NTTデータ先端技術の セキュリティ

NTT DATA
Trusted Global Innovator

INTELLILINK セキュリティ情報配信サービス
注目されているセキュリティ事故・事件に関する情報
＜2022年12月版 (第43号)＞(選り抜き版)

2022年12月27日
ＮＴＴデータ先端技術株式会社
サイバーセキュリティ事業本部

今回のサマリー

「Emotet」感染再拡大に関する注意喚起

2022年7月13日頃から観測されていなかったEmotetと呼ばれるマルウェアの攻撃メールの配信が、2022年11月2日から新規の攻撃手法を用いて再開されていることが観測されました。本記事ではEmotetの新規攻撃手法を紹介するとともに企業での対策について改めて解説します。

「Emotet」感染再拡大に関する注意喚起

1. はじめに

2022年7月13日頃から観測されていなかったEmotetと呼ばれるマルウェアの攻撃メールの配信が、2022年11月2日から新規の攻撃手法を用いて再開されていることが観測されました。

Emotetの活動再開については、セキュリティベンダだけでなく、NISC、警察庁、IPA、JPCERT/CCも注意喚起を出しています。

また、2022年12月21日にAIG損害保険株式会社が代理店のパソコンがEmotetに感染したことによる個人情報の漏えいについて発表するなど、実際に被害が発生しています。

本記事ではEmotetについて以下の順で解説します。

- 「Emotet」とは
- Emotetの新規攻撃手法
- Emotetに感染してしまった場合の対処法
- Emotetへの感染を防ぐ対策

2. 「Emotet」とは

■ 「Emotet」とは

Emotetは2014年頃に初めて観測されて以降、何度か活動停止してはいますが形を変えながら長期間活動しているマルウェアであり、メールアカウントとパスワード、アドレス帳などの情報を抜き取るマルウェアとして知られています。

Emotetの実態は攻撃者からの不正なメールに添付されるファイルを実行することで感染するマルウェアです。しかし、ファイルそのものに悪性の挙動を示す機能はなく、適宜C2からの指令を受けて動作します。

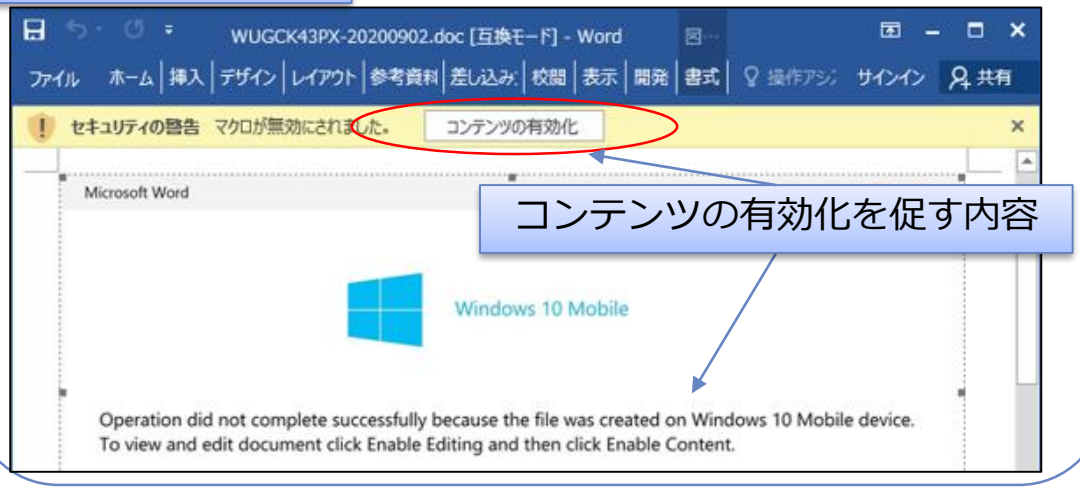
また、モジュール型の構造で汎用性が高い特性を持つため、モジュールを送り込まれて起動されたときにどのようなアクションが起きるか予想することが難しく、検知や事前の対策が困難となる可能性があります。

結果として、個人情報の窃取、なりすまし、ランサムウェア感染被害からの身代金の要求など、攻撃者の意図によって様々な被害がもたらされます。

3. Emotetの新規攻撃手法 (1/2)

　メールに添付されたファイル内に書かれている偽の指示が、これまではコンテンツの有効化を促す内容でしたが、新規のEmotetでは特定のフォルダへのファイルの移動を促す内容に変化しました。

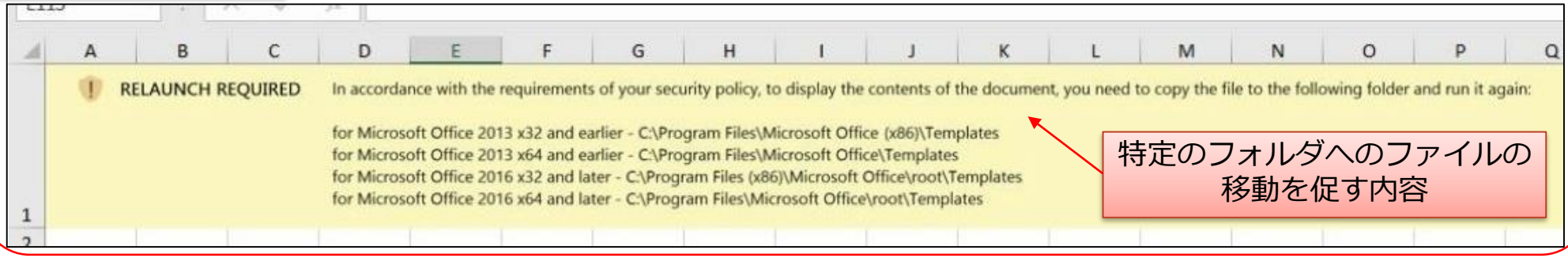
これまでの攻撃手法



コンテンツの有効化を促す内容

Emotetの添付ファイルに書かれている偽の指示は、あたかもシステムやMicrosoft Officeが表示しているように見せかける文面となっています。

新規の攻撃手法



特定のフォルダへのファイルの移動を促す内容

出典：マルウェアEmotetの感染再拡大に関する注意喚起：https://www.jpcert.or.jp/at/2022/at220006.html
出典：Emotet（エモテット）と呼ばれるウイルスへの感染を狙うメールについて：https://www.ipa.go.jp/security/announce/20191202.html

3. Emotetの新規攻撃手法 (2/2)

添付ファイルの偽の指示に従って、Templatesフォルダにファイルをコピーして開くと、マクロを無効化する設定にしていてもファイルに含まれている悪意のあるマクロが強制的に実行されてしまいます。

これは、コピー先のTemplatesフォルダが『信頼できる場所』としてMicrosoft Officeのデフォルトで設定されているためで、このフォルダに格納されたファイルは安全性の高いファイルとみなされ、マクロが実行可能になります。

例）Microsoft Office 2016 (64bit)Excelの 『信頼できる場所』

- %ProgramFiles%¥Microsoft Office¥Templates¥
- %AppData%¥Roaming¥Microsoft¥Templates¥
- %AppData%¥Roaming¥Microsoft¥Excel¥XLSTART¥
- %ProgramFiles%¥Microsoft Office¥Office16¥XLSTART¥
- %ProgramFiles%¥Microsoft Office¥Office16¥STARTUP¥
- %ProgramFiles%Microsoft Office¥Office16¥Library¥

また、類似した手法として、 2022年9月版(第42号)の記事では「Microsoft Officeのスタートアップ機能を悪用したマルウェア」を紹介しました。こちらは Microsoft Officeのスタートアップ機能を悪用することで悪意のあるマクロをMicrosoft Excelを起動する度に強制的に実行するものです。

今回とりあげた事例はEmotetをTemplatesフォルダへの配置を促す内容ですが、仮にスタートアップフォルダへの配置を促す内容だった場合、Microsoft Excelを起動する度にEmotetが起動することになります。

4. Emotetに感染してしまった場合の対処法

Emotetは他のマルウェアを感染させる機能や情報窃取機能を有する場合があります。そのため、「Emotet本体の駆除」と「Emotetによる二次被害の対策」の両面を実施することが求められます。

Emotet本体の駆除

- **感染源となったメールなどの削除**
- **感染端末でのEmoCheck(※)の実行**
- **感染端末でのマルウェアスキャン**
- **『信頼された場所』に不審なファイルが存在するかの確認、不審なファイルがあれば削除**

今回の攻撃手法で追加した対策

Emotetによる二次被害の対策

- **感染端末で使用していたメールアカウント、サービスなどのパスワード再設定**
- **感染端末以外でのEmoCheck実行**
- **感染端末以外でのマルウェアスキャン**
- **適切な情報公開によって、取引先などの関係者に自組織を騙ったEmotetが来る可能性をお知らせする**

※「Emocheck」とはJPCERT/CCが提供するEmotetの感染有無を確認できるツールで、以下からダウンロードが可能です。
https://github.com/JPCERTCC/EmoCheck/releases

5. Emotetへの感染を防ぐ対策 (1/2)

Emotetによる攻撃は手法を変えながら今後も続くと考えられます。Emotetの感染を防げるよう以下の対策を実施することをお勧めします。

Emotetの感染を防ぐための対策

- **Microsoft Officeの設定で文書ファイルのマクロを無効にする※**
- **スクリプトファイル(PowerShell、Wscriptなど)の実行を無効にする※**
- **不必要なアプリケーションからの外部への通信をWindowsファイアウォールでブロックする**
- **メールに添付されたファイルや、本文に記されたリンクを不用意に実行/クリックしないように、定期的にユーザ教育を実施する**
- **OS/アプリケーション/ウイルス対策ソフトを最新の状態に保つ**
- **グループポリシーで“信頼できる場所”を無効化する※**
- **グループポリシーでMicrosoft Officeのスタートアップ機能を無効化する※**

今回の攻撃手法で追加した対策

※当該対策を実施する際は、業務に影響を与えないことを確認した上で、実施することをお勧めします

5. Emotetへの感染を防ぐ対策 (2/2)

　また、Emotetだけに限らず他のマルウェアの攻撃へ備えるためにもマルウェア感染対策を常に実施することが大切です。

マルウェア感染後の被害極小化を図る一般的な対策

- **ネットワークセグメントの分割とアクセス制御リスト(ACL)の最小化**
  ネットワークを細分化し、ネットワーク間の通信を必要なもののみに制限することで、感染拡大の防止と業務影響の最小化が期待できます。
- **ユーザに与える権限の最小化**
  共通ファイルサーバへのアクセス権や端末の管理者権限を最小限に抑えることで、不正なファイルの読み書きや設定変更の防止が期待できます。
- **定期的なバックアップ取得**
  ランサムウェアに感染しファイルが暗号化されてしまったとしても、感染する前の状態に戻すことができます。
- **EDRによる自動的な端末のネットワーク切り離し**
  感染端末から他の端末への感染拡大、インターネット上のC2サーバへのアクセスなどを防止できます。
- **マルウェア感染を想定した訓練の実施**
  マルウェア感染に備えて、各種ログや受信メールのアーカイブなど感染ルートを明らかにするための情報の確保や、確保したログの分析、ログの分析結果に即した対応を行えるように訓練を行うことで、被害をより小さくすることが期待できます。

6. まとめ

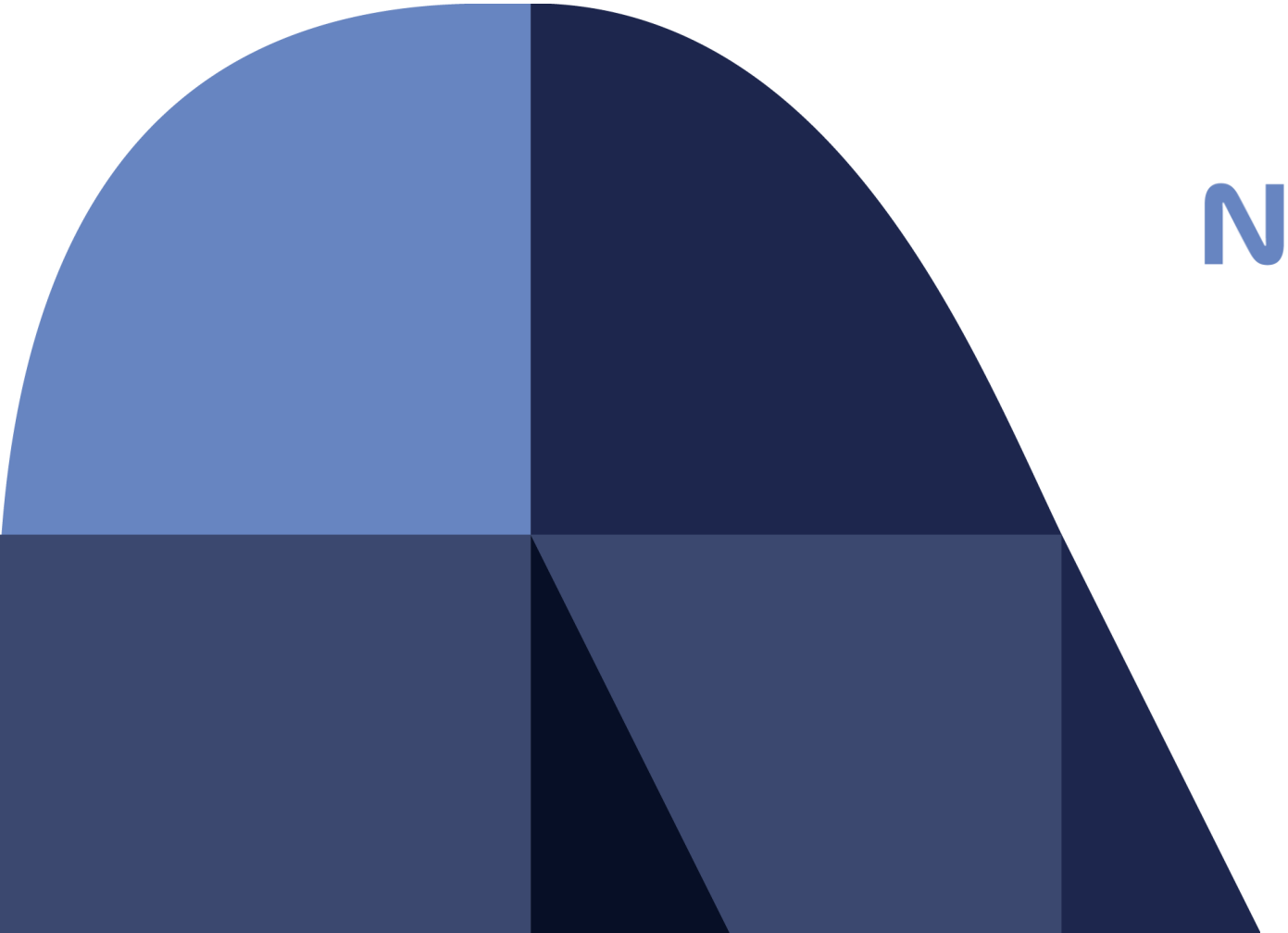
Emotetは攻撃者からの不正なメールに添付されるファイルを実行することで感染するマルウェアで、ファイルそのものに悪性の挙動を示す機能はなく、適宜C2からの指令を受けて動作します。

また、モジュール型の構造で汎用性が高い特性を持っているため、攻撃者によって新規の機能を持たせることができます。実際に、2022年11月2日から新規の攻撃手法を持つEmotetによる攻撃メールの配信が観測されていますので今後も手法を変えながら攻撃が続くと考えられます。

そのため、Emotetだけでなく、Emotetで利用される可能性がある脆弱性や攻撃手法の情報についても、常に最新情報を収集し継続して対策を実施していくことが大切です。

7. 参考URL

- Emotet（エモテット）と呼ばれるウイルスへの感染を狙うメールについて
  https://www.ipa.go.jp/security/announce/20191202.html
- マルウェアEmotetの感染再拡大に関する注意喚起
  https://www.jpcert.or.jp/at/2022/at220006.html
- マルウェアEmotetの活動再開に関する注意喚起について
  https://www.npa.go.jp/cybersecurity/pdf/20221104press.pdf
- メールをばらまくマルウェアEmotetが活動再開
  https://www.nisc.go.jp/pr/column/20221108.html
- 当社代理店における個人情報漏えいについて
  https://www.aig.co.jp/sonpo/company/news/2022/20221221-01



NTT DATA

Trusted Global Innovator