2019年
11月
NOVEMBER

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

新種のランサムウェア「NextCry」

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

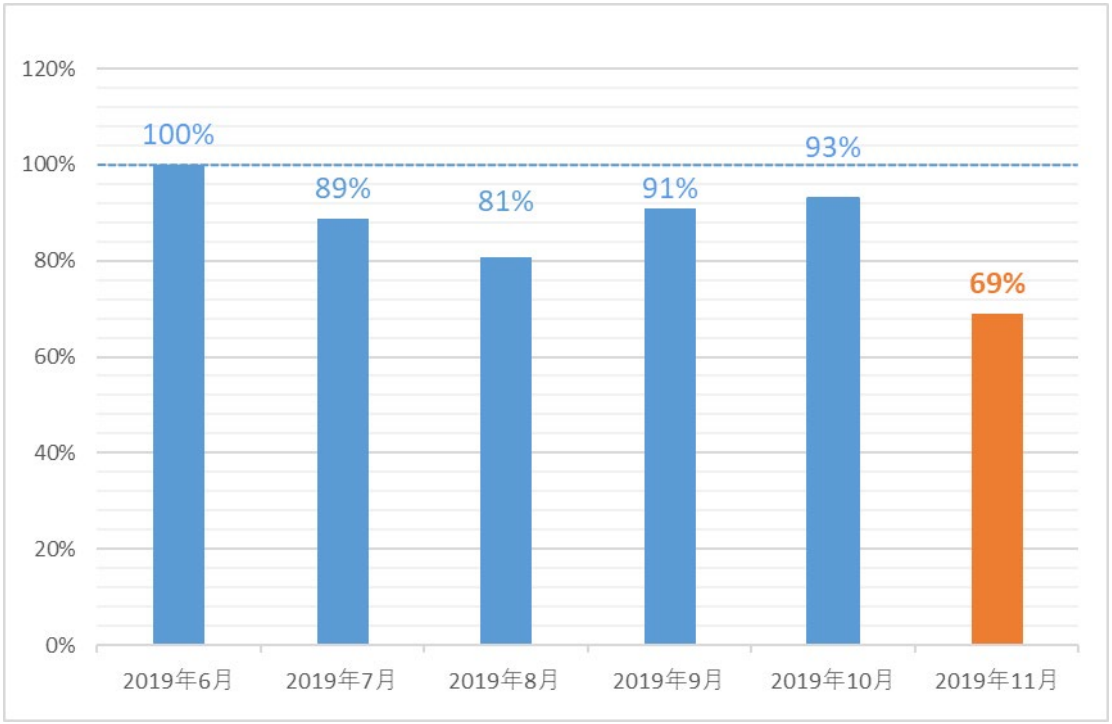
国内のマルウェア検出状況についてまとめたレポートです。

ショートレポート「2019 年 11 月マルウェア検出状況」

1. 11 月の概況
2. 新種のランサムウェア「NextCry」

1. 11 月の概況について

2019 年 11 月（11 月 1 日～11 月 30 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 6 月*2 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。

*2 半年前を基準としています。

2019 年 11 月の国内マルウェア検出数は、増加していた 10 月と変わって、減少しました。直近 6 か月間の中で最も検出数の少ない月となっています。
検出されたマルウェアの内訳は以下のとおりです。

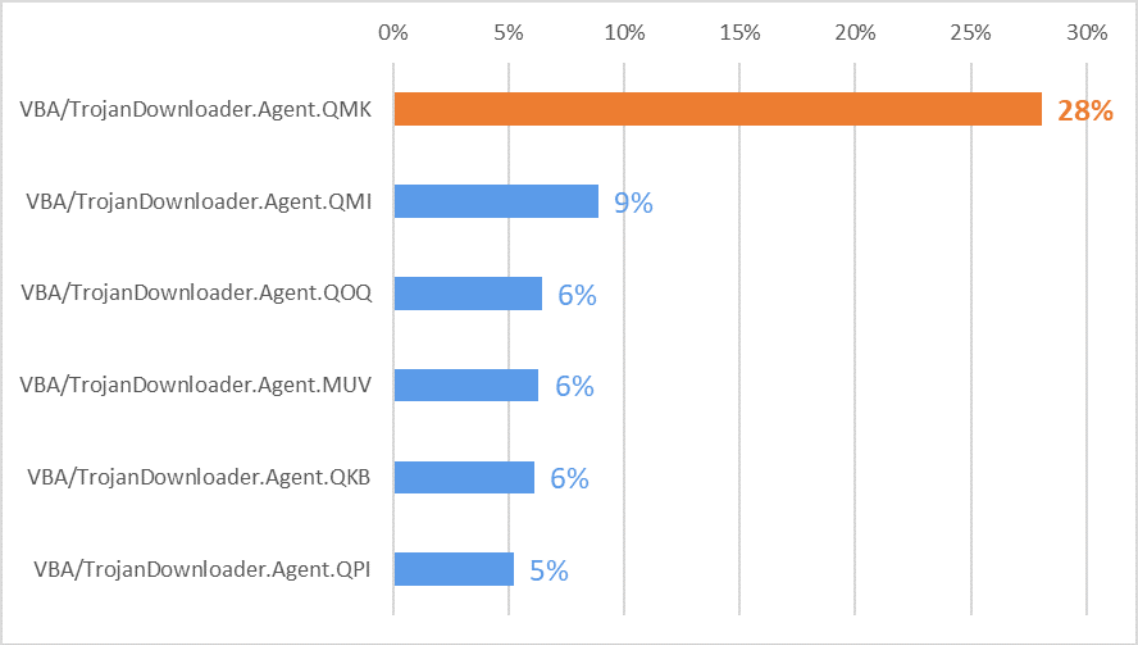
国内マルウェア検出数*3 上位（2019 年 11 月）

順位	マルウェア名	割合	種別
1	HTML/ScrInject	17.2%	HTML に埋め込まれた不正スクリプト
2	JS/Adware.Agent	14.5%	アドウェア
3	VBA/TrojanDownloader.Agent	6.4%	ダウンローダー
4	HTML/FakeAlert	4.8%	偽の警告文を表示するスクリプト
5	DOC/Fraud	3.3%	詐欺サイトのリンクが埋め込まれた doc ファイル
6	HTML/Refresh	1.8%	別のページに遷移させるスクリプト
7	Win32/Exploit.CVE-2017-11882	1.5%	脆弱性を悪用するマルウェア
8	Win32/Injector.Autoit	1.2%	他のプロセスにインジェクションするマルウェア
9	DOC/Abnormal	1.0%	トロイの木馬
10	JS/Redirector	1.0%	別のページに遷移させるスクリプト

*3 本表には PUA を含めていません。

11 月に国内で最も多く検出されたマルウェアは、10 月に引き続き HTML/ScrInject でした。HTML/ScrInject は HTML に埋め込まれた不正スクリプトで、Web サイト閲覧時に実行されます。

3 位の VBA/TrojanDownloader.Agent は、Office 製品で利用されるプログラミング言語の VBA で作成されたダウンローダーです。ファイル形式は、doc あるいは xls 形式であることが大半です。他のマルウェアをダウンロードすることで知られていますが、中には、10 月から被害が多く報告されている「Emotet」のダウンローダーとして機能するものもあります。
VBA/TrojanDownloader.Agent の検出の中で、最も多く検出された亜種は VBA/TrojanDownloader.Agent.QMK でした。その割合は、VBA/TrojanDownloader.Agent の検出数の約 28%でした。

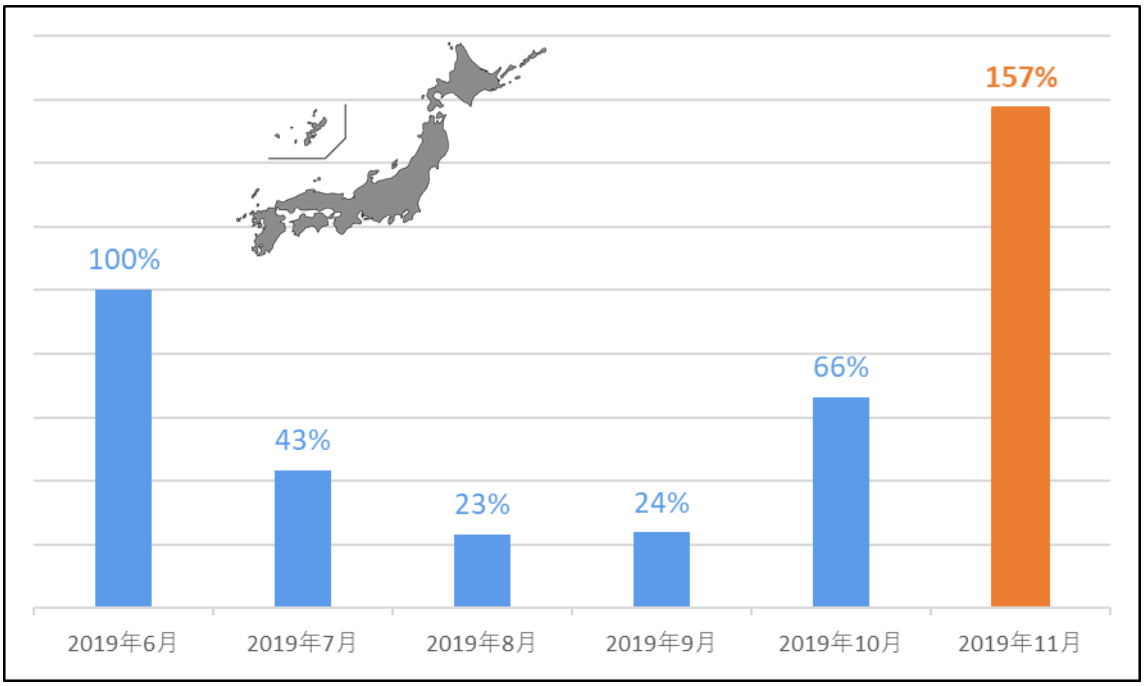


日本国内における VBA/TrojanDownloader.Agent の亜種内訳（11 月）

VBA/TrojanDownloader.Agent.QMK は、バンキングマルウェア「Dridex」をダウンロードするダウンローダーでした。また、検出数第 2 位の VBA/TrojanDownloader.Agent.QMI は、確認できたものではバンキングマルウェアをダウンロードしていました。
Dridex とは、バンキングマルウェアであり、ボットネットを形成することでも知られています。また、2019 年 12 月 5 日に US-CERT が注意喚起を行っており、今後も注意が必要なマルウェアの一つです。

Office 製品のマクロ自動実行が無効であるかを確認することやネットバンキングの利用履歴に怪しいものがないかを確認することが重要です。

国内で検出された VBA/TrojanDownloader.Agent は、直近 6 か月の中では最も多く検出されました。減少傾向にあった検出数も 9 月頃から次第に増加し始めており、10 月から 11 月にかけては約 2 倍増加しています。



VBA/TrojanDownloader.Agent の国内での検出数の推移
（2019 年 6 月の検出数を 100%として比較）

2. 新種のランサムウェア「NextCry」

新種のランサムウェア NextCry が発見されました。
NextCry による被害として、オンラインストレージサービス NextCloud 上のデータが暗号化される事例が確認されています。本事例の侵入経路には、PHP-FPM（FastCGI Process Manager）の脆弱性が用いられました。

■PHP-FPM の脆弱性
PHP-FPM とは、Web サイトのパフォーマンスを向上させるために用いられる、PHP の実行環境です。
10 月末に、PHP-FPM に対して境界外書き込みに関する脆弱性（CVE-2019-11043）の情報と、その修正パッチが公開されました。また、本脆弱性を悪用する PoC も公開されているため、悪用が比較的容易です。
本脆弱性が悪用されると、リモートの攻撃者が任意のコードを実行する可能性があります。

警察庁 @police から注意喚起も出ており、本脆弱性の悪用を目的としたアクセスの観測結果が公開されています。

■NextCry の解析結果
NextCry は、Linux 上で動作する ELF 形式のバイナリファイルです。

```
user01@ubuntu:/home$ hexdump -C nextcry | head
00000000  7f 45 4c 46 02 01 01 00  00 00 00 00 00 00 00 00  |.ELF............|
00000010  02 00 3e 00 01 00 00 00  75 1a 40 00 00 00 00 00  |..>.....u.@.....|
00000020  40 00 00 00 00 00 00 00  f0 0c 52 00 00 00 00 00  |@.........R.....|
00000030  00 00 00 00 40 00 38 00  08 00 40 00 1d 00 1c 00  |....@.8...@.....|
00000040  06 00 00 00 05 00 00 00  40 00 00 00 00 00 00 00  |........@.......|
00000050  40 00 40 00 00 00 00 00  40 00 40 00 00 00 00 00  |@.@.....@.@.....|
00000060  c0 01 00 00 00 00 00 00  c0 01 00 00 00 00 00 00  |................|
00000070  08 00 00 00 00 00 00 00  03 00 00 00 04 00 00 00  |................|
00000080  00 02 00 00 00 00 00 00  00 02 40 00 00 00 00 00  |..........@.....|
00000090  00 02 40 00 00 00 00 00  1c 00 00 00 00 00 00 00  |..@.............|
```

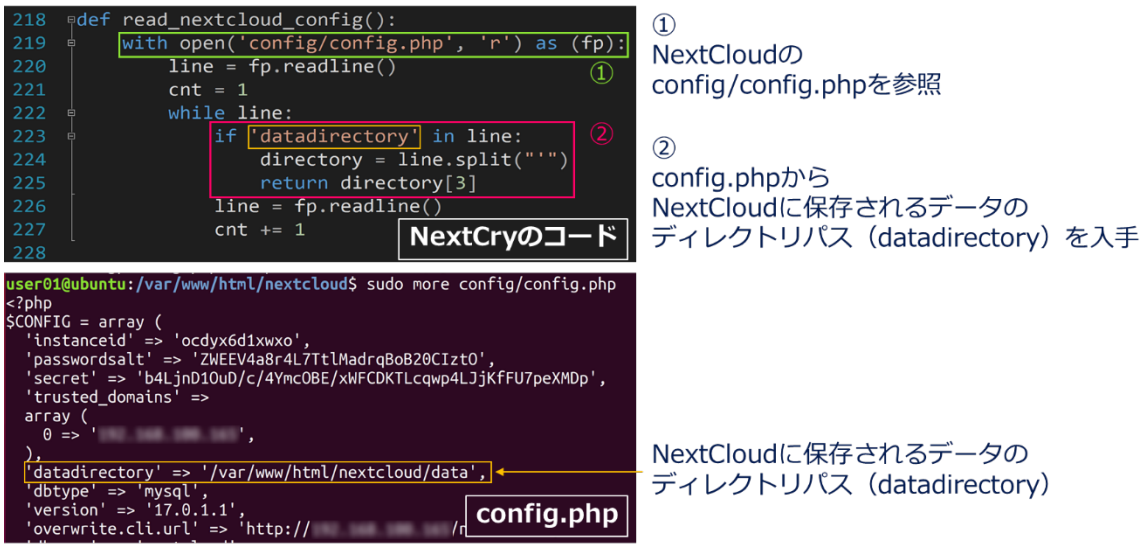
NextCry のファイル形式

本ランサムウェアをデコンパイルすると、Python で記述されたコードを確認することができます。コードの中には、'NEXT-CRY Ransomware'の文字列が記載されています。

```
241 if __name__ == '__main__':
242     print 'NEXT-CRY Ransomware'
243     nextcloud_data_patch = read_nextcloud_config()
244     del_bad_dir(nextcloud_data_patch)
245     nextcloud_data_patch = read_nextcloud_config()
246     files = find_files(nextcloud_data_patch)
247     aeskeys_b64patchs = start_encryption(files)
```

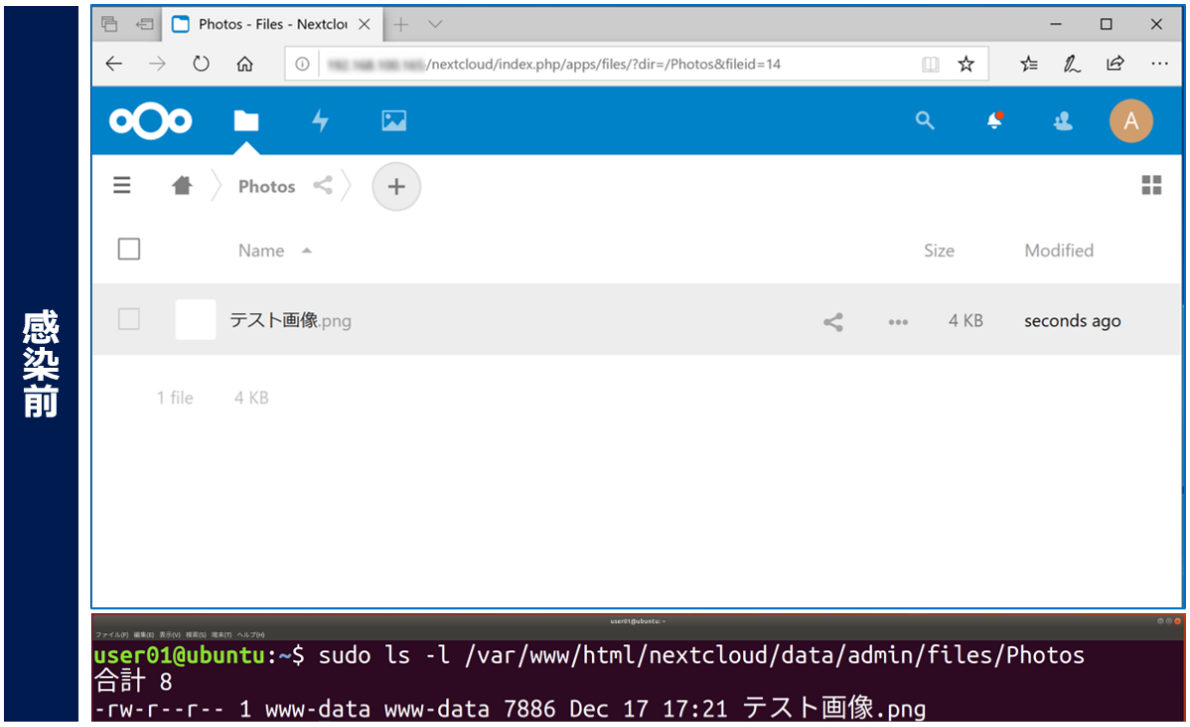
NextCry のコード内容（一部抜粋）

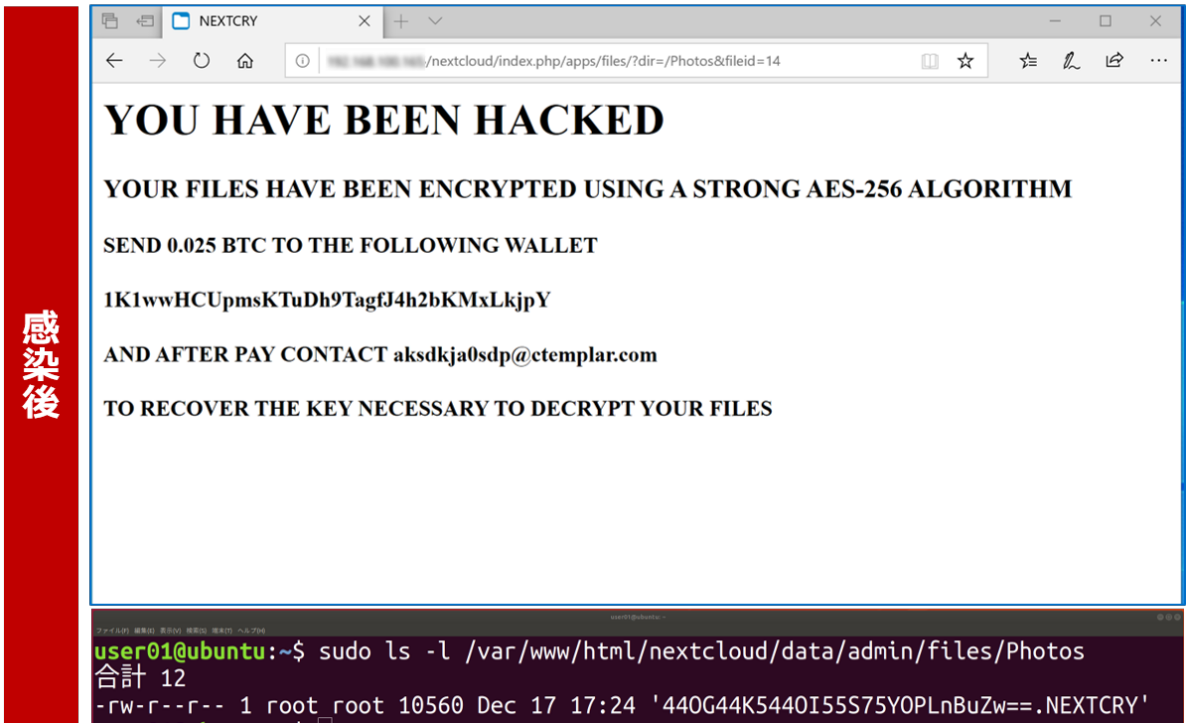
本ランサムウェアが実行された際の主な挙動を以下にまとめます。
まず、NextCloud の設定が記述された config.php を参照し、NextCloud に保存されるデータのディレクトリパスを入手します。



NextCry による主な挙動（暗号化対象の選定）

その後、入手したディレクトリ内のデータを暗号化します。そして、ユーザーが NextCloud の管理画面や操作画面にアクセスすると脅迫文が表示されます。





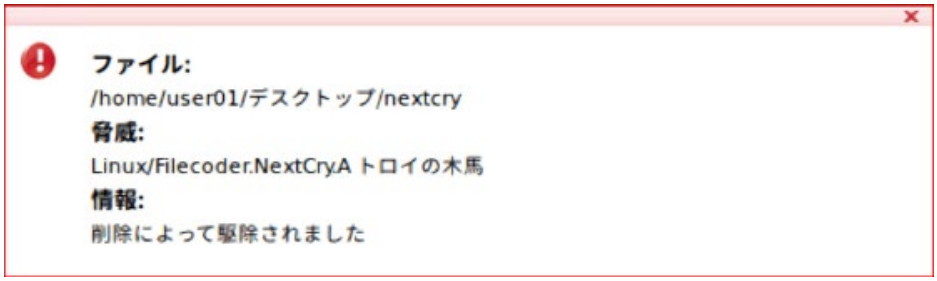
NextCry による主な挙動（ファイルの暗号化と脅迫文の表示）

脅迫文には、AES-256 を用いてデータを暗号化したことと、復号するためには 0.025 ビットコイン（2019 年 12 月現在およそ 20,000 円）を支払い、指定のメールアドレスにその旨を連絡する必要がある、という内容が記載されています。

拡張子を含めたファイル名は、Base64 を用いて符号化され、その後に新たな拡張子「.NEXTCRY」が追加されます。

ファイル名の符号化（検証）

現在、ESET 製品では、本ランサムウェアを Linux/Filecoder.NextCry として検知し、駆除します。



ESET File Security for Linux による検出画面

本ランサムウェアによる事例では、事例発生日の約 10 日前に公開された脆弱性が、侵入経路として用いられました。使用しているソフトウェアの脆弱性が公開された際には、修正パッチを適用する等、即急に対策を行うことが重要です。

ご紹介したように、11 月は Web ブラウザー上で実行される脅威に加えて、ダウンローダーも多く検出されました。また、新種のランサムウェア NextCry が発見されました。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］

- Alert (AA19-339A) Dridex Malware | US-CERT [英語]
  https://www.us-cert.gov/ncas/alerts/aa19-339a

- env_path_info underflow in fpm_main.c can lead to RCE | PHP Bug Tracking System [英語]
  https://bugs.php.net/bug.php?id=78599

- PoC | マルウェア情報局
  https://eset-info.canon-its.jp/malware_info/term/detail/00008.html

- PHP-FPM の脆弱性（CVE-2019-11043）を標的としたアクセス の観測等について | 警察庁 @Police
  https://www.npa.go.jp/cyberpolice/detect/pdf/20191128.pdf

Canon

キヤノンマーケティングジャパン株式会社