2024年
6月
JUNE

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

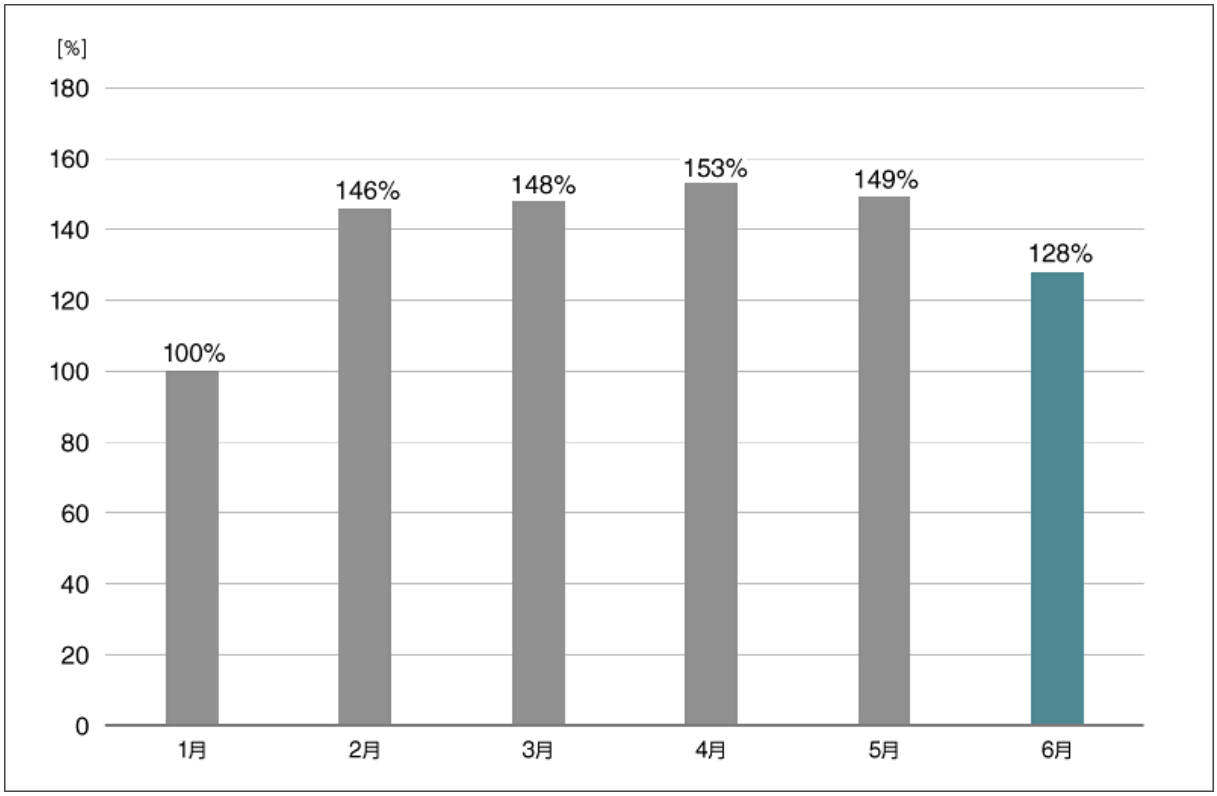
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「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 6 月マルウェア検出状況

2024 年 6 月（6 月 1 日～6 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

（2024 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。

2024 年 6 月の国内マルウェア検出数は、2024 年 5 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 6 月）

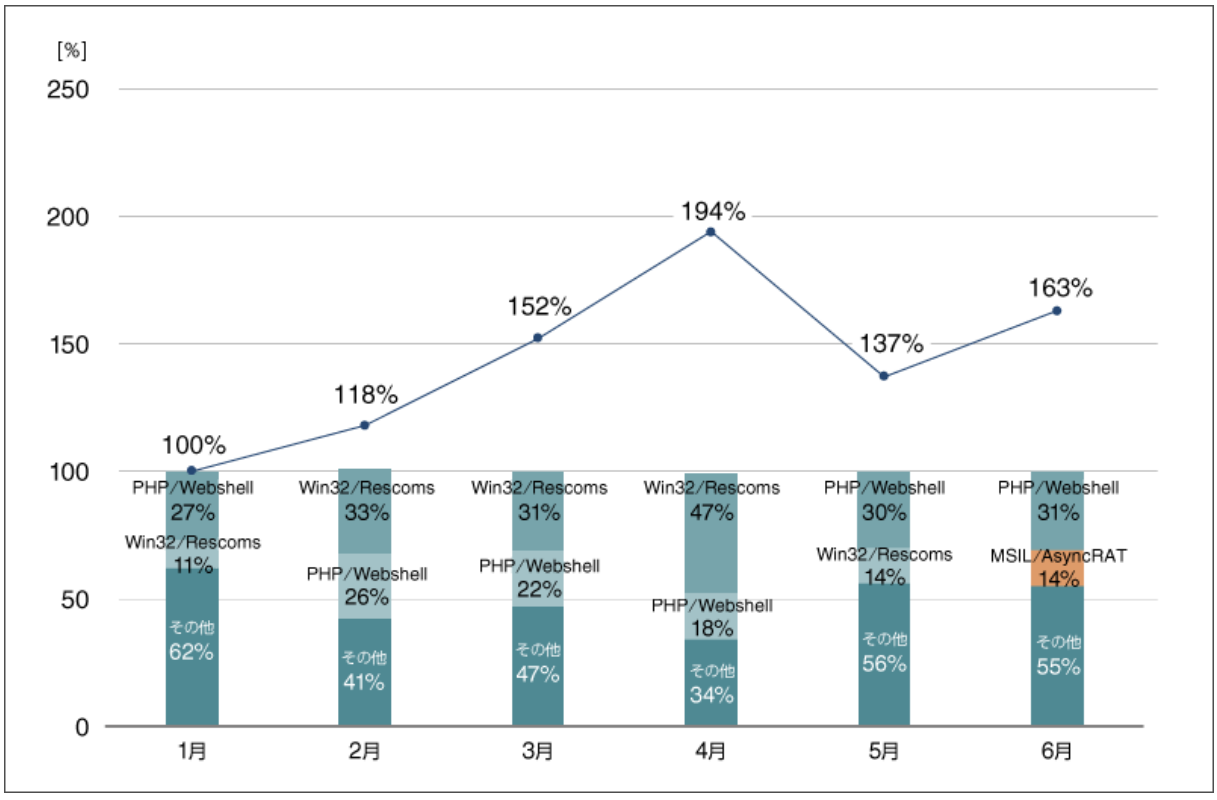
順位	マルウェア	割合	種別
1	JS/Adware.TerraClicks	20.5%	アドウェア
2	JS/Adware.Agent	15.4%	アドウェア
3	HTML/Phishing.Agent	13.4%	メールに添付された不正な HTML ファイル
4	DOC/Fraud	10.2%	詐欺サイトのリンクが埋め込まれた DOC ファイル
5	JS/Agent	3.5%	不正な JavaScript の汎用検出名
6	MSIL/TrojanDownloader.Agent	1.7%	ダウンローダー
7	JS/Danger.ScriptAttachment	1.5%	メールに添付された不正な JavaScript
8	HTML/Fraud	1.3%	詐欺サイトのリンクが埋め込まれた HTML ファイル
9	Win64/Riskware.PEMalform	1.0%	ブラウザハイジャッカー
10	JS/Adware.Sculinst	1.0%	アドウェア

*2 本表には PUA を含めていません。

6 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、Web サイト閲覧時に実行されるアドウェアです。感染すると、アドウェアサイトへのリダイレクト、アドウェアコンテンツの配布やブラウザー拡張機能としてアドウェアをインストールするなどの被害を生じさせる可能性があります。

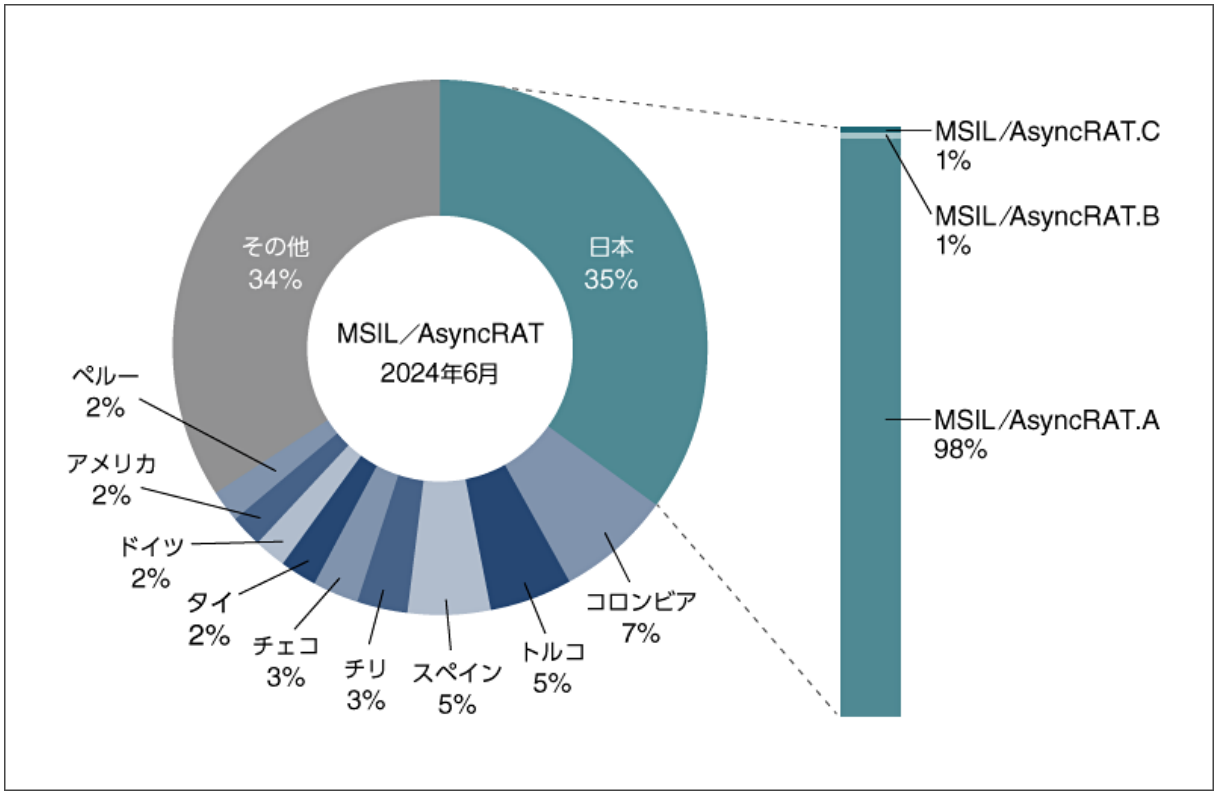
Backdoor マルウェアの増加と MSIL/AsyncRAT の急増

2024 年 1 月以降、国内では Backdoor に分類されるマルウェアの検出数が増加傾向にあることを確認しています。また各月の Backdoor マルウェアの検出内訳を見ると、基本的には PHP/Webshell と Win32/Rescoms の検出数が多いですが、6 月は MSIL/AsyncRAT の検出数が急増して Backdoor マルウェアの中で 2 番目に多かったことが判明しました。



Backdoor マルウェアの国内検出数推移とその内訳
（検出数推移は 2024 年 1 月の値を 100%として比較）

この MSIL/AsyncRAT について、6 月における全世界の検出割合を確認すると、日本が世界で最も多い 35%を占めていました。これは 2 番目に多かったコロンビアの 7%と比較すると 5 倍も検出数が多く、日本を標的にした攻撃が展開されたことが推測されます。また 6 月に日本で観測された MSIL/AsyncRAT の亜種の内訳を見ると、MSIL/AsyncRAT.A が大半を占めていました。この MSIL/AsyncRAT.A はオープンソースで公開されているオリジナルの AsyncRAT に対する検出名であり、MSIL/AsyncRAT.B と MSIL/AsyncRAT.C はそれから派生した亜種に対する検出名です。よって従来から存在するオリジナルの AsyncRAT を使った攻撃が、6 月に国内で活発に行われたことが分かります。



2024 年 6 月の MSIL/AsyncRAT の国別検出割合と国内における亜種の割合

AsyncRAT の概要

AsyncRAT はほかの PC を遠隔から監視または制御する RAT（Remote Access Tool）型のマルウェアです。2019 年にオープンソースのツールとして公開されましたが、その機能を悪用して攻撃キャンペーンで使用されたこともあり、多くのセキュリティ製品ではマルウェアとして検知します。
AsyncRAT は感染までの手法を変化させながら多様な攻撃に使用されています。その様子が分かる事例として、AsyncRAT が使用された過去の脅威活動を 3 つ紹介します。

1 つ目は ESET 社が報告 [1)]した事例で、2020 年にコロンビアの組織をターゲットとしたオペレーション Spalax と呼ばれる攻撃です。この事例では悪意のある PDF ファイルを添付したメールから組織への侵入が行われました。このメールは運転の違反を通知する内容や銀行口座の差し止めを通知する内容など、特定の組織を狙った文面ではなく汎用的なばらまき型の文面であり、被害者に感染させるマルウェアとして AsyncRAT を含む 3 つの RAT が使用されました。

2 つ目は Fortinet 社が報告 [2)]した事例で、2021 年に世界各国の航空会社を標的としたスピアフィッシング攻撃です。この事例は 1 つ目の事例と同様に悪意のある PDF ファイルを添付したメールから初期侵入が行われました。1 つ目の事例と異なり、航空会社を標的に絞った文面で従業員を騙すことで AsyncRAT への感染を引き起こしました。

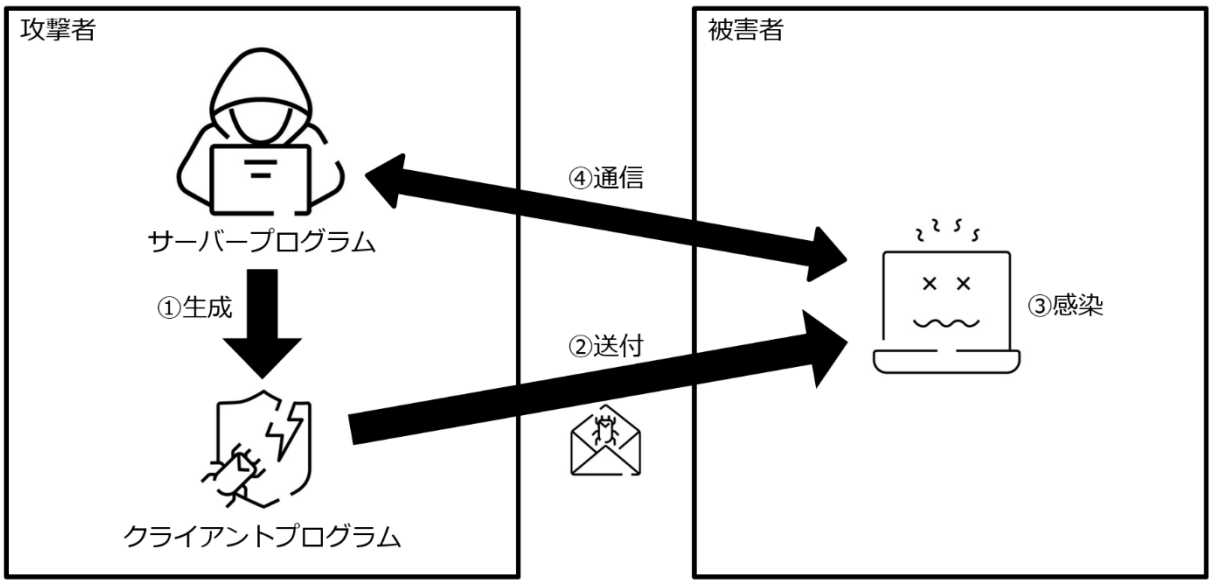
3 つ目は Splunk 社が 2023 年に報告 [3)]したスピアフィッシング攻撃の事例です。この事例では、上記 2 つの事例と同様にメールの添付ファイルから初期侵入が試みられましたが、その添付ファイルとして Microsoft OneNote が使用されました。

OneNote を悪用した攻撃が使われた背景の 1 つとして、インターネットから入手した Microsoft Office ファイルの VBA マクロがデフォルトで実行されないようになるアップデートを Microsoft 社が配信した [4)]ことが考えられます。セキュリティ対策の進歩に応じて攻撃者も悪用手法を変化させており、Splunk 社の事例は AsyncRAT も例外ではないことを表しています。

以上から、AsyncRAT は不特定多数をターゲットにした攻撃の事例から標的型攻撃の事例まで幅広く観測されていること、最新のセキュリティ対策を回避するために攻撃手法を変化させながら現在も攻撃者によって使用されていることが分かります。

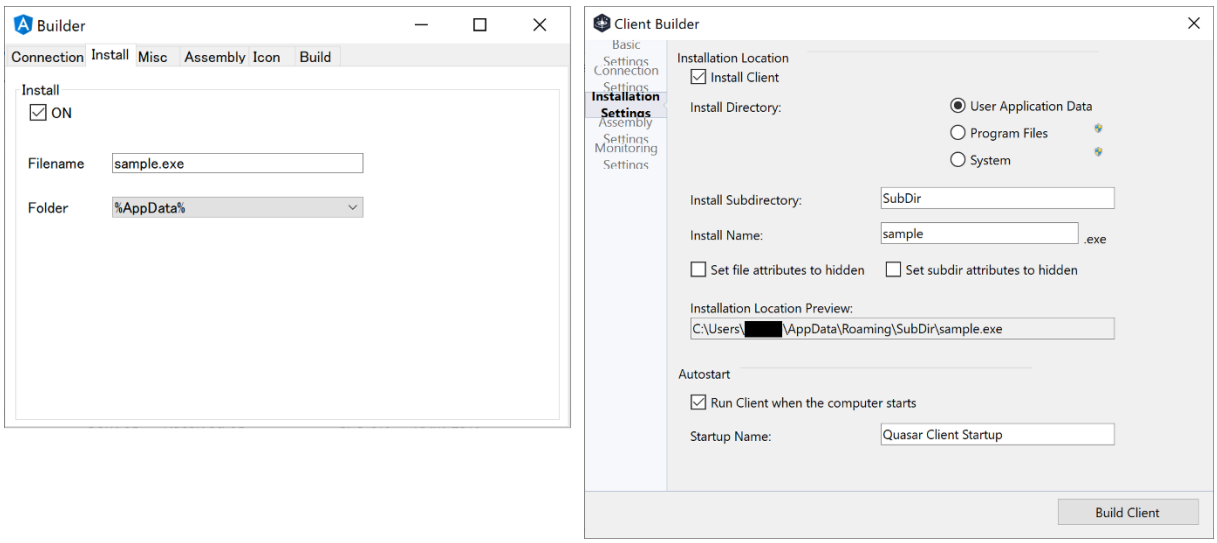
容易に使用可能な AsyncRAT

AsyncRAT が攻撃者に人気である理由として、オープンソースツールであり入手が容易であることに加え、ターゲットに感染させるプログラムの設定が単純明快で分かりやすいことが考えられます。
AsyncRAT を含む RAT の基本構成は、攻撃者の端末で操作するサーバープログラムと、ターゲットに感染させて接続を待ち受けるクライアントプログラムの 2 つです。クライアントプログラムはサーバープログラム上で作成することができ、その際に細かく機能を設定することが可能です。



RAT マルウェアが攻撃者端末とセッションを確立するまでの流れ

AsyncRAT は QuasarRAT と呼ばれるマルウェアから派生したものであり、QuasarRAT のソースコードを一部流用して作成されたと考えられています[5)]。ここからは AsyncRAT と QuasarRAT を比較しながら、AsyncRAT のクライアントプログラム作成がどのくらいシンプルであるかを確認してみます。
以下の画像では、AsyncRAT と QuasarRAT のクライアントプログラム作成時における、被害端末へのインストールに関する設定画面を比較しています。QuasarRAT では永続化（PC の再起動時に自動でマルウェアを実行する機能）の有無やプログラムのコピー先について細かく設定することができます。一方で、AsyncRAT はプログラムのコピー先を簡易的に設定することしかできません。しかし AsyncRAT のクライアントプログラムを実行すると、設定項目に無かった永続化を RUN レジストリキーによって行う挙動が確認できます。このように AsyncRAT には機能を大きく削らず設定項目を簡略化する工夫が見られ、誰もが容易に扱うことができるため、現在も攻撃者に利用されていることが推測されます。



AsyncRAT（左）と QuasarRAT（右）のクライアントプログラム作成画面の比較

AsyncRAT による被害を防ぐための対策

上述したとおり、6 月は国内における AsyncRAT の検出数が増加しており、今後も活動が本格化する恐れがあります。これらの脅威から組織を守るためには、感染を防ぐ対策に加えて、感染してしまった場合の影響を最小限に抑える体制を用意することが重要です。前者については OS やセキュリティ製品を最新の状態に保つこと、不審なメールに警戒するよう従業員に教育することなどが有効です。後者については不要なポートを閉じておくこと、SOC（Security Operation Center）のサービスを利用して組織の通信を監視すること、EDR 製品を活用して組織内の不審なアクティビティを監視すること、機密データをセキュリティが強固な場所に分離して容易にアクセスされないようにすることなどが有効です。

■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) Operation Spalax: Targeted malware attacks in Colombia | ESET
https://www.welivesecurity.com/2021/01/12/operation-spalax-targeted-malware-attacks-colombia/
2) Spear Phishing Campaign with New Techniques Aimed at Aviation Companies | Fortinet
https://www.fortinet.com/blog/threat-research/spear-phishing-campaign-with-new-techniques-aimed-at-aviation-companies
3) 打倒 AsyncRAT：検出と防御 | Splunk
https://www.splunk.com/ja_jp/blog/security/asyncrat-crusade-detections-and-defense.html
4) インターネットからのマクロは、Office で既定でブロックされます - Deploy Office | Microsoft
https://learn.microsoft.com/ja-jp/deployoffice/security/internet-macros-blocked
5) Quasar Family による攻撃活動 | JPCERT/CC
https://blogs.jpcert.or.jp/ja/2020/12/quasar-family.html

Canon

キヤノンマーケティングジャパン株式会社