2023年
9月
SEPTEMBER

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

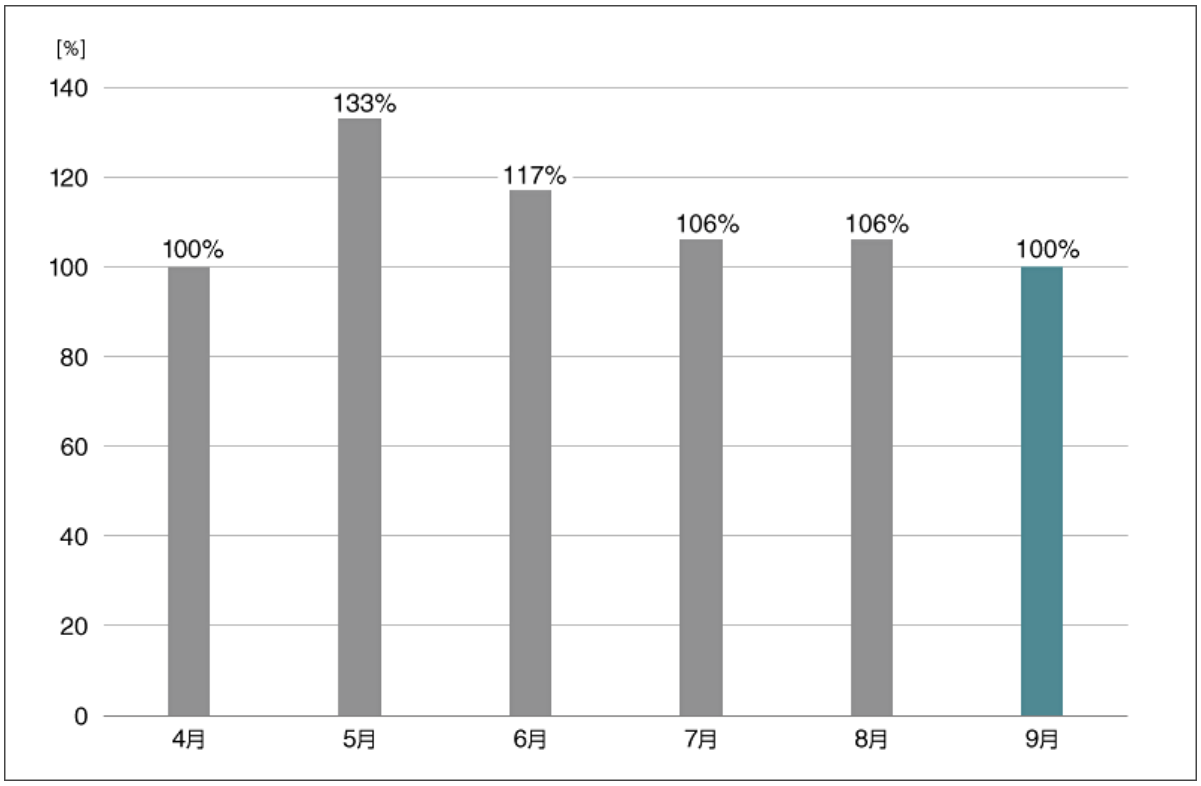
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「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 9 月マルウェア検出状況

2023 年 9 月（9 月 1 日～9 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
（2023 年 4 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 9 月の国内マルウェア検出数は、2023 年 8 月と比較して微減しました。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 9 月）

順位	マルウェア	割合	種別
1	DOC/Fraud	21.4%	詐欺サイトのリンクが埋め込まれた DOC ファイル
2	JS/Adware.Agent	15.2%	アドウェア
3	HTML/Phishing.Agent	12.0%	メールに添付された不正な HTML ファイル
4	JS/Adware.TerraClicks	7.4%	アドウェア
5	JS/Adware.Sculinst	5.2%	アドウェア
6	JS/Agent	3.9%	不正な JavaScript の汎用検出名
7	HTML/Fraud	2.6%	詐欺サイトのリンクが埋め込まれた HTML ファイル
8	Win32/Exploit.CVE-2017-11882	1.8%	脆弱性を悪用するマルウェア
9	JS/Adware.Subprop	1.3%	アドウェア
10	MSIL/TrojanDownloader.Agent	1.2%	ダウンローダー

*2 本表には PUA を含めていません。

9 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おり、2023 年ではセクストーション（性的脅迫）を目的としたものが確認されています。

Qakbot ボットネットのテイクダウン

2023 年 8 月 29 日、アメリカ連邦捜査局（FBI）と司法省（DOJ）はフランス、ドイツ、オランダ、ルーマニア、ラトビアと協力し、マルウェア Qakbot（クアックボット）のボットネットを解体する多国籍作戦（Operation Duck Hunt）を実施したと公表しました。この作戦は、多数の被害を出している Qakbot ボットネットのインフラを解体することを目的とした作戦です。この作戦によって、70 万台以上の感染が疑われる端末が特定され、Qakbot のアンインストールが行われました。加えて、Qakbot のアクターから約 900 万ドル（約 13 億 4,770 万円相当）の暗号資産（仮想通貨）を押収しています。ほかにも、Qakbot アクターによって侵害されたアカウント資格情報が特定され、無償のデータ漏えいチェックサイトである Have I Been Pwned へ提供されています。
Qakbot をアンインストールするために、FBI はボットネットの通信を FBI 管理のサーバーへリダイレクトするように変更し、法執行機関が作成したアンインストーラーを感染端末にダウンロードしました。このアンインストーラーは、感染端末をボットネットから切り離し、Qakbot を介した更なるマルウェアのダウンロードを防ぐように設計されています。アメリカの CISA（Cybersecurity and Infrastructure Security Agency）から今回の作戦に関連した Qakbot の詳細情報や IoC が提供されています。
この作戦によってテイクダウンされた Qakbot は、どのような脅威だったのかを解説します。

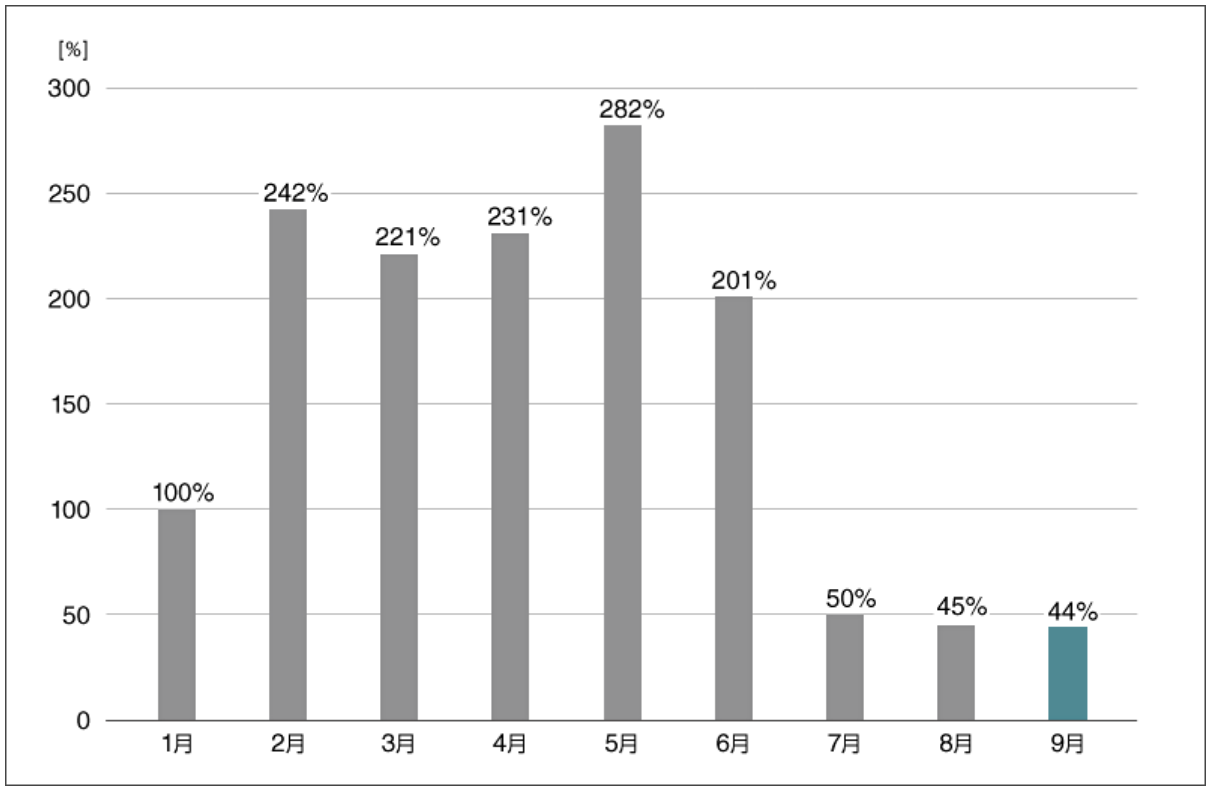
Qakbot（クアックボット）について

Qakbot（別名：Qbot、Pinkslipbot）は、2008 年頃から確認されているモジュール型のマルウェアです。モジュールによってさまざまな機能を有することができ、ESET 製品では Win32/Qbot や Win64/Qbot として検出します。Qakbot に感染すると、機密情報の窃取やほかのマルウェアをダウンロードされる被害に遭う可能性があります。実際に、REvil や Black Basta、Royal といったランサムウェアグループに利用されていました。また、非営利団体の The Shadowserver Foundation から公開された 2019 年 7 月から 2023 年 8 月までに Qakbot へ感染した端末に関するレポートによると、日本では約 40,000 台の端末が確認されていました。
主な感染経路としては、メールに添付されたファイルや本文に書かれた URL が確認されています。ダウンローダー

の中には、2022 年 5 月に確認された Windows サポート診断ツール（Microsoft Support Diagnostic Tool：MSDT）の脆弱性 CVE-2022-30190（Follina）を悪用したものや OneNote 形式のファイル、ISO ファイルを悪用したものがありました。

Qakbot の検出状況について

ESET 製品によって検出される Qakbot の検出状況の変化をまとめました。以下のグラフは、全世界における Win32/Qbot と Win64/Qbot の検出数の月別推移です。



Win32/Qbot と Win64/Qbot 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

検出数が多かった上半期と比較して、下半期は検出数が減少しています。そして、テイクダウン後の 9 月は、8 月と比較して微減しています。大きな変化が見られない理由として、テイクダウン時に端末がオフラインだったなどの理由によって、アンインストールされずに端末に残ってしまったものが検出された可能性があります。また、ほかの

マルウェア経由で Qakbot がダウンロードされてしまった可能性も考えられます。現在、Qakbot への感染を狙った大きな活動は確認されていませんが、Qakbot の関係者・関連アクターが活動を継続しているという報告も出ています。今後も検出状況を注視していきます。

テイクダウンされた脅威の復活について

今回の作戦によって Qakbot ボットネットは解体されましたが、Qakbot の関係者や関連アクターが活動継続している報告もあります。今後、Qakbot ボットネットの活動が再開する恐れがあります。実際に、テイクダウンされた脅威の活動が再開した事例もあります。有名なものとして、Ramnit や Emotet が挙げられます。報道でも話題になった Emotet は、2021 年 1 月にテイクダウンされ、2021 年 11 月に活動が再開しています。Ramnit は 2015 年にテイクダウンされたマルウェアですが、現在も活動が確認されています。実際に ESET 製品による国内の検出状況は、今月の検出数が 2023 年を通して最も多くなっていました。検出数全体は多くありませんが、依然として注意が必要です。

まとめ

Qakbot ボットネットが 8 月にテイクダウンされました。この作戦によって大きな脅威の 1 つが解体され、ランサムウェアといったほかのマルウェアをダウンロードされるといった被害が減ることが考えられます。一方、注意すべき点もあり、「Qakbot ボットネットを再形成するためにばらまきメールやフィッシングメールの配布といった活動」が起きる可能性があります。脅威動向を収集し、組織内へ情報共有・注意喚起を行ってください。
特に、感染経路がメールの添付ファイルである脅威は、活動再開時に新たなダウンローダーを使用するといった変化が見られることがあります。セキュリティ製品をはじめとしたシステム面の対策に加えて、ユーザーが添付ファイルを実行しないように手法を伝えていく必要があります。そのためにも、IPA や JPCERT 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。

■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 Japan
https://www.eset.com/fileadmin/ESET/JP/Blog/threat-report/H1-2023_Threat-Report_JP_FINAL.pdf
■Qakbot Malware Disrupted in International Cyber Takedown | U.S. Department of Justice
https://www.justice.gov/opa/pr/qakbot-malware-disrupted-international-cyber-takedown
■have I been pwned | have I been pwned
https://haveibeenpwned.com/
■Check your hack | Dutch National Police
https://www.politie.nl/en/information/checkyourhack.html#check
■FBI, Partners Dismantle Qakbot Infrastructure in Multinational Cyber Takedown | FBI
https://www.fbi.gov/news/stories/fbi-partners-dismantle-qakbot-infrastructure-in-multinational-cyber-takedown
■Qbot/QakBot Malware | CISA
https://www.cisa.gov/resources-tools/resources/qbotqakbot-malware
■Qakbot Historical Bot Infections Special Report | The Shadowserver Foundation
https://www.shadowserver.org/news/qakbot-historical-bot-infections-special-report/
■Windows の脆弱性「Follina」が招いた危険性 | サイバーセキュリティ情報局
https://eset-info.canon-its.jp/malware_info/special/detail/230411.html
■Identification and Disruption of QakBot Infrastructure | CISA
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-242a
■Qakbot-affiliated actors distribute Ransom Knight malware despite infrastructure takedown | Cisco Talos
https://blog.talosintelligence.com/qakbot-affiliated-actors-distribute-ransom/

Canon

キヤノンマーケティングジャパン株式会社