# OSINTによるランサムウェア感染経路推定の検証

思索駆動コース　吉田美咲

## 背景

### ランサムウェアとは

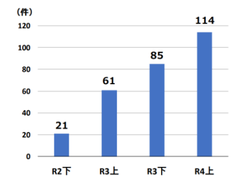
ランサムウェア（ransomware）は、**ransom（身代金）+software**の造語。感染によってデータの暗号化などが行われると、データを人質にとって金銭を要求する文書が表示される。脅迫にも、リークサイトへのデータ暴露やDDoS攻撃を行うなど様々な手法がある。

### OSINTとは

OSINT（Open Source Intelligence）は、**一般に公開されている情報をもとに、情報の収集・分析などを行い、関連付けを行いインテリジェンスを作成する活動**のこと。

### 国内組織の被害

令和4年9月に警察庁が発表した「令和４年上半期におけるサイバー空間をめぐる脅威の情勢等について」によると、令和４年上半期中に警察庁に報告された被害件数は114件で、件数は**右肩上がり**となっている。被害によって生産・販売などの業務が一時的に停止に追い込まれた。
被害による調査・復旧の費用については、55%の組織が1,000万円以上となっていた。感染経路については、**ＶＰＮ機器からの侵入**、**リモートデスクトップからの侵入**、**強度の弱い認証情報の利用**などが報告されている。



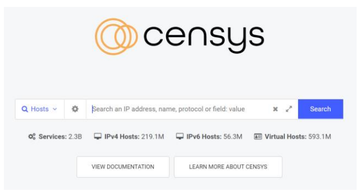

「ランサムウェア被害報告件数の推移」警察庁より

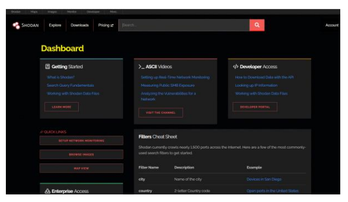
## 検証を行った理由・目的

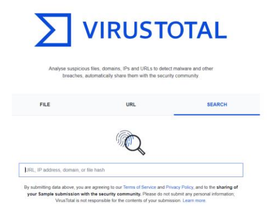
- 近年増加している国内のランサムウェア被害について、現状を把握したいと感じたため
- 感染経路について、報告された結果が正しいかどうか、傾向を知りたいと考えたため
- 攻撃者も同じように公開情報から侵入できそうな組織の機器を探すため、攻撃者の視点で対策などを検討できるようになると考えたため
- **手法を共有することによって、より多くの人が関心を持って調べるきっかけとなってほしい。**

## 使用するツールなど

各種検索エンジン、SNS、Censys、Shodan、VirusTotal、Joe Sandbox、ANY.RUN、Hatching Triage、Hybrid Analysis…

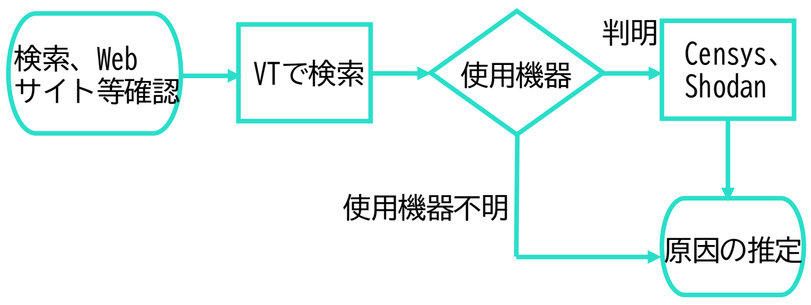



## OSINTによる感染経路推定の手法

①組織の公式Webサイト・公式SNSアカウントや「組織名+ランサムウェア（ransomware）」などで検索を行い、プレスリリースなどを確認
②①で出てきた組織のドメインをコピー
③コピーしたドメインをVirusTotalで検索
　：**自組織のドメインなどを調べると、どのような脆弱性が残っているかを確認することができる**
　　→　**予防としての効果もある**
④「RELATIONS」から「Subdomains」を参照
　：「ssl」、「vpn」、「autodiscover」など、使用機器の目途をつける
⑤機器に関連するIPをコピー（必要な場合はマスク範囲も調べる）
⑥Censys・ShodanでそのIPを検索　→　使用している機器やバージョンなどを確認することができる
　：他に、Censysで組織のドメインを直接検索する方法もある




## 手法の検証


感染経路の推定ができたのは、**国内組織54社中31社（57.4%）**
多いものは、Fortinet社製品、MS Exchange Serverなど
※VPNとしたものは、使用機器の特定までは至らなかったもの

対策が既に行われているとOSINTによる特定は難しくなるため、経路の推定ができない事例もあった。

- ランサムウェアアクターとインシデント発生時期を時系列でまとめることによって、特定するための根拠の一つになるのではないか？
- 今回の手法で調査をすると、**まだ被害は受けていないものの脆弱性が残ったままになっている組織が多い**ことが分かった。

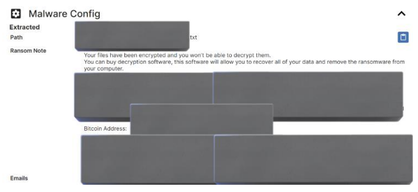
## 検体からアクターの情報を収集する手法

①「IoC ransomware」などと検索してヒットしたレポート内のIoCからSHA256やMD5の情報を収集
　また、Twitterで「ransomware sample」や「ransomware MD5（SHA256、SHA1）」などと検索して収集する方法もある。
　※オンラインのマルウェアサンドボックスツールでランサムウェアアクターなどのタグで検索もできるが、正確ではない場合もある。

②①で集めたMD5などをコピー

③Joe Sandbox、ANY.RUN、Hatching Triage、Hybrid Analysis、VirusTotalなどのツールで、②でコピーしたものを検索し、検体を見る。

④ランサムノート（身代金要求文書）を見る。
　探しやすいものから順に…
　→Hatching Triage　　：「Malware Config」内に「Ransom Note」や「Emails」が見える場合がある。
　　ANY.RUN、JoeSandbox：プレビューの画面として表示される場合がある。
　　Hybrid Analysis　　：txtになっているため、「onion」などと文字検索をしてヒットする場合がある。




得られる情報の例

- **要求文書**の内容（言い回しなど）
- **リークサイト**のURL
- **ビットコイン**アドレス
- **メールアドレス**

GitHubにまとめている個人はいるが、**更新が追い付いていない**場合が多い。

## 今後の展望

手法の共有を行ったため、**より多くの人にこの手法を実践してもらいたい。**
今回は使用しなかったツールが他にもあるため、他のツールも使用しながらその効果を検証したい。また、新たなツールの開発などによってより最適な手法が検討できるため、そういった面でも検証を続けたい。

## その他

画像　：https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_kami_cyber_jousei.pdf

連絡先：ufdgi347dehwki@protonmail.com

謝辞：本作品の制作にあたり、SecHack365関係者の皆さまに大変お世話になりました。ありがとうございました。