2020年８月

サイバーニュース

Emotet感染メールの配布活動が再開!!

ＪＰＣＥＲＴコーディネーションセンターによると、本年２月以降、観測されていなかったマルウェア「Emotet（エモテット）」の感染に繋がるメールの配布が７月後半から再開したとしています。

○ Emotetってどんなマルウェア？

Emotetは、感染した端末の情報窃取を行うほか、窃取した情報を利用してスパムメールを送信し、更に感染拡大を試みる機能などを有したマルウェアです。

○ Emotetの感染経路は？

添付ファイル又は本文中にリンクを含むメールが感染元となります。

添付ファイル又はリンクからダウンロードされるファイルを実行すると、マクロの有効化（コンテンツの有効化）を促す内容が表示され、マクロを有効にすると、Emotetに感染することが確認されています。

なお、Ｅｍｏｔｅｔ の感染に繋がるメールは、実在する複数の企業・団体が送信元となっており、その中には石川県内に実在する企業も含まれています。

○ Emotetへの感染防止対策は？

- 組織内への注意喚起の実施
- Ｗｏｒｄなどオフィスソフトにおけるマクロの自動実行の無効化
- メールセキュリティ製品によるマルウェア付きメールの検知
- メールの監査ログの有効化
- ＯＳへのパッチの適用（ＳＭＢの脆弱性への対策）
- 定期的なオフラインバックアップの実行（ランサムウェアへの対策）

○ Emotetに感染した場合は？

- 感染端末のネットワークからの隔離
- 感染端末が利用していたメールアカウントのパスワード変更
- 組織内全端末のウイルス対策ソフトによるフルスキャン
- 感染端末を利用していたアカウントのパスワードの変更
- ネットワークトラフィックログの監視
- 調査後の感染端末の初期化

詳細についてはＪＰＣＥＲＴコーディネーションセンターのＨＰをご確認ください!!

石川県警察本部生活安全捜査課サイバー犯罪対策室

076－225－0110　　cyber@police.pref.ishikawa.lg.jp