MWS企画セッション①
マルウェアとの付き合い方
～ヒヤリハット事例共有会～

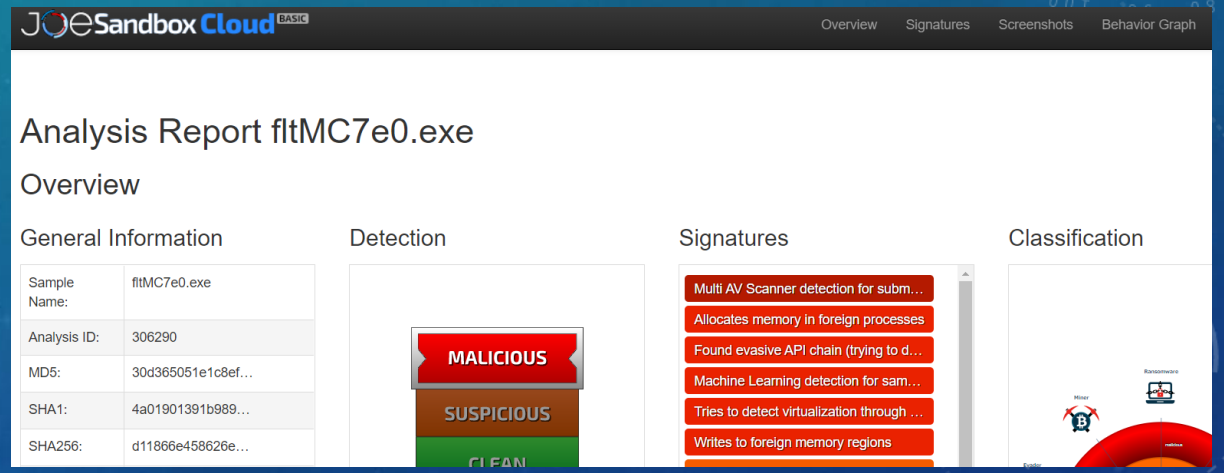
東@トレンドマイクロ

本発表は、話者個人の見解であり**所属**する**組織**とは**無関係**です。

外部解析サービスとどう付き合ってますか？

外部解析サービス

- 対象とするマルウェアの大まかなふるまいを把握
- セキュリティコミュニティへの貢献
  - サンプル自体の共有
  - メタ情報・周辺情報の蓄積



https://www.virustotal.com/
https://www.hybrid-analysis.com/
https://www.joesandbox.com/
https://any.run/

MWS研究用データセットの使用に関する覚書

第３条(禁止事項)

乙は有償無償を問わず以下の行為をしてはならないものとします。

(１)当該データの全部又は一部を第三者に対して譲渡し、移転し、貸与し、再許諾し又は担保に供すること

(２)当該データを用いて公序良俗に反すると認められる行為をすること

(３)当該データを第三者のセキュリティを脅かす恐れのある行為に使用すること

(４)当該データを第三者のプライバシーを侵害する恐れのある行為に使用すること

(５)その他、当該データを個人の特定など、目的外の利用に使用すること

しないでください。

- **研究用データセットをオンライン解析サービスなどに投入しないでください。**

  第３条(禁止事項)(1)で、「当該データの全部又は一部を第三者に対して譲渡し、移転し、貸与し、再許諾し又は担保に供すること」を禁止しています。

外部解析サービスを使うリスク・問題

- サンプル内に保持者が把握できていない情報が含まれている
  - ターゲットに関連する機微な情報
  - 攻撃者が攻撃の進行状況を把握するための情報
- その他リスクは？

マルウェアの通信とどう付き合ってますか？

マルウェアの通信を

出せる時

- 攻撃に関連する情報を取得できる
  - 2次、3次検体
  - Config類
  - コマンド・命令類
- 感染状況のコントロールが難しい
  - 予期しない検証環境の感染
  - 予期しない情報の流出
- 攻撃者へ情報を提供してしまうことも

出せない時

- 攻撃に関連する情報を取得が難しい
  - 本体部分が入手できない・動かない
- 感染状況のコントロールは容易

重要なのは

- ルールがある場合はルールを順守する
- 自分の振る舞いは誰かに
  見られているという意識を持つ
  - 痕跡を残さず調査するのは難しい
  - 一方で、痕跡を残すことが
    必ずしも悪いわけではない