2018年
8月
AUGUST

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

バンキングマルウェア感染を狙う IQY ファイル悪用のばらまき型攻撃を観測

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

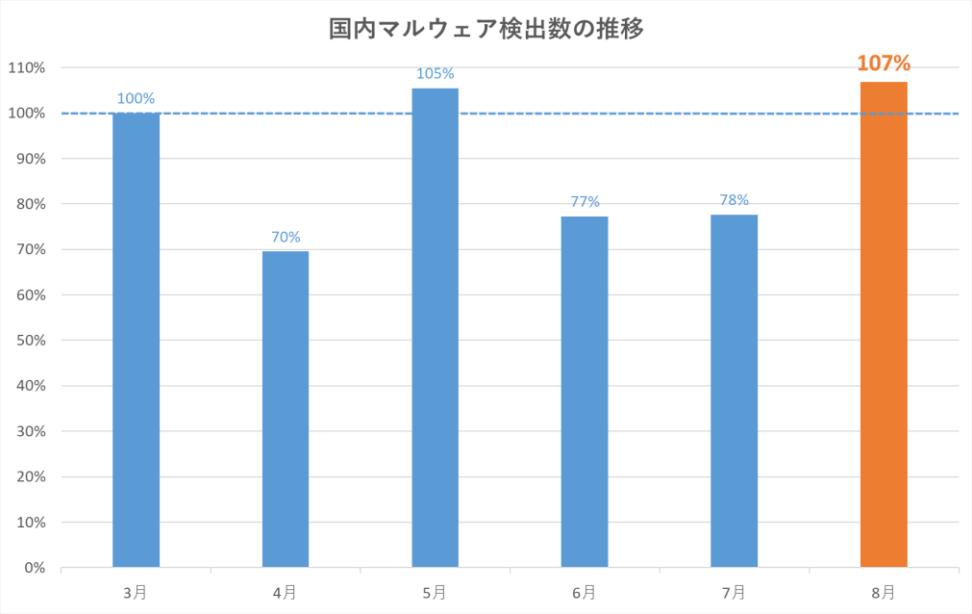
国内のマルウェア検出状況についてまとめたレポートです。

ショートレポート「2018 年 8 月マルウェア検出状況」

1. 8 月の概況について
2. バンキングマルウェア感染を狙う IQY ファイルを用いたばらまき型メール攻撃
3. Outlook ユーザーを狙うバックドア

1. 8 月の概況について

2018 年 8 月（8 月 1 日～8 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の推移(※1)

（※1） 2018 年 3 月の全検出数を 100%として比較

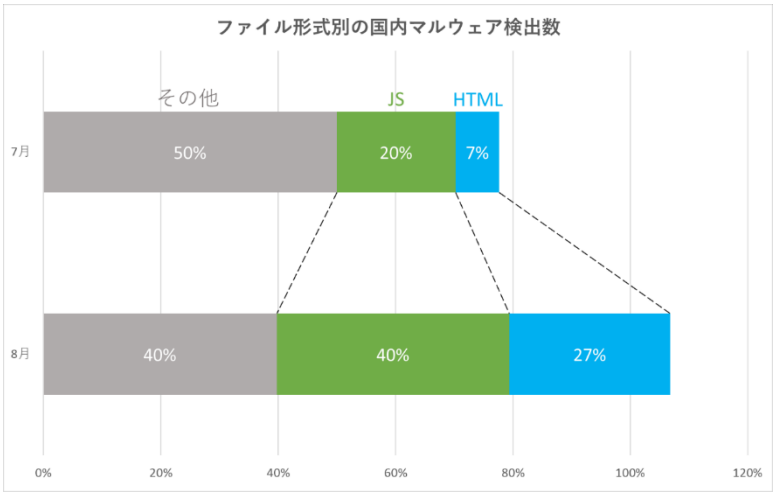
8 月の国内マルウェア検出は、過去半年の中でも最多となりました。そのマルウェアの内訳は、以下のとおりです。

国内マルウェア検出数上位（2018 年 8 月）

順位	マルウェア名	比率	種別
1	JS/Adware.Agent	25.9%	アドウェア
2	HTML/FakeAlert	6.0%	偽の警告文を表示するスクリプト
3	HTML/ScrInject	5.9%	埋め込まれた不正なスクリプト
4	VBA/TrojanDownloader.Agent	5.0%	ダウンローダー
5	JS/Redirector	4.3%	リダイレクター
6	JS/Mindspark	3.0%	アドウェア
7	Win32/IObit	2.7%	PUA（※2）
8	JS/CoinMiner	2.2%	マイニングスクリプト
9	DOC/TrojanDownloader.Agent	1.8%	ダウンローダー
10	PDF/Phishing	1.5%	フィッシング目的の PDF ファイル

（※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

8 月に検出されたマルウェアでは、ファイル形式が JS（JavaScript）と HTML のものが上位を占めました。これらの検出数を 7 月と比較した結果は、以下のとおりです。



ファイル形式別の国内マルウェア検出数(※3)

（※3） 2018 年 3 月の全検出数を 100%として比較

上図からわかるように、ファイル形式が JS または HTML 以外のマルウェアは減少している一方で、ファイル形式が JS または HTML のマルウェアは共に大きく増加し、全体の検出数を押し上げています。
これらのマルウェアは、Web 上で動作するものが大半です。そのため、Windows だけではなく、他の OS を搭載した PC やスマートフォンなど、Web ブラウザーを搭載しているあらゆるプラットフォームが攻撃の対象となります。

Web 上で動作するマルウェアが流行している要因として、以下の背景があると考えられます。

- 攻撃者の関心が詐欺広告による収益に向けられている。
- PhaaS の出現（参考：2018 年上半期マルウェアレポート）などによって詐欺サイトの作成が容易になっている。
- プラットフォームに依存しないため攻撃範囲が広く収益性が高い。

ESET 製品では、Web 上で動作するマルウェアに対しても、検出・遮断し、実行を防ぎます。

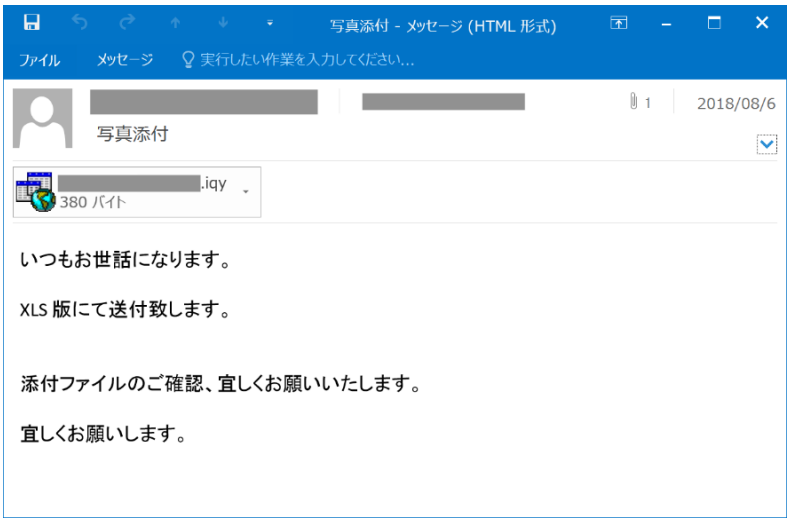
2. バンキングマルウェア感染を狙う IQY ファイルを用いたばらまき型メール攻撃

近年、バンキングマルウェアへの感染を狙うばらまき型メール攻撃が頻繁に発生しています。バンキングマルウェアに感染するとインターネットバンキングの認証情報（ユーザーID やパスワード等）やクレジットカード情報を窃取され、銀行口座からの不正送金やクレジットカードの不正利用などの被害に遭う可能性があります。

8 月は、バンキングマルウェア Ursnif に感染させようとする、新たなばらまき型メール攻撃が観測されました。この攻撃は、一般的にあまり使用されない「.iqy」という拡張子のファイルを用いていることが特徴です。

.iqy ファイル（Web クエリファイル）は Excel の Web クエリ機能（※4）で用いられるアクセス先 URL を記載したファイルで、今回の攻撃ではメールの添付ファイルとして拡散されました。

※4 Web クエリ機能：Web 上のデータをダウンロードして表計算に利用する機能



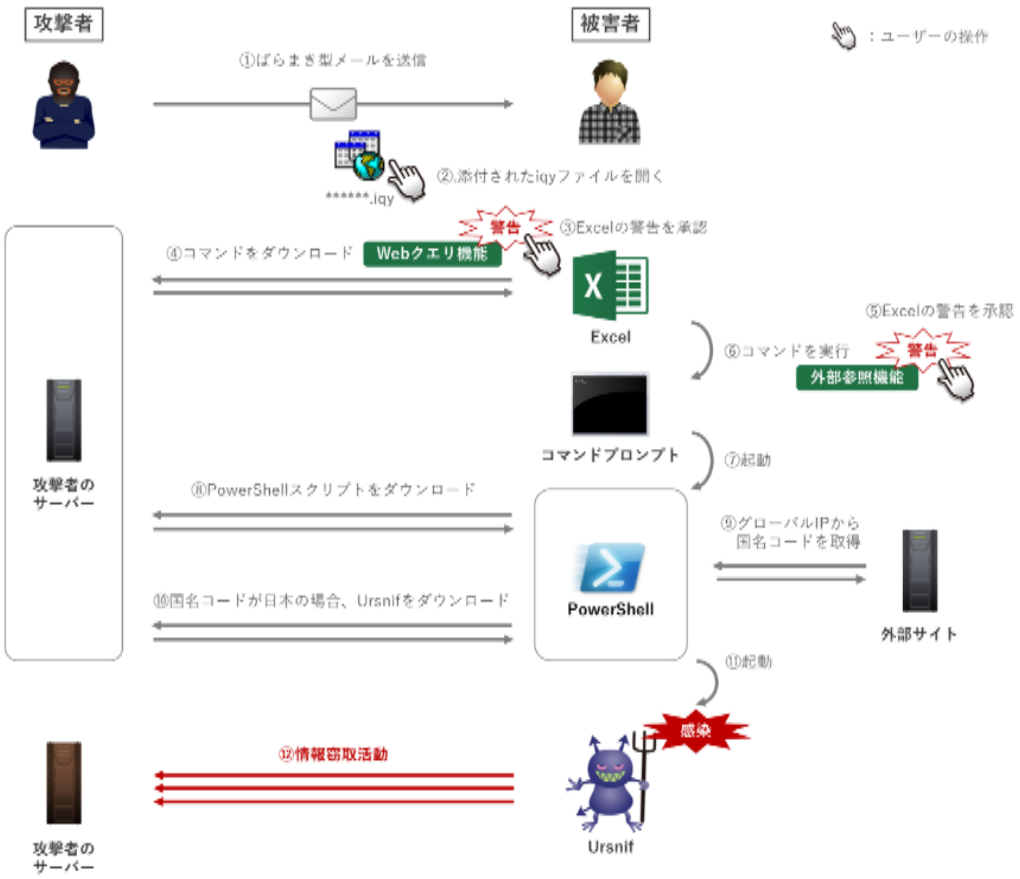
Web クエリファイルが添付されたメール

メールの件名は、「写真添付」「写真送付の件」「ご確認ください」「お世話になります」といったものが確認されています。

このばらまき型メール攻撃は 8 月 6 日に第一波、8 月 8 日に第二波が確認されています。いずれも数十～数百万通規模で拡散されたとみられ、各セキュリティベンダーなどから注意喚起が出されているほか、多くのニュース

メディアでも取り上げられました。国外では、Necurs ボットネットを利用して FlawedAmmyy と呼ばれる RAT（遠隔操作ツール）に感染させようとする同様の攻撃が 5 月に確認されています。

この攻撃の流れを以下の図に示します。

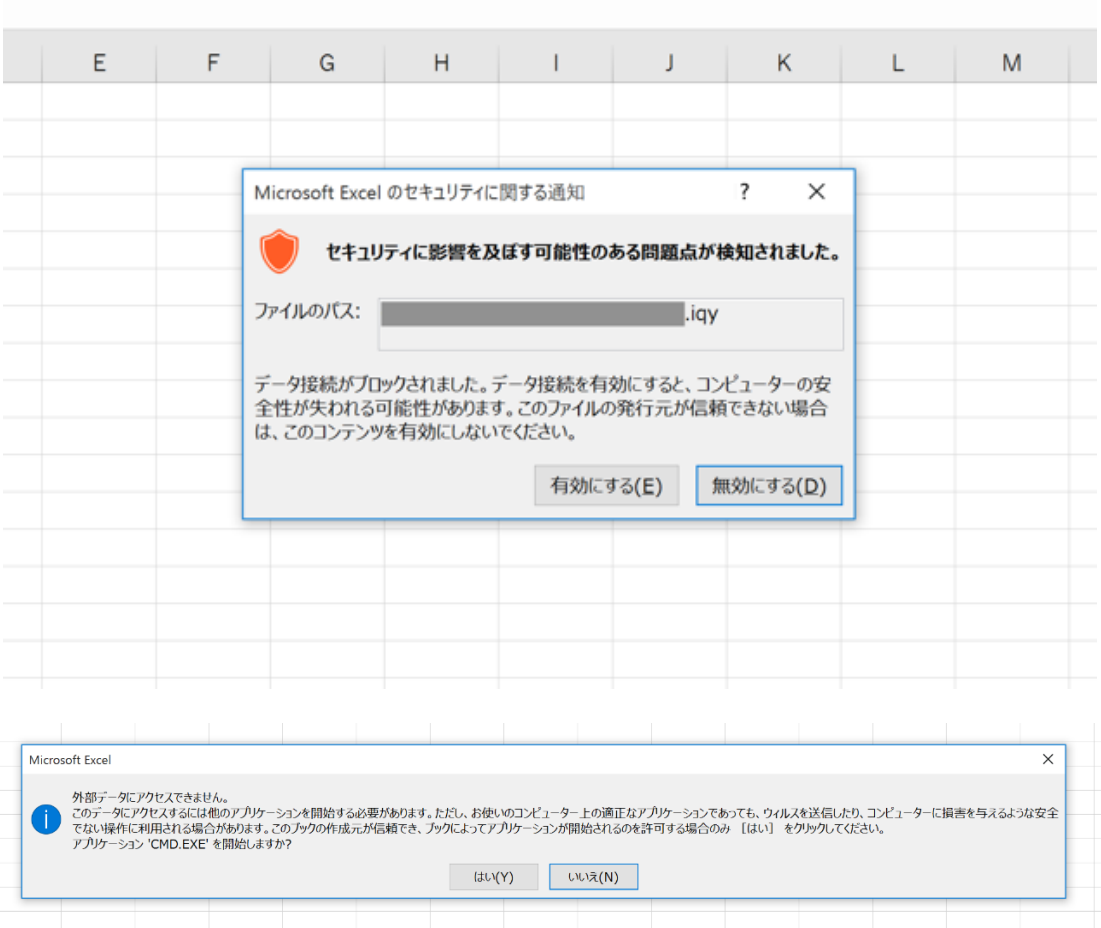


感染までの流れ

メールに添付された Web クエリファイルを開くと、まず Excel の Web クエリ機能を利用してコマンドをダウンロードします［図中④］。このコマンドは Excel の数式に組み込まれており、コマンドプロンプトを利用して PowerShell を起動するように細工されています。このコマンドが外部参照機能（※5）によって実行される［図中⑥］と、PowerShell スクリプトがダウンロード・実行され［図中⑧］、Ursnif がダウンロード・実行されます［図中⑪］。

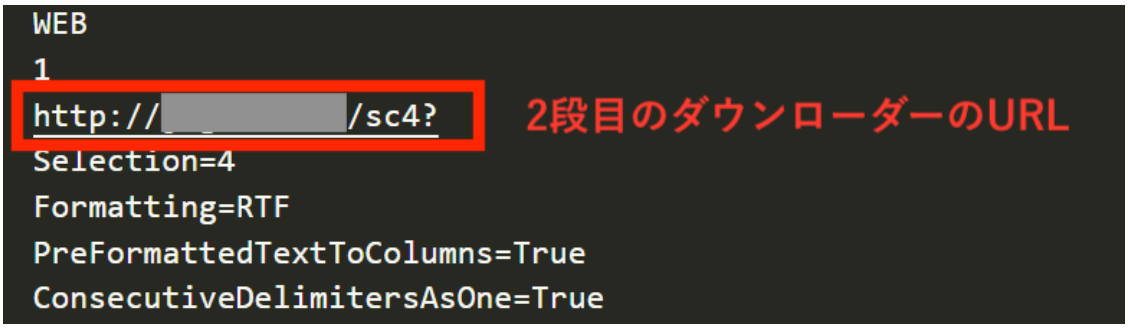
※5 外部参照機能：他の Excel ファイルや Excel 以外のプログラムのデータを利用する機能

今回の攻撃では、実際に Ursnif がダウンロード・実行されるまでに警告画面が 2 回表示され［図中③, ⑤］、この両方で「有効にする」あるいは「はい」をクリックして実行に同意しなければ Ursnif への感染は起こりません。



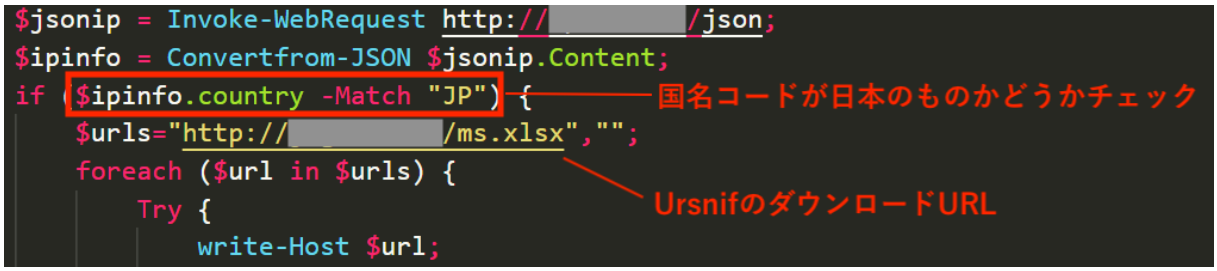
Excel によって表示される警告（上：「感染までの流れ」図中③、下：同図中⑤）

Web クエリファイルは URL や付加情報がプレーンテキストで記載されているのみの単純なファイルです。そのため、内部の URL を改変することで簡単に亜種を作成することができ、攻撃者にとっては比較的利用しやすい形式であると言えます。



Web クエリファイルの内容
（「感染までの流れ」図中②でダウンロードされたもの。抜粋）

また、この攻撃においては被害者 PC のグローバル IP アドレスから国名コードを取得することで被害者が日本にいるかどうかを判定しており［図中⑨、⑩］、日本を選択的に攻撃している様子が伺えます。



PowerShell スクリプトの内容
（「感染までの流れ」図中⑧でダウンロードされたもの。抜粋した上で整形）

ESET 製品では、この一連のマルウェアを以下のような名称で検出します。

- DOC/TrojanDownloader.Agent.UR（Web クエリファイル［図中②］）
- PowerShell/TrojanDownloader.Agent.XF（PowerShell スクリプト［図中⑧］）
- Win32/Spy.Ursnif.AO（Ursnif［図中⑩］）
- Win32/GenKryptik.CHHW（Ursnif［図中⑩］）

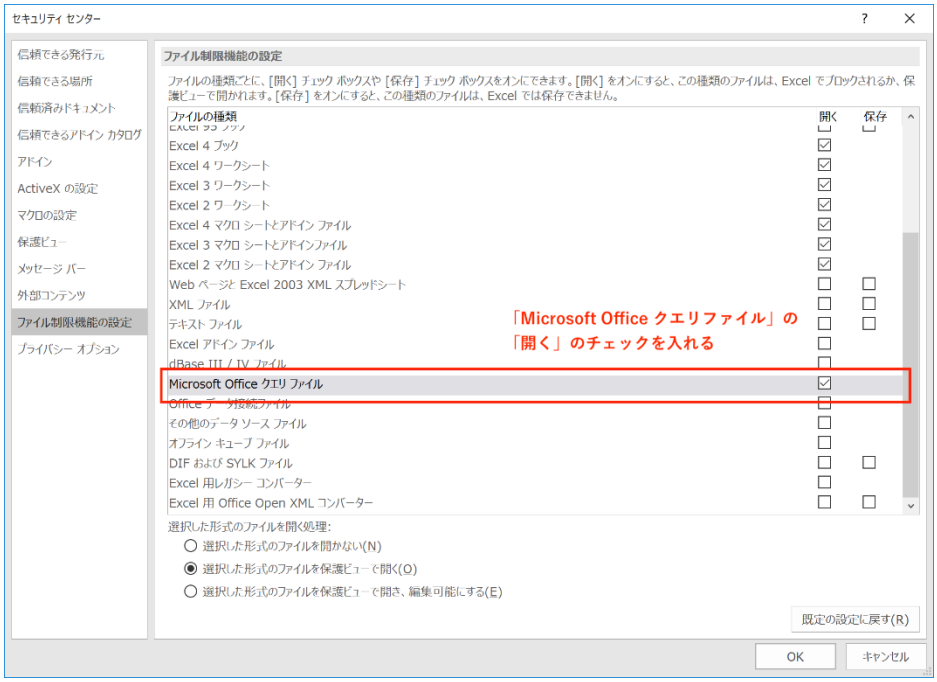
Web クエリファイルを日常的に使用していない場合は、以下のような対策によって感染を防ぐことが可能です。

＜ユーザー側での対策例＞

- Microsoft Excel の［オプション］-［セキュリティセンター］-［ファイル制限機能の設定］にて、「Microsoft Office クエリファイル」のチェックを外す。
- Web クエリファイル（.iqy）の関連付けをメモ帳などに変更して、Web クエリファイルをダブルクリックしても Excel が起動されないようにする。

＜システム管理者側での対策例＞

- メール経路上のセキュリティ製品などで、メールの添付ファイルに対して拡張子によるフィルタリングを行い、Web クエリファイル（.iqy）を受信しないよう設定する。



Microsoft Excel のセキュリティセンターの設定変更

Web クエリファイルを日常的に使用している場合は、実行しようとしている Web クエリファイルが正当なものかどうか十分に確認してから実行してください。

また、個別の攻撃手法に対する対策だけではなく、新たな攻撃にも対応できるよう以下のような心構えを持っておくことも重要です。

- メールで受信したファイルや Web からダウンロードしたファイルはマルウェアかどうか疑い、安易に開かない。
- OS や Office 製品の警告が表示されても安易に許可・同意しない。

バンキングマルウェア感染を狙う攻撃手法は日々変化しています。一つの対策のみに頼らず、複数の対策を講じていくことが重要です。

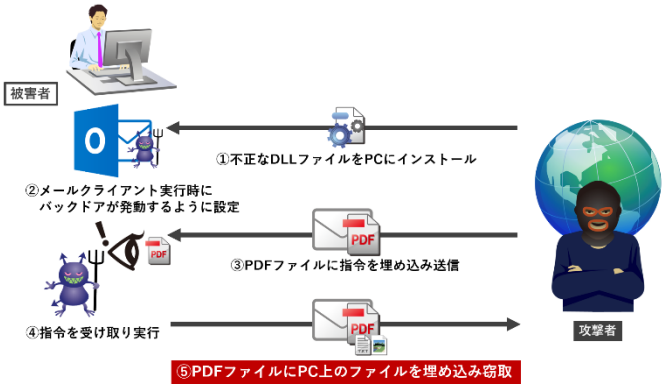
3. Outlook ユーザーを狙うバックドア

ESET は、Turla Outlook Backdoor と呼ばれるマルウェアを解析し、8 月にその詳細をホワイトペーパーで報告しました。
このマルウェアは、Outlook ユーザーを狙ったバックドアです。サイバースパイ集団の Turla によって作成されたと考えられており、2009 年に確認されて以降、継続的にアップデートされています。実際に被害も発生しており、ドイツ外務省がこのバックドアに感染し、機密情報が搾取された可能性が示唆されています。

近年の Turla Outlook Backdoor の大きな特徴は、従来とは異なる手法で感染端末を制御することです。

バックドアの感染端末に対する制御は、コマンド＆コントロールサーバー（以下 C&C サーバー）を介して行われるものが一般的です。一方、Turla Outlook Backdoor は、C&C サーバーを介さなくても、感染端末を制御することが可能です。感染端末は、攻撃者から送信されたメールに添付されている PDF ファイルによって制御されます。

Turla Outlook Backdoor の感染から、感染端末が制御されるまでの、流れを説明します。



Turla Outlook Backdoor 感染に伴う、一連の流れ

Turla Outlook Backdoor は、DLL 形式のファイルです。Turla Outlook Backdoor は、PC にインストールすると、Outlook が実行される都度、自身が起動するように、レジストリーを変更します［図中①、②］。

Turla Outlook Backdoor が起動すると、感染端末に届いたすべてのメールをチェックして、指令が埋め込まれた PDF ファイルを待ち受けます。 その後、攻撃者が細工された PDF ファイルを添付したメールを送信することで［図中③］、感染端末に対してユーザーの操作に関係なく、以下の制御を施すことが可能となります［図中④＆⑤］。

- ファイルのダウンロード
- PowerShell コマンドの実行
- メッセージボックスの表示
- ファイル、プロセスの生成・削除
- 取集したログ（メールのメタデータ、コマンドの結果など）を攻撃者に送信

```
RECIVE ->{
  From: sender@example.com
  To:   receiver@example.net
  Cc:
  Bcc:
  Subj: Mail subject
  Att:  an_attachment.pdf
}
```

収集されたメールのメタデータ

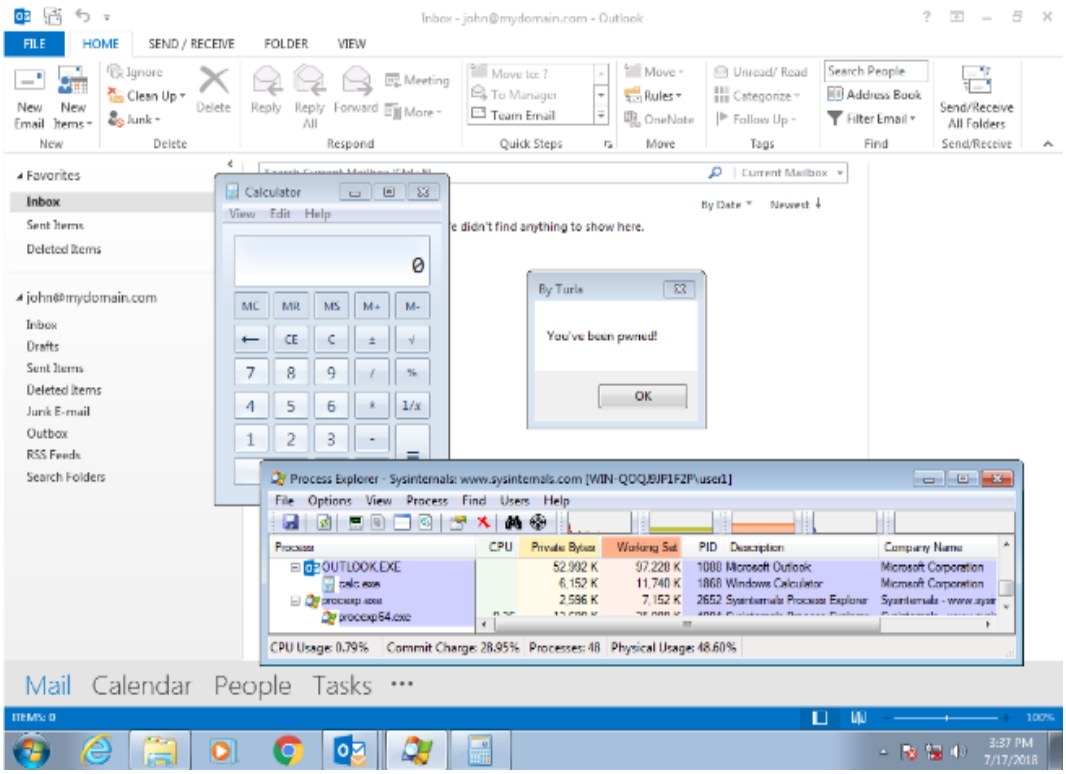
また、細工された PDF ファイルを受信した際には、以下の動作を行います。

- メール受信を知らせるポップアップ通知を非表示化
- メールの削除

そのため、感染端末のユーザーが、攻撃者から送られるメールに気づくことは困難です。

なお、一番新しいと考えられているバージョンには非常に強力な機能が備わっています。Empire PSInject と呼ばれる技術を用いることで、ユーザーが PowerShell の実行を無効に設定していても、PowerShell コマンドの実行が可能となっています。

今回取り上げたバックドアの実証コードはすでに公開されています。
実証実験として、「メッセージボックスの表示」と「電卓の実行」を命令する PDF ファイルを作成し、感染端末に対して添付ファイル付きメールを送信した際の結果を、以下のスクリーンショットに示します。



メールに添付された PDF ファイルによって制御される感染端末

メッセージボックスが表示され、電卓が起動していることがわかります。加えて、PDF ファイルが添付されたメールを受信したにもかかわらず、受信箱（Inbox）にメールが存在していないことを示す「didn't find anything to show here」というメッセージも確認できます。

このように、攻撃者は新しい手法を日々開発しています。
Turla Outlook Backdoor は、Outlook の最新バージョンにおいても動作します。ESET 製品では、このマルウェアを Win32/Turla として検出し、駆除します。

ESET Endpoint Security における検出画面

ご紹介したように、今月はバンキングマルウェア感染を狙う新たな攻撃が確認され、Outlook ユーザーを狙ったバックドアの解析報告がありました。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/