ransomware news scrap

2021-01-23

概要

- 2021/01/17の週で、ransomware関連として公開されたニュースを確認した
- その中で、侵害等が表現されたものを集めた
  - How to ...や Top N Ransome ...のような纏め記事は除外
- 本scrapの意図は以下の通り
  - 海外での現状を知ってもらいたい
    - 日本とは少し違う状況、など

no1. スコットランド環境保護省(SEPA)

- 状況
  - スコットランド環省(SEPA)が、ransomware被害
  - 電子メールとコンタクトセンターがロックされているようだ
  - 1.2GB, 4000このファイルが取得された可能性がある
    - ビジネス、調達、プロジェクト情報、およびスタッフに関連する個人情報が含まれている可能性がある
  - 2020/12/24 00:01に重大なサイバー攻撃が発生
- 対応
  - SEPA最高責任者は「公的資金から身代金を出すことはない」と述べる

no2. IObit

- Windowsユーティリ発者のIObitがハッキングされた
- ユーザに向け、DeroHE RansomwareのURLが含まれる、偽装されたプロモーションメールが送付された
- フォーラムは(時期作成時点で)まだ侵害されているようだ
- 追加情報見ると、フォーラムはvBulletinで作られており、この脆弱性を利用されたようだ
- DeroHE Ransomwareの詳細が書かれている

no3. トラフォードのごみ収集や清掃を担当する会社

- Amey PLCが、Mount Lock Ransomwareグループによる攻撃を受けた
- 2020/12/16に侵害され、12/26からデータ公開がされた
- 漏洩情報は、契約書や財務情報、パスポートのスキャン運転免許証等も含まれているようだ
- 143GB盗まれ、その半分ほどがリークサイトで公開されている

no4. ベルギーのCHwapi病院

- 攻撃者により、40台のサーバがBitLockerにより暗号化された
  - 別記事及び記事内で、300台中80台との記載もある
  - 攻撃者が40台と通知しているようだ
  - 100TBが人質になった
- 攻撃により医療業務に影響が出ている
  - 緊急の症例を他の病院に回しているようだ
  - 外科手術は再開したようだ

Ransomware対策として

- リリース時のパッチ適用
- 更新プログラムの適用
- 更新がされなくなった場合第外ソフトウェアへの置き換え
- バックアップバックアップの隔離
- 対応フローなどを用意する
    - CTOやCIOや情報部門だけではなく、広報などの部門も含める

Appendix

no1. The Scottish Environmental Protection Agency

- https://www.letsrecycle.com/news/latest-news/sepa-responds-to-ransom-demands-in-cyber-attack/
- https://www.heraldscotland.com/news/19015832.hideous-scotlands-environment-regulator-refuses-pay-ransom-cyberattack-cripples-systems/
- https://www.zdnet.com/article/ongoing-ransomware-attack-leaves-systems-badly-affected-says-scottish-environment-agency/

no2. IObit

- https://www.bleepingcomputer.com/news/security/iobit-forums-hacked-to-spread-ransomware-to-its-members/

no3. Amey

- https://www.manchestereveningnews.co.uk/news/greater-manchester-news/trafford-bin-collection-firm-suffers-19653193

no4. CHwapi hospital

- https://www.bleepingcomputer.com/news/security/chwapi-hospital-hit-by-windows-bitlocker-encryption-cyberattack/
- https://www.lavenir.net/cnt/dmf20210118_01546284/le-chwapi-victime-d-une-cyber-attaque-des-operations-annulees