2018年
12月
DECEMBER

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

12 種類の新たな Linux の OpenSSH バックドアを ESET 社が発見

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

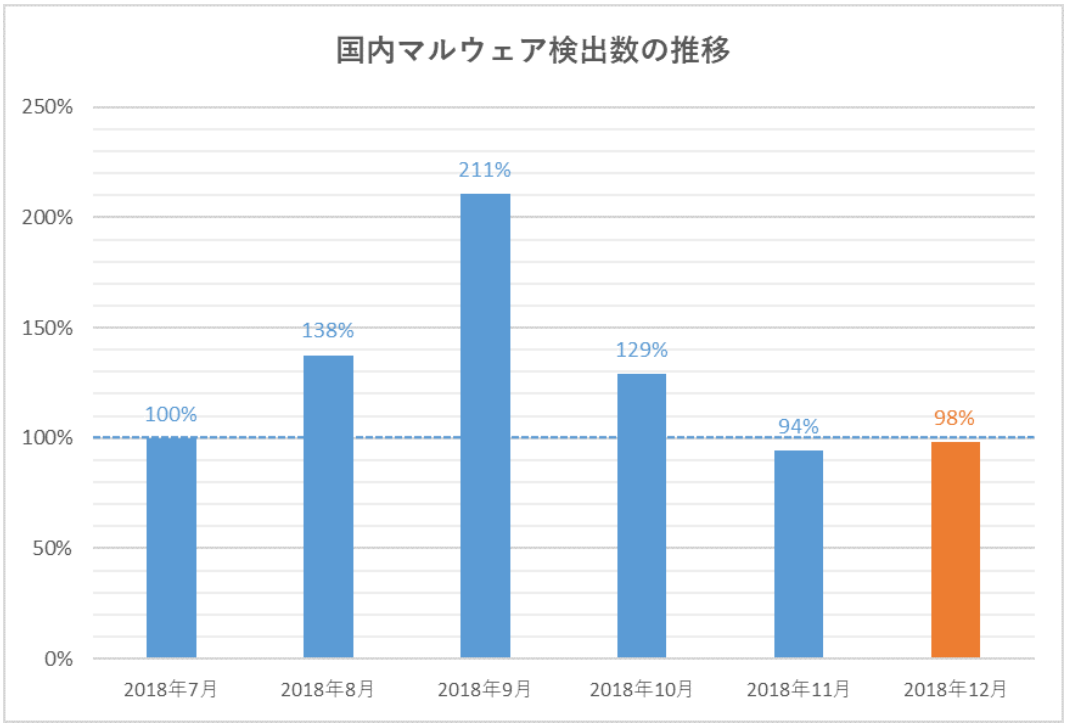
国内のマルウェア検出状況についてまとめたレポートです。

ショートレポート「2018 年 12 月マルウェア検出状況」

1. 12 月の概況について
2. 12 種類の新たな Linux の OpenSSH バックドアを発見

1. 12 月の概況について

2018 年 12 月（12 月 1 日～12 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 7 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。

12 月の国内マルウェア検出数は、11 月と同程度であり、検出数が増加した 8 月～10 月より落ち着きました。

検出されたマルウェアの内訳は以下の通りです。

国内マルウェア検出数*2 上位（2018 年 12 月）

順位	マルウェア名	比率	種別
1	JS/Adware.Agent	11.6%	アドウェア
2	HTML/ScrInject	10.2%	HTML に埋め込まれた不正スクリプト
3	VBA/TrojanDownloader.Agent	8.6%	ダウンローダー
4	JS/CoinMiner	5.5%	マイニングスクリプト
5	JS/Mindspark	4.6%	アドウェア
6	DOC/TrojanDownloader.Agent	4.6%	ダウンローダー
7	JS/Redirector	3.0%	リダイレクター
8	Win32/RiskWare.PEMalform	1.4%	ブラウザハイジャッカー
9	HTML/Refresh	1.2%	別のページに遷移させるスクリプト
10	HTML/FakeAlert	1.1%	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。

12 月に国内で最も多く検出されたマルウェアは、Web 閲覧中に不正広告を表示させる可能性があるスクリプトである JS/Adware.Agent でした。JS/Adware.Agent は、2018 年 6 月以降、常に国内マルウェア検出数の上位 3 位以内にランクインしています。加えて、12 月は世界全体においても、本マルウェアが最も多く検出されました。数多くの攻撃者が、不正広告を利用した収益に対して、継続的に関心を示していることが考えられます。

検出数が最も多かった JS/Adware.Agent も含め、今月も Web 上で動作するマルウェアが多く検出されました。12 月の国内マルウェア検出数上位 10 件のうち、8 件が Web 上で動作するものです。Web 上で動作するマルウェアは、OS の種類やプラットフォームに関係なく、あらゆる環境で動作することが可能なため、汎用性が高いです。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。

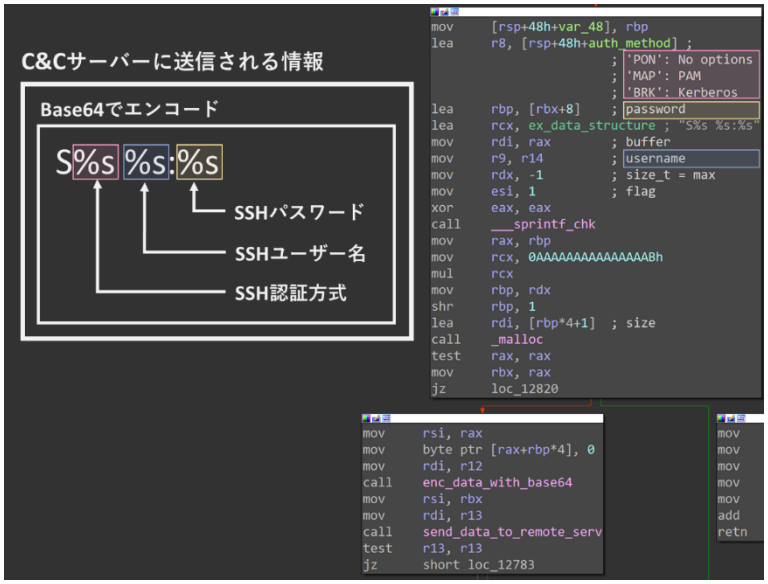
2. 12 種類の新たな Linux の OpenSSH バックドアを発見

2018 年 12 月 5 日、ESET 社は 21 種類の Linux バックドアについて解析結果を公表しました（ESET 社ブログ）。このうち 12 種類は、これまで詳細が知られていなかった新しいバックドアです。
バックドアは「裏口」を意味するマルウェアで、攻撃者がシステムに侵入した際、次回以降侵入しやすくする目的で設置されます。感染した場合、情報が窃取されるほか感染端末を不正行為の踏み台として使われるおそれがあります。

今回公表されたバックドアはすべて OpenSSH を基に作成されています。OpenSSH はオープンソースの SSH (Secure Shell) ソフトウェアで、ほとんど全ての Linux ディストリビューションに搭載されていることから、一般に広く使われています。
OpenSSH が攻撃者に好まれる理由として、無償でソースコードを入手できるため改変（バックドア化）がしやすいこと、隠密に攻撃活動を行えることなどが考えられます。
本稿では、中でも特徴的な 4 種類のバックドアをご紹介します。

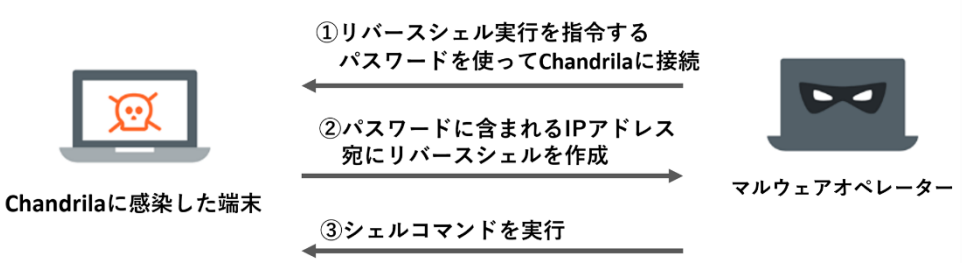
■ パスワードを介して指令を受け取る「Chandrila」

Chandrila は情報窃取を目的としたバックドアです。C&C サーバー（攻撃者の指令サーバー）に SSH の接続情報（認証方式、ユーザー名、パスワード）を送信します。



C&C サーバーに送信される SSH の接続情報

Chandrila は情報窃取機能のほかに、攻撃者のコマンドを実行するボット機能を持ちます。 ここで特徴的なのは、攻撃者が Chandrila に接続する際に入力したパスワードをコマンドとして使用する点です。パスワードには 2 つの形式があり、1 つ目はシェルコマンドを実行するパスワードです。パスワードに含まれるシェルコマンドが感染端末上で実行されます。2 つ目はリバースシェルを作成するパスワードです。リバースシェルは標的から攻撃者に向けて逆向きに（リバース）接続するコマンド実行環境（シェル）のことで、ファイアウォールを回避しやすいことから攻撃者に好まれています。



リバースシェルを使ったコマンド実行までの流れ

■ 暗号通貨を採掘する機能を持つ「Bonadan」

Bonadan は暗号通貨を採掘する機能を備えたバックドアです。Bonadan の暗号通貨採掘モジュールははじめに、他の仮想通貨採掘プログラムが実行されているかどうかをチェックし、実行されていた場合そのプロセスを終了します。

```
; char aKillallCircleM[]
aKillallCircleM db 'killall Circle_MI.png wnTKYg ddg.2011 JN7sb maldet EYgnU ddg.2020'
                                        ; DATA XREF: remove_other_miners+1C↑o
                                        ; remove_other_miners+28↑o
```

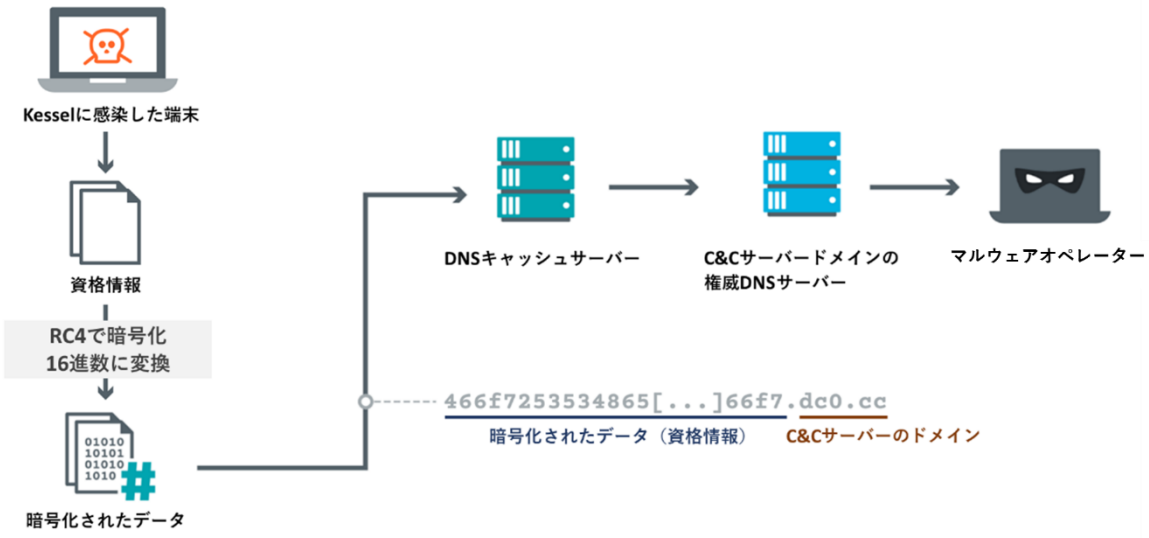
他の仮想通貨採掘プログラムを終了する処理（黄枠はプログラムのプロセス名）

Bonadan は次に C&C サーバーに OS バージョンなどの端末情報を送信し、対応する仮想通貨発掘プログラムをダウンロード・実行します。このプログラムは Monero と呼ばれる仮想通貨を採掘します。採掘された仮想通貨は、設定されたウォレットアドレスに送金されます。Bonadan は他のバックドアと同様に、情報を窃取する機能も持っています。

■ 様々なプロトコルで情報を持ち出す「Kessel」

Kessel は今回 ESET 社が発見した中で、最も高度で最も新しいバックドアです。2018 年 8 月から活動が確認されています。認証情報を窃取する機能とボットの機能を持ちます。
Kessel の大きな特徴として、C&C サーバーとの通信に様々なプロトコルを使用することが挙げられます。一般的な HTTP、TCP プロトコルに加えて、DNS プロトコルによる通信機能を備えています。
DNS を用いた情報窃取は以下の順序で実行されます。

1. 資格情報（リモートホスト名、リモートユーザー名、ローカルユーザー名、パスワード等）をハードコードされた鍵を用いて RC4（暗号方式）で暗号化する
2. 暗号化したデータを 16 進数に変換し、ラベル（ドメイン名中のドットで区切られた文字列）の文字長制限に収まるように 63 文字以下に分割する
3. 分割した文字列と C&C サーバーのドメイン名を連結してドメイン名を作成する
4. 作成したドメインを用いて DNS サーバーに問い合わせを行うことで、情報を送信する



Kessel の DNS を使った情報窃取

■ 全く異なる 2 つの攻撃に使われた「Kamino」

Kamino の特徴はその歴史にあります。このバックドアが初めて使われたのは 2013 年のことです。DarkLeech（Apache サーバーに設置された不正なモジュール）との組み合わせで感染を拡大し、数多くの被害をもたらしました。また、翌年の 2014 年には Carbanak として知られる攻撃者グループによってロシアの金融機関に対する標的型攻撃に使われました。
下図のとおり、2 つの攻撃で使われた Kamino のコードはほとんど一致しています。

C&C サーバーとの通信部分のコード比較（反転箇所を除き同一の処理）

いずれも金銭を目的とした攻撃で、Carbanak が発見された後すぐに DarkLeech が姿を消したことから、同一の攻撃者グループによる犯行の可能性が大いに考えられます。
一方で、DarkLeech がアンダーグラウンドのフォーラムで販売されていたことを考慮すると、異なる攻撃者グループがそれぞれ Kamino を入手し、使用した可能性もあります。
攻撃者の帰属（アトリビューション）には常に慎重であるべきでしょう。

ESET 製品ではこれらの OpenSSH バックドアを以下の検出名で検出し、攻撃を防ぎます。

- Linux/SSHDoor

世界で公開されている Web サイトの 37%は Linux サーバーで動作しているという調査結果（2019 年 1 月時点の W3Techs の統計）もあり、Linux に対する攻撃は今後も続くことが予想されます。
今回ご紹介したようなマルウェアによる攻撃を防ぐために、以下のことを推奨します。

- OS やアプリケーションを最新の状態に保つ（更新パッチを適用する）
- 公開鍵認証方式の SSH を利用する
- root のリモートログインを無効にする
- 多要素認証を利用する

ご紹介したように、今月も引き続き Web 上で動作するマルウェアが国内で検出されたほか、ESET 社が新たな OpenSSH バックドアを発見しました。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

キヤノンマーケティングジャパン株式会社