2021年
10月
OCTOBER

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

Canon キヤノンマーケティングジャパン株式会社

はじめに

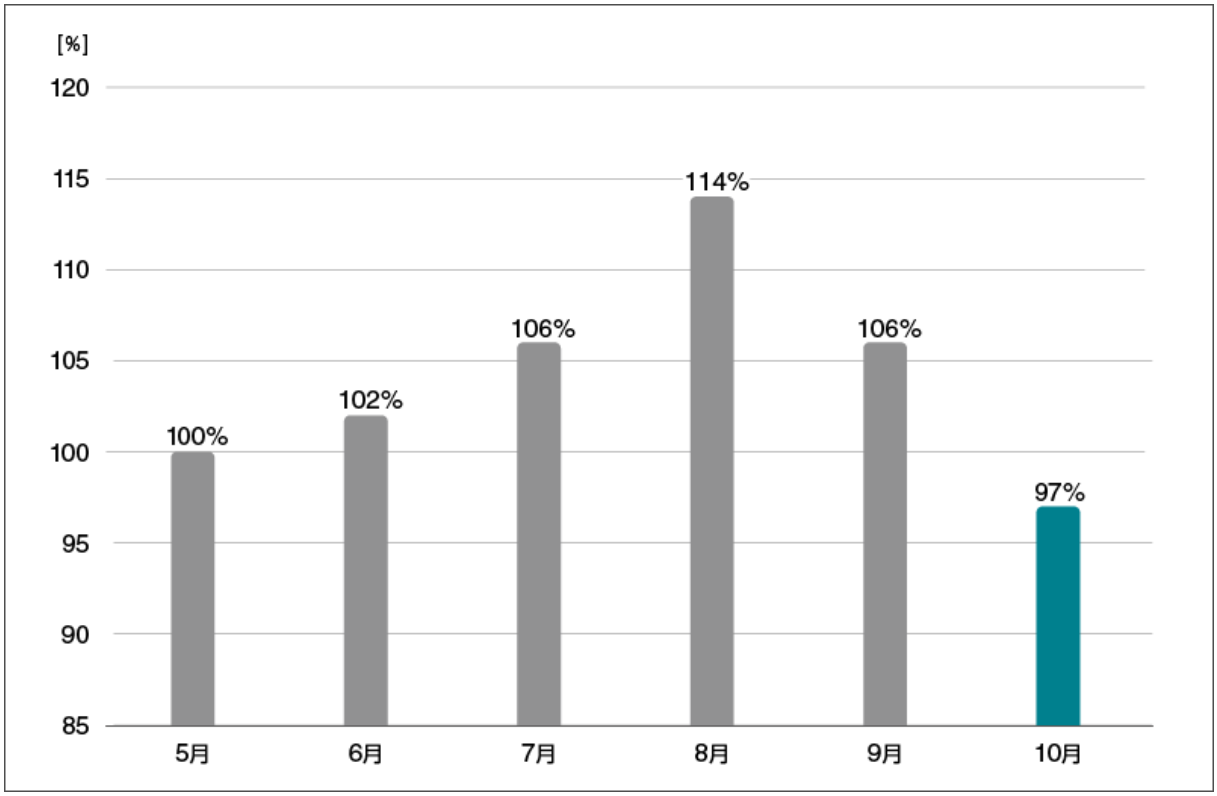
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「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。

2021 年 10 月マルウェア検出状況

2021 年 10 月（10 月 1 日～10 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

(2021 年 5 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。

2021 年 10 月の国内マルウェア検出数は、2021 年 9 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（2021 年 10 月）

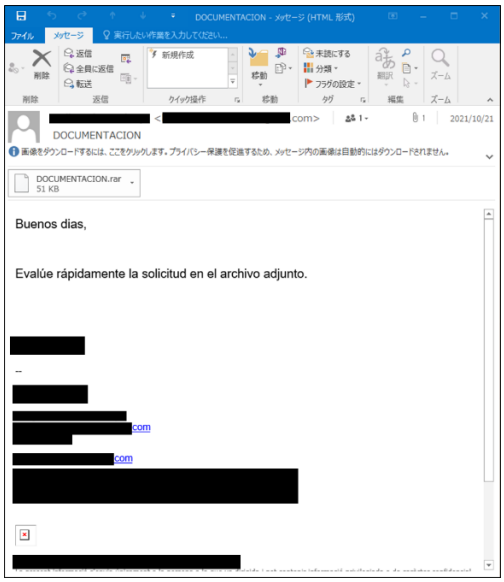
順位	マルウェア	割合	種別
1	JS/Adware.Agent	22.3%	アドウェア
2	HTML/Phishing.Agent	10.7%	メールに添付された不正な HTML ファイル
3	JS/Adware.Sculinst	9.2%	アドウェア
4	JS/Adware.TerraClicks	4.8%	アドウェア
5	JS/Adware.Subprop	3.3%	アドウェア
6	JS/Adware.Inpagepush	1.8%	アドウェア
7	HTML/FakeAlert	1.7%	偽の警告文を表示させる HTML ファイル
8	JS/Adware.PopAds	1.5%	アドウェア
9	HTML/ScrInject	1.1%	HTML に埋め込まれた不正スクリプト
10	Win32/Exploit.CVE-2017-11882	0.9%	脆弱性を悪用するマルウェア

*2 本表には PUA を含めていません。

10 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。

今月は検出数が減少傾向にありましたが、さまざまなマルウェアによる脅威を引き続き検出しています。
その中でも、今月は情報窃取型マルウェアの 1 つである「AgentTesla」についてご紹介します。
AgentTesla は、2014 年頃から活動しており、MaaS（Malware-as-a-Service）として配布されています。確認されてから 7 年経っていますが、依然として検出され続けています。
AgentTesla は、資格情報や Cookie 情報などの窃取機能や、キーロガー機能を持っています。ほかにも、画面のスクリーンショットやクリップボードの内容を取得する機能を持っています。
電子メールの添付ファイルが、主な感染経路として確認されています。また、添付ファイルには、さまざまな形式のファイルが使われています。さまざまな形式のファイルを利用する理由として、より効果的にユーザーを騙すために変化し続けてきたことやセキュリティ製品を回避することが考えられます。
実際に感染した例では、ダウンローダーは 2 つの段階に分かれて動作していました[*3]。
1 つ目が、悪意のあるコードのダウンロードサイトへ接続し、コードを実行する段階です。2 つ目が、AgentTesla をダウンロード・実行する段階です。また、この段階では、実行環境（サンドボックスや仮想環境かどうか）やデバッガーが実行されているかを確認します。

*3 WeliveSecurity「Agent Tesla: principales características de este malware」



AgentTesla のダウンローダーが添付されたメールの一例

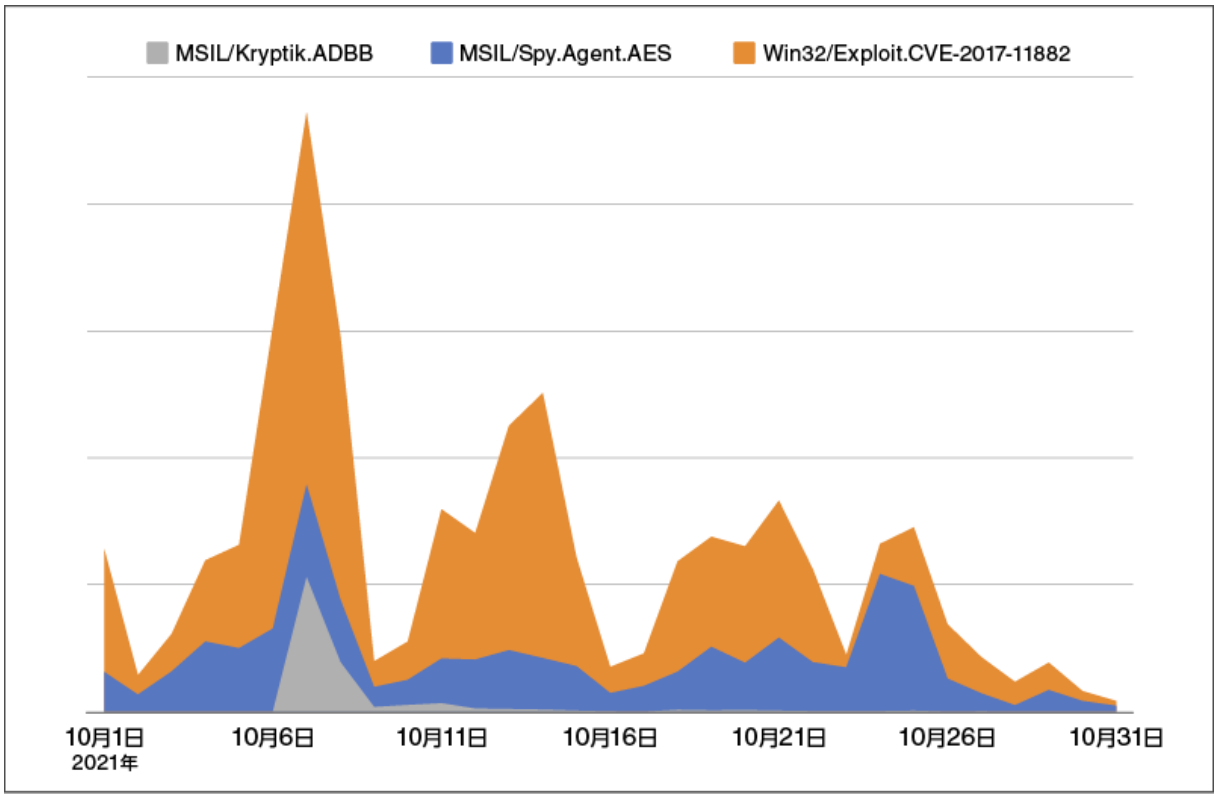
ESET 製品では、以下のようにファイル形式ごとに AgentTesla のダウンローダーの検出名が分かれています。

AgentTesla のダウンローダーの検出名とファイル形式の一例

ファイル形式	検出名*4
exe ファイル/rar ファイル	MSIL/Spy.Agent.AES MSIL/Kryptik の亜種 (例：MSIL/Kryptik.ADBB)
ppam ファイル	VBA/TrojanDownloader.Agent.WJE VBA/TrojanDownloader.Agent.WIK
RTF ファイル（拡張子が.doc となっている） (VBS ファイルが埋め込まれている)	VBS/TrojanDownloader.Agent.VYW RTF/Agent.A
xls ファイル	Win32/Exploit.CVE-2017-11882

*4 検出名は一例です。これら以外にも、ほかの亜種や汎用検出名などで検出されることがあります。また、同じ検出名でも、検体によってはダウンロードする検体が異なる場合があります。

AgentTesla のダウンローダーの検出状況（2021 年 10 月・国内）は、以下のとおりです。



AgentTesla のダウンローダー（2021 年 10 月・国内） *5

*5 この統計では、AgentTesla 以外のマルウェアをダウンロードするものも検出数としてカウントされています。Win32/Exploit.CVE-2017-11882 は、さまざまなマルウェアのダウンローダーとして使われています。2021 年 9 月には、マルウェアレポートでご紹介したとおり、「FormBook」などもダウンロードします。

10 月は添付ファイルとして rar ファイルや exe ファイルなどが多く利用されていることが分かります。また、検出名は異なりますが、同じ時期に検出されていることが分かります。この傾向の理由の 1 つとして、多くのユーザーへの感染を狙ってさまざまなファイル形式で同時期にばらまきメールを送信していることが考えられます。

ご紹介したように、AgentTesla にはさまざまなダウンローダーが存在しており、感染手法も多岐にわたります。
長年使用されている中で、攻撃主体や標的に合わせて変化していると考えられます。
手法以外にも、攻撃者は AgentTesla の機能更新を行っており、セキュリティ製品の回避や解析者を妨害するための難読化も使用しています。

このような情報窃取型マルウェアの被害に遭わないためにも、電子メールの添付ファイルを不容易に開かないことが必要です。ほかにもソフトウェアをダウンロードする場合は、信頼できる Web サイトから行ってください。
情報窃取型マルウェアは自身で感染に気付くことが難しいので、EDR 製品などのセキュリティ製品を導入して正しく運用することが重要です。

■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

■WeliveSecurity「Agent Tesla: principales características de este malware」
https://www.welivesecurity.com/la-es/2021/04/28/agent-tesla-principales-caracteristicas-este-malware/

Canon

キヤノンマーケティングジャパン株式会社