最新セキュリティマネジメント（第21回）

パスワード付き添付ファイルの送受信リスク

2023.02.24

“PPAP問題”をご存じだろうか。PPAPとは添付ファイル付きのメールを送信する際に、添付ファイルを暗号化したZIPファイルで送信し、別のメールで暗号化したファイルを解凍するパスワードを送るという方法だ。メールでファイルを共有する際にセキュリティを担保するために広まったPPAPだが、セキュリティリスクが大きいと指摘され使用を禁止する企業や組織が増えている。なぜだろうか。

パスワードが盗まれマルウエア感染の恐れ

PPAPはIT用語でよくある英文の頭文字をとって略称にしたものではない。「Password付きZIP暗号化ファイルを送ります」「Passwordを送ります」「Aん号化（暗号化）」「Protocol」のことだ。送信者としては操作が簡単で誤送信防止にもなるため、リスクを減らしてメールでファイルを共有する方法として普及してきた。

広く使われてきたPPAPがなぜ危険なのか。その原因の一つが一通目のパスワード付きファイルを送ったメールと、二通目のパスワードを通知するメールが同じ経路で送信されているからだ。メールはいくつものサーバーをたどって送信されるため、途中で盗み見られる危険がある。一通目を盗み見られた場合、二通目も盗み見られてしまう。これでは暗号化した意味がない。

ファイルを自動で暗号化するPPAPは送信側が手軽にできる一方で、二通目のメールのパスワードでファイルを解凍する必要があるため、受信者側には負担が大きい。なのにセキュリティ上の効果がないのであればやる意味がない、と指摘されるようになった。

さらに大きな問題として浮上したのが、添付ファイルに対してウイルスチェックが効かないという点だ。セキュリティ製品の多くは送られてきたメールをチェックしているが、パスワード付きのZIPファイルの中身はチェックできない。メールが盗み見られてマルウエア付きのファイルにすり替えられても、検知できないことになる。

このような事態は実際に発生していて、独立行政法人情報処理推進機構（IPA）では2020年9月2日に「パスワード付きのZIPファイルを添付したEmotetの攻撃メール」を確認したと報告している。Emotetはこの連載の第18回でも紹介した、悪意を持って作られた代表的なプログラムである。ファイルを開くとデバイスがマルウエアに感染してしまう。

代替手段はクラウドストレージの活用… 続きを読む