サイバーセキュリティ最前線

なぜ多くのセキュリティ対策ツールは「EMOTET」の侵入を許してしまうのか!?

前号ではマルウェア（悪意のあるプログラムの総称）の一種であり、一般的なセキュリティ対策では検知しにくい「EMOTET（エモテット）」が猛威を振るっている様子をお伝えした。それにしてもどうしてEMOTETには従来のセキュリティ対策が通用しないのか。今号ではそのあたりのメカニズムを解説したい。

セキュリティ対策の限界

「ウイルス対策」の代表的な手法には「パターンベースのウイルス対策」と「振る舞い検知」がある。まず「パターンベースのウイルス対策」はパソコン利用が一般化して以降、セキュリティソフトとしてパソコン購入時にバンドル（同梱）されたことを背景に急速に普及してきた。そのセキュリティ手法は有害ファイルのパターンファイル（指名手配犯リスト）をもとに、メールの添付やディスク上に保存されたファイル群から有害なファイルを見つけ出すというものだ。そのため、多くのセキュリティ会社がパターンファイルの更新のはやさや対応範囲などを競ってきたが、パソコンに送り付けられるマルウェアの多くがそのつど、異なる固有性を持った「ポリモーフィック（多態）型」（パソコンに保存される際に変形するもの）となっている今日、この方法だけではマルウェアによる攻撃の50％も防げないといわれている。

では、もう一方の「振る舞い検知」はどうか。こちらはプログラムファイルなどの動作を監視して、悪意のある動作（振る舞い）を感知し、遮断する仕組みのこと。たとえば、画面上で見えない形で外部のサーバーと通信をはじめたり、ほかのファイルをダウンロードしたりすると、怪しい動作と判定する。だが、コンピュータプログラムには多様な種類があり、プログラマーもユーザーも自由にプログラムを作成、利用できる状態にあるため、それらを一つひとつ正しく「振る舞い検知」することはできない。事実、「現在のパソコンのソフトは非常に高機能化しており、ユーザーが何の操作もしていない『アイドリング状態』でも、画面から見えないところで無数の処理が実行されている。いわばつねに『ノイズ』が多い状態にあるので、すり抜け防止を強化する過程で正当な動作をブロックしてしまいかねない」とセキュリティシステムの最前線で防御システムの事業に取り組む㈱ブロード（東京都千代田区）は指摘する。

巧妙化するマルウェア

こうした状況に加え、最近はマルウェアが急速に巧妙化しているという問題がある。実際、「現在のマルウェアの主流は、広く普及しているOfficeソフトやWindows OSに標準装備された機構を悪用しているため、非常に検知されにくい」という。とりわけ一定パターンの操作をプログラムとして登録する機能（マイクロソフトの場合はマクロと呼ばれる）などを悪用されると、Officeソフトやそれ用の文書ファイルを介してマルウェアに侵入されてしまうことがあるので注意が必要だ。

もうひとつ気をつけなければならないのがプログラムの脆弱性（抜け穴）だ。多くのセキュリティ製品はOSやプログラムが設計通り動くことを前提としてつくられているため、想定外の脆弱性に対しては無防備な状態となっている。時折、そういった脆弱性が開示され、プログラムの更新などが促されるが、その対応が遅れると脆弱性という抜け穴からマルウェアの侵入を許すことになってしまうのだ。実際、今年3月にはセキュリティ製品を扱う企業自身が、4段階の対策を講じていたにもかからず、EMOTETの侵入を許してしまっている。

まさに八方ふさがりの状況だが、「HP Sure Click Enterprise」はセキュリティに対する考え方が根本的に異なるため、巧妙化するマルウェアにもシッカリと対応できる。マイクロVM（仮想パソコン）でメールやインターネットなど外部から受領するファイルの一切を開いて閲覧、操作するため、あらかじめすべてのファイルを隔離することができるのだ。まずは一度、その実力を試してみてほしい。