題だ。パーソナルファイアーウォールは工場出荷時の状態で不要なポートは閉じてあり、こうした感染への防御はできるようになっているが、たとえば特定のメッセージングソフトなどを使う際に、不用意にポートを開けてしまう可能性がある。そこから感染が広がってしまう可能性はあるだろう。しかし結局は個人のパソコンの使い方に帰結する問題になるので、強制的に対応を迫ることは難しい。ワクチンベンダーや公的機関などが情報を流し、対応策を普及させていくしかないだろう。

トレンドマイクロはもちろん、各セキュリティーベンダーは個人向けに対応策を提供している

新常識7「個人もネットワーク管理者だという意識が必要」

情報処理振興事業協会（IPA）
セキュリティセンター主任研究員 小門寿明氏

今回はウィンドウズの修正プログラム自体にも課題はある。特定の脆弱性を塞ぐことはできるけれども、ほかに影響が出てくる可能性があったり、あるいは動かしているアプリケーションへの影響を考慮しなければならなかったり……と言った問題があり、企業側はベンダーがリリースしたからといって、すぐに修正プログラムを適用できるわけではない。また、修正プログラムのリリースからウイルスの出現までわずか1か月となると、このジレンマをどう回避するかは非常に頭の痛い問題だ。もう1つの問題は、今回のBlasterは個人ユーザーが大規模に巻き込まれたことだ。したがってパソコンがコモディティー（日用品）化していく中で、どうセキュリティー意識を持つように啓発していくのかという課題は大きい。個人ユーザーであっても、自分もネットワーク管理者であるという意識を持ってもらうことが必要だろう。

新常識8「利用者にパソコンの設定は変えさせない」

世田谷区情報政策課長 福田督男氏

世田谷区役所では、パソコンの設定を職員などが勝手に変更できない。ウィンドウズのアップデートも、職員ではなく係員が随時行っている状態だ。世田谷区役所のネットワークがBlasterに感染したのは、外部と接続されていないはずのネットワーク内部に感染源があったことと、このアップデート作業が間に合わなかったことが原因。もちろん、個人にパッチ当てなどをまかせて、セキュリティー対策を効率化する方法もあるのだが、職員すべてを教育するのは並大抵のことではない。そこで、現在、ネットワークを利用して個々のクライアントを管理し、効率的にパッチを当てるソフトの導入を検討している。

世田谷区役所には個人情報が多くあるので、メールの送信ですら上司の承認がいるなど、ある意味でパソコンの便利さを殺しているところがある。もちろん、自宅のパソコンを会社で使うことなどもってのほかだ。今後も、この方針を徹底し、効率的なパッチ当てをすることでセキュリティーを守っていく。Blasterで学んだのは、個人にパソコンをまかせない方法で、いかに効率的に個々のパソコンのセキュリティー管理を徹底していくことが重要かということだ。

［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