IT時事ネタキーワード「これが気になる！」（第90回）

エモテット10カ月ぶり活動再開

2022.01.26

IPAは昨年11月16日、「Emotetの攻撃活動再開について」というリリースで、「2021年11月14日頃から、Emotetの攻撃活動再開の兆候が確認されたという情報があります。また、Emotetへの感染を狙う攻撃メール（Emotetの攻撃メール）が着信しているという情報も複数観測している状況です」と注意喚起した。今回の復活は今後、攻撃メールの大規模なばらまきに発展する恐れがあり、改めて警戒する必要があるという。

Emotet（エモテット）とは2014年頃から登場し2019年後半から猛威を振るった、主に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。

さらにエモテットは、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う。添付ファイルはそれらしい表題を付けたオフィス書類や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）で問題視されたZipファイルも用いるなど、各国の事情を熟知した巧妙なものだ。

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。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るといわれていた。

2021年1月27日、ユーロポール（欧州刑事警察機構）が、欧米8カ国の協力により、エモテットのコントロールサーバー（ウイルスメールをばらまいたり、感染したマシンを操作したりする機器）をテイクダウンした（停止させた）と発表。その後、感染端末の時刻が2021年4月25日になると、すべてのエモテット・マルウエアが停止する機能が加えられ、以降、世界および日本における感染もほぼ観測されなくなっていた。

当連載でもエモテットの脅威や経緯を何回か紹介した。4月時点での“完全制圧”は喜ぶべきことだが、サイバー犯罪の入り口としてメールは非常に有効な手段ゆえ、似たような動きをするマルウエアはなくならないだろうとも想像していた。

復活のいきさつと世界、日本での現状… 続きを読む