米国国防省が求める脅威インテリジェンスの世界

2019年11月7日（木） | 13:25 - 14:10 | Room 1

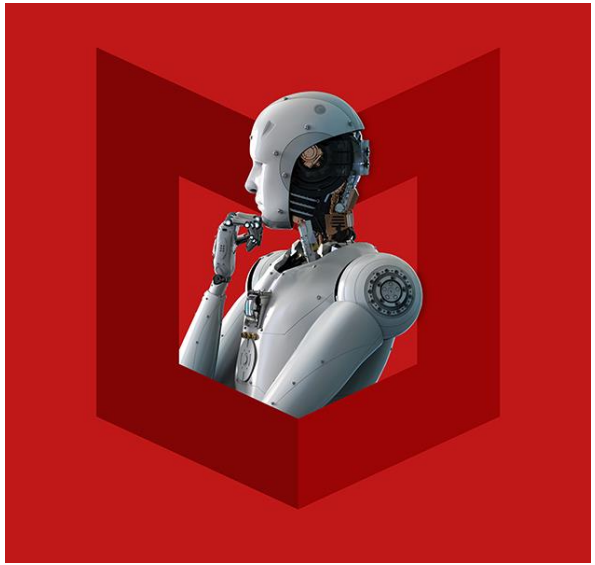
ライアン・シャーストビットフ
McAfee, LLC
アドバンスドスレットリサーチ
セキュリティリサーチャー

講演者

ライアン・シャーストビットフ
McAfee, LLC
アドバンスドスレットリサーチ
メジャーキャンペーン担当シニアアナリスト

アジェンダ

- マカフィーの脅威調査とインテリジェンス
- 標的型攻撃までの道筋を分析する
- 国家の支援を受けているサイバー犯罪集団「Hidden Cobra」 / 「Lazarus」の正体に迫る



マカフィーの脅威調査部門

MPOWER CYBERSECURITY SUMMIT

- マカフィーには、脅威調査とインテリジェンスにフォーカスした技術部門が複数存在。各部門のミッションは少しずつ異なる。
  - **マカフィー アドバンスドスレットリサーチ（*McAfee Advanced Threat Research: ATR*）**
    - 一般人を狙う脅威の調査
    - 出版物や講演を通じたソートリーダーシップの開発
    - 国際警察機構によるサイバー犯罪撲滅活動への協力
    - 脆弱性の調査と開示
  - **マカフィー アドバンスドプログラムズグループ（*McAfee Advanced Programs Group: APG*）**
    - サービスとしてのインテリジェンス（INTAAS）
    - Global Threat Intelligence（GTI）プライベートクラウド
  - **マカフィーラボ マルウェアオペレーションズ （*McAfee Labs Malware Operations*）**
    - セキュリティコンテンツ（脅威の検知・防御）に関連する調査
    - お客様からの脅威に関するエスカレーションとオンデマンドでのコンテンツ生成

アドバンスド スレットリサーチ（ATR）の業務内容

大規模キャンペーンやマルウェアの調査

- 国家の支援を受けている犯罪集団やサイバー犯罪活動の調査と情報開示
- 著名なキャンペーンの背後にある脅威や攻撃者を明らかにするための、一般人を狙った脅威の研究を通じた、ソートリーダーシップの形成
- マカフィーのお客様や、さらにはサイバーセキュリティコミュニティにとって信頼の置けるアドバイザーとしての存在
- 国際警察機構による捜査や犯罪撲滅活動への協力

アドバンスド スレットリサーチ（ATR）の業務内容

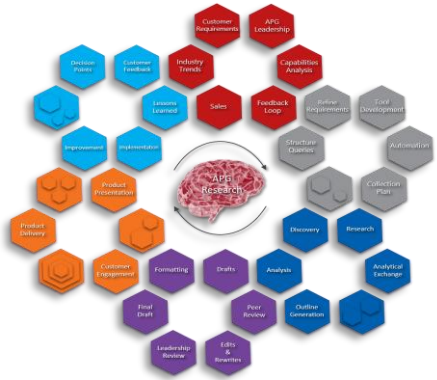
脆弱性調査

- 次世代テクノロジーに潜む新たな脅威（スマートビル、自動運転車、衛星テクノロジーなど）
- 明確に定義されたテクノロジーおよび／またはレガシーテクノロジー（各種業界のハードウェア、ソフトウェア、ネットワーク化された製品など）に特化した脅威調査
- さまざまな攻撃における実際の脅威情勢に基づいた、偏りのない攻撃的な脆弱性の調査
- 実証実験から完全なるデモまで、常に攻撃者が最大限影響を与え、最大限見返りを得るために活用するであろうシナリオを提示
- 最先端のハードウェア調査研究所：特殊なハードウェアベースの調査や分析に対応
- 現在の注力分野：敵対的機械学習、スマート製品、産業制御システム、医療テクノロジー、コンシューマーデバイスなど

アドバンスドプログラムズグループ（APG）の現在の業務内容

アドバンスドプログラムズグループ（APG）：「信頼の置けるアドバイザー」

- **サービスとしてのインテリジェンス（INTAAS）**
  - カスタムインテリジェンスレポート
  - 全域にわたっての情報収集サービス
  - ATRレポートに関する高度な通知
  - お客様独自の要件に基づく
  - 顧問契約形態、またはお客様オンサイトのAPGアナリストサポートとして課金
- **プライベートGTI（pGTI）**
  - 隔離されたネットワークを使用しているお客様用に開発されたプライベートGTIインスタンス
  - お客様の要件に基づき、小・中規模から大規模なイタレーションを実施
- **案件ごとにダッシュボードモジュールをパッケージング**



APGのインテリジェンスサイクル

MPOWER CYBERSECURITY SUMMIT

原理上のアプローチ

計画と方向性

- お客様はインテリジェンスを利用できる状態にあるか？
- サイバー攻撃／脅威を特定し、一連の活動や条件を確認して、攻撃者を明らかにする
- 契約締結

活用

- セキュリティプロトコルの更新／強化やLE対応など、エンドユーザに対して、一連のアクション機能を提供
- 新たな要件や再攻撃の特定

収集

- 開発チームのエンジニアが、要件に特化させた機能を開発および活用
- 内外のソースから収集した情報を集約
- 開発チームが複雑な技術データを実用的な情報に変換
- 継続的な要件の改善とデータ収集

流布

- プライベートリリースに限定もしくはNDA

処理と利用

- 収集したデータを理解可能な形式に変換（豊富でテキストベースのデータから視覚的な図表へ）、アトリビューション
- オールソースアナリシス、テクニカル分析、リバースエンジニアリング、マルウェア解析の分野における35年以上の経験を集約

生産

- 図表、データ、業界レポートを統合し、攻撃／脅威に対する包括的な対応策を生成
- 博士号保有者やプリンシパルエンジニアが編集
- エグゼクティブ向けに記述

アジア太平洋地域の脅威情勢

- 日本およびアジア太平洋地域を含むさまざまな地域を対象としたATRの高度なモニタリング活動を通して得られる地域ごとの脅威に関するインサイト
- 各種偵察行為からリモートデスクトッププロトコル（RDP）その他の不正トラフィックが発生していることを継続的に確認
- 攻撃者は、日本、韓国を始めとする各国の環境をスキャンし、侵入口を探している

標的型攻撃までの道筋

MPOWER CYBERSECURITY SUMMIT

- リモートデスクトッププロトコル（RDP）に対する攻撃は、標的を定めた侵入の糸口となる
- 高度な攻撃者は、この方法を使って被害者の環境への侵入口を発見
- ATRは、そうした侵入の詳細やその後の活動を追跡

- 侵入された結果、 Active Directoryの侵害、認証情報の窃盗、知的財産の窃盗など、さらに深刻な侵害に至る可能性がある
- さらなる追加攻撃に活用できる標的を見つけるために、 RDPスキャンツールが使われている
- ATRの調査から、深刻な侵害を引き起こす可能性がある安全ではないリモートデスクトップ設定のまま、多くの資産が放置されていることが判明

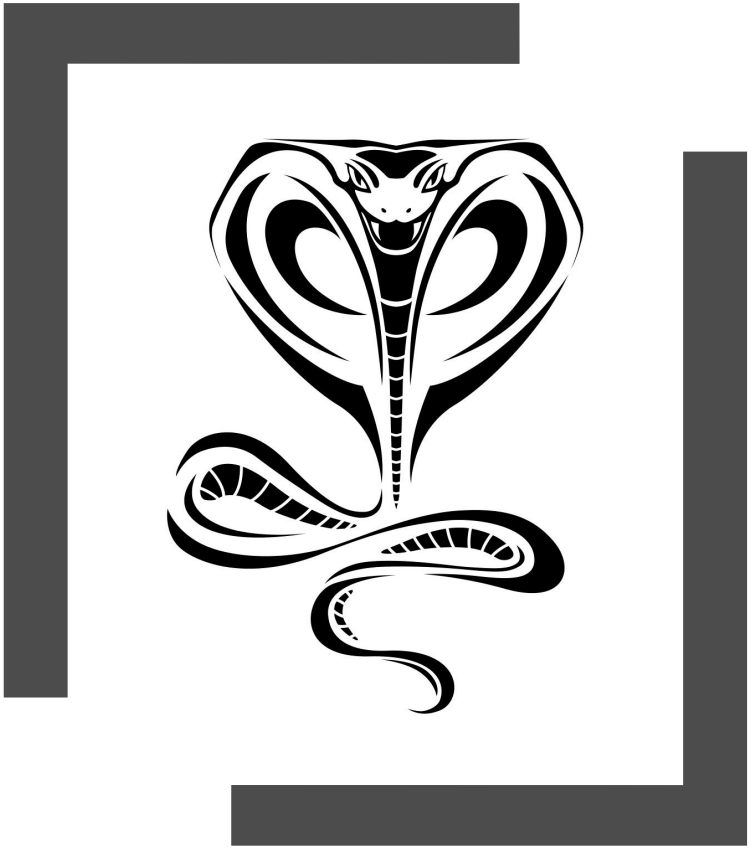
攻撃者の追跡

- 攻撃者やその進化するトレードクラフト（Tradecraft）の追跡は、ATRの主要業務の1つ
  - トレードクラフトは経時的に進化する可能性があるため、時系列に沿って追跡することが重要

- ATRの攻撃者追跡方法
  - データから得られるインサイト（テレメトリに対するビッグデータ分析）
  - 攻撃者によるコード使用法の進化 – 過去に該当のコードまたはその一部が確認されていないか
  - 被害者情報と標的設定の変化

トレードクラフト（Tradecraft）を追跡する理由と価値

- トレードクラフト：攻撃者がサイバー空間で使用しているインテリジェンス収集技術
- 攻撃者の行動パターンを時系列に沿って明らかにすることが可能
- 監視対象の攻撃者に特有な行動を見つけるための指標
- 「Hidden Cobra」：ATRがトレードクラフトの特定において注目していた攻撃集団の1つ



「Hidden Cobra」について

- 「Hidden Cobra」：広域に渡ってサイバー活動を展開しており、北朝鮮と関係しているといわれる犯罪集団に対する米国政府の呼称
  - 「Lazarus」、「Andariel」および「Blueonoff」の活動も含まれる
  - 全集団がHidden Cobra傘下にあるが、各集団の目的は異なる
- 金銭目的の攻撃と防衛企業基盤（DIB）を狙う攻撃
- マカフィーは 「Operation Troy」に関するレポートの発表後、継続的な追跡と監視を実施

「Hidden Cobra」によるサイバー脅威の概略

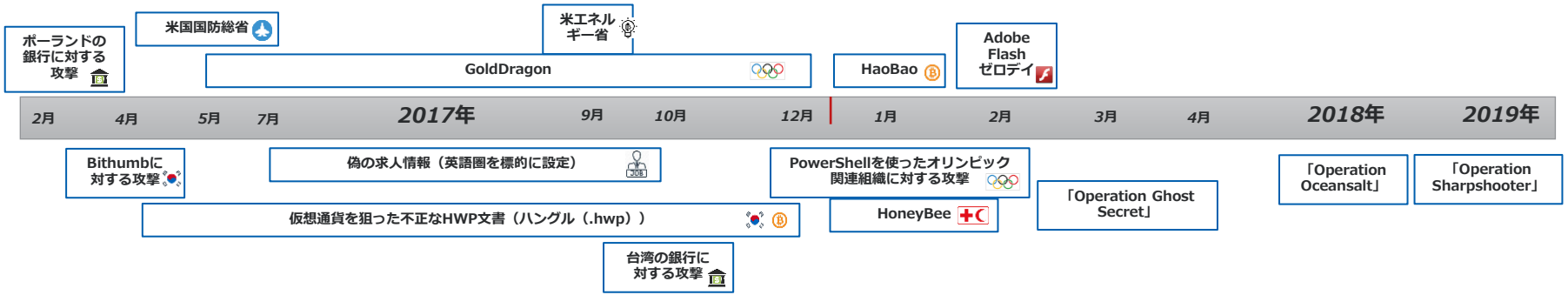
MPOWER CYBERSECURITY SUMMIT

- Hidden Cobraは2009年から韓国／米国を標的としてデジタルサイバー戦争活動を展開
- Hidden Cobraによるものとされる主な攻撃
  - 「Dark Seoul」（サイバーテロ攻撃）：2013年
  - 「Operation Troy」（対軍スパイ活動）：2009年～2013年
  - ソニー・ピクチャーズ（北朝鮮に否定的なメディアへの報復行為）：2014年
  - 南カリフォルニアのエネルギー企業（攻撃計画）：2014年
  - 韓国のエネルギー分野（攻撃計画）：2014年／2015年
  - バングラデシュの銀行への攻撃：
  - 世界的なWannaCry攻撃：
  - 仮想通貨交換所を狙った攻撃：
  - 「Operation Ghost Secret」
- 2018／2019年、Hidden Cobraは精力的に金銭目的の活動を展開

サイバー集団「Hidden Cobra」に関するインサイト

- 精度や標的範囲が進化している脅威集団
  - 韓国以外も標的に設定
  - 目的が異なる複数の下部組織が確認されている
  - 金銭目的へと方向性が転換したことで、Hidden Cobraが分散化
  - 韓国語以外の言語も標的に設定

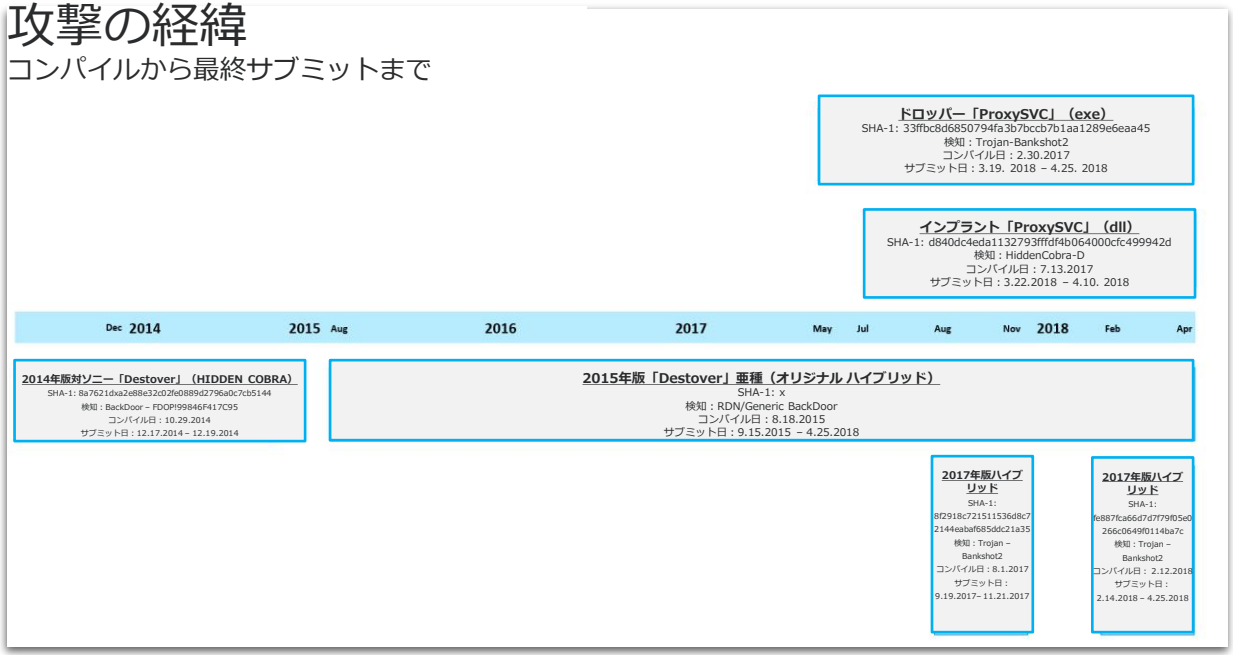
「Hidden Cobra」による活動の履歴



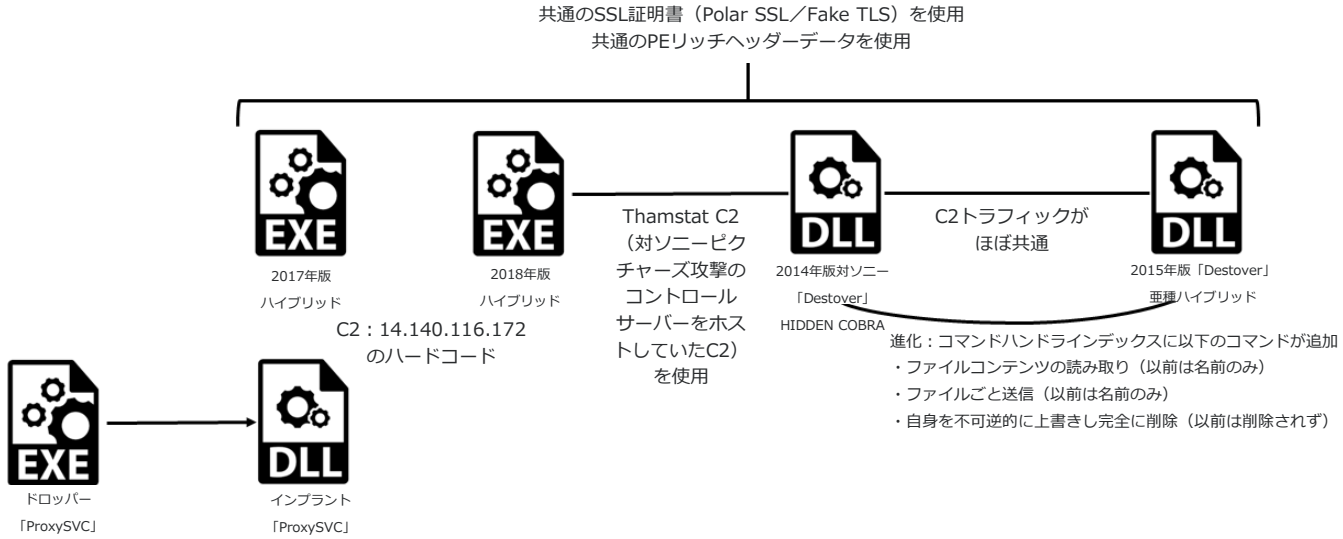
ATRが調査した活動

攻撃の経緯

コンパイルから最終サブミットまで



「Operation Ghost Secret」の内幕



「Operation Ghost Secret」の技術的つながり

「Operation Ghost Secret」の技術における重要なポイント

インプラントが重要なポイント

2014年版対ソニー「Destover」

HIDDEN COBRA

8a7621dba2e88e32c02fe0889d2796a0c7cb5144

・**PEリッチヘッダデータ**と**SSL証明書**が以下と共通：
- ・2015年版「Destover」亜種ハイブリッド
- ・2017年版ハイブリッド
- ・2018年版ハイブリッド

2015年版「Destover」亜種ハイブリッド

7fe373376e0357624a1d21cd803ce62aa86738b6

・**PEリッチヘッダデータ**と**SSL証明書**が以下と共通：
- ・2014年版対ソニー「Destover」
- ・2017年版ハイブリッド
- ・2018年版ハイブリッド

・**進化**：2014年版以降、コマンドハンドラーインデックス内のコマンドが増えている
- ・ファイルコンテンツの読み取り（以前は名前のみ）
- ・ファイルごと送信（以前は名前のみ）
- ・自身を不可逆的に上書きし完全に削除（以前は削除されず）

・また、以下と**同じコード**を含む
- ・2015年版「Destover」亜種ハイブリッド
- ・2017年版ハイブリッド

2017年版
ハイブリッド

8f2918c721511536d8c72144eabaf685ddc21a35

・**「ProxySVC」**と共通の**C2**（14.140.116.172）を使用

・**PEリッチヘッダデータ**と**SSL証明書**が以下と共通：
- ・2014年版対ソニー「Destover」
- ・2015年版「Destover」亜種ハイブリッド
- ・2018年版ハイブリッド

・**影響を受けた業界**
- ・電気通信　・ヘルスケア　・金融　・重要インフラ　・エンターテイメント

・以下と**同じコード**を含む
- ・2015年版「Destover」亜種ハイブリッド
- ・2017年版ハイブリッド

2018年版
ハイブリッド

fe887fcab66d7d7f79f05e0266c0649f0114ba7c

・C2：203.131.222.83

・**PEリッチヘッダデータ**と**SSL証明書**が以下と共通：
- ・2014年版対ソニー「Destover」
- ・2015年版「Destover」亜種ハイブリッド
- ・2017年版ハイブリッド

・以下と**同じコード**を含む
- ・2015年版「Destover」亜種ハイブリッド
- ・2017年版ハイブリッド

インプラント「ProxySVC」

ドロッパー「ProxySVC」

d840dc4eda1132793fffdf4b064000cfc499942d

・2017年版ハイブリッド型原種と共通のC2（14.140.116.172）を使用

・マカフィーのテレメトリ分析は主に**高等教育機関**で登場

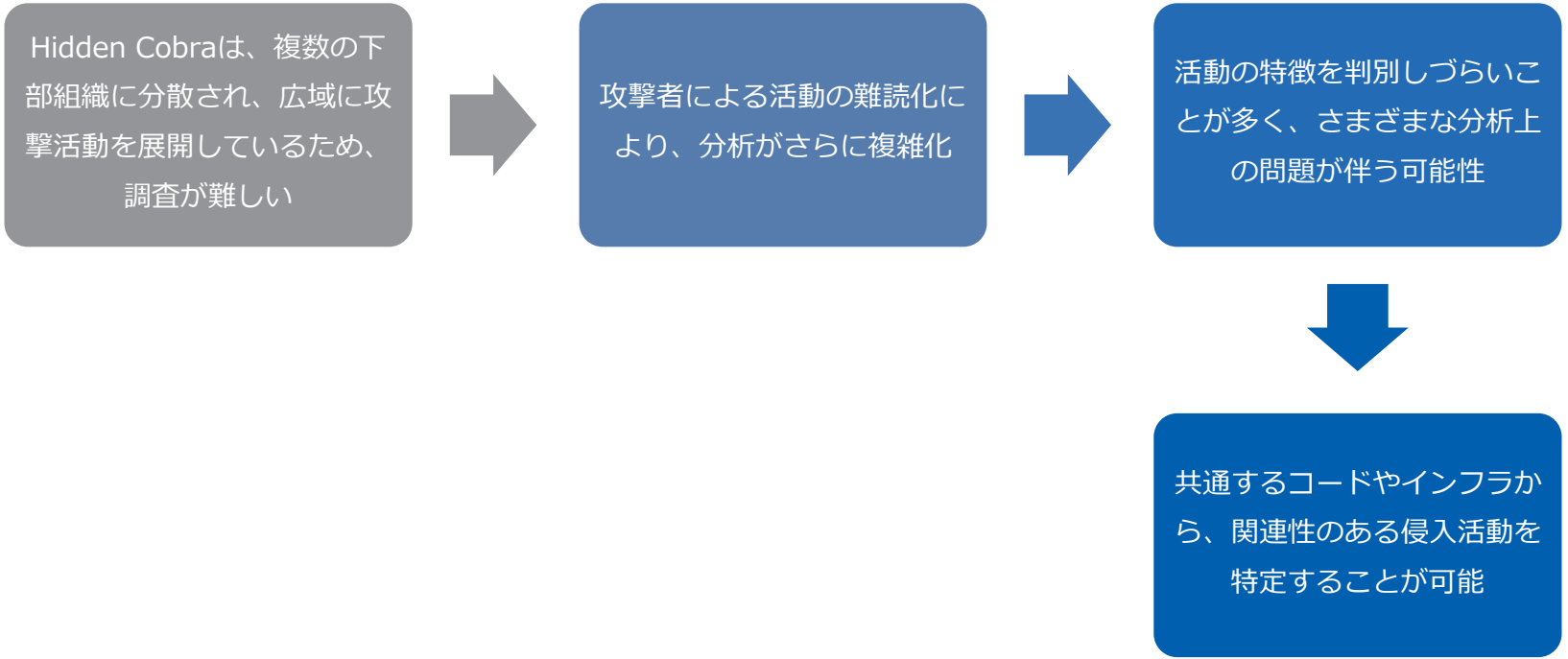
・「ProxySVC」：偵察とその後のペイロード送信を目的として、443ポートにバインドおよびこれをリッスンしてC2接続と機能を提供する**データ収集インプラント**

・この**SSLリスナー**によって、ハードコードされたIPアドレスへの依存性を解消し、インバウンドの接続のみを受け入れることで、複数のコントロールサーバー接続に対応。これにより、コントロールサーバーの匿名性を確保

・**IPアドレスのブラックリスト**を保持し、外部からの接続を点検

・「ProxySVC」は、主に攻撃者のコントロールアドレスを漏らすことなく、エンドポイントにペイロードを追加送信するためのダウンローダーと思われる

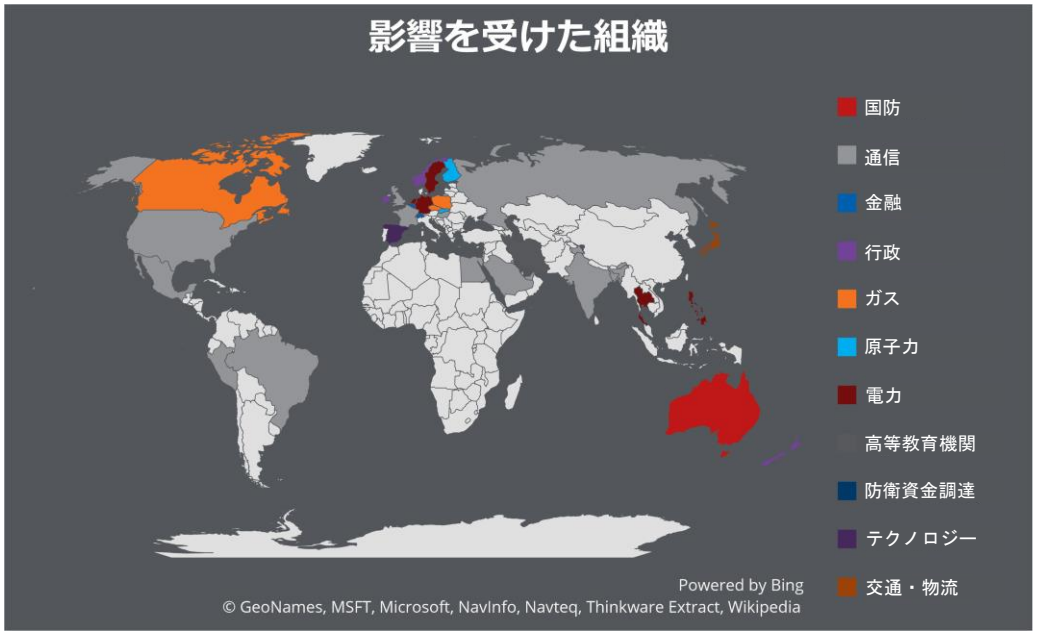
我々は何を学んだのか


Hidden Cobraは、複数の下部組織に分散され、広域に攻撃活動を展開しているため、調査が難しい
攻撃者による活動の難読化により、分析がさらに複雑化
活動の特徴を判別しづらいことが多く、さまざまな分析上の問題が伴う可能性
共通するコードやインフラから、関連性のある侵入活動を特定することが可能

実際にHidden Cobraの追跡は可能か？

MPOWER CYBERSECURITY SUMMIT

- マカフィーATRは、データから得られるインサイトや脅威中心のテレメトリを通して、攻撃者の影響力が最も大きい場所を特定可能
- 分析によって、世界各地で展開されている攻撃活動を特定可能
- ATRによるコードや類似性の分析により、埋め込まれたコードやその進化を追跡可能
- Hidden Cobraのケースでは、インサイトのデータを使ってインプラントである「Rising Sun」を追跡



「*Operation Sharpshooter*」の