IT時事ネタキーワード「これが気になる！」（第73回）

# ウイルス「エモテット」制圧

2021.03.29


1月27日、ユーロポールは、世界中で猛威を振るっていたコンピューターウイルス「エモテット」について、オランダ、ドイツ、米国、英国、フランス、リトアニア、カナダ、ウクライナ各国の警察と協力し、エモテットのメインサーバーを止め、パソコンやハードディスクなどを押収した。サーバーの2台はオランダに、もう1台はウクライナにあった。

この作戦でエモテットの制圧に成功した、というニュースが世界中に流れた。エモテットのネットワークを効果的に解体して再構築の可能性を阻止するには、関係する複数の国で同時に行動を起こす必要があったという。

ウクライナでの押収の様子は、YouTubeのウクライナ国家警察の公式チャンネル動画で見られる。コンピューター機器のほか、金塊や札束も大量に押収された。盗んだ情報を公開すると脅す「暴露型」の活動を収入源としていたと思われる（最近よく聞く「暴露型ウイルス」参照）。エモテットの被害は世界で25億ドルに上り、ウクライナ警察に拘束された2人は最大12年の懲役が科されるという。

エモテットは、メールの添付ファイルやメール中のリンクを開くことで感染する。オランダ警察によれば、押収されたデータの中から、数百万件のパスワード付きメールアドレスが見つかったという。オランダ警察のページのフォームから、押収されたデータに自分のアドレスが含まれるかどうかチェックできる。

なお、海外の捜査当局から警察庁に対して、日本でエモテットに感染している機器の情報提供があった。2月下旬から情報をISPに提供し、記載されている機器の利用者を特定。注意喚起が行われている。詳しくは警察庁の「マルウェアに感染している機器の利用者に対する注意喚起の実施について」と総務省の「マルウェアに感染している機器の利用者に対する注意喚起の実施」を参照しよう。

そもそも「エモテット」（Emotet）とは？… 続きを読む