2019年
5月
MAY

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

新たに発見された脆弱性 BlueKeep が悪用される危険性を解説

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が運営する

「マルウェアラボ」が「ESETセキュリティ ソフトウェア シリーズ」の検出データを基に

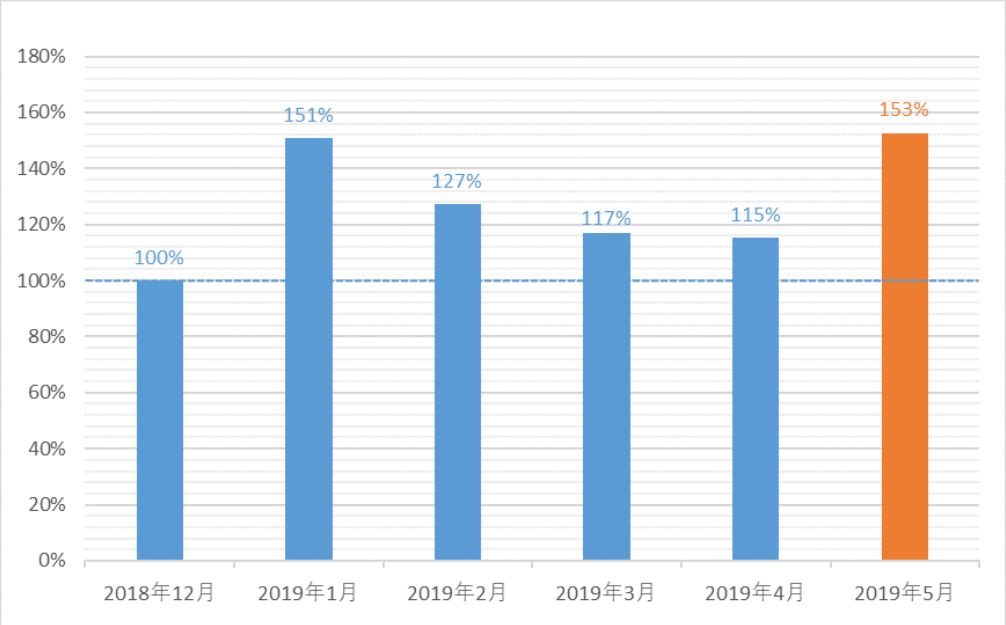
国内のマルウェア検出状況についてまとめたレポートです。

ショートレポート「2019 年 5 月マルウェア検出状況」

1. 5 月の概況について
2. WannaCryptor の大規模感染から 2 年、新たな脆弱性 BlueKeep が発見される

1. 5 月の概況について

2019 年 5 月（5 月 1 日～5 月 31 日）に ESET 製品が国内で検出したマルウェアの検出数は、以下のとおりです。



国内マルウェア検出数*1 の推移

（2018 年 12 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。

2019 年 5 月の国内マルウェア検出数は、2018 年 12 月と比較し約 1.5 倍になり、2019 年では一番多い月になりました。

検出されたマルウェアの内訳は以下のとおりです。

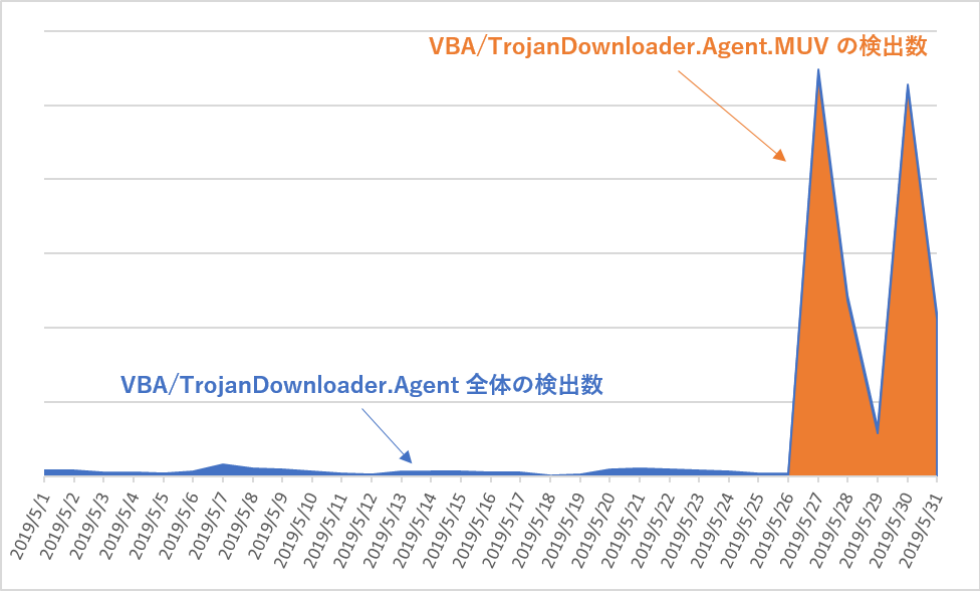
国内マルウェア検出数*2 上位（2019 年 5 月）

順位	マルウェア名	比率	種別
1	VBA/TrojanDownloader.Agent	18.0%	ダウンローダー
2	JS/Adware.Agent	9.4%	アドウェア
3	HTML/ScrInject	4.9%	HTML に埋め込まれた不正スクリプト
4	JS/Danger.ScriptAttachment	4.7%	ダウンローダー
5	PowerShell/TrojanDownloader.Agent	3.9%	ダウンローダー
6	JS/Adware.Subprop	2.6%	アドウェア
7	JS/Redirector	2.1%	リダイレクター
8	HTML/Refresh	1.3%	別のページに遷移させるスクリプト
9	DOC/Abnormal	1.1%	トロイの木馬
10	HTML/FakeAlert	0.9%	偽の警告文を表示するスクリプト

*2 本表には PUA を含めていません。

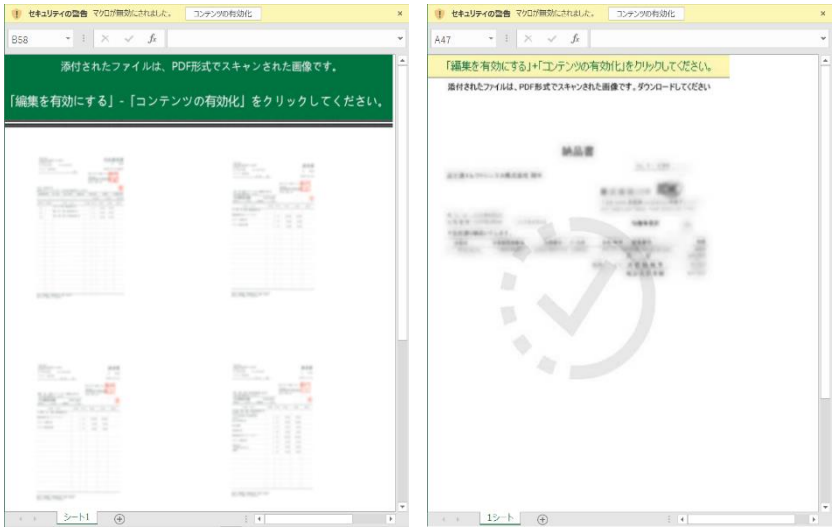
5 月に国内で最も多く検出されたマルウェアは、4 月と同様に VBA/TrojanDownloader.Agent でした。本マルウェアは、VBA（Visual Basic for Applications）で記述されたダウンローダーで、実行されるとバンキングマルウェアなどをダウンロードします。主にメールの添付ファイルとして拡散されています。

VBA/TrojanDownloader.Agent の検出数は、5 月 27 日、30 日にばらまかれたメールに添付された VBA/TrojanDownloader.Agent.MUV の検出が大部分を占めています。



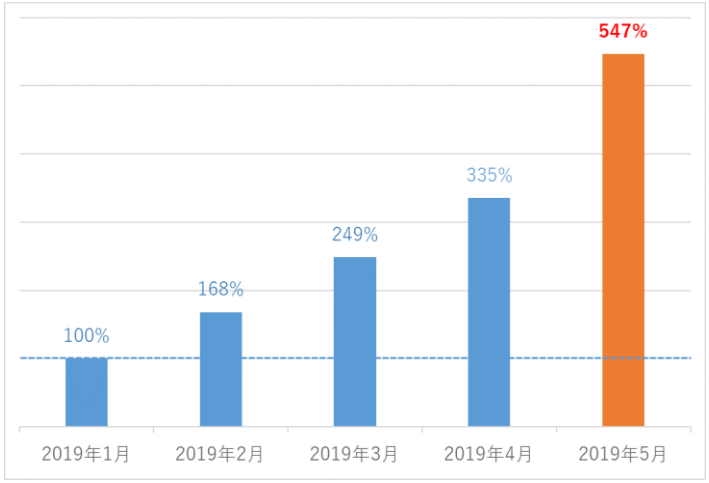
日本国内における VBA/TrojanDownloader.Agent 全体の検出数と VBA/TrojanDownloader.Agent.MUV の検出数

下記は VBA/TrojanDownloader.Agent.MUV で使用されたエクセルファイルの一例です。下記のようにエクセル内の画像はぼかしが掛ったような表示になっています。はっきりとした画像をみるために、「コンテンツの有効化」を押させることを狙っているのかもしれません。



5 月に確認された VBA/TrojanDownloader.Agent.MUV の一例

2019 年 4 月のマルウェアレポートでもご紹介したように、日本国内における VBA/TrojanDownloader.Agent の検出数は年初に比べ大幅に増加しています。



日本国内における VBA/TrojanDownloader.Agent の検出数
(2019 年 1 月の全検出数を 100%として比較)

2. WannaCryptor の大規模感染から 2 年、新たな脆弱性 BlueKeep が発見される

■ EternalBlue を悪用した攻撃を継続して観測

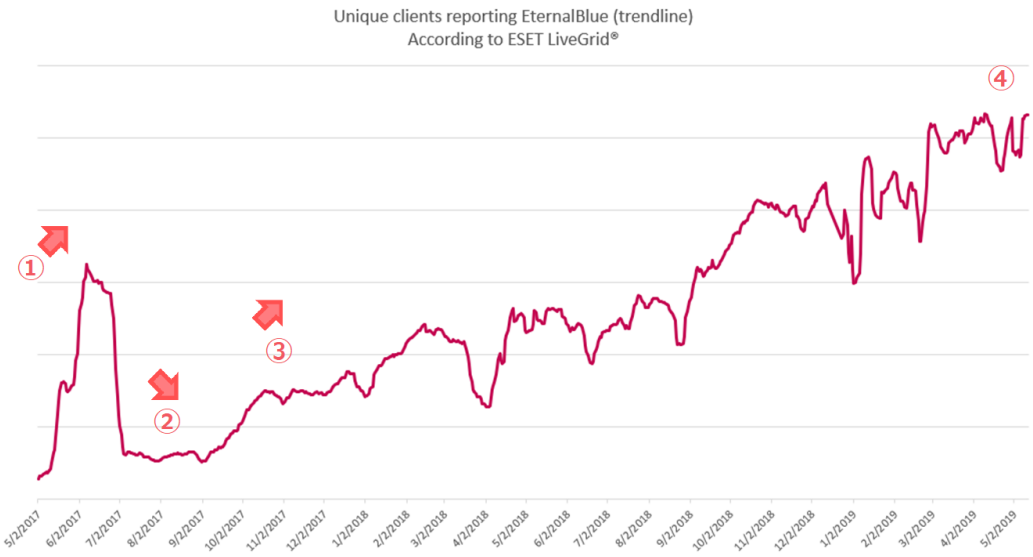
今年 5 月で、ランサムウェア WannaCryptor（別名：WannaCry）の大規模感染から 2 年を迎えます。WannaCryptor は、2017 年 5 月に確認されて以来、世界規模で感染を拡大し、日本を含む約 150 ヶ国で、23 万台以上のコンピューターに被害を与えたと言われています。

WannaCryptor（別名：WannaCry）の脅迫画面

ランサムウェア WannaCryptor では、EternalBlue と呼ばれるプログラムが悪用されました。このプログラムは、ファイル共有やプリンタ共有で使用される通信プロトコル Server Message Block 1.0 (SMB v1.0)の内部処理に起因する脆弱性を利用したプログラムで、悪用するとリモートから任意のコードを実行することができます。

そのため、WannaCryptor では、他のコンピューターに感染を広げる目的で EternalBlue が悪用されました。

WannaCryptor の脅威は収束していますが、WannaCryptor で使われた EternalBlue を悪用した攻撃は、現在でも継続して観測されています。
以下のグラフは、EternalBlue を悪用した攻撃を検出したクライアントの数です。

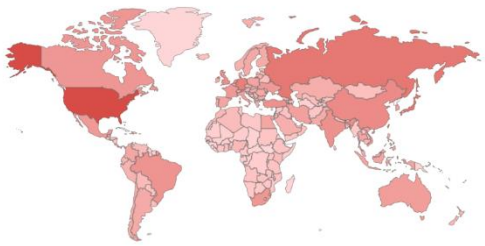


EternalBlue の攻撃を検出したクライアントの数
（出典：WeLiveSecurity「EternalBlue reaching new heights since WannaCryptor outbreak」）

2017 年 5 月から 6 月、WannaCryptor の大規模感染により、多くのコンピューターで、EternalBlue を悪用した攻撃を検出しました（グラフ①の箇所）。 その後、WannaCryptor の脅威が収束すると共に、EternalBlue を悪用した攻撃も減少します（グラフ②の箇所）。しかし、2017 年 9 月頃から増加に転じ（グラフ③の箇所）、現在では、WannaCryptor の大規模感染時（グラフ①の箇所）を上回る数のクライアントで、攻撃を観測しています（グラフ④の箇所）。

上記のように EternalBlue を悪用した攻撃が増加している要因は、複数考えられます。
たとえば、要因の 1 つとして、古いバージョンのファイル共有プロトコルである SMB 1.0 を使用しているコンピューターが、いまだにインターネット上に多く公開されており、これらのコンピューターに EternalBlue の更新プログラム（MS17-010）が適用されていないことが考えられます。

以下の図は、インターネットに接続されている機器情報を検索するサービス「Shodan」で検索した SMB 1.0 のポートをインターネット上に公開しているコンピューターの数です。



Top Countries

1. United States	411,329
2. Japan	73,852
3. Russian Federation	68,175
4. Germany	48,524
5. Taiwan	45,644
6. China	27,712
7. United Kingdom	22,147
8. Hong Kong	21,203
9. Netherlands	21,160
10. Turkey	17,986

Shodan の検索結果

（出典：Shodan）

ご覧の通り、SMB 1.0 のポートをインターネット上に公開しているコンピューターは、約 100 万台以上存在します。これらのコンピューターは、ほとんどがアメリカに存在しています。しかし、日本でも約 7 万台以上のコンピューターが存在しており、「EternalBlue」の更新プログラム（MS17-010）が適用されていないコンピューターも多く含まれていると推測します。

また、他の要因としては、WannaCryptor の大規模感染以降、他のマルウェアでも EternalBlue が悪用されるようになったことやペネトレーションテストの目的で EternalBlue が使用されていることが考えられます。

たとえば、EternalBlue は、WannaCryptor の大規模感染以降、2017 年 7 月に流行した DiskCoder.C（別名:Petya）や 2018 年 4 月に流行した Satan といったランサムウェアをはじめ、仮想通貨を採掘するマイニングマルウェアや一部の標的型攻撃（Sednit など）でも悪用されており、これらのマルウェアの感染拡大を助ける役割を果たしています。
また、現在では Metasploit などのペネトレーションツールを使って、EternalBlue を悪用した攻撃を簡単にテストすることができます。そのため、ペネトレーションテストなどセキュリティ目的での検出も一部含まれていると考えられます。

以上のように、WannaCryptor 自身の脅威は収まりましたが、EternalBlue を悪用した攻撃は、現在でも依然として多く観測されています。

■ 新たに発見された脆弱性 BlueKeep

EternalBlue を悪用した攻撃が継続して観測される中、今年 5 月マイクロソフトは、Windows XP などサポートを終了した製品を含むオペレーティングシステム（OS）に対して、異例の更新プログラムを提供しました。

この更新プログラムで修正される脆弱性（CVE-2019-0708）は、リモートデスクトップサービスに関連する脆弱性で、別名 BlueKeep と呼ばれています。 この BlueKeep の脆弱性を悪用すると、攻撃対象のシステムに対して特別に細工した要求を送信することで、リモートから任意のプログラムを実行できる可能性があります。そのため、EternalBlue と同様に、マルウェアを他のコンピューターに感染させる目的で悪用される恐れがあります。

現在のところ（2019 年 5 月 25 日時点）、この脆弱性を悪用したサイバー攻撃は確認されていません。しかし、ランサムウェア WannaCryptor の時と同様に、脆弱性が明らかになってから数か月後に、この脆弱性を悪用したマルウェアが拡散され、世界的な大規模感染につながる可能性があります。
そのため、BlueKeep の脆弱性を含むオペレーティングシステムを利用している場合、更新プログラムを適用するか、リモートデスクトップサービスを無効にするなどのリスク軽減策を行うことを推奨します。

◆ **マイクロソフト CVE-2019-0708 セキュリティ更新プログラム ガイド**
リモート デスクトップ サービスのリモートでコードが実行される脆弱性

◆ **マイクロソフト CVE-2019-0708 ユーザー向けガイダンス**
リモート デスクトップ サービスのリモートでコードが実行される脆弱性: 2019 年 5 月 15 日

■ 改めてセキュリティ対策の確認を

これまでご説明した通り、EternalBlue を悪用した攻撃は、未だに多数確認されています。また、今年 5 月にリモートデスクトップサービス（RDP）の重大な脆弱性 BlueKeep が新に発見され、WannaCryptor の時と同様に、発見された脆弱性がサイバー攻撃に悪用される恐れが高まっています。この機会に過去の教訓に学び、管理されていない端末がないか、セキュリティ対策が適切か、改めて確認してみてはいかがでしょうか。

ご紹介したように、5 月は VBA を悪用したダウンローダー型マルウェアが多く検出されました。Microsoft Office 形式のファイルを開く際には、十分ご注意下さい。また、BlueKeep と呼ばれる重大な脆弱性が発見されました。常に最新の脅威情報をキャッチアップし、対策を実施していくことが重要です。

■ 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. ESET 製品プログラムの検出エンジン（ウイルス定義データベース）を最新にアップデートする
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おります。
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）を最新にアップデートしてください。

2. OS のアップデートを行い、セキュリティパッチを適用する
ウイルスの多くは、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い、脆弱性を解消してください。

3. ソフトウェアのアップデートを行い、セキュリティパッチを適用する
ウイルスの多くが狙う「脆弱性」は、Java、Adobe Flash Player、Adobe Reader などのアプリケーションにも含まれています。
各種アプリのアップデートを行い、脆弱性を解消してください。

4. データのバックアップを行っておく
万が一ウイルスに感染した場合、コンピューターの初期化（リカバリー）などが必要になることがあります。 念のため、データのバックアップを行っておいてください。

5. 脅威が存在することを知る
「知らない人」よりも「知っている人」の方がウイルスに感染するリスクは低いと考えられます。ウイルスという脅威に触れてしまう前に「疑う」ことができるからです。
弊社を始め、各企業・団体からセキュリティに関する情報が発信されています。このような情報に目を向け、「あらかじめ脅威を知っておく」ことも重要です。

Canon

キヤノンマーケティングジャパン株式会社