回　覧　印　印　印　印　印　印　印　印　印　印　印　印

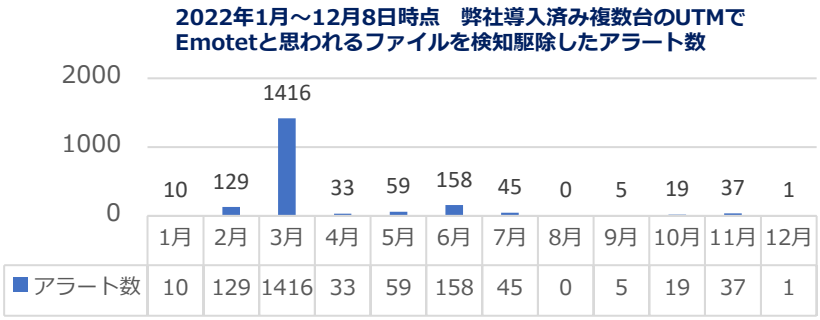
ASAMA Security Newsletter Vol.91

あさまセキュリティニュースレター

2022年　２大セキュリティ脅威のまとめ

（2022年12月8日）

◆Emotet（取引先を装い、メールの添付ファイルを開かせ情報搾取）



Emotetは2022年も1月から検知、2月に急増、**3月に爆発的に検知**。
現在も検知が続いています

ファイル名は、**Report**や**日付**のエクセル形式で送られてくるケースが多く、差出人や本文は取引先を装うケースも
（Emotet感染させて、盗んだ情報を悪用）

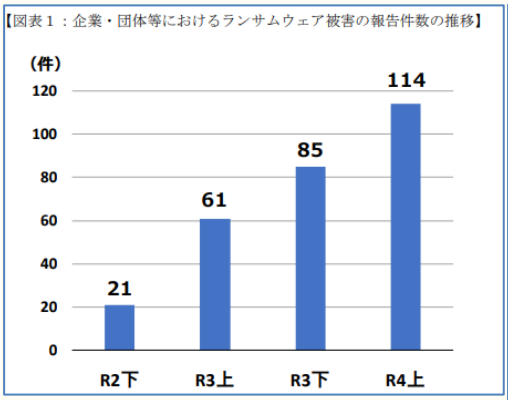
filename: [redacted] report.xls
virus: XLM.Trojan.Abracadabra.8.Gen

↑ **12月検知のファイル名もxx-0000 report.xls といったエクセルファイルです**

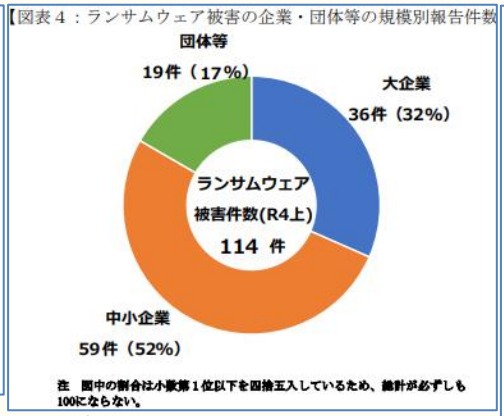
Emotetは、主にメールの添付ファイルを開くことで感染、パソコン内の様々な情報を搾取し悪用します
取引先へ勝手にメールを送り、受け取った側は知っている人のメールのため開いてしまい感染と増え続けます。
搾取したデータや感染させたPCをもとにさらなる攻撃を仕掛けます。
不審な添付ファイルを開いたら、速やかに社内で情報共有とEmocheckで検査を！

◆ランサムウェア（感染すると社内のファイルを勝手に暗号化、暗号化解除に身代金を要求）

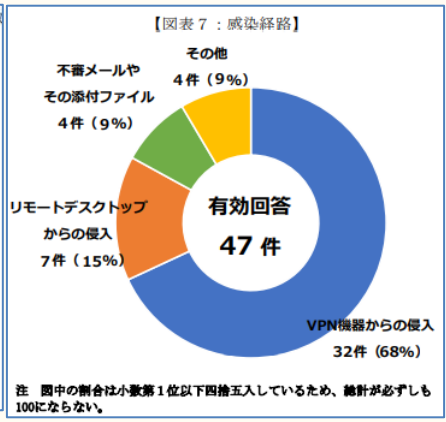
警察庁発表の令和４年上半期におけるサイバー空間をめぐる脅威の情勢等について　から抜粋



企業・団体等におけるランサムウェア被害として、**令和４年上半期に 都道府県警察から警察庁に報告のあった件数は114件**であり、令和２年下半期以降、**右肩上がりで増加**している。



被害（114件）の内訳を企業・団体等の規模別にみると、大企業は36件、中小企業は59件であり、その**規模を問わず、被害が発生**している。



ランサムウェアの感染経路について質問したところ、47件の有効な回答があり、このうち、**VPN機器からの侵入が32件**で68%

ランサムウェアは感染すると、社内のデータが暗号化され開けなくなる＝業務に莫大な影響を及ぼします
暗号化したデータを戻すための金銭要求のみならず、社内データを外部に公開するといった2重の脅迫が主流です
定期的にネットワーク機器・セキュリティ対策のアップデートや見直し、データのバックアップの確認を

情報源

JPCERT　マルウェアEmotetの感染再拡大に関する注意喚起　https://www.jpcert.or.jp/at/2022/at220006.html

警察庁WEBサイト　https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_kami_cyber_jousei.pdf

浅間商事株式会社　〒110-0005　東京都台東区上野7-15-70 浅間第一ビル　0120-830-414