もしもの時にどうすればよい？

ランサムウェアの対策と感染時に行うべきこと

2017/08/08

感染するとパソコンやスマホをロックして金銭を脅し取ろうとする身代金要求型ウイルス「ランサムウェア」の脅威が深刻です。ランサムウェアの侵入手口を知って有効な対策を行ないましょう。万一、ランサムウェアに感染したときに行うべきことも紹介します。

ランサムウェアは Web サイトとメール経由でやってくる

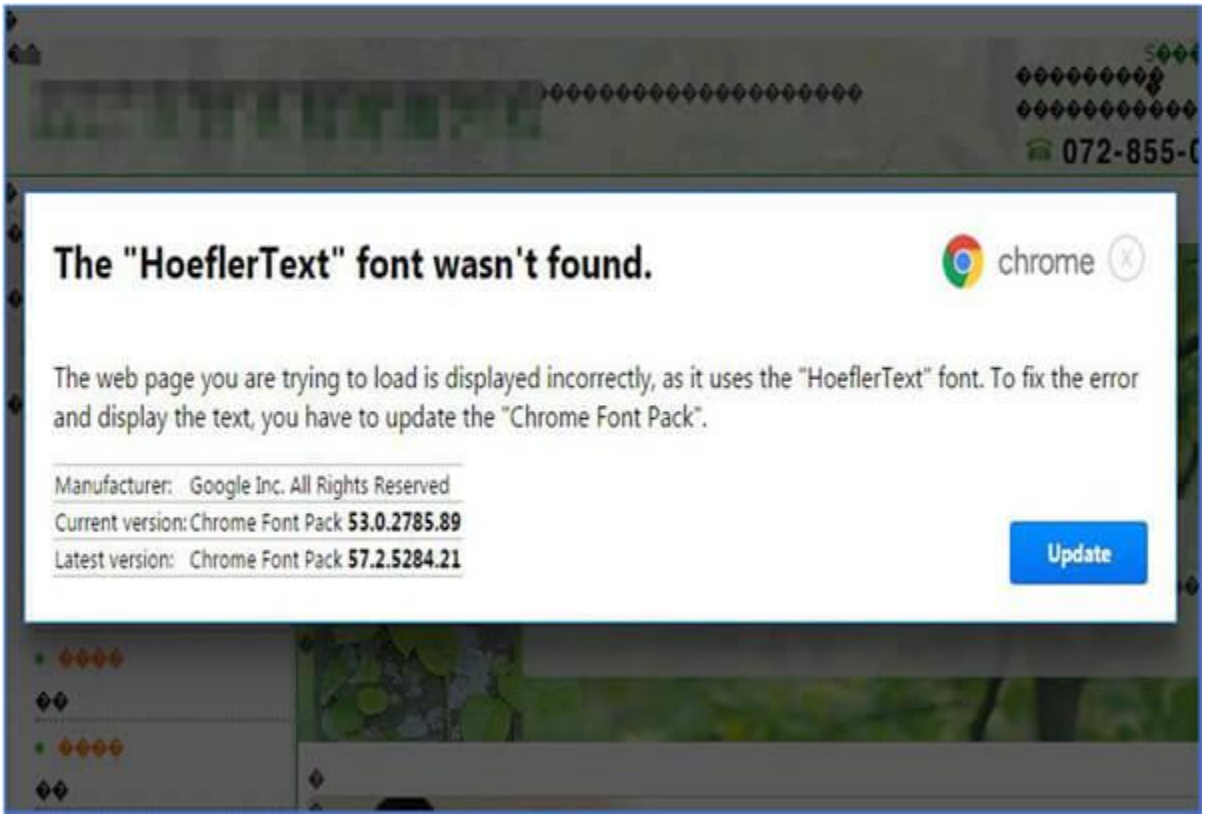
2017 年 5 月中旬、WannaCry とよばれる身代金要求型ウイルス（ランサムウェア）による世界規模の被害が大きな騒ぎになりました。ランサムウェアは、端末本体をロックして操作不能にしたり、端

末内の写真や文書を暗号化して読み込めなくしたりして、元に戻す条件として金銭（身代金）を要求するウイルスです。病院で急患対応や手術が行なえなかったり、工場が操業停止に追い込まれたりといった被害も報道されています。

ランサムウェアの侵入手口は大きく Web とメールの 2 つですが、2017 年に入ってからは Web サイト経由での侵入が目立っています。代表的な手口が、OS やソフトの脆弱性（セキュリティ上の弱点）を攻撃して、端末利用者が気づかないうちにウイルスを送り込む手法です。OS やソフトにセキュリティ更新プログラムが適用されておらず、脆弱性を残したままのパソコンでは、攻撃者が仕掛けを施した Web サイト（正規の Web サイトに攻撃者が侵入し勝手に書き換えている場合もあります）を見ただけでランサムウェアに感染してしまうことがあるのです。

見ただけで感染する不正広告の脅威【トレンドマイクロ公式 YouTube】

さらに、最近では脆弱性攻撃に加え、ユーザの油断を誘ってランサムウェアをインストールさせる手口を併用するものも出現しています。例えば、Google Chrome からアクセスした場合には「フォントがインストールされていないため文字化けしている」という趣旨のメッセージを表示し、フォントをインストールするように見せかけて代わりにランサムウェアをインストールさせる手口がありました。



図：フォントファイルのインストールに見せかけ

ランサムウェアをダウンロードさせようとする画面の例

一方、メールを使った攻撃では、メール本文のリンクをクリックさせたり、添付ファイルを開かせたりすることでランサムウェアに感染させる手口が定番です。「請求書」や「不在通知」に見せかけたメールで添付されたファイルを開かせる手口には注意が必要です。文書ファイルを開くつもりが、端末にランサムウェアを感染させてしまう恐れがあります。

図：国内でランサムウェアの拡散に用いられた迷惑メールの例

ランサムウェアの被害を防ぐために必須の対策

こまめにバックアップする

一度、ランサムウェアによって暗号化されたファイルを元に戻すことはかなり困難です。クラウドや外付けハードディスクなどの複数の場所に重要なファイルのコピーを常に予備として保管しておきましょう。

OS やソフトの脆弱性を修正する

パソコンの OS やソフトの脆弱性を残していると、脆弱性攻撃を受けてランサムウェアに感染してしまう可能性があります。Windows Update などのソフトウェアの自動更新を有効にするなど、OS やソフトの開発元から更新プログラムが提供されたら速やかに適用し、脆弱性を修正してください。

パソコン内のソフトのバージョンが最新かどうかわからない方は、IPA が無償で公開する「MyJVN バージョンチェッカ」を使って確認することもできます。

My JVN バージョンチェッカ　｜IPA

http://jvndb.jvn.jp/apis/myjvn/vccheck.html

（※クリックすると IPA のサイトに移動します。）

メールのリンクや添付ファイルを安易に開かない

メールによるウイルス拡散攻撃では、不特定多数にメールを送りつけ、本文内のリンクをクリックさせたり、添付ファイルを開かせたりしようとします。実在する企業を名乗るメールなど、一見それらしいものでも本当に自分に心当たりがあるかを振り返ったり、その企業のホームページを参照して注意喚起情報をチェックしたり、ホームページ上の問い合わせ先に電話したりして慎重に内容の事実確認をしましょう。

セキュリティソフトを最新の状態で利用する

セキュリティソフトを利用すれば、自身で気づくことが難しいメールに添付された不正サイトへのリンクや不正なファイルを検知して感染をブロックしてくれます。新たな脅威に対抗するため、セキュリティソフトは、最新の状態に更新して利用しましょう。ランサムウェア対策強化機能を搭載したセキュリティソフトもあるため、ソフト購入時にはこれらの機能があるかも確認してみましょう。

もしもランサムウェアに感染したときには？

ランサムウェアに感染させるだましの手口は巧妙です。ランサムウェアに感染して端末本体や端末内のデータを人質にとられてしまったときの対処法を紹介します。

金銭を支払わない

ランサムウェアに感染して金銭を要求されても決して言いなりになってはいけません。支払ったところで犯罪者が暗号化したファイルを確実に元に戻してくれる保証はない上、ランサムウェアの拡散にうまみを感じたサイバー犯罪者の攻撃を助長してしまうことにもなります。

ネットワークから感染端末を外す

自宅のネットワークでほかの端末とファイル共有などをしている場合には、他の端末が感染したり暗号化されるデータが増えてしまったりするリスクがあります。気付いたタイミングによっては被害を抑えることもできるので、有線であれば LAN ケーブルを外す、無線の場合は Wi-Fi をオフにし、感染した端末をネットワークから外しましょう。

復旧ツールを試し、駆除する

ランサムウェアにより端末内の写真や動画、文書を暗号化され、読み込めなくなった場合、トレンドマイクロが無償で提供する「ランサムウェアファイル復号ツール」などのセキュリティベンダ提供の復旧ツールを試してみましょう。一部のランサムウェアで暗号化されてしまったファイルを復号できる可能性があります。

※暗号化されたすべてのファイルの復号を保証するものではありません。

ランサムウェア　ファイル復号ツール　|　トレンドマイクロ

https://esupport.trendmicro.com/support/vb/solution/ja-jp/1114210.aspx

（※クリックするとトレンドマイクロのサポートページに移動します。）

利用中のセキュリティソフトのサポート窓口に連絡する

上記の対処策と並行して、ランサムウェアの感染が疑われる場合には、まずはご利用のセキュリティソフトを提供する企業のサポート窓口に問い合わせることをおすすめします。あるいは、契約中のインターネットプロバイダやパソコンを購入した量販店のサポート窓口に相談することも有効です。

ウイルスバスターウイルスバスター ヘルプとサポート｜トレンドマイクロ

https://esupport.trendmicro.com/ja-jp/consumer/support/vb/home.aspx

（※クリックするとトレンドマイクロのサポートページに移動します。）