コンピューターウイルスの動向

鈴木 直美　フリーライター

オートラン悪用ウイルスでLAN内パソコンにも大規模被害
年末年始はガンブラー攻撃によるサイト改ざんが急速拡大

メール、ウェブサイト、USBメモリーなどのリムーバブルメディアと、さまざまな経路から感染を試みようとするコンピューターウイルス（トロイの木馬やワーム、スパイウェアなども含む）。2009年に特に目立ったのは、システムの脆弱性を狙って感染を広げるウイルスが、大規模な被害へと発展してしまったケースだ。パッチが未提供の状態で攻撃が始まってしまうゼロデイ攻撃も幾度かあったが、1年を通じて展開されたのは、修正済みの脆弱性攻撃だ。セキュリティーパッチを適用していれば回避できたはずのウイルスが次々とシステムに感染し、セキュリティーパッチの重要性を見せつけられた年だった。

内部ネットワークを汚染したConficker

インターネットから隔離されたLAN内のパソコンにまで大規模な感染被害を出したのが、「Conficker」「Downadup」「Downad」などの名前で呼ばれるウイルスである。Confickerは、Windowsの共有機能を提供するServerサービスの脆弱性を突いて感染を広げるウイルスとして、2008年10月に登場。年末には、Windowsのオートラン機能を悪用し、USBメモリーなどを介して感染する機能も実装され、インターネットにつながっていないLAN内へのウイルス侵入が懸念された。脆弱性攻撃の開始を受けて緊急パッチが提供されたものの、閉じたネットワーク内のパソコンではパッチの適用がルーズになりがちで、ウイルス対策ソフトを導入していないケースもあるからだ。

そんなLAN内にWindowsのネットワークを介して拡散するウイルスが侵入すればどうなるか。2009年の年明け早々からその危惧が現実のものとなってしまった。4月にかけ、自治体や警察、病院などが次々と被害にあい、業務に支障をきたす事態を招いた。中には千台を超える業務用パソコンに感染が広がったケース、復旧までに1週間を費やしたケースもある。

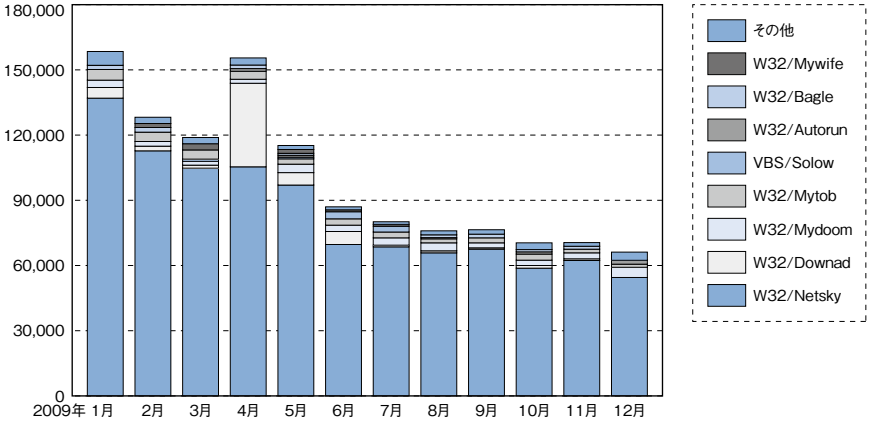
ウェブサイトを汚染したガンブラー

ウェブサイトを閲覧したユーザーのパソコンに、許可なくプログラムをインストールする行為を「ドライブ・バイ・ダウンロード」という。ウイルス感染の手段としてこの攻撃を仕掛けるために、2008年頃から主にSQLインジェクションという手法を用いて一般のウェブサイトを改ざんする行為が横行した。年末から2009年の年明けにかけてピークを迎え、その後急速に減少した。これに代わって目立つようになったのが、盗み取ったFTP情報を使っての改ざんだ。一般に「ガンブラー」の名で総称されるが、実際には大小多数の異なる攻撃があり、3月頃から絶え間なく繰り返された。

国内のウェブサイトに多数の被害を与えた最初の攻撃は、「zlkon.lv」「gumblar.cn」「martuz.cn」といった特定の攻撃サイトに誘導するタイプだった。攻撃サイトでは、Adobe Readerなどの脆弱性を突いて閲覧者のパソコンに通信内容を盗聴するウイルスを仕掛ける。これがウェブサイト更新用のFTP情報を盗み取り、今度は閲覧者が管理していたサイトが改ざんされる。さらなる感染者を生み出していくやり方で勢力を拡大していった。攻撃は2009年3月に始まり、4月に入ると国内でも被害報告が出始める。ゴールデンウィーク前後には、国や自

USBメモリーウイルス「Autorun」や「Downad」が猛威をふるう

資料6-2-9　ウイルス別検出数の推移

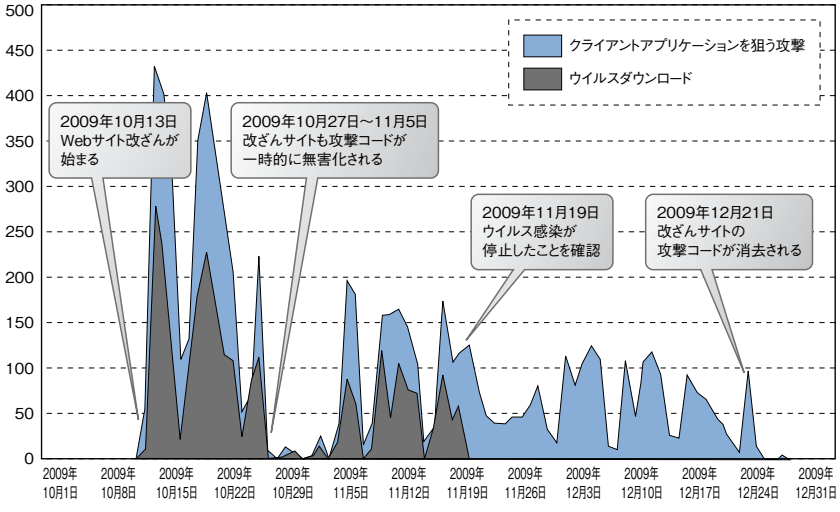


2004年に登場したNetskyやMydoom、2005年のMytobといったマスメーリング型のウイルスが相変わらず届出件数の上位を占める中、USBメモリーなどを介して感染を広げるAutorunやDownadといった新しいウイルスも勢いを見せている。Downadは、Windowsの脆弱性を悪用するConfickerの別の呼び名で、4月には検出数が著しく増加。Netskyに次ぐ検出数となっている。

出所　IPA「2009年コンピュータウイルスの届出状況について」2010年1月
http://www.ipa.go.jp/security/txt/2010/documents/2009all-vir.pdf

ガンブラー攻撃によるウェブ改ざんとウイルス感染が猛威

資料6-2-10　2009年秋から年末にかけてのガンブラー攻撃（Gumblar.x）の検知件数の推移



国内のウェブサイトが次々に改ざんされ、閲覧者にウイルスを感染させようとする悪質なコードが埋め込まれた通称「ガンブラー」。2009年3～5月に行われた国内初の大規模攻撃は、5か月の沈黙を経て10月に再襲来。12月には、継続して行われていた8080系の攻撃（ガンブラーと類似した攻撃）が国内でも本格的に始まり、2010年の年明けにかけて多数のサイトが次々に陥落していく事態となった。

出所　日本IBM「2009年下半期 Tokyo SOC 情報分析レポート」2010年2月
http://www-935.ibm.com/services/jp/iss/pdf/tokyo_soc_report2009_h2.pdf

治体、企業など多数のウェブサイトへと波及した。5月末の攻撃サイト閉鎖とともにいったん終息を迎えるも、10月半ばには、攻撃サイトにも多数の一般サイトを用いた新たな手法で攻撃が再開された。

12月に入ると、ガンブラーに類似した別の攻撃被害が国内で報告されるようになった。一般には「ガンブラー亜種」などと呼ばれているこの攻撃は、春から継続して行われているものの1つで、改ざんサイトから5台のサーバーで構成した攻撃サイトへと誘導する。誘導先のドメイン名には、当初は主に中国（.cn）、国内に上陸した12月にはロシア（.ru）を多用し、改ざんサイトには、これらドメインの8080ポートに接続する難読化されたコードが埋め込まれた。ガンブラー同様に、脆弱性攻撃を仕掛けるが、感染ウイルスはさらに悪質で、盗聴のほかにも各種情報の窃取やメールの送信、バックドア、DoS、偽セキュリティーソフトなど、さまざまなプログラムがインストールされる。年末から年初にかけ、この攻撃による改ざん被害が国内で急速に拡大していった。

参考文献
・日本IBM「2009年上半期 Tokyo SOC 情報分析レポート」2009年8月
http://www-935.ibm.com/services/jp/iss/pdf/tokyo_soc_report2009_h1.pdf
・日本IBM「2009年下半期 Tokyo SOC 情報分析レポート」2010年2月
http://www-935.ibm.com/services/jp/iss/pdf/tokyo_soc_report2009_h2.pdf

［インターネット白書ARCHIVES］ご利用上の注意

このファイルは、株式会社インプレスR&Dが1996年～2012年までに発行したインターネットの年鑑『インターネット白書』の誌面をPDF化し、「インターネット白書ARCHIVES」として以下のウェブサイトで公開しているものです。

http://IWParchives.jp/

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、データ、URL、名称など）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・図の作成者、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掲載されていない場合があります。
- このファイルの内容を改変したり、商用目的として再利用したり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される際は、出典として媒体名および年号、該当ページ番号、発行元（株式会社インプレスR&D）などの情報をご明記ください。
- オリジナルの発行時点では、株式会社インプレスR&D（初期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。

お問い合わせ先 | 株式会社インプレスR&D | ✉ iwp-info@impress.co.jp