新型Emotetが再流行！
その原因と対策

第1.2版

2022年6月

ソリューション営業本部

© SECOM Trust Systems CO., LTD.
お客様専用の資料となりますので、第三者への開示・転用はお控えください

なぜまたEmotetが流行っているのか？

「新種のマルウェア」ではなく「新型」「再開」⇒　つまり手口は同じ

＜Emotetの歴史＞

2019年11月　　メディアで取り上げられる
↓
2020年9月～11月　**世界的に大流行**
↓
2021年1月　　欧州刑事警察機構（EUROPOL）によるC2サーバーのテイクダウン
↓
2021年11月　　C2サーバーなど再構築して**活動再開**
↓
2022年2月～　　再び猛威を振るう

© SECOM Trust Systems CO., LTD.　お客様専用の資料となりますので、第三者への開示・転用はお控えください

Emotet再流行の理由

１．典型的な感染経路

・メールで広まるばらまき型。
・珍しい手口ではないが、Emotetが過去に残した歴史や被害が物語る。

２．更なる工夫の追加

・毎日変化を加えている。
・Wordマクロ(.docm)だけではなくExcelマクロ(.xlsm)も利用。
・アプリ（PDFリーダー）のインストールを装う手口も。
・ショートカットファイル（.lnk）を添付する手口も。
・自然な日本語の文面で不審さを感じにくい。
・HTTPSを利用。

３．根本的な対策がまだ取れていなかった

・喉元過ぎれば。。。
・原因としてはこれが一番大きいのでは。。。

© SECOM Trust Systems CO., LTD.
お客様専用の資料となりますので、第三者への開示・転用はお控えください

Emotetの「更なる工夫」とは？？

◆毎日変化を加えている

・パターンマッチング型ウイルス対策ソフトでは検知出来ない。
・次にどのような手口で来るのか予測できない。いたちごっこ。

◆メールの添付ファイルがセキュリティをすり抜ける

・ZIP暗号化ファイルのメール添付（いわゆるPPAP）を廃止する流れも。

◆WordだけでなくExcelのマクロを利用、更にアプリのインストーラーを偽装

・WordよりもExcelでマクロを使用するユーザーが多い。
・Wordのマクロは無効化していても、Excelのマクロは業務上使う人が多いことを狙ったか？
・アプリ（PDFリーダー）のダウンロードを偽装。スマホアプリの感覚でインストールしてしまう。
・ショートカットファイル（.lnk）を添付してPowerShell／VBScriptを実行させる手口も登場。
・メール本文に自然な日本語、差出人が知り合い（偽装の場合もあり）等、不審さを感じにくい。

◆HTTPSを使用

・通信の特徴をもとにC2通信を見つけ出すことが難しくなった。
・UTMやプロキシサーバーのウイルススキャンを素通り。　※既にトラフィックの95%がHTTPS化
・しかしSSLデコード（復号）ができている企業はまだまだ少ない。

© SECOM Trust Systems CO., LTD.　お客様専用の資料となりますので、第三者への開示・転用はお控えください

Emotetに対する「根本的な対策」がまだ取れていないのでは？？

新型になったとはいえ、

これまで通り一般的なマルウェア対策を確実に、粛々と行っていただく

「Emotetの感染を予防、あるいは仮に感染した場合に被害を最小化する」ための方策

- 組織内への注意喚起の実施
  →不審なファイルは開かない、URLをクリックしない、知ってる人からのメール返信でも
- Word マクロ、Excelマクロの自動実行の無効化
  →ADグループポリシーで適用、資産管理ツールで確認
- メールセキュリティ製品の導入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に定期的にパッチを適用（OSの脆弱性対策）
- 定期的なオフラインバックアップの取得
  →マルウェア対策としてだけでなく一般的にやっておくべき

出典：JPCERT/CC マルウエア Emotetの感染に関する注意喚起(2019/11/27)をもとに加筆修正
https://www.jpcert.or.jp/at/2019/at190044.html

© SECOM Trust Systems CO., LTD.
お客様専用の資料となりますので、第三者への開示・転用はお控えください

では「根本的な対策」とは？

信頼される安心を、社会へ。
SECOM
セコムトラストシステムズ株式会社

これが決め手！

◆NGAV＋EDR＋SOC

- 感染ポイントはPCです。PCを監視して守る。
- 日々変化するウイルスには実際の挙動を監視する「振る舞い検知」で対応。
- 検知後もサポートしてくれること。（初動対応、誤検知の見極めなど）
- 導入までに必要となる作業や、日々の運用についても確認しておく。

多層防御（網掛け）の観点から推奨される対策

◆SWG

- トラフィックの監視と怪しい通信のブロック。
- SSLデコード（復号）対応。（EmotetもHTTPSを使用）　※オンプレ型では処理能力の観点で復号対応が困難
  →クラウド型SWGが主流

◆メールサーバーへのDMARC導入

- 差出人を偽装したメールをブロック。（ばらまき型メールに効果あり）
- 現在利用中のメールサーバーが対応しているか確認。（Exchange Online、Google等は対応済み）

◆点ではなく面での網羅的なセキュリティ強化

- セキュリティの課題は他にもあり、長期目線で継続的に脆弱性の潰し込みを行う。（リスク分析）

© SECOM Trust Systems CO., LTD.　お客様専用の資料となりますので、第三者への開示・転用はお控えください

セコムトラストシステムズ株式会社

www.secomtrust.net

お問い合わせ

ソリューション営業本部
03-5931-5210
受付時間：9～12時・13時～18時
土・日・祝日・年末年始（12/30～1/3）は除きます。

© SECOM Trust Systems CO., LTD.
お客様専用の資料となりますので、第三者への開示・転用はお控えください