2023年
11月
NOVEMBER

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

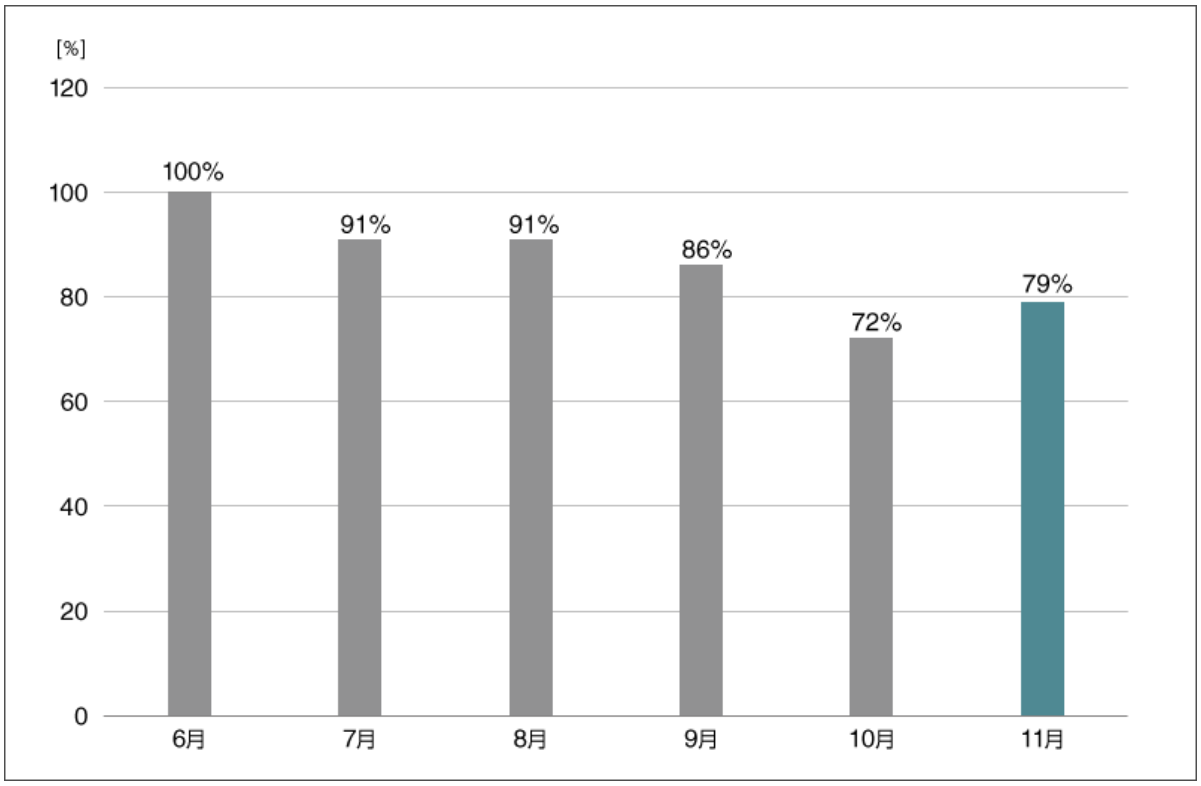
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「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 11 月マルウェア検出状況

2023 年 11 月（11 月 1 日～11 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 6 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 11 月の国内マルウェア検出数は、2023 年 10 月と比較して増加しました。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 11 月）

順位	マルウェア	割合	種別
1	DOC/Fraud	34.9%	詐欺サイトのリンクが埋め込まれた DOC ファイル
2	HTML/Phishing.Agent	9.1%	メールに添付された不正な HTML ファイル
3	JS/Adware.TerraClicks	8.9%	アドウェア
4	JS/Adware.Agent	8.4%	アドウェア
5	JS/Adware.Sculinst	5.8%	アドウェア
6	JS/Agent	3.5%	不正な JavaScript の汎用検出名
7	Win32/Exploit.CVE-2017-11882	1.5%	脆弱性を悪用するマルウェア
8	JS/ScrInject	0.9%	不正な JavaScript の汎用検出名
9	HTML/Hoax.Nomani	0.9%	偽の警告文を表示させる HTML ファイル
10	HTML/Phishing	0.8%	詐欺を目的とした不正な HTML ファイル

*2 本表には PUA を含めていません。

11 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。

利用の広がる QR コード

携帯電話の登場とともに、画像で簡単に URL や連絡先をやり取りできるツールとして QR コードは広く世の中に普及しました。近年、政府のキャッシュレス決済推進[*3]を背景に、QR コード決済という新しい利用の形も急速に広まっています。

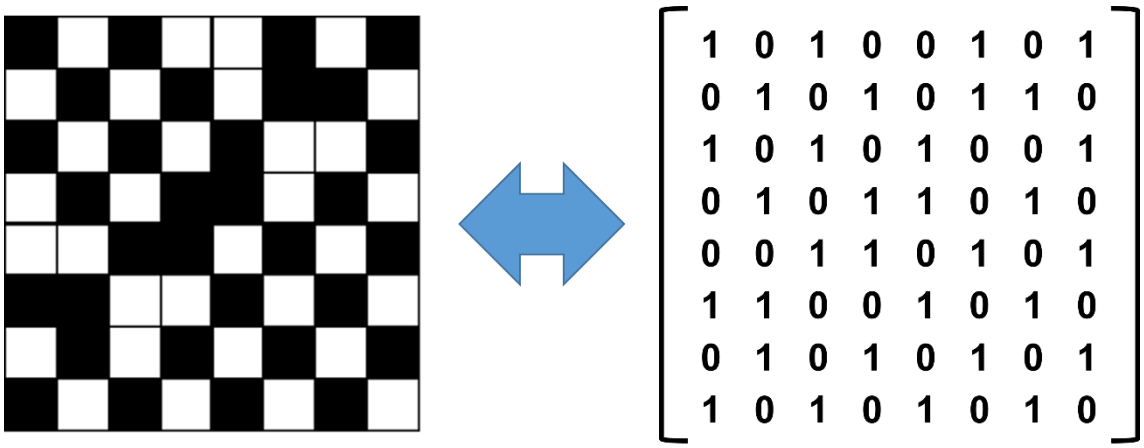
*3 総務省 ｜ 統一 QR「JPQR」の普及によるキャッシュレス化の推進

コンビニや自動販売機を利用する際に活用している方や財布を持ち歩く頻度が減ったという方もいるのではないでしょうか。
旧来のデータ共有の手法としても、チラシや広告など至る所で QR コードを目にします。
来年以降も、こうした利用シチュエーションは増えていくものと思われます。

利用の広がる QR コードですが、実は多くの悪用事例が発生しています。
2023 年 11 月にも、QR コード生成サービスに関連したトラブルが発生していました。
今月のマルウェアレポートでは、QR コードを悪用する手法とどのような対策が必要かを紹介します。

QR コードの仕組み

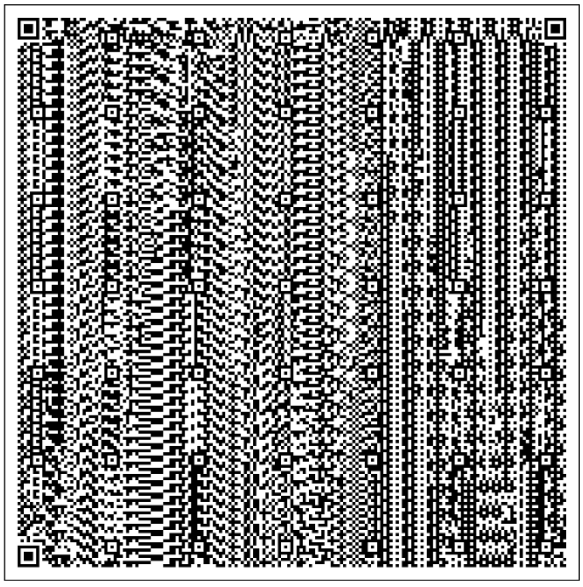
まず、簡単に QR コードの仕組みを紹介します。
QR コードはマトリクス型二次元コードに分類されます。マトリクスとは数学の行列を指しており、QR コードは正方形の縦横からなるセルを白と黒で塗り分けることで、0 と 1 で構成された行列のようにデータを表すことができます。



QR コードと行列の相互変換イメージ

上図に示したのはあくまでもイメージであり、実際にはより複雑な変換を行っていることに注意してください。
縦と横のセルの数は QR コードのバージョンによって決まっており、バージョン 1 であれば 21 セル、最大のバージョン 40 であれば 177 セルを並べることができます。

バージョン1



バージョン40

最小と最大の QR コード

上図に示したのは、ともにサイバーセキュリティ情報局のトップページの URL を埋め込んだ QR コードです。埋め込まれたデータが同じでも、バージョンによって異なる QR コードになることがわかります。

QR コードが持てるデータ量は、バージョン 40 でも 2,953 バイトと決して大きくはありません。これは漢字や仮名文字を用いた文章であれば、約 1,800 文字程度です。インターネットを介すれば一瞬で送ることができるデータ量ですが、画像経由で高速かつ手軽にやり取りできるのが QR コードの魅力です。
商品や情報の識別や管理に使用されるコードという意味では、QR コードはバーコードの仲間と考えることができます。しかし、バーコードは一次元コードであるため、情報の密度や誤り訂正機能の点で QR コードの方が優れています。

QR コードが備える便利な機能をいくつか紹介します。

- ファインダパターン

QR コード内には、いくつかの小さな正方形が配置されています。これがファインダパターンです。ファインダパターンによって、どの角度から QR コードを読み取っても正しいデータを得ることができます。

- 誤り訂正機能

QR コードには誤りを訂正する機能が備えられています。それによって、QR コードの一部が汚れていたり、破損していたりしても正しい読み取りを行うことができます。

QR コードを悪用したフィッシング

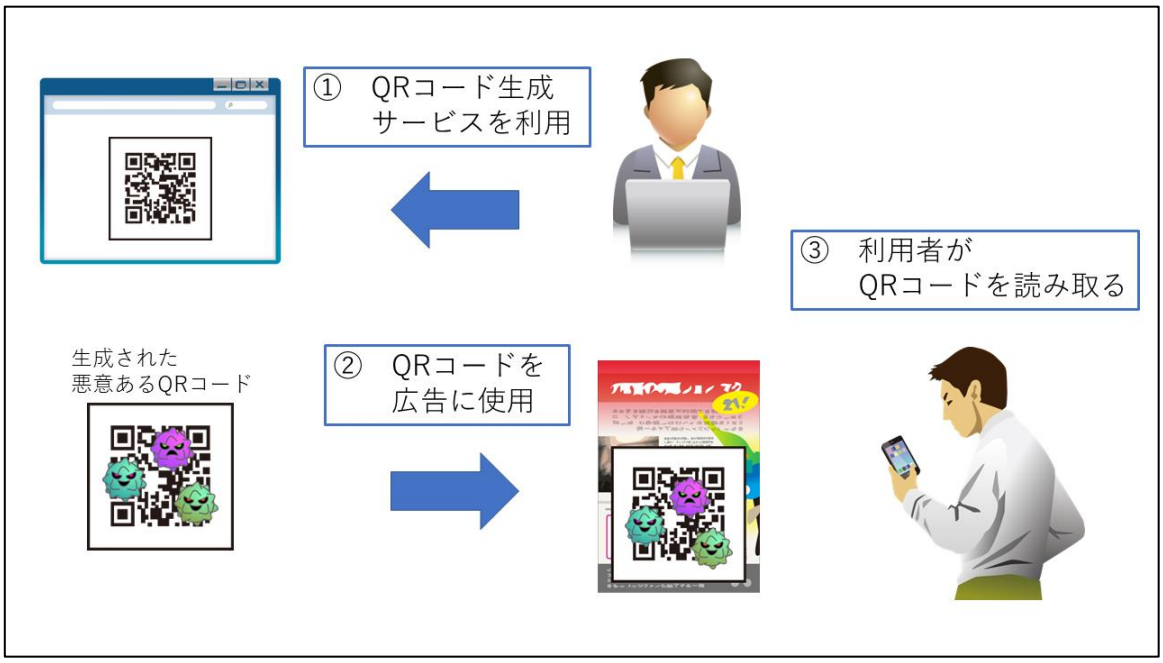
QR コード決済や会員登録のためのリンクなど、QR コードが利用されるシチュエーションには金銭の支払いが絡むシーンや個人情報を入力するシーンが目立ちます。
また、不審なメールに添付されていた URL や SNS のリンクと比べて、公式に提供されている QR コードはどうしても警戒心が緩む傾向にあります。
攻撃者はこのような状況や心理を利用して、巧妙なフィッシング詐欺を行います。こうした悪用のパターンについて紹介します。

- QR コード生成サービス

無料のオンラインサービスとして、無数の QR コード生成サービスが提供されています。URL やメールアドレス、文

字列を入力して、オプションを設定すると、それに応じた QR コードを生成してくれるサービスです。
非常に便利なサービスですが、中にはフィッシングを目的として提供されている QR コード生成サービスもあります。

そうした悪意のあるサービスを利用すると、QR コードのリンク先が自分の設定した Web ページから、サービス側が設定したフィッシングサイトにすり替えられてしまう可能性があります。すり替えられた QR コードが広告などに掲載された場合、厄介なフィッシングの構図が出来上がります。「公式の QR コードだから」と信頼した利用者は、その QR コードを通じてフィッシングサイトに誘導されてしまいます。



利用者がフィッシングサイトに誘導される流れ

- QR コードの偽装

駅など街中には、数多くの QR コードが掲載された広告が貼られています。利用者は QR コードを読み取るだけで、公式サイトにアクセスしたり、会員登録を行ったりすることができます。
QR コードの偽装では、それらの広告を利用し、QR コードの部分に上から別の QR コードをシールで貼り付けます。二重になっていることに気付かず QR コードを読み取った利用者は、フィッシングサイトなど悪意のあるアクセス先に誘導されます。
こうした攻撃は利用者の警戒が緩みやすいという点で、攻撃者にとってリターンが大きいと推測できます。また、仕組みが単純なため、誰でも簡単に再現できてしまいます。

上に挙げた二例は、QR コードを利用する人々が注意深く確認すれば被害を未然に防げる可能性があります。しかし、日常生活で何気なく利用する QR コードに対し、常に警戒し続けられる人は多くはありません。だからこそ、事前に正しい対策を理解することが大切です。

QR コードの悪用への対策

QR コードの悪用への対策は、提供者と利用者の両面で考えることができます。

QR コードを提供する側で行える対策としては、以下のようなものが考えられます。

- QR コードは信頼できる方法で作成する
- 実際に操作して、QR コードが想定どおりに機能しているか確認する
- QR コードが悪用されていないか定期的に確認する

プログラミングの知識があれば、Python のライブラリーなどを用いて QR コードを生成することもできます。QR コードに限らず、外部のサービスを利用するときは、サービス内部で行われている処理がブラックボックスであることに留意してください。

利用者側で行える対策としては、以下のようなものが考えられます。

- カメラアプリの設定を確認し、自動的にアクセスする機能などがあればオフにする
- 読み取りには信頼できるアプリを使用する
- ブラウザーの設定を見直す
- アプリや OS のバージョンは可能な限り最新の状態にする
- セキュリティソフトを使用する

まとめ

キャッシュレス決済での利用が拡大している QR コードについて仕組みを解説し、どのように悪用されるのかを紹介しました。
QR コードは非常に便利な技術であり、今後も利用が広がるものと思われます。一方で、利用シーンやその特性から攻撃者のターゲットにもなっています。
未知の攻撃に対しては、対策や警戒も難しいものです。だからこそ、どのような技術が使われているのか、どのように悪用される可能性があるのかを理解することが重要です。

提供者や利用者に求められる対策について、「QR コードの悪用への対策」の項で紹介しました。安全かつ便利に技術を活用するために、QR コードを使用する環境を見直し、上記の対策を実施してみてください。

■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

■総務省 | 統一 QR「JPQR」の普及によるキャッシュレス化の推進

https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r02/html/nd266250.html

Canon

キヤノンマーケティングジャパン株式会社