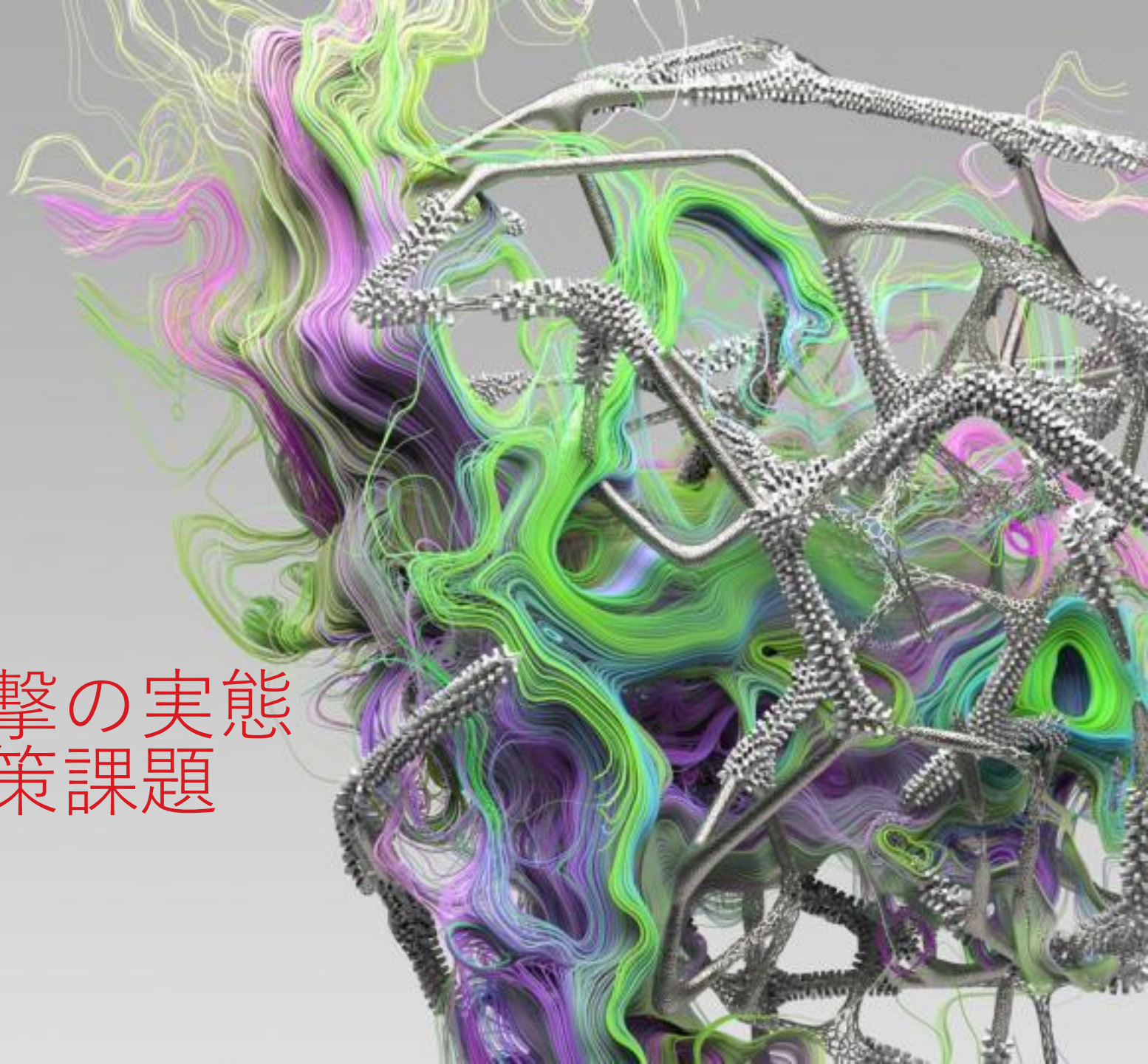
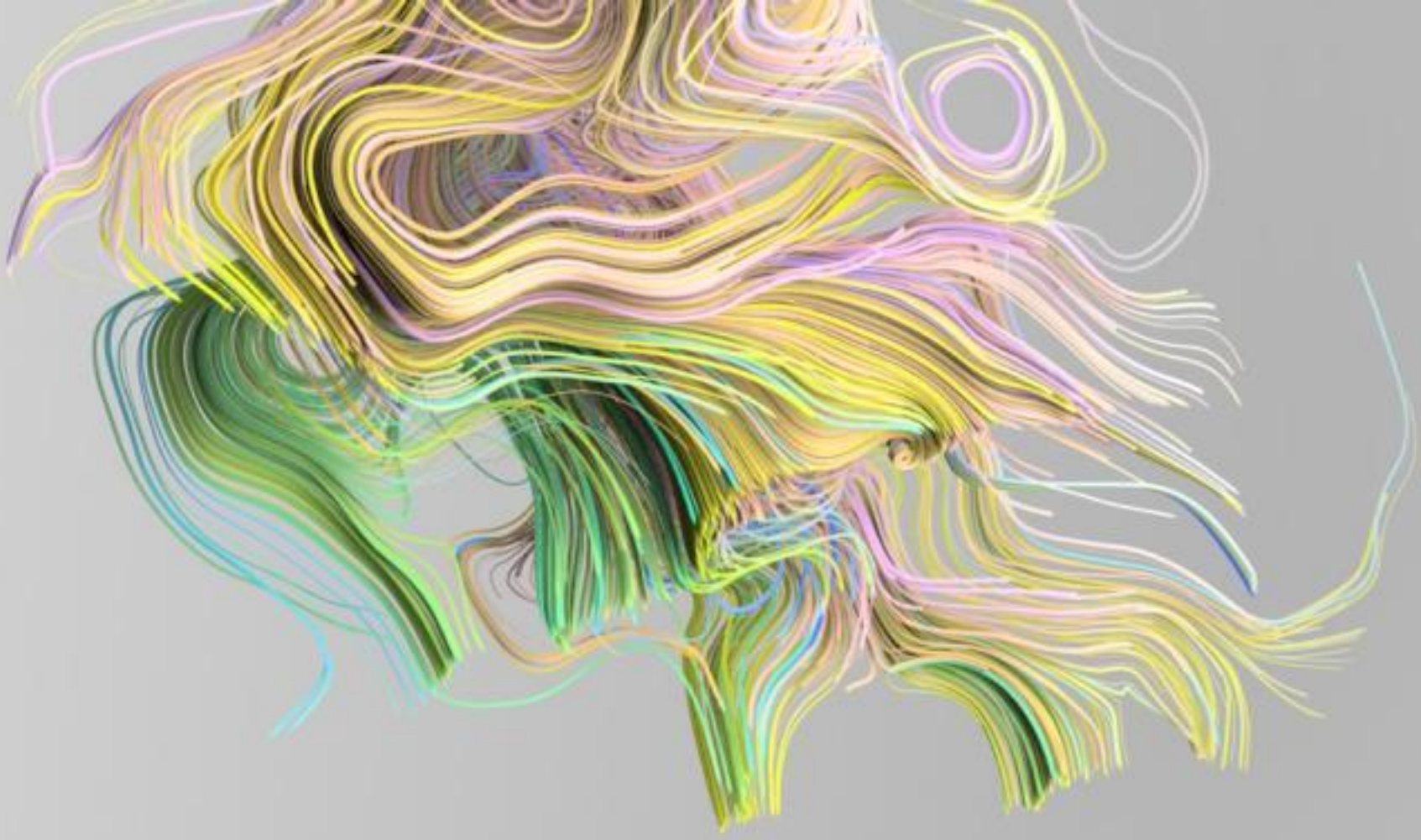


最新のサイバー攻撃の実態とセキュリティ対策課題

トレンドマイクロ株式会社

アジェンダ

1. 標的型サイバー攻撃の動機とは
2. ランサムウェアの最新傾向
3. 新型コロナウイルスに便乗した脅威
4. サプライチェーン攻撃
5. テレワークの弱点を狙う脅威
6. 対策ポイント
7. まとめ



1. 標的型サイバー攻撃の動機とは

サイバー空間をめぐる脅威の分類

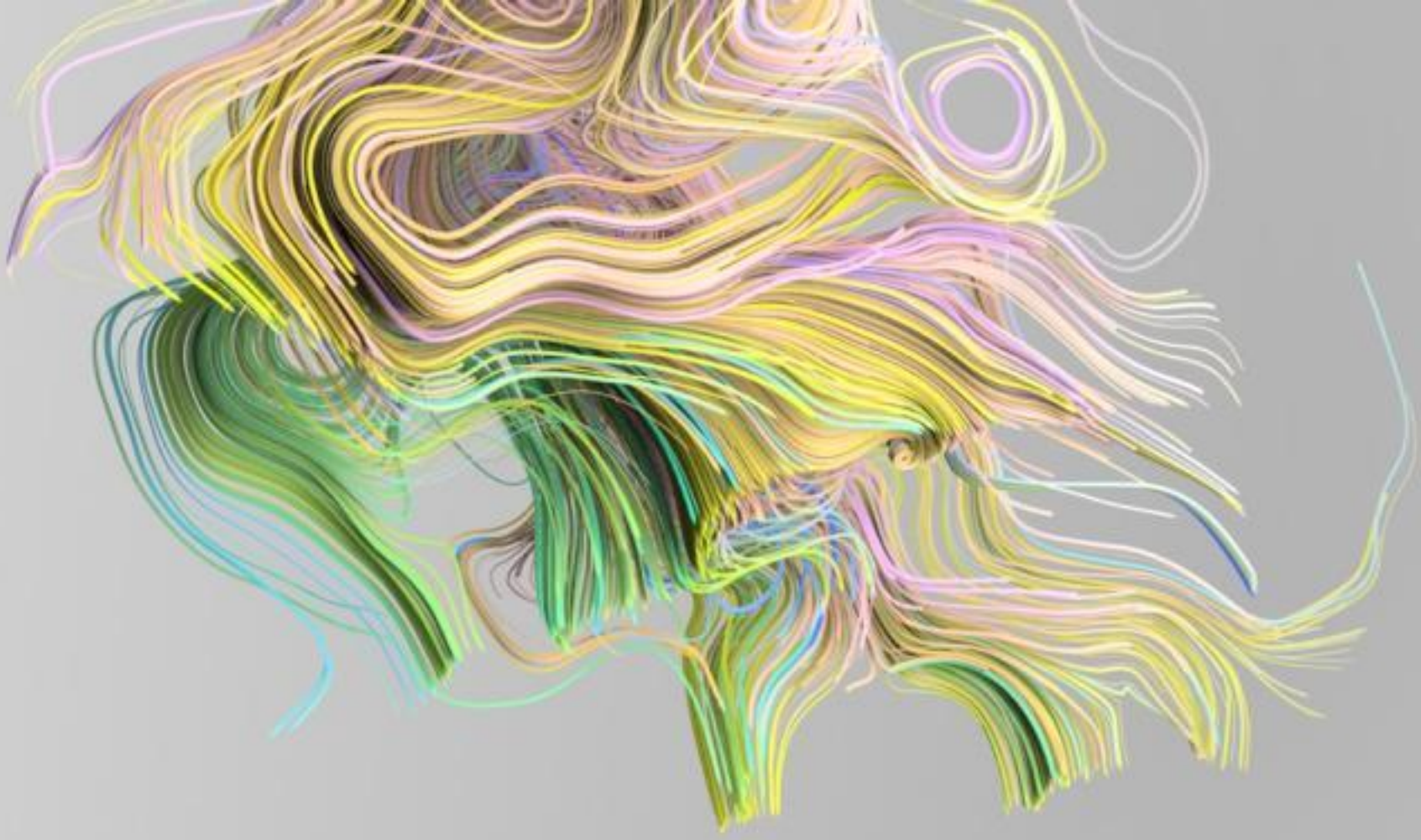
※参考：公安調査庁 - サイバー空間をめぐる脅威
http://www.moj.go.jp/psia/ITH/topics/column_02.html

目的・動機	活動の主な類型	主な事例
国家や特定組織・企業の諜報活動	✓ 情報窃取・サイバー諜報	➢ **日本年金機構における個人情報125万件流出事案** 日本年金機構の職員がメールに添付されたマルウェア付きファイルを開封した結果，PC端末が外部から遠隔操作され，加入者の個人情報約125万件が流出した。 ➢ **中国を拠点とする「APT10」によるサイバー諜報** 米国司法省は2018年12月，セキュリティ業界で「APT10」と呼ばれるサイバー攻撃集団のメンバーである中国人ハッカー2人を起訴したと発表した。2人は10年以上の間，中国の情報機関である国家安全部と連携して，米国内外の数十に及ぶ企業及び政府機関のシステムに侵入し，航空・宇宙分野などの機微な技術情報などを窃取したとされる。
国家や特定組織・企業へ妨害工作	✓ 情報システムの破壊・機能妨害（サイバー破壊活動） ✓ 心理戦・影響力工作（オンライン・インフルエンス・オペレーション）	➢ **「Stuxnet」によるイラン核関連施設攻撃事案** イラン・ナタンツに所在するウラン濃縮施設のシステムに，「Stuxnet」（スタックスネット）と呼ばれるマルウェアが侵入し，同施設の遠心分離機を秘密裏に誤作動させ，約1,000台に物理的な破壊を引き起こしたとされる。 ➢ **ウクライナにおける大規模停電事案** ウクライナの電力会社がサイバー攻撃を受け，制御システムが不正に操作された結果，同国西部で数時間に及ぶ停電が発生し，約22万5,000人が影響を受けた。 ➢ **韓国・平昌冬季オリンピック大会妨害事案** 平昌冬季オリンピックの開会式に際し，会場内でのWi-Fi接続，公式ウェブサイト，チケット発券などの機能が一時停止するシステム障害が発生した。 ➢ **米国大統領選挙へのロシアの干渉** 米国政府の発表によると，ロシアは，2016年米国大統領選挙に影響を与える取組として，①ロシア軍当局者が民主党及びクリントン候補陣営のメールなどをハッキングにより窃取し，ネット上で公開・拡散する活動，②ロシア政府に近い企業が偽情報の流布やソーシャルメディア上での工作を行う活動を展開したとされる。
不正な金銭獲得	✓ 人質型攻撃 ✓ フィッシング ✓ オークション詐欺 ✓ 金融アカウント乗っ取り など	➢ **ランサムウェア「WannaCry」の世界規模での感染事案** ネットワーク経由で急速に自己伝染する機能を持つランサムウェア「WannaCry」（ワナクライ）が世界中に拡散し，我が国を含む約150か国の政府機関，医療機関，企業などが感染被害を受けた。 ➢ **暗号資産交換所における不正送金事案** 我が国企業が運営する暗号資産交換所のシステムが，外部からの不正アクセスを受けた結果，約580億円相当（当時のレート）の暗号資産が不正に送金された。
劇場型・愉快犯的動機	✓ アカウント乗っ取り ✓ 虚偽の書き込み（爆破予告など） ✓ 個人情報暴露　など	➢ **有名人のInstagramのアカウント乗っ取り** ➢ **ファイル共有ソフト（Winny, Shareなど）を介して個人情報などを流出** ➢ **掲示板やメールによる爆破予告**

日本の組織を狙う主な攻撃者グループの存在

- 日本国内で活動が確認された主な攻撃者グループと紐づくツール・マルウェア（以下は一例）
- 赤字のツール・マルウェアは日本国内で多数確認

攻撃者グループ	代表的なツール・マルウェア
APT10	ChChes, RedLeaves, koadic, ANEL, Cobalt Strike
BlackTech	PLEAD(TSCookie), KIVARS, BIFROSE
Taidoor	DALGAN, EXFRAM, SIMBOT, TAILD, TALERET
Tick	Daserf, Datper, xxmm, down_new, Avenger
DragonOK	Sysget, Upheart(CHWRITER)
APT28	Zebrocy
APT29	WellMess
Gamaredon	TROJ_RELSLOADR, VBS_GAMADLOAD, W97M_GAMADROP



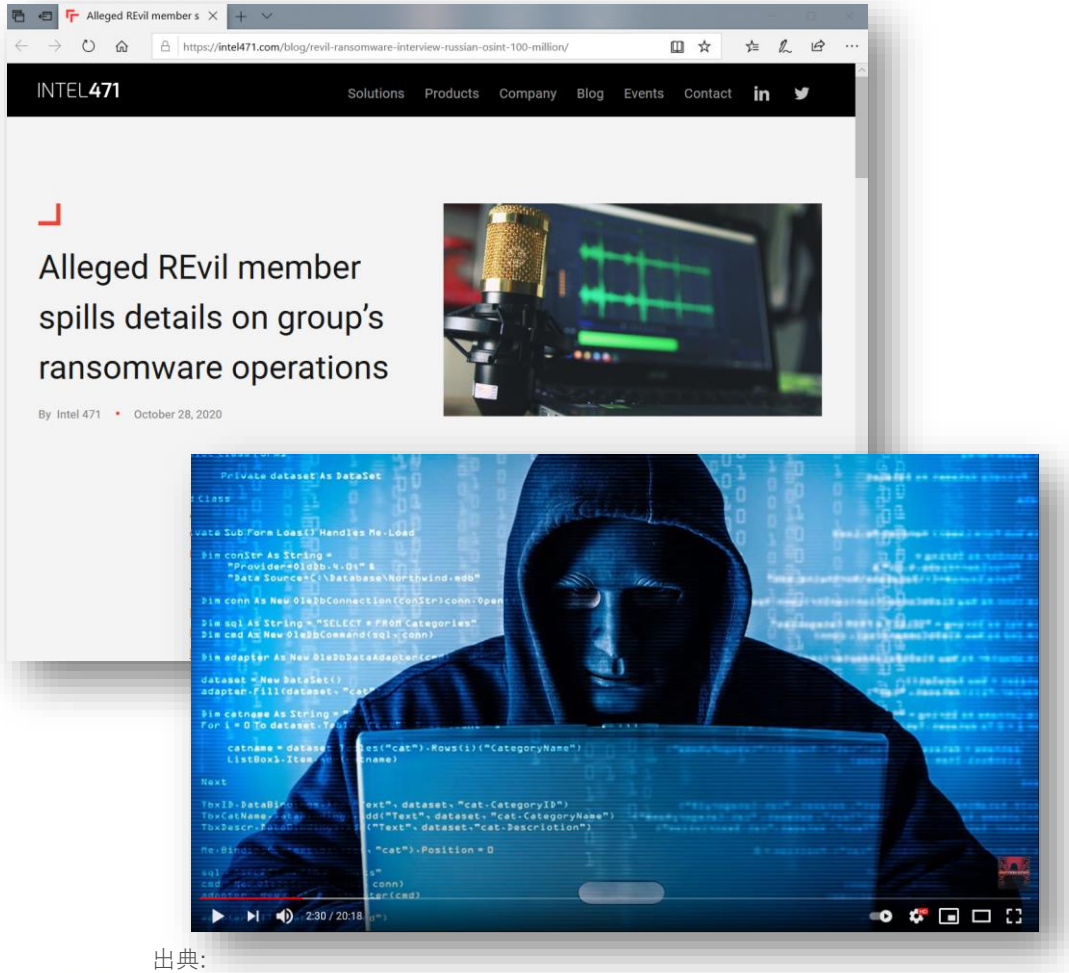
2. ランサムウェアの最新傾向

ランサムウェアとは？

- ランサムウェア（英：Ransomware）
  - 感染したPCを強制的にロックしたり、PC内のファイルを暗号化し、元に戻すことと引き換えに「身代金」を要求する不正プログラム
  - 「身代金要求型不正プログラム」とも呼ばれる
  - 語源：Ransom（身代金）＋Software

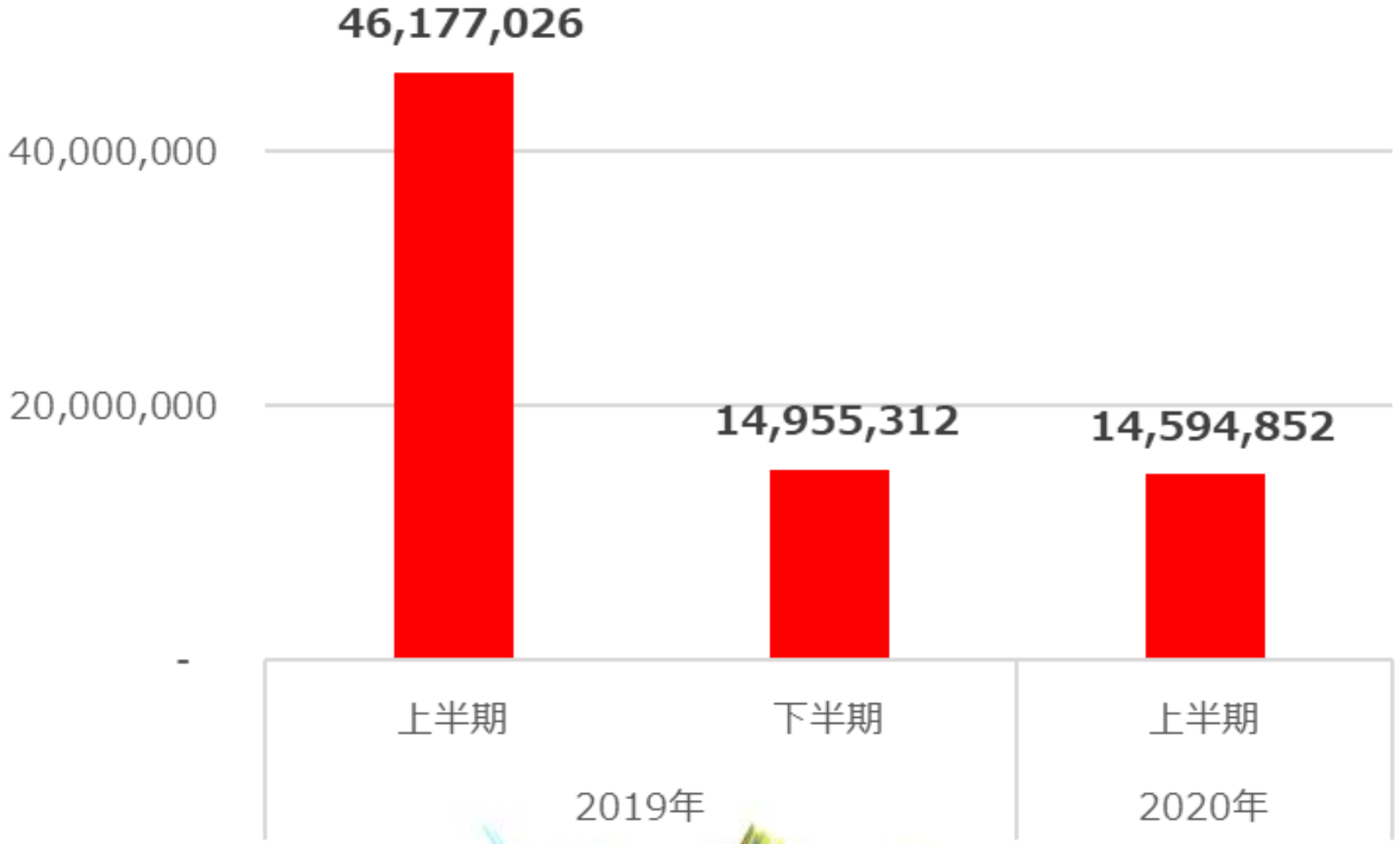
ランサムウェア開発者へのインタビュー

- REvil/Sodinokibi開発者へのインタビュー
  - ロシア語の話者
  - 年商は年間100億円以上
  - 被害にあった大企業の1/3が支払いに応じた
  - 外貨両替のトラベレックス社やテキサス州の行政機関にも攻撃を実施
  - 侵入方法はRDPが一般的
  - 3分で侵入できるケースもある



出典:
https://intel471.com/blog/revil-ransomware-interview-russian-osint-100-million/
https://www.youtube.com/watch?v=ZyQCQ1VZp8s&feature=youtu.be

全世界でのランサムウェアの動向

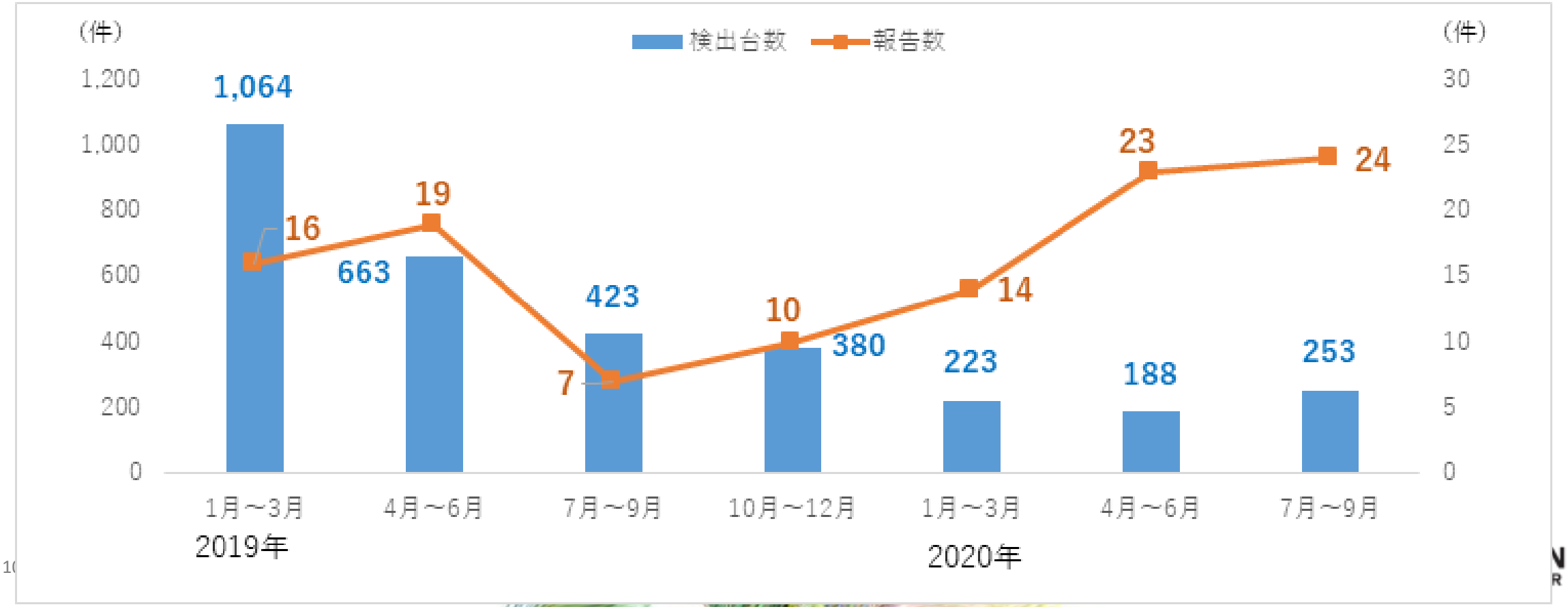


図：全世界におけるランサムウェア攻撃総数推移

ランサムウェアの感染報告数

- 国内法人におけるランサムウェア検出台数と国内法人からのランサムウェア感染報告数推移（2019年～2020年9月）

※トレンドマイクロによる調査（2020年11月）

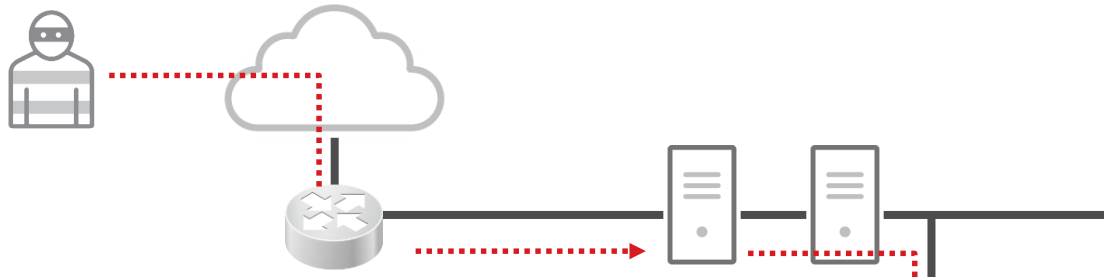


ランサムウェア攻撃の最新傾向

1）不特定多数へのばらまき→法人を標的とした攻撃

- 従来のメール経由、Web経由による侵入に加え、
  脆弱性攻撃や不正アクセスによる遠隔からの直接侵入事例を確認
- 侵入後、内部活動により攻撃基盤を拡大した後、ランサムウェア感染
- 遠隔実行による感染に加え、グループポリシーによる配信・実行
- 具体例：
  2020年に入り医療業界での被害が報告されている「MAZE」の事例では、
  RDPのブルートフォースを起点にネットワーク内に侵入、内部活動により
  ActiveDirectoryサーバを侵害しグループポリシーを利用してランサムウェアを拡散させたことが報告されている

昨今のランサムウェアの特徴：概要図



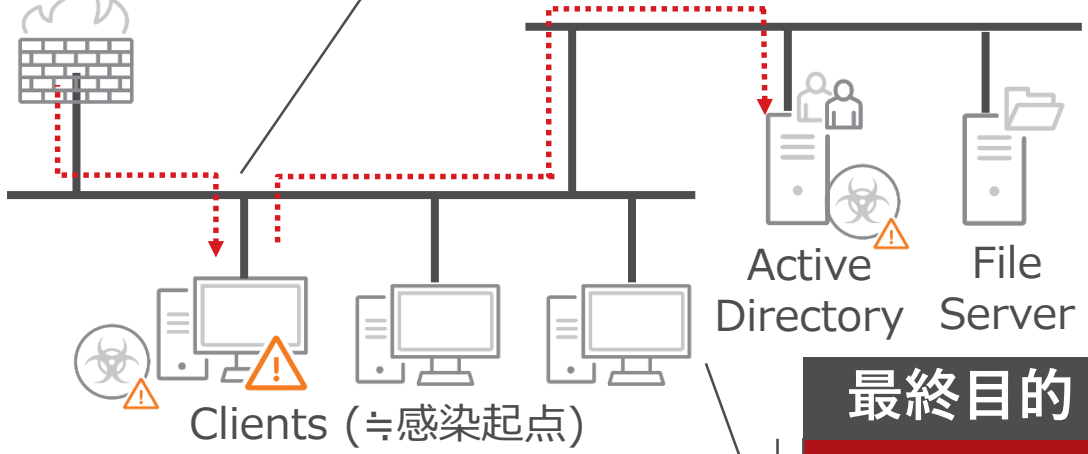
Public service
(VPN,RDP,SSH..)

侵入

・VPNサービス等の脆弱性
・安易なID,パスワード

内部活動による拡散準備

・ハッキングツールの利用
・セキュリティ対策の無効化
・Active Directoryの侵害



Active Directory

File Server

Clients (≒感染起点)

最終目的・ランサム感染

・遠隔実行
・GPO機能による配信・実行
・データ暗号化＋情報リーク

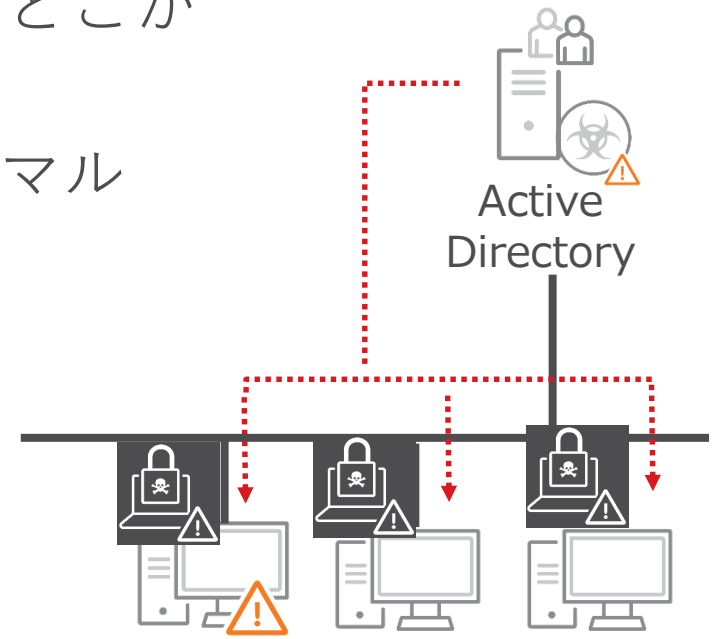
昨今のランサムウェアの特徴：補足

- 外部からの侵入手法
  - RDPやSSHなどのハッキング（ブルートフォースによる安易なパスワードの突破など）
  - 外部からアクセス可能な脆弱性の利用（VPNサービス等）
- 侵入後、標的型攻撃で使用されるツールや手法を利用した内部活動
  - パスワード窃取（Mimikatz等）
  - セキュリティ対策製品の強制終了（Process Hacker、PC Hunter等）
  - 内部ネットワークの情報探索（Advanced IP Scanner等）
  - 遠隔実行（PowerShell、PsExec、TaskScheduler、Cabalt Strike等）

昨今のランサムウェアの特徴：補足

- グループポリシー（GPO）を利用した拡散
  - 攻撃者がActive Directoryにログオン、あるいは侵害したクライアントにドメイン管理者権限があればどこからでも設定可能
  - ADからマルウェア配信 or 特定ファイルパスのマルウェアを実行

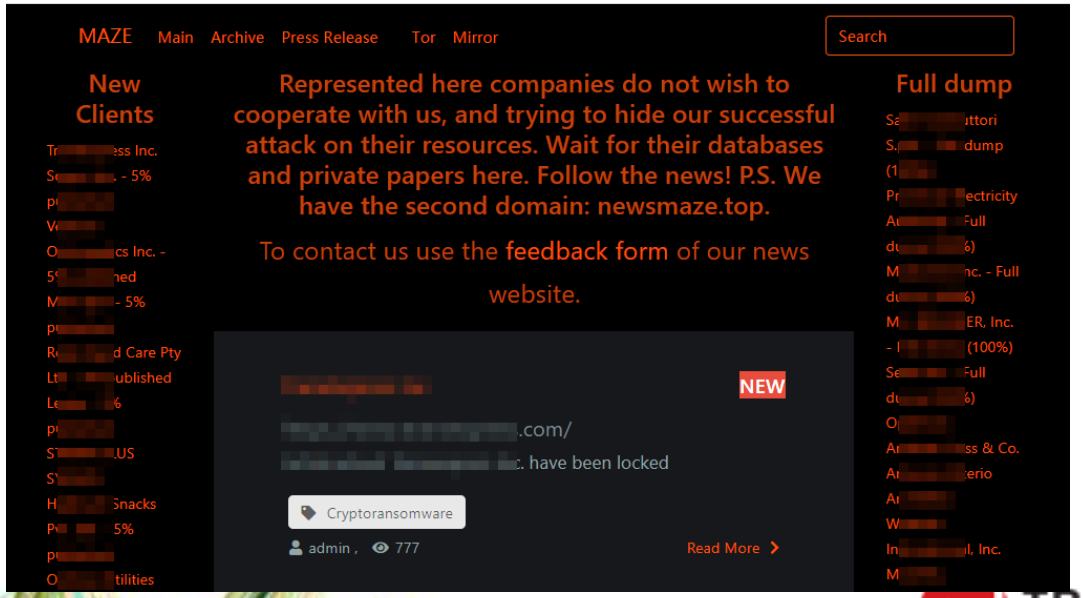
    注：配信はマルウェアがmsi形式である必要がある



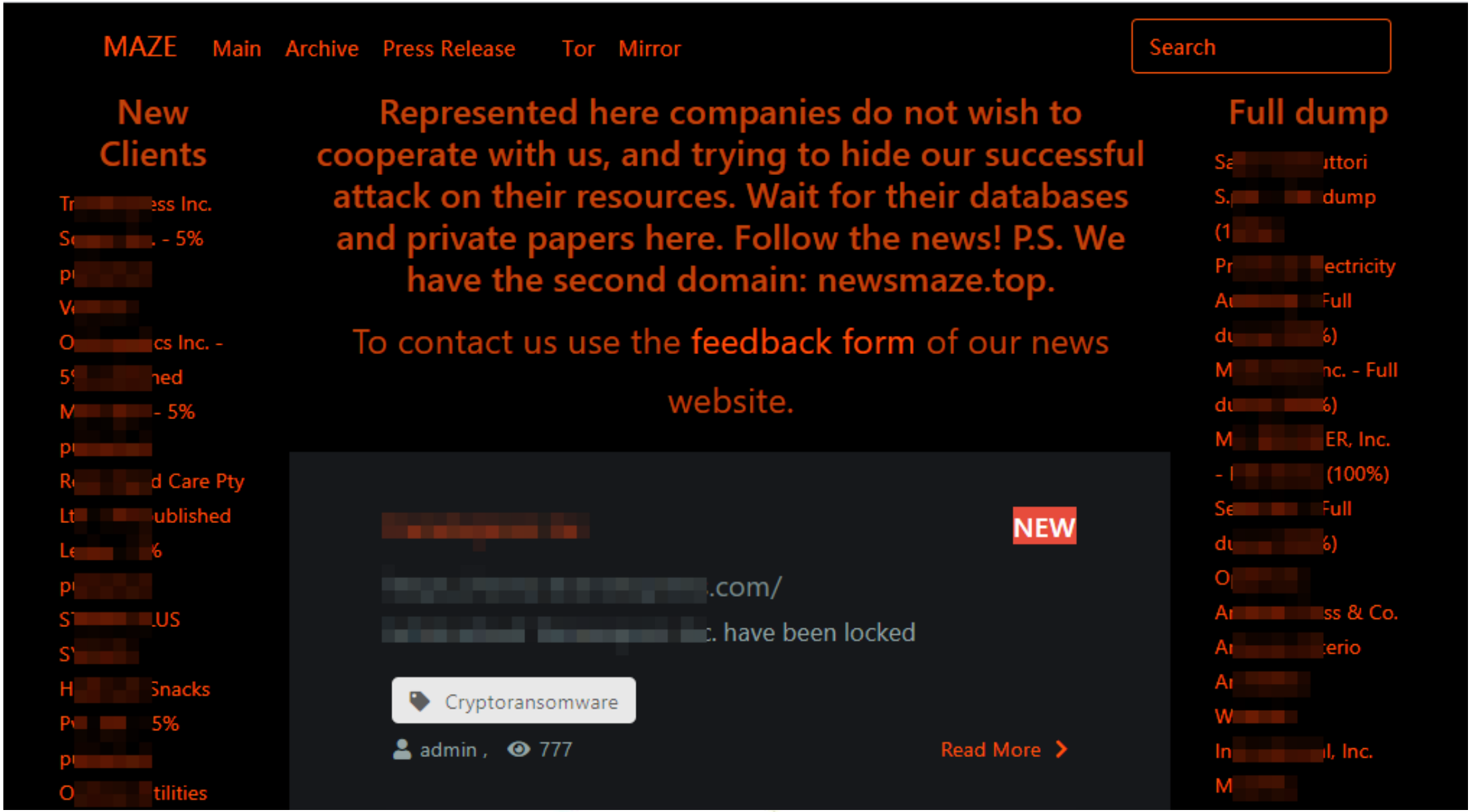
ランサムウェア攻撃の最新傾向

2）情報暴露による脅迫

- データの暗号化前に情報を窃取、身代金を払わない場合には窃取した情報を暴露すると脅す
  - 「MAZE」、「SODINOKIBI/REvil」、「DOPPELPAYMER」、「NetWalker」など
- 自身のサイトで身代金を支払わない企業名を公開、実際に情報が暴露されたり闇市場で販売された例も



図：MAZEランサムウェアの暴露サイト例



図：MAZEの情報暴露サイト

!!!_READ_ME_ !!!.txt - メモ帳

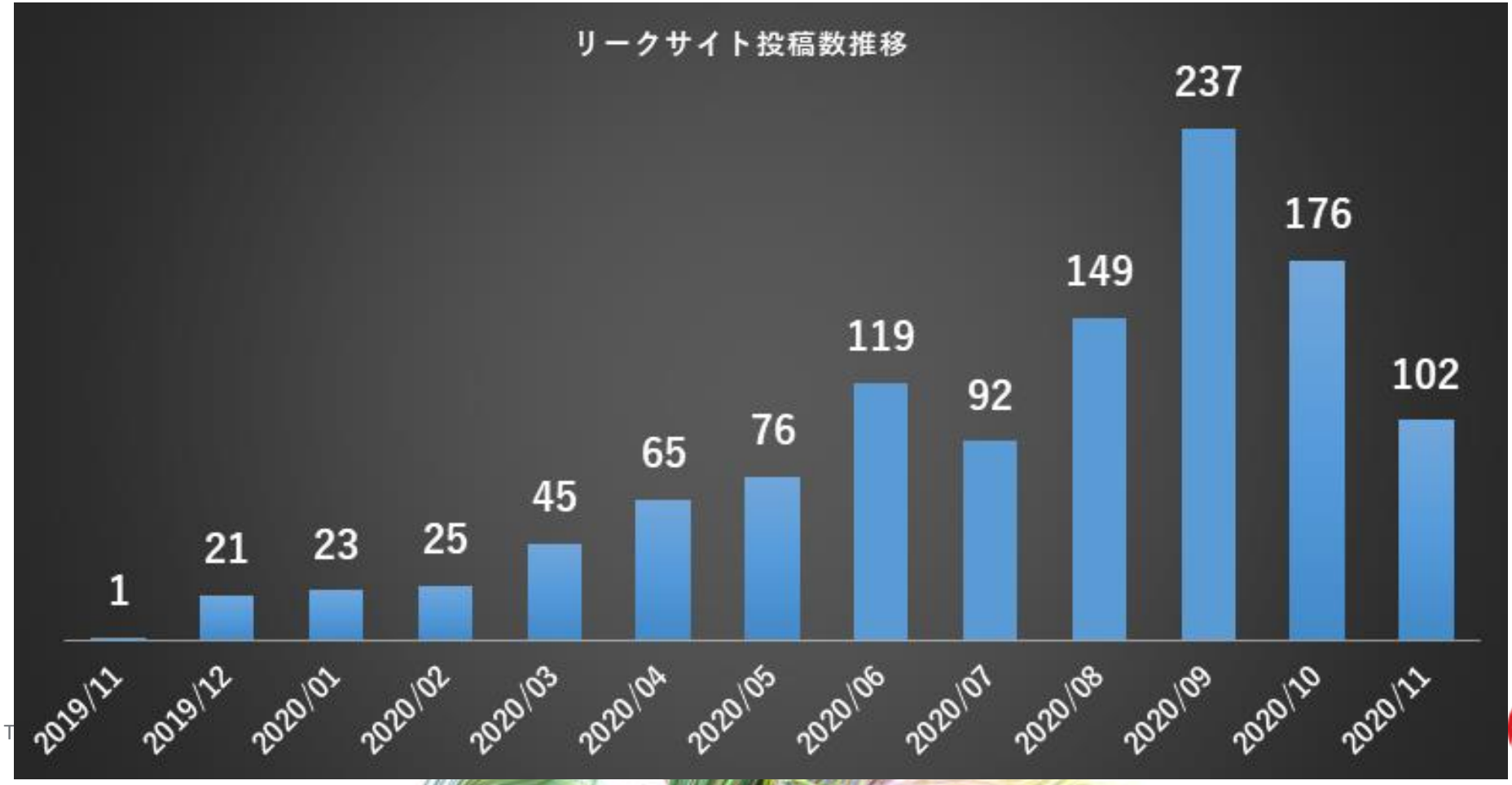
ファイル(F) 編集(E) 書式(O) 表示(V) ヘルプ(H)

```
**********************************************************************************************************************

                                        HELLO !

If you reading this message, it means your network was PENETRATED and all of your files and data has been ENCRYPTED

                                    by  R A G N A R  L O C K E R !

**********************************************************************************************************************
                    *YOU HAVE TO CONTACT US via LIVE CHAT IMMEDIATELY TO RESOLVE THIS CASE AND MAKE A DEAL*
                          (contact information you will find at the bottom of this notes)

                                        !!!!! WARNING !!!!!

DO NOT Modify, rename, copy or move any files or you can DAMAGE them and decryption will be impossible.
DO NOT Use any third-party or public Decryption software, it also may DAMAGE files.
DO NOT Shutdown or Reset your system, it can DAMAGE files
-----------------------------------

There is ONLY ONE possible way to get back your files - contact us via LIVE CHAT and pay for the special DECRYPTION KEY !
For your GUARANTEE we will decrypt 2 of your files FOR FREE, to show that it Works.

Don't waste your TIME, the link for contact us will be deleted if there is no contact made in closest time and you will NEVER restore your DATA.
!!! HOWEVER if you will contact us within 2 day since get penetrated - you can get a very SPECIAL PRICE.

                                        ! WARNING !
                              ! Whole your International Corporate Network was fully COMPROMISED !
```

ランサムウェアによる情報暴露事例

- ランサムウェアによるリーク企業延べ数（全世界）

※調査時期は2019年11月～2020年11月15日。本数値は2020年11月16日時点の情報です。再調査などで一部数値が変更になる可能性があります。

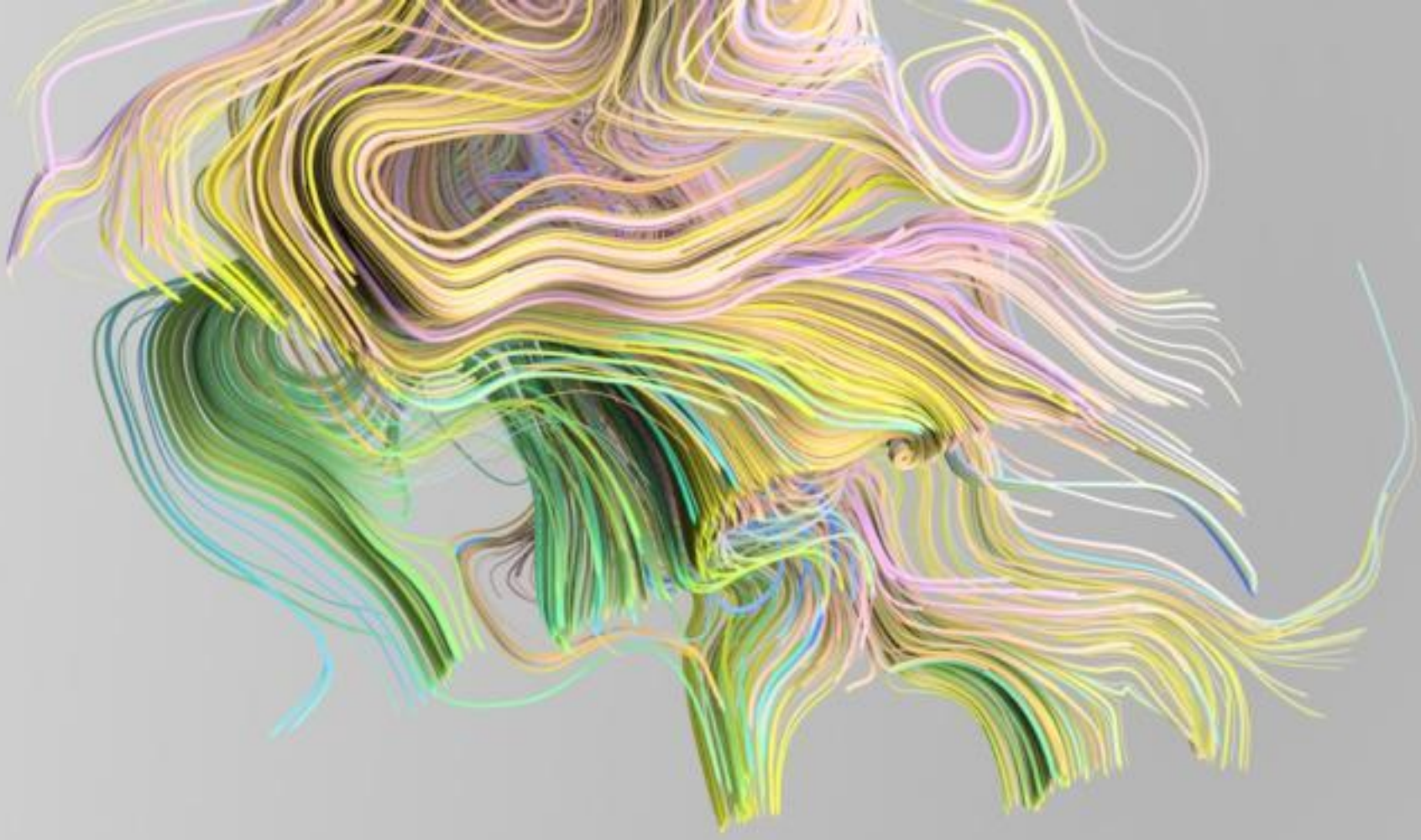


ランサムウェアによる情報暴露事例

- ランサムウェアによるリークサイト投稿数（全世界）

ランサムウェアによる情報暴露事例

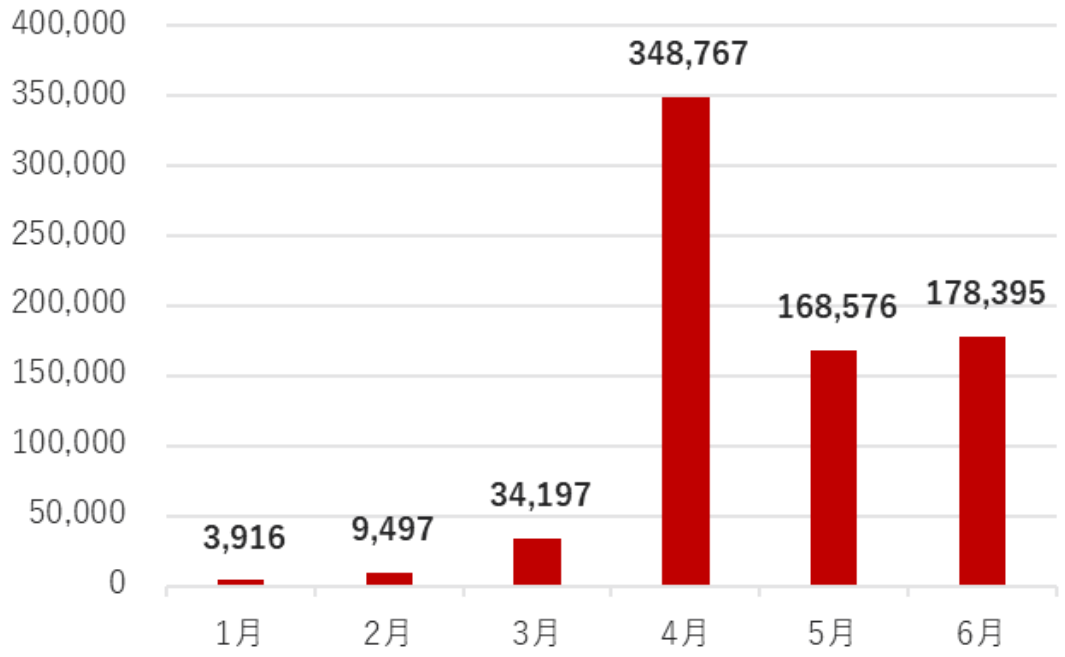
- ランサムウェアによるリーク企業延べ数（日本企業のみ（日本企業の海外支社や拠点を含む））



3. 新型コロナウイルスに便乗した脅威

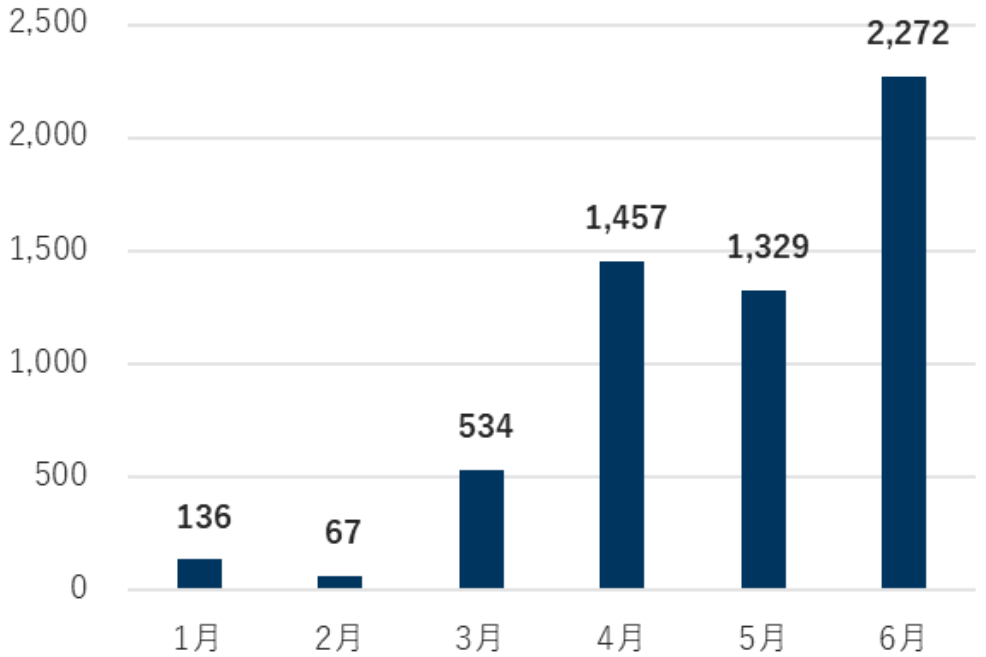
新型コロナウイルスに便乗した不正サイトやマルウェアの出現

不正サイト



■図：全世界におけるCOVID-19関連*不正サイトへ誘導されたアクセス数の推移（2020年、トレンドマイクロSPNより）

マルウェア



■図：全世界におけるCOVID-19関連*マルウェアの検出台数推移（2020年、トレンドマイクロSPNより）

※抽出条件：ファイル名に”covid”、”covid-19”、”ncov”、”coronavirus”を含むもの

コロナに便乗した脅威 - 法人組織を狙った事例①

EMOTETを拡散するスパムメールで悪用（国内）


FW: 通知

宛先

メッセージ　添.doc (133 KB)

管内　通所・施設系障害福祉サービス事業者　様

お世話になっております。

新型コロナウィルス関連肺炎については、中国武感市を中心に患者が報告され、
国内でも■■県で患者が報告されているところであり、
今後、訪日者の増加が見込まれることを受けて、別添の通知が発出されました。

つきましては、別添通知をご確認いただき、
感染予防対策についてよろしくお願いいたします。
なお、並行して■■■■■■■■ページへの掲載準備をしております。

（内容）
○入所者・利用者に咳、発熱等の症状があり、次のいずれかに該当する場合は、
速やかに所管保健所に連絡するとともに、医療機関の受診を勧奨すること。
・本人に中華人民共和国での滞在歴・渡航歴がある場合
・中華人民共和国での滞在歴・渡航歴がある親族等との濃厚な接触がある場合
○石けん及び流水による手洗い、席エチケット（マスクの着用）の励行について周知を図ること
○可能な限り、施設の入り口等に消毒用エタノールを設置すること。
○施設設備について、消毒用エタノール又は0.05~0.5%次亜塩素酸ナトリウム希釈液で清拭すること。

＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊
■■■■■■■■保健所福祉室（担当：■■■
〒■■■■■■■■■■■■■■■■■■■■
電　話：■■■■■■■■■■■■■■■■■■■■
ＦＡＸ：■■■■■■■■■■■■■■■■■■■■
＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊

■図：EMOTETを拡散するマルウェアスパムでの悪用
（国内で2020年1月28日に確認）

標的型攻撃グループによる攻撃で悪用（国内）

- 標的型攻撃グループ「Gamaredon」による日本への攻撃
  標的型メールの件名が「Coronavirus (2019-nCoV)」


TREND MICRO　トレンドマイクロ セキュリティブログ
セキュリティ専門家による脅威情報・ニュースをお届けします。

ホーム » Search results for: Gamaredon

標的型攻撃グループ「Gamaredon」による日本への攻撃を初観測

投稿日: 2020年3月30日
脅威カテゴリ: サイバー攻撃
執筆: Cyber Threat Research Team（CTRT）

「Gamaredon（ガマレドン）」は2013年頃から活動していると言われる、標的型攻撃のグループです。このグループはこれまで、ウクライナの政府機関に対して集中的にサイバー攻撃を仕掛けてきたことで知られています。しかしトレンドマイクロでは2020年3月、Gamaredonのものと思われるマルウェアを添付したメールが日本国内において複数回着弾するのを観測しました。また、ハンガリー等欧州諸国にも同様のマルウェアが着弾した可能性があります。Gamaredonは2018年秋頃から活発化し、2019年夏以降はさらに活発化しているとみられ、今回Gamaredonが活発化する中で日本も攻撃対象に含められたのか、あるいは偶然に「流れ弾」が着弾しただけであるかの判断には至っていません。ただし、ワーストケース（＝日本が攻撃対象に含まれたこと）を想定し、このブログ記事ではGamaredonとその攻撃手法について報告します。

●標的型攻撃グループ「Gamaredon」による日本への攻撃を初観測
https://blog.trendmicro.co.jp/?s=Gamaredon

- 2019年12月頃から日本を標的として利用されている遠隔操作ツール「LODEINFO」を拡散するメールで悪用

コロナに便乗した脅威 - 法人組織を狙った事例②

ビジネスメール詐欺での悪用（グローバル）

Good morning Paul,

How are you? (I hope that everything is okay)

Following the dramatic situation in Europe and in many countries,I am personally managing a financial operation in collaboration with the Valther Avocats in France.

Mr.Theron is representing them.

I will need you to assist him,and give him the necessary support on the subject.

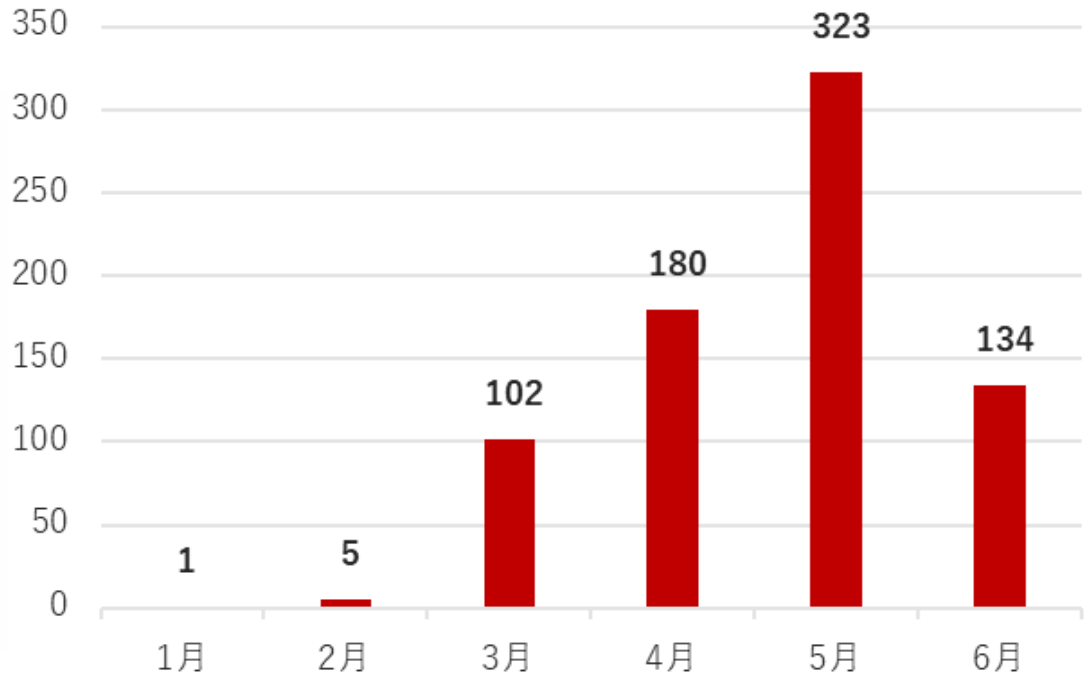
It is important to manage this file ASAP because we are already late due to the corona situation...

This file is confidential for the moment, I count on your absolute discretion.

Mr.Theron was suppose to contact you this morning, has it been done ?

Kind regards,

■図：COVID-19関連の内容を含むBECメールの本文例



■図：全世界におけるCOVID-19関連*の文言が含まれる
ビジネスメール詐欺（BEC）のメール検知数推移
（2020年、トレンドマイクロSPNより）

※抽出条件：ファイル名に”covid”、”covid-19”、”ncov”、”coronavirus”を含むもの

コロナに便乗した脅威 - 個人を狙った事例

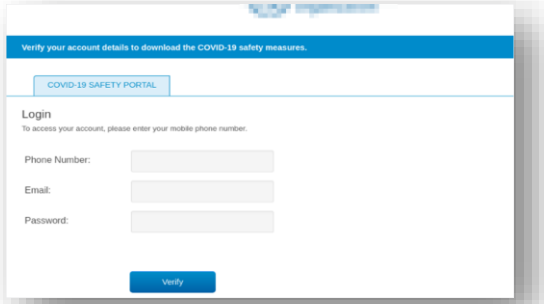
マスク不足や給付金に便乗するフィッシングサイト・SMS（国内）

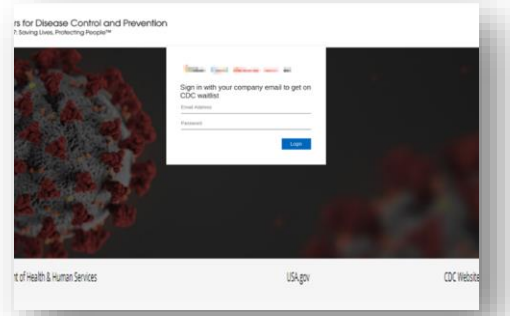
■図：マスク送付を騙るSMS（2020年2月確認）

■図：マスク販売を騙る不審サイト（2020/3/5に確認）

■図：「コロナ対策補助金」メールから誘導される当選詐欺サイト（3/12, 4/7確認）

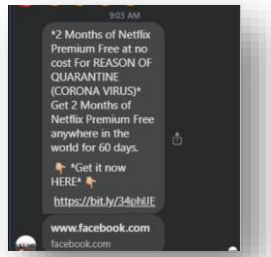
公的機関を装ったフィッシングサイト（グローバル）



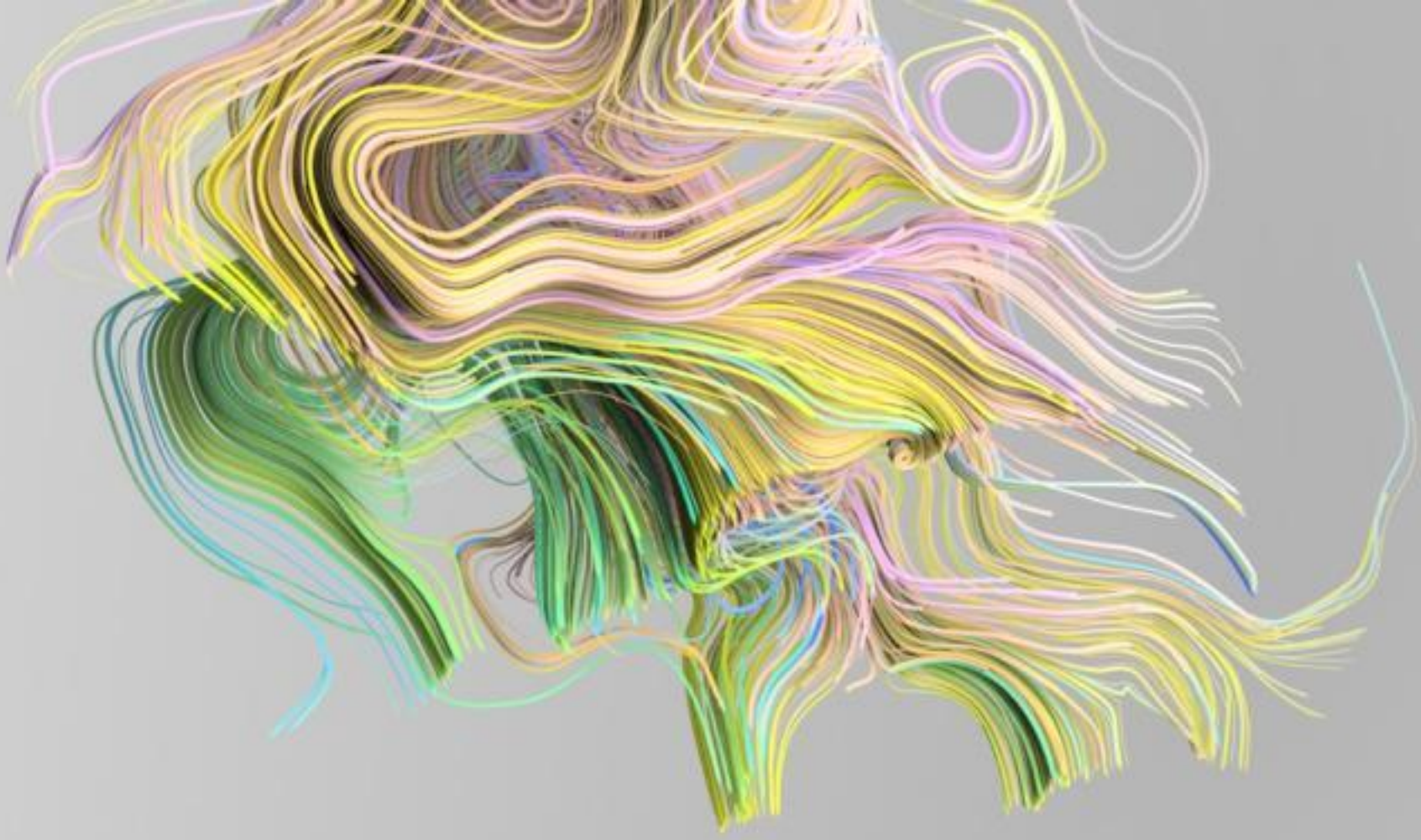


■図：WHO・CDCを偽装したフィッシングサイト

ソーシャルメディア上での不正な投稿（グローバル）



■図：Facebook MessengerでNetflix 2か月無料を謳う不正なメッセージ



4. サプライチェーン攻撃事例

SolarWinds Orionを介したサイバーインシデント

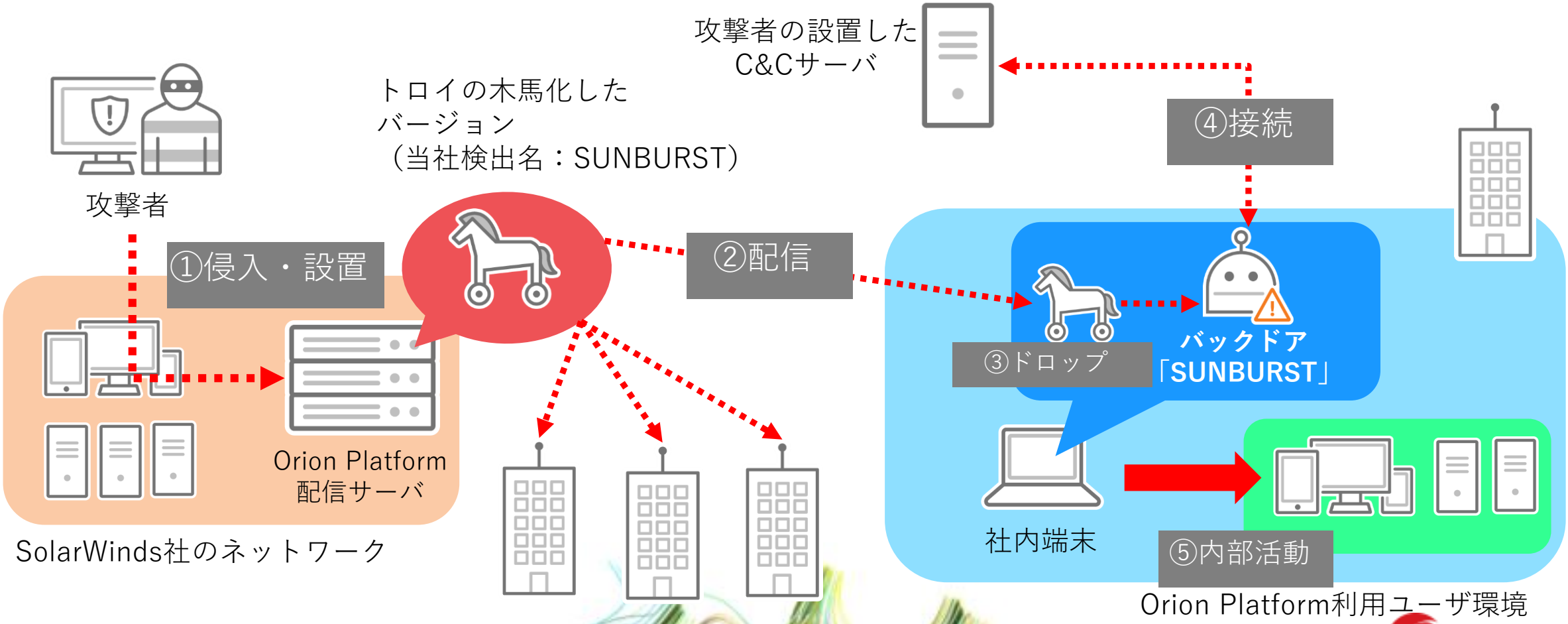
- 米財務省を含む2つの米政府機関がサイバー攻撃を受けたと発表
  - 2020/12/13に公表、数か月に渡りネットワークへの侵入があった
  - SUNBURSTと呼ばれるバックドアを使用された
  - IT管理/監視プラットフォームであるSolarWinds Orionのアップデート機能を悪用し、ソフトウェア利用者の端末にバックドア(SUNBURST)を感染させる

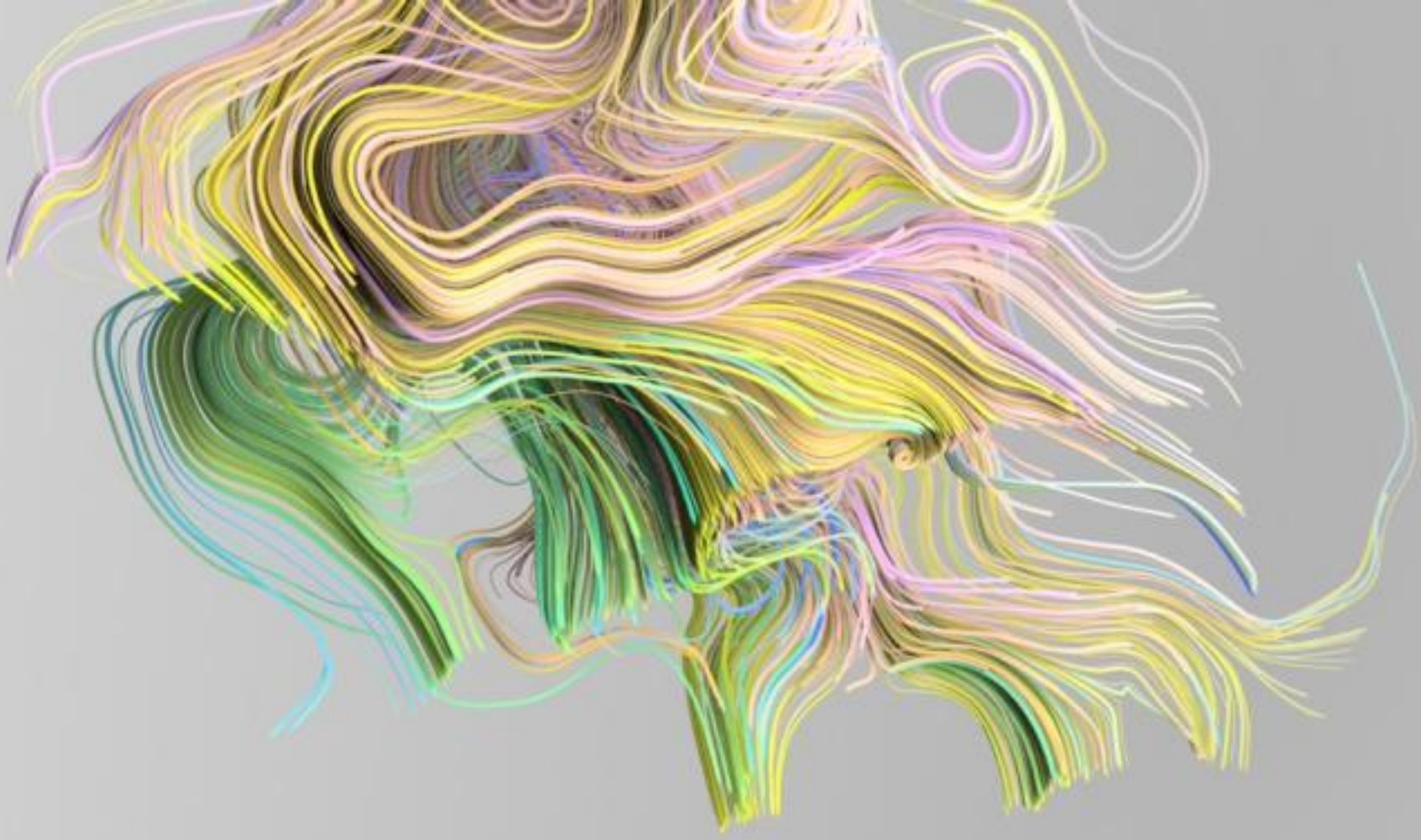
https://www.afpbb.com/articles/-/3321124
https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html
https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks

- 製品のアップデート機能を悪用してマルウェア感染させる手口は以前から確認されている
  - GOM PlayerやASUS等の事例が過去に確認されている

攻撃の全体像

◆バックドア型マルウェア「SUNBURST」を用いた攻撃イメージ図





5. テレワークの弱点を狙う脅威

テレワークの弱点を狙う脅威

- テレワークで使用するソフトに便乗する攻撃
- テレワークで使用するサービスの認証情報を狙う攻撃
- テレワークで利用される経路を狙い侵入する攻撃

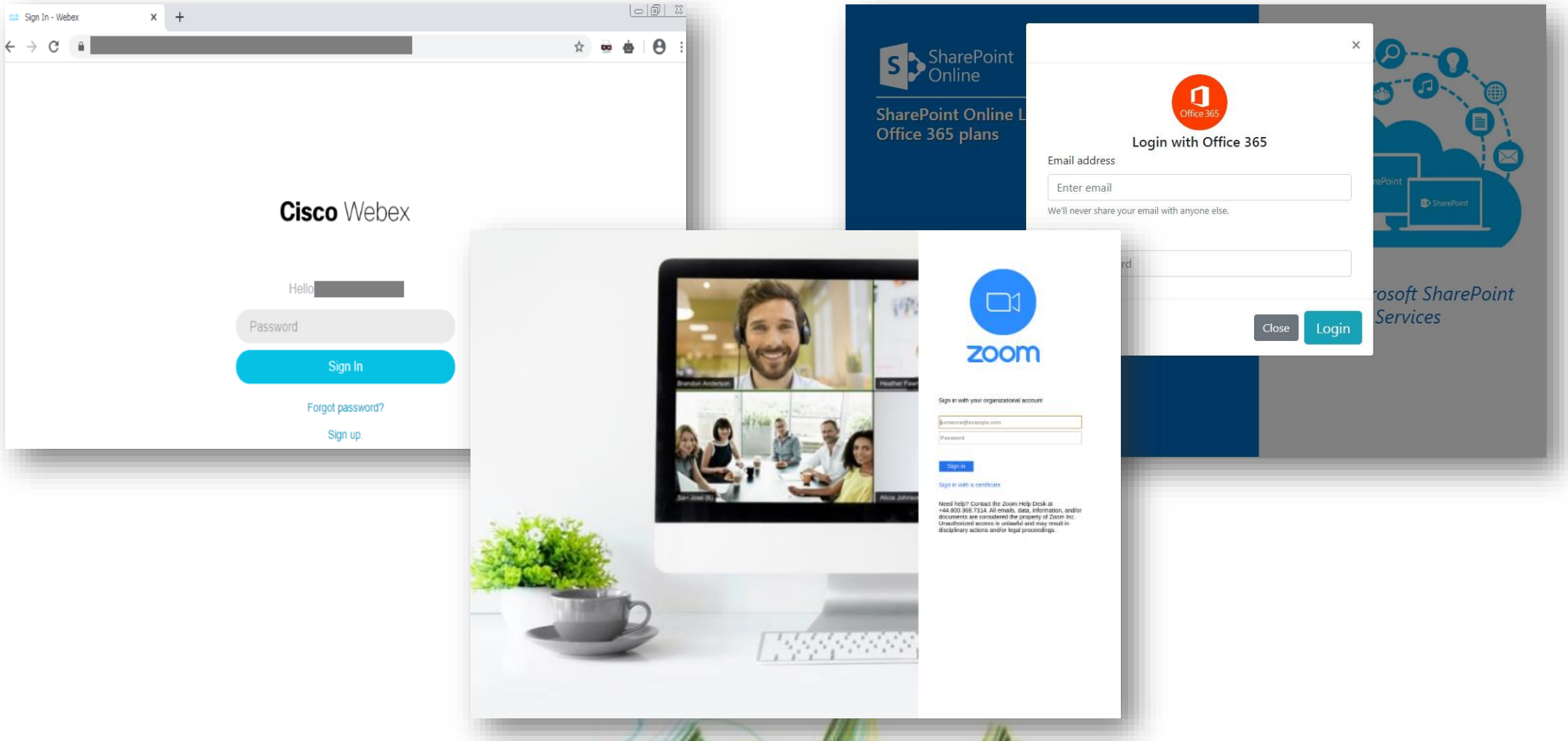
テレワークで使用するソフトに便乗する攻撃

- ビデオ会議ソフトの偽インストーラを偽装し、正規のソフトウェアと共にマルウェアをインストールさせる手口
  - 正規のソフトウェアがダウンロードされるため、**被害者は自身が感染したことに気付きにくい**
  - いずれも正規サイトではなく不審なWebサイトで配布されている
  - 確認された例：コインマイナー、バックドア、RAT

有効な対策：

- アプリは正規サイトから入手する
- 基本的なセキュリティ対策
  （メール対策、Web対策、マルウェア対策）

テレワークで使用するサービスの認証情報を狙う攻撃

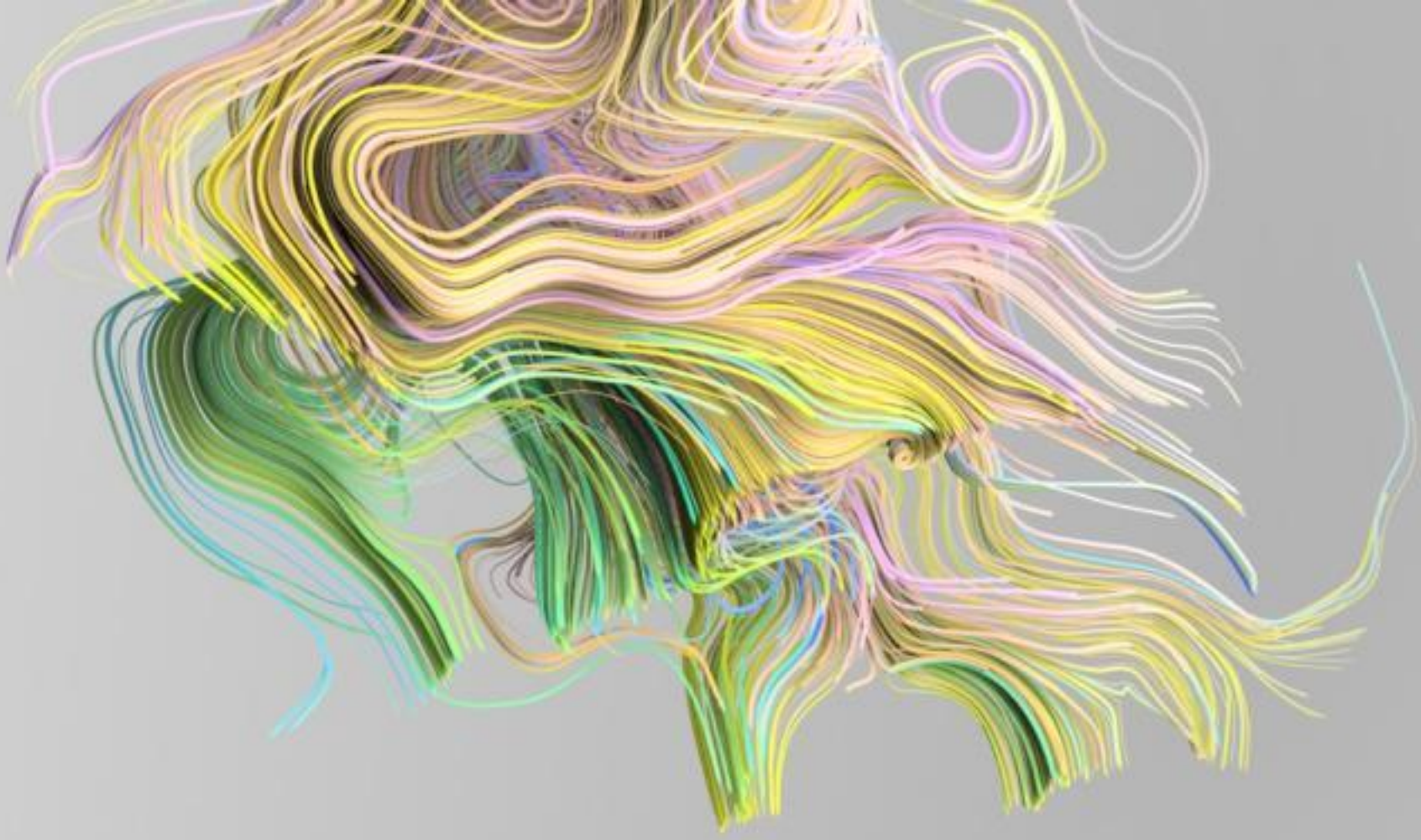


テレワークで利用される経路を狙い侵入する攻撃

- 社外からのアクセスするための仕組みが狙われる
  - 仕組み：VPN、VDI、RDP（リモートデスクトップ）など
  - 攻撃方法：脆弱性攻撃、詐取情報を使用した認証突破、持ち出しPCへの感染

有効な対策：

- サービス・ソフトウェアの最新バージョンへの更新
- 認証強化やアクセス制限の実装
- ログ監視、ネットワーク監視の強化
- 基本的なセキュリティ対策（メール対策、Web対策、マルウェア対策）



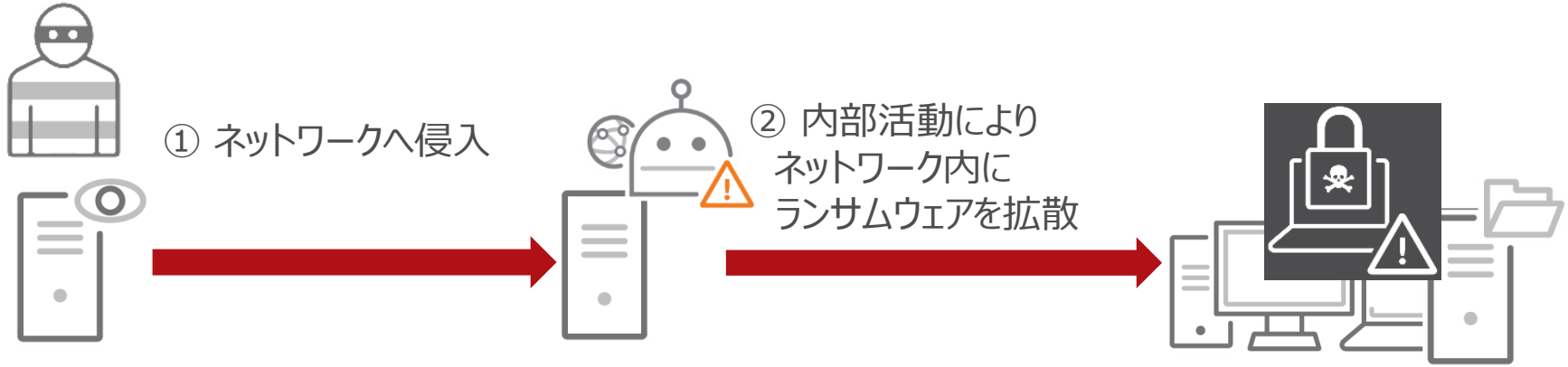
6. 対策ポイント

被害に遭わないためには

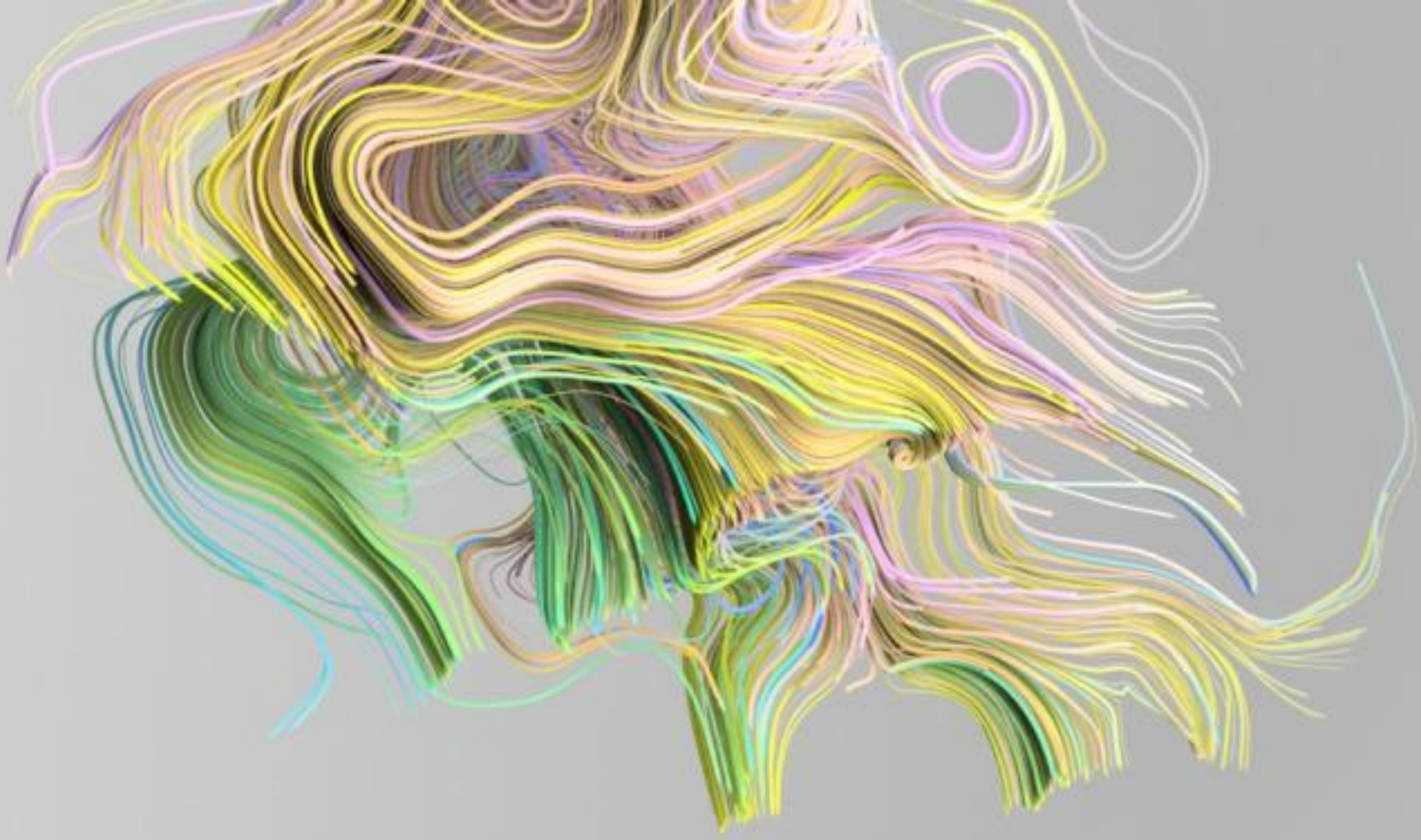
1. セキュリティ対策製品を常に最新に保つ運用の徹底
   - 不正メール、不正サイト、不正ファイル対策機能の利用
2. 脆弱性対策
   - ネットワーク内外の脆弱性対策
3. 不正な活動の監視
   - ログの保存および定期確認
   - サーバでの侵入・改ざん防止やログ監視機能の利用
   - 内部の不審を可視化するためのネットワーク監視
   - 認証強化やアクセス制限などの不正ログイン対策
   - 意図せず露出しているポートの把握
4. 重要なファイルのバックアップ

対策のポイント

- 昨今のランサムウェア事例では、攻撃者による侵入と内部活動によりランサムウェアがネットワーク内で拡散し、被害拡大したと推測される
  → 標的型攻撃対策と同じ多層防御が重要



※従来からの基本的なランサムウェア対策については以下のサポート情報をご参照ください
「ランサムウェア対策のベストプラクティス」
https://success.trendmicro.com/jp/solution/1114803



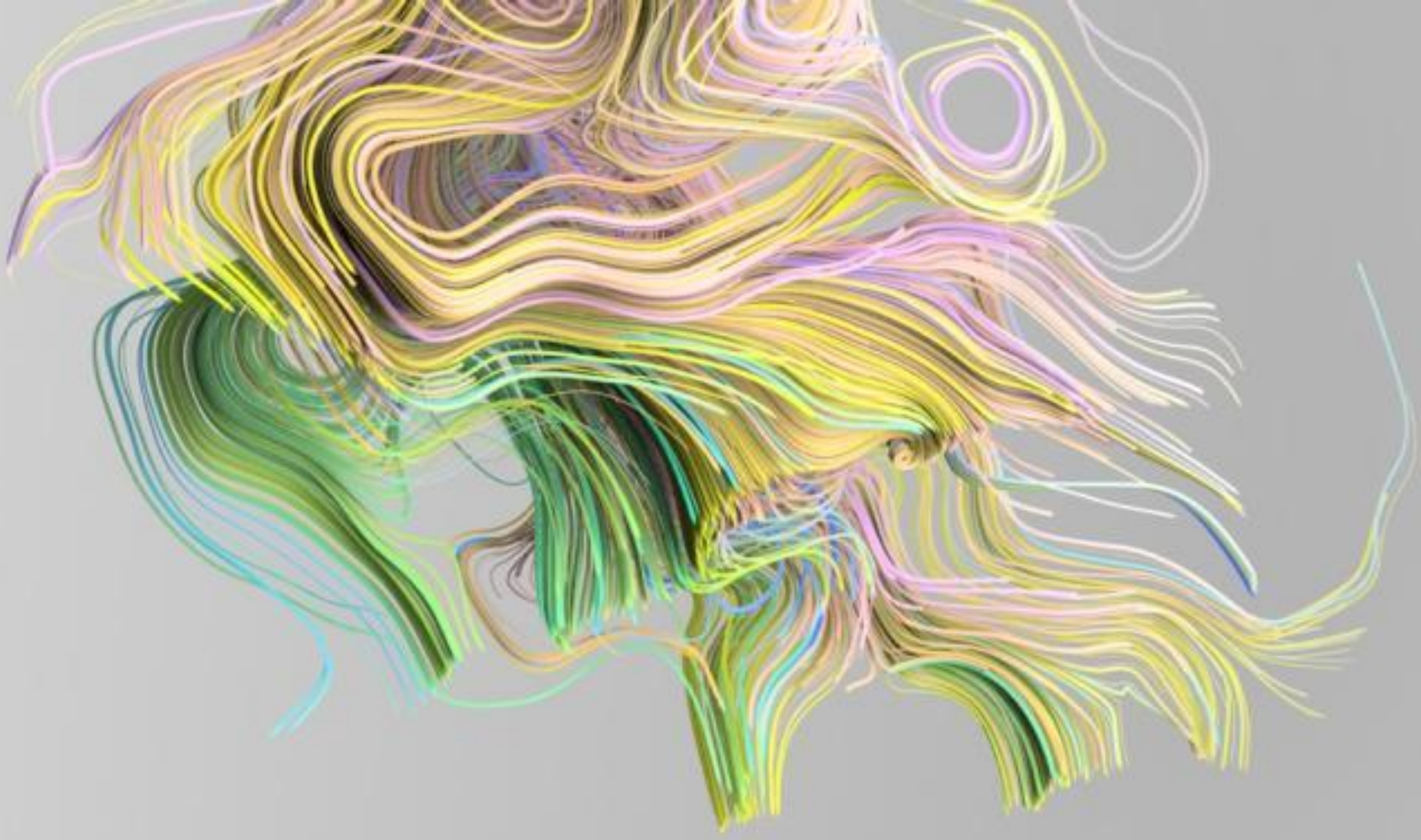
7. まとめ

まとめ

- 最新の攻撃手法を知ることで、対策に活かすことできる
- ランサムウェアによる攻撃の被害にあった場合、データが暗号化されるだけでなく、情報が暴露され、身代金が要求されることがある
- 新型コロナウイルス等の状況変化に便乗した脅威、サプライチェーン攻撃、テレワークの弱点を狙う攻撃にも注意が必要

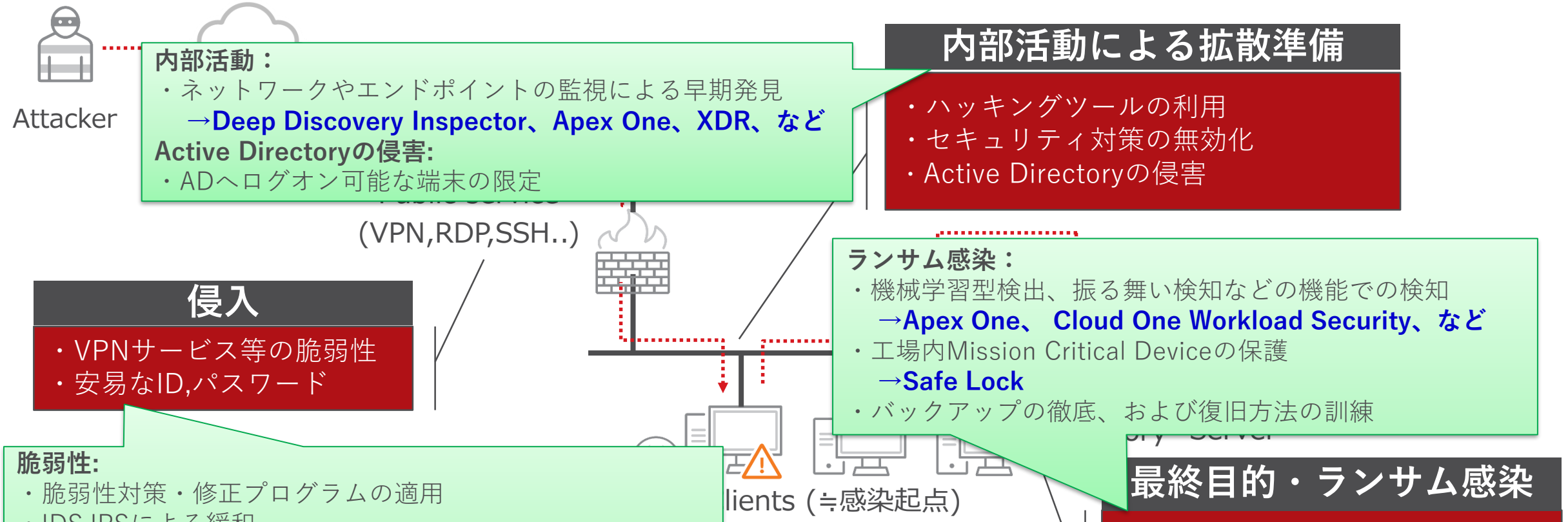
ありがとうございました

TREND MICRO



Appendix

技術的ソリューションのポイント



トレンドマイクロの検出対応

- 従来型検出（パターンマッチング）
- 機械学習型検索
- 挙動監視：ファイル暗号化の活動を検出しブロック
- サンドボックス

パターン未対応段階でも
複数技術で検出可能