サイバー攻撃の未然防止のために

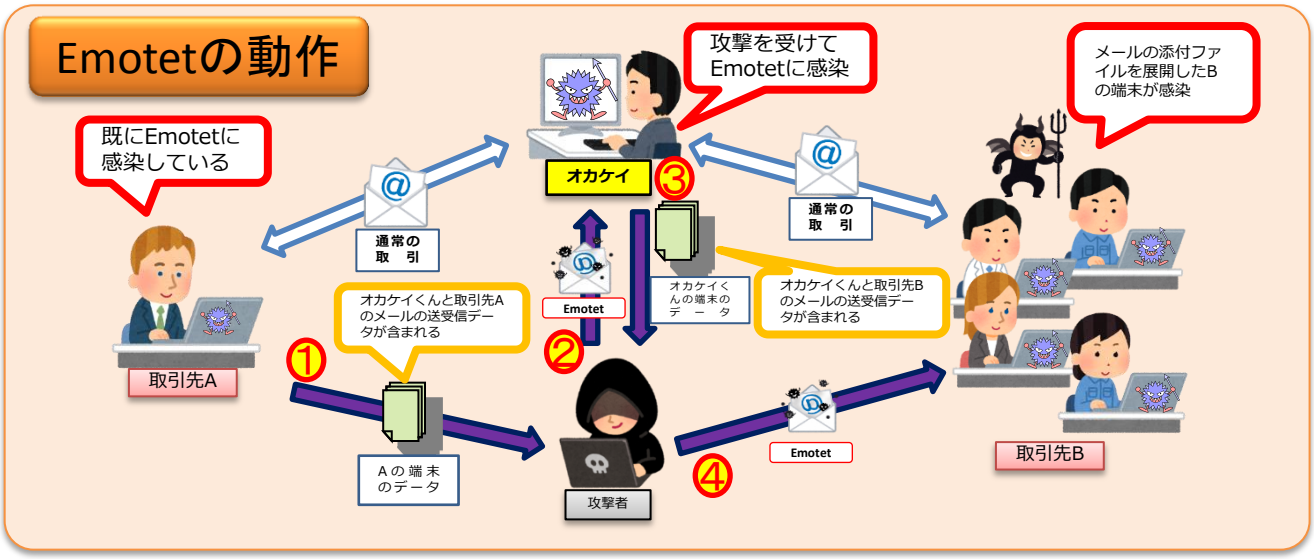
POLICEファイアウォール

2号
2022年

取引先からのメールだと思って、添付ファイルをクリックしてみたら、会社のパソコンが今流行のマルウェア「Emotet」に感染してしまった件。

ミスターB

今回も前回と同様にマルウェア**「Emotet」**をテーマにしました。
トレンドマイクロ社のブログによると、本年２月末現在で感染拡大を継続しており検出件数が過去のピーク時（2020年10月前後）に迫る状況まできているとのことです。
今回は、下の図で**オカケイくん**が取引先からのメールでEmotetに感染したという設定でEmotetの挙動を確認してみたいと思います。
「敵（彼）を知り己を知れば百戦危うからず」と故事にあるように、Emotetの動きからその怖さを知り、併せて自社のセキュリティを確認することでEmotetを見破る強さを身につけましょう。



★★ミスターHの解説★★

上のEmotetの動作について解説をします。
まず今回、Emotetに感染したオカケイくんは、Ａ社、Ｂ社と取引があり、取引先のＡ社は既にEmotetに感染しているという設定です。
①の矢印は、攻撃者が既に感染している取引先ＡからＡの端末のデータを盗んでいます。
このデータの中に、Ａとオカケイ君のメールの送受信データが含まれています。
②の矢印は、攻撃者がＡを装いオカケイくんにEmotet付きのメールを送っています。
③の矢印は、Emotetに感染したオカケイくんの端末からデータが盗まれています。
このデータに、オカケイくんと取引先Bのメールの送受信データが含まれています。
④の矢印は、攻撃者がオカケイくんを装いBにEmotet付きのメールを送っています。
このメールによって、Bがエモテットに感染すると、同じ要領で社内外へ次々と感染を拡大していきます。
これは、あくまで一例ですが、Emotetはこのようにして実際に取引のある事業者を装うことで、受信者の警戒心を解かせ、添付ファイル（Emotet）を開かせます。
そして、感染した端末を通じて外部と交信し、ランサムウェアなどの別のマルウェアを呼び込んで、被害を大きくしていくのです。

質疑などがございましたら、岡山県警察本部警備部公安課サイバー攻撃対策係（086-234-0110 内線5576）までご連絡ください。