インテリジェンスコミュニティーの最前線から見た脅威の現状と日本

Bob Gourley
29 May 2019
bob@ooda.com

プレゼンテーションについて...

- 最新のサイバー脅威に対する洞察
- サイバーセキュリティ分野における新興分野の展望：
  人工知能のセキュリティ
- 実用的な提言のまとめ

脅威について

私達が今日目にしているもの:

- フィッシングはいまだ主要な方法、、、同情と好奇心の人間の特性を悪用します。
- 敵対者は戦術を変えます。フィッシングが機能しない場合は、他にもたくさんの方法があります。
- ここにIoTがあります、、、しかしIoT デバイスは安全に出荷されていません。
- ランサムウェアは進化していて予防や対処が難しくなっています。
- モバイルデバイスの脆弱性：アカウント情報を取得するために悪用されます。
- **敵対者もハードウェアの脆弱性を悪用する**（Spectre and meltdown）
- 国家はより露骨になっています。ロシア、中国、イラン、北朝鮮が主な追跡対象。

新しいハイテク“冷戦”なのか？

- 開かれた社会（USと日本を含む）は閉ざされた社会（ロシア、中国、北朝鮮を含む）からのサイバー脅威に気づき始めています。
- USではNDAA（国防権限法）が中華人民共和国政府の南シナ海の好戦的行為のみならずサイバーの位置づけに対する深い懸念により変わりました。
- 数十年来の中華人民共和国政府支援の知的財産の窃盗の後、USは2013年より法的措置を取り始めました。
- 中華人民国政府支援の企業による国際的犯罪やスパイ行為が捜査され、共産党が対応しました。
- 中華人民共和国製品に対するUS関税はハイテク製品を含みます。
- ZTEの規制や現在のファーウェイの規制は長年の研究の結果です。
- 中華人民共和国は独自のスマートフォンOSを作ると予測されます。

近い将来

- フィッシング詐欺に対する防御と戦術は変わりますが、フィッシング詐欺は依然として重要な方法です。
- フィッシング以外にも他の方法が常に存在します。不正なデバイス、サプライチェーン、物理的アクセスは常に狙われます。
- 中規模企業が中心的ターゲットです。
- **サイバーインシデントだけでなく、成長するインサイダーの脅威。従業員の過激化を防ぐ必要があります。**
- **閉ざされた社会はネットワークのスパイ活動による利益を常に探し続けます。**

アクション: 敵を知る

- 驚きに備える: 歴史と現在の脅威の研究の双方からの大きな教訓。驚かないように、事件対応計画を立てそれを練習しておきましょう。

- 敵対者にも弱点があることを知る: 彼らも、防御側と同じ物理法則に従わなければなりません。彼らがあなたのネットワークにいるとき、彼らはあなたに有利な芝生の上にいます。あなたの防御が弱点を利用できるように十分機敏であるようにしましょう。

アクション: 己を知る

- 自分の組織を知る: 評価と理解: 組織の機能にとって最も重要なデータ、システム、および機能を把握し、それらの状態を継続的、自動的に認識しましょう。

- チームに勝つにはチームが必要: 現代のサイバー犯罪集団や国家の技術的才能に匹敵する組織はありません。今すぐ信頼に基づくチームを構築しましょう。あなたの防御のために他の組織の力を活用しましょう。セキュリティの専門家、法執行機関、クラウドサービスプロバイダ。

- 自身をテストする: 独立したアセスメントと現実的なトレーニング/評価による（机上の演習）

アクション: 防御力を上げる

- 防御を強化する: サイバースペースの敵対者は革新を続けています。つまり、私たちは防御を見直し現代化し続けなければなりません。構成管理の自動化、検出の自動化、応答の自動化。

- 封じ込めの設計: システムが敵対者を封じ込めるように設計されている場合は、早期検出と迅速なインシデント対応が可能になります。攻撃の封じ込めは悪意のあるコードで特に重要です。IoTデバイスはセグメント化が不可欠です。

- バックアップを確保する: 重要なシステムはすべてバックアップを取り、回復方法を定義してテストする必要があります。

セキュリティの自動化

- 前のスライドの項目：
  - 敵を知る
  - 己を知る
  - 防御力を上げる

- これらはすべて自動化する必要があります
- 全社にわたり、デスクトップからサーバーまで
- 新しい攻撃に備えるためにAIベースの機能が必要です
- 多層防御がキーとなります

AIからの新しい脅威

AIとは何か?

実務家の視点から見たAI:

- AIは思考機械の実世界の問題への応用です。

この観点から、AIは結果がすべてです。そして科学であると同時に芸術でもあります。

システムの観点からのAIの理解

技術要素:

- 分析アルゴリズム (機械学習、深層学習を含む)
- 自然言語処理
- ロボット工学
- コンピュータビジョン
- データ管理
- センサー
- ハードウェアアーキテクチャ
- 技術的セキュリティ対策

非技術要素:

- 新規事業戦略
- サイバーセキュリティポリシー
- ビジネスリスクポリシー
- 倫理
- 法制度および規則制度
- トレーニングおよびテスト
- 運用とメンテナンス
- 雇用、昇進、キャリア管理

ODALOOP

AIが間違った時

AIを扱う際の主要な問題

- 自己破損
  - 自分自身を教えることができるアルゴリズムは自分自身を破壊することができます
- 不可測性
  - 機械学習アルゴリズム、特にバックプロパゲーションを使用するディープラーニングアルゴリズムは、非常に多くの「機能」または変数を追加する事で理解できなくなる
- バイアス
  - アルゴリズムにバイアスがコーディングされる例が多く報告されている。人間がプログラミングするためや自己破損のため。
- データ保護とアルゴリズム保護
  - すべてのAIはデータを必要とします。すべてのデータが敵対的な改ざんから保護されているわけではありません。モデルやアルゴリズムも同様です。
- 欺かれやすい性質
  - ほとんどのAIはデータが信頼できると想定しています。AIを欺くのは簡単です。

AIが間違った例

- スマートスピーカー
  - 米国外の非ネイティブアクセントを理解する可能性が30%低い
- 顔認識
  - 多くの人が使用していたが、後に非白人の顔では認識率が悪いことがわかった
- 量刑ガイドライン
  - COMPASシステムのよく引用される事例
- Amazon履歴書システム
  - 2017年にミソジニスト（女性蔑視者）になりました
- Microsoft Tay
  - 2016年に人種差別主義者になりました
- スパムフィルター
- 検索アルゴリズム

ODA LOOP

AIの軍事利用

あなたは以前同様の状況を見たことがあります

- テクノロジーは私たちを驚かせます
- イノベーションは価値を生み出し、展開は加速し、そしてセキュリティ問題が発見されます
- AIはこれらと違うのだろうか:
  - 電信
  - 電話
  - インターネット
  - サーバー
  - スマートフォン
  - IoT

ODA LOOP

AIセキュリティフレームワーク

AIセキュリティの4つの要素

- AIインフラストラクチャを保護する
- アルゴリズムを保護する
- トレーニングデータを保護する
- 外部データの依存関係とリスクを保護する

このフレームワークを最適化するにはAIセキュリティ戦略が必要です

次はどうするの？

- OODAloop.comとAIセキュリティを深く知ろう
  - 無料のデイリーニュースレター
- ディスカウントコードで無料でメンバーシップ機能にアクセスしよう:
  - OODAIO

Bob Gourley bob@ooda.com

OODAloop.com

OODA LLC

- OODAは、お客様がグローバルなリスクと不確実性を特定、管理、対応しながら、新たな機会を模索し、将来のための頑強で適応的な戦略を開発するのを支援します。グローバルな企業や政府に対して、高度な情報と分析、戦略と計画のサポート、投資の適正評価、リスクと脅威の管理、トレーニング、意思決定支援、危機対応、およびセキュリティサービスを提供しています。

- OODAは、共同創設者のMatt DevostとBob Gourleyが率いるユニークな国際的専門家チームで構成されています。