滋賀県警からのサイバーセキュリティに関するお知らせ

マルウェア「Emotet」の感染被害が拡大
メールの添付ファイルの開封にご注意ください。

JPCERTコーディネーションセンター（JPCERT/CC）によりますと、2019年10月後半より「Emotet（エモテット）」というマルウェアの感染が日本でも拡大しているとして、企業等に注意を呼び掛けています。

Emotetは、主にメールに添付されたWord形式のファイルを開き、コンテンツの有効化を実行することで感染します。メールアドレスやメール本文が窃取されるほか、実在する組織や人物になりすましたメールの送信元にされる被害が発生しています。

マルウェア「Emotet」とは？

Emotetに感染すると、

- 端末やブラウザに保存されたパスワード等の認証情報が窃取される
- 窃取されたパスワードを悪用されネットワーク内に感染が広がる
- メールアカウントとパスワードが窃取される
- メール本文とアドレス帳の情報が窃取される
- 窃取されたメールアカウントや本文などが悪用され、Emotetの感染を広げるメールが送信される

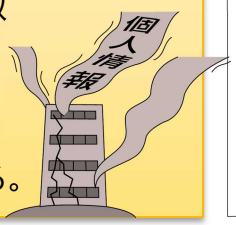
などの被害が発生する可能性があります。

また、Emotetに感染した端末が別のマルウェアをダウンロードしたり、ランサムウェアに感染しデータを暗号化されるおそれもあります。

Emotet感染による実例

2019年10月、某法人において、実在する雑誌社を騙るメールの添付ファイルを職員が開封したところ、法人内に不審なメールが送信された。

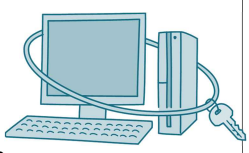
その後の調査結果によると、Emotetに感染し、当該職員とメールの送受信を交わした一部のメールアドレスが窃取されたことが判明。メールボックスには1万件以上の送受信メールが保存されており、外部流出の可能性がある。



Emotet感染予防対策

感染予防対策として下記の事項を検討して下さい。

- **組織内への注意喚起の実施**
- **Wordマクロの自動実行の無効化**
  （マクロの設定で「警告を表示してすべてのマクロを無効にする」を選択）
- **マルウェア検知機能付きメールセキュリティ製品の導入**
- **メールの監査ログの有効化**
- **OSに定期的にパッチを適用**
- **定期的なオフラインバックアップの取得**



詳しくは、JPCERT/CCの公式Webサイト「マルウェアEmotetの感染に関する注意喚起」をご覧ください。
（https://www.jpcert.or.jp/at/2019/at190044.html）

[INFORMATION] Windows7の延長サポートは2020年1月14日で終了します。
終了後はソフトウエア更新等のサポートが受けられません。詳しくは、「Microsoftの公式サイト」で確認して下さい。