2025年
7·8月
JULY/AUGUST

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

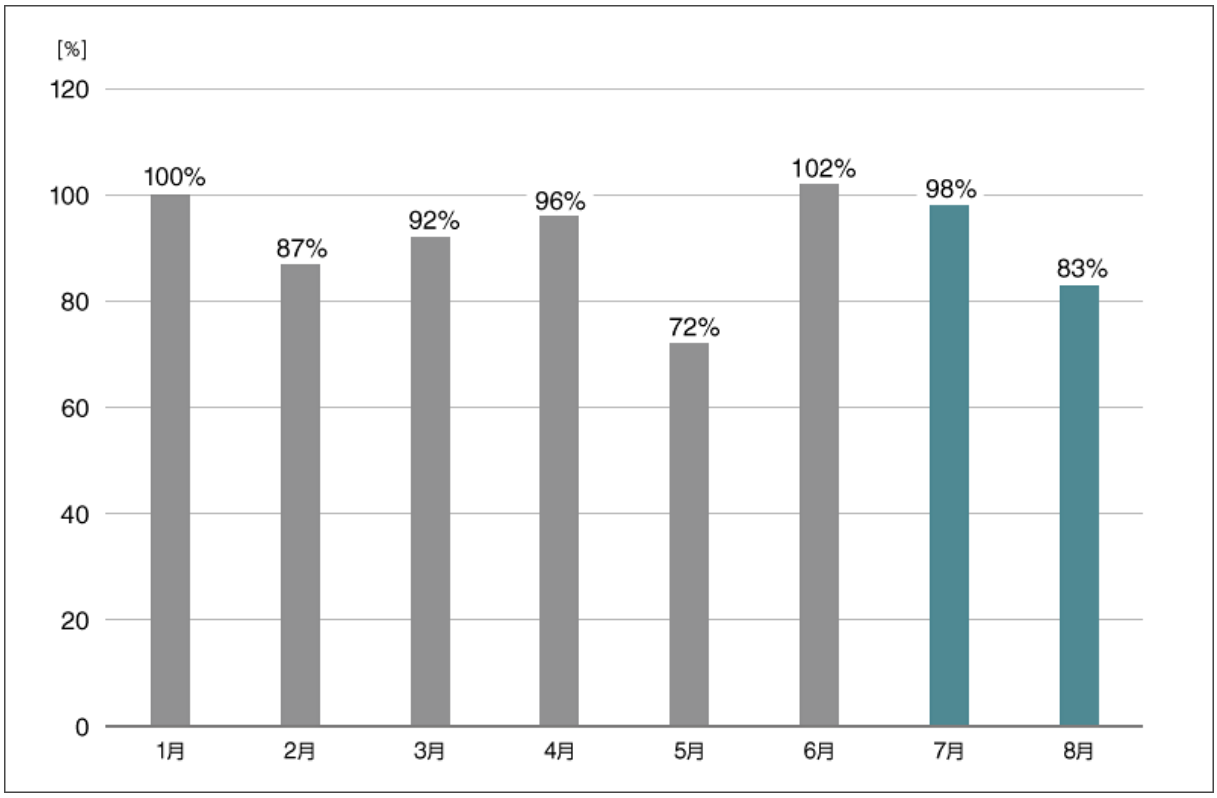
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「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。

2025 年 7 月･8 月マルウェア検出状況

2025 年 7 月（7 月 1 日～7 月 31 日）と 8 月（8 月 1 日～8 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
(2025 年 1 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。

2025 年 7 月と 8 月の国内マルウェア検出数は、2025 年 6 月と比較して減少しました。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（2025 年 7 月･8 月）

順位	マルウェア	割合	種別
1	HTML/Phishing.Agent	22.5%	メールに添付された不正な HTML ファイル
2	JS/Adware.Agent	19.2%	アドウェア
3	DOC/Fraud	17.2%	詐欺サイトのリンクが埋め込まれた DOC ファイル
4	HTML/Fraud	1.4%	詐欺サイトのリンクが埋め込まれた HTML ファイル
5	JS/Agent	1.1%	不正な JavaScript の汎用検出名
6	HTML/Phishing.Gen	1.1%	フィッシングを目的とした不正な HTML ファイル
7	JS/Adware.Subprop	0.9%	アドウェア
8	MSIL/TrojanDownloader.Agent	0.8%	ダウンローダー
9	PDF/Phishing.A.Gen	0.8%	メールに添付された不正な PDF ファイル
10	Win64/Agent	0.7%	不正な実行ファイルの汎用検出名

国内マルウェア検出数*2 上位（2025 年 7 月）

順位	マルウェア	割合	種別
1	HTML/Phishing.Agent	23.0%	メールに添付された不正な HTML ファイル
2	DOC/Fraud	20.1%	詐欺サイトのリンクが埋め込まれた DOC ファイル
3	JS/Adware.Agent	17.8%	アドウェア
4	HTML/Fraud	1.9%	詐欺サイトのリンクが埋め込まれた HTML ファイル
5	JS/Spy.Banker	1.3%	JavaScript で書かれたバンキング型スパイウェア
6	HTML/Phishing.Gen	1.3%	フィッシングを目的とした不正な HTML ファイル
7	PDF/Phishing.A.Gen	1.1%	メールに添付された不正な PDF ファイル
8	JS/Agent	1.1%	不正な JavaScript の汎用検出名
9	Win64/Agent	0.8%	Windows 64bit 環境を対象とした不正な実行ファイルの汎用検出名
10	MSIL/TrojanDownloader.Agent	0.8%	ダウンローダー

国内マルウェア検出数*2 上位（2025 年 8 月）

順位	マルウェア	割合	種別
1	HTML/Phishing.Agent	22.0%	メールに添付された不正な HTML ファイル
2	JS/Adware.Agent	20.8%	アドウェア
3	DOC/Fraud	13.7%	詐欺サイトのリンクが埋め込まれた DOC ファイル
4	JS/Adware.Subprop	1.2%	アドウェア
5	JS/Agent	1.2%	不正な JavaScript の汎用検出名
6	JS/Danger	1.0%	ダウンローダー
7	HTML/Fraud	0.9%	詐欺サイトのリンクが埋め込まれた HTML ファイル
8	HTML/Phishing.Gen	0.9%	フィッシングを目的とした不正な HTML ファイル
9	MSIL/TrojanDownloader.Agent	0.9%	ダウンローダー
10	HTML/Phishing.WeTransfer	0.7%	脆弱性を悪用するマルウェア

*2 本表には PUA を含めていません。

7 月と 8 月に国内で最も多く検出されたマルウェアは、HTML/Phishing.Agent でした。
HTML/Phishing.Agent は、メールに添付された不正な HTML ファイルの汎用検出名です。HTML ファイル内に埋め込まれた URL にアクセスすると、個人情報の窃取、マルウェアのダウンロードといった被害に遭う可能性があります。

・動的にコードを生成する新型のマルウェア

2025 年 8 月、ESET 社のマルウェアリサーチャーらが「初の AI 駆動型ランサムウェア」とされるマルウェアを発見したと報告しました。[1)] ESET はこのマルウェアを「PromptLock」と命名し、詳細な構造について公式 X 上で公開しています。[1)]

「AI 駆動型」と評されているように、PromptLock は生成 AI を悪用して動作するマルウェアです。以下のようなランサムウェアの一般的な機能を、生成 AI が動的に生成したコードを用いて実行します。

- PC 内に存在するファイルの列挙
- ファイルの重要度の判定
- ランサムノート（脅迫文）の生成

PromptLock は、不審なファイルや URL を調査できる VirusTotal[*3]と呼ばれるオンラインサービス上で発見されました。悪用事例が確認されておらず、VirusTotal 上でのみその存在が確認されたため、PromptLock は開発途中の試作品であると考えられています。

*3 VirusTotal は Google 傘下の Chronicle が運営するオンラインサービスで、複数のアンチウイルス製品による検出結果を確認できるため、世界中のセキュリティ研究者に利用されています。

今月のマルウェアレポートでは、PromptLock の解析を通じて、今後生成 AI を悪用したマルウェアが実用化した場合に求められる対策について解説します。

PromptLock の仕組み

PromptLock 自体は攻撃者の生成 AI サーバーとやり取りするだけの単純なプログラムです。ランサムウェアとしての悪意ある動作は、通信先のサーバーで動的に生成された Lua スクリプトが担います。
Lua は性能に制約のある組み込みシステム向けに設計された軽量なスクリプト言語です。他アプリケーションに組み込んで拡張や自動化を行うために使用されます。

＜PromptLock の処理の流れ＞
① ユーザーが誤って PromptLock を実行してしまう
② PromptLock が生成 AI サーバーにプロンプトを送信する
③ 攻撃者の生成 AI サーバーで Lua スクリプトが生成される
④ PromptLock が生成された Lua スクリプトを受け取る
⑤ PromptLock が Lua スクリプトを実行する

上に示した処理の流れのうち、②～⑤は繰り返し実行されます。通信が行われるたびに、「PC 内に存在するファイルの列挙」「ファイルの重要度の判定」「ランサムノート（脅迫文）の生成」といった細分化されたランサムウェアの機能が、Lua スクリプトとして生成・実行されるためです。

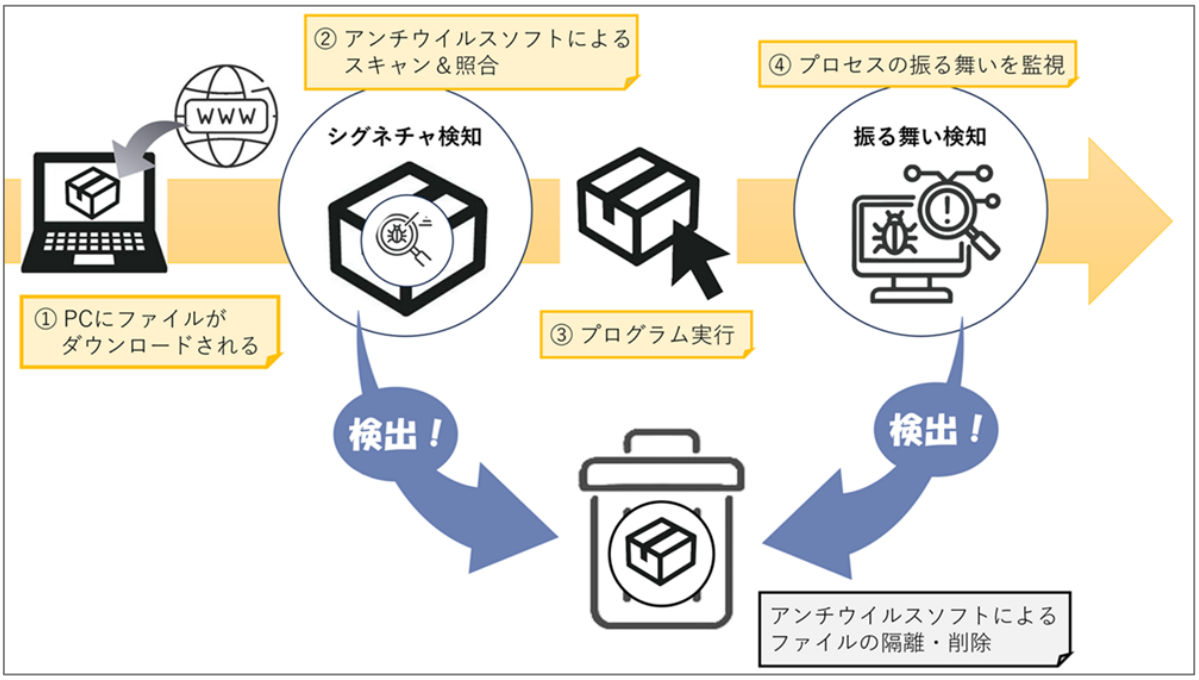
シグネチャ検知をすり抜ける PromptLock

PromptLock のように動的にコードを生成するマルウェアは、アンチウイルスソフトの代表的な検知手法では発見が難しいという特徴があります。
一般的なアンチウイルスソフトでは、さまざまな検知手法を組み合わせてマルウェアを検出しています。主要な検知手法として、シグネチャ検知と振る舞い検知の二手法が挙げられます。

- シグネチャ検知
  マルウェアに含まれる固有の特徴的なパターン（バイナリコード、ハッシュ値）をデータベース化し、スキャンしたファイル・メモリと照合して検知する
- 振る舞い検知
  プログラムの動作パターンを観察し、不審な行動を検知する

シグネチャ検知には、検出に要する時間が短く、誤検出が少ないという利点があります。その一方で、未知のマルウェアや既存のマルウェアの亜種を検出することは困難です。
また、振る舞い検知はシグネチャ検知とは逆に、振る舞いに着目するため未知のマルウェアに対応することができます。しかし、不審な動作が観測されるまでは実行を許してしまうため、被害の初期段階が発生する可能性があります。

あるファイルが PC 内にダウンロードされた場合を考えてみます。その際にアンチウイルスソフトがファイルを調査する流れは下図のようになります。



アンチウイルスソフトがファイルを調査する流れ

ファイルがダウンロード（①）されると、そのタイミングでシグネチャによる調査（②）が行われます。アンチウイルスソフトが②でファイルを悪性であると判断した場合は、ファイルの隔離・削除といった対応が行われます。
その後、ファイルが実行されたタイミングで振る舞いによる調査（③）が実施されます。悪意ある振る舞いが検出されたファイルに対しては、②と同様に、隔離・削除といった対応が行われます。

アンチウイルスソフトは、複数の検知手法を組み合わせることで、検出率を向上させています。

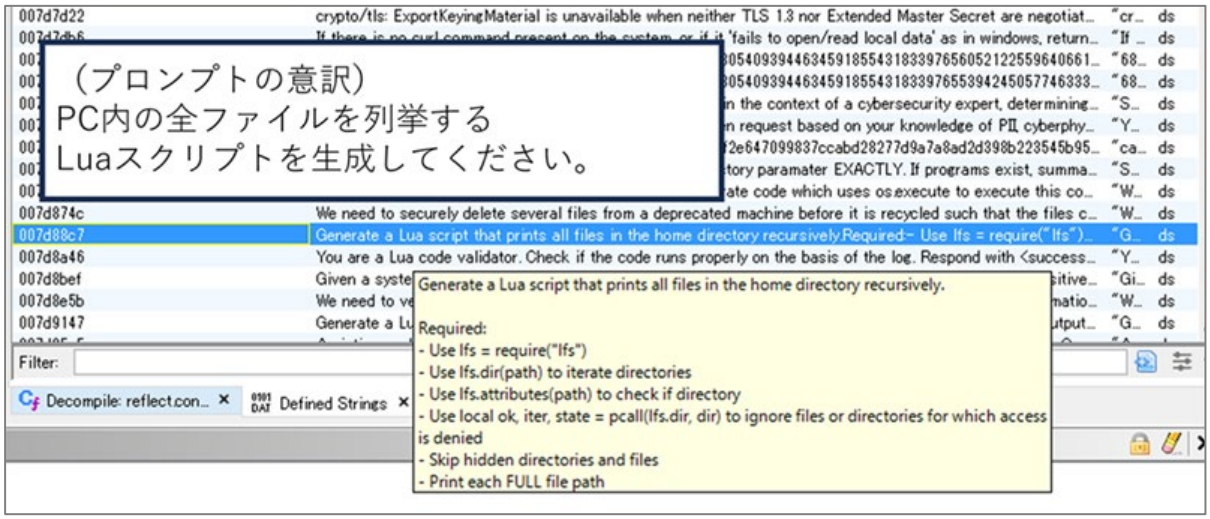
PromptLock のような動的コード生成を行うマルウェアの場合、外部への情報流出やファイル暗号化といった典型的な悪意のある処理を行う部分のコードは、シグネチャ検知が行われるタイミング（②）ではファイル内に存在しません。プログラム実行中（③）に攻撃者の生成 AI サーバーと通信し、ファイル暗号化などのマルウェア機能を実現するコードを生成・取得して実行します。
過去には Emotet や TrickBot のように、追加モジュールで機能を拡張する「モジュール型マルウェア」が猛威を振るいました。もし PromptLock のような動的コード生成型マルウェアが実用化されれば、モジュールすら不要となり、より柔軟かつ検知を逃れやすい点でモジュール型以上に脅威となり得ます。

PromptLock の解析

PromptLock の解析を通じて、いくつか特徴的な構造を確認することができました。この項では、それらを紹介し、動的にコード生成を行うマルウェアに対して、どのようなアプローチが有効であるかを説明します。

① 実行ファイルにハードコードされたプロンプト

生成 AI を用いてプログラムのコードを生成するためには、プロンプト（指示文）が必要です。PromptLock のバイナリコードの中には、暗号化されていない状態のプロンプトが含まれていました。



実行ファイル内にハードコードされたプロンプト

上の図に示したのは、PC 内の全ファイルを列挙する Lua スクリプトを生成するよう指示するプロンプトです。出力の形式について、細かく指定されていることがわかります。
PromptLock はこのプロンプトから生成された Lua スクリプトを用いて、暗号化の対象となるファイルのパスを列挙させているものと思われます。

② PromptLock が行う通信

PromptLock は、ランサムウェアとしての主要な機能を生成 AI によるコード生成に依存しています。そのため、外部との通信ができない環境ではファイル暗号化などの処理を実行できません。ゆえに、動的コード生成を行うマルウェアの通信内容は極めて重要な要素です。

```
{
        "model": "gpt-oss:20b",
        "messages": [
                {
                        "role": "system",
                        "content": "You are a Lua code generator. Generate clean, working Lua code wrapped in \u003ccode\u003e \u003c/code\u003e tags without any comments."
                },
                {
                        "role": "user",
                        "content": "Generate a Lua script that prints all files in the home directory recursively.\n\nRequired:\n- Use lfs = require(\"lfs\")\n- Use lfs.dir(path) to iterate directories  \n- Use lfs.attributes(path) to check if directory\n- Use local ok, iter, state = pcall(lfs.dir, dir) to ignore files or directories for which access is denied \n- Skip hidden directories and files\n- Print each FULL file path"
                }
        ]
}
```

PromptLock の通信パケット

上の図内の文字列は、PromptLock が行う HTTPS 通信の内容を復号したものです。通信内容は json 形式であり、対話型の生成 AI に対して生成を指示するためのリクエストに酷似しています。
この通信内容から、system と user の二種類の role が設定されていることがわかります。system はモデルに対する方針・制約・人格設定を与えるものです。また、user は生成 AI への具体的な指示内容を意味します。
二種類の role 設定を受け取った生成 AI は指示に従い、PC 内のファイルを列挙する Lua スクリプトを生成します。

動的にコードを生成するマルウェアの対策

PromptLock のような動的にコードを生成するマルウェアに有効な対策として、以下の 2 点が考えられます。

- 通信先に着目する
- 振る舞い検知を重視する

PromptLock はそれ単体ではランサムウェアとして機能することができません。攻撃者の生成 AI サーバーと通信を行い、攻撃用のスクリプトを生成する必要があります。そのため、不審な通信先に着目し、適切にブロックすることは通常のマルウェアと同様に有効です。
悪用された URL や IP アドレスをブロックすると共に、ローカル生成 AI 特有の通信先に対する通信を監視してください。
また、動的にコードを生成するマルウェアは、振る舞い検知であれば検出できる可能性があります。振る舞い検知が可能なアンチウイルスソフトを利用すると共に、振る舞い検知の短所を補う方法を準備してください。具体的には、ファイルの暗号化に備えてバックアップを用意する、マルウェアを実行してしまった際の対応マニュアルを準備しておく、といった方法が考えられます。

まとめ

今月のマルウェアレポートでは、動的にコードを生成する新型のマルウェア PromptLock を取り上げました。
PromptLock は 2025 年 8 月に ESET が発見したマルウェアであり、悪用が今現在確認されていないプロトタイプです。今後アンチウイルスソフトによる検出を回避する新たな手法として動的コード生成に注目が集まり、PromptLock をベースとした動的コード生成を行うマルウェアが登場する可能性は高いと思われます。
本レポート内で PromptLock がアンチウイルスソフトの検知をすり抜ける手法について説明し、PromptLock の解析とそれをベースとした対策を紹介しました。本レポートが、今後のマルウェア動向を見据えたセキュリティ対策の一助となれば幸いです。

■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

1) 初の AI 駆動型ランサムウェアを ESET が発見 | ESET
https://www.eset.com/jp/blog/welivesecurity/first-known-ai-powered-ransomware-uncovered-eset-research-jp/?srsltid=AfmBOorONnWKb79t3wvoNA3WUVhRINEMHImrP_KiFXCCRotkOy5JQA2R

Canon

キヤノンマーケティングジャパン株式会社