最新セキュリティマネジメント（第18回）

攻撃を再開したマルウエア「Emotet」の脅威

2022.11.24

悪意を持って作られたプログラムであるマルウエアの代表的な存在、「Emotet（エモテット）」が2022年11月から活動を再開したという報告があり、独立行政法人情報処理推進機構（IPA）がホームページ上で注意喚起を呼びかけている。Emotetはどんなマルウエアで、どんな手段を使って侵入し、どんな被害を及ぼすのか。感染防止策を含めて解説する。

2022年11月2日から再開を観測

Emotetとは、情報を盗み出したりする悪意を持って作られたプログラムだ。2016年頃に登場し、2020年7月頃には世界中で猛威を振い、数多くのサーバーやパソコンが感染して大問題となった。2018年頃からは日本語での攻撃も出現している。

2021年1月27日にはEUROPOL（欧州刑事警察機構）が、欧米8カ国の法執行機関・司法当局の共同作戦によって、Emotetの攻撃基盤をテイクダウンした。テイクダウンとは攻撃に使われるサーバーを差し押さえ、メンバーを逮捕し、感染した端末を法執行機関のサーバーとだけ通信できるように設定して、攻撃を停止させることだ。

この大掛かりな捕物劇によってEmotetの攻撃や被害が停止、あるいは大幅に減少し、IPAでもEmotetに関する情報の提供が徐々に少なくなり、2021年4月26日以降は日本におけるEmotetの感染はほぼ観測されなくなったとされていた。

ところが2022年11月4日、IPAホームページに再びEmotetに関する警告が掲示された。追記された文面は「2022年7月13日頃より、Emotetの攻撃メールの配信が観測されない状態が続いていましたが、2022年11月2日から再開されたことを観測しました」とある。この警告を受けて、改めてEmotetの攻撃手法、被害の内容、感染防止策をまとめておきたい。

Emotetの攻撃の手口はある意味シンプルだ。偽のメールに不正なファイルを添付し、それをクリックするよう誘導しデバイスに感染させる。ウイルス対策の基本として不用意に添付ファイルを開かないということは周知されているので、簡単には引っかからないような気がするが、Emotetは考えている以上に巧妙な攻撃を仕掛けてくる。

IPAのホームページでは実際の攻撃例が掲載されているが、最も警戒が必要なのは「正規のメールへの返信を装う手口」である。実際に攻撃メールの受信者自身が送信したメールが丸ごと引用され、送信者も取引メールの送信相手になりすまし、件名も同じだ。ただし、不正なファイルが添付されている。

日頃の対策と感染チェックで被害を防ぐ… 続きを読む