2022年
4月
APRIL

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

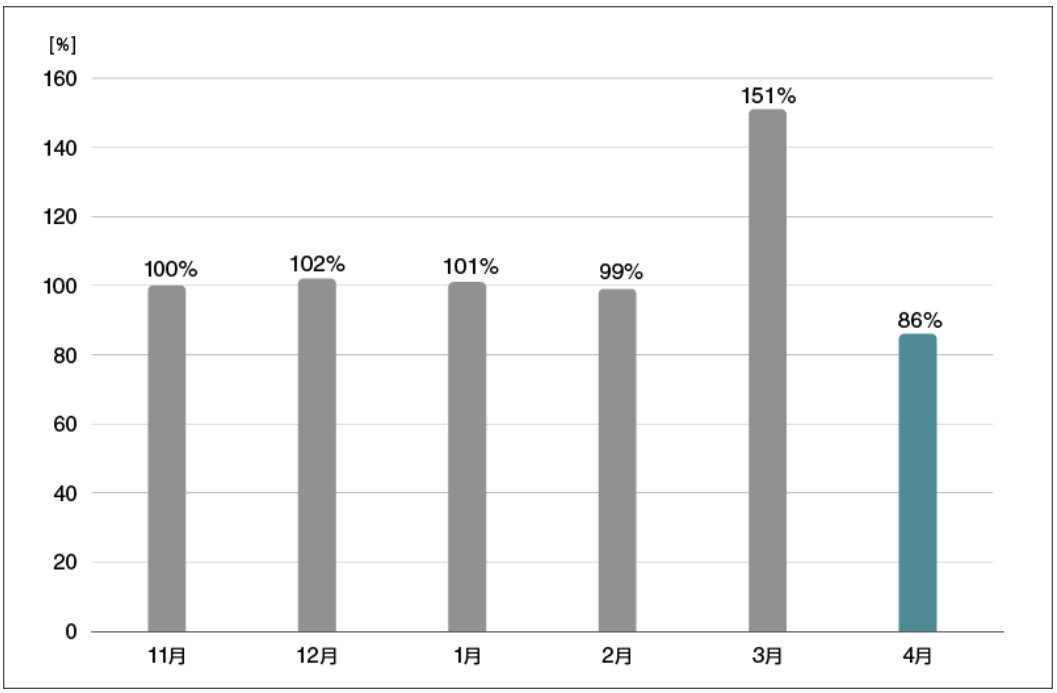
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「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。

2022 年 4 月マルウェア検出状況

2022 年 4 月（4 月 1 日～4 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 11 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。

2022 年 4 月の国内マルウェア検出数は、2022 年 3 月と比較して急減しました。検出されたマルウェアの内訳は以下のとおりです。

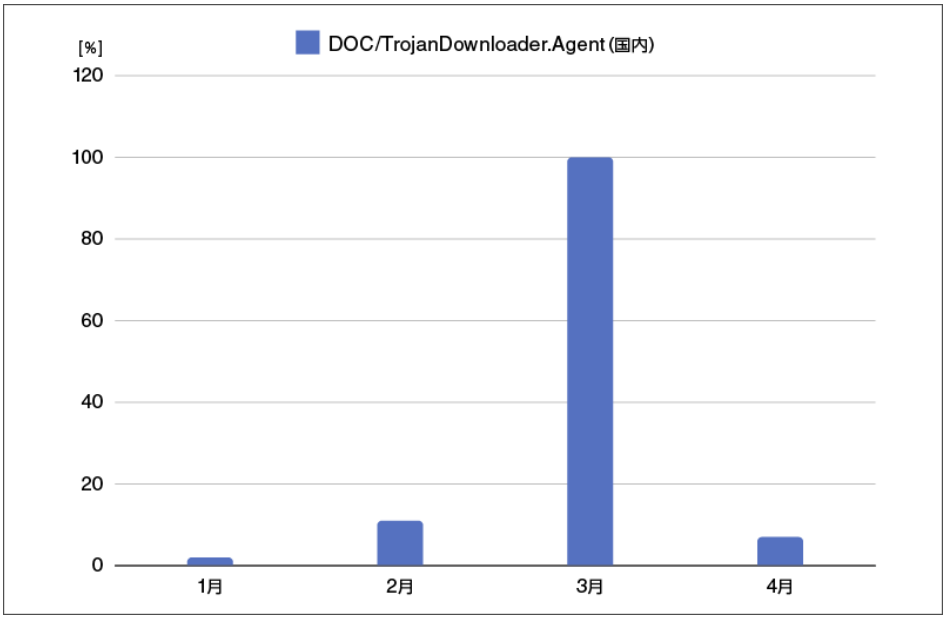
国内マルウェア検出数*2 上位（2022 年 4 月）

順位	マルウェア	割合	種別
1	JS/Adware.Agent	15.1%	アドウェア
2	HTML/Phishing.Agent	10.1%	メールに添付された不正な HTML ファイル
3	JS/Adware.Sculinst	7.5%	アドウェア
4	JS/Adware.TerraClicks	5.9%	アドウェア
5	HTML/FakeAlert	4.8%	偽の警告文を表示させる HTML ファイル
6	DOC/TrojanDownloader.Agent	4.0%	ダウンローダー
7	MSIL/Kryptik	1.9%	難読化された MSIL で作成されたファイルの汎用検出名
8	JS/Packed.Agent	1.9%	パックされた不正な JavaScript の汎用検出名
9	HTML/ScrInject	1.8%	HTML に埋め込まれた不正スクリプト
10	MSIL/TrojanDownloader.Agent	1.1%	ダウンローダー

*2 本表には PUA を含めていません。

4 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。

国内マルウェア検出数を見てみると、4 月は 3 月と比較して 4 割以上減少しました。2022 年 3 月 マルウェアレポートで、マルウェア Emotet のダウンローダーに関連する DOC/TrojanDownloader.Agent の検出数が増加したことを紹介しました。この検出数が大きく減少したことで、4 月の国内マルウェア検出数も大きく減少しました。



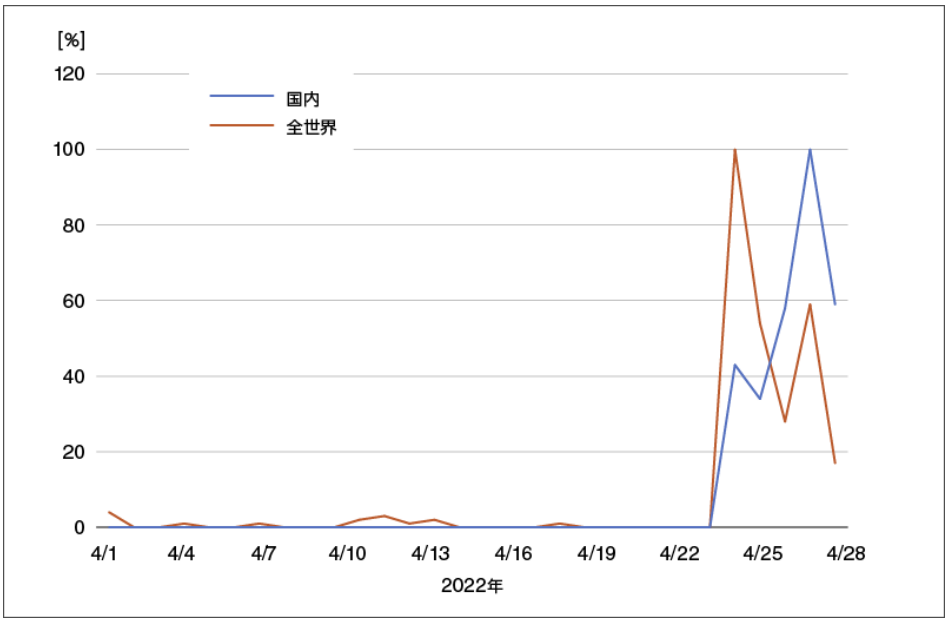
2022 年における国内の DOC/TrojanDownloader.Agent 検出数推移
（最も検出数の多い 3 月を 100%として比較）

一方で 4 月後半になると、Emotet のダウンローダーが MS Office 形式のファイルに代わって LNK 形式（ショートカット形式）のファイルが使用されるようになったと、複数の機関が報告*3,4 しました。ESET では LNK 形式の Emotet ダウンローダーを、LNK/TrojanDownloader.Agent として検出*5 します。この検出数は国内および全世界で 4 月 26 日以降に急増しており、ESET の検出状況においても世界規模で脅威が拡大した様子が観測されました。

*3 「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

*4 マルウェア Emotet の感染再拡大に関する注意喚起 | 一般社団法人 JPCERT コーディネーションセンター

*5 Emotet 以外のマルウェアのダウンローダーも同様の検出名で検出する可能性があります。

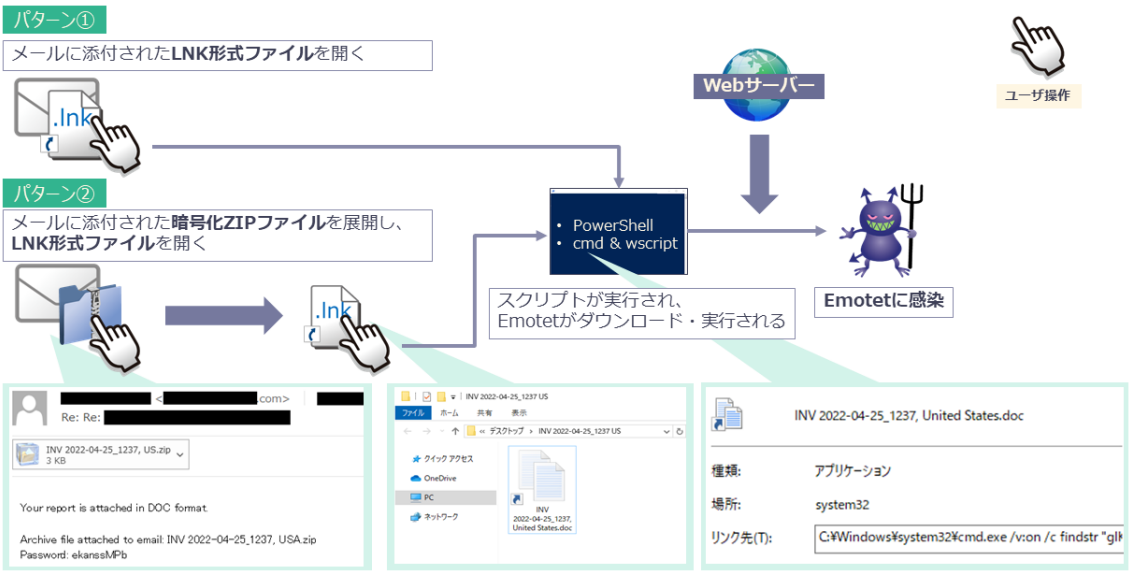


2022 年における LNK/TrojanDownloader.Agent の検出数推移
（最も検出数の多い 4 月 29 日（国内）、4 月 26 日（全世界）を 100%として比較）

この LNK 形式のダウンローダーは、電子メール経由で以下の 2 つの方法によって配信されていることが確認されています。

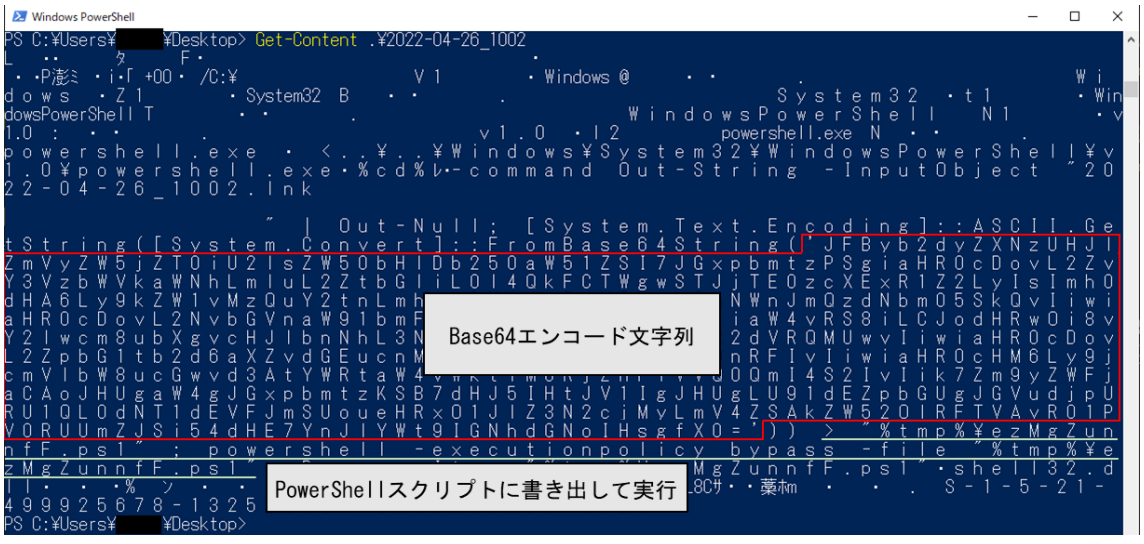
① 電子メールに LNK 形式ファイルが直接添付されている。
② 電子メールに暗号化 ZIP ファイルが添付されており、解凍すると LNK 形式ファイルが展開される。

そしてユーザーが LNK 形式ファイルを開くことにより、スクリプトが実行され、最終的に Emotet へ感染します。



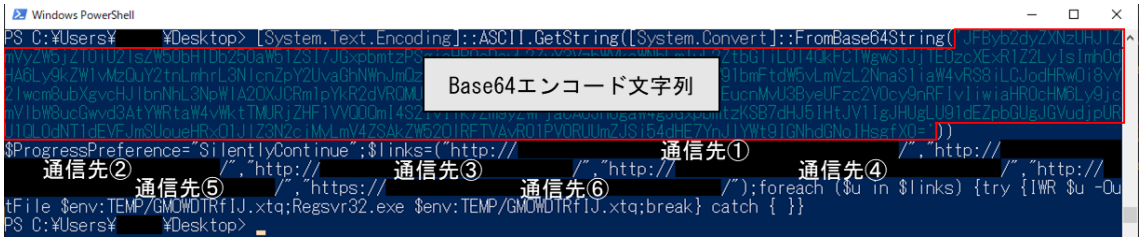
LNK 形式ファイルから Emotet の感染に至るまでの流れ

4 月 26 日以降に観測した LNK 形式の Emotet ダウンローダーの一例を見てみます。ファイルの中身を確認すると、Windows 標準ツールの PowerShell へのリンクとなっており、ファイル内に埋め込まれた Base64 エンコードされた文字列をデコードする様子が分かります。また、デコードしたデータを PowerShell スクリプトに書き出し、そのスクリプトを実行する様子も読み取ることができます。



4 月 26 日以降に Emotet ダウンローダーとして使用された LNK 形式ファイル

埋め込まれている Base64 エンコード文字列を実際にデコードしてみると、6 個の通信先の記載が確認できます。この通信先に対して順次接続し、ペイロードのダウンロードが成功すると、Regsvr32.exe を使用してこのペイロードを実行します。



LNK 形式ファイル内の Base64 エンコード文字列をデコードした様子

2022 年 1 月・2 月 マルウェアレポートで紹介した、Excel 4.0 マクロを使用した Emotet ダウンローダーは、複数の通信先に順次接続を行いダウンロードしたペイロードを実行するという処理が実装されていました。これは今回の LNK 形式ファイルと比較しても、処理方法に大きな違いはありません。しかし、処理開始のためにコンテンツの有効化が必要な MS Office ファイルのマクロと異なり、LNK 形式ファイルの場合はファイルを実行するだけで処理が開始されてしまうため注意が必要です。

2021 年 11 月に Emotet の活動が再開されて以降、ダウンローダーとして使用されてきた MS Office 形式ファイルのマクロの実装方法がアップデートされながら、継続して Emotet は猛威を奮ってきました。そんな中、2022 年 4 月はダウンローダーのファイル形式に変化が見られました。ファイル形式が異なると、上述したようにマルウェアの処理が開始されるトリガーも異なる場合があります。従ってマルウェアの最新動向に関する情報収集を常時行い、どこまで操作すると感染する可能性があるのかを理解し、ユーザーに周知することが重要です。

■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

■「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#L20

■マルウェア Emotet の感染再拡大に関する注意喚起 | 一般社団法人 JPCERT コーディネーションセンター
https://www.jpcert.or.jp/at/2022/at220006.html

Canon

キヤノンマーケティングジャパン株式会社