5分でわかるシリーズ

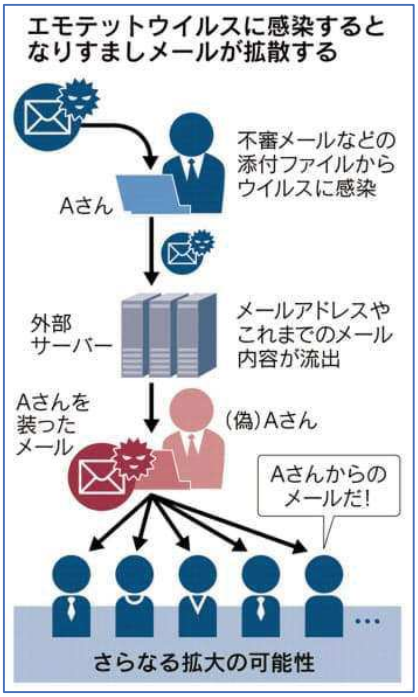
なりすましメール拡散ウイルス国内本格上陸 マルウェア「Emotet（エモテット）」について

RICOH imagine. change.

欧米で流行しているコンピューターウイルス「Emotet（エモテット）」が日本に本格上陸し、被害が拡大しています。
感染すると**メールアドレスや本文を盗まれ、本人になりすましたメールが次々と関係者に送られる被害が多数報告されています。**
少なくとも400以上の団体・企業で被害が出ているとされ、民間団体などが注意を呼びかけています。

○「Emotet（エモテット）」はどんなマルウェア？

2014年にバンキングマルウェアとして確認されたマルウェア「Emotet」がボットネットとして進化し、2018年以降、世界中で猛威を振るっています。
感染したコンピューター内で所有者に気付かれることなく、様々な悪質なタスクを実行しています。**日本でも感染被害が増加**しております。



日本経済新聞　2019/11/29

【これまでのマルウェアとEmotetとの違いの特長】
実在の組織や人物になりすましたメールに添付されたファイルから**感染メールそのものが盗まれる**点

<侵入経路>
ほとんどがメール経由
（細工された**Wordファイル**によってEmotetに感染するケースが多い）

<感染により発生する被害>
- **取引先や顧客の連絡先とメールの内容が窃取され外部に送信される**
- **（取引先以外の）外部の組織に大量の不審メールを送信してしまう**
- **他のマルウエアがダウンロードされ感染する恐れ**
- **感染した端末内の資格情報やシステム上の脆弱点を利用した、ネットワーク内の別の端末への感染拡大**

<感染被害が拡大している理由>
- コマンドプロンプトやPowerShellなど正規のプロセスを悪用しているため検出が困難
- 自身が頻繁に更新されるため、シグネチャによる検出が難しい。
- 本体に悪意のあるコードをできるだけ持たず、シグネチャによる検出が難しい。
- 解析環境であることを確認すると活動しないため、サンドボックスによる検出や、マルウェアの解析が難しい（シグネチャの作成が難しい）。

エモテットの感染被害

首都大学東京 (11/1)	教員が受信したメールの添付ファイルを開封しＰＣが感染。相次いで教職員などへ不審メールが届いた。
双葉電子工業 (11/8)	フィリピン子会社のＰＣがウイルスに感染。子会社の従業員とメールでやりとりした一部のアドレスが盗まれた。
京都市観光協会 (11/25)	同協会の職員のＰＣがウイルスに感染。職員を装ったメールが相次いで送信された。

(注)日付はウイルスへの感染を発表した日

日本経済新聞　2019/11/29