IT時事ネタキーワード「これが気になる！」（第77回）

サイバー攻撃に勝利。エモテット完全停止

2021.06.28

世界中で猛威を振るってきたコンピューターウイルス「エモテット」（Emotet）は1月27日、ユーロポールと欧米各国の共同作戦により制圧された。1月27日のテイクダウン（倒す、破壊する、という意味）によってサーバーを差し押さえ、メンバーは逮捕。感染端末は法執行機関が管理するサーバーとのみ通信を行うよう書き換えられた。

日本ではサイバー攻撃対策の民間団体「JPCERTコーディネーションセンター」（JPCERT/CC）が中心となり、捜査当局から提供された感染者のデータに基づき、1月下旬からISPなどと協力して、感染者への通知と対策の案内を行ってきた。

その後、エモテットは感染端末の時刻が4月25日正午の時点で停止する機能を加えた無害化ファイルで自動的に更新され、以降、感染がほぼ観測されなくなった。これが事実上のエモテットの完全制圧といえる（JPCERT/CC「マルウェアEmotetのテイクダウンと感染端末に対する通知」より）。

エモテットの猛威

エモテットは2014年ごろから登場し2019年後半から猛威を振るった。偽メールを手段としたコンピューターウイルスだ。メールの添付ファイルを開くなどで、ウイルスに感染したコンピューターはマルウエアをインストールされ、情報を次々に送信したり他のウイルスの感染を広める踏み台にされたりしてしまう。

ここ最近のエモテットは日本語を巧みに使い、乗っ取ったコンピューターのアドレス帳まで盗み見て、リアルな偽メールを作成しターゲットを狙っていた。添付ファイルはそれらしい表題を付けたオフィス書類はもちろん、いわゆるPPAP（パスワード付きzipファイルをまず送り、別メールでパスワードを送るメール手法。少し前までセキュリティが高いとされ盛んに行われていた）で問題視されたZIPファイルも用いるなど、各国の世の中の流れを熟知し巧妙に利用していた。

エモテットの主たる目的は、メールをきっかけに盗んだ情報を公開すると企業を脅す「暴露型」としての活動だ（最近よく聞く「暴露型ウイルス」参照）。なお、エモテットの犯罪グループは、攻撃メールから情報の盗用までのエキスパートとして動き、その先は他の組織が担当というような、組織横断的な犯行にも絡んでいたといわれる。

エモテット完全制圧も続く偽メールの脅威。テレワークを狙った攻撃も… 続きを読む