サイバーセキュリティ最前線

「検知しづらい」悪質で巧妙なマルウェアが急増！「EMOTET（エモテット）」の恐ろしさと対策

サイバー攻撃が多様化・複雑化しており、大企業や省庁の情報流出の可能性も指摘されるなど、もはや日本経済や国家を揺るがす巨大なリスクとなっている。とくに専門家らは一般的なウイルス対策ソフトで検知することが非常に難しいマルウェア「EMOTET（エモテット）」に危機感を覚えている。早急な対策が必要だ。

今年の1月20日、三菱電機㈱が不正アクセス被害を受けたことを発表した。当初は「機密の流出はない」としていたが、その後の防衛省の発表で防衛機密に関する情報が流出した可能性があることが明らかとなった。攻撃者は「ファイルレスマルウェア」を用いて、同社の中国拠点から日本国内にある同社のウイルス対策管理サーバーへと感染を広げたという。東京工業大学情報理工学院サイバーセキュリティ研究センター長の田中圭介教授によれば、このファイルレスマルウェアはウィンドウズの一部機能を悪用して情報を抜き取る手口で、従来のウイルスと違ってハードディスクにファイルとして保存されないため、「システム上に不審な動きがあって初めてそれを検知するウイルス対策ソフトウエアでは歯が立たない」とのこと。「いつ入り込んだのかわからず、潜伏期間もあるので、人体に病気を引き起こすウイルスと同じで予防策が立てづらい」のだ。

こうした「検知しづらい」悪質なマルウェアが、ここ数年で激増している。なかでも感染力・拡散力が強いマルウェアとして各方面で甚大な被害をもたらしているのが「EMOTET（エモテット）」だ。セキュリティ会社である㈱ブロードによると、これは「約5年前からネットバンキング分野で知られるようになったマルウェアで、それ自体が動作するというよりも、別の種類のマルウェアをインターネット経由でダウンロードする機能に長けている」という。「ウイルスに感染したかどうかが目に見えないのが特徴。無関係に他人にウイルスメールを送信したり、ほかのマルウェアをダウンロードするなどの用途に使われる可能性がある」など、その恐ろしさは類を見ないといわれている。このエモテットを一般的なウイルス対策ソフトで検知するのが困難な理由はさまざまあるが、ひとつには「ポリモーフィック型マルウェア（多態系）」だということがあげられる。「マルウェアのパターンをすべて変化させることで、毎回、新種と同じ状態にすることができる」ため、従来のウイルス対策では発見が難しいのだ。

当然、このあらたな脅威に対応するべく対策ソフトを強化・改善したいところだが、そこにも難しい点がある。「セキュリティソフト開発には、世の中に実際に出回っているマルウェアを研究して対策を講じるという方法があるが、エモテットはその内容が巧妙に隠され、わかりにくくなっているので、どうしても対策が遅れてしまう」という。そこで、注目したいのが一般的なセキュリティソフトのようにマルウェアやウイルスなどを検知・判定してブロックするのではなく、いったんマイクロVM（仮想パソコン）にすべてを取り込み、使用後に仮想パソコンごと削除するという斬新なソフトだ。たとえば「Bromium（ブロミアム）」（発売元は前出のブロード）がそれだ。米国発のこのソフトは、セキュリティ対策として推奨されるネットワーク分離と同等の効果を柔軟に実現できることから、日本のサイバーセキュリティのレベルを一気に向上させる可能性を持っていると期待されている。今後さらに増加していくサイバー攻撃からいかにして身を守るか、こうしたソフトがその頼もしい味方になるはずだ。

新型肺炎騒動に乗じた保健所を名乗る詐欺メールへの注意喚起が促されているが、脅威の本質を知り、それに応じた対策を講じることが重要だ。