

あさまセキュリティニュースレター



今一度、セキュリティ対策やバックアップのご確認を

(2019年7月10日)



ランサムウェア「WannaCry」の感染に悪用された攻撃 (EternalBlue) を検出したクライアントの数



2017年5月に世界規模で流行したランサムウェア WannaCryptor (別名: WannaCry) の脅迫画面



世界規模で感染したランサムウェアWannaCryの脅威は収束しても、悪用した攻撃は年々増加！
 現在もランサムウェア被害のご相談が入っています
 攻撃がなくなることはないため、
 今一度、社内のセキュリティ対策の見直し、
 重要データのバックアップのご確認を！！

攻撃のパターン

- 仕事に関係のある件名、興味を引く内容で、添付やURL付メールを送る
- 添付ファイルはPDF、Zip、Word、Excel、画像などファイルを装い、開くと感染ファイルが暗号化し開けなくする（開いても文字化けしたファイルに）
- 感染したPCのみならず、ネットワーク上の共有ファイルを暗号化
- 警告画面を表示し、金銭要求

被害

社内データの損失

ウイルス感染による業務停止

企業信用、信頼の失墜

対策

- 不審なメールは開かない、開いてしまった場合でも、添付やリンクはクリックしない
- 最新の脅威を知る、手口を知る、全社員がセキュリティに対し意識をもつ
- Windowsアップデート、利用ソフトの最新化(全PC)
- ウイルス対策ソフト未導入のPCがないか、未対策PCを社内ネットワークにつながらない
- インターネットの出入り口で不正な通信、ウイルスチェックするといった多層防御の仕組み
- 重要データのバックアップ (外付けHDD等も暗号化対象のため、バックアップ後は取り外す)

情報源

ESET https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1905.html