2021年
7·8月
JULY/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

キヤノンマーケティングジャパン株式会社

はじめに

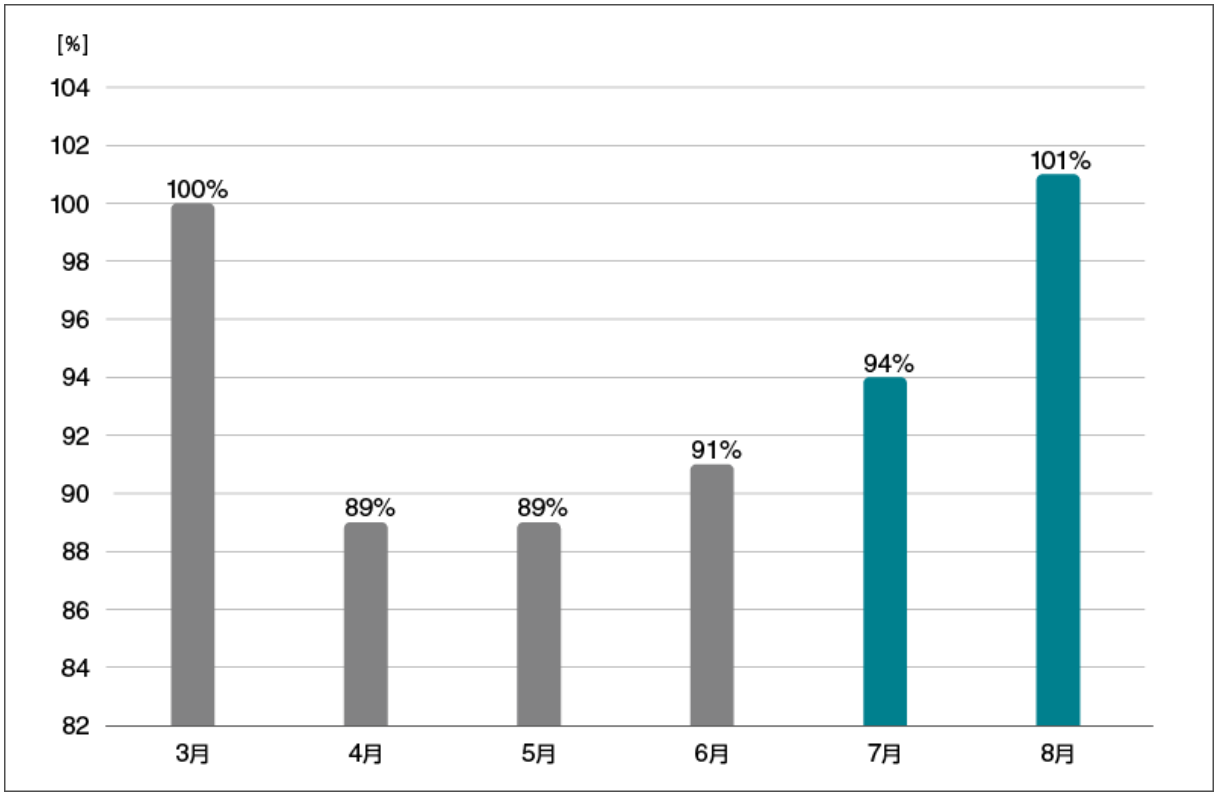
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「サイバーセキュリティラボ」が「ESET セキュリティソリューションシリーズ」の

マルウェア検出データを基に国内のマルウェア検出状況を分析し、まとめたレポートです。

2021 年 7 月 8 月マルウェア検出状況

2021 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の推移は、以下のとおりです。



国内マルウェア検出数*1の推移

(2021 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。

2021 年 7 月と 8 月の国内マルウェア検出数は、増加傾向にあります。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（2021 年 7 月 8 月）

順位	マルウェア	割合	種別
1	JS/Adware.Agent	20.2%	アドウェア
2	JS/Adware.Sculinst	8.8%	アドウェア
3	HTML/Phishing.Agent	8.4%	メールに添付された不正な HTML ファイル
4	DOC/Fraud	7.0%	詐欺サイトのリンクが埋め込まれた doc ファイル
5	JS/Adware.TerraClicks	4.8%	アドウェア
6	JS/Adware.Subprop	4.8%	アドウェア
7	HTML/ScrInject	1.5%	HTML に埋め込まれた不正スクリプト
8	HTML/Fraud	1.5%	詐欺サイトのリンクが埋め込まれた HTML ファイル
9	JS/Adware.PopAds	1.5%	アドウェア
10	HTML/FakeAlert	1.5%	偽の警告文を表示させる HTML ファイル

*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（2021 年 7 月）

順位	マルウェア	割合	種別
1	JS/Adware.Agent	20.0%	アドウェア
2	JS/Adware.Sculinst	8.8%	アドウェア
3	HTML/Phishing.Agent	6.5%	メールに添付された不正な HTML ファイル
4	DOC/Fraud	6.0%	詐欺サイトのリンクが埋め込まれた doc ファイル
5	JS/Adware.TerraClicks	5.3%	アドウェア
6	JS/Adware.Subprop	4.3%	アドウェア
7	HTML/Phishing	2.3%	悪意のある HTML の汎用検出名
8	HTML/ScrInject	2.0%	HTML に埋め込まれた不正スクリプト
9	JS/Adware.PopAds	1.5%	アドウェア
10	HTML/Fraud	1.4%	詐欺サイトのリンクが埋め込まれた HTML ファイル

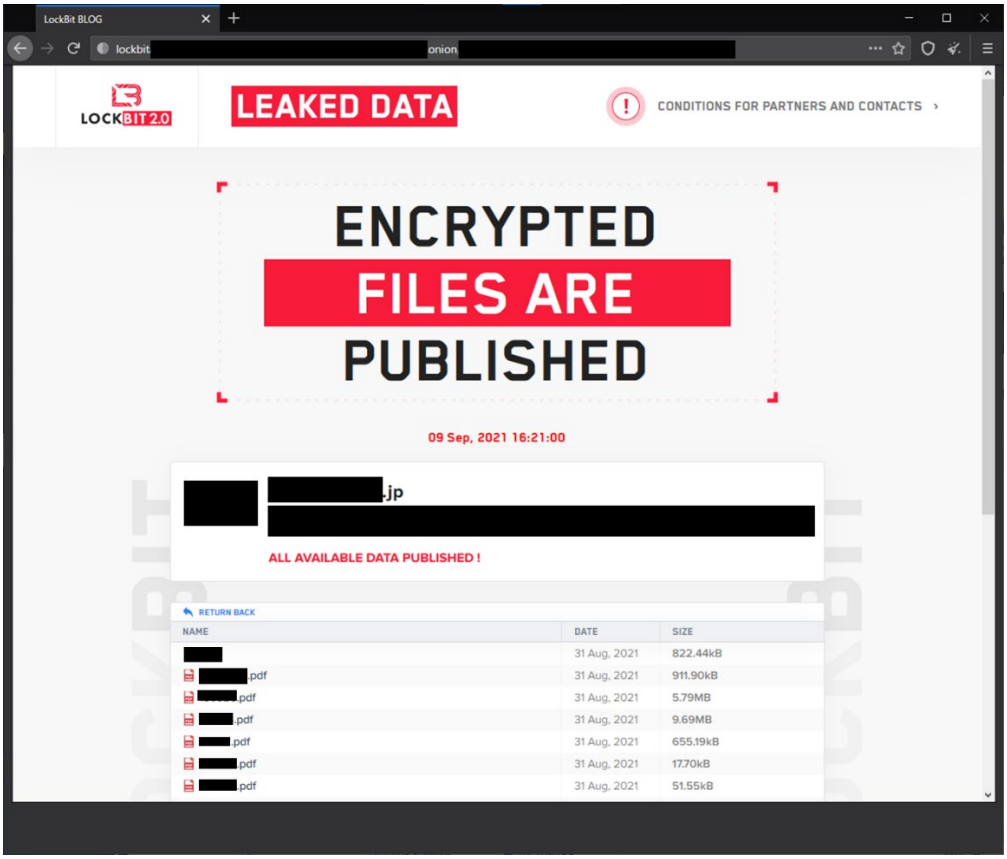
国内マルウェア検出数*2 上位（2021 年 8 月）

順位	マルウェア	割合	種別
1	JS/Adware.Agent	20.4%	アドウェア
2	HTML/Phishing.Agent	10.1%	メールに添付された不正な HTML ファイル
3	JS/Adware.Sculinst	8.8%	アドウェア
4	DOC/Fraud	7.8%	詐欺サイトのリンクが埋め込まれた doc ファイル
5	JS/Adware.Subprop	5.2%	アドウェア
6	JS/Adware.TerraClicks	4.4%	アドウェア
7	HTML/FakeAlert	2.2%	偽の警告文を表示させる HTML ファイル
8	HTML/Fraud	1.7%	詐欺サイトのリンクが埋め込まれた HTML ファイル
9	JS/Adware.PopAds	1.6%	アドウェア
10	HTML/ScrInject	1.1%	HTML に埋め込まれた不正スクリプト

*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、JS/Adware.Agent でした。
JS/Adware.Agent は、悪意のある広告を表示させるアドウェアの汎用検出名です。Web サイト閲覧時に実行されます。

7 月と 8 月も、Web ブラウザー上で実行される脅威が多数検出されています。検出数上位 10 種には、アドウェアやフィッシング詐欺を狙った脅威が入っています。
これらの脅威以外にも、7 月と 8 月には、ランサムウェア LockBit 2.0 による被害が国内外の企業で確認されています。
LockBit は、2019 年頃に初めて確認されたランサムウェアです。2021 年 6 月頃にバージョン 2.0 へとアップグレードされました。
LockBit 2.0 は、ファイルの暗号化だけでなくデータの窃取も行います。そして、窃取したデータを公開するといったドキシングによる脅迫行為も確認されています。

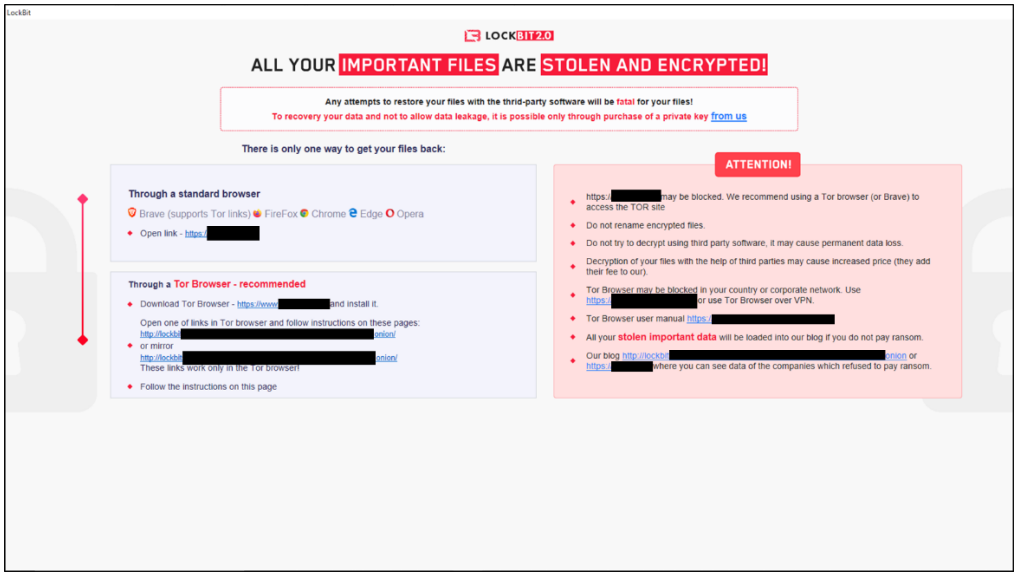


国内の企業から窃取した情報を公開している LockBit 2.0 のブログ

現在確認されている感染経路としては、ネットワーク機器に存在する脆弱性の悪用などが挙げられます。
LockBit 2.0 に感染すると、ファイルが暗号化され、拡張子を「lockbit」に変更されます。
また、感染後に PC の壁紙を以下の画像に変更されます。

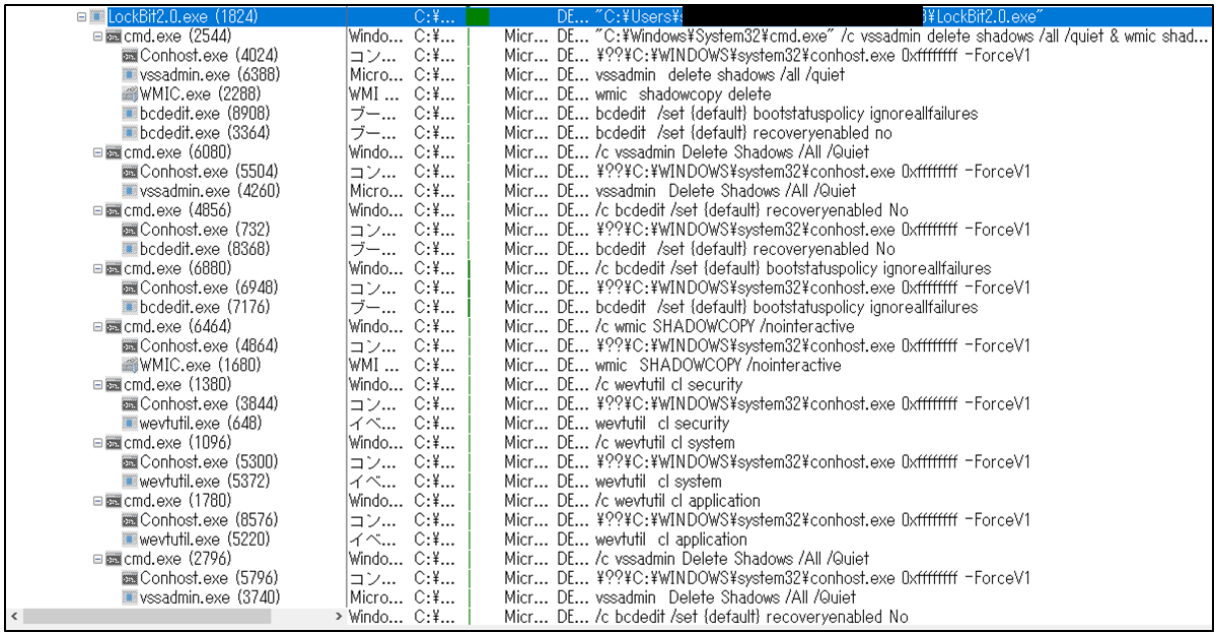
国内の企業から窃取した情報を公開している LockBit 2.0 のブログ

併せて、hta（HTML アプリケーション）形式のランサムノートも表示されます。ランサムノートには、Tor ブラウザーのインストール方法、感染した PC に起きたことの説明、注意事項について書かれています。



感染後に表示されるランサムノート

サンプル実行時のプロセスを見ると、多数の子プロセスを作成していることがわかります。
子プロセスではシャドウコピーの削除、Windows 自動修復機能の無効化やイベントログの削除などを行っています。

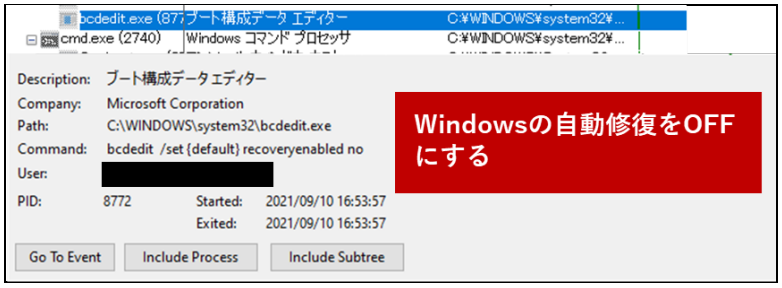


LockBit 2.0 に感染した時の親プロセスと子プロセスの一部

シャドウコピーを削除する目的は、暗号化したファイルの復元を妨害するためだと考えられます。また、確実にシャドウコピーを削除するために、さまざまなコマンドで実行しています。

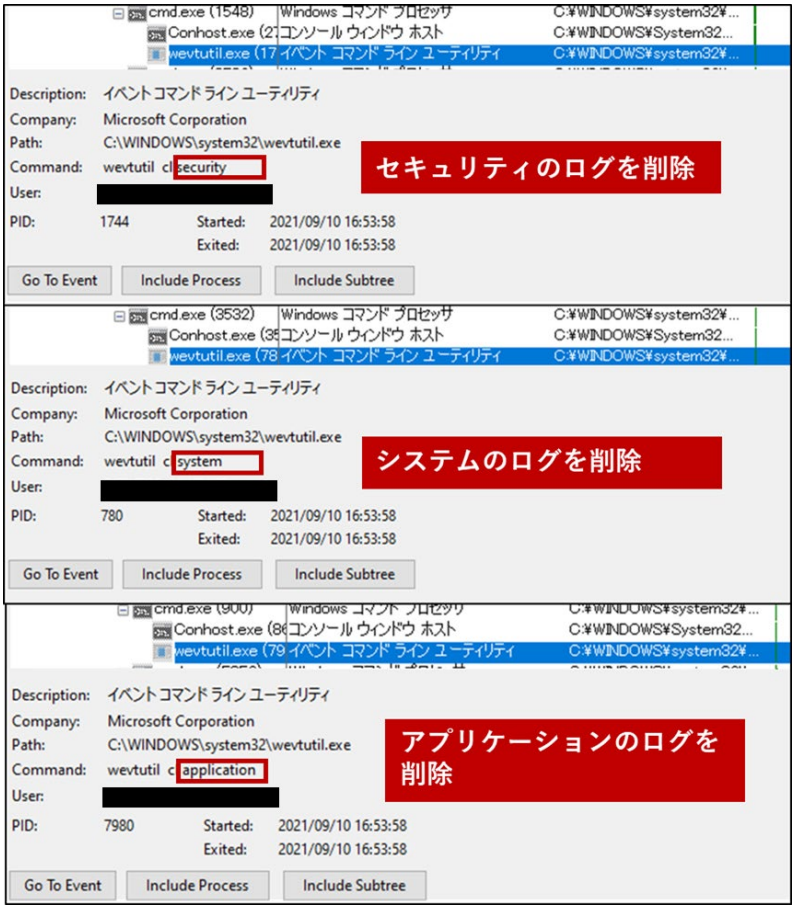
シャドウコピーを削除するコマンドを実行しているプロセス

Windows が正常に起動しない際のトラブルシューティングをオフにすることで、システムの復元などを妨害していると考えられます。



Windows の自動修復機能をオフにしているプロセス

セキュリティログやシステムログ、アプリケーションログを削除する理由として、自身の痕跡を隠すことが考えられます。



イベントログを削除するプロセス

また、解析したサンプルでは起動していた解析ツールを終了させる動作もありました。今回は、ファイル名をデフォルトから変更することで、終了させずにツールを使用することができました。自身を解析させないことなどが、目的として考えられます。
ご紹介したように、7 月と 8 月は、ランサムウェア LockBit 2.0 による被害を確認しています。このような被害に遭わないためにも、セキュリティ製品を正しく運用することが重要です。また、オフラインバックアップを取得することで、ランサムウェアの被害に遭った際に被害を軽減できる可能性があります。

■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
マルウェアの多くは、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
マルウェアの多くが狙う「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
万が一マルウェアに感染した場合、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」の方がマルウェアに感染するリスクは低いと考えられます。マルウェア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。

引用・出典元

■welivesecurity「Accenture es víctima de un ataque del ransomware Lockbit 2.0」
https://www.welivesecurity.com/la-es/2021/08/12/accenture-es-victima-de-ataque-del-ransomware-lockbit-2-0/?utm_campaign=welivesecurity&utm_source=twitter&utm_medium=social

Canon

キヤノンマーケティングジャパン株式会社