2023年
12月
DECEMBER

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

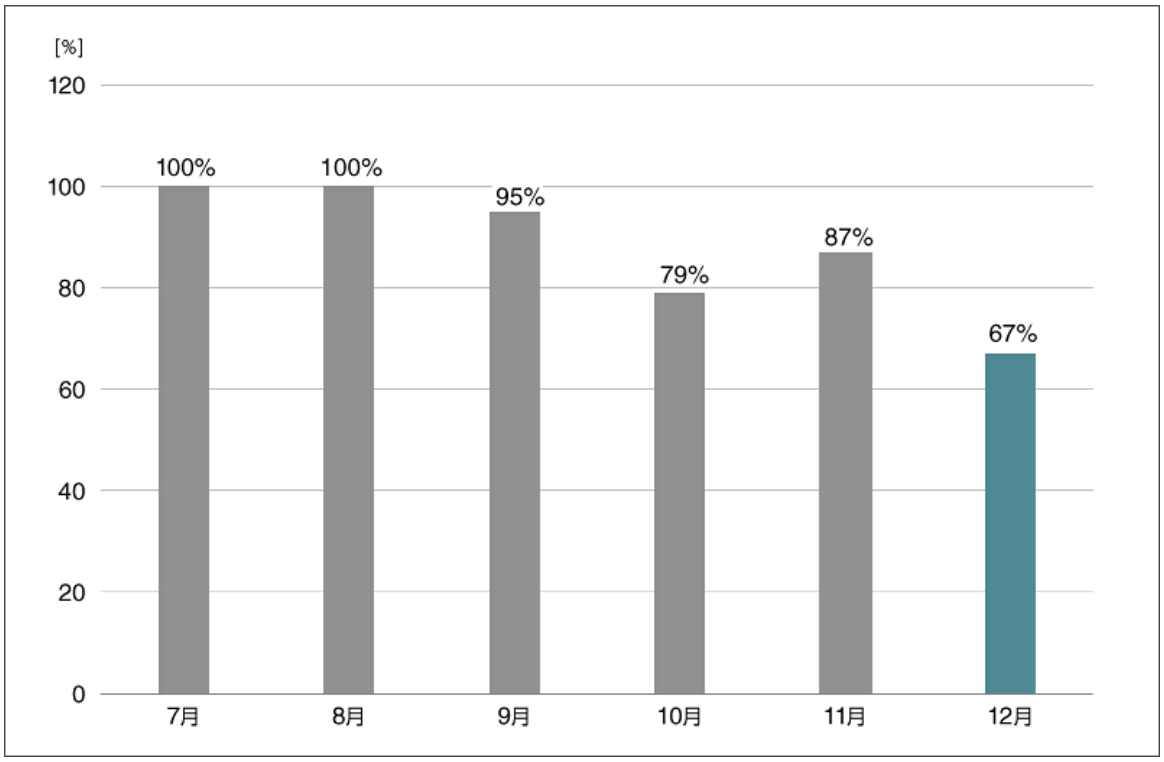
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「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。

2023 年 12 月マルウェア検出状況

2023 年 12 月（12 月 1 日～12 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 7 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。

2023 年 12 月の国内マルウェア検出数は、2023 年 11 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（2023 年 12 月）

順位	マルウェア	割合	種別
1	DOC/Fraud	16.7%	詐欺サイトのリンクが埋め込まれた DOC ファイル
2	JS/Adware.TerraClicks	13.3%	アドウェア
3	JS/Adware.Agent	11.6%	アドウェア
4	HTML/Phishing.Agent	11.0%	メールに添付された不正な HTML ファイル
5	JS/Adware.Sculinst	7.3%	アドウェア
6	JS/Agent	3.4%	不正な JavaScript の汎用検出名
7	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
8	MSIL/Spy.AgentTesla	1.2%	情報窃取型マルウェア
9	Win32/Exploit.CVE-2017-11882	1.2%	脆弱性を悪用するマルウェア
10	Win64/Riskware.PEMalform	0.9%	ブラウザーハイジャッカー

*2 本表には PUA を含めていません。

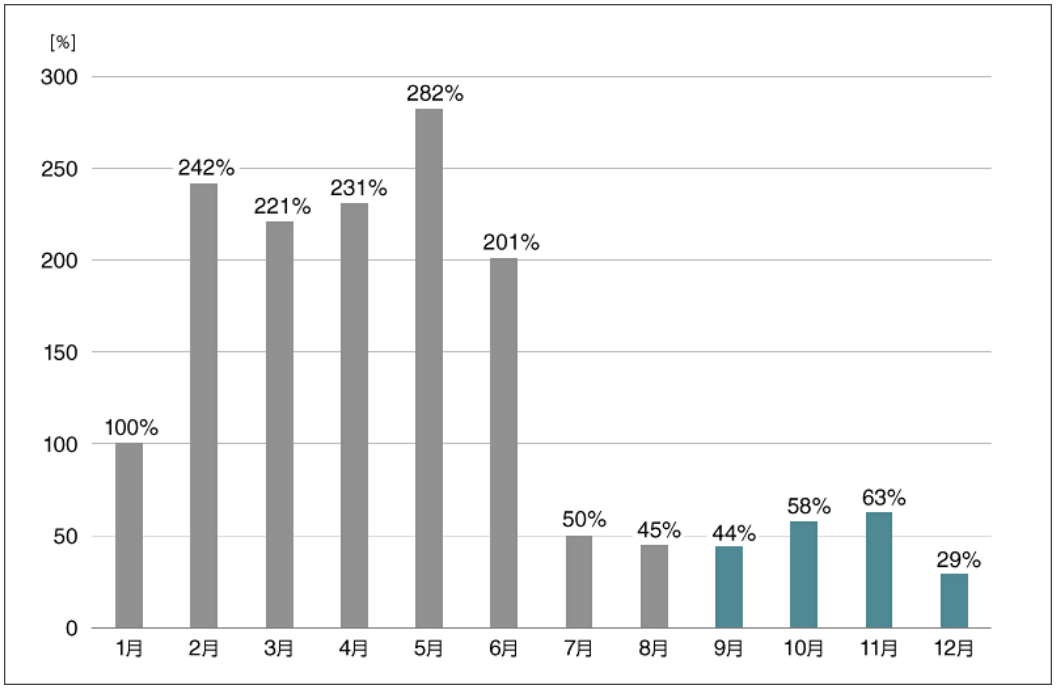
12 月に国内で最も多く検出されたマルウェアは、DOC/Fraud でした。
DOC/Fraud は、詐欺サイトへのリンクまたは詐欺を目的とした文章が書かれている Word ファイルです。主にメールの添付ファイルとして確認されています。2023 年上半期にはセクストーション（性的脅迫）を目的とした攻撃が確認されており、ESET 脅威レポート 2023 年上半期で報告されていました。

テイクダウン以降の Qakbot（クアックボット）について

2023 年 9 月マルウェアレポートで紹介したとおり、FBI によるテイクダウン作戦によって Qakbot ボットネットがテイクダウンされました。この作戦によって全世界で 70 万台以上の感染が疑われる端末も特定されています。ランサムウェアの配布にも利用されていた Qakbot ボットネットがテイクダウンされたことによって被害は減少傾向に向かっていましたが、2023 年 12 月 11 日頃から Qakbot への感染を狙ったフィッシングメールのキャンペーンを確認したと、Microsoft 社が X（旧 Twitter）で注意喚起を行いました。それによると、このキャンペーンは IRS（アメリカ合衆国内国歳入庁）職員を装い、サービス業をターゲットにしていたとされています。
注意喚起内ではフィッシングメールの件数は少ないと報告されていましたが、今後活動が活発化していく恐れがあるため、動向に注意が必要です。
続いて、テイクダウン以降の Qakbot の ESET 製品における検出状況を解説します。

ESET 製品における検出状況について

2023 年の Qakbot の ESET 製品における検出状況は以下のとおりです。
Qakbot は、ESET 製品では Win32/Qbot や Win64/Qbot などの検出名で検出されています。テイクダウンの翌月である 9 月以降のグラフを青色にしています。

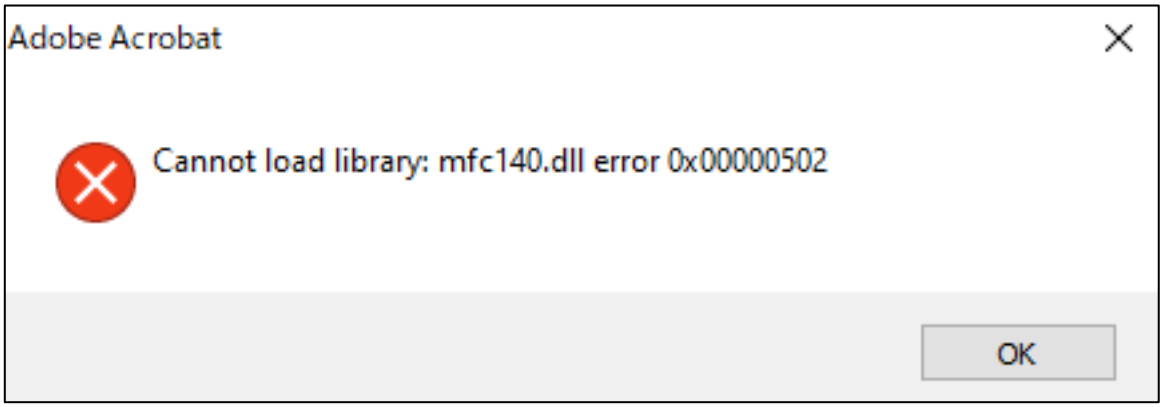


2023 年における Win32/Qbot と Win64/Qbot の全世界での検出数月別推移
（2023 年、全世界）
※2023 年 1 月の検出数を 100%として比較

2023 年 8 月のテイクダウン以降の検出数を見ると、10 月から 11 月にかけては増加していることがわかります。2023 年 9 月マルウェアレポートでも紹介した Qakbot の関係者・関連アクターによる活動継続や、テイクダウン時にアンインストールされずに端末に残された Qakbot の影響が考えられます。ほかにも、テイクダウンされた Qakbot を調査・研究するための試験用端末で検出された可能性も考えられます。
続いて、活動再開した Qakbot の変化について紹介します。

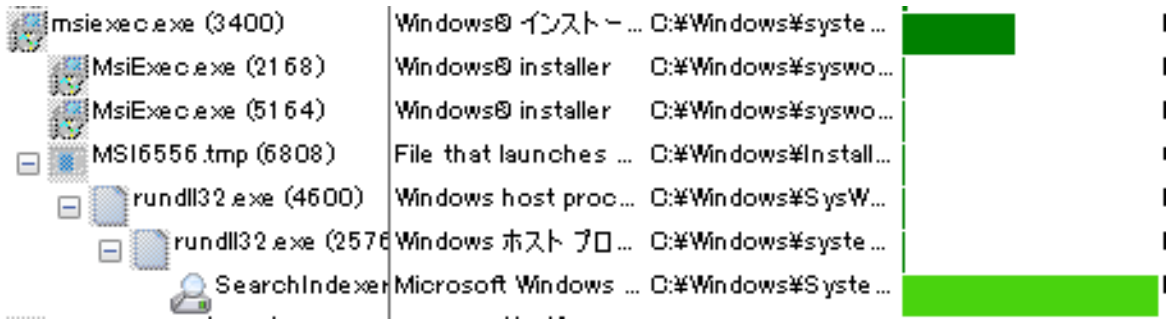
今回確認された Qakbot について

フィッシングメールに添付された PDF からダウンロードされた msi ファイルによって Qakbot がインストールされます。msi ファイルを実行すると、Adobe Acrobat を装ったエラー通知を出し、ユーザーに対して Adobe の正規プログラムであると誤認させます。



Adobe Acrobat を装ったエラー通知

今回確認した Qakbot の感染までの流れは以下のとおりです。



Qakbot 感染までの流れ

msi ファイルから起動される tmp ファイルが、rundll32.exe に悪意のある dll ファイルをバックグラウンドで実行させます。悪意のある dll ファイルが実行されることで、Qakbot へ感染します。

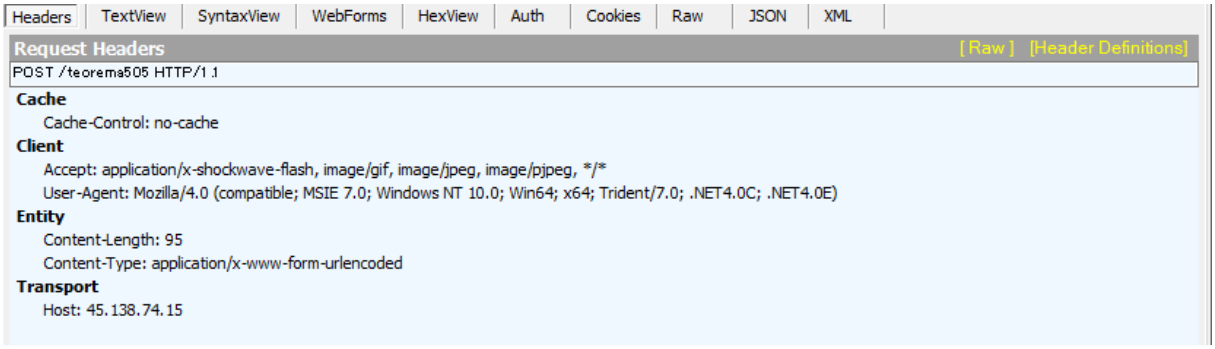
tmp ファイルが rundll32.exe に悪意のある dll ファイルを実行させている様子

この検体では、Qakbot は Windows 正規アプリケーションである SearchIndexer.exe を悪用して動作しています。
また、SearchIndexer.exe による C&C サーバーへの通信を確認しています。いずれの通信も「/teorema505」に対して通信を行っています。

HTTPS	45.[redacted]	/teorema505	258	text/html	searchindexer:8168
HTTPS	65.[redacted]	/teorema505	258	text/html	searchindexer:8168

Fiddler で確認した SearchIndexer.exe の通信

通信のヘッダー情報を確認すると、上記は POST 通信ということがわかります。



SearchIndexer.exe の通信詳細

SearchIndexer.exe による Qakbot 実行や「/terema505」への POST 通信を調べることで、感染の有無確認や感染防止に役立てることができます。ただし、今後通信先や Qakbot が実行されるアプリケーションは変わる可能性に注意が必要です。

まとめ

今回紹介したように、テイクダウンされた Qakbot について 12 月にフィッシングメールキャンペーンが確認されています。今回のキャンペーンの規模は大きくありませんでしたが、今後活動が活発化していく可能性も考えられます。小さな活動であっても流行につながる恐れがあるため、動向や感染手法について情報収集を行うことが重要です。情報収集先として IPA や JPCERT/CC をはじめとした機関やセキュリティベンダーから出される注意喚起を確認してください。また、収集した情報を組織内で共有してください。

■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

■ESET 脅威レポート 2023 年上半期 | ESET
https://www.eset.com/fileadmin/ESET/JP/Blog/threat-report/H1-2023_Threat-Report_JP_FINAL.pdf
■2023 年 9 月マルウェアレポート | サイバーセキュリティ情報局
https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware2309.html
■Microsoft Threat Intelligence | X（旧 Twitter）
https://twitter.com/MsftSecIntel/status/1735856754427047985
■JPCERT/CC インシデント報告対応レポート | JPCERT/CC
https://www.jpcert.or.jp/pr/2023/IR_Report2023Q2.pdf
■Qakbot Returns | K7 Security Labs
https://labs.k7computing.com/index.php/qakbot-returns/

Canon

キヤノンマーケティングジャパン株式会社