マルウェア Emotet 2022年3月感染大爆発

取引先、知り合いになりすましたメール起因のマルウェア脅威

610件（2022年2月第一週）

4380件（2022年3月第一週）

- **Emotetに感染すると…**
  - メール関連の情報を窃取（メールアカウント、メール本文、アドレス帳など）
  - 感染の拡大（メールを拡散）
  - 様々なサービスの認証情報窃取（ブラウザ保存のID、パスワードなど）

  - 他マルウェアの感染踏み台
    - データ暗号化によるデータの人質（ランサムウェア）
    - オンラインバンクなどの金銭の窃取
    - 遠隔操作・トロイの木馬（RAT）

    など

©2022 – Vade

マルウェア Emotet の特徴

特徴１．正規メールの返信を装う　開封率が極めて高い

- **実際のメールアカウントを利用して送られる**
  - 人の警戒心および従来型検知をすり抜ける可能性が極めて高い

- **差出人・件名・本文・ファイル名などに受信者と関係のある文言を使う**
  - 件名に「過去メールを引用」、「汎用的なビジネス文言」、「受信者の名前」など

特徴２．パスワード付 zipファイル　PPAPへの慣れ

- 既存エンドポイントなどのシグネチャソリューションでは対応できない
- EDRなどのソリューションでも発症するまで検知できない可能性あり

特徴３．感染していないのに送信元名に悪用される場合あり

©2022 – Vade

マルウェア Emotet の一例（2022年3月）

©2022 – Vade

マルウェア Emotet の一例（2022年3月）

マルウェア

未処理

3月 [redacted]

2022 [redacted]

差出人 [redacted]

宛先 [redacted]

件名 Fwd:清水 [redacted]

添付ファイル

SY9540298873_202203011247.zip

・件名に名前（受信者名）が入るパターンも多く確認
・Re:***、Fwd:***、空件名　（***は受信者名）

・ファイル名、ファイル種類はさまざま
・YYYY-MM-DDの形式を多く確認
（自動で日付情報付与するファイルサービスを模倣？）

高脅威スパム

削除済み

2月 [redacted]

2022 [redacted]

差出人 [redacted]

宛先 [redacted]

件名 Re: Masaki, [redacted]

添付ファイル

2022-02-08_1654.zip

©2022 – Vade

マルウェア Emotet への対策

Emotet はメール起因の脅威です。
予防的対策であり入口対策であるメールセキュリティは Emotet 対策に最も投資対効果が高いソリューションです。

「予防」か「発見」か

メールセキュリティは脅威が発現する前に捕らえる予防的対策です。一方で、EDRやSIEMなどは主に脅威が活動してから捕らえる「発見的対策」ソリューションです。どちらも同じ脅威に対応できるとすると、「予防的対策」が簡単で即効性があり、投資対効果が高いソリューションになります。

「入口近くで」か「組織内で」か

メールセキュリティは組織の入り口近くで脅威検知を行うソリューションです。一方で 、EDR などは組織内に入った後に脅威検知を行うソリューションです。どちらも同じ脅威に対応できるとすると、入口付近で行うほうが簡単で、かつ投資対効果も高いソリューションです。

©2022 – Vade