サイバーセキュリティ通信 Vol.7

令和２年７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

マルウェア「Emotet」に要注意！

昨年度大流行したマルウェア「Emotet」が、復活の兆しを見せています。
実在の組織や人物になりすましたメールなどにより拡散しているマルウェア「Emotet」。メールには、不正なOffice文書ファイルが添付されており、ファイルを開くと、マクロの有効化を促す内容が表示されます。マクロを有効化すると、Emotetの感染につながります。添付ファイルの代わりに、Office文書をダウンロードするリンクが添付されていることもあります。

○　被害に遭わないために知っておきたいポイント

- □　疑わしいメールを受け取った場合、**ファイルやリンクは開かず**、組織のセキュリティ担当者に相談しましょう
- □　ファイルを開いてしまっても、**マクロを有効にせず**、そのままファイルを閉じて組織の担当者の指示に従いましょう

「Emotet」とは、感染した端末から情報を盗み出したり、感染を広げるためのスパムメールを送信したりするマルウェアだよ。
今年の２月以降静かだったけど、７月に入って活動再開したらしいよ。

「Windows Server」のDNS機能に脆弱性

今年７月、マイクロソフト社は、Windows DNSサーバーにおける重大な脆弱性情報（CVE-2020-1350）があるとして、修正プログラムを提供しています。
DNSサーバーの機能を有効にすると影響を受ける脆弱性で、外部からサーバーを乗っ取られるおそれがあります。７月時点で、サーバーを乗っ取るまでには至りませんが、サービス停止（DoS）状態に陥らせる実証コードが出回っているとのことです。
今後、脆弱性を悪用するウイルスが出回るおそれがありますので、注意してください。

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