５月１３日１１時４５分くらいからプロバイザーのメールの隔離や注意が喚起されておりました。不明なメールが来たり、自動的に送ったり困惑しておりましたが、Emotet ではないかとのことでしたので、ネットで検索するとかなりの被害が出ている様子でした。チェックの方法があると出ていたので、これも疑いながら覚悟してやってみました。

結果は陽性でした。ユーザーホルダーの中にファイルが入っています。削除してみても使用中で削除できません。

仕方なくハードディスクを取り換えて、時間をおいて１０時３０分に PC を起動しました。

ディスクのチェックが陰性であることを確認し本件の報告を作成しました。

ことのはじめは、事務的な事案に関する zip ファイルが受信され、これを解凍したのでここで感染したと思われます。

おかしいと思ったのは、通信相手の欄がアドレス帳に記録しているスペルではなかったこと、ファイルとパスワードを一緒に添付されていること、通常は別々に来ますよね。

丁度２件とも懸案作業中でしたので、プロバイザーの警告も気が付かずに、つい手を出してしまい後悔しておりますが後の祭りでした。

皆さん方に迷惑をおかけしましたことに深くお詫びします。

Emotet チェック方法について

Emotet(エモテット)感染を疑ったら － 警視庁から

https://github.com/JPCERTCC/EmoCheck/release

ダウンロードしたらフォルダの中の.EXE を実行するとそのままチェックに入ります。

しばらくすると、結果が表示されます。ファイルはダウンロードされます。

以上対策はしましたが、５月１４日１０時３０分以降もメールが届くようでしたらお知らせください。(Ja6hug0604@vir.bbiq.jp)

--