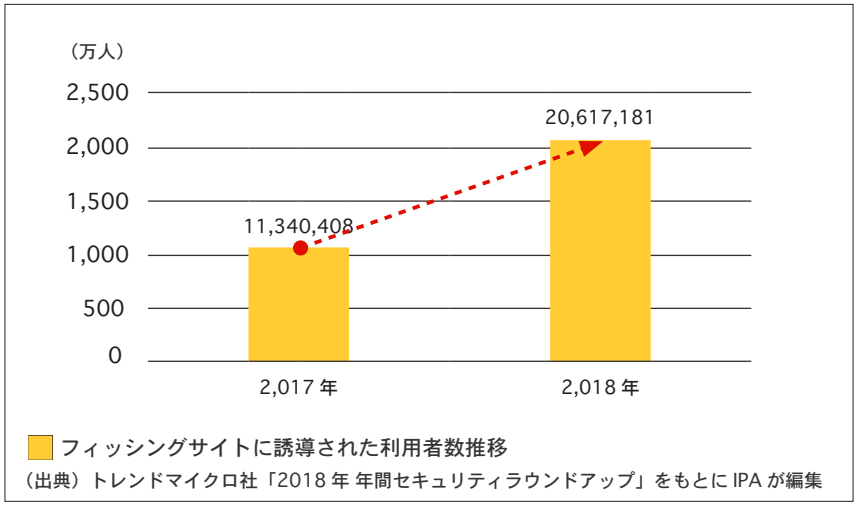
CloudCoffer の AI 技術が実現する、
攻撃者の一歩先を行くセキュリティシステム

多様かつ複雑化し続ける脅威

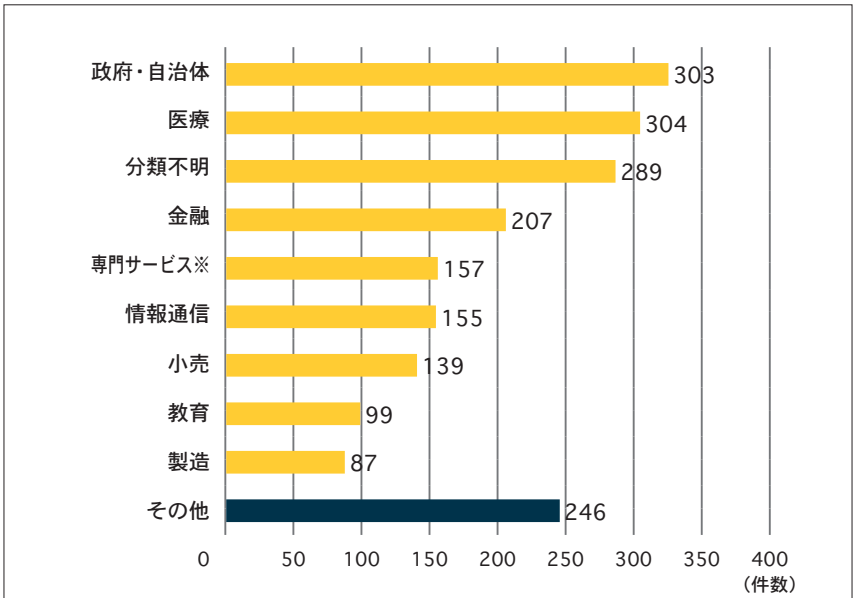
2018 年に世界中で情報セキュリティに投じられた金額は 1,100 億ドルとも 1,200 億ドルとも言われています。その費用の大半は、検知とその対策に使われ、続いて GDPR を始めとする個人情報保護規制に基づく個人情報保護、ディジタル・ビジネスリスク対策などが続きます。

これだけの費用を投じても、最近では、フェイスブックやマリオットの事件でも大きく知られるように、メールアドレスなどの大量のデータ流出が発生し、7 億 7300 万件の流出情報がダークウェブで取引されているという報道もあります。悪意のあるハッカー達によって、フィッシングサイトに誘導された利用者も以下のグラフが示すように異常な伸びを示しています。



（出典）トレンドマイクロ社「2018 年 年間セキュリティラウンドアップ」をもとに IPA が編集

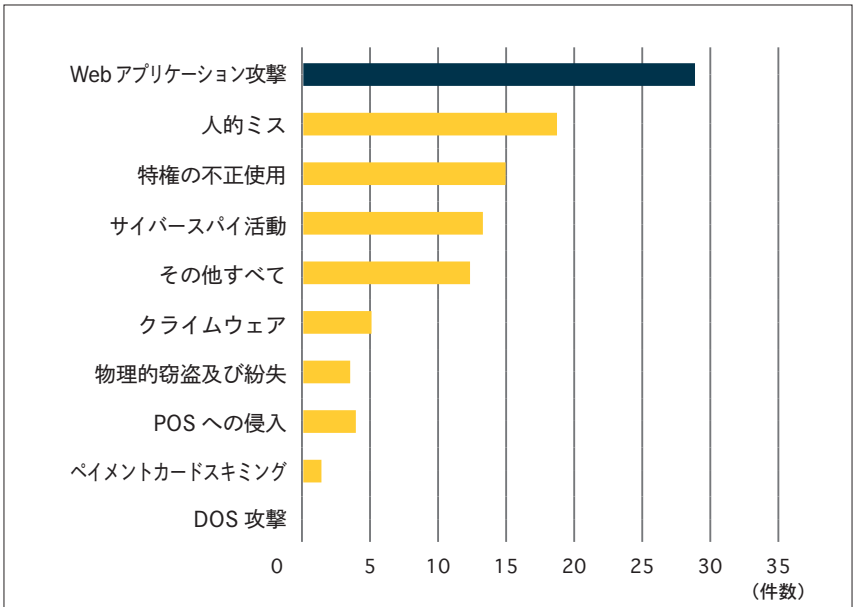
この情報漏洩に限ってみても、また、以下のグラフの示すように、様々な分野でインシデントは発生しており、しかもビジネスの利便性などのために用意された Web アプリケーションを介したケースが全体の 29%もの比率を占めています。



※専門サービスとは、法律事務所、広告代理店を指す

業種別の情報漏えいの件数

（出典）Verizon 社「2019 Data Breach Investigations Report」をもとに IPA が編集



情報漏えい事件の分類

（出典）Verizon 社「2019 Data Breach Investigations Report」をもとに IPA が編集

近年は、利便性もあって、Web アプリケーションを使ったサービスが多様に展開されており、個人向けのオンラインショッピングやオンラインバンキングなどにとどまらず、企業間の取引、公共機関や病院などによる各種サービスの予約や申請など、Web アプリケーションの活用の広がりはとどまるところを知りません。
悪意のあるハッカーたちはそれらシステムに対して、最新技術に精通しつつ革新的に伝統的な方式や手続きなどに縛られず攻撃を行います。認知されているエクスプロイト、マルウェア、ファイルレス等の攻撃だけでも数 10 億件を超え、この数は日々増え続けています。専門家たちは毎年 1 億以上の新たな脅威を発見し続けていますが、このギャップはますます広がるばかりです。更にモバイルやクラウド技術の広がりによってインターネットに接続される機器が増大する中で、仮想空間と物理空間の境目がますます曖昧になってきており、攻撃手法も今までの考え方では簡単に捉えられなくなってきています。

従来型のセキュリティツールでは限界がある

一般的なゲートウェイ型のソリューションとして、Firewall、WAF（Web Application Firewall）や IDS（Intrusion Detection System）、IPS(Intrusion Protection System）などがありますが、Firewall を除くソリューションは、シグネチャマッチング技術を使っております。これらは、通常のトラフィックや不正なトラフィックを見分ける上で、ある意味有効なのですが、既知の脅威にしか対応できません。シグネチャマッチングでは、エクスプロイトやファイルレス攻撃、マルウェアなどの新種や偽装したような亜種の攻撃に対しては効果がありません。また、有効に機能させるためには、シグネチャの更新や、カスタムシグネチャなどを必要としますが、未知もしくは亜種の攻撃に対しては有効ではありません。これらのゲートウェイ型のセキュリティ製品は、侵入を防ぐという目的で使われることが多いのですが、攻撃側からすると、たった一度でも成功すれば良くて、一方のセキュリティ製品側としては、一度でも侵入を許したら存在意味が薄れてしまいます。その意味では、シグネチャ型製品は、有効性に限界があるということができます。また、一般的にゼロデイ攻撃が発見されると、そのパッチがリリースされるまでには数か月を要し、専用のカスタムシグネチャを作るとしても、脆弱性の詳細、攻撃方法、被害内容などの情報を収集し検証を行うためには高度なスキルと時間が必要なため、一般的には対処が完了するまでの長時間、システムは危険な状態のままになっています。

従来型のソリューションの限界

攻撃検知能力に限界があるセキュリティ製品を使ってゆくためには、かなりの人手を使って運用する仕組みを作らなければなりません。セキュリティ分析担当者は、様々なシステムからのログを集め、セキュリティ製品を通過したトラフィックの中に、セキュリティイベントが含まれているかを細かく精査する必要があるのですが、経験の深い解析エンジニアにとっても、骨の折れる膨大な作業になります。スキルの高いハッカーたちは、それらの目をかいくぐり、バックドアをしかけたり、知らないうちにマルウェアを埋め込んだりというようなことを行います。もはや人力で対応することは難しくなっているといえます。

A.I. という賢い選択肢

悪意あるハッカーの攻撃側とシステムを脅威より防ぐ専門家による防御攻防においては、残念ながら常に攻撃側にリードされ続けていると言わざるを得ません。セキュリティ部門は、常に新しい攻撃に対応するために、OS、アプリケーション、上記各セキュリティソリューションのアップデートに追われ、SOC などのインシデント対応チームも常に最新の情報に精通し、既存のシステムを迂回する攻撃がないかに目を光らせていなければなりません。この無尽蔵に人的リソースを食いつぶす状況を回避するため、近年 A.I. 技術を取り入れた製品が、徐々にセキュリティ分野にも現れ始めました。

ガートナー社 が、“A.I. は組織の在り方を変える可能性があり、ディジタルビジネスの中心的存在になる”と言うように、 A.I. を使った新たな手法は、人手による人海戦術的な方法をやめ、効率的に未知の攻撃、攻撃の脅威の検出精度を大いに向上させネットワークの可視化にも大いに役立つものです。

以下に、A.I. がセキュリティ問題について貢献できる点についてまとめてみました。

脅威の予測	次はどこから攻撃がやってくるかなどの予測に役立つもので、同様の技術を自動攻撃などに悪用される可能性があるものの、A.I. 技術を活用することで、少なくとも攻撃者と対等に渡り合い、あるいは一歩先に行くことが可能となる。
アプリケーションのセキュリティ確保	シグネチャーマッチングに依存した従来型のセキュリティ製品とは異なり、トラフィックデータそのものをパターンマッチングを使わずに解析し、不正な動きを検知できる可能性を持っている。
セキュリティチームの効率的な行動	A.I. 技術の活用 によって、セキュリティ担当は、バグフィックスやアップデートの実装に時間を費やすことなく、本来の防御対策により力を注ぐことができるようになる。脅威を特定するための時間を短縮するだけでなく、より効率的に行動できるようになる。
脆弱期間が不要	A.I. によって未知の脅威や既知の攻撃の亜種、難読化などを検知・遮断することができるようになると、脆弱期間を気にしなくて済むようになります。

A.I. を用いた CloudCoffer

A.I. 技術によって、CloudCoffer は脆弱性などを突いた攻撃・脅威を検知、遮断、解析します。既知・未知のいずれの脅威に対しても、CloudCoffer はそれらによるシステムの侵害を防ぎ、情報漏洩・窃盗からシステムを守ります。優れた AI エンジンを搭載した従来型のセキュリティツールとは一線を超えたツールとなっています。

	CloudCoffer	シグネチャーベースの製品
OWASP Top 10 などの既知の攻撃	○	○
既知の攻撃の亜種	○	△
ヘッダーに攻撃文が隠されている場合	○	○
ペイロードに攻撃文が隠されている場合	○	×
ペイロードが暗号化されている場合	○	×
ゼロデイ攻撃	○	×

脆弱期間を持った他の従来型のセキュリティソリューションと違い、CloudCoffer は、日々進化し続けるネットワーク環境において、脆弱期間を大幅に短縮するか完全に無くしてくれます。

CloudCoffer の特徴を以下にまとめてみました。

柔軟な導入形態	CloudCoffer の解析に使われる A.I. エンジンは、様々な形でユーザの環境に合わせて導入することができる柔軟性があります。
簡単なユーザインタフェース	CloudCoffer はダッシュボード上に、ログ、攻撃内容、サマリなどを確認することが可能で、システムやネットワークの監視が容易です。またサマリなどをレポート出力することも可能です。
包括的な解析	CloudCoffer はレイヤ３～７のネットワーク層を解析することができます。また、ヘッダー、ペイロード、リクエスト先の URL などを解析することも可能です。
他システムとの統合・連携	CloudCoffer は、連携する WAF, IDS, IPS, SIEM などのフォーマットに合わせてカスタムルールやシグネチャ作成の支援を行うことができるため、既存の従来型のセキュリティソリューションで最新の脅威に対抗することを可能にします。
攻撃の再現	CloudCoffer には、検証のために、捕捉した攻撃を他のアドレス（一般にはテストサイト）に対して再現したり、マルウェアやエクスプロイトを検体としてダウンロードする機能が装備されています。それらの機能によって、自社環境に合わせて当該攻撃のリスクレベルを特定することができます。

CloudCoffer の A.I. エンジンが優れている訳

CloudCoffer の A.I. エンジンは、世界中のインターネット上に配置された 16 万以上に及ぶハニーポットやスパイダーで収集されたデータを使って、専任のトレーナーによって学習したものです。また、グループ会社 RayAegis 社の 250 名に及ぶ優秀なホワイトハッカーによる徹底的な攻撃及び、RayAegis 社の持つ先進的な脆弱点探索ツールやエクスプロイト発生ツールなども使ってエンジンを鍛え上げました。CloudCoffer の開発チームは、学習に使われた攻撃が正しく分類されていることをしっかりと確認しています。この CloudCoffer の専任トレーナーと開発チームによる監修のもと、A.I. エンジンは、不正なトラフィックか良性なものかを 400 以上のベクタを使って正しく判別します。

類似の脅威を検知

A.I. 技術を使う利点の一つとして、不正な動きである可能性の高い異常値を見つけられる能力があります。CloudCoffer の A.I. エンジンは、既知の脅威との類似性を判断し、それらのパターンを認識することができます。そのため、CloudCoffer は脅威の発展形や亜種を見つけ出すことに優れています。また、その脅威がどのような発展形に育つか、どのような偽装が行われるかをファジング技術によって推測することができます。つまり、ハッカー達を後から追いかけるのではなく、先回りすることができるのです。そのために、最新のエクスプロイトに対してもリアルタイムで対応することが可能となっています。

フィードバックループを減らす

A.I. エンジンは、実際に使われる環境を使って、大量のデータによる学習が必要ですが、CloudCoffer はユーザサイトでの学習は、以下の３つの理由から行っておりません。

1. A.I. エンジンは、正しくカテゴリ毎に分類された、膨大な量の不正トラフィックのサンプルで学習を済ませており、またその学習結果も時間をかけて検証しているため、CloudCoffer の AI エンジンが新たな脅威を発見するに十分な能力を備えているという自負があります。

2. A.I. エンジンの学習は、システムリソースを大量に消費します。ユーザ先での学習をするようなシステムでは、膨大な CPU とメモリを搭載したシステムを必要とし、ユーザにとって現実的な選択肢ではなくなります。

3. ハッカーによる攻撃によって A.I. エンジンを狂わせたり、偏向を持たせたりすることを避けるためです。CloudCoffer の A.I. エンジンは、既に学習を終え自己完結したものを使っているため、エンジンの整合性を保証し、外部からの影響を受けることはありません。

CloudCoffer の導入の仕方

CloudCoffer は、使い方によってその機能や表情を変えてきますが、基本的な使い方、導入スタイルは以下の表の通りです。類似製品として、WAF, IPS/IDS との比較ができるように体裁を整えました。

＊＊ CloudCoffer の透過モード（WAF/IPS/IDS 機能が使える）は、2020 年春にリリースの予定。

	CloudCoffer			WAF (Web application firewall)	IPS/IDS (Intrusion detection/ prevention system)
	WAF	WAF/IPS/IDS			
動作モード	リバースプロキシ	ミラー	透過モード（インライン）	リバースプロキシ・インライン	インライン
導入スタイル	オンプレミス（アプライアンスまたはソフトウェア）もしくはクラウド	オンプレミス（アプライアンスまたはソフトウェア）	オンプレミス（アプライアンスまたはソフトウェア）	オンプレミス（アプライアンスまたはソフトウェア）もしくはクラウド	オンプレミス（アプライアンスまたはソフトウェア）
検知ネットワークレイヤ	Layer 7	Layer 3 - 7	Layer 3 - 7	Layer 7	Layer 3 - 7
プロトコル	http/https	TCP/IP上の主要プロトコル	http/https を含む TCP/IP上の主要プロトコル	http/https	一般的に使われる TCP/IP上の主要プロトコル
ssl/https の復号化・再暗号化	可	不可	IPS/IDS モードでは使用しないことを推奨	可	製品による（行わないのが一般的）
保護対象システム	Webアプリケーションサーバ	Webサーバを含む主要アプリケーションサーバ	Webサーバを含む主要アプリケーションサーバ	Webアプリケーションサーバ	Webサーバを含む主要アプリケーションサーバ
検出可能な脅威	不正な http/https リクエスト	Layer 3 - 7 の不正なトラフィック	Layer 3 - 7 の不正なトラフィック	不正な http/https リクエスト	Layer 3 - 7 の不正なトラフィック
マルウェアの検知	オプションの Sandbox が必要			不可	不可
ゼロデイ攻撃	可			困難	困難
偽装、難読化	可			困難	困難
仮想パッチ	可（AI エンジンにより実現）			可だが限定的	可だが限定的
ペイロードの検査	バイナリも検査可能			バイナリは検査不可	バイナリは検査不能
他社 WAF/IPS/IDS 用のカスタムシグネチャ作成支援	可			ほぼ不可	ほぼ不可
技術	AI エンジンによる不正リクエスト、トラフィックの検知			シグネチャマッチング	シグネチャマッチング
アップデート周期	パッチなどを適用することなく AI エンジンによって新たな脅威を検知 AI エンジン自身のアップデートは最大で年 2 回以内			新たな攻撃パターンが現れる都度パッチ適用が必要	新たな攻撃パターンが現れる都度パッチ適用が必要
脆弱期間	なし 未知の脆弱性も守れる			未知の脆弱性には対応するパッチ、カスタムシグネチャが必要	未知の脆弱性には対応するパッチ、カスタムシグネチャが必要
暗号化された攻撃文の検知	可 多くの場合、暗号文を解読することができる			可 解読できるケースには限りがある	アプリケーション層への攻撃検知力は限定的。暗号化されたトラフィックは通常検査しない

CloudCoffer についての問い合わせ

CloudCoffer についてのお問い合わせ、デモの要請などは、国内総代理店である株式会社アリスまでお問い合わせください。メールでのお問い合わせは、new-sales@aris-kk.co.jp までお願いします。