M's PRESS 015

エムズ・システムサービス 情報誌
2023 年 11 月 発行

コンピュータウィルスは中小企業もターゲット！

昨年末に大流行した「Emotet（エモテット）」や「ランサムウェア」。テレビやネットでも大騒ぎだったので、知っている方も多いのではないでしょうか。中小企業はもちろん、個人のパソコンまでもウィルスのターゲットになっており、エモテットとランサムウェアは、それぞれ違う特性を持ち、非常に悪質な症状をもたらします。

エモテット

1 取引先、知り合いから送られたメールに偽装する。メール本文はもちろん、件名も過去の送受信メールから分析され、あたかも本人から送られたメールのように偽装されているのが特徴です。

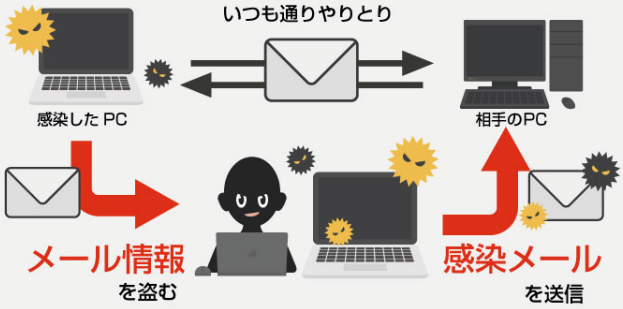
2 送られてきたメールに添付されたファイルを間違ってクリックすると、その時点でパソコンがウィルスに感染。
この時、パソコンには見た目では何も症状が現れず、感染した事に気づけない事がほとんどです。

3 感染したパソコンの内部データは、専用のサーバへ自動的に送付されます。この時にメールデータもすべて取集されることで、取引先のアドレスや、メールの内容もすべて悪質なサーバに回収されてしまいます。
同時に、社内 LAN 内に設置されているパソコンすべてにウィルスを送付・感染させます。

4 サーバに回収されたメールアドレス一覧に対して、エモテットは偽装メールをさらに送付します。感染が一瞬で拡大してしまうのはこの為です。

5 もし、ウィルス感染に気が付いてパソコン側のウィルス除去を行ったとしてもサーバに回収されたデータを消去する事は出来ません。このため、全ての取引先に対してエモテットウィルス感染のメールを送付し続けることになります。

6 悪質なサーバから感染したパソコンに対して、新たに別の種類のコンピュータウィルスを送り込みます。この時、初めてパソコンに大きな症状が現れます。



ランサムウェア

1 外部からのアタックや悪質な WEB サイトの閲覧、ウィルス感染したメールやファイルの共有などによって感染します。

2 感染したパソコンは、ある日突然ロックされ、「お金（仮想通貨）を支払ってくれれば、ロックを解除します」という画面が表示され、何もできなくなります。

3 HDD は特殊な構造に暗号化され、パソコン本体を分解してデータを抜き出したとしても復旧は出来ません。

4 お金(暗号資産)を支払ったとしてもロックが解除される保証は無く、またデータも流出してしまいます。

5 ターゲットはパソコンだけでなく、データサーバなども感染する恐れがあります。

ランサムウェア（ワナクライ）の身代金要求画面

ウィルスに感染したら

ウィルスに感染する事で業務がストップし、担当者の方は非常に困惑するかと思います。
まずは落ち着いて、次の対応を行ってください。

1. パソコンをインターネットから切り離す

まずは、ウィルス感染を防ぐためにネットからパソコンを遮断してください。
- Wi-Fi のスイッチを切る
- LAN ケーブルを抜く

2. 可能であれば、パソコン画面の写真を撮る

スマートフォンやデジカメ等で、症状が分かる画面上の写真を撮ってください。この時、パソコン本体のスクリーンショット機能は使用しないように！

3. パソコンの電源を切る

一般的には電源ボタンの長押しでパソコン電源を切ることが出来ます。これにより、ウィルスの感染拡大を防ぐことが出来ます。
もし、上記①②が出来なければ、すぐに電源を切っても大丈夫です。
この作業は、早ければ早いほど感染を防ぐ可能性が上がります。

4. 専門業者に連絡する

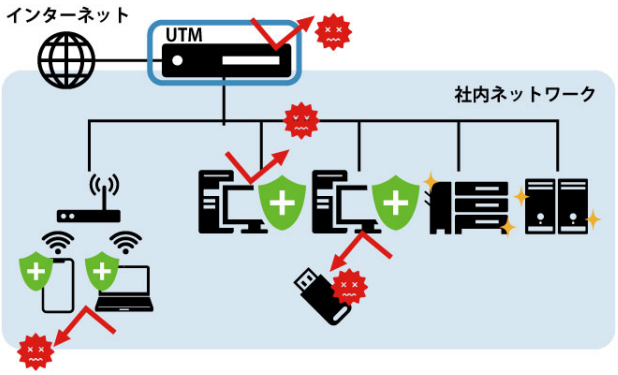
パソコン専門業者に連絡し、対応をお願いしてください。
エムズ・システムサービスでも症状の確認・対応が可能です。
お気軽にお申し付け下さい。

どうやったら感染を防ぐことが出来るのか…裏面へ

ウィルス感染の防御は、大きく２種類

1 パソコンに対して対策する「セキュリティソフト」

セキュリティソフトは、インストールされたパソコン対してのみ機能します。主な機能は、「ウィルスの検知・駆除」です。パソコンにアクセスしたファイルに対してスキャンをかけ、ウィルスに感染している事が分かり次第、除去します。
人間で例えると、マスクをつける・手洗いうがい・薬を飲む　という事になります。



2 ネットワークに対して対策する「UTM」等

UTM は、インターネットの入り口に設置する機械です。
一般的には「ルーター」といったものがインターネットの入り口として機能しており、ルータ１つで社内や家庭のインターネットを全て行っています。
このルータのすぐ後ろに UTM を設置する事で、インターネット経由のデータをチェックし、ウィルスに感染されたデータが発見された場合に除去します。
又、外部からのアタックに対してもブロックを行う事が出来ます。
例えるなら、病院の隔離病棟やエアーシャワーのようなものです。

上記のような対策を行っても、残念ながら
100% 感染を防ぐことは不可能です。
インターネットが身近になった今、まずはできる
対策から実施してください。

機器のバージョンアップが必要かもしれません

インターネット機器は、バグや不具合を直す為のバージョンアップファイルが定期的に発表されています。
特にNWカメラ・録画機は、バージョンの古い新しいなどの組み合わせによって、不具合が出る事があります。
エムズにて機器を導入頂いている機器は、弊社にて無償で点検をさせて頂きますので、ご希望の方は一度弊社までご連絡下さいませ。

11月でGROWとアオイベースは
２周年
になりました！
2nd ANNIVERSARY

インスタグラム
@karasuma_grow2021

TikTok
@grow_karasuma

編集後記

今年でエムズも 13 期目に突入しました。干支でいえばちょうど２週目に入ります。
これをきっかけに、皆様により一層ご期待に添えるようなサービスを展開するため、社内の部署体制を大きく変更する事になりました。私自身もより一層身が引き締まる思いでおりますので、引き続きどうぞよろしくお願いいたします。

株式会社 エムズ・システムサービス
☎0120-377-167
http://www.ms-sys.co.jp

本　社
〒525-0071 滋賀県草津市南笠東1丁目14-36 エムズスクエア 1F-A
TEL:077-563-2377 / FAX:077-563-2388

彦根営業所
〒525-0081 滋賀県彦根市京町1丁目3-15 SUN VALLEY 彦根
TEL:0749-49-2388 / FAX:0749-49-2399

京都営業所
〒600-8216 京都市下京区西洞院通木津屋橋上ル東塩小路町 607 辰巳ビル 5F
TEL 075-353-1670 / FAX 075-353-1680

AOIBASE KARASUMA
〒600-8082 京都市下京区高倉通四条下る高材木町 225-1 Metro Miru Building 5F
TEL:075-353-0006 FAX:075-353-0006

バックナンバーはこちらをチェック！