IT時事ネタキーワード「これが気になる！」（第95回）

エモテット、ここへきて大流行。対策してみた

2022.05.18

完全制圧されたといわれたEmotet（エモテット）が10カ月ぶりに復活したと1月のコラム「エモテット10カ月ぶり活動再開」で述べた。IPAの直近の追記「Emotetの攻撃活動の急増」「感染被害の大幅拡大/日本語で書かれた新たな攻撃メール」によると2022年2月から3月にかけて、日本国内組織での感染被害が大幅に拡大しているという。

IPAの「情報セキュリティ安心相談窓口」では、2022年3月1日～8日に323件もの相談を受けた。これは前月同時期（2月1日～8日）のおよそ7倍に相当し、JPCERT/CC「マルウェアEmotetの感染再拡大に関する注意喚起」のグラフからも激増の様子がうかがえる。記事には、「2022年3月に入り、Emotetに感染しメール送信に悪用される可能性のある.jpメールアドレス数が2020年の感染ピーク時の約5倍以上に急増しています」とある。

サイバーセキュリティ総研の「Emotet感染の被害にあった企業事例一覧」によれば、2021年12月～2022年3月の感染被害企業一覧には、名だたる企業・団体の名前が並ぶ。

おさらい。マクロ付きメール添付ファイルや、ダウンロードリンクで感染

エモテットは基本的に、メールに添付されたWordやExcelファイルを開き、「コンテンツの有効化」「マクロを有効にする」を実行することで感染する。メールは流ちょうな日本語を用い、実在の組織や人物をかたったり、コロナ禍などタイムリーな話題を取り入れたりなど、巧妙極まりないのが特徴だ。

メールの添付ファイルではなく、メール本文に記載されたURLのクリックで感染する場合もある。ショートカットファイル（LNKファイル）またはそれを含むパスワード付きZipファイルを添付したメールが新たに観測されている。エモテットは時代に合わせて常に手口を変えてくるので、常に最新情報のチェックが有効だ。

エモテットの主たる目的は、メールをきっかけにサーバーのデータをロックしたり、盗んだ情報を公開すると企業を脅したりするランサムウエアとしての活動だ。厳重なシステムやセキュリティ対策をしていて当然と思われる有名大企業が続々と被害に遭うのは、個人を狙ったなりすましメールで誘う「人的ミス」を入り口にしていることが一因だろう。

感染対策には、先述の「Emotet（エモテット）と呼ばれるウイルスへの感染を狙うメールについて」内の「対策」を参照しよう。これは感染防止にとどまらず、一般的なウイルス対策の基本でもある。自分の“ついつい”な行動で、組織が今まで築き上げた信用や大量の金銭を失うことや組織の存亡に関わる点をよく自覚して、メールのみならずIT周りのセキュリティに心を配り、慎重に行動しよう。

JPCERT/CCのEmoCheckでパソコンをチェックしてみた… 続きを読む