2022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

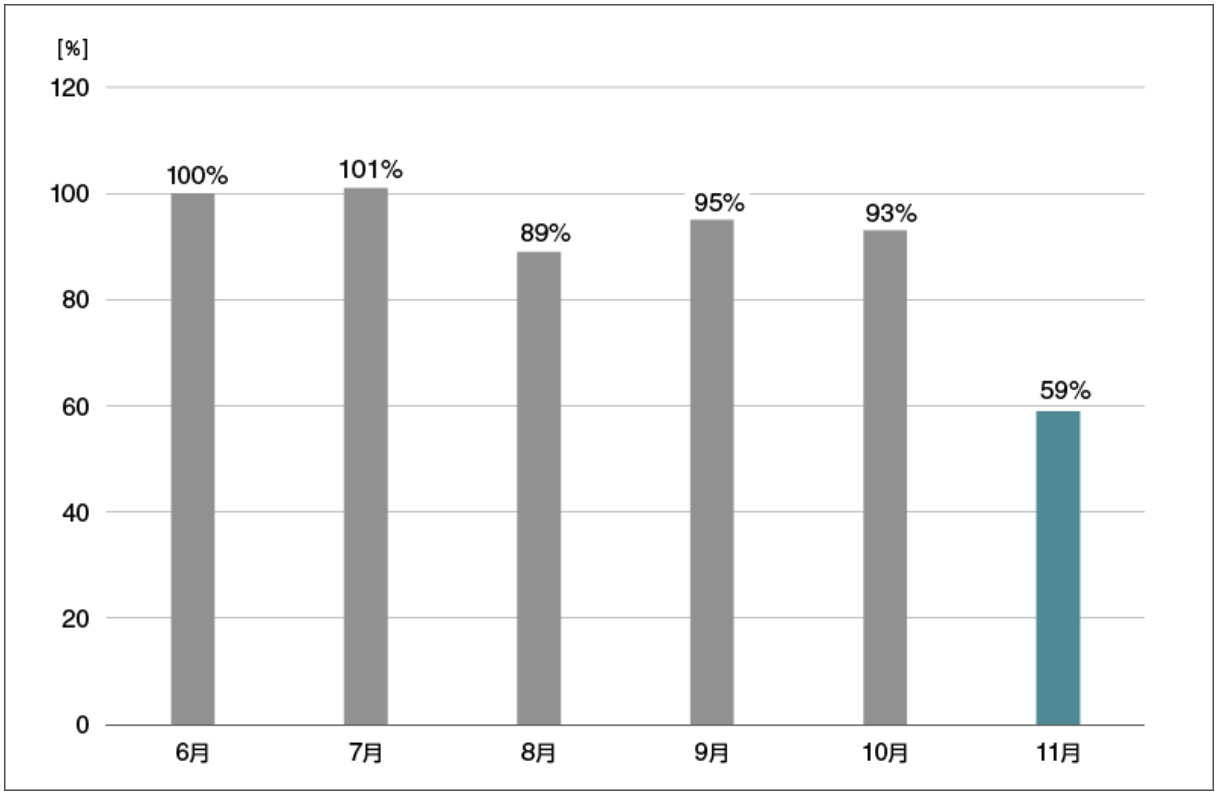
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「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。

2022 年 11 月マルウェア検出状況

2022 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
(2022 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。

2022 年 11 月の国内マルウェア検出数は、2022 年 10 月と比較して大きく減少しました。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（2022 年 11 月）

順位	マルウェア	割合	種別
1	JS/Packed.Agent	12.3%	パックされた不正な JavaScript の汎用検出名
2	JS/Adware.Agent	11.3%	アドウェア
3	JS/Adware.TerraClicks	7.5%	アドウェア
4	DOC/TrojanDownloader.Agent	5.7%	ダウンローダー
5	HTML/Phishing.Agent	3.9%	メールに添付された不正な HTML ファイル
6	JS/Adware.Sculinst	3.5%	アドウェア
7	HTML/Pharmacy	3.5%	違法薬品の販売サイトに関連する HTML ファイル
8	HTML/FakeAlert	3.3%	偽の警告文を表示させる HTML ファイル
9	HTML/ScrInject	2.0%	HTML に埋め込まれた不正スクリプト
10	MSIL/Kryptik	1.5%	難読化された MSIL で作成されたファイルの汎用検出名

*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、JS/Packed.Agent でした。
JS/Packed.Agent は、パッカーと呼ばれる圧縮ツールを使い、自己解凍形式で圧縮した JavaScript のマルウェアです。ファイルが圧縮されると符号化により元のデータから変化します。このようにデータを容易に難読化することができるため、パッカーはシグネチャーを基にマルウェアを判定するセキュリティ製品の検出から回避させたり、解析しにくくさせたりする目的で、マルウェアに悪用されることがあります。

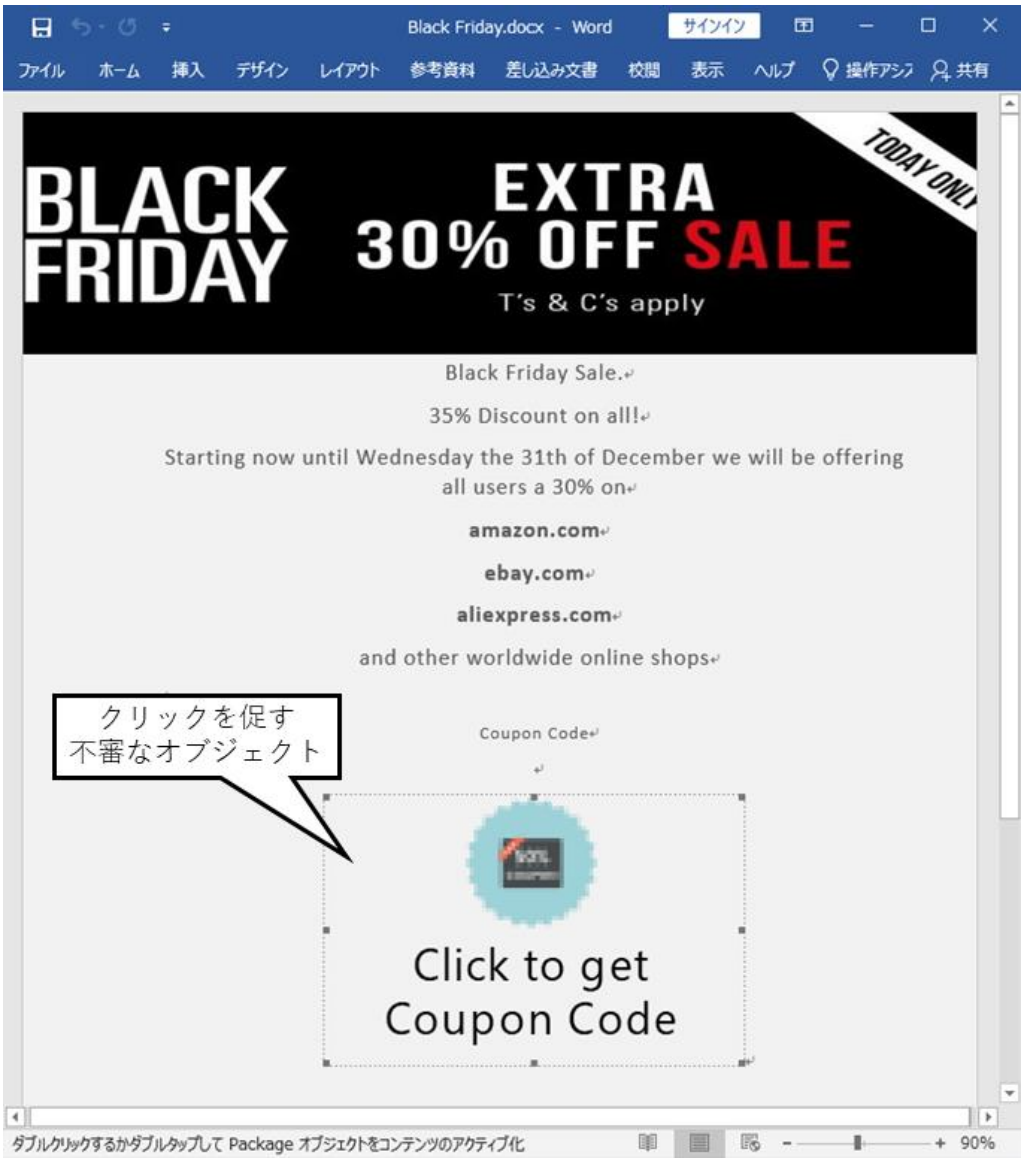
11 月の下旬はブラックフライデーおよびサイバーマンデーと呼ばれる、EC サイトや小売店の大規模なセールが開催されました。このセールに向けてサービス提供者はユーザーに集客メールを配信して購買を促しますが、悪意のある攻撃者にとっても集客メールを装ったスパムメールをばらまく絶好の機会となります。今回はブラックフライデーに便乗してマルウェアへの感染を狙ったマルスパムを紹介します。

サイバーセキュリティラボでは、ブラックフライデーで使用できるクーポンを添付したというマルスパムを確認しました。メールの件名や本文には割引価格で商品を購入できる、期間限定のセールである、といった主旨の内容が記載されており、メール受信者の購買意欲を掻き立たせて添付ファイルの確認へと誘導しています。

ブラックフライデーに便乗したスパムメールの例

メールには「Black Friday.zip」という ZIP ファイルが添付されています。この ZIP ファイルからは「Black Friday.docx」という DOCX ファイルが展開されます。DOCX ファイル内の文書下部には、クーポンコードが取得できるかのように誤認させてクリックを促す不審な OLE（Object Linking & Embedding）オブジェクト*3 が埋め込まれています。

*3 Windows のアプリケーション間でデータを連携または共有するための仕組みです。

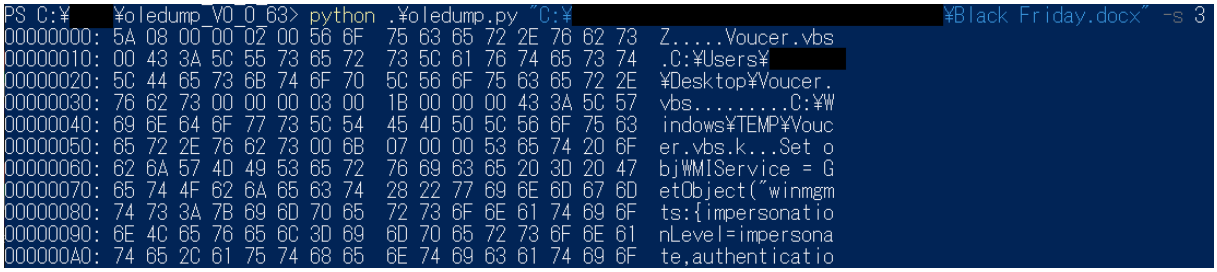


メールに添付された DOCX ファイル

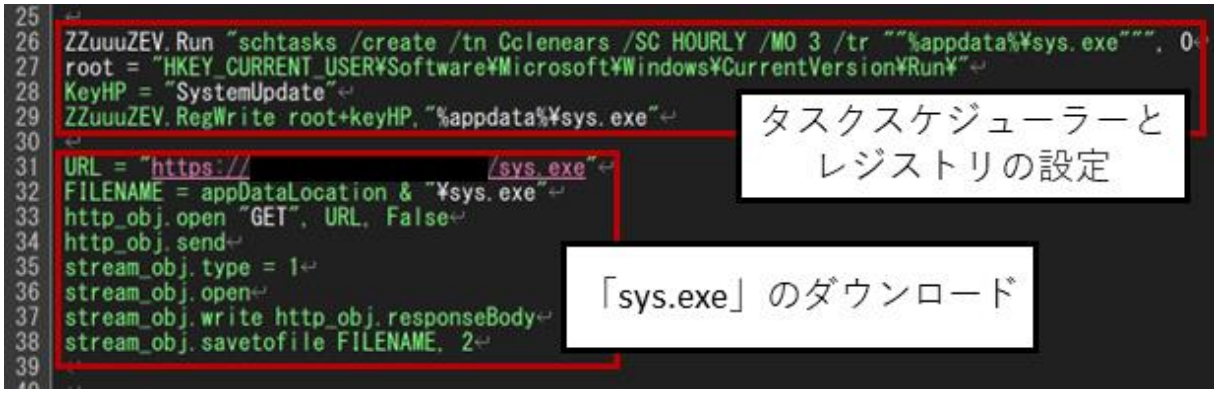
OLE オブジェクトを解析するツール*4 を使用して内部データを解析すると、不審な VBScript の埋め込みが確認できます。この VBScript には以下に示す処理が実装されており、OLE オブジェクトが埋め込まれた部分をダブルクリックすることでスクリプトが実行されマルウェアに感染する可能性があります。

① 外部サーバーに通信を行い、「sys.exe」という名前の EXE ファイルをダウンロードする。
② 「sys.exe」が 3 時間ごとに実行されるよう、「Cclenears」という名前のタスクをタスクスケジューラーに登録する。
③ PC 起動時に「sys.exe」が実行されるようにレジストリを設定する。
④ 「sys.exe」が実行され、PC の情報が窃取されたり遠隔から PC を操作されたりする。

*4 oledump.py Quick Reference | SANS



DOCX ファイルに存在する OLE オブジェクトの内部データ



OLE オブジェクトに含まれている VBScript コードの一部

今回はブラックフライデーに便乗したマルスパムを紹介しましたが、同様にブラックフライデーに便乗したフィッシングメールも確認*5 されています。また、ブラックフライデーのセール期間中にスパムメールが増加するという報告*6 もあります。ブラックフライデーに限らず、クリスマスセールや各オンラインストアのセールに合わせて、スパムメールが増加する可能性は十分あります。よってこういったスパムメールからマルウェア感染や個人情報窃取の被害を防ぐために、以下に示すような対策を心掛けてください。

- 利用したことのないサービスからの広告メールは無視する。
- メール内のリンクや添付ファイルを安易にクリックしない。
- Web ブラウザーのブックマークや公式アプリからサービスにアクセスする。

*5 10 to 15 Percent of Black Friday Emails Are Malicious | Vade Secure
*6 Gearing up for Black Friday: online shopping threats in 2022 | Kaspersky

---

■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

- oledump.py Quick Reference | SANS
  https://www.sans.org/posters/oledump-py-quick-reference/
- 10 to 15 Percent of Black Friday Emails Are Malicious | Vade Secure
  https://www.vadesecure.com/en/blog/10-to-15-percent-of-black-friday-emails-are-malicious
- Gearing up for Black Friday: online shopping threats in 2022 | Kaspersky
  https://securelist.com/black-friday-report-2022/108042/

Canon

キヤノンマーケティングジャパン株式会社