2018年
6月
JUNE

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

Windows プロトコル「SMB」の脆弱性を悪用する攻撃が増加傾向

キヤノン IT ソリューションズ株式会社

はじめに

「マルウェアレポート」は、キヤノンITソリューションズが運営する

「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

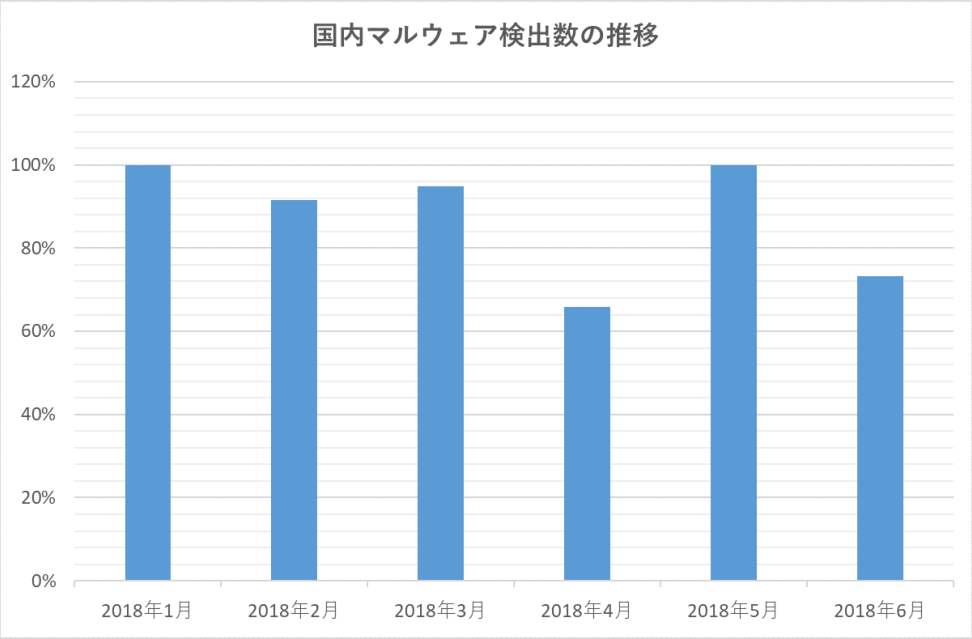
国内のマルウェア検出状況についてまとめたレポートです。

ショートレポート「2018 年 6 月マルウェア検出状況」

1. 6 月の概況について
2. Windows プロトコル「SMB」の脆弱性を悪用する攻撃を多数確認
3. ワールドカップに関連した詐欺メール

1. 6 月の概況について

2018 年 6 月 1 日から 6 月 30 日までの間、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の推移(※1)**（2018 年 6 月）**

（※1） 2018 年 5 月の検出数を 100%として比較

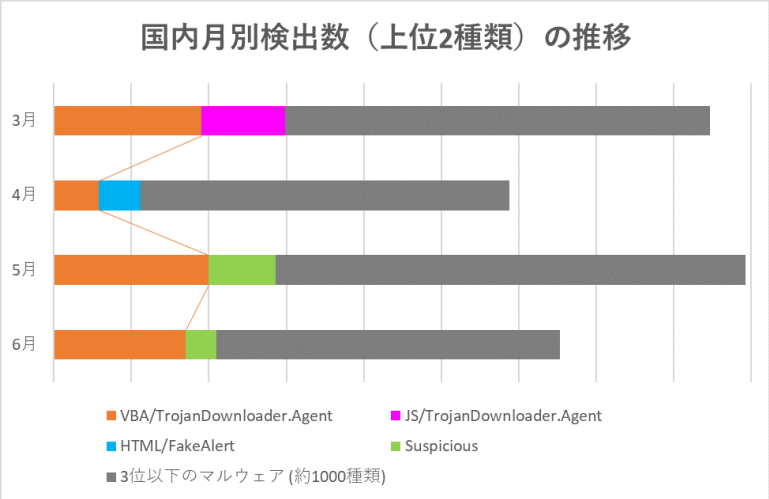
6 月の国内マルウェア検出数は、5 月と比較して 73%でした。ファミリー別の割合は以下のとおりです。

国内マルウェア検出数上位（2018 年 6 月）

順位	マルウェア名	比率	種別
1	VBA/TrojanDownloader.Agent	26.0%	ダウンローダー
2	Suspicious	6.0%	未知の不審ファイル呼称
3	JS/Adware.Agent	5.9%	アドウェア
4	JS/Redirector	5.5%	リダイレクター
5	JS/Mindspark	4.5%	アドウェア
6	JS/CoinMiner	4.4%	マイニングスクリプト
7	Win32/RealNetworks	3.0%	PUA（※2）
8	Win32/RiskWare.PEMalform	1.7%	PUA（※2）
9	Win32/FusionCore	1.4%	PUA（※2）
10	Win32/KingSoft	1.3%	PUA（※2）

（※2）Potentially Unwanted Application（望ましくない可能性のあるアプリケーション）：コンピューターの動作に悪影響を及ぼすことや、ユーザーが意図しない振る舞いなどをする可能性があるアプリケーション

6 月に最も検出されたマルウェアは「VBA/TrojanDownloader.Agent」でした。このマルウェアの月別検出割合は 2018 年 3 月以降、約 1,000 種類のマルウェア中、最大の割合を占めています。



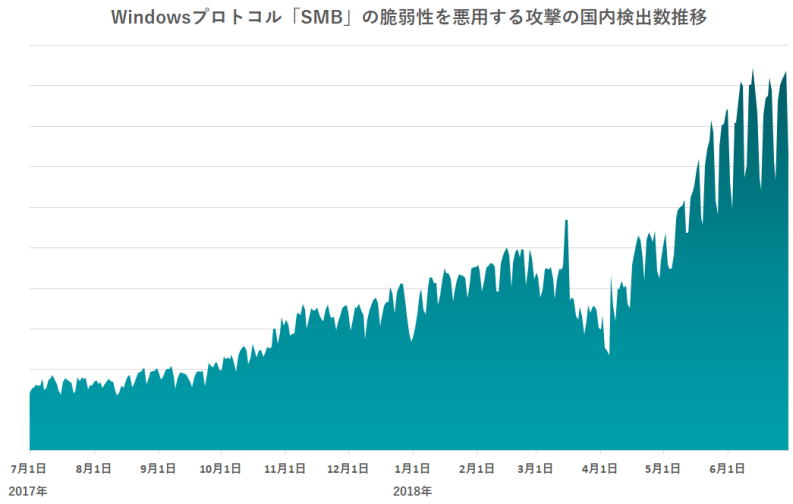
国内月別検出数（上位 2 種類）の推移

「VBA/TrojanDownloader.Agent」は VBA（Visual Basic for Applications）で書かれたダウンローダーで、ファイル形式はマクロを含む Microsoft Word 文書や Microsoft Excel 文書です。主にメールの添付ファイルとして拡散されています。

2. Windows プロトコル「SMB」の脆弱性を悪用する攻撃を多数確認

Windows の SMB（Server Message Block、ファイル共有などに使われる通信プロトコル）に関する脆弱性（MS17-010 にて修正。以下、本脆弱性）を悪用する攻撃を 6 月多数確認しています。

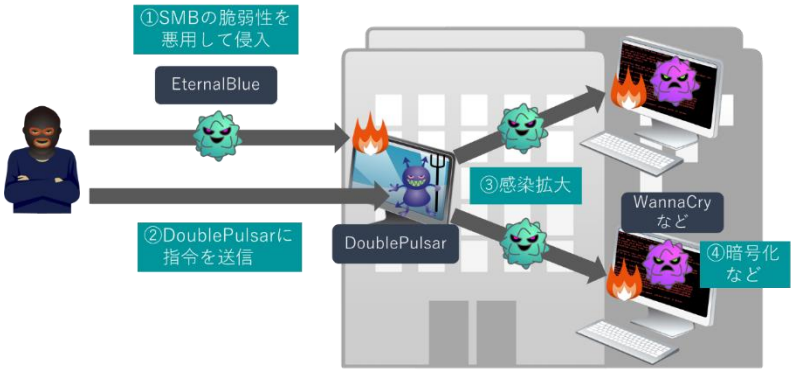
本脆弱性に対処するセキュリティ更新プログラム MS17-010 は昨年 3 月の時点で公開されていますが、本脆弱性を悪用する攻撃の検出数は増加傾向にあります。



Windows プロトコル「SMB」の脆弱性を悪用する攻撃の国内検出数推移（※3）

（※3）攻撃活動のほかに、脆弱性を検査する目的や研究目的で使用されたものも含まれています

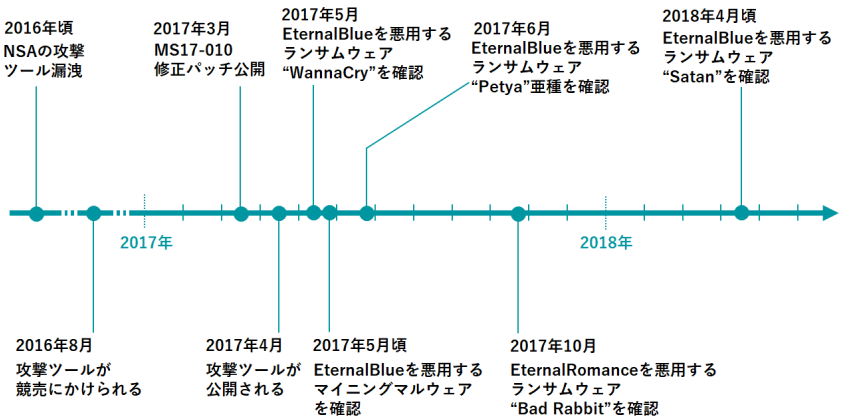
本脆弱性を悪用するツール（もしくは機能）として、EternalBlue（ESET 検出名：SMB/Exploit.EternalBlue）と DoublePulsar（ESET 検出名：SMB/Exploit.DoublePulsar）がよく知られています。
EternalBlue と DoublePulsar を悪用したマルウェア WannaCry（ESET 検出名：Win32/Filecoder.WannaCryptor）による攻撃の流れを説明します。



EternalBlue および DoublePulsar を用いた攻撃の流れ

1.はじめに、EternalBlue が本脆弱性を悪用して PC に侵入します。
2.PC に侵入すると、DoublePulsar と呼ばれるバックドアを設置します。
3.この DoublePulsar が、同じネットワーク上に感染を拡大させます。
4.最後に、WannaCry が PC 上のファイルを暗号化し、身代金として金銭を要求します。

EternalBlue および DoublePulsar は WannaCry の他にも様々なマルウェアの感染に使われています。



Windows プロトコル「SMB」の脆弱性に関する出来事

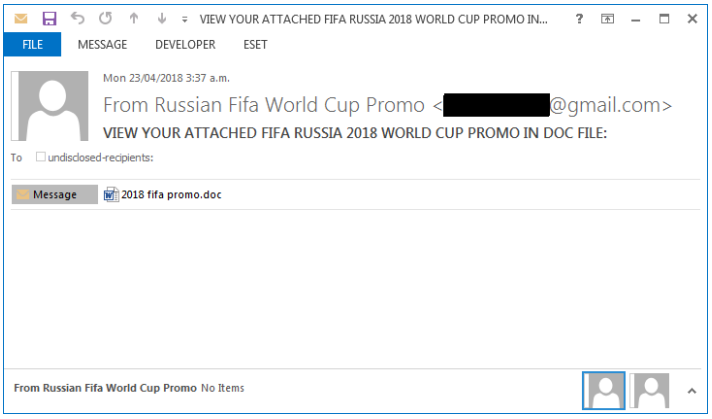
2016 年頃に NSA（アメリカ国家安全保障局）が開発したとされる脆弱性攻撃ツール群（EternalBlue および DoublePulsar が含まれる）が、Shadow Brokers というハッカー集団によって盗まれました。
2017 年 4 月には攻撃ツールに関する情報が広く一般に公開され、5 月には WannaCry と呼ばれるランサムウェアが大流行します。ほどなくして WannaCry の脅威は収まりましたが、本脆弱性を悪用する攻撃は今なお続いています。

今一度、お使いの攻撃の影響を受けるすべての Windows に修正プログラム（MS17-010）が適用されているか確認されることを推奨します。

ESET 製品では、ネットワーク攻撃保護機能で本脆弱性を悪用する攻撃を検知・ブロックします。

3. ワールドカップに関連した詐欺メール

オリンピックやワールドカップなど、世界的な注目を集めるイベントはサイバー攻撃者にとって絶好の攻撃機会となります。先日行われた平昌オリンピックでは、その開会式を狙ってマルウェアが仕掛けられていた可能性があることが大きな話題となりました（このマルウェアは ESET 製品では Win32/OlympicDestroyer.A として検出します）。現在開催されているワールドカップにおいても、それと関連した詐欺メールを確認しています。

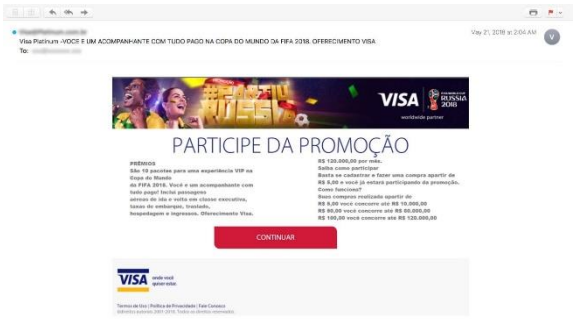


ワールドカップに関連した当選詐欺メール

詐欺メールに添付された Microsoft Word 文書

このような詐欺メールの常套手段として、「直ちに返信しなければ賞金を得る権利は失われます」と受信者を急き立てることが知られています。受信者に考える猶予を与えず、返信させるためです。
今回確認した Word 文書ファイルには、不正な動作を行うコードは含まれていませんでしたが、同様の手口で悪性 Word 文書ファイルが配布される可能性は十分に考えられます。

また、ワールドカップへの無料招待を装った手口も確認しています。この手口はブラジルのサッカーファンを標的としていて、本文はポルトガル語で書かれています。



ブラジルのサッカーファンをターゲットにした詐欺メール（ポルトガル語）

攻撃者の主たる狙いは、このような詐欺に対して返信する（＝詐欺に遭いやすい）ユーザーの個人情報を得ることと考えられます。その情報をもとに、次の攻撃を仕掛けてくる可能性は高いでしょう。このようなメールには、決して興味本位で返信しない（メール本文中の URL にアクセスしない）ようご注意下さい。

ご紹介したように、今月は Windows の脆弱性を狙った攻撃や、ワールドカップに関連した攻撃が確認されました。常に最新の脅威情報をキャッチアップ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. ESET 製品プログラムの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、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 ITソリューションズ株式会社

eset-info.canon-its.jp/