2021年
11月
NOVEMBER

MALWARE REPORT

マルウェアレポート

国内のマルウェア検出状況を解説

キヤノンマーケティングジャパン株式会社

はじめに

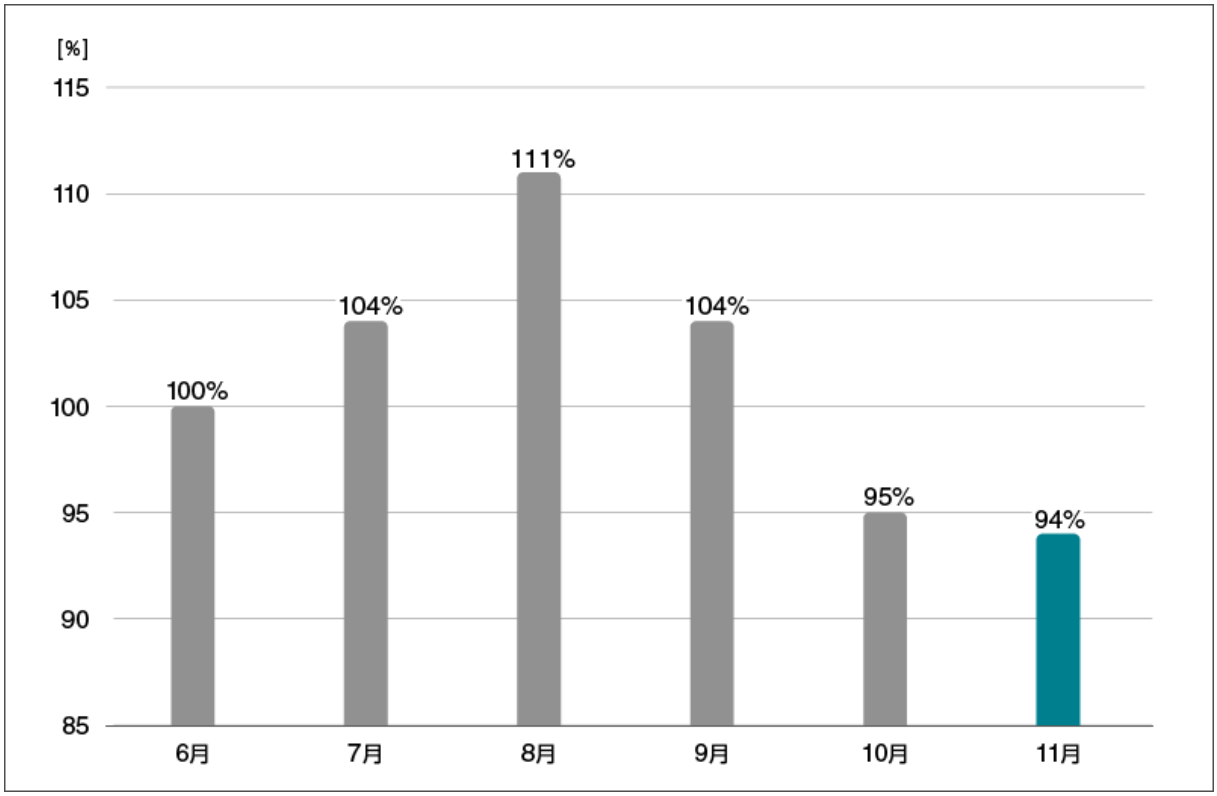
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「サイバーセキュリティラボ」が「ESET セキュリティソリューションシリーズ」の

マルウェア検出データを基に国内のマルウェア検出状況を分析し、まとめたレポートです。

2021 年 11 月マルウェア検出状況

2021 年 11 月（11 月 1 日～11 月 30 日）に ESET 製品が国内で検出したマルウェアの検出数の推移は、以下のとおりです。



国内マルウェア検出数*1の推移

(2021 年 6 月の全検出数を 100%として比較)

*1 検出数には PUA（Potentially Unwanted/Unsafe Application; 必ずしも悪意があるとは限らないが、コンピューターのパフォーマンスに悪影響を及ぼす可能性があるアプリケーション)を含めています。

2021 年 11 月の国内マルウェア検出数は、2021 年 10 月と比較して微減しました。検出されたマルウェアの内訳は以下のとおりです。

国内マルウェア検出数*2 上位（2021 年 11 月）

順位	マルウェア	割合	種別
1	JS/Adware.Agent	22.1%	アドウェア
2	HTML/Phishing.Agent	12.5%	メールに添付された不正な HTML ファイル
3	JS/Adware.Sculinst	8.3%	アドウェア
4	JS/Adware.TerraClicks	4.2%	アドウェア
5	JS/Adware.Subprop	3.5%	アドウェア
6	HTML/FakeAlert	2.4%	偽の警告文を表示させる HTML ファイル
7	JS/Adware.PopAds	1.5%	アドウェア
8	HTML/ScrInject	1.3%	HTML に埋め込まれた不正スクリプト
9	Win32/Exploit.CVE-2017-11882	1.1%	脆弱性を悪用するマルウェア
10	JS/Redirector	0.9%	別のページに遷移させるスクリプト

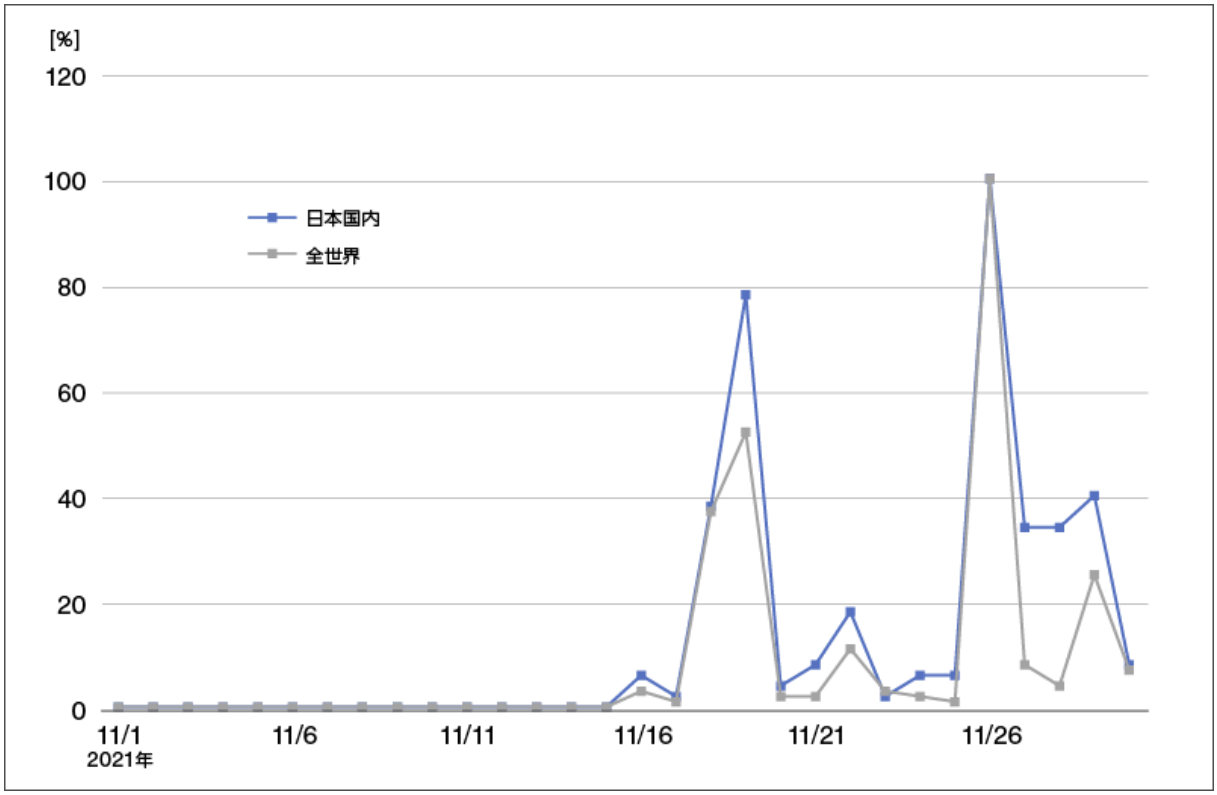
*2 本表には PUA を含めていません。

11 月に国内で最も多く検出されたマルウェアは、JS/Adware.Agent でした。
JS/Adware.Agent は、悪意のある広告を表示させるアドウェアの汎用検出名です。Web サイト閲覧時に実行されます。

11 月は、欧州刑事警察機構（Europol）によってテイクダウンが報告[1)]されたマルウェア「Emotet」について、およそ 10 ヶ月ぶりに活動再開が確認[2)]されました。ESET 製品では活動再開した Emotet およびそのダウンローダーを、「Win32/Emotet」、「DOC/TrojanDownloader.Agent」などの検出名で検出します。これらの検出数は 11 月半ば頃から増加しており、Emotet 再開の影響を窺うことができます。

活動再開後の Emotet およびそのダウンローダーに対する、ESET 製品による検出名の例

検出対象	ESET 検出名
Emotet	＜Emotet＞ ・Win32/Emotet ＜汎用検出名＞ ・Win32/GenKryptik ・Win32/Kryptik ・Win64/Kryptik 他
Emotet ダウンローダー	＜ダウンローダー＞ ・DOC/TrojanDownloader.Agent ・VBA/TrojanDownloader.Agent ・VBA/TrojanDropper.Agent ＜汎用検出名＞ ・GenScript ・Generik 他

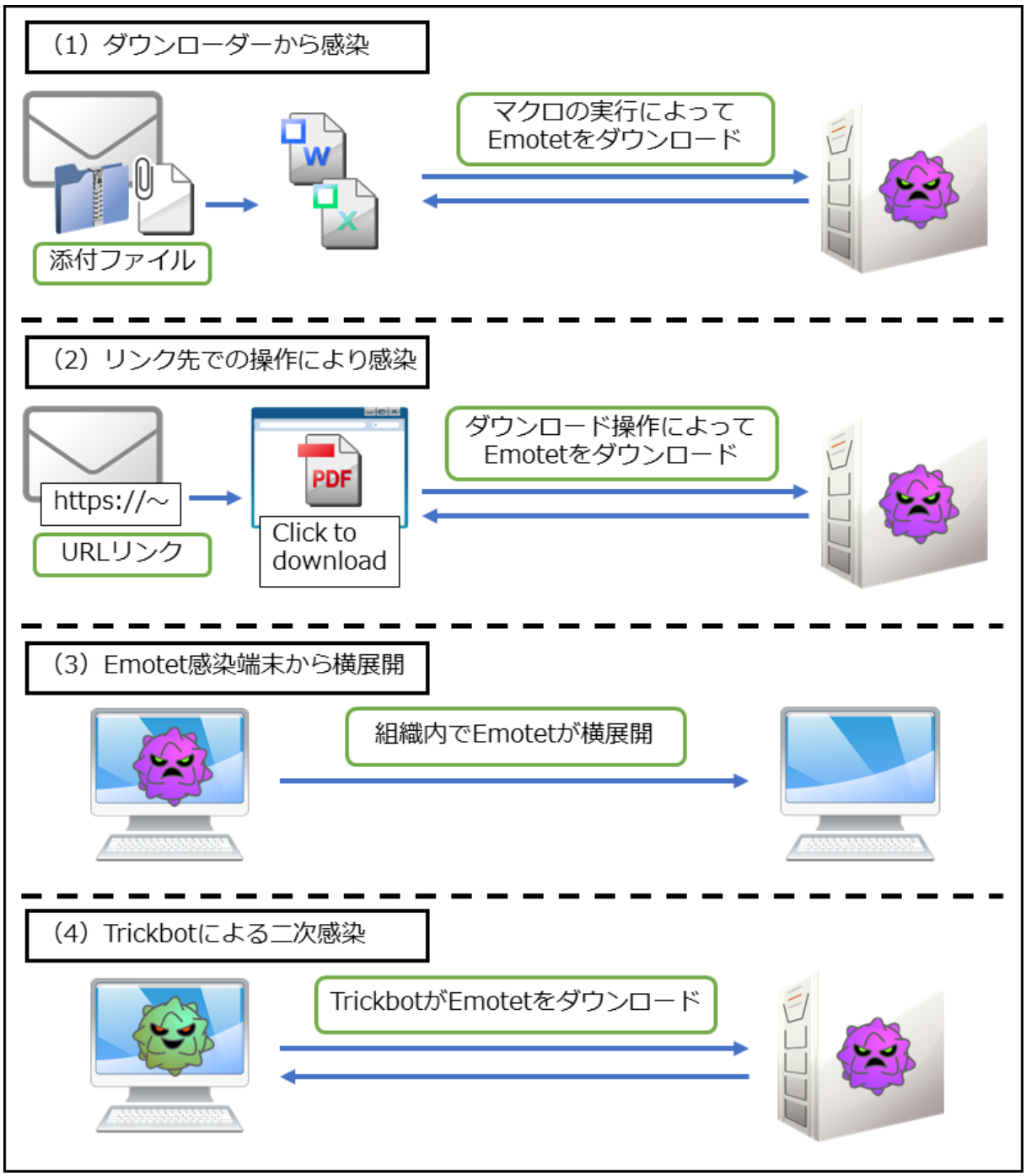


11 月に活動再開した Emotet およびそのダウンローダーに関連する検出数の推移
(検出数が最も多い 11 月 26 日を 100%として表示)

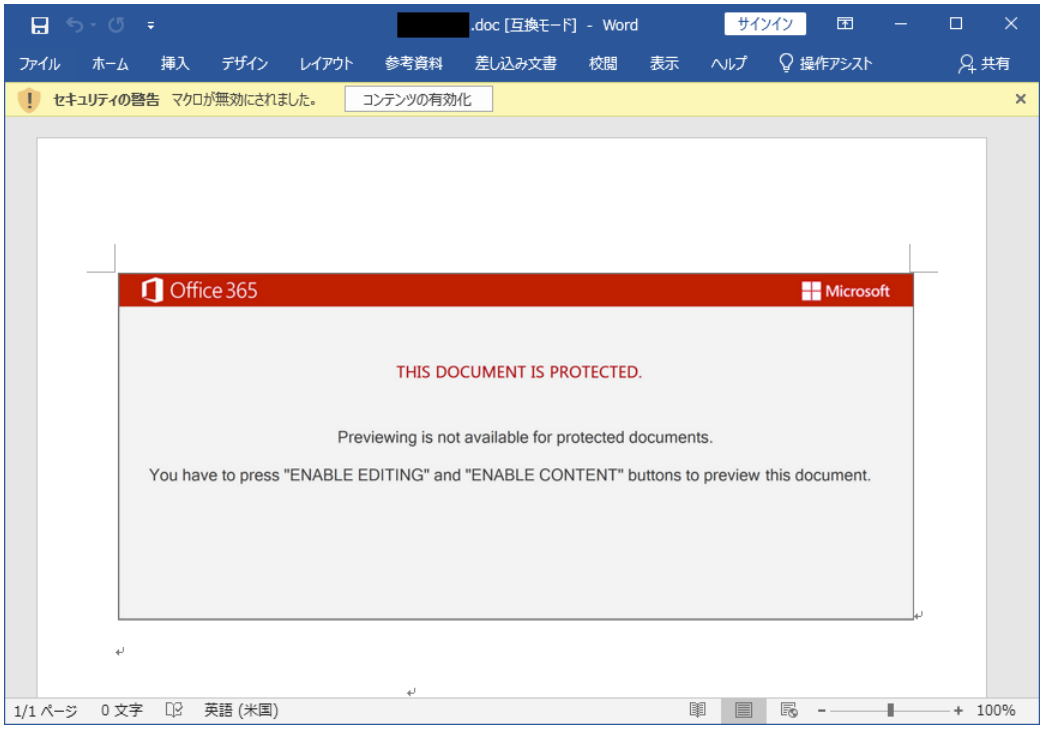
Emotet の感染経路としては、以下の 4 つのパターンが確認[3)4)]されています。

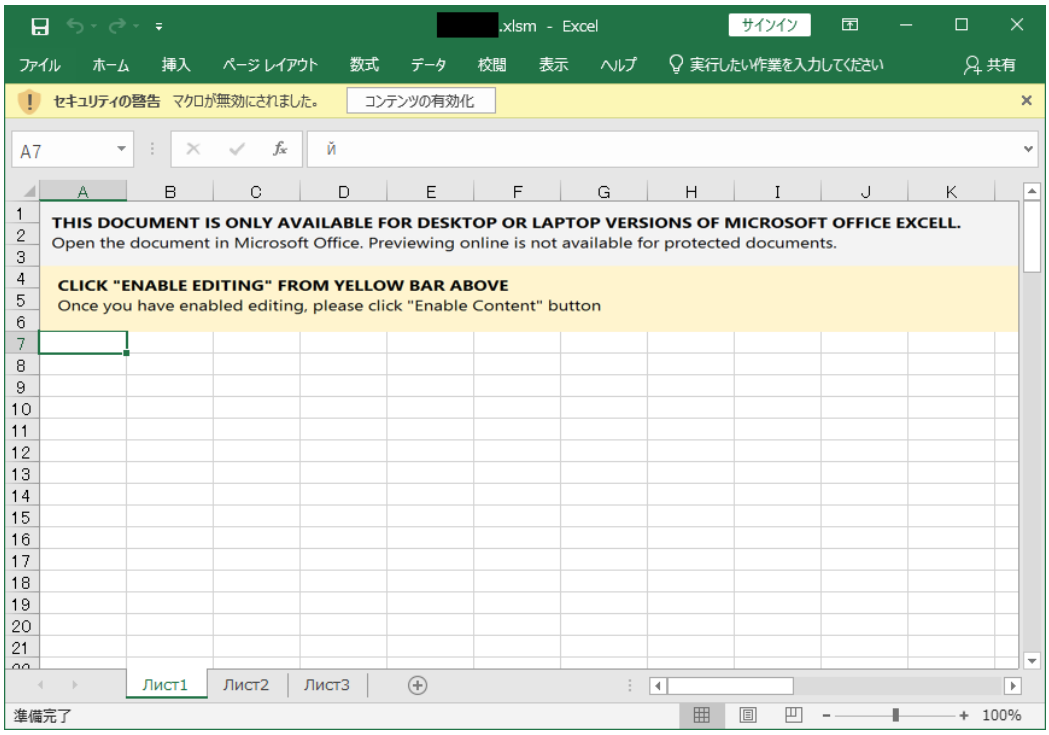
(1) 電子メールに添付されたダウンローダー（不正な VBA マクロを含む Microsoft Office ファイル）を実行することによって感染
(2) 電子メールに記載された URL リンク（Adobe PDF ファイルのダウンロードを促す Web サイト）にアクセスし、その Web サイト上から Emotet をダウンロードしてしまうことで感染
(3) 既に Emotet に感染した別の端末から横展開されて感染
(4) マルウェア「Trickbot」によってダウンロードされることで感染

このうち活動再開後から出回っているダウンローダーについて、サイバーセキュリティラボでは Word ファイルや Excel ファイル、これらを内包したパスワード付き ZIP 圧縮ファイルという 3 つの形式を確認しています。



これまでに確認されている Emotet の感染経路





11 月から出回っている Emotet ダウンローダーの例

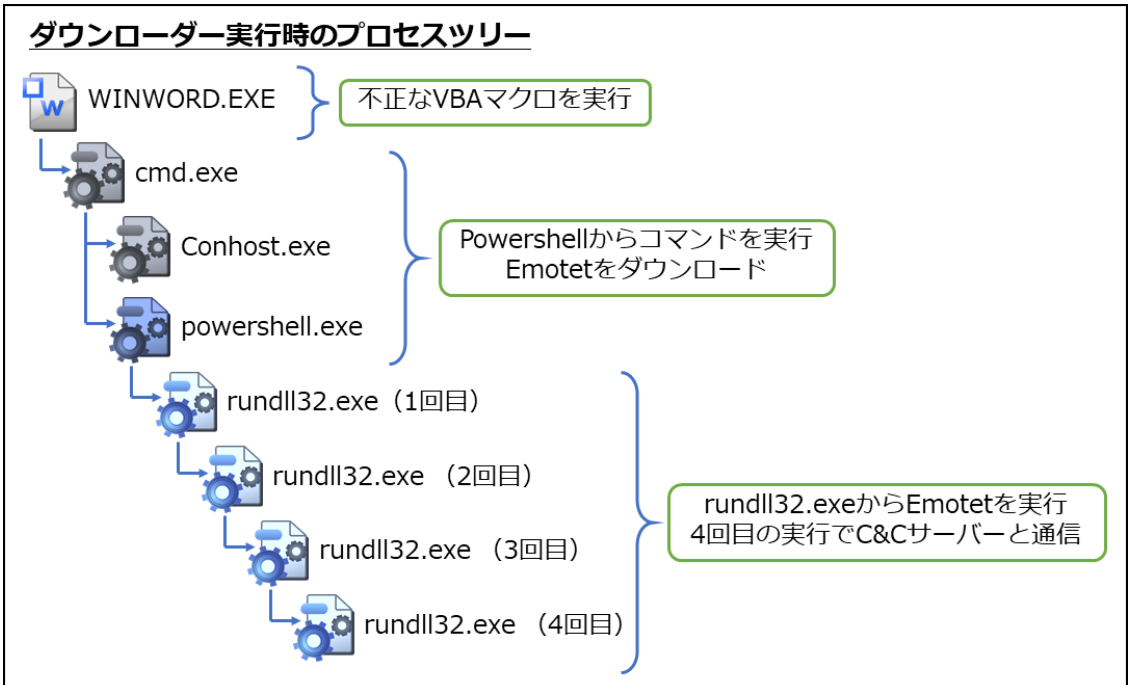
ダウンローダーの実行から Emotet 感染までの挙動については、テイクダウン前の検体と比較して大きな変化はありません。まずダウンローダーである Microsoft Office ファイルの「コンテンツの有効化」を行うと、不正な VBA マクロが実行されます。続いて PowerShell にコマンドが渡され、複数の通信先に対して順に接続を行います。通信が成功すると DLL ファイル形式の Emotet がダウンロードされます。最後に rundll32.exe を使用して Emotet が実行されます。

今回確認した挙動では、ダウンローダーが実行されると Emotet をダウンロードし、「%ProgramData%¥」配下に配置します。ダウンロードされた Emotet は rundll32.exe を使用して自身を 4 回起動[*3]し、最終的に C&C サーバーに対して通信を行います。

rundll32.exe に関して、1 回目はランダムな文字列、2 回目は Emotet 本体のエクスポート関数として定義されている「Control_RunDLL」という文字列を引数[*3]にして Emotet を実行します。2 回目の実行によって、Emotet は「%ProgramData%¥」配下から「%LocalAppData%¥（ランダムな文字列）¥」配下にファイルロケーションが変わります。そして 2 回目は 1 回目と同様にランダムな文字列、4 回目は 2 回目と同様に「Control_RunDLL」という文字列を引数[*3]にして Emotet を実行します。

テイクダウン前の Emotet は、C&C サーバーへの通信時に HTTP プロトコルを使用していました。しかし活動再開後の Emotet では、HTTPS プロトコルが使用されていることを確認しています。

*3 Emotet の起動回数や rundll32.exe の引数は、実行環境によって異なる可能性があります。



不正なマクロが実行されてから C&C サーバーに通信するまでの挙動

C&C サーバーに対して HTTPS プロトコルで通信を試みている様子

テイクダウン前の Emotet は Epoch1、Epoch2、Epoch3 と呼ばれる 3 つのボットネットを形成することで猛威を奮っていましたが、Europol を含む世界各国の機関によってこれらのボットネットが無害化されたため、Emotet による脅威は収束したと考えられていました。しかし、Trickbot 経由で Emotet に感染する動きが 11 月に報告 [5]されたことで、活動再開が認知されるようになりました。同時に Epoch4 や Epoch5 と呼ばれる新たなボットネットが形成され、Emotet に感染した端末からマルスパムが配信されるようになったと推測されます。今後は Emotet 感染端末が増加し、大規模な攻撃キャンペーンが展開される可能性も考えられるため注意が必要です。

ご紹介したとおり、Emotet の活動再開が確認されましたが、感染対策としては 2021 年 1 月のテイクダウン前の Emotet と同様です。不審な電子メールを受信した場合、添付ファイルを開かないことや URL リンクにアクセスしないことが重要です。またダウンローダーである Microsoft Office ファイルを開いてしまった場合でも、コンテンツを有効化しないよう注意してください。

■常日頃からリスク軽減するための対策について
各記事でご案内しているようなリスク軽減の対策をご案内いたします。
下記の対策を実施してください。

1．セキュリティ製品の適切な利用

1-1. ESET 製品の検出エンジン（ウイルス定義データベース）をアップデートする

ESET 製品では、次々と発生する新たなマルウェアなどに対して逐次対応しています。最新の脅威に対応できるよう、検出エンジン（ウイルス定義データベース）を最新の状態にアップデートしてください。

1-2. 複数の層で守る

1 つの対策に頼りすぎることなく、エンドポイントやゲートウェイなど複数の層で守ることが重要です。

2．脆弱性への対応

2-1. セキュリティパッチを適用する

マルウェアの多くは、OS に含まれる「脆弱性」を利用してコンピューターに感染します。「Windows Update」などの OS のアップデートを行ってください。また、マルウェアの多くが狙う「脆弱性」は、Office 製品、Adobe Reader などのアプリケーションにも含まれています。各種アプリケーションのアップデートを行ってください。

2-2. 脆弱性診断を活用する

より強固なセキュリティを実現するためにも、脆弱性診断製品やサービスを活用していきましょう。

３．セキュリティ教育と体制構築

3-1．脅威が存在することを知る

「セキュリティ上の最大のリスクは“人”だ」とも言われています。知らないことに対して備えることができる人は多くありませんが、知っていることには多くの人が「危険だ」と気づくことができます。

3-2．インシデント発生時の対応を明確化する

インシデント発生時の対応を明確化しておくことも、有効な対策です。何から対処すればいいのか、何を優先して守るのか、インシデント発生時の対応を明確にすることで、万が一の事態が発生した時にも、慌てずに対処することができます。

４．情報収集と情報共有

4-1．情報収集

最新の脅威に対抗するためには、日々の情報収集が欠かせません。弊社を始め、各企業・団体から発信されるセキュリティに関する情報に目を向けましょう。

4-2．情報共有

同じ業種・業界の企業は、同じ攻撃者グループに狙われる可能性が高いと考えられます。同じ攻撃者グループの場合、同じマルウェアや戦略が使われる可能性が高いと考えられます。分野ごとの ISAC（Information Sharing and Analysis Center）における情報共有は特に効果的です。

引用・出典元

1） World’s most dangerous malware EMOTET disrupted through global action | Europol
https://www.europol.europa.eu/media-press/newsroom/news/world%e2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

2)「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 | IPA 独立行政法人 情報処理推進機構
https://www.ipa.go.jp/security/announce/20191202.html

3)【注意喚起】マルウェア Emotet が 10 カ月ぶりに活動再開、日本も攻撃対象に | セキュリティ対策のラック
https://www.lac.co.jp/lacwatch/alert/20211119_002801.html
4) Emotet now spreads via fake Adobe Windows App Installer packages | BleepingComputer
https://www.bleepingcomputer.com/news/security/emotet-now-spreads-via-fake-adobe-windows-app-installer-packages/
5) a Trickbot Rebirths Emotet: 140,000 Victims in 149 Countries in 10 Months | Check Point Software
https://blog.checkpoint.com/2021/12/08/trickbot-rebirths-emotet-140000-victims-in-149-countries-in-10-months/

Canon

キヤノンマーケティングジャパン株式会社