サイバーセキュリティ最前線

あらゆるセキュリティ対策をすり抜けるEMOTETの脅威にどう立ち向かうか

なりすましメールの巧妙化などによって、マルウェアの一種であるEMOTET（エモテット）による被害が急増している。はたして、EMOTETにはどのような特徴があり、どういったことに注意を払うべきなのか。あらためて、そのあたりのポイントをまとめてみた。

なりすましメールが発端に

EMOTET（エモテット）とはマルウェア（悪意のあるプログラムの総称）の一種で、一般的なセキュリティ対策では検知しにくいのが特徴。被害の8～9割がなりすましメールを発端としているが、その手口は日増しに巧妙化している。「以前は明らかに海外から送られたとみられる奇妙な文面が多かったが、最近は実在する金融機関や携帯キャリア、大手通販サイトなどがアカウントの再認証を求める内容だったり、直前まで取引先とやりとりしていたメールに割り込んできたりと、思わずダマされてしまうようなものになっている」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）は話す。

そして「しかも」とつづける。「ひとたびEMOTETに感染すると、今度はそのパソコンを起点にさらに被害が拡大する恐れがある」というのだ。たとえば、そのパソコンに登録されたメールアドレスや実際に使ったメールの文章、文末に記載される「シグネチャ（署名）」などを模倣したマルウェアメールを、普段やりとりしている相手などに勝手に送ることがあるそうだ。

が、昨今のマルウェアの脅威はそれだけにとどまらない。いったんパソコンのなかに入り込むと、つぎからつぎへと別のマルウェアを受信したり、パソコン内のデータを犯行者側に送信したり、別のパソコンやサーバーに感染を試みるなど、目に見えない状態で犯行を繰り返すのだ。

「仮想パソコン」による対策を

つまり、EMOTETは万全と思われるセキュリティ対策も見事にすり抜けるのだ。事実、セキュリティ関連の製品・サービスを提供する企業ですらこの3月の下旬に、EMOTETの被害に遭ったことを公表。それによると、同社は4段階のセキュリティ対策をとっていたそうだが、それでも感染してしまったのだ。「EMOTETがいまだに多様なセキュリティ対策をすり抜ける理由のひとつに、マルウェアか否かの判定が過去の事例との比較によるものになっていることがあげられる。それはちょうど『こういう電話がかかってきたら、オレオレ詐欺の可能性を疑え』といった防犯の注意喚起に似ており、それでは従来のパターンとは異なるマルウェアやまったく新しいマルウェアに対して意味をなさない」と前出のブロードは説明する。他方、セキュリティレベルを上げて「疑わしいもの」をすべて〝クロ〟と判定する方法も考えられるが、そうすると今度は業務上必要なメールやファイルまで使用できない状態に陥ってしまう。さらに「先進的なマルウェアの一部には、こうしたセキュリティ対策を最初に停止させる特性もある」そうなので、まさに打つ手なしといった感すらある。

こうした状況を受けて、経済産業省をはじめとした関係省庁はサイバー攻撃に関する注意喚起の文書を発表。そのなかには「メールの添付ファイルやリンクを不用意に開かない」といった対策が記されているが、実際に取引先とやりとりしたメールの文面などを模倣されると、全社員がそのすべてを正しく判断できるとはかぎらない。そこで、役に立つのが「HP Sure Click Enterprise」だ。このシステムを導入すれば、判定や判断をすることなく、自動的にパソコン本体から独立した「仮想パソコン」で危険かもしれないメールやファイルを開くため、マルウェア感染を未然に防ぐことができるのだ。備えあれば憂いなしのたとえを実感できるはずだ。