DigitalArts

PRESS RELEASE

2020.09.17

報道関係者各位

デジタルアーツ株式会社

再度活性化した「Emotet」の解析情報を公開

～「i-FILTER®」・「m-FILTER®」で、パスワード付きZIPファイルなど最新の手口もブロック～

情報セキュリティメーカーのデジタルアーツ株式会社（本社：東京都千代田区、代表取締役社長：道具　登志夫、以下 デジタルアーツ、証券コード2326）は、2019年後半に猛威を振るい、2020年7月から活動を再開したマルウェア「Emotet（エモテット）」に感染させると考えられるメール・URLの解析情報を公開したことを発表いたします。

2014年に初めてその活動が報告されたのち、何度も進化を繰り返してきたマルウェア「Emotet」は、2019年9月に改ざんされたWebサイトからダウンロードされ感染するケースを弊社で確認し、その年の12月頃まで攻撃の手口を変えながら、国内で感染を拡げていきました※1。そして、今年の7月頃より活動を再開し、情報処理推進機構（IPA）・コーディネーションセンター（JPCERT）から注意喚起が発表されています※2。

手口は従来と同様、メールに添付されたWordファイル、または添付ファイルやメール本文に記載されたURLからダウンロードしたWordファイルのマクロを実行することで感染させられるもので、9月に入ってからは新たにパスワード付きZIPファイルを用いるケースも確認されています※3。

Webセキュリティ製品「i-FILTER」Ver.10・メールセキュリティ製品「m-FILTER」Ver.5の最新の機能では、「Emotet」から同製品のユーザー様を守ることができました。特に、最新のパスワード付きZIPファイルを用いた攻撃は、「m-FILTER」の『添付ファイル強制検査機能』によって添付ファイル内を検査し、悪意のあるマクロが仕掛けられたWord文書ファイルを検知して、受信者の手元にメールが届く前に無害化します。

このたび、弊社にて9月2日に観測した「Emotet」に感染させるとみられるアクセスログから、攻撃に用いられたメールの件名や添付ファイル、URLの特徴等について、弊社Webサイト上で公開しました。

「Emotet」が「感染爆発の兆し」が見えるまで被害を拡大させている要因の一つは、受信者が過去にメールのやり取りをしたことのある、実在の相手の氏名、メールアドレス、メールの内容等が攻撃メールに流用され、業務上必要なものと勘違いするなどして開封してしまうことだと考えられます。今後も形を変え、巧妙に仕組んだ攻撃メールで更に活動を拡げてくる可能性があるため、これらの情報を活用いただき、今後継続的に注意していただく必要があります。

また、こうした攻撃メールはもはや人間の目では判断が難しいため、しっかりと製品で対策を取っていただくことをお勧めします。

マルウェア「Emotet」の解析情報

以下、弊社コーポレートサイト上にて公開しております。

■ 公開ページ

サイバーリスク情報提供サービス「Dアラート」

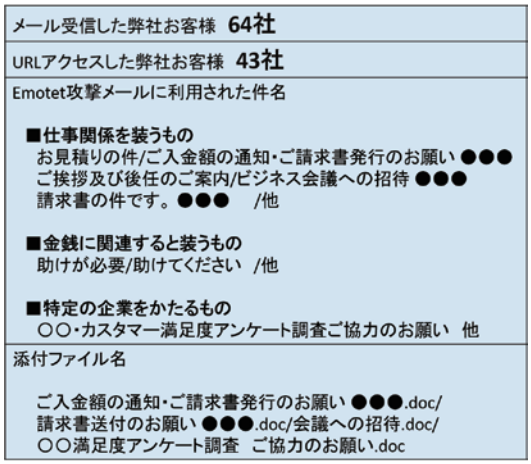
https://www.daj.jp/bs/d-alert/bref/?bid=93&year=2020&month=9

■ 公開している情報

・メールの件名　・感染プロセス　・添付ファイル名

・マクロ実行時に通信するURL　・添付ファイルのHASH値

・弊社製品の対応状況　・対処手順



公開した情報の一部

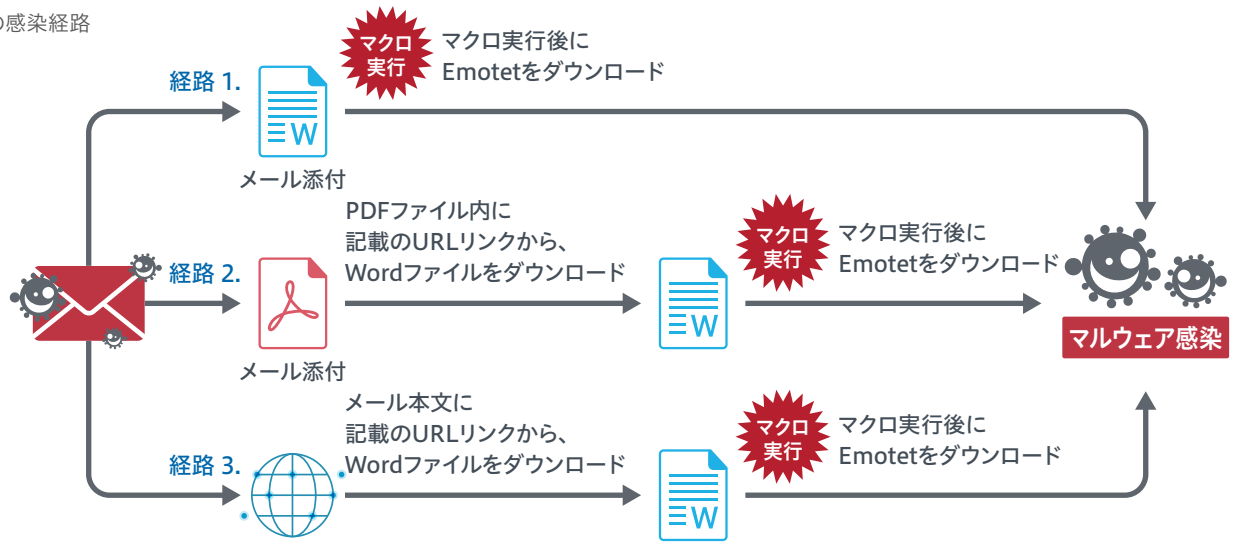
弊社製品によるマルウェア「Emotet」への対処

今回の攻撃メールの脅威に対して、弊社のお客様が利用されている「i-FILTER」と「m-FILTER」の機能によって、未然にブロックしております。

「Emotet」をブロックした機能

「Emotet」の主な感染経路は、メールに添付されたWordファイルのマクロ実行（経路1）、または添付ファイルやメール本文に記載されたURLにアクセスすることでWordファイルをダウンロードしマクロ実行（経路2,3）することで、感染させられるもので、今回新たにパスワード付きZIPファイルを用いたケースも確認されました。

Emotetの感染経路

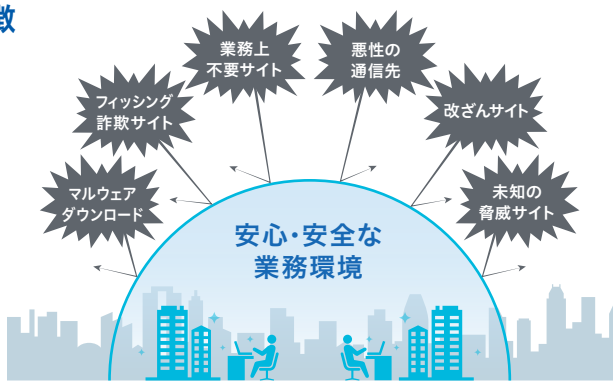


Webセキュリティ製品「i-FILTER」Ver.10の機能と特徴

■ 安全と判断したWebサイトのみアクセス可能とする、「ホワイト運用」でフィルタリング

・国内で検索可能なWebサイトを網羅し、弊社で安全と確認されたWebサイトのURLのみアクセス可能とし、安全が確認できないURLまたは未知の危険なURLは全てブロック

・業務上必要なURL等を事前に登録し、組織の運用ルールに従ってフィルタリングによるアクセス許可／不許可等を設定することも可能

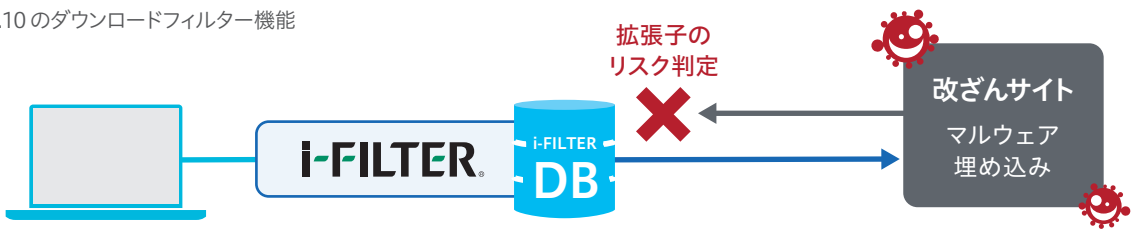


未知の脅威サイトをブロックする「ホワイト運用」

■ 「ホワイト運用」と「ダウンロードフィルター機能」で「Emotet」ダウンロードを確実にブロック

「ホワイト運用」でマクロ実行後のアクセス先となる「Emotet」ダウンロードURLへのアクセスをブロックします。また、改ざんされた正規のWebサイトにマルウェアが直接埋め込まれた場合であっても、「ダウンロードフィルター機能」でマルウェアのダウンロードをブロックし、「Emotet」の感染を防ぎます。

「i-FILTER」 Ver.10 のダウンロードフィルター機能



メールセキュリティ製品「m-FILTER」Ver.5の機能と特徴

■ 安全と判断したメールのみ受信可能とする、「ホワイト運用」で攻撃メールをブロック

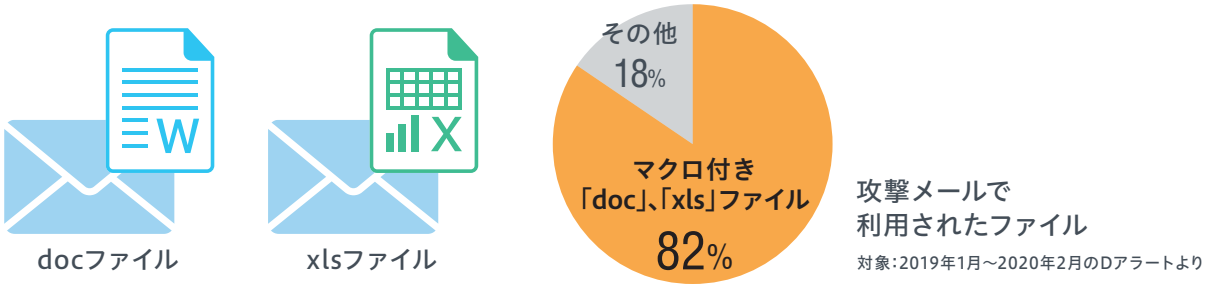
・安全な「IPアドレス」と「メールドメイン」の組み合わせを収集し、安全と判定された送信元のメールのみ受信可能

・送信元偽装メールや偽装した添付ファイル、本文を偽装したメール等を判定し、隔離。添付ファイル削除、リンク無効化等、メール無害化が可能

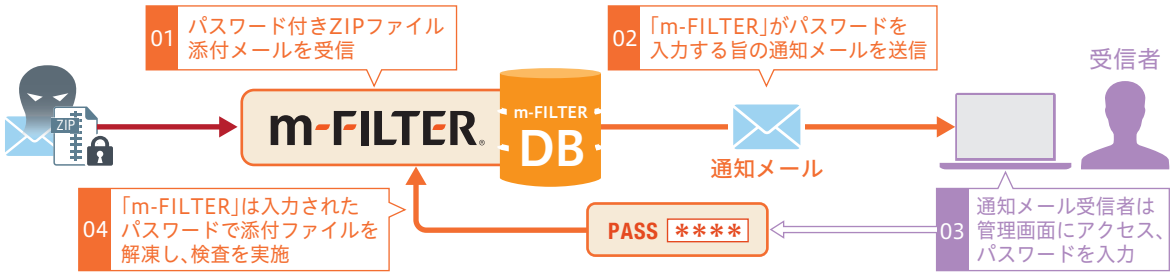
■ 「添付ファイル強制検査機能」で、最新の攻撃でもメールが受信者の手元に届く前にブロック

「Emotet」の手口に多く用いられる古い形式のマクロ付きWordやExcelを添付したメールをブロックします。
また、9月から新たに観測された、パスワード付きZIPファイルを用いたパターンであっても、これを強制捜査し偽装を判定してブロックします。

「m-FILTER」 Ver.5 の旧形式のマクロ付き Word/Excel ブロック機能



「m-FILTER」 Ver.5 の ZIP パスワードロックファイル判定機能



■ Web セキュリティ製品「i-FILTER」
詳細 ▶ https://www.daj.jp/bs/i-filter/

■ メールセキュリティ製品「m-FILTER」
詳細 ▶ https://www.daj.jp/bs/mf/

※1 詳細は下記の弊社セキュリティレポートをご参照ください
https://www.daj.jp/security_reports/191017_1/

※2 IPA「Emotet」と呼ばれるウイルスへの感染を狙うメールについて(最終更新日9月2日)
https://www.ipa.go.jp/security/announce/20191202.html

※3 JPCERT 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(最終更新日9月4日)
https://www.jpcert.or.jp/newsflash/2020090401.html

デジタルアーツ株式会社　概要

Web、メール、ファイルなどのセキュリティソフトウェアの提供を核に事業展開する情報セキュリティメーカーです。1995 年の創業以来、「より便利な、より快適な、より安全なインターネットライフに貢献していく」を企業理念とし、有害情報の閲覧を制限する Web フィルタリングソフトを開発、以来企業・公共・家庭向けに情報セキュリティ製品を提供しております。東京都千代田区大手町 1-5-1 大手町ファーストスクエア　ウエストタワー 14F　URL: https://www.daj.jp/

<本リリースに関するお問い合わせ>
デジタルアーツ株式会社　広報担当　山田
※新型コロナウイルス感染症拡大に伴う在宅勤務実施中のため、お電話でのお問い合わせ先は以下とさせていただきます
TEL : 090-1555-7254 / E-mail : press@daj.co.jp

DigitalArts
より便利な、より快適な、より安全なインターネットライフに貢献していく