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。

●Avastが無償で提供するランサムウェア復号ツール、現在全14種に対応

http://www.itmedia.co.jp/pcuser/articles/1702/13/news057.html
https://www.avast.com/ransomware-decryption-tools

このニュースをザックリ言うと・・・

- 2月13日（現地時間）、セキュリティベンダーのAvast社が無償で提供している、ランサムウェアに暗号化されたファイルの復号ツール（以下、復号ツール）について、新たに3種類に対応した復号ツールの提供開始が発表されました。
- 同社の復号ツールは個々のランサムウェアに対して提供されており、今回は「HiddenTear」「Jigsaw」「Stampado」に対応したものが登場しています。
- その他に対応しているランサムウェアは、「Alcatraz Locker」「Apocalypse」「BadBlock」「Bart」「Crypt888」「CrySiS」「Globe」「Legion」「NoobCrypt」「SZFLocker」「TeslaCrypt」となっています。

AUS便りからの所感等

- Avast社はランサムウェアに対する復号ツールを昨年から提供している他、多くのセキュリティベンダーや警察機構等が参加する「No More Ransom」プロジェクトからも無償で復号ツールが提供されています（http://internet.watch.impress.co.jp/docs/news/1035579.html）。
- 一方で、ランサムウェア側でも、現在出ている復号ツールでは対応できないような暗号化を行う亜種が日々大量に発生し、勢いは衰えることを知りません。
- 決して「復号ツールがあるから」と安心することなく、アンチウイルスやUTMの活用はもちろん、確実にデータの保全が行えるような適切なデータバックアップ体制、PC内のOSやアプリケーション等のソフトをすべて最新の状態にしておくことも重要です。

ITmedia PC USER

ニュース　2017年02月13日 12時01分 更新

Avast、14種に対応したランサムウェア復号ツールを無償で提供開始

[井上輝一，ITmedia]

セキュリティソフトベンダーのAvastは2月13日、全14種のランサムウェアに対応した復号ツールを無償提供することを発表した。復号ツールは以前から提供しているもので、今回新たに3種のランサムウェアに対応した。

（ランサムウェア：PC内のファイルを暗号化し、金銭を払わないと復号キーを渡さない、情報を流出させるなど感染者を脅迫するマルウェア）

今回対応したランサムウェアは「HiddenTear」「Jigsaw」「Stampado/PhiladelphiaCrySiS」の3種。この3種は直近数カ月間で攻撃が活発化し被害が拡大している上、暗号化キーと内部アルゴリズムが大きく変わっているという。

INTERNET Watch

「No More Ransom」参加ベンダー4社のランサムウェア復号ツールの無償提供が開始

サイトが5カ国語に対応、新たに30超の組織が参加

岩崎 宰守　2016年12月16日 17:10

ロシアのKasperskyは15日、「No More Ra
としてBitdefender、Emsisoft、Check Point
Microの4社が参加し、これらのベンダーが開発
する復号ツールの提供が開始されたことを発表

No More Ransomは、KasperskyとIntel Securityの2社が、ヨーロッパの警察機構であるユーロポール、オランダ国家警察と共同して立ち上げたウェブサイト。

ランサムウェアによる被害時に、そのランサムウェアが作成されたツールキットを自動検出し、解読キーを提供する7種類10バージョンのツールを提供しており、これまでに約6000人が復号ツールを利用し、サイバー犯罪者に金銭を支払うことなくファイルの復号に成功しているという。

No More Ransomには、現在の14カ国の警察組織に加え、今回、オーストリア、クロアチア、デンマーク、フィンランド、マルタ、ルーマニア、シンガポール、スロベニアの計8カ国の警察機関が参加する。

さらにG DATA Software、ESETなどのセキュリティソフトベンダーや、EU、ルクセンブルク、スロベニア、アイルランドの各CERTなど、30の組織も新たにNo More Ransomへ参加するほか、これまでの英語に加え、オランダ語、ロシア語、フランス語、イタリア語、ポルトガル語のウェブサイトも開設する。

Kaspersky Labのグローバル調査分析チーム（GReAT）セキュリティリサーチャーのジョーント・ファン・デア・ウィール氏は、「ランサムウェアの攻撃を受ける可能性は誰にでもある。弊社の調査データによれば、2016年1月には2分間に1回だった企業への攻撃は、10月には40秒に1回になり、個人に対する攻撃は20秒に1回から10秒に1回へ増加している。これは新しいタイプのランサムウェアの急増と一致している。金銭の支払い以外の選択肢はないと考える人は依然として多いが、支払いを行ったとしても、ファイルを取り戻せないケースは多々ある」と述べている。

●WordPress「最悪級の脆弱性」、サイトの改ざん被害は150万件超に

http://www.itmedia.co.jp/enterprise/articles/1702/13/news045.html

このニュースをザックリ言うと・・・

- 2月9日（現地時間）、WordPress向けセキュリティプラグイン等を提供する米Feedjit社より、2月1日に発表されたWordPress 4.7.0～4.7.1の脆弱性（AUS便り 2017/2/13号参照）を悪用したWebサイトの改ざん状況が発表されました。

- 発表によれば、同社が把握しているだけでも20あまりの攻撃者グループがそれぞれ攻撃を行っており、改ざんされたページ数は150万件を超えているとのことです。

- また、WordPressを狙った改ざん攻撃は2014年半ばから現在までほとんど成功しない状況が続いていましたが、今回の脆弱性の発表により、その成功率が急上昇したとのことで、同社では、「WordPressのアップデートを行わない限り、何度も何度も改ざんされ続ける」と警告しています。

AUS便りからの所感等

- 先週のAUS便りで「最も頻繁に活動しているとみられる」としていた攻撃者グループ（被害件数151,000件）をさらに凌ぐ2つのグループが存在し、それらによる被害はそれぞれ397,000件と242,000件、合わせて639,000件にも上っています。

- 一部先週の繰り返しとなりますが、とにかく今回の脆弱性への対策としてはWordPressを4.7.2にアップデートすること、併せてWordPress向けセキュリティプラグインやWAF等の導入により、さらに防御を固めること、加えて利用しているソフトウェアに関するセキュリティ情報を随時確認し、素早く対応できる体制を整えることが重要です。

●「わたしは○○人からブロックされています…」Twitter偽アプリによるスパム拡散に注意

https://togetter.com/li/1078670

このニュースをザックリ言うと・・・

- 2月6日（日本時間）、Twitterガイドサイト「ツイナビ」より、悪意のあるTwitterアプリによる「わたしは○○人からブロックされています…」というスパムツイートの拡散に対する警告が出されています。

- ツイートにあるサイトにアクセスすると、「自分が何人のユーザからブロックされているか」を教えるとしてアプリ連携を要求し、実際には「わたしは25人からブロックされています」のような一定の数字を示す定型文からなるツイートを投稿するものとなっています。

- Twitter上では、このような不審なアプリと連携した場合は、速やかに解除するよう呼びかけられています。

AUS便りからの所感等

- Twitterにて「自分が誰をブロックしているか」は設定ページから確認できますが、「誰からブロックされているか」等は直接確認できない仕様となっており、また「何人からブロックされているか」を確認できるアプリは実際に存在しますが、これはアプリと連携した各ユーザがブロックしているユーザの情報を提供することで成り立っています。

- アプリとの連携は、ユーザ自身が持つ、ツイートやDMの送信（あるいは自分が投稿したツイート、送受信したDMを見る）権限をアプリに許可することを意味し、そして、そのためのTwitterへのアクセスは必ずしもユーザ自身のPCやスマホ等から発生するものとは限らないため、UTM等での通信の遮断による防御も困難です。

- アプリとの連携の際は、必ずユーザに対して連携を行うか否か、あるいはアプリがどういった権限を要求するか尋ねられますので、Twitterやその他の情報源を検索した上で信用できるアプリか判断すること、そして、連携するアプリを必要最小限に留めることが肝要です。