— AUS（アルテミス・ユーザ・サポート）便り 2016/08/08号 —
http://www.artemis-jp.com

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。

●ランサムウェア被害者の6割以上「身代金を支払った」･･･トレンドマイクロ調査

http://www.itmedia.co.jp/enterprise/articles/1608/01/news092.html
http://www.trendmicro.co.jp/jp/about-us/press-releases/articles/20160727064652.html

このニュースをザックリ言うと･･･

- 8月1日（日本時間）、大手セキュリティベンダーのトレンドマイクロ社より、企業・組織のITに関する意思決定者や関与者534人を対象とした「企業におけるランサムウェア実態調査」の結果が発表されました。

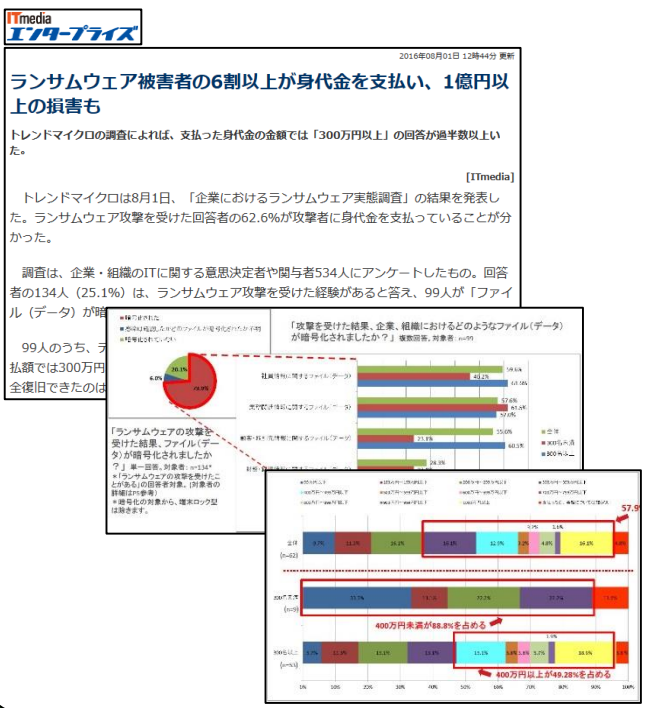
- 回答者の25.1%にあたる134名が「ランサムウェアによる攻撃を受けたことがある」、その中で73.9%にあたる99名が「データが暗号化された」、そしてさらにその中で62.6%となる62名が「実際に身代金を支払った」と回答しています。

- また、「身代金を要求されたら支払う」と回答した241名（全体の45.2%）に対し、さらに「身代金を支払う理由」について質問（複数回答可）したところ、「業務が滞ってしまうから」69.3%、「自社では復旧できないから」61.4%、「PCが利用できなくなるから」41.1%、「支払った方が復旧時間が短縮できると判断するから」8.7%、といった結果が出ています。

AUS便りからの所感等

- 「身代金を支払い実際に復元してもらった」というケースがこれまでもたびたび報告され、そして今回の調査でも多く回答されていることから、身代金の支払われる確率を上げたい攻撃者の思惑としては、比較的実現しているものと見受けられます。

- ベンダーがリリースする復元ツールでデータ復元が可能なケースも少なからずあるとは言え、ランサムウェアへの感染は大抵はデータを破壊され、利用できなくなることであると認識し、アンチウイルス・UTMの活用や適切な手順によるデータのバックアップを含め、普段から「感染しない」「感染しても被害を最低限にとどめる」ための行動をとることが重要です。


ITmedia エンタープライズ

2016年08月01日 12時44分 更新

ランサムウェア被害者の6割以上が身代金を支払い、1億円以上の損害も

トレンドマイクロの調査によれば、支払った身代金の金額では「300万円以上」の回答が過半数以上いた。

[ITmedia]

トレンドマイクロは8月1日、「企業におけるランサムウェア実態調査」の結果を発表した。ランサムウェア攻撃を受けた回答者の62.6%が攻撃者に身代金を支払っていることが分かった。

調査は、企業・組織のITに関する意思決定者や関与者534人にアンケートしたもの。回答者の134人（25.1%）は、ランサムウェア攻撃を受けた経験があると答え、99人が「ファイル（データ）が暗

99人のうち、ラ
払額では300万円
全復旧できたのは

TREND MICRO Securing Your Journey to the Cloud

企業におけるランサムウェア実態調査 2016

～ランサムウェアの被害に遭わないと思う理由、
45.7%が「自社は大企業または有名企業ではないから」と回答～

2016年8月1日

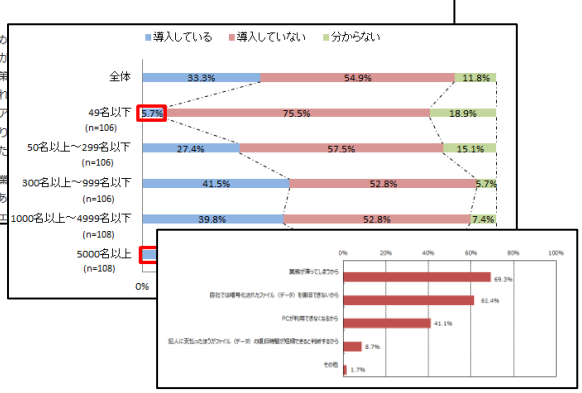
トレンドマイクロ株式会社（本社：東京都渋谷区、代表取締役社長 兼 CEO：エバ・チェン、東証一部：4704、以下、トレンドマイクロ）は、2016年6月に、企業・組織においてITに関する意思決定者および関与者534名を対象に「企業におけるランサムウェア実態調査 2016」を実施しました。本調査の調査結果は以下の通りです。

※調査結果のパーセンテージは、小数点以下第二位を四捨五入した数値です。
※本調査において、ランサムウェアは次のように定義しています。「感染したPCの操作をロックしたり、PC内のファイル（データ）を暗号化して復旧の代わりに金銭を要求する不正プログラム」

1. 34.8%がランサムウェアの被害に遭う可能性が「ない」と回答。半数近くが「自社は大企業または有名企業ではないから」と回答

534名の対象者に「動め
ころ、34.8%の186名
ろ、「セキュリティ対策
という回答が多く見られ
しかし、ランサムウェア
が感染する可能性があり
とが明らかになりました

一方で、勤めている企業
（134名）が「攻撃にあ
算になり、ランサムウェ



●IPA、「夏休みにおける情報セキュリティに関する注意喚起」発表

https://www.ipa.go.jp/security/topics/alert280804.html

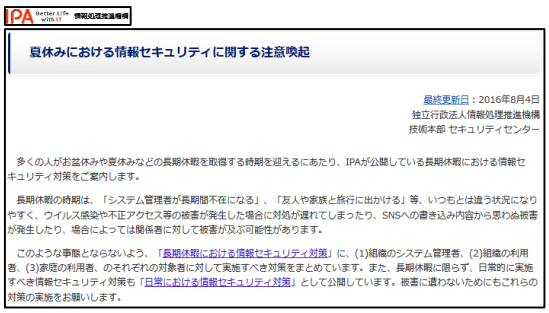
このニュースをザックリ言うと・・・

- 8月4日（日本時間）、情報処理推進機構（IPA）より「夏休みにおける情報セキュリティに関する注意喚起」が発表されました。

- 内容としては、IPAが以前から発表している「長期休暇における情報セキュリティ対策」(①)および「日常における情報セキュリティ対策」(②)の改めての参照を促すことが主となっています。
①https://www.ipa.go.jp/security/measures/vacation.html
②https://www.ipa.go.jp/security/measures/everyday.html

- 特に前者に関連して、「長期休暇の時期は、『システム管理者が長期間不在になる』、『友人や家族と旅行に出かける』等、いつもとは違う状況になりやすく、ウイルス感染や不正アクセス等の被害が発生した場合に対処が遅れてしまったり、SNSへの書き込み内容から思わぬ被害が発生したり、場合によっては関係者に対して被害が及ぶ可能性がある」としており、「組織のシステム管理者」「組織の利用者」「家庭の利用者」それぞれの対象者に対して実施すべき対策がまとめられています。

AUS便りからの所感等


IPA 情報処理推進機構

夏休みにおける情報セキュリティに関する注意喚起

最終更新日：2016年8月4日
独立行政法人情報処理推進機構
技術本部 セキュリティセンター

多くの人がお盆休みや夏休みなどの長期休暇を取得する時期を迎えるにあたり、IPAが公開している長期休暇における情報セキュリティ対策をご案内します。

長期休暇の時期は、「システム管理者が長期間不在になる」、「友人や家族と旅行に出かける」等、いつもとは違う状況になりやすく、ウイルス感染や不正アクセス等の被害が発生した場合に対処が遅れてしまったり、SNSへの書き込み内容から思わぬ被害が発生したり、場合によっては関係者に対して被害が及ぶ可能性があります。

このような事態とならないよう、「長期休暇における情報セキュリティ対策」に、(1)組織のシステム管理者、(2)組織の利用者、(3)家庭の利用者、のそれぞれの対象者に対して実施すべき対策をまとめています。また、長期休暇に限らず、日常的に実施すべき情報セキュリティ対策も「日常における情報セキュリティ対策」として公開しています。被害に遭わないためにもこれらの対策の実施をお願いします。

- 発表において示されている、長期休暇および日常における情報セキュリティ対策はいずれも普遍的な内容であり、直前になって準備を始めるのではなく、普段から文書化や各社員での意識合わせ等をしておくべきものです。

- クライアントPCの各ソフトウェアを最新に保つことは言うまでもありませんが、意識が及びにくい可能性もあるサーバ、さらにはUTMをはじめとするネットワークアプライアンス等においても、ソフトウェア・ファームウェアが古いものから更新されないままになっていないか、適宜確認しておくべきでしょう。

●Apple IDの奪取を狙うSMSフィッシング詐欺が複数発生

http://www.atmarkit.co.jp/ait/articles/1608/03/news084.html

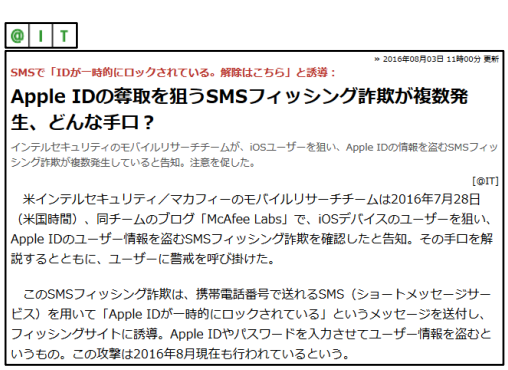
このニュースをザックリ言うと・・・

- 7月28日（米国時間）、大手セキュリティベンダーのマカフィー(インテルセキュリティ)社より、iOSデバイス（iPhone、iPad等）のユーザを狙い、Apple IDのユーザ情報を盗むSMSフィッシング詐欺が確認されたと同社ブログにて注意喚起が出されました。

- SMSメッセージは7月22日と27日に大量送信されたとみられており、「New message」あるいは「Urgent!!(緊急)」というメッセージと短縮URLによるリンクのみが記載され、リンクをクリックすると「Appleアカウントが一時的に停止されているため、Apple社のサイトへ行き“安全に”アカウント情報の再認証を行ってください」という意味の英文メッセージを表示するサイトに誘導され、さらにそこからApple社サイトに偽装した偽のログインフォームに誘導される模様です。

- 同社では、電話番号からのメッセージは基本的に怪しいと判断し、リンクをクリックする前にメッセージやリンクが正当なものであるかを調べることを推奨しています。

AUS便りからの所感等


@IT

※ 2016年08月03日 11時00分 更新

SMSで「IDが一時的にロックされている。解除はこちら」と誘導：

Apple IDの奪取を狙うSMSフィッシング詐欺が複数発生、どんな手口？

インテルセキュリティのモバイルリサーチチームが、iOSユーザーを狙い、Apple IDの情報を盗むSMSフィッシング詐欺が複数発生していると告知。注意を促した。

[@IT]

米インテルセキュリティ／マカフィーのモバイルリサーチチームは2016年7月28日（米国時間）、同チームのブログ「McAfee Labs」で、iOSデバイスのユーザーを狙い、Apple IDのユーザー情報を盗むSMSフィッシング詐欺を確認したと告知。その手口を解説するとともに、ユーザーに警戒を呼び掛けた。

このSMSフィッシング詐欺は、携帯電話番号で送れるSMS（ショートメッセージサービス）を用いて「Apple IDが一時的にロックされている」というメッセージを送付し、フィッシングサイトに誘導。Apple IDやパスワードを入力させてユーザー情報を盗むというもの。この攻撃は2016年8月現在も行われているという。

- 警告記事を見る限り、偽サイトはHTTPSによるものでもなければ、URLを「apple.com」に似せたものでもなく、今回のフィッシング詐欺は技術的には稚拙なものですが、このレベルであってもアカウント情報を奪取される被害はある程度出るものとみられ、サイトやメッセージの内容をより洗練・巧妙化した攻撃も近いうちに現れることでしょう。

- とは言え、警戒すべきことやとるべき対策は電子メールによるフィッシングと殆ど変わらず、前述のような自らの判断のみならず、可能な限りブラウザー・UTM等のアンチフィッシング機能と組み合わせることによる防御が肝要となります。