DARKTRACE

データシート

金融サービス業界のサイバー防御

新たな脅威の時代に立ち向かう自己学習テクノロジー

エグゼクティブ サマリー

今日のサイバー環境は急激に変化を続けており、サイバー脅威はますます動きを速め高度化しています。無言のステルス型攻撃はネットワーク内に何週間も静かに潜伏し、ユーザーの動作を真似、トラフィックやノイズに紛れ込んで情報を収集します。組織が侵入されたことに気づくまで、攻撃者は平均で208日もの間、ネットワーク内にとどまっています。

金融機関はこの新しいタイプの攻撃の主要な標的です。ハッカー達は他の業界よりも300%多く金融サービスを標的としています。これらの脅威がますます複雑化する中で、従来型のセキュリティではもはや不十分です。あらゆる規模の金融機関は、ルールやシグネチャにとらわれず、従業員教育にも限界があることを考慮に入れて、サイバー防御に対する革新的なアプローチをとらねばなりません。

FINRAやSEC、ニューヨーク州金融サービス局といった規制当局は脅威の進化に対応してコンプライアンス基準の強化を行っています。投資家もまたサイバー防御に関するアカウンタビリティを強く要求するようになっています。このような関心の高まりにより、サイバーセキュリティに関する話題は役員会レベルにまで引き上げられています。

サイバー防御テクノロジーで世界をリードするDarktraceはあらゆる規模の金融機関をサポートし、ケンブリッジ大学の専門家により開発された機械学習と数学理論をベースに、これまでに知られていない脅威に対してもネットワークに出現次第、リアルタイムに検知しています。企業ポリシーや規制の変化に対応したカスタマイズが可能なEnterprise Immune Systemはその独自の能力により、業界における新しい要件に対応し、信頼の毀損をもくろむ攻撃から情報、デバイス、ユーザーを保護する企業の取り組みをサポートします。

データ操作：信頼に対する脅威

データ流出は今日のネットワークに対する最大の脅威ではなくなりました。最も危険な攻撃は境界内で行われ、データを盗み出すのではなく、データを変更したり追加したりするものです。数字を1つだけ変更する、あるいは新しいユーザープロフィールを追加するといったことで組織のデータ整合性を損なうのです。

データ操作攻撃は投資家の信頼を傷つけるものであり、金融サービス業界にとって現実的な脅威です。取引やトランザクションの失敗、アルゴリズムの変更、あるいは口座の残高の間違いなどは金融機関の信用と損益を損ないます。

データ操作は大手金融機関に対する一般市民の信頼を崩壊させ、社会的安定を損なう恐れもあります。私達の金融資産の情報が正しいことを信じられなくなったら、どうなってしまうでしょうか？

> 「常に侵入発生モードの心構えです。侵入されることはわかっているからです。見張り、見つけ出し、叩き出さなければなりません。」
>
> **Troels Oerting, CISO, Barclays, FT Cyber Security Summit 2016**

重要データと業界での評判

重要情報はブラックマーケットでは高値で取引されます。クライアントの個人情報、取引戦略、口座残高、そして値付業者への注文の詳細などもハッカーには大きな利益をもたらします。万里の長城のような社内の防御策も、情報を悪用しようとする内部関係者や市場の混乱を狙った第三者による侵入の危機に瀕しています。

このようなサイバー脅威の新時代においては、投資家は資金をどこに預けるかを決める際、ネットワークセキュリティにより大きな注意を払うようになっています。年金基金や投資信託など機関投資家はサイバーセキュリティをデューデリジェンスやオンサイト訪問時の議題に含めています。

このような調査の厳密化に耐えるには、金融機関は強固なサイバー防御策を提示し、データの安全性を確保するだけでなく、高度な進化するサイバー脅威を早期に検出するための対策を行う必要があります。

金融機関に対するサイバーリスク

内部からの脅威

不満を抱える従業員が競合他社に取引情報を伝える、あるいは悪意のないユーザーがフィッシングメールの被害者となってしまうなど、内部関係者による脅威は知的財産盗難の危険性をもたらします。また、投資家の機密情報が明らかになってしまうことで重要な関係を損なう結果となる可能性もあります。

一見無害な行動、たとえば間違ったリンクをクリックしてしまう、あるいはプロジェクトをサードパーティのクラウドにアップロードしてしまうなどの行動も、重要なデータをリスクにさらす恐れがあるのです。この種の内部関係者によるインシデントの発生をトレーニングによって減らすことは可能ですが、完全になくすことはできません。

悪意のある内部関係者の場合は目的がよりはっきりしているため、外部からの攻撃よりもさらに甚大な被害をもたらす可能性があります。すでにネットワーク内に存在している、権限を持ったユーザーは境界防御という障壁を超える必要がありません。つまり、ファイアウォールのような従来型のセキュリティツールは彼らの行動を検知、あるいは防止することはできないのです。

この場合の防御策はステルス性の高い脅威であっても発見し対応することが可能であると同時に、従業員に対しては職務を遂行するのに必要なアクセスと柔軟性を提供しなければなりません。これら両方のニーズに対応するには、いかなるセキュリティアプローチの場合もそれぞれのネットワーク独自の環境において何が定常な状態であるかについての完全な理解から始まる必要があります。そうすることで初めて、問題のごく初期の兆候であることが非常に多いわずかな異常も見つけ出し、重大な危機に発展する前にこれらの異常に対処するための情報を持つことができるのです。

DoS攻撃

どのような業務の中断も莫大な金銭的損失や生産性低下の危険性が伴います。金融機関は特にDoS攻撃に対して弱みを持っています。DoS攻撃は取引の不成立や遅延、データのライブストリームの遅れ、当事者間のコミュニケーションの阻害につながり、何百万ドルもの損害が発生する可能性があります。

データ流出

金融機関は大口投資家について社会保障番号にとどまらない詳細なPII（個人識別可能情報）を保有しています。金銭的利益を狙うハッカーや政治的動機を持つ者たちはこの情報全体を取得しようと狙っています。口座番号、クレジットカード情報、そして取引戦略などは金融機関が保護しなければならない貴重な、そして弱みともなるデータの例です。

悪意のある人の手に渡った場合、これらの機密データは投資家および従業員の富と身体的安全の両方を危険にさらすことになります。この情報を守る上で境界セキュリティは重要な手段ですが、今日の攻撃はファイアウォールをいともたやすく破ることができます。情報が悪意のあるものの手に渡る前に流出を阻止するには、金融機関はデータがネットワーク上のどこにあるのかを確認できなくてはなりません。

実際の攻撃事例

J.P. Morgan のデータ流出事件

2014年、ハッカー達はアップデートを怠っていたサーバーを利用してJ.P. Morganの8300万人の顧客の個人情報を盗みました。2要素認証システムはアクティベートされていなかったため、攻撃者はより簡単にネットワークに侵入し顧客データを取り出すことができました。

バングラデシュ中央銀行の不正送金事件

バングラデシュ中央銀行からSWIFT（Society for Worldwide Interbank Financial Telecommunication）ネットワークを使った指示により8100万ドルが不正送金されました。ハッカー達は攻撃を開始する前に銀行内のシステムに1ヶ月以上も潜伏して情報を収集し、キー入力のロギングなどによってパスワードを調べました。攻撃が中止されたのは送金依頼の1つにスペルミスがあったことによるものでした。これに気が付いた中継銀行が照会を行い、その結果、不正な送金の中止につながりました。

ランサムウェア

ランサムウェアによる攻撃を含めたネットインフラの犯罪目的利用は3500%増加しており、被害の大きいこの攻撃は金融機関にとってこれまでにない大きなリスクとなっています。ランサムウェアによる攻撃は重要なファイルやサーバーを暗号化した後、その復旧に対する身代金の支払いを要求するものです。ランサムウェアを即座に検出することは、攻撃がネットワーク内に急速に広がる前に被害を抑える上で極めて重要です。

アタックサーフェスの拡大

管理業務、法務、IT管理作業などを外部のサービスプロバイダーに委託することにより組織の脆弱性が増大します。大量のデータを処理することが多いこのようなサービスの利用はネットワークへのエントリポイントを増やす結果となり、その金融機関のアタックサーフェスを広げてしまいます。外部のプロバイダーを監督することは脅威への脆弱性を軽減したいあらゆる金融機関にとって必要なことです。

個人秘書やIoT機器の増加もネットワーク脆弱性の広がりの原因に含まれます。外部クラウドインフラへのシフトは従来のセキュリティツールの大きな盲点であり、問題を一層複雑化させています。

通貨と取引のデジタル化により、ネットワーク上に誰が、そして何が存在するかを知る能力が極めて重要となり、完全な可視性はかつてないほど重要に、あるいは難しくなりつつあります。

規制をとりまく環境

規制による調査がますます厳しくなる兆候があらわれています。政府機関は金融機関に対し、攻撃に遭う前にサイバーセキュリティのコンプライアンスを強化するよう強く求めています。問題が起こった後で適切に事後対応するだけではもう通用しないのです。

米国では、州および連邦レベルの両方でより厳しいコンプライアンス基準が適用されています。FINRAとSECは引き続きサイバーセキュリティと市場の安定性へのその影響に対する懸念を表明しています。SECのOCIE（Office of Compliance, Inspections, and Examinations）が発行した2015年度 'Risk Alert' 報告書には、登録ブローカーおよびディーラー、投資アドバイザーに対する今後の審査においてSEC監査人が重視する優先項目を紹介し、金融機関が対応しなければならないサイバーセキュリティ上のガバナンスおよびリスク評価の様々な側面について説明しています。

規制への抵触：RT Jones

SECは2016年、より厳しい姿勢を明確にしました。その様々な意向書を裏付ける形で、典型的な「サプライチェーン攻撃」に遭った小規模な地方の投資会社であるRT Jonesに対して厳しい措置を取ったのです。

外部ウェブサーバーに中国から侵入されたことにより、同社の証券取引の顧客10万件の情報が漏えいしました。RT Jonesはデータセキュリティポリシーおよび手順の不実施に関して譴責を受けました。メッセージは明確です。サイバー攻撃が来る前に自社の体制を整えろということです。

ヨーロッパ議会は2016年、ネットワークおよび情報システムセキュリティ指令（NIS Directive）を発行し、金融サービス企業がセキュリティ違反を報告し、防止のための対策を実施することを義務付けました。

地方政府も州レベルで経済活動を保護するための施策を実行しています。2016年9月、ニューヨーク州は特に金融サービス分野を対象としたサイバーセキュリティ規制を提案しました。この規制の下では、金融機関はサイバーセキュリティプログラムを確立し、書面によるサイバーセキュリティ方針を策定しなければなりません。CISOを任命することに加えて、金融機関は外部のサービスプロバイダからアクセス可能なデータを保護するための対策を講じなければなりません。これは明らかにRT Jonesに対するSECの譴責を反映しています。「規制下の法人は問題の責任を負うことになります」と、ニューヨーク州金融サービス局長Maria Vullo氏は警告しています。

このように、規制をとりまく環境も一気に複雑化し、厳罰化しています。現在の最小限のコンプライアンス基準を満足するだけでは、各種規制の強化に対応し、変化を続ける脅威の動向に備えることはできません。むしろ、サイバー防御に対して境界侵入が避けられないことを前提として、ネットワークに侵入してきた脅威を捕まえることができる、積極的なアプローチをとる必要があります。

役員会とテクノロジー

企業のエグゼクティブと技術部門のセキュリティ担当者の間の知識のギャップは以前にもまして顕著です。Ponemon Instituteによる調査では、ITプロフェッショナルのほぼ60%が自社の役員はサイバーセキュリティを理解していないと答えました。自社のサイバーセキュリティのガバナンスが適切にできていると回答した役員は60%であったのと対照的に、ITスタッフではわずか18%でした。

情報セキュリティは経営上の課題であり、役員会の監督が必要な問題であることが規制当局によりますます強調される中、役員会レベルで重要な戦略的重点課題としてサイバーセキュリティに取り組むには技術者と経営陣の間のコミュニケーションを強化することが必須です。

金融サービス分野での Enterprise Immune System

DarktraceのEnterprise Immune Systemは変化する脅威環境の先を行き、データを保護し、コンプライアンス要件に対応しようとする金融機関に幅広く採用されています。また、Enterprise Immune Systemでは内部関係者による脅威を含め、ネットワークが直面するあらゆる種類のサイバー脅威から防御しつつ、柔軟性も維持することが可能になります。

侵入が避けられないことを踏まえた上で、Darktraceはセキュリティに積極的アプローチをとり、各組織の「自己」の姿を学習します。ネットワークの「通常」を基準とすることで、Enterprise Immune Systemは脅威の可能性のある異常な挙動の出現を検知します。

DarktraceのEnterprise Immune Systemはケンブリッジ大学で開発された教師なし機械学習と数学理論を基盤とした自己学習テクノロジープラットフォームです。

この自己学習テクノロジーはデータ環境や脅威動向に関する何らの事前知識も必要とすることなく動作し、シグネチャやルールにも依存しません。Darktraceは変化するエビデンスに基づいて蓋然性を絶え間なく計算し、すべてのデバイス、ユーザー、ネットワークの動作をモデル化することによりその環境内で何が通常で何が異常であるかの精密な理解を構築します。

動きの速い、価値の高いデータを大量に処理するネットワークにおいては、100%の可視性を担保することが防御にとって極めて重要です。しかしネットワークアクティビティの可視化もまた難しい課題であり、経営陣と技術担当者のどちらにも脅威を伝えることのできるインターフェイスの必要性も問題を複雑にしています。

DarktraceのThreat Visualizerインターフェイスはネットワークおよびサブネットから個別のユーザーおよびデバイスに至るまで、企業のネットワーク全体をグラフィカルに3Dで可視化します。アラートを詳細に調査したり、特定のインシデントの前後関係を理解、あるいはイベントを時系列でさかのぼって調べることも可能で、脅威を軽減するためのあらゆるインテリジェンスを取得することができます。

Darktraceのサイバー分析エキスパートが作成する週次のThreat Intelligenceレポートとあわせて、Threat Visualizerを利用することにより検知された異常をビジネス担当者、セキュリティ担当者が共に理解することができます。これにより両者が迅速な問題解決に向けて協力して取り組み、人的リソースを最大化し、重要な情報を保護し、継続的にリスクや脅威の軽減を図ることができるのです。また、Threat Visualizerはセキュリティインシデントや調査をダッシュボード内で管理することができ、完全な監査証跡を残すことができます。

Darktraceが提供する可視性はクラウド、SaaSアプリケーション、およびオンサイト仮想環境にも対応しています。企業は今やサプライヤのセキュリティツールにも責任を持たざるを得ず、この監督能力はかつてない重要性を持っています。Darktraceはサードパーティ環境と企業環境の間のやり取りを監視することによりこれらの外部ベンダーの管理を支援します。

Enterprise Immune Systemは既存のセキュリティスタックに整然と組み込むことができ、規制基準の変化に応じて更新できる調整可能なモデルを提供しています。また、Darktrace APIを使うことにより、ログやイベントデータなどの構成変更可能なデータ入力、SIEMを含むサードパーティ製ワークフローやダッシュボードとの完全な統合、電子メール、syslogアラートおよびCEF（Common Event Format）などを含む新たなアラート出力への対応が可能です。これによりMSSP（マネージド型セキュリティサービスプロバイダ）は、Darktraceの検知結果を簡単かつ即座に活用することが可能になります。

まとめ

信頼は金融サービス業界にとって極めて重要です。ますます複雑化するネットワークと最近のステルス型攻撃により、サイバーセキュリティに関してこの信頼を維持することが難しくなっています。「何か」が起こるのは単に時間の問題とも言えます。そして攻撃に遭った後、評判と世間の信頼を再構築するのには何年もかかります。

現在の最も洗練されたハッカー達が引き続き金融サービス企業を標的としている中で、業界はほぼ不可能な課題に直面しています。それは、かつて鍵のかかった部屋だと思われていたものを守ることなのです。

規制が強化され、投資家の調査が厳しくなっていることは積極的にサイバー防御策を推進することの重要性を裏付けています。貴重な情報を守り業界の信用を保護するには、全く新しいアプローチが必要です。それはネットワークを内側から保護することが境界の保護と同様に重要であることを認識することです。

将来を見据える企業は、従来のセキュリティ手法に不安を持ちながらも依存するのではなく、イノベーションを取り入れる必要があります。Darktraceの導入により、金融機関は投資家、役員会、顧客、同業他社に対して、今日の絶え間なく変化する脅威および規制をとりまく環境に適応可能な、成熟したサイバー防御態勢を整えたということを示すことができます。Enterprise Immune Systemはこれまでに出現したことがない攻撃を防御し、信用を含めたあらゆる資産の安全を守るのに役立ちます。

参考資料

Darktraceのウェブサイトにはこのデータシートの情報を補完する次のような参考資料があります。

データシート：サイバーセキュリティとコンプライアンス：New York State Regulations 2016

ニューヨーク州金融サービス局が指定する新しいサイバーセキュリティ基準に対応するためのDarktraceの使い方について紹介されています。https://www.darktrace.com/resources/#data-sheets

ケース スタディ：Macrosynergy

世界的ヘッジファンド、MacrosynergyでのDarktrace導入事例は次の場所にあります。
https://www.darktrace.com/resources/#case-studies

ケース スタディ：Billtrust

業界をリードする課金および支払サービスプロバイダ、BilltrustでのDarktrace導入事例は次の場所にあります。
https://www.darktrace.com/resources/#case-studies

ホワイト ペーパー：Enterprise Immune System

組織全体でDarktrace Enterprise Immune Systemを幅広く活用する方法を紹介したホワイトペーパーは次の場所にあります。
https://www.darktrace.com/resources/#white-papers

Darktraceが発見するもの：2016年世界脅威ケーススタディ

2016年にDarktraceが様々な顧客のネットワークで発見した脅威を解説したホワイトペーパーは次の場所にあります。
https://www.darktrace.com/resources/#white-papers

Darktraceについて

ダークトレースは、世界をリードするサイバー防御企業の1つです。数々の受賞歴を誇るダークトレースのEnterprise Immune System技術は、ケンブリッジ大学の専門家により開発された機械学習と数学理論をベースに、組織内のあらゆるデバイス、ユーザーおよびネットワークの生活パターンを学習し、ルールやシグネチャに依存せず、新たな脅威を自動的に検知し、損害が出る前にサイバー脅威を特定・軽減します。エネルギーおよび小売、電気通信、製造、金融サービス、ヘルスケアを含む世界各国のあらゆる産業分野の企業がダークトレースの自己学習型アプライアンスを導入しています。本社は米国サンフランシスコと英国ケンブリッジにあり、ロンドン、ニューヨーク、ミラノ、ムンバイ、パリ、シンガポール、シドニー、東京、トロントおよびワシントンD.C.を含む世界に20以上の拠点を置いています。

お問い合わせ

米国：+1 (415) 229 9100
ヨーロッパ：+44 (0) 1223 394 124
日本：(03) 5456-5537

電子メール: japan@darktrace.com

www.darktrace.jp

金融サービス業界の概況

業界の課題

銀行、保険会社その他の金融機関に保管される金融データの量は膨大であり、他のどの業界よりも多くの組織的なサイバー攻撃に遭遇しています。事実、金融機関に対するサイバー犯罪は40%増大しています。これに対応して様々な規制が実施されましたが、規制に対応するための最小限の対策ではもはや十分とは言えません。

現代の金融機関は、より速く、より効率的であれというプレッシャーに常に直面しています。この期待に応えるためにプロセスの自動化、クラウドサービスの急速な取り入れが進み、ますます多くのIoTデバイスが使用されるようになりました。この急激な変化は、データを盗み、あるいは操作し企業の信用を著しく損なわせる脅威アクターに対して大きな機会を与えることになりました。

さらに、盗まれた、あるいは流出したデータは企業にとって非常に大きなリスクとなるほか、内部関係者からの脅威も常に存在する脆弱性です。トレーニングや厳しいコンプライアンス対策は内部関係者からの脅威を防ぐのに役立ちますが、従業員が疑わしい行動をしているのかどうかを知るのは可視性と個々のアクションに対する情報がなくてはほぼ不可能です。

> バングラデシュ銀行は2016年に発生した1回の不正送金事件で9億5100万ドルを盗まれました。この攻撃は銀行の従業員が手引きをしたものでした。

脅威の内訳

2016年にランサムウェアは6000%増大

金融データを狙ったランサムウェアはかつてない規模で使用されています。業界の報告書によれば、ランサムウェアは2016年に6000%という規模で急激に増大し、10億ドル産業になろうかという勢いです。

米国の大手銀行20社のうち75%がマルウェアに感染

米国の大手銀行の4社のうち3社のネットワークにマルウェアが存在しています。業界全体ではこの数字はさらに高くなります。規模がより小さい銀行ではサイバーセキュリティ専任のリソースが少ないためです。

データ流出のコスト増大

データ流出はそのコストと規模が増大しています。金融関連データ流出の1レコードあたりのコストは221ドルであり、平均値の158ドルを大きく上回ります。数値化されているコスト以上に、長期的には信用の毀損がはるかに大きなコストとなります。

Enterprise Immune System

Darktraceは受賞歴のある脅威検知および自己防御テクノロジーにより、金融機関におけるセキュリティーソリューションとして急速に業界標準になりつつあります。DarktraceのEnterprise Immune Systemは、ケンブリッジ大学で開発された教師なし機械学習と数学理論を基盤とした自己学習テクノロジープラットフォームです。どのネットワークにもサイバー脅威は既に存在していることを前提とした上で、Darktraceは各システムの「自己」について学習し、脅威であるかもしれない異常を特定します。

サイバー攻撃の頻度とコストが高まる中、企業はサイバーセキュリティに対して積極的なアプローチをとることが非常に重要です。攻撃者が発見されるまでに企業ネットワーク内に留まっている期間は平均197日間であり、脱出する前にデータを盗む十分な時間が与えられているのです。ネットワークアクティビティの理解をボトムアップで構築することにより、Darktraceはこれらの攻撃者を見つけ出し、損害が発生する前に動的に対応することが可能です。このテクノロジーは新しいエビデンスに照らして適応を続けるため、金融機関はあらゆる種類の脅威に対して幅広く防御することが可能になります。ネットワークを継続的に監視し変化の速い脅威の動向にシームレスに適応するDarktraceの能力は、あらゆる企業のセキュリティ確保に極めて重要な役割を果たします。

billtrust　ING BANK　PRUDENTIAL　JACKSON