サイバーセキュリティ最前線

「EMOTET（エモテット）」による被害がコロナ禍の日本においても急拡大中!!

東京2020大会を目前に控え、日本でも高度なマルウェア（悪意を持ったソフトウェア）による被害が急拡大している。コロナ禍にあって、テレワークやリモートワークが日常的なものとなった今、中小企業はどのような対策を講じればいいのだろうか。今号では「EMOTET（エモテット）」の脅威とその対策について紹介したい。

もはやEMONETは対岸の火事ではない

本誌2020年1月号の本コーナーで取り上げた高度なマルウェア「EMOTET（エモテット）」が、日本でも急拡大している。事実、今年2月に「国内の少なくとも3200社が感染している」（JPCERTコーディネーションセンター）との発表があったほか、昨年4～6月はわずか1件のみだった情報処理推進機構への相談が、7～9月には308件にも達するといった事態が生じている。日本でのこの急拡大ぶりは世界的にみても目立っており、セキュリティ企業のESETによると、日本におけるエモテットの検出率（20年10月）はギリシャについで世界で2番目に多い数字になっているという。

もはや対岸の火事ではなくなったエモテットだが、このマルウェアにはどのような特徴があるのだろうか。長年、セキュリティシステムの提案をしている㈱ブロード（東京都千代田区）によると「エモテットには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させたり、一般的なウイルス対策ソフトで検知しづらくしたりする機能が盛り込まれている」という。しかも、最近はその拡散方法がさらに複雑化している。たとえば「不正な添付ファイルがウイルス対策ソフトに検出されるようになると、パスワードで保護された『zip』などの圧縮ファイルを添付する手法が増えてきた」という。メールの本文に記載されたパスワードをユーザーが入力するとエモテットが自動的にダウンロードされるようになっているのだ。そのうえ、そういった経緯でエモテットに感染すると、今度はそのコンピュータを起点として第三者に返信メールとして不正なファイルを勝手に送るといったケースも増加している。そうなると、返信メールをもらった側はこれまでにやりとりをしていた相手からのメールであるため、違和感を覚えることなく、添付データなどを開いてしまい、さらに被害が拡大していくことになる。エモネットは実に厄介なマルウェアなのだ。

EMONET対策に最適な仮想技術を用いたセキュリティ対策

こうした特性を持つエモテットの対策は非常に難しい。実際、多くのセキュリティソフトとイタチごっこがつづいているのが現状だ。そこで、あらためて注目したいのが、仮想技術を用いた米国発のセキュリティ製品「Bromium（ブロミウム）」だ。販売代理店を務めるブロードによると「この製品を使えば、PC本体のハードウェアから完全に隔離された仮想環境でウェブサイトの閲覧やドキュメントファイルの開封などを行えるため、エモテットがOSやネットワークに侵入するのを防ぐことができる」という。まさにこれならこわいものなし、安心してテレワークやリモートワークに臨むことができそうだ。日増しに高まるサイバーリスクに備えるためにも、ブロミウムの導入を検討してみてはどうだろうか。