注目されているセキュリティ事故・事件に関する情報 ＜2021年6月版 (第37号)＞(選り抜き版)

2021年6月29日
ＮＴＴデータ先端技術株式会社
セキュリティ事業本部

今回のサマリー

総務省などによるEmotet感染端末利用者への注意喚起が開始
2020年度はコロナ禍に便乗しEmotetの脅威が拡大した一年でした。その中で、総務省/警察庁/ICT-ISACは、2021年2月末よりEmotet感染端末の利用者に向けた注意喚起を開始すると発表しました。2020年度のEmotetの動向と企業での対策について改めて解説します。

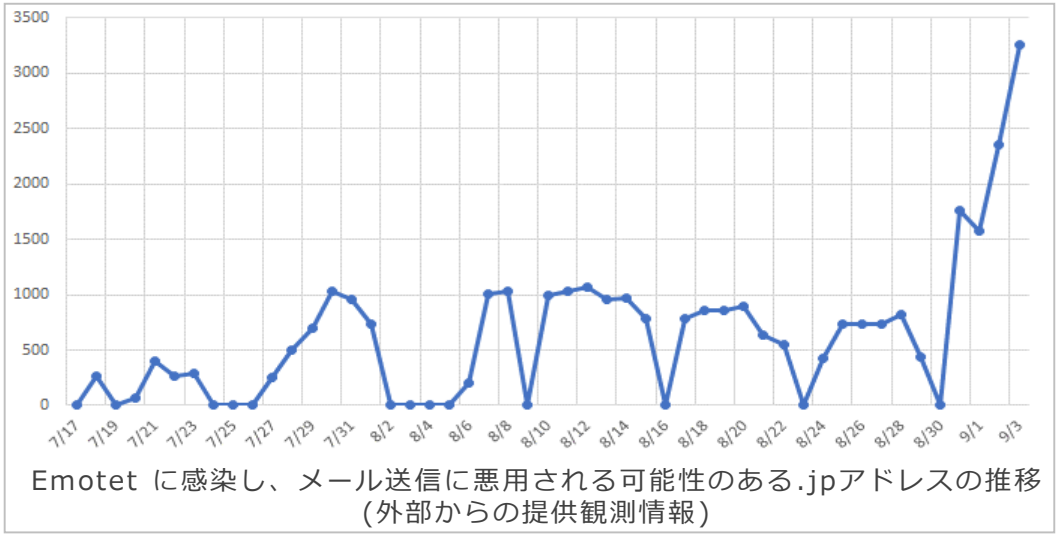
総務省などによる
Emotet感染端末利用者への
注意喚起が開始

1. 2020年度のEmotet動向 (1/2)

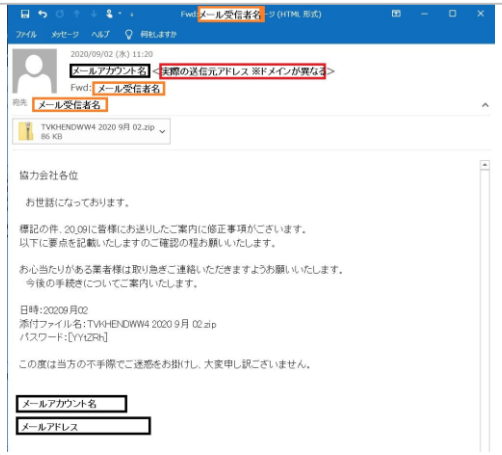
2020年度は世界各国でEmotetの脅威が拡大した一年でした。Emotetは主にメールを使用して感染拡大を試みますが、7月～9月には日本国内で新たな手法が登場したことで、被害を受ける企業も多数発生しました。

【7月～9月で観測された新たな手法】

- コロナ禍に便乗したメール文面で添付ファイルを開かせる手法
- メールの添付ファイルをパスワード付きzipで送ること(いわゆるPPAP)で、セキュリティ機器の検知/受信者の警戒感をすり抜ける手法



Emotet に感染し、メール送信に悪用される可能性のある.jpアドレスの推移
(外部からの提供観測情報)



パスワード付き zip ファイルが添付された
Emotet のメール例

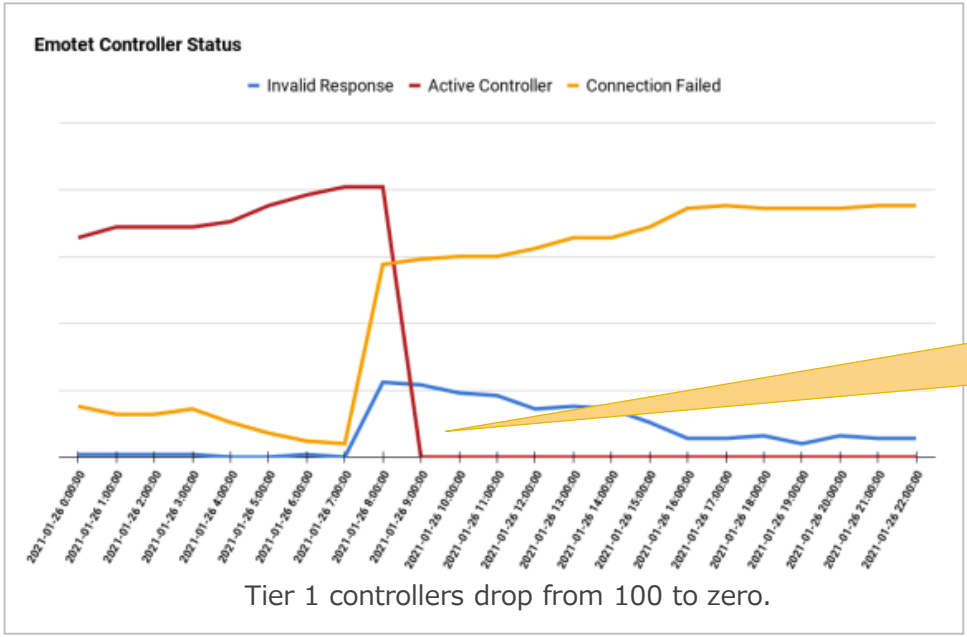
引用：JPCERT/CC「マルウェア Emotet の感染拡大および新たな攻撃手法について」
<https://www.jpcert.or.jp/newsflash/2020090401.html>

1. 2020年度のEmotet動向 (2/2)

Emotetの急速な感染拡大が話題となった一方で、Emotetの脅威を断ち切る活動も進められました。

2021年1月には、ユーロポール(欧州刑事警察機構)が調整し、8か国の司法機関が連携してEmotetのC2サーバが稼働するアジトを壊滅させる作戦が行われました。

セキュリティ企業のTeam Cymruによる調査では、この作戦により、稼働中のC2サーバが0になった(テイクダウンした)と報告しました。壊滅作戦が一定の効果を上げたと言えます。



壊滅作戦により、2021年1月26日以降、稼働中のC2サーバが0件になった

引用：Taking Down Emotet
<https://team-cymru.com/blog/2021/01/27/taking-down-emotet/>

2. 参考：Emotetとは

Emotetは、2014年ごろに初観測されたマルウェアです。当初はバンキングマルウェアとして、オンラインバンキングなどの認証情報の窃取のみを行うマルウェアでした。しかし、昨今では、様々なマルウェアの感染/拡散を行うためのプラットフォームマルウェアとして猛威を振るっています。

Emotetは一般的に以下の特徴を持っています。

Emotetの主な特徴

1. **悪性の挙動を示す機能を、本体ではなくモジュールとして実装**
   過去のメールのやり取りの窃取、認証情報の窃取、他のマルウェアへの感染など、様々な機能を後付け(拡張)することが容易

2. **本体およびモジュールは攻撃者が任意のタイミングでアップデートすることが可能**

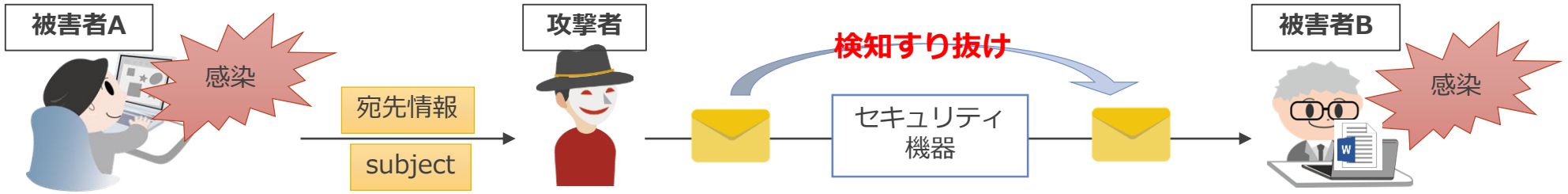
3. **本体に悪性の挙動を示す機能がないため、ウイルス対策製品に検知されにくい**

4. **モジュールはファイルとして保存されず、メモリ上にのみ展開されるため、解析されにくい**

3. 参考：Emotetの感染経路

Emotetの主な感染経路はメールの添付ファイルです。感染端末で過去にやりとりされたメールを引用し、あたかも正規のやり取りのように見せかける手法で相手をだまし、添付ファイルを開かせて感染を拡大しました。2020年の夏頃からは、添付ファイルがパスワード付きzip化されたことで、セキュリティ機器での検知や受信者の警戒感をすり抜けるようになり、結果として感染拡大を後押ししました。

Emotetの感染の流れ



1. 「Emotet」に感染することで、攻撃者にメールの宛先情報や、subject(題名)が窃取される

	2. 攻撃者は窃取したメールの宛先に対してメールを送付する。	3. メールに添付されたWord(MS Office)ファイルを開くことによりマクロが実行され、「Emotet」がダウンロードされることにより感染する。
～2020年6月		
2020年7月～	添付ファイルがパスワード付きzipとなり、セキュリティ機器での検知が困難になった。	「マルウェアがパスワード付きzip かつPPAPで来ることはないだろう」という受信者の先入観により、zip内のWordファイルを開いてしまう。

4. 総務省などによるEmotet感染端末利用者への注意喚起 (1/2)

2021年1月に行われたEmotetのC2サーバのテイクダウンにより、攻撃者から直接Emotetの制御を行うことは事実上できなくなったと言えます。しかし、Emotetは多機能なマルウェアであり、既に感染している端末が存在する場合、以下の二次被害が発生している可能性もあります。

①：その端末から認証情報が窃取され悪用されている可能性

②：他のマルウェアの感染、別端末への感染拡大が発生している可能性

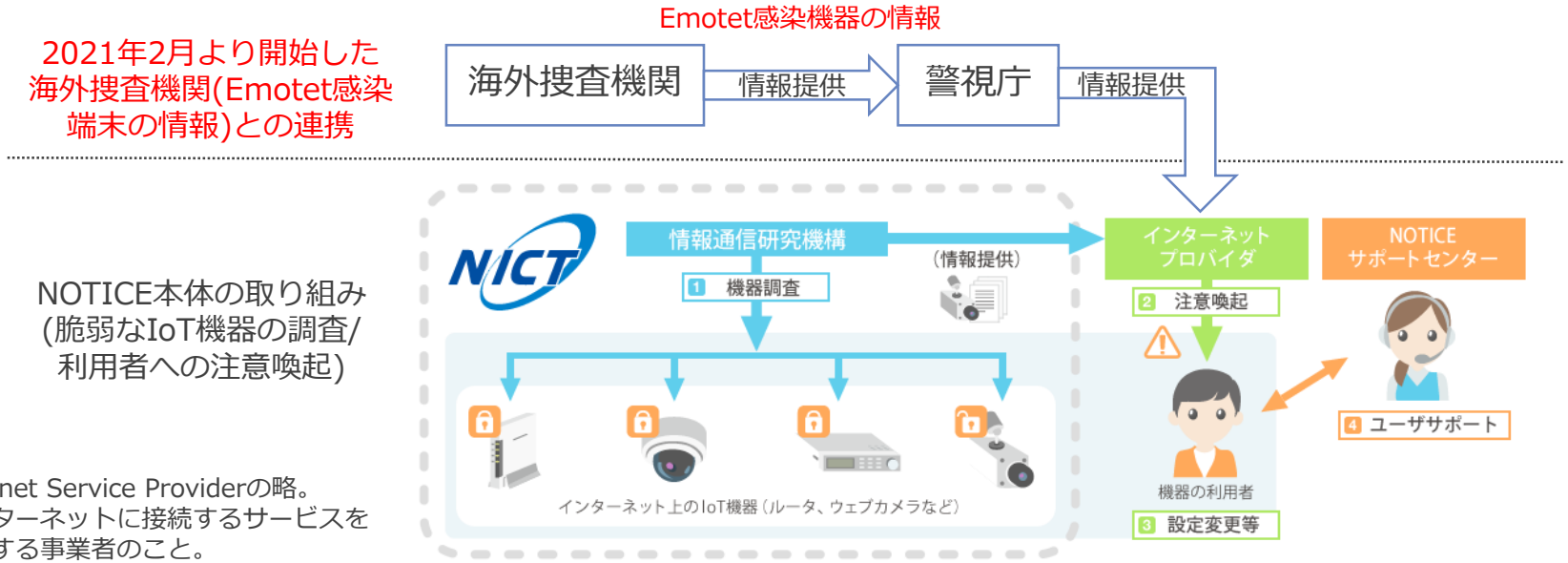
Emotet感染による影響を最小化するため、総務省/警察庁/ICT-ISACは2021年2月末より、NOTICEの仕組みを活用したEmotet感染端末利用者への注意喚起を開始しました。

4. 総務省などによるEmotet感染端末利用者への注意喚起 (2/2)

そもそもNOTICEとは、総務省/NICT/ISP(※1)が連携し、サイバー攻撃に悪用される可能性がある「脆弱なIoT機器の調査」を行い、その機器の利用者へ「注意喚起」する取り組みです。

Emotet感染端末利用者への注意喚起には、このNOTICEの仕組みが活用され、海外の捜査当局から得たEmotet感染機器の情報をもとに、ISP経由で感染端末の利用者に注意喚起が通知されます。

なお、ISP経由での注意喚起であるため、企業においては端末利用者ではなく、インターネット回線の契約名義人(情報システム部門や総務部門など)に通知が届く可能性があります。



※1 Internet Service Providerの略。
インターネットに接続するサービスを
提供する事業者のこと。

5. 企業に求められる対応 (1/3)

ISPより注意喚起を受け取った場合は、Emotetの感染端末が存在している可能性が高いと推測されます。また、Emotetは他のマルウェアを感染させる機能や情報窃取機能も有する場合があります。このため、「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

- **感染端末でのEmoCheck(※1)の実行**
- **感染端末でのマルウェアスキャン**

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**

※1 マルウエアEmotetへの対応FAQ
2. Emotet の感染有無を確認するためにはどうすればよいですか?
<https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html#2>

5. 企業に求められる対応 (2/3)

　また、EmotetのC2サーバがテイクダウンされたとはいえ、新たなC2サーバや攻撃手法が登場する可能性もあります。Emotetに限らず一般的なマルウェア感染対策は常に実施することが大切です。

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**

※本対策を実施することで文書マクロや、スクリプトの実行が無効になるため、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

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。
- **定期的にバックアップを取得しておく**
  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。

5. 企業に求められる対応 (3/3)

NOTICEを活用した注意喚起は、外部の組織から「直接」かつ「具体的」な通知が届くこれまでにない取り組みとも言えます。一方で、自組織のインシデントに関する情報を他組織から受け取った場合を想定した準備をしておかなければ、迅速かつ適切な対応はできません。そのため、以下の検討をお勧めします。

検討すべき事項

- **外部からの通知の受付や、他部署が受け取った情報の集約をする窓口となり、インシデント対応を主体的に行うためのCSIRTのような体制や組織の整備**
  通知先は必ずしも情報システム/セキュリティ部門とは限りません。契約名義によっては、総務/法務など様々な組織に通知が飛ぶ可能性を考慮して体制を構築する必要があります。

- **体制や組織を形式だけにとどめず、有事の際に適切に対応できるように訓練を実施**
  社内外の複数の部門間での情報伝達や有事の際のサービスの継続判断など、インシデント対応マニュアルやBCPなどに従って適切に対応ができるか、訓練を通じて実際に確認します。確認の結果、必要に応じて体制やマニュアルの修正も行います。

6. まとめ

2020年度はコロナ禍に便乗しEmotetの脅威が拡大した一年でした。新たな手法が登場したことも相重なり、国内でも被害を受ける企業が多数発生しました。一方で、2021年1月には、ユーロポールによってEmotetのC2サーバがテイクダウンされました。また、国内においては、同年2月からNOTICEの仕組みを活用したEmotet感染端末利用者への注意喚起が行われました。

現状、このような取り組みにより、Emotetの感染端末数は大幅に減少し、Emotetの猛威は沈静化した状態となっています。しかし、新たなC2サーバや攻撃手法が登場する可能性は否定できません。マルウェアの感染や、感染した際の影響を最小限に抑えるため、日頃のセキュリティ対策が重要になります。

なお、今回の国内での注意喚起は、「他組織から自組織に対する注意喚起」が官民一体となって行われた過去に例のないものです。しかし、このような注意喚起を受け取った場合を想定した準備をしておかなければ、迅速かつ適切な対応はできません。企業においては、体制整備や対応訓練などの実施が求められます。

7. 参考URL

- 総務省｜報道資料｜マルウェアに感染している機器の利用者に対する注意喚起の実施
  https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00095.html
- Emotetへの対応 | NOTICE｜サイバー攻撃に悪用されるおそれのあるIoT機器の調査、注意喚起を行うプロジェクト
  https://notice.go.jp/emotet
- マルウェアに感染している機器の利用者に対する注意喚起の実施について
  https://www.npa.go.jp/cyber/policy/mw-attention.html
- マルウエアEmotetへの対応FAQ
  https://blogs.jpcert.or.jp/ja/2019/12/Emotetfaq.html
- マルウェアに感染している機器の利用者に対する注意喚起の実施
  https://www.ict-isac.jp/news/news20210219.html
- 国内PC2万6千件、「エモテット」感染か　注意喚起へ
  https://www.asahi.com/articles/ASP2M3CCNP2LUTIL05S.html
- Taking Down Emotet
  https://team-cymru.com/blog/2021/01/27/taking-down-emotet/
- マルウェアEmotetのテイクダウンと感染端末に対する通知
  https://blogs.jpcert.or.jp/ja/2021/02/emotet-notice.html
- World’s most dangerous malware EMOTET disrupted through global action | Europol
  https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action
- 最も危険なマルウエア「Emotet」が壊滅、アジト急襲のウクライナ警察が見たもの
  https://xtech.nikkei.com/atcl/nxt/column/18/00676/030500073/
- 最恐ウイルスEmotetをテイクダウンしたOperation Ladybirdについてまとめてみた
  https://piyolog.hatenadiary.jp/entry/2021/01/28/180000

NTT DATA

Trusted Global Innovator