2022年
3月
MARCH

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

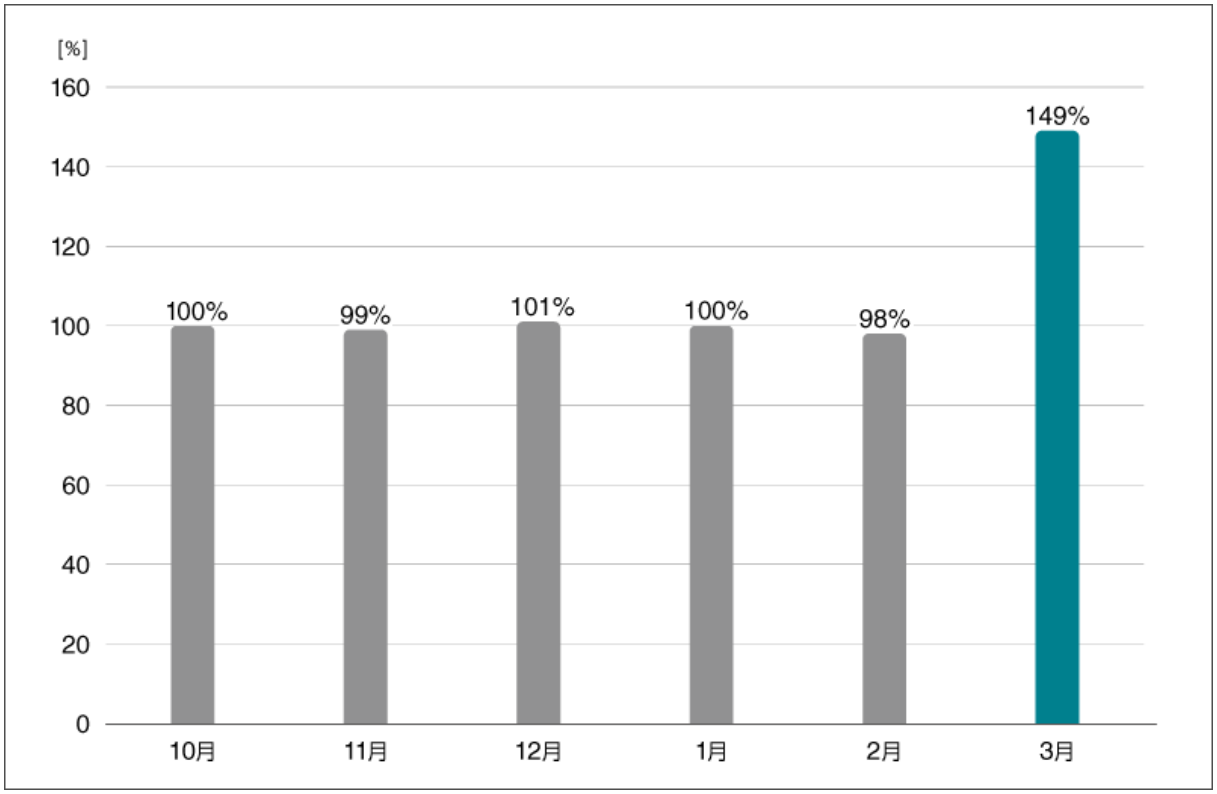
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「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 3 月マルウェア検出状況

2022 年 3 月（3 月 1 日～3 月 31 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 10 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。

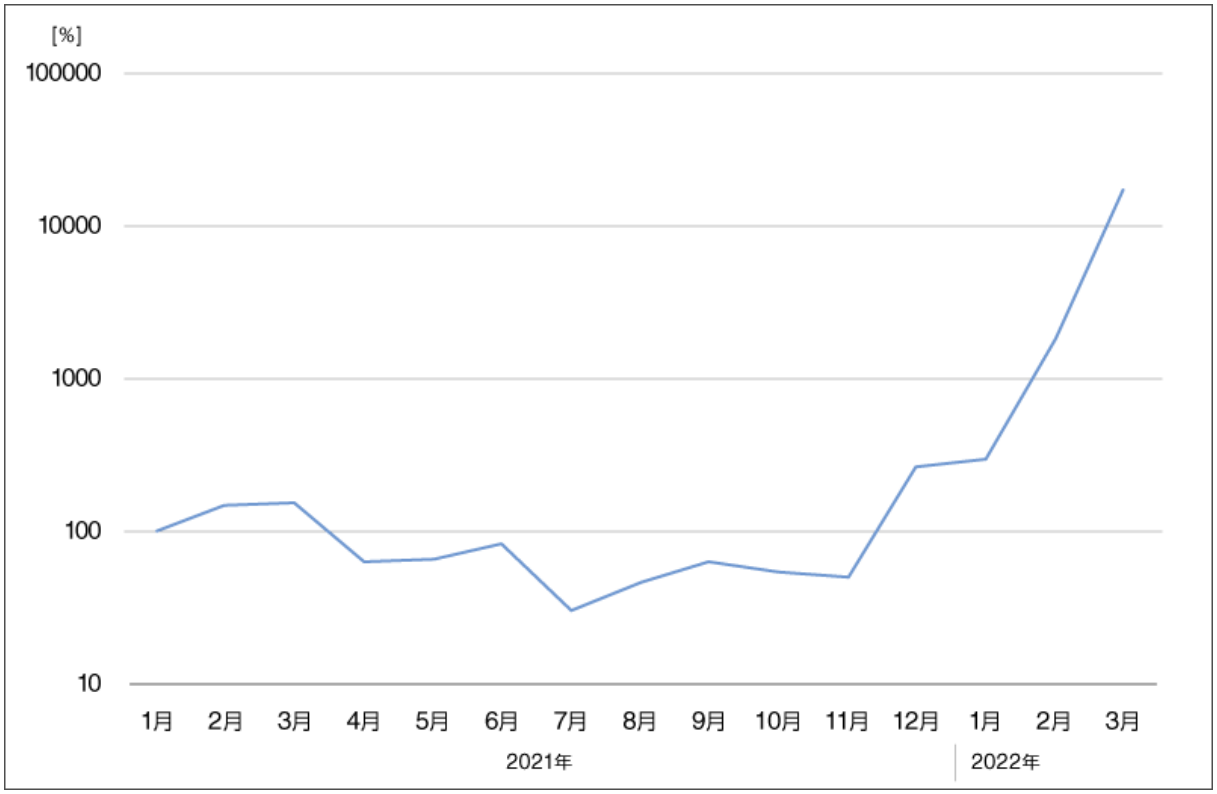
2022 年 3 月の国内マルウェア検出数は、2022 年 2 月から増加しています。主な要因としては、DOC/TrojanDownloader.Agent の急増が挙げられます。
検出されたマルウェアの内訳は以下のとおりです。

国内マルウェア検出数*2 上位（2022 年 3 月）

順位	マルウェア	割合	種別
1	DOC/TrojanDownloader.Agent	33.6%	ダウンローダー
2	HTML/Phishing.Agent	8.8%	メールに添付された不正な HTML ファイル
3	JS/Adware.Agent	7.7%	アドウェア
4	JS/Adware.Sculinst	5.4%	アドウェア
5	HTML/FakeAlert	4.7%	偽の警告文を表示させる HTML ファイル
6	JS/Adware.TerraClicks	3.9%	アドウェア
7	HTML/ScrInject	1.5%	HTML に埋め込まれた不正スクリプト
8	MSIL/Kryptik	1.3%	難読化された MSIL で作成されたファイルの汎用検出名
9	JS/Adware.ClickAdu	1.2%	アドウェア
10	JS/Packed.Agent	1.1%	パックされた不正な JavaScript の汎用検出名

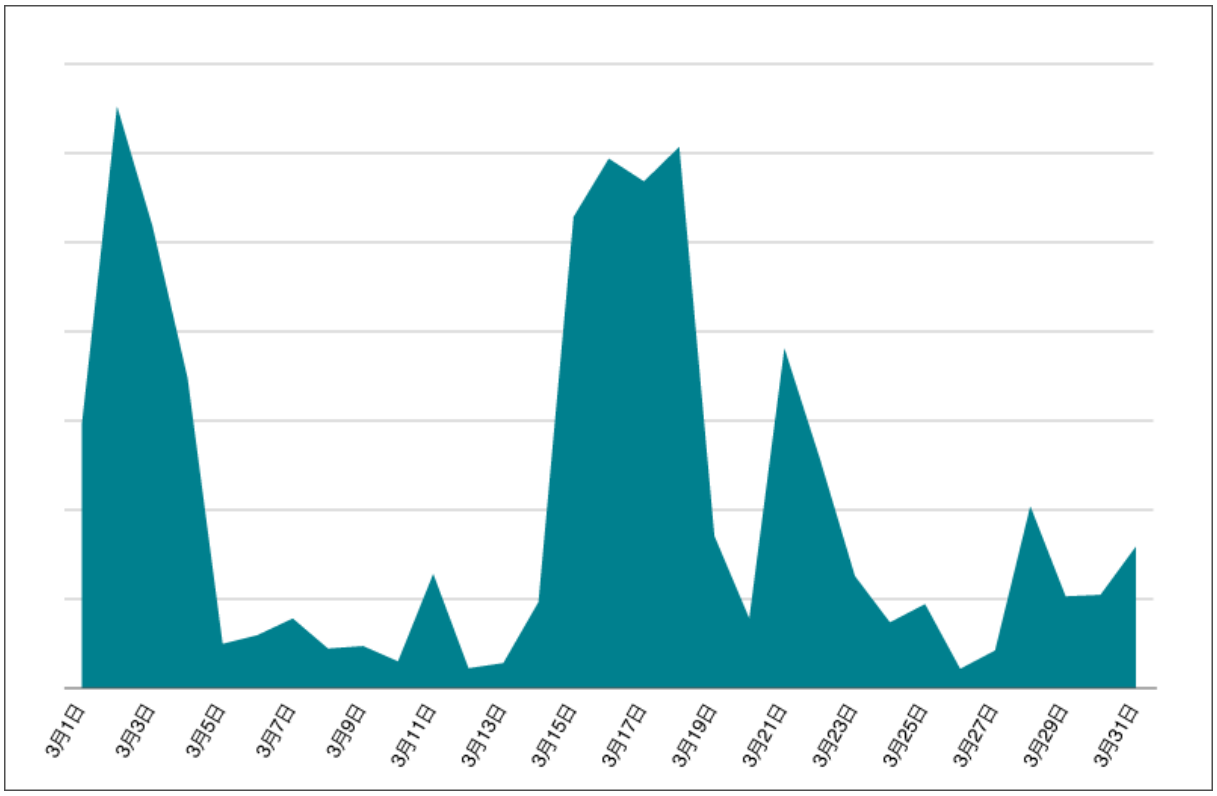
*2 本表には PUA を含めていません。

3 月に国内で最も多く検出されたマルウェアは、DOC/TrojanDownloader.Agent でした。
DOC/TrojanDownloader.Agent は、メールに添付された Word ファイルや Excel ファイルに加えて、それらを含んだ ZIP ファイルを検出しています。また、メール本文内に書かれた URL のアクセス先からダウンロードされる Word ファイルや Excel ファイルが検出される場合もあります。これらのファイルを実行すると、Dridex や Emotet などさまざまなマルウェアがダウンロードされます。3 月に多数検出されていた DOC/TrojanDownloader.Agent は、主に Emotet をダウンロードするものでした。



DOC/TrojanDownloader.Agent の検出数の月別推移（2021 年～2022 年･国内）
（2021 年 1 月の検出数を 100%として比較、縦軸を対数軸として表記）

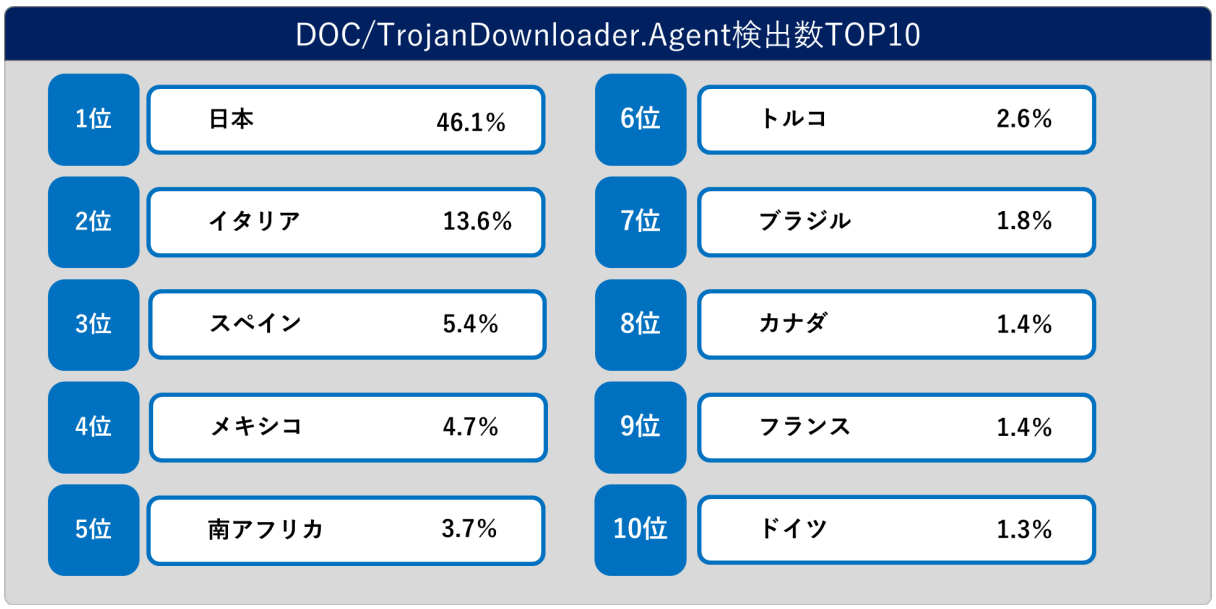
Emotet が活動休止する直前の 2021 年 1 月から 2022 年 3 月までの DOC/TrojanDownloader.Agent の検出数の推移は上記のとおりです。検出数の増加した幅が大きいため、縦軸を対数軸として表記しています。
3 月における日別検出数の推移は以下のとおりです。



DOC/TrojanDownloader.Agent の日別検出数の推移（2022 年 3 月・国内）

3 月 1 日～4 日、15 日～18 日、21 日、28 日に多数の DOC/TrojanDownloader.Agent の検出を確認しています。

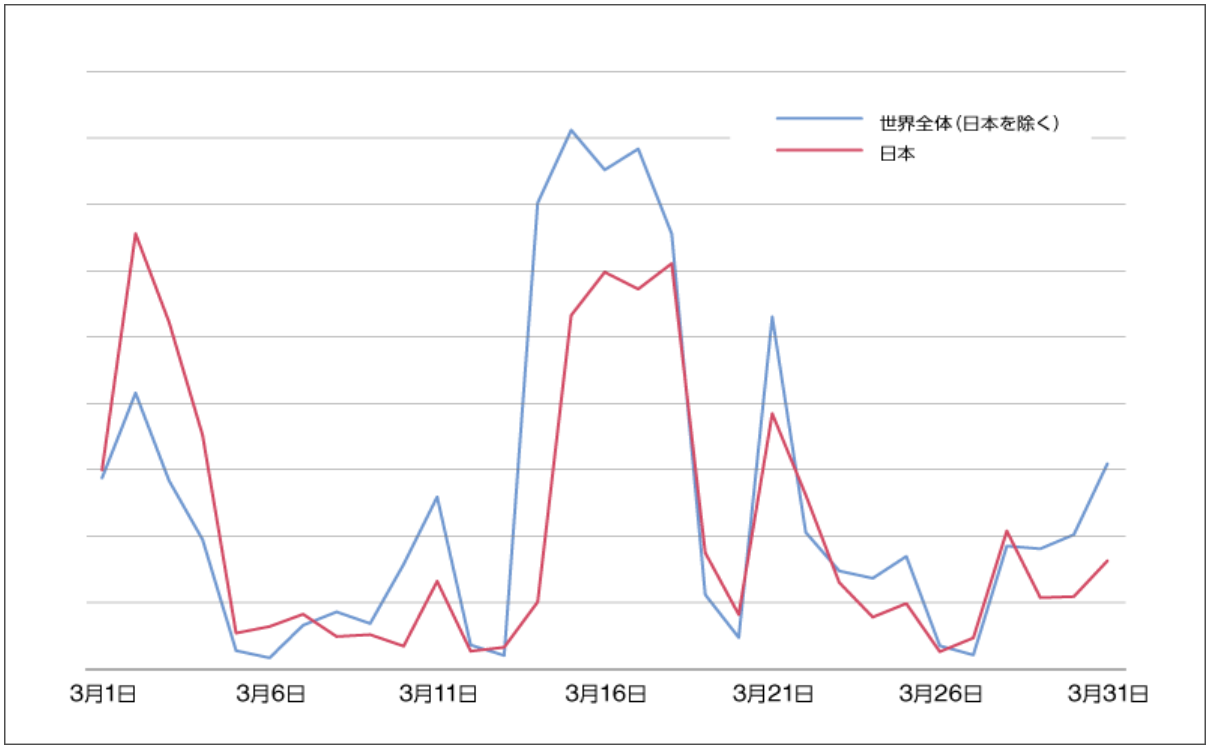
3 月の DOC/TrojanDownloader.Agent の検出数を国別にみると、日本が最も検出数が多い国でした。ヨーロッパを始めとしてさまざまな国や地域で検出されていることがわかります。



DOC/TrojanDownloader.Agent 検出数 TOP10

実際に、Lumen Technologies 社の Black Lotus Labs の報告においても Emotet ボットがさまざまな国で確認されています。上記 TOP10 内のイタリア、メキシコや南アフリカなどの国がボットの多い国として挙げられています。

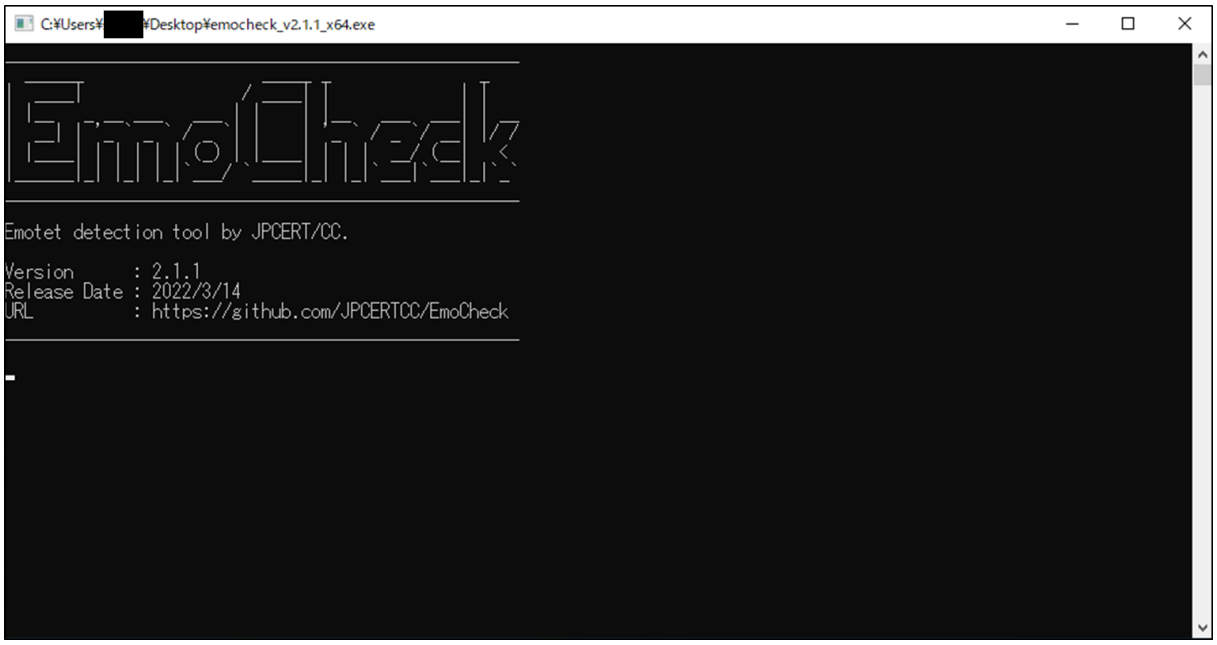
全世界の DOC/TrojanDownloader.Agent 検出数を日本国内と世界全体を分けたグラフは以下のとおりです。



国内と世界全体（日本を除く）の DOC/TrojanDownloader.Agent の日別検出数の推移（2022 年 3 月）

日本を除く世界全体と日本での検出傾向は大きく変わらないことがわかります。日本のみが狙われた攻撃というわけではなく、日本を含む世界全体が対象となった攻撃だと考えられます。そして、世界全体を狙った攻撃の中で、「2022 年 3 月に入り、Emotet に感染しメール送信に悪用される可能性のある.jp メールアドレス数が 2020 年の感染ピーク時の約 5 倍以上に急増しています」という JPCERT/CC の報告のとおり、日本国内での感染が拡大しボットが増加したことで、国内に向けたメールが増加したと考えられます。結果としては、ESET での DOC/TrojanDownloader.Agent の世界全体検出数の半数近く（46.1%）を日本における検出が占めていました。

今後も Emotet への感染を狙った攻撃が続いていく中で、ばらまきメールの本文に書かれる日本語がさらに巧妙化していくことに注意が必要です。
もし、自身で管理している端末が Emotet へ感染しているか不安な場合は、JPCERT/CC が提供している「EmoCheck」が有効です。このツールは、Emotet への感染の有無を調べることができます。現在、バージョン 2.2 が公開されており、2022 年 4 月にアップデートされた Emotet の挙動にも対応しています。



EmoCheck を起動した際の画面（2022 年 3 月）

ご紹介したとおり、2022 年 3 月は Emotet への感染を狙ったダウンローダーの検出数増加を確認しています。このような脅威の被害に遭わないためにも、添付ファイルを不用意に開かないことやメール本文に書かれた URL に不用意にアクセスしないことが重要です。また、添付ファイルを実行してしまった場合も、コンテンツの有効化をクリックしないようにしてください。そして、Emotet に感染した場合の影響や被害範囲を把握しておくことも対策として重要です。

■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

■JPCERT/CC | 「JPCERTCC/EmoCheck」
https://github.com/JPCERTCC/EmoCheck/releases
■JPCERT/CC | 「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
■Lumen Technologies | Black Lotus Labs「Emotet Redux」
https://blog.lumen.com/emotet-redux/

Canon

キヤノンマーケティングジャパン株式会社