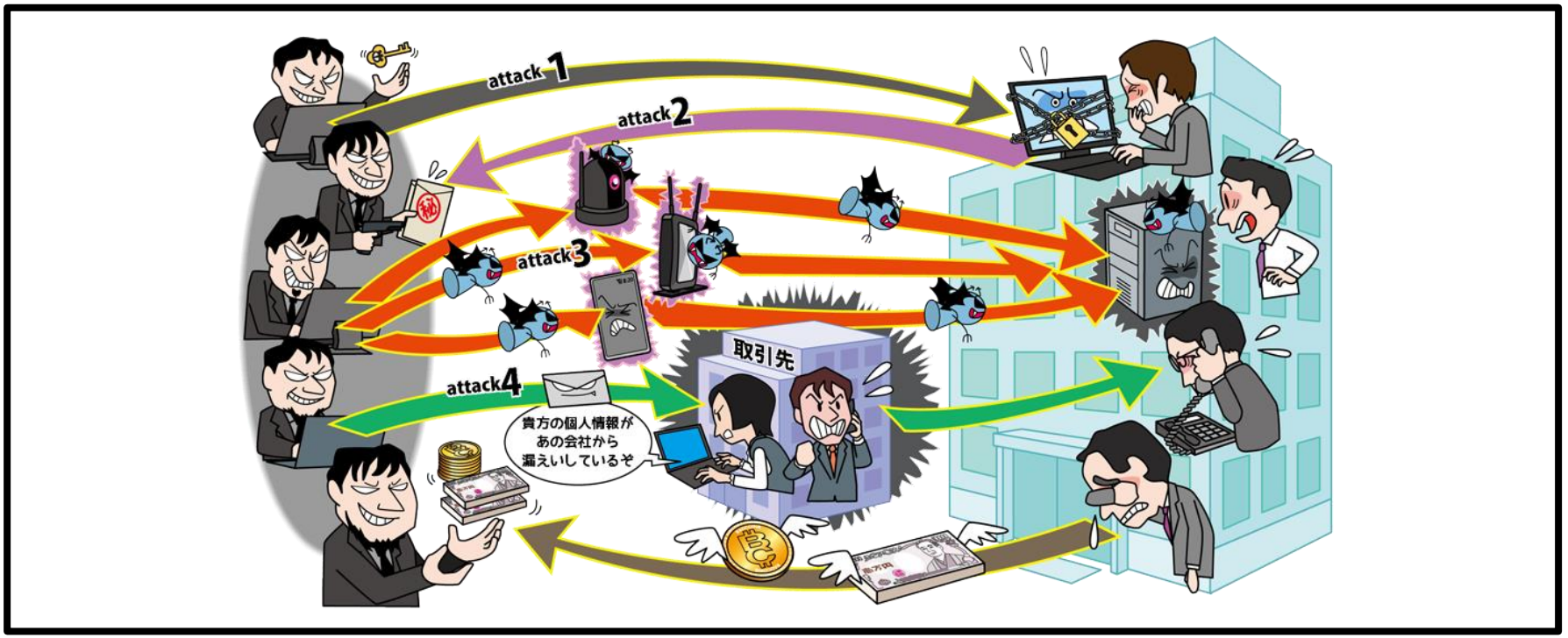
【1位】ランサムウェアによる被害

～猛威を振るうランサムウェア。四重の脅迫で被害者を逃がさない～



- PC等に保存されているファイルを暗号化され**使用不可に**
- 復旧と引き換えに**金銭を要求される**
- 情報を窃取しそれを**公開する**、攻撃を受けている事を**ビジネスパートナー等に公表**すると脅迫するケースも

Copyright © 2023 独立行政法人情報処理推進機構

【1位】ランサムウェアによる被害

～猛威を振るうランサムウェア。四重の脅迫で被害者を逃がさない～

攻撃手口

・ウイルス（ランサムウェア）に感染させて金銭を要求

メールを利用した手口

- 不正な**添付ファイル**を開かせる
- **メール内のリンク**をクリックさせる

ウェブサイトを利用した手口

- ランサムウェアをダウンロードさせるように**ウェブサイトを改ざん**
- 当該サイトを閲覧するように**メール等で誘導**

Copyright © 2023 独立行政法人情報処理推進機構

【1位】ランサムウェアによる被害

～猛威を振るうランサムウェア。四重の脅迫で被害者を逃がさない～

攻撃手口

・ウイルス（ランサムウェア）に感染させて金銭を要求

脆弱性を悪用した手口

- ソフトウェアの**脆弱性を悪用**しウイルスを実行（感染させる）
- 攻撃ツール等を利用して**ネットワーク越しに次々と感染**させる

不正アクセスによる手口

- 管理用のRDP（リモートデスクトップ）等で**サーバーに不正アクセス**
- サーバー上で攻撃者がウイルスを実行（感染させる）

Copyright © 2023 独立行政法人情報処理推進機構

【1位】ランサムウェアによる被害
～猛威を振るうランサムウェア。四重の脅迫で被害者を逃がさない～

- 2022年の事例/傾向①
  - 脆弱性を悪用してランサムウェアを配置（※1）
    - 2022年3月、東京コンピュータサービスは、同社のシステムがランサムウェアに感染し、社内管理情報や顧客の**情報等を窃取された**
    - Active Directoryを管理するためのウェブサービスにリバースプロキシサーバ経由でアクセスされ、**ウェブサービスの脆弱性を悪用されて**ADサーバに侵入された
    - ランサムウェアを自動で配布するバッチファイルを設定され、組織内の機器がランサムウェアに感染した

【出典】
※1 ランサム感染で顧客情報の流出を確認 - ソフトウェア開発会社（Security NEXT）
https://www.security-next.com/135115

Copyright © 2023 独立行政法人情報処理推進機構

【1位】ランサムウェアによる被害

～猛威を振るうランサムウェア。四重の脅迫で被害者を逃がさない～

IPA

2022年の事例/傾向②

リモートデスクトップ経由によるランサムウェア感染(※1)

・2022年6月、ヴィアックスは同社の勤怠管理システムのサーバーがランサムウェアに感染したことを公表

・ランサムウェアにより従業員1,871人、退職者2,167人の情報が暗号化された

・勤怠管理システムのウェブサーバーはメンテナンス用に外部からリモートデスクトップ接続が可能となっていた

・ウェブサーバーへのパスワードの総当たり攻撃により不正侵入されたものとみられる

【出典】

※1 勤怠管理システムサーバに対する攻撃について（株式会社ヴィアックス）
https://www.viax.co.jp/pdf/20220601.pdf

Copyright © 2023 独立行政法人情報処理推進機構

【1位】ランサムウェアによる被害
～猛威を振るうランサムウェア。四重の脅迫で被害者を逃がさない～

- **対策**
  - **経営者層**
    - 組織としての対応体制の確立
      - 対策の**予算の確保**と継続的な対策の実施
      - CISO/CIO など**専門知識を持つ責任者**を配置

Copyright © 2023 独立行政法人情報処理推進機構

【1位】ランサムウェアによる被害
～猛威を振るうランサムウェア。四重の脅迫で被害者を逃がさない～

- 対策
  - システム管理者、従業員
    - ・被害の予防
      - －迅速、継続的に対応できる体制（CSIRT等）の構築
      - －多要素認証の設定を有効にする
      - －添付ファイルやリンクを安易にクリックしない
      - －提供元が不明なソフトウェアを実行しない
      - －機器の脆弱性対策を迅速に行う
        - －パッチ適用を迅速に行う
        - －サポート切れのOSは利用停止
      - －セキュリティ対策ツールの利用や設定見直し
        - －アプリケーション実行制限や、メールおよびウェブのフィルタリング
        - －ポリシー設定を見直し、遮断設定を極力有効にする
      - －セキュリティ診断やペネトレーションテストを行う

Copyright © 2023 独立行政法人情報処理推進機構

【1位】ランサムウェアによる被害
～猛威を振るうランサムウェア。四重の脅迫で被害者を逃がさない～

- **対策**
  - **システム管理者、従業員**
    - ・被害の予防
      - －ネットワーク分離
      - －共有サーバー等への**アクセス権の最小化と管理の強化**
      - －公開サーバーへの**不正アクセス対策**
      - －**バックアップ**の取得
        - ※3-2-1 バックアップルールを参考にバックアップを検討
        - ※バックアップから復旧できることを定期的に確認

Copyright © 2023 独立行政法人情報処理推進機構

【1位】ランサムウェアによる被害
～猛威を振るうランサムウェア。四重の脅迫で被害者を逃がさない～

- **対策**
  - **システム管理者、従業員**
    - ・被害を受けた後の対応
      - －組織の方針に従い各所へ**報告、相談**する
        ※上司、CSIRT、関係組織、公的機関等
      - －バックアップからの**復旧**
      - －復号ツールの活用
      - －影響調査および**原因の追究、対策の強化**
      - －**迅速な隔離**を行い、関連組織、取引先への**被害拡大の防止**

＜身代金の支払いと復旧業者の選定について＞
－身代金を支払ってもデータ復旧や情報流出を**防げるとは限らない**

Copyright © 2023 独立行政法人情報処理推進機構