ＩＳＩＳＳ通信

R元.11
Vol.29

Ishikawa Small and Medium Businesses Information Security Support News

マルウェア「Emotet」にご注意!!

JPCERTコーディネーションセンターによると、本年10月後半から、マルウェア「Emotet」の感染に関する相談を多数受理しているとしています。特に**実在の組織や人物になりすましたメール**に添付された**悪質なWord文書ファイル**による感染被害の報告を多数受けているとのことです。

○ 感染経路

主にメールに添付されたWord形式のファイルを実行し、マクロを実行することでEmotetに感染します。

感染に繋がるメールは、Emotetが窃取した情報などを元に独自に作成されるものに加え、**実際のメールのやり取りの内容を転用**することで、**感染元から感染先への返信を装う**ものがあります。そのため、正規のメールに見えても実際にはEmotetによる**なりすましメール**の可能性があります。

○ Emotetに感染した場合の影響

- 端末やブラウザに保持されたパスワードなどの**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SMB(※)により**社内ネットワークに感染**が広がる（※SMBとは、ネットワークを用いてプリンタやファイル共有を利用する際に使用される機能）
- **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(感染元となる)
- Emotetに感染した端末が、別のマルウェアをダウンロードし、その結果、**ランサムウェア(データを暗号化するマルウェア)に感染**する

○ Emotetへの対策

- 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**
- 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**
- OSへの**パッチの適用**(SMBの脆弱性への対策)
- 定期的な**バックアップの実行**(ランサムウェアへの対策)

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!!

サイバー犯罪（インターネットに関する犯罪）の通報やご相談は･･･

石川県警察本部生活環境課サイバー犯罪対策室

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