SecHack365

GTotal

ー アンチウイルスは本当に正確？ ー

研究駆動コース No.30 野村和也

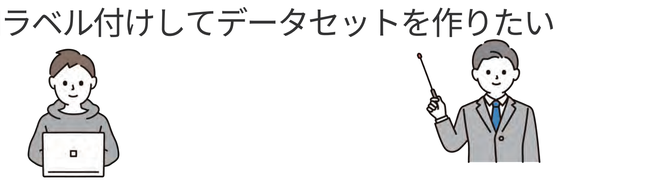
背景：VirusTotal の活用事例と現在の問題

複数のウイルス対策ソフトで怪しいファイルの検査を行える「**VirusTotal**」[1] というサイトは，その信頼性の高さからセキュリティエンジニアをはじめとして様々な人に使われています．マルウェアを検出したエンジンの数や，その内容を見ることができますが，常に結果は正確なのでしょうか？実は VirusTotal の結果は時間によって変わったり，各ベンダが示す結果がバラバラな場合もあります．

私は，VirusTotal の結果を基にした判断が「**①間違いやすい場合を発見**」し，その上で「**②できるだけ間違わないように**」する２つの成果を目指しました．

VirusTotal を使っている人たちの例

☑怪しいファイルが本当にヤバイのか知りたい
☑どんな被害をもたらすのか知りたい
☑ラベル付けしてデータセットを作りたい

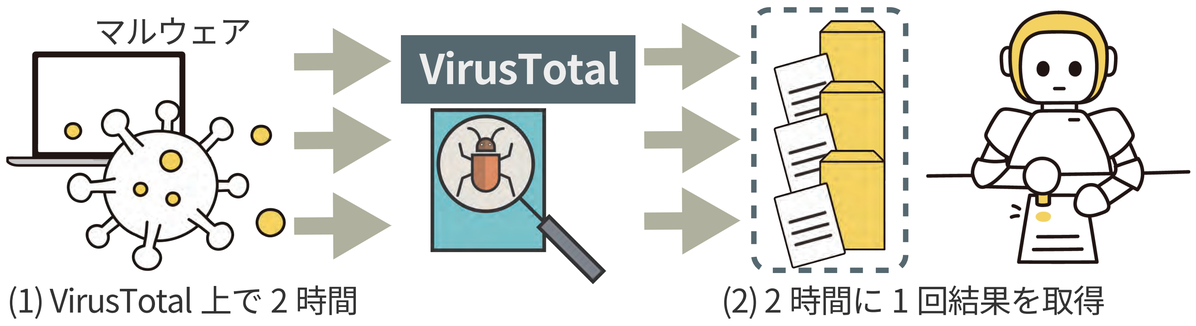


セキュリティエンジニア　　データサイエンティスト

もし判断を間違えると超困る

手法：調査とツールの仕組みの概要

本研究で行った調査とツールの仕組みの概要



(1) VirusTotal 上で 2 時間に 1 回検査を行う

(2) 2 時間に 1 回結果を取得 集計してファミリ名を決定

１つのマルウェアにつき 2 週間分繰り返す

まずは現状の調査と評価を行うために様々な手段で新鮮な怪しいファイルを収集し，VirusTotal で 4 ヶ月間毎日休まず検出を行いました．結果，**334,513 個**の検出結果を取得し，先行研究 [2] を用いて集計しました．

これらの結果を基に，「結果はいつも本当に正しいのか」「どのような場合に間違えやすいのか」を評価し，得られた知見をもとに同様の仕組みを持つツールを開発しました．

成果①：間違いやすい場合を発見

研究成果として発表

☑マルウェアのファミリやファイルタイプによって，悪性判定するエンジンの割合が異なる．

機械的に「〜個,〜%以上検出したからマルウェア」と判断する時（マルウェアのラベル付など）注意する必要がある．GTotal ではフォーマットを統一し過去の検出結果を集計．ファミリ名やファイルタイプを一意に表示し，判断の参考にすることが可能．

☑最後にスキャンされたタイミングが重要である．

検索やアップロードのたびに検出が行われているわけではないため，結果が古い可能性がある．GTotal では定期的にスキャンと検出結果の取得を行い，推移を可視化．右のグラフからも VirusTotal の結果が時間で変化することが明らか．

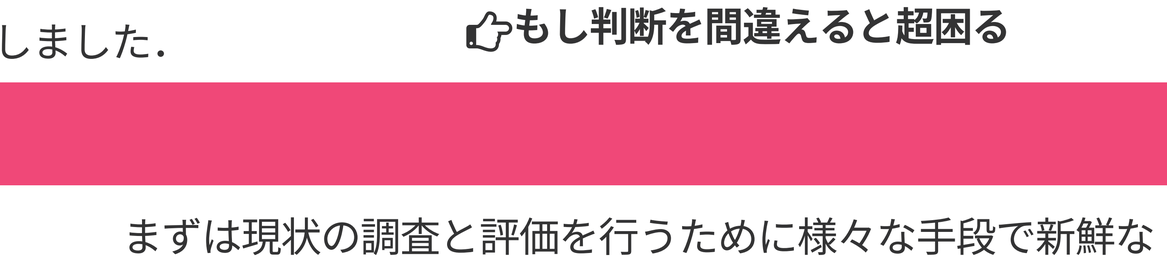
☑各ベンダが示す検出内容の粒度に注意！

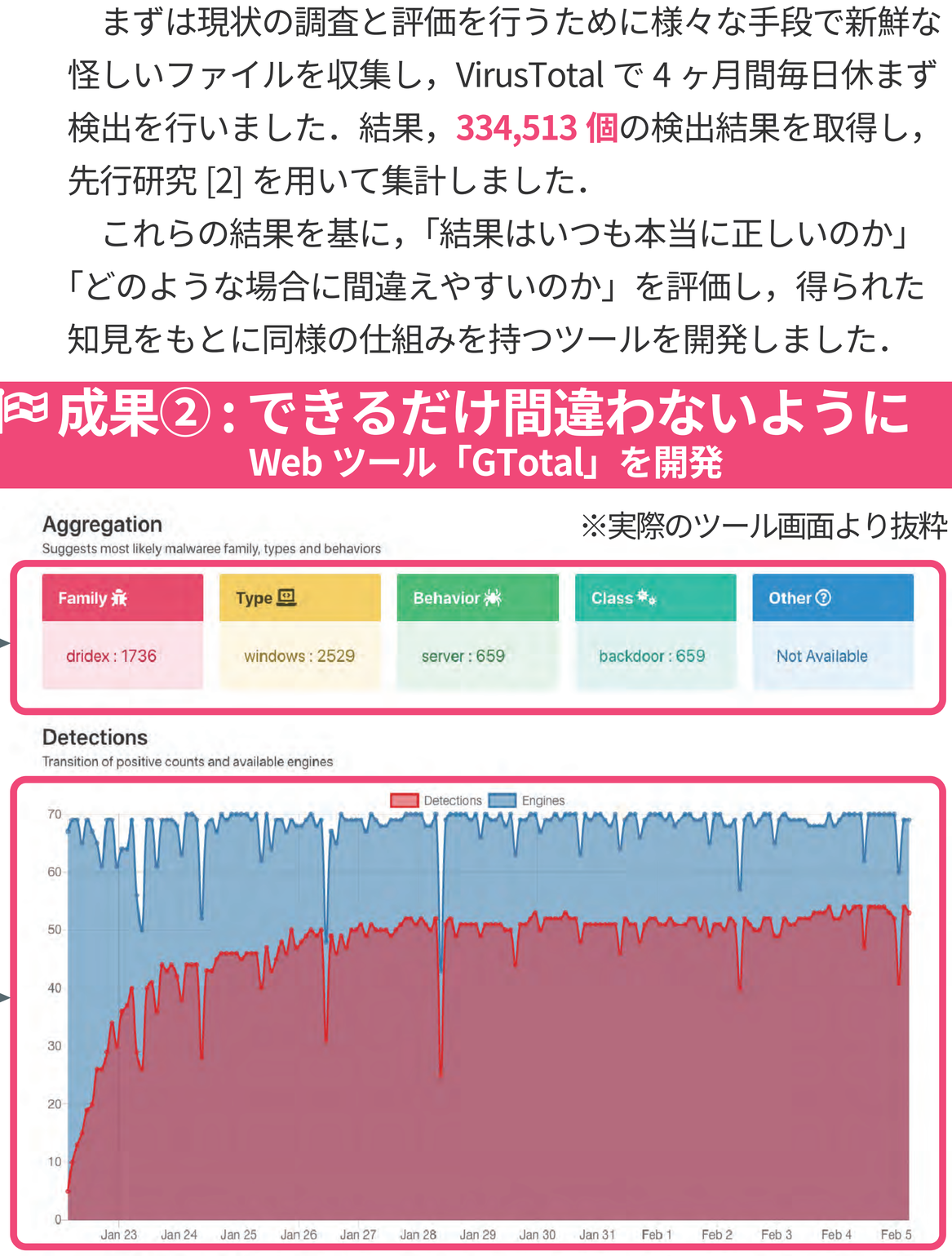
「怪しいと思う」くらいの結果から具体的なファミリ名まで示しているものまで様々．なんと，具体的なファミリ名を示しているからといって，必ず正解とは限らない．GTotal ではこの曖昧さの指標にエントロピーを導入．過去の結果からファミリ名を絞り込める検出結果をサジェストできる．

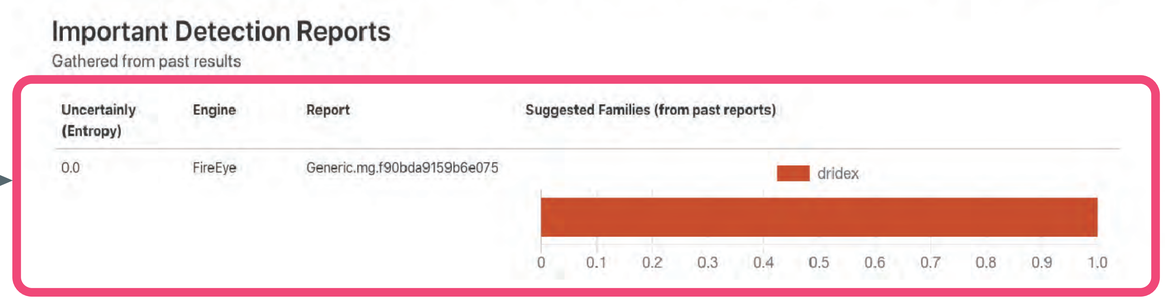
成果②：できるだけ間違わないように

Web ツール「GTotal」を開発

※実際のツール画面より抜粋







研究成果を学会（ICSS 研究会）にて発表

野村和也，秋山満昭，神薗雅紀，笠間貴弘．**「複数アンチウイルスエンジンにおける検出結果の不確実性の評価」**

学会発表・論文化によりアカデミアでの活用を期待．

Web ツール「GTotal」を GitHub にて公開

https://github.com/kazuya-n/GTotal

MIT ライセンスで公開．Docker をサポートし容易にデプロイが可能．研究者やエンジニアの活用を期待．

国立研究開発法人 情報通信研究機構

最後に …

多くの人が活用でき，今後のサイバーセキュリティの発展に貢献できる成果を目指しました．ぜひツールや論文をチェックしてみてください！

[1] “Virustotal” . https://www.virustotal.com/.

[2] S. Sebastián and J. Caballero, “Avclass2: Massive malware tagextraction from av labels, ”ACSAC’20: Annual Computer Se-curity Applications Conference, p.42–5