ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

●2019年はランサムウェア・仮想通貨採掘・パスワード詐取マルウェアに注意？…Cylanceが脅威レポート発表

https://news.mynavi.jp/article/20190423-813284/
https://scan.netsecurity.ne.jp/article/2019/04/24/42250.html

このニュースをザックリ言うと・・・

- 4月22日（日本時間）、セキュリティベンダーのCylance Japan社より、同社ソリューションによって2018年1月1日～12月31日の間に収集された匿名脅威データを基にした「BlackBerry Cylance 2019年脅威レポート」の日本語版が発表されました。

- 2018年に確認されたマルウェアの総数は前年比で10%増加したとし、攻撃の標的となった業種の上位は、食品業界、ロジスティック業界、非営利団体だったとのことです。

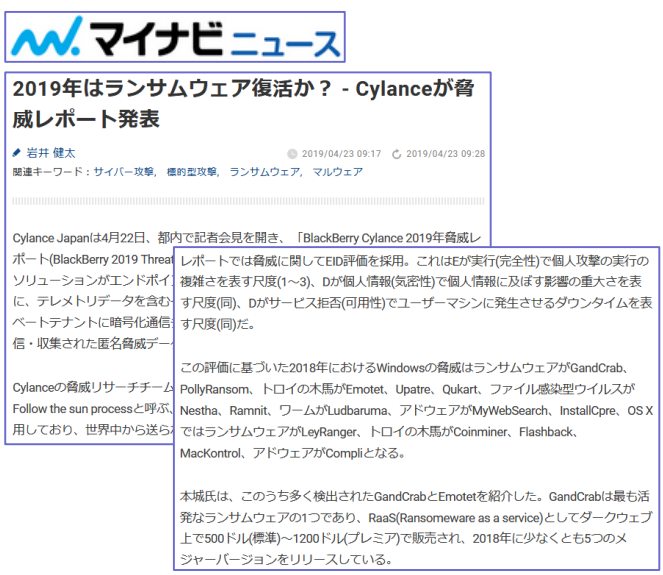
- 発表に伴う同日の記者会見では、ランサムウェアの感染企業数が26%減少、仮想通貨採掘マルウェアの感染企業数は47%増加しているものの、後者の増加は一時的なものであるとして、ランサムウェアの勢いも復活する可能性を示唆しています。

- 記者会見では主なマルウェアとしてランサムウェア「GandCrab」や金融機関を狙いパスワードの詐取を行う「Emotet」等を挙げた上で、今後の傾向として「金銭目的の攻撃は続く」「日本ではEmotet等(のパスワード詐取マルウェア)が出てくる」「仮想通貨のブームが下火となり、採掘マルウェアは逆風となるが盛り返すことに加え、最近ではランサムウェアとの機能が統合されているため、両方ともに増加する可能性がある」としています。

AUS便りからの所感等

- GandCrabは2018年に発生したランサムウェアで、今年1月初頭にはこれへの感染を目的としたメールが日本を中心に約400万通拡散したことにより、トレンドマイクロ社等から注意喚起が出されています（AUS便り 2019/01/15号参照）。

- 昨年よく注目されたとみられるランサムウェアおよび仮想通貨採掘マルウェア、またそれより前から発生していたパスワード詐取マルウェアの脅威は今年も依然続くとみられますが、これらや既知の攻撃のみならず全く新しい攻撃が発生する可能性にも注意を払い、情報収集と啓発を行い、アンチウイルスやUTM等による防御を確実に固めることを常に心がけることが重要です。



●2020年Flashサポート終了に向け２つの動き

https://www.itmedia.co.jp/enterprise/articles/1904/17/news081.html
https://japan.cnet.com/article/35131252/

このニュースをザックリ言うと･･･

- 4月15日（現地時間）、セキュリティベンダーのFireEye社より、不正なFlashファイルを自動的に検出・分析するツール「FLASHMINGO」が発表されました。

- FLASHMINGOはオープンソースとして公開され、個別のアプリケーションとして使うことや、ライブラリとして使うことが可能とされています。

- 一方Webブラウザでは、7月リリース予定の「Chrome 76」および9月リリース予定の「Firefox 69」において、デフォルトでFlashが無効化される予定とされています。


ITmedia エンタープライズ

さよならFlash、去らぬ脅威――FireEyeがFlashマルウェア分析ツールをオープンソース化

「Flashの提供終了後はセキュリティパッチが公開されなくなるため、脅威は増大する」とFireEyeは予想する。

2019年04月17日 12時00分 公開　[鈴木聖子，ITmedia]

印刷　43　Share　B!　18

セキュリティ企業のFireEyeは4月15日、Adobe Flash Player（以下、Flash Player）の脆弱（ぜいじゃく）性を突く不審なファイルを自動的に検出して分析できるツール「FLASHMINGO」を開発し、オープンソースとして公開した。


cnet Japan

9月の「Firefox 69」で「Flash」プラグインをデフォルト無効に

Liam Tung （Special to ZDNet.com） 翻訳校正： 佐藤卓 高橋朋子 （ガリレオ） 2019年01月15日 12時13分

シェア 24　ツイート　B! 2　Pocket 41　印刷　メール　保存　クリップ

「Firefox」ブラウザを開発するMozillaは、2019年にリリース予定の「Firefox 69」で、Adobeの「Flash」プラグインのサポート終了に向けた次の大きなステップを踏み出す。

Mozillaは、以前からバグの多いFlashプラグインのサポート終了を段階的に進めており、Firefox 69はその完了に向けた3つ目のステップとなる。2020年12月31日に提供終了となるFlashは、Firefoxが今もサポートする最後のNPAPIプラグインだ。

AUS便りからの所感等

- Flash Playerは長年脆弱性の温床とされたこともあり、サポートが2020年末をもって終了することが2017年7月に発表されています（AUS便り 2017/07/31号参照）が、依然Flashコンテンツを利用しているサイトは少なくありません。

- FLASHMINGOは大手セキュリティベンダー開発とはいえ、現状での検出精度がどれほどかは未知数ですが、オープンソースであることから、今後の開発や各社アンチウイルス等での採用が進むことに期待したいものです。

- ユーザ側においては、根本的な対策として必ずFlash Playerを最新バージョンに保つこと、さらに不正なFlashコンテンツを遮断できるようアンチウイルスを確実に導入することを心がけるようにしましょう。

●佐川急便や日本郵便をかたるフィッシングサイトに誘導…偽SMSに注意

https://www.post.japanpost.jp/notification/notice/2019/0507_01.html

このニュースをザックリ言うと･･･

- 5月7日（日本時間）に日本郵便より、同8日には日本サイバー犯罪対策センター（JC3）より、スマートフォンのショートメール（SMS）によって偽サイトに誘導するフィッシングについて注意喚起が出されています。

- JC3では以前より佐川急便をかたり不正なAndroidアプリをインストールさせる等のフィッシング（AUS便り 2018/07/30号参照）を確認していましたが、今回調査の過程で、新たに日本郵便をかたるSMSと「jppost-●●●.com」といったドメインのフィッシングサイトを確認したとのことです。

- 日本郵便では現時点でSMSによる不在連絡のお知らせは行っておらず、Webサイト等に掲載するURLにおいても「.com」を使用していないとしています。

AUS便りからの所感等

- 大手運送企業等をかたるフィッシングは以前から存在しており、今回の日本郵便あるいは佐川急便の偽サイトは本物のサイトに良く似せたデザインとなっている模様です。

- 佐川急便でもSMSによる案内は行っていないとし、今まで確認されたフィッシングメールやSMSの情報を随時更新しています。

- 不審なSMSやメールを受信した場合は、こういった情報やTwitter等での報告がないか調査し、JC3も呼び掛けているように「心当たりがないメッセージは開かない」「メッセージに記載されたURLへ安易に接続しない」「信頼できるところからしかアプリはダウンロードしない」「ID・パスワードを入力する際は正規サイトであることを確認する」等に注意し、落ち着いて行動しましょう。


JP POST 日本郵便

ご注意ください

当社の名前を装った迷惑メール及び架空Webサイトにご注意ください。

2019年5月7日

当社を装った迷惑メールおよび架空のWebサイトが発見されました。
このWebサイトにアクセスしますと、お客さまの情報を盗み出そうとしたり、不正なアプリケーションがダウンロードされるおそれがありますのでご注意ください。
なお、当社ではショートメールによるご不在連絡のお知らせは行っておらず、また、Webサイト等に掲載するURLにおいて「.com」を使用しておりません。
このような不審なサイトを発見された場合は、アクセスすることのないよう、ご注意ください。

迷惑メールの文面（例）

お客さま宛にお荷物のお届けにあがりましたが、不在のため持ち帰りました。下記よりご確認ください。
http://jppost-●●●.com