潜行するサイバー攻撃（第7回）

なりすましメールでウイルス感染「Emotet」

2020.09.09

「取引先とのやり取りのメールに返信がきて、添付されたWordファイルを開いた」。こんな日常茶飯事のコミュニケーションが、コンピューターウイルス感染のきっかけになってしまったら……。困ったことに、「Emotet」（エモテット）と呼ぶマルウエアは、冒頭のような日常のやり取りからパソコンや社内システムに忍び込む。

Emotetは、国内でも2019年10月からしばらく感染事例が相次いでいた。その後、2020年2月以降にはいったん活動が収束したと見られたが、20年7月になるとまた息を吹き返してきた。コンピューターセキュリティの情報を収集し、インシデント対策の支援を行うJPCERTコーディネーションセンターは、7月に「Emotetの感染につながるメール配布が確認されている」として注意喚起を促した。この夏はコンピューターウイルスでも第二波による脅威にさらされて、今後の感染被害拡大に注意を払い続ける必要がありそうだ。

まずEmotetの振る舞いを確認しておきたい。ウイルスとして、複数の顔を持つ手ごわい相手といえる。まずEmotetは、感染したパソコンから情報を盗み出す。端末やブラウザーに保存されたパスワードなどの認証情報を窃取した上で、メールアカウントとパスワードを盗み出し、さらにメール本文やアドレス帳の情報をも取り出してしまう。次いで、端末から情報を窃取するだけでなく、そのアドレス帳情報を使って他の端末に感染を広げるメールを送信する。それだけではなく、Emotetが作り上げた感染ネットワークを使って、他のウイルスの感染を広めるプラットフォームの役割も果たすのである。

知り合いからのメールだから開いてしまう… 続きを読む