標的型・暴露型のランサムウェア

攻撃事例 ホンダ(本田技研工業)

- 2020年6月9日以降、報道
- 公式発表は無い
- ランサムウェア感染による被害
  →メール送信やファイルサーバーへの接続不可、完成車出荷前検査システム障害により2工場での出荷を一時停止、海外約10工場で生産停止
- 第三者の解説（ブログやツイート）

Maze

- ランサムウェアとしての特徴
  - データ暗号化（復号化のために金銭を要求）
  - データ窃盗（データ公開したいために金銭を要求）
  - 暗号鍵を使用法が熟慮された実装
- Attack vector
  - 動画再生用プラグインの脆弱性
  - RDPの脆弱性
- 耐解析技術の実装

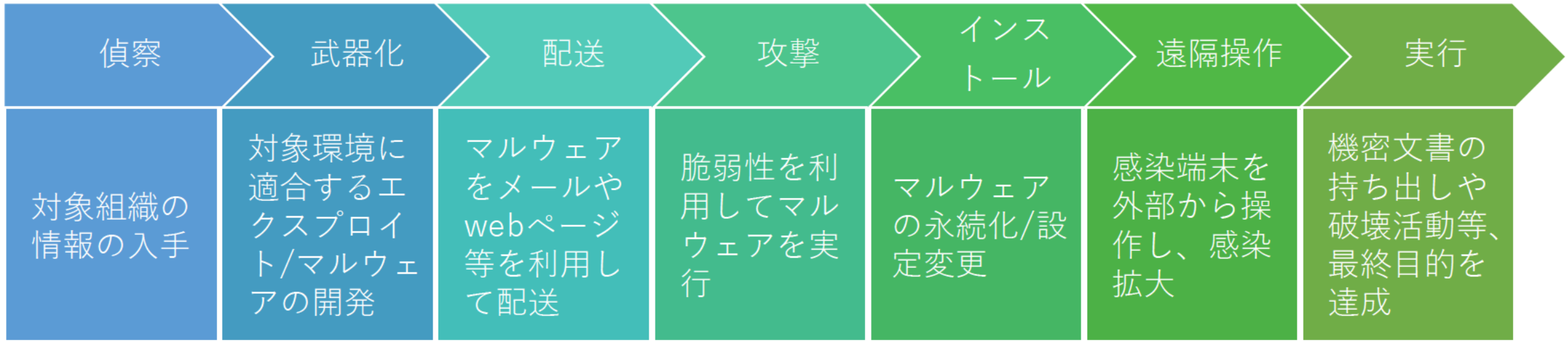
Ragnar Locker

- カプコンが被害に遭った
- 付属の脅迫文に、被害に遭った企業名を挿入
  →狙いを定めていた（事前に調査活動を行っていた）可能性を示唆
- 窃盗データの一部が、一時公開された

暴露型ランサムウェアの留意点

- バックアップだけでは善後策にならない
- 身代金を支払う前に、一部の窃盗データが公開される事例がある
- 身代金を支払ったとしても、データを消去してもらえるとは限らない
- 支払った身代金は、保険の対象外であることが多い

早期発見のために



- 標的型攻撃の場合、ランサムウェア投入・発動の前に、必ず索敵活動があるはず
- 何の目的かは不明なもののバックドアやRATが検知された場合は、次の攻撃としてランサムウェアが控えていることも想定すべき
- 具体的被害が出ていないものの、企業内プロキシを把握しているマルウェアが検知された場合も要注意