2019年
7·8月
JUL / AUG

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

ランサムウェア「Sodinokibi」の被害が世界中で拡大

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

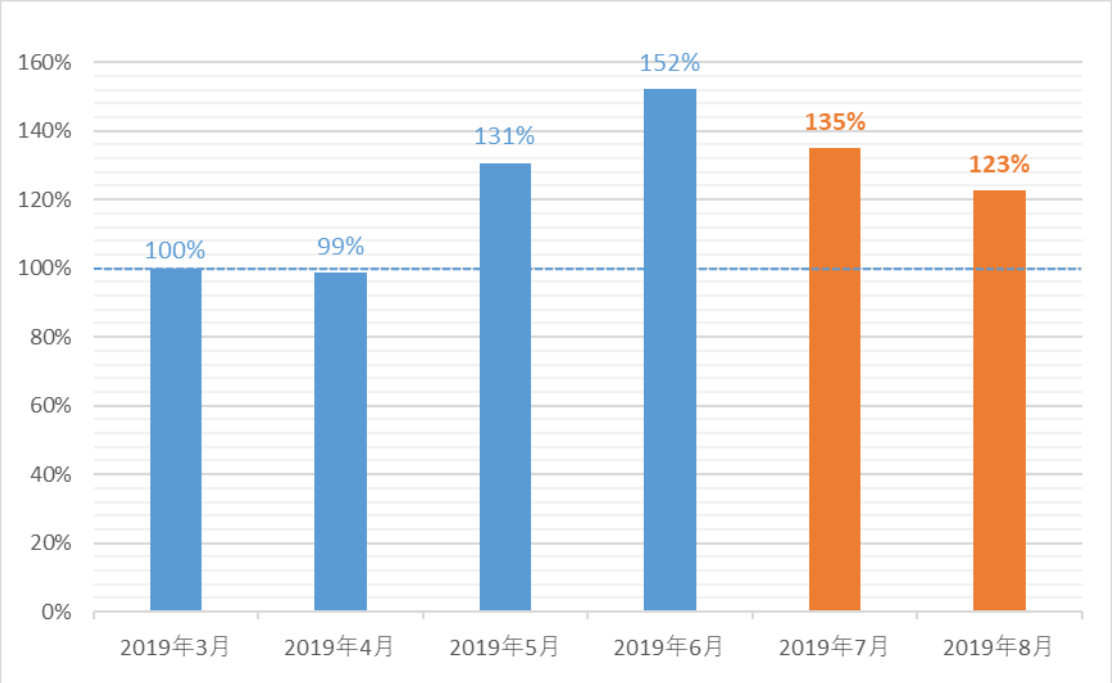
国内のマルウェア検出状況についてまとめたレポートです。

ショートレポート「2019 年 7 月･8 月マルウェア検出状況」

1. 7 月と 8 月の概況
2. ランサムウェア Sodinokibi の脅威

1. 7 月と 8 月の概況について

2019 年 7 月（7 月 1 日～7 月 31 日）と 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*1 の推移

（2019 年 3 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 7 月と 8 月の国内マルウェア検出数は、6 月と比較すると減少しましたが、4 月以前と比較すると高い水準にあります。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 7 月･8 月）

順位	マルウェア名	割合	種別
1	JS/Adware.Agent	16.8%	アドウェア
2	JS/Adware.Subprop	8.1%	アドウェア
3	HTML/ScrInject	7.5%	HTML に埋め込まれた不正スクリプト
4	HTML/IFrame	4.0%	別のページに遷移させるスクリプト
5	HTML/Refresh	2.0%	別のページに遷移させるスクリプト
6	HTML/FakeAlert	1.7%	偽の警告文を表示するスクリプト
7	JS/Redirector	1.6%	別のページに遷移させるスクリプト
8	Win32/Exploit.CVE-2017-11882	1.4%	脆弱性を悪用するマルウェア
9	PDF/Fraud	1.3%	フィッシング目的の PDF ファイル
10	Win32/Injector.Autoit	1.1%	他のプロセスにインジェクションするマルウェア

*2 本表には PUA を含めていません。

国内マルウェア検出数*2 上位（2019 年 7 月）

順位	マルウェア名	割合	種別
1	JS/Adware.Agent	15.8%	アドウェア
2	JS/Adware.Subprop	8.8%	アドウェア
3	HTML/ScrInject	6.6%	HTML に埋め込まれた不正スクリプト
4	HTML/IFrame	4.2%	別のページに遷移させるスクリプト
5	HTML/FakeAlert	2.3%	偽の警告文を表示するスクリプト
6	HTML/Refresh	2.0%	別のページに遷移させるスクリプト
7	JS/Redirector	1.5%	別のページに遷移させるスクリプト
8	Win32/Exploit.CVE-2017-11882	1.5%	脆弱性を悪用するマルウェア
9	VBA/TrojanDownloader.Agent	1.4%	ダウンローダー
10	Win32/Injector.Autoit	1.3%	他のプロセスにインジェクションするマルウェア

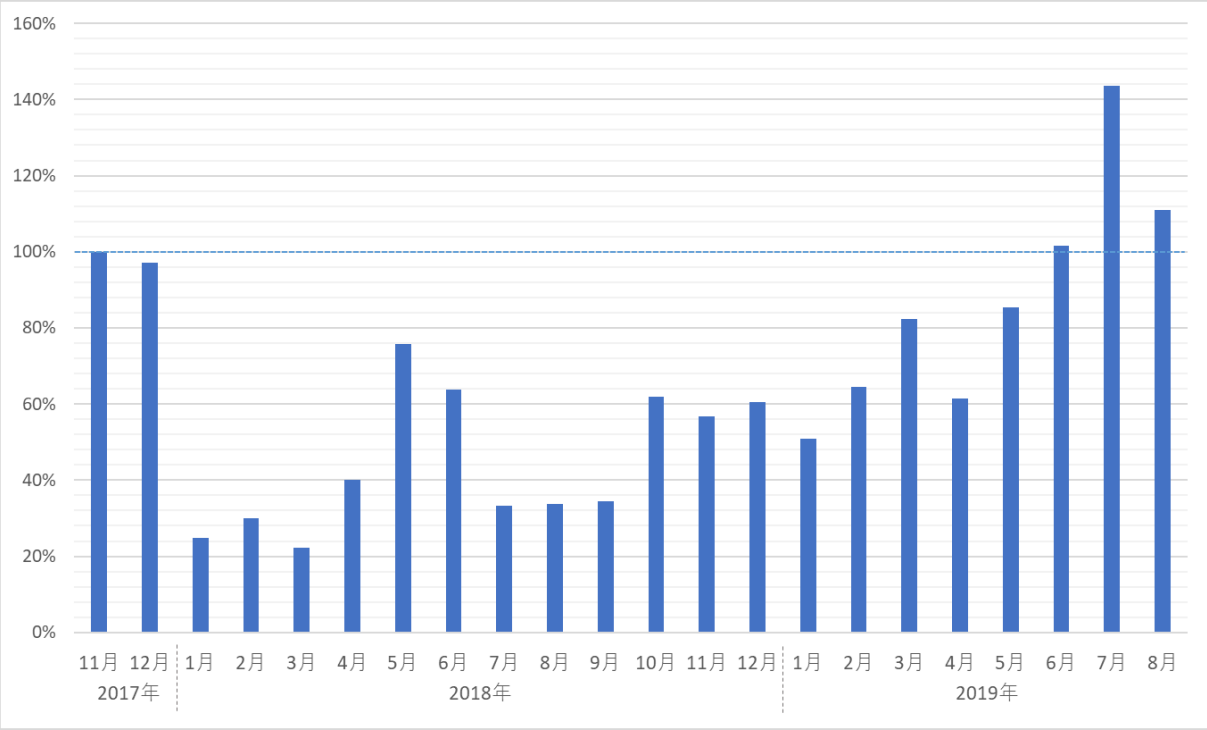
国内マルウェア検出数*2 上位（2019 年 8 月）

順位	マルウェア名	割合	種別
1	JS/Adware.Agent	17.8%	アドウェア
2	HTML/ScrInject	8.6%	HTML に埋め込まれた不正スクリプト
3	JS/Adware.Subprop	7.4%	アドウェア
4	HTML/IFrame	3.8%	別のページに遷移させるスクリプト
5	PDF/Fraud	2.0%	フィッシング目的の PDF ファイル
6	HTML/Refresh	2.0%	別のページに遷移させるスクリプト
7	JS/Redirector	1.7%	別のページに遷移させるスクリプト
8	Win32/Exploit.CVE-2017-11882	1.3%	脆弱性を悪用するマルウェア
9	DOC/Abnormal	1.1%	ドキュメント形式のマルウェアの汎用名
10	HTML/FakeAlert	1.0%	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。

7 月と 8 月に国内で最も多く検出されたマルウェアは、6 月に引き続き JS/Adware.Agent でした。JS/Adware.Agent は不正な広告を表示させるアドウェアで、Web サイト閲覧時に実行されます。2 番目に多く検出された JS/Adware.Subprop も同様の動作をするアドウェアです。上位 7 種までのマルウェアはすべて Web ブラウザー上で実行される脅威で、不正広告やエクスプロイトキットが設置されているサイトに誘導するスクリプト等が該当します。

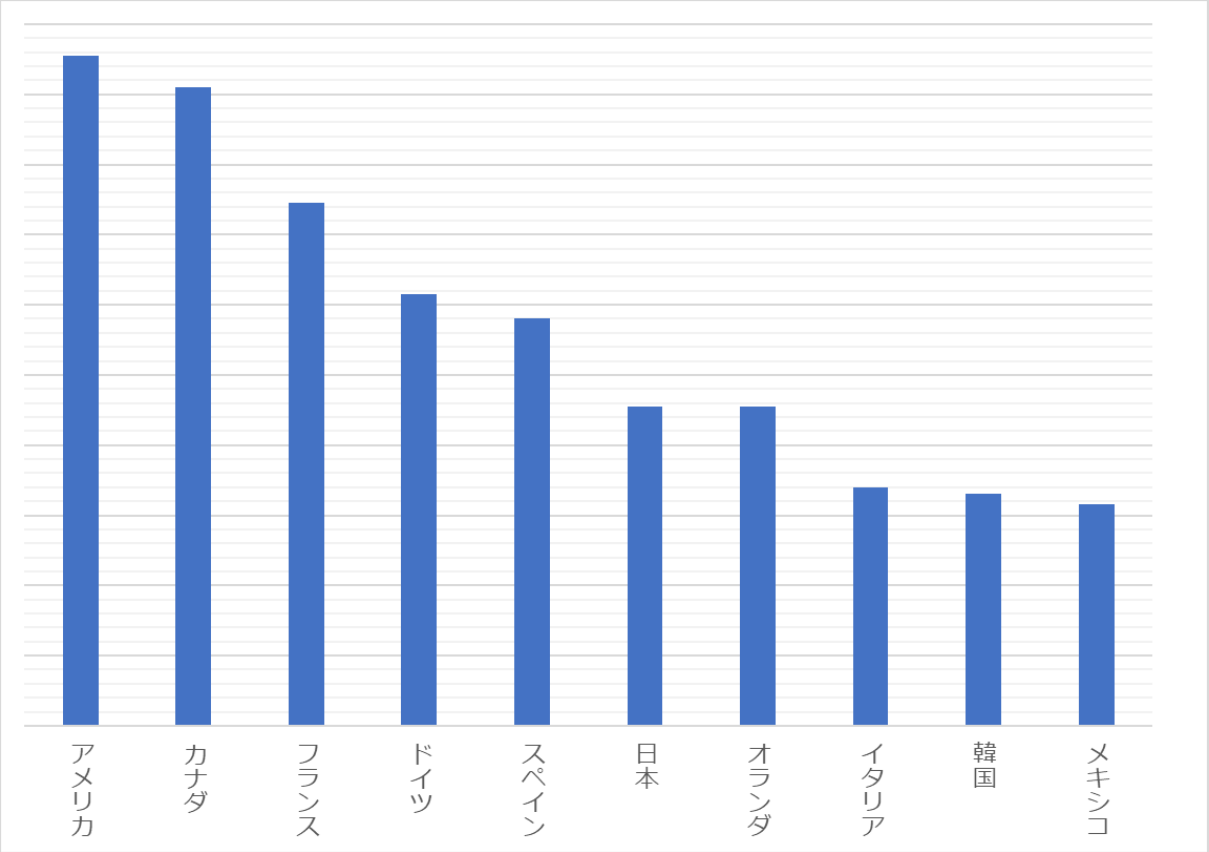
8 位の Win32/Exploit.CVE-2017-11882 は Microsoft Office 数式エディターに存在する脆弱性（CVE-2017-11882）を悪用するマルウェアです。今年初めから徐々に検出数が増加し、2019 年 6 月には脆弱性発見時（2017 年 11 月）の検出数を上回りました。CVE-2017-11882 に対処した修正プログラムは 2017 年の 11 月の時点で公開されましたが、未だにその脆弱性を悪用する攻撃が続いています。お使いの PC に修正プログラムが適用されているかどうか、今一度ご確認下さい。



Win32/Exploit.CVE-2017-11882 の検出数（国内）
(2017 年 11 月の全検出数を 100%として比較)

2. ランサムウェア Sodinokibi の脅威

2019 年 4 月以降、Sodinokibi（ESET 検出名：Win32/Filecoder.Sodinokibi）と呼ばれるランサムウェアが国内外で猛威を奮っています。
8 月の中旬にはアメリカ･テキサス州で 23 か所の地方自治体が Sodinokibi の被害にあったほか、8 月末にはアメリカの数百か所以上の歯科医院で同ランサムウェアの感染が発生しています。
Sodinokibi が特に多く検出されている国はアメリカやカナダで、欧州の国々が続きます。
日本においては世界に 6 番目に多く検出されています。

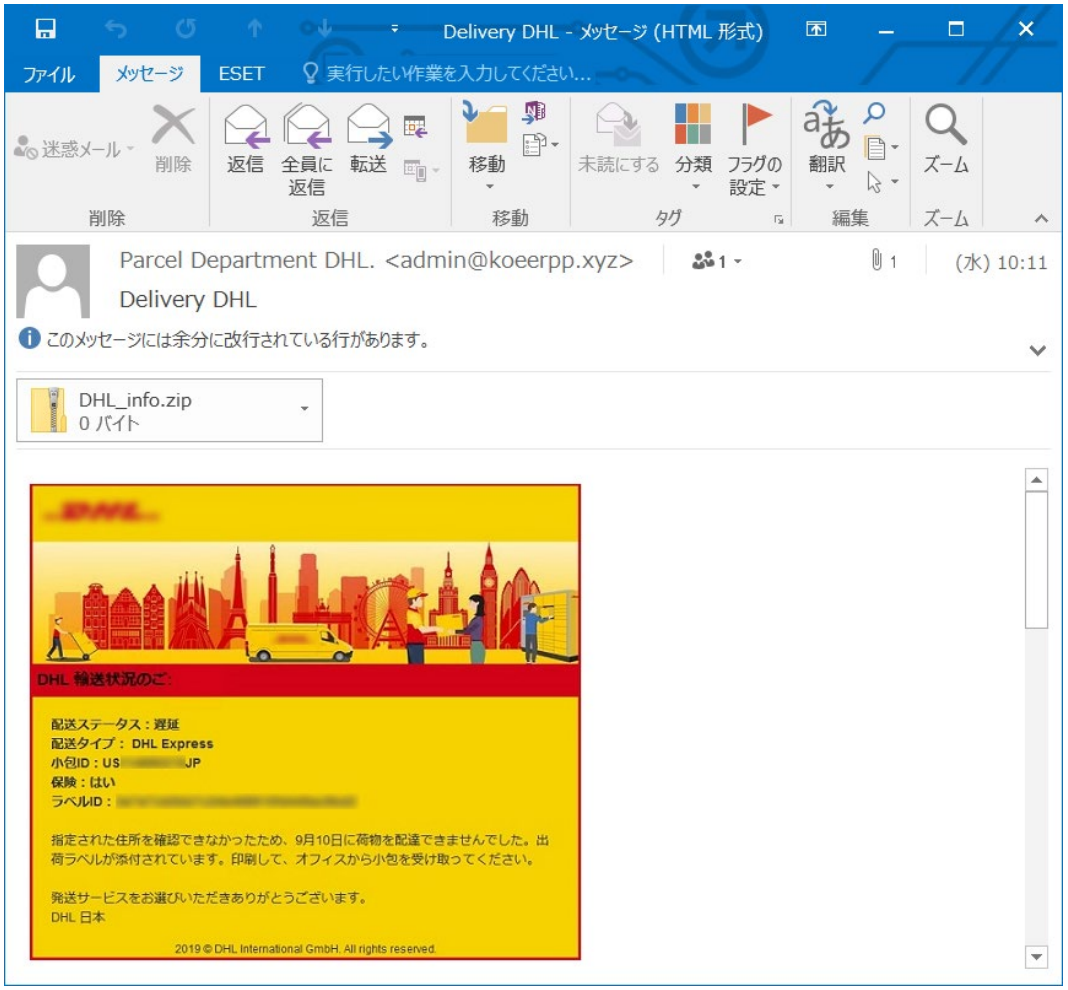


Win32/Filecoder.Sodinokibi の国別検出数（2019 年）

Sodinokibi の特長として、感染経路が多岐にわたることが挙げられます。以下は一例です。

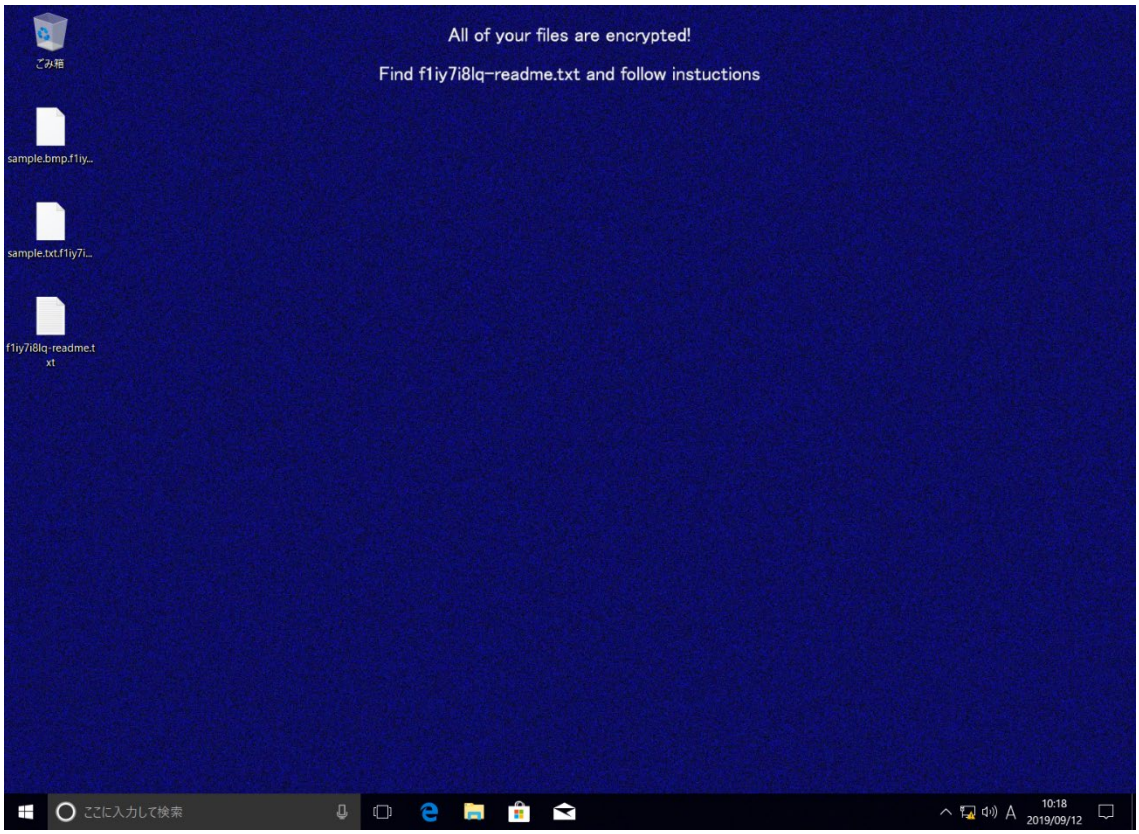
1. メールの添付ファイルを実行する
2. メールに記載された URL からファイルをダウンロード・実行する
3. Exploit Kit（CVE-2018-4878 等を悪用）が設置された Web サイトを閲覧する
4. Oracle WebLogic Server の脆弱性（CVE-2019-2725）を悪用され、攻撃者サーバーからファイルを送り込まれる

ここでは最も代表的な[1.] メールの添付ファイル経由の感染について解説します。
今回確認したメールは実在する運送会社を装っており、出荷ラベルを送付するとの名目で受信者が添付ファイルを開くよう誘導します。



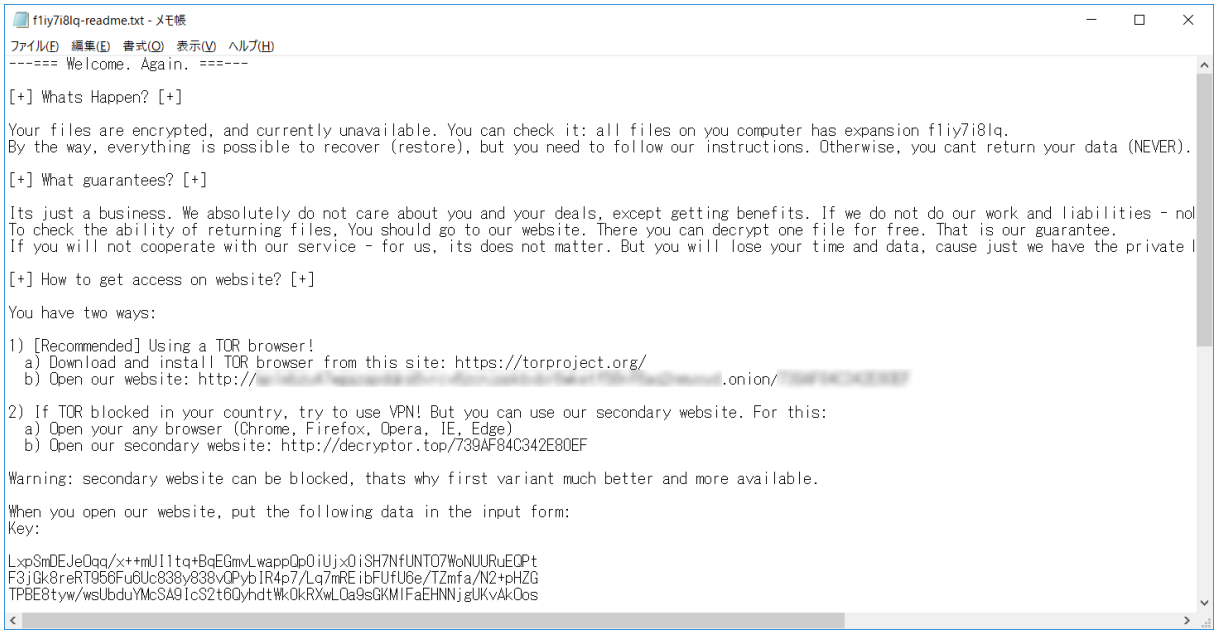
実在の運送会社を騙ったメール

メールに添付された zip ファイルを展開し中にある exe ファイルを実行すると、Sodinokibi ランサムウェアに感染します。ディスク上のファイルは暗号化され、拡張子がランダムな英数字（いずれのファイルも同じ）に変更されます。その後、デスクトップの壁紙が変更されます。



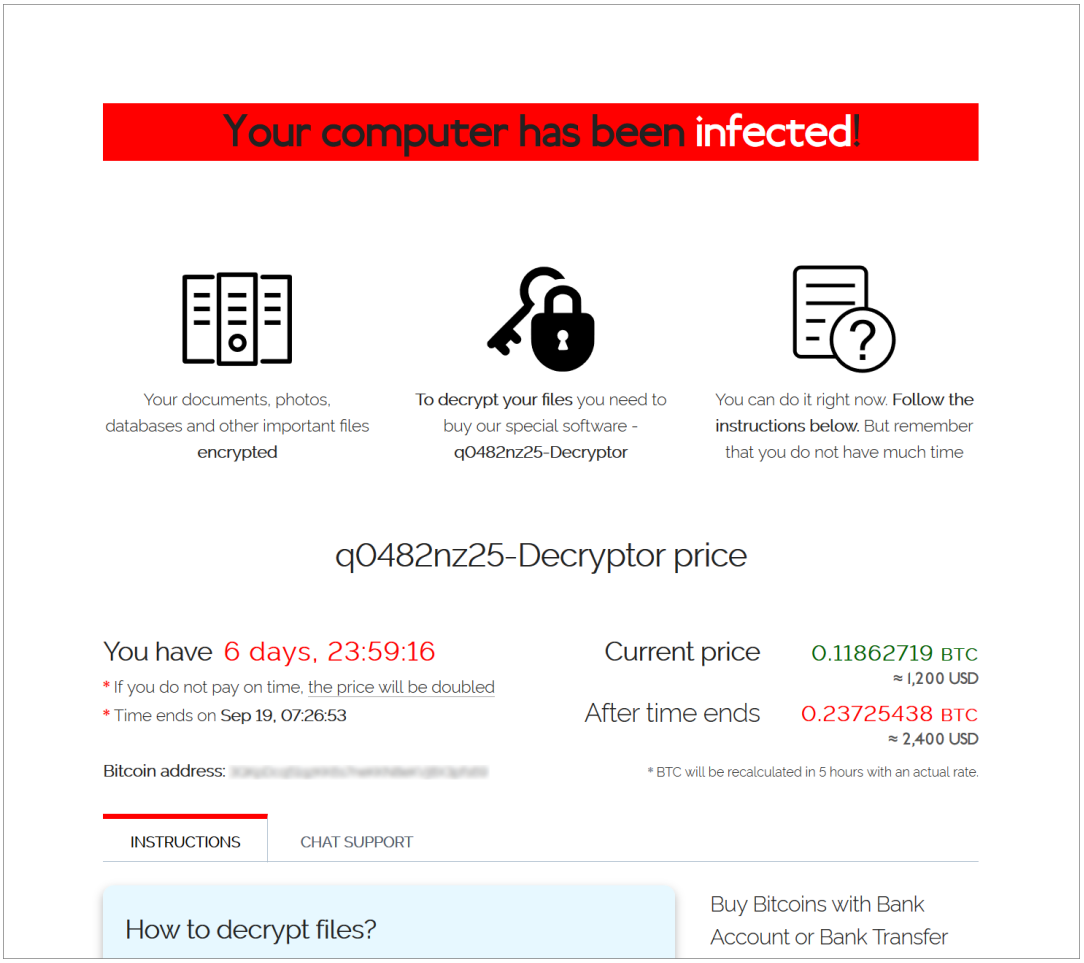
Sodinokibi 感染後のデスクトップ画面

暗号化されたファイルと同じフォルダーにはテキストファイルが作成されます。テキストファイルの中には、ファイルを元に戻す方法として攻撃者が用意した Web サイトにアクセスする方法が記載されています。



Sodinokibi のランサムノート（身代金要求文書）

攻撃者の Web サイトには、身代金の支払い方法と金額が記載されています。
身代金の要求額は 0.11862719 ビットコイン（2019 年 9 月現在およそ 129,000 円）で、7 日以内に支払わなかった場合は身代金が倍増すると書かれています。身代金を支払ったとしても、すべてのファイルが元に戻る保証はありません。



身代金支払い用のサイト

Sodinokibi は感染手法が最も洗練されたランサムウェアの一つです。今後その手法がさらに巧妙化することも考えられます。また、最近のランサムウェアは個人だけではなく、政府機関や医療機関など重要度の高いデータを持つ組織を狙う傾向にあります。重要なデータは頻繁にバックアップを取得し、ネットワークから隔離しておくことを推奨します。

ご紹介したように、7 月 8 月は Web ブラウザーを実行環境とする脅威が多く検出されました。また、Sodinokibi と呼ばれるランサムウェアの被害が世界中で広がっています。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