サイバーセキュリティ通信 Vol.13

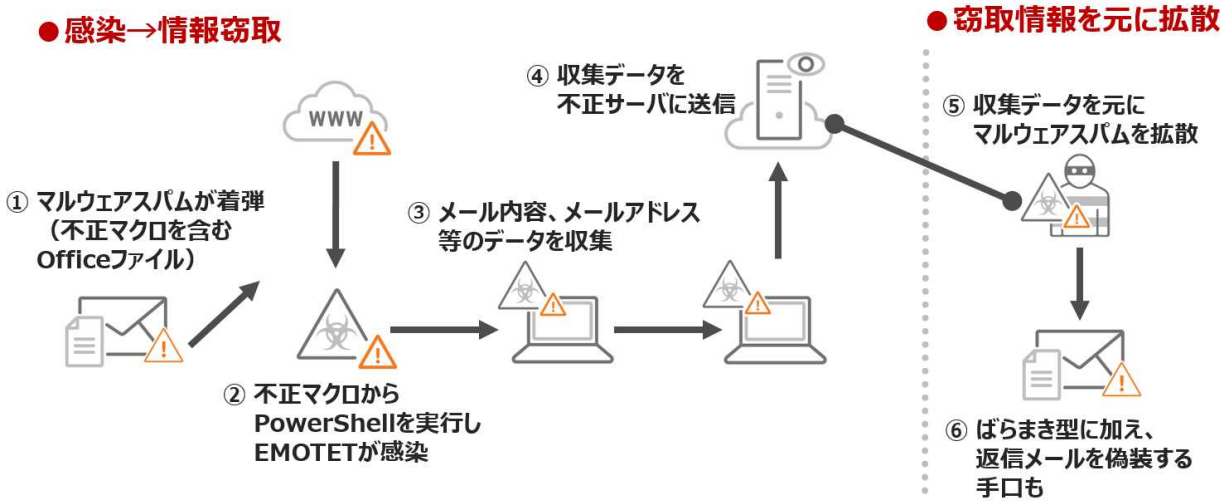
令和２年10月
【長崎県サイバーセキュリティに関する相互協力協定機関】

サイバァちゃん

Ｅｍｏｔｅｔ検出数が過去最大規模に！

トレンドマイクロ社によると、マルウェア（悪意のあるソフトウェア）のＥｍｏｔｅｔ（エモテット）に感染した端末が国内で爆発的に増加しているとのことで、今年８月と比較すると、９月に検出した感染台数は約８倍、検出数は過去最大規模になったことが分かりました。

Ｅｍｏｔｅｔとは？
　メール経由で拡散するマルウェアで、Microsoft Officeファイルに含まれる不正なマクロを実行すると感染します。不正なマクロを実行したパソコンは、Windowsの標準コマンドラインツールであるPower Shellを起動し、Power Shellのコマンドでマルウェア本体をダウンロードして実行します。



＜Ｅｍｏｔｅｔに感染する流れ（トレンドマイクロ株式会社ホームページより引用）＞

＜感染を防ぐために＞

Emotetの感染を防ぐには、Officeソフトウェアの設定を「マクロを無効にする」、「マクロを実行しない」にすることが有効です。

初期設定ではマクロは無効になっていますが、マクロを含むOfficeファイルを開くと、メッセージバーに「コンテンツの有効化」ボタンが表示されます。ボタンを押してしまうと、マクロが有効になってしまい、感染リスクが高まります。

よって、どうしてもマクロを含むファイルをやり取りする場合は、事前に知らせてもらうなどの対策が必要です。

また、Power Shellを使わない環境であれば、Power Shellを無効にしておくことも有効です

長崎県警察本部サイバー犯罪対策課
095-820-0110（3451・3452）
ﾒｰﾙｱﾄﾞﾚｽ e103108@police.pref.nagasaki.jp

サイバー犯罪対策課　LINE ID：@387ojopi
公式LINEアカウントで
情報配信中！
友だち登録お願いします！