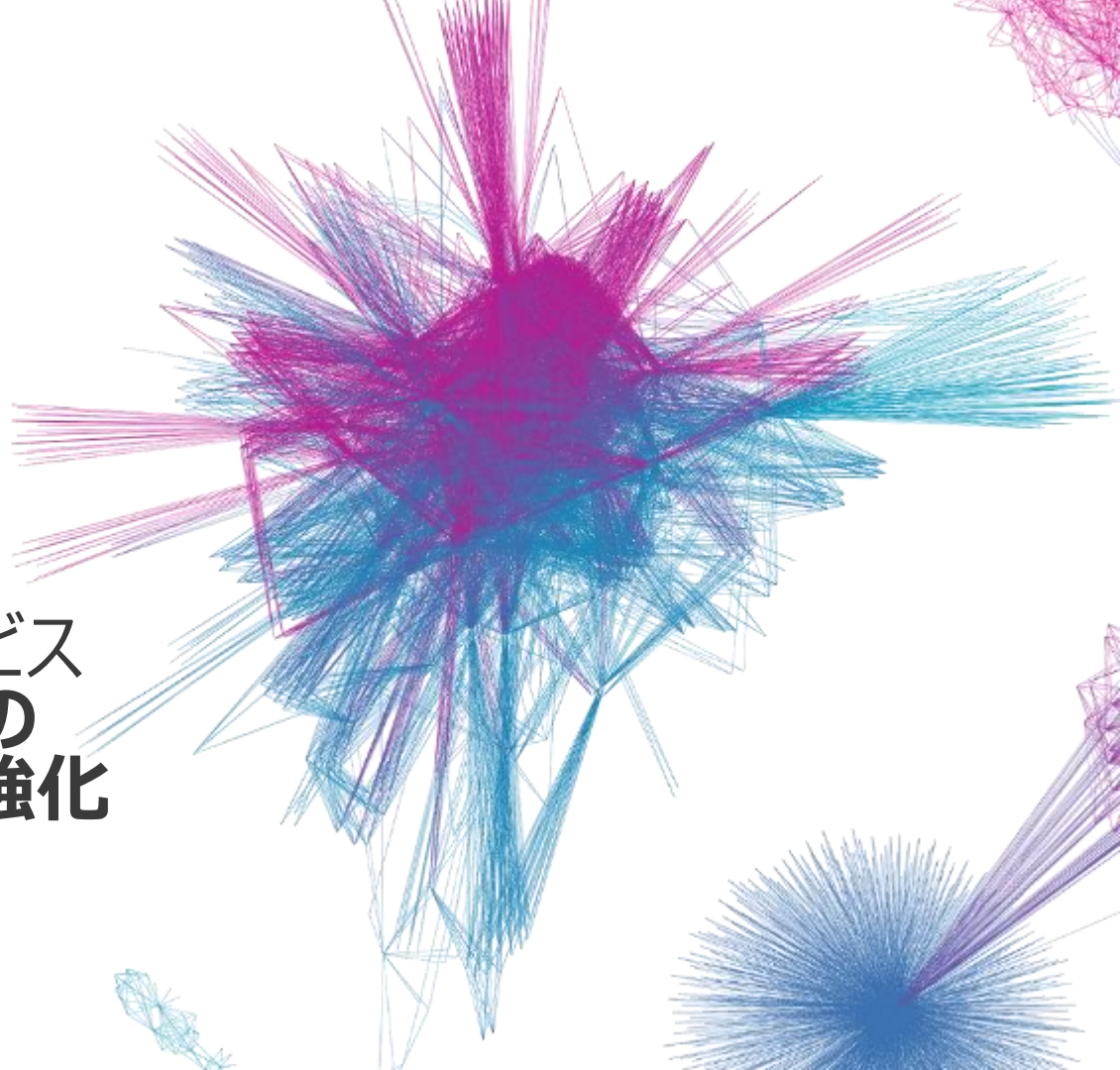




ウイルスバスター ビジネスセキュリティサービス EMOTET対策のための リアルタイム検索機能強化

トレンドマイクロ株式会社





はじめに

本資料は、マルウェア「EMOTET」へのさらなる対策を主目的として2022年5月23日リリースされる予定のリアルタイム検索の機能強化(CVEセキュリティホールの検索)について記載した資料です。

本資料に記載のマルウェアの拡散手法は、現時点でのものであり今後変化する可能性があります。

用語と略語

用語や略称	正式名称、または用語の意味
VBBSS	ウイルスバスター ビジネスセキュリティサービス
CVE	Common Vulnerabilities and Exposures

改訂履歴

バージョン	公開日/作成日	改定内容
1.0	2021/5/17	初版として作成



EMOTETとは

「EMOTET」（エモテット）は、ExcelやWordファイルなどのマクロ機能を悪用したマルウェアで、最近では2022年2月にEMOTETによる急速な感染拡大が確認されています。

感染により、情報流出、スパムメールに利用される、ランサムウェアといった別マルウェアの感染に繋がるといった被害を引き起こすことで知られています。

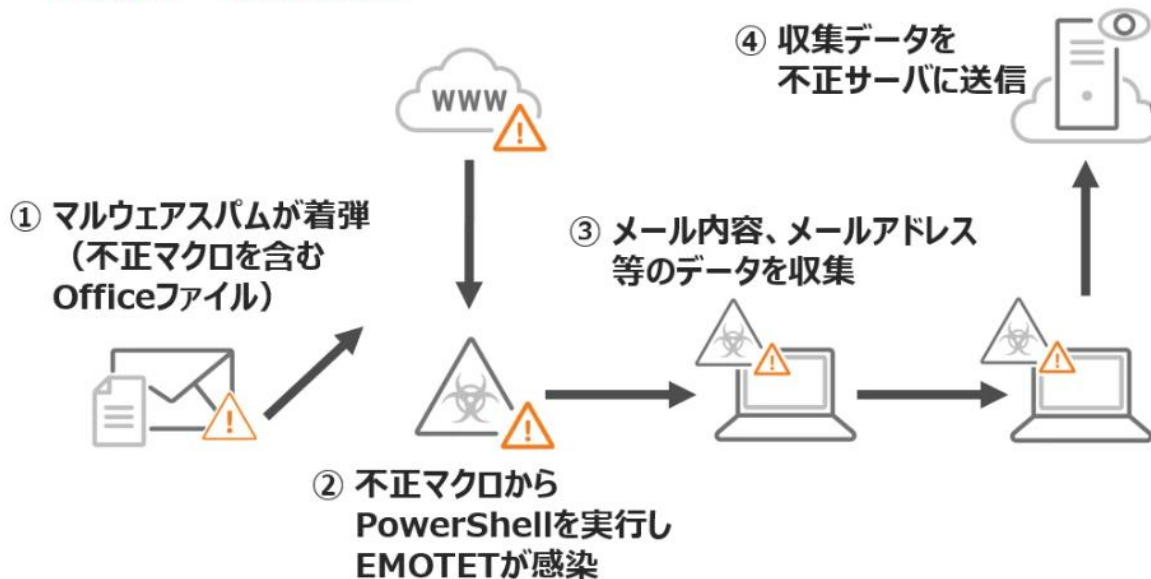
具体的な攻撃内容や対策については、以下をご参照ください。

EMOTET概要から対策まで)

https://www.trendmicro.com/ja_jp/business/campaigns/emotet.html

参考) EMOTETの拡散手法

● 感染→情報窃取



● 窃取情報を元に拡散




※EMOTET概要から対策まで) https://www.trendmicro.com/ja_jp/business/campaigns/emotet.html (参照 2022/5/16)

リアルタイム検索の機能強化(CVEセキュリティホールの検索)

共通脆弱性識別子(CVE) システムに基づいて、Webおよびメールからダウンロードした文書ファイルに埋め込まれた攻撃コードおよび既知の脆弱性を検索する機能が、リアルタイム検索に追加されます。

本機能についての設定項目はありません。リアルタイム検索が有効であれば、本機能も有効になります。

※今後のリリースでは、この機能の設定を管理コンソールで行えるようにする可能性があります

 ウイルスバスター ビジネスセキュリティサービス

🕒 16:58 UTC+09:00

☰ ? 📄

ログ

日時: 受信 ▼

セキュリティリスクの検出: すべて ▼ 📅 過去7日間 ▼ 脅威/違反

2件 📄 エクスポート

受信	カテゴリ	脅威/違反 ↓	ユーザ	詳細
2022年04月20日 16:54:56	ウイルス/不正プログラム	HEUR_XLSB.XLM	Administrator	📄 ▶
2022年04月20日 16:54:56	ウイルス/不正プログラム	HEUR_XLSB.XLM	Administrator	📄 ▶

本機能はヒューリスティック検出のため、検出ログには「HEUR_」のように、ヒューリスティック検出を示す接頭辞が付きます。

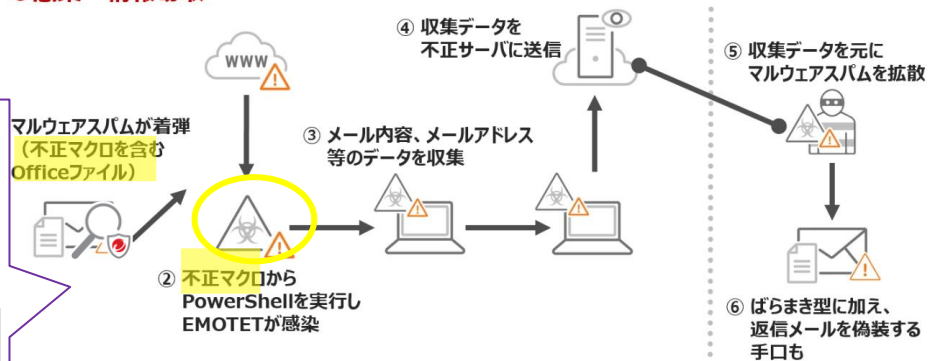
本機能によるEMOTET対策強化のポイント

メール添付またはメール本文中のダウンロードURLを経由して、ExcelやWordのマクロ機能を悪用した文書ファイルなどを送り付け、それを開きマクロを有効化することでEMOTETに感染してしまいます※¹。最近では、Windowsのショートカットリンク(.lnk) ファイルを悪用したファイルも確認されています※²

本機能は、このようなマクロ付きの不審な文書ファイルやショートカットリンクファイルの実行をブロックすることができます。

● 感染→情報窃取

● 窃取情報を元に拡散



本機能により、
メールの添付ファイルやメール本文内のURLリンクからダウンロードされたマクロ付きのOfficeファイルやショートカットリンクファイル(lnkファイル)の検索/ブロック力を強化！

【文書ファイルを送り付ける手法】※¹



※¹ 拡散手法は今後変化する可能性があります。

※² トレンドマイクロ セキュリティブログ <https://blog.trendmicro.co.jp/archives/31142> (参照 2022/05/16)

Copyright © 2022 Trend Micro Incorporated. All rights reserved.



EMOTET対策 推奨設定

VBBSSではEMOTET対策として、リアルタイム検索機能に加え、挙動監視、機械学習型検索、Webレピュテーションを活用した防御を推奨しております。

この機会に、各機能が有効になっているか設定をご確認ください。

EMOTET概要から対策まで「各製品の推奨設定」)

https://www.trendmicro.com/ja_jp/business/campaigns/emotet.html



THE ART OF CYBERSECURITY

An Innovative Approach to Cybersecurity

トレンドマイクロのクラウドセキュリティプラットフォームによる、日本におけるハイブリッドクラウドワークロードの自動保護。実際のデータを使用し、トレンドマイクロの脅威リサーチャーでアーティストでもあるJindrich Karasekによって作成されました。