第6回 SECURITY USERS CONFERENCE

～　『機械学習』をサイバーセキュリティ対策に　～

開催レポート

2018.12.4(TUE)

2018年12月4日（火）、ベルサール東京日本橋にて、株式会社インテリジェント ウェイブ主催「第6回セキュリティユーザカンファレンス ～『機械学習』をサイバーセキュリティ対策に～」を開催いたしました。

当日のセミナー風景

基調講演 『サイバー脅威の現状と対応』

日本サイバー犯罪対策センター（JC3）　理事、東京オリンピック・パラリンピック競技大会組織委員会
CISO　坂　明　氏

日本サイバー犯罪対策センター
坂　明氏

ゲストスピーカーであるJC3 坂氏は、1981年に警察庁に入庁し、目黒警察署長を手始めに、数々の主要なポストを歴任し、現在は生活安全局セキュリティシステム対策室長、情報技術犯罪対策課長として勤務し、まさにサイバー犯罪対策の最前線で活躍されています。
今回の基調講演は、サイバーセキュリティ対策の現場で今も活躍されている坂氏にお話を伺いました。坂氏曰く、現状の国内のサイバーセキュリティ犯罪への対策は、約4年前より産官学が一体となって取り組まれています。これは、従来の「愉快犯」的または「不特定多数」をねらった攻撃と違い、攻撃自体が特定の目的（平昌オリンピックへの破壊活動など）を持って実施されることや、「攻撃コードを書く」側とそれを「使用する側」というように分業化されてきたことにより、守る側も業界を超えて連携するようになってきたことによります。
これは世界的な傾向であり、 FBIやJC3（日本）が NCFTA（米国）やCDA（英国）などNPO団体およびIC4（米国）やJ-CAT（欧州）など法執行機関と連携するようになりました。
また幸いなことに、国内の全体の犯罪発生件数は平成14年をピークに減少傾向で、今年も昨年に続き、戦後最低になりそうです。ただしサイバー犯罪の相談受理件数については増加傾向で、平成25年の8万件から平成29年には13万件に増加しました。中でもインターネットを利用した不正送金は平成27年にはピークを向え、その後平成27年～29年には仮想通貨の不正使用（番号盗用）が増加しています。これは、特定のサイト（特にWordpressで作られたサイト）に訪問するだけで、Gozi/DreamBotなどのRATに感染し、通貨が勝手に自動送金されてしまうという攻撃によるもので、被害総額はわかっているだけでも、200億円以上にのぼり、本年7月末だけでも警察庁が334件の事案を喚起しています。クレジットカード情報を搾取するマルウェアの代表的なものは、上記Gozi/DreamBot以外にも亜種としてRamnit/Zeus-Pandaなどがあり、搾取された情報は海外へ売られています。また全世界の端末の約50～100台がこれらに感染し、その約20%の端末が日本に所在すると推定されています。※本年3月27日にはArbor社より、日本をターゲットにしたZeus-Pandaが検出され、クレジットカード情報が搾取されている旨公表されました。**なおJC3では、サーバや端末がこれらのマルウェアに感染しているかどうか調べることができるサイトを用意しているので、ぜひ1度お調べください。**
また2009年から様々なサイバー犯罪に使われてきた大規模マルウェアサービスであるAvalancheが、一昨年にFBI/インターポールにより一斉摘発されました。ハッカーはWordpress（ホームページの代表的なCMS）の脆弱性を常に狙っていて、このツールで作り放しの状態のHPは、脆弱性が見つかり次第、攻撃者に乗っ取られ、マルウェアツールを埋め込まれ、C&Cサーバと通信したり、閲覧者の端末に感染します。これらが摘発されたのですが、いまだに日本にはこれらのマルウェアの活動が観測されています。その他の最新のネット犯罪としては、クレジットカード番号が騙し取られ、旅行予約情報が転売されたり、運送会社を装った攻撃により、不正なアプリをインストールしてしまうなどの手口などをご紹介いただきました。最後にまとめとして、『攻撃側が分業され、攻撃自体がますます高度化・国際化される中、守る側としてもTokyo2020オリンピック・パラリンピックに向けて、オールジャパンとして一丸となってサイバー攻撃に対応していくこと』をお伝えいただき、基調講演を締めていただきました。

基調講演に続いて、Paloalto社より、xDRの紹介とインテリジェント ウェイブの機械学習（AI）を利用した各種セキュリティソリューションを順次紹介しました。

EDRはもう古い　- セキュリティ自動化に向けたxDRとは？（Palo Alto Networks社）

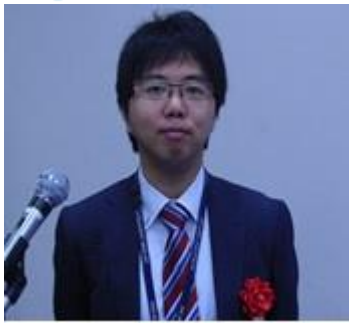
パロアルトネットワークス株式会社

広瀬氏

Trapsの主な特徴は、エンドポイントでの脆弱性対策・マルウェア対策・ランサムウェア（挙動の静的解析）の３つで、マルウェアが検出された場合コンソールに表示されます。またPAN社の脅威インテリジェンスであるAutoFocus は、インシデントを地域/侵入経路/他の攻撃との関連性などとタグ付けした脅威分析クラウドを提供しています。ただしPAN社では、セキュリティの監視サービスは提供していません。PAN社のxDRは、SOC運用向けの新たな提案であり、相関関連分析型のSIEMを導入した企業における手作業による環境構築や実運用を支援します。AIを用いて、アクティブログをディクテーションし、エンドポイントやネットワークの普段の状態を学習し、AIが専門家に代わって異常な行動を自動検出する仕組で、付属のMagnifierにより、侵入経路や手段を可視化することができます。
これからの新世代の脅威解析はオペレーションを自動・基盤化することで、EDRのように人手を介すことなく、セキュリティシステムの運用が可能になります。

Traps（Palo alto Networks社）- OS(Win7)の環境移行の波を乗り越える為に

Traps Version 5.0



株式会社インテリジェント ウェイブ

高橋　一巨

Windows7が2020年1月14日でサポート終了となります。国内法人市場でのWindows 10への移行状況は51.5%にとどまり、いまだ約3割の企業は移行する計画がないという状況です。そこで、Windows7のEOLに備えてTrapsを導入することで、セキュリティパッチ不適用によるセキュリティリスク、および移行による業務不可を軽減しませんか? TrapsではMicrosoftのOSサポート終了から約5年間、脆弱性/マルウェア対策が提供され続けます。そのためOSのセキュリティパッチが不在であるために発生するセキュリティリスク等を防ぎます。実際に大手製造業様の事例では、WindowsXPのサポート終了時に、OS移行による業務影響やコスト負荷を踏まえ、「OSサポートの延命措置」を目的とし、数万台のXP端末に対しTrapsを導入頂いております。また、アンチウィルスソフトでは検出できなかった脅威を検出した実績がございます。Trapsを導入することで、パッチが配信されなくなった環境においても、Trapsの脆弱性/マルウェア対策は有効的です。

Morphisec（Morphisec社）- 新世代のエンドポイント保護

株式会社インテリジェント ウェイブ

中原　正貴 with Morphisec

Morphisecは、「攻撃対象となるアプリケーションのメモリアロケーションを変化させることで攻撃を成立させない」という新たな手法でエンドポイントを保護する新発想のソリューションであり、既存のマルウェアテクニックや情報からの推測による検知しかできないアンチウィルス製品とは一線を画す製品です。
Moving Target Defense(MTD)という最新技術により、アプリケーションに割り当てられるアドレスをランダム化させることで、起動ごとにメモリアロケーションを変化させ、手法を問わず攻撃を成立させません。これにより、既存のエンドポイント製品のような常時スキャンによる高負荷・頻繁なアップデートや、多機能ゆえに複雑な設定になることを回避し、オフラインでも通常通り動作するので、セキュリティ業務にかかる負荷を大幅に軽減することが可能です。

Cybear（Cybear社）- SOCインシデント分析をAIロボットで分析代行

株式会社インテリジェント ウェイブ

市川　悟

Cybearは、SOCアナリスト人材不足問題に対応すべく、AIロボットのSOCアナリストでインシデント分析の代行を実現するべく、現在企画開発中の製品です。ロボットは当初SOCアナリスト（メンター）に分析トレーニングを受け学習、学習工程を終わると独自にインシデント分析を開始します。これにより発生インシデント数と対応インシデント数のギャップの増大を埋めあわせる事が出来る様になります。ロボットSOCアナリストは、以下の処理を実現します。

・学習完了後にインシデント及び関連ログを自動で調査・分析し、インシデントレポートを配信
・継続的な学習とクラウドシステムに蓄積共有される分析情報を活用して、分析動作を改善する
・インシデント詳細レポート、経営層向けの統計レポートを作成してSOC運営を可視化します
・SOCの“Dark Side”ワークロードを担い、アナリストが重要業務に注力できる様にします

Cybearは現在イスラエルの某カード事業者と大手銀行のSOCで人間のアナリストと並行稼働してその効果の実証測定と、問題検出、さらなる改善を継続中です。

eyeShare（ayehu社） - IT自動化の導入事例と効果

株式会社インテリジェント ウェイブ
秋山　茎一郎

ayehu社のeyeShareは、セキュリティ製品の導入とCSIRT/SOC運用の慢性的な人手不足という問題を解決するITPA（ITプロセスオートメーション）ツールです。
本セッションでは、製品の導入効果と事例を中心にご紹介させていただきました。eyeShareの視覚的な業務プロセスワークフロー作成機能を用いることで、多種多様な業務システムを統合管理し、既存環境へのスムーズな導入/展開が可能です。
ある企業様の場合、ServiceNowで受け付けるパスワードリセットリクエストのみをeyeShareで自動化した結果、年間約$500,000のコスト削減を実現した事例もございます。また別の企業様での製品をご検証いただいた例ですと、C&Cサーバ通信プログラムの接続先ブラックリスト情報収集管理業務にeyeShareを導入し、不定形なメールフォーマットから任意の情報だけを特定、抽出し、メールの可否の判断に必要な情報収集及びUTM機器への登録、リスト更新作業プロセスを標準化することで、1件あたり約60分かかっていた業務を、5分に短縮することに成功しました。

クレジット決済のリアルタイム不正対策ソリューション

国内におけるカード不正利用被害は、平成29年には前年の1.7倍236億円に増加し、第三者によるカードの不正が全体の約88%に及んでおり、不正利用対策は決済業界に置いても喫緊の課題となっています。
リアルタイム不正検知システムに求められることとは、
1.リアルタイムに不正取引を検知・対処できること
2.いつでもルール条件を変更・攻撃に対応できること（ルール）
3.いつもと異なる取引に自動的に反応できること（スコア）
にあります。当社の提供するリアルタイム不正対策ソリューションは、具体的には不正手口をルール化し、同パターンの利用があった際に、カード取引自体を自動拒否・保留・モニタリングすることで、不正を防止します。当社は、これまで提供してきたルール・スコアベースの不正検知に加え、イスラエルのAIソリューションなどを活用した機械学習モデルの不正検知など、次世代不正検知の提供に向けて更なる取り組みを実施して参ります。

株式会社インテリジェント ウェイブ
加藤　涼介

最新のイスラエル動向のご紹介

株式会社インテリジェント ウェイブ
手塚　弘章

現在のサイバー攻撃のメインは、組織的金銭目的や国家間の紛争であり、攻撃活動自体が組織的になっています。また2016年ごろからセキュリティ対策は攻撃の「検知と検知後対策」となり、2017年ごろから機械学習（AI）とインテリジェンスを利用した「検知・事前事後対策」へ変遷しています。
また昨今のセキュリティの常識としては、**100%の防御を目指しても限界があり、"攻撃を受けること"を前提としたセキュリティ対策が必要**という考え方に変わってきています。
本日担当者ごとに、各セッションでご紹介したイスラエルの最先端の製品群は、隠れた脅威の検出やインシデント発生時の分析や対応の迅速化を計るための、攻撃を受けることを前提とした対策（製品）になります。
カンファレンスの冒頭で当社社長の井関より紹介したように、当社ではセキュリティソリューションマップを用意し、このマップに足りないセキュリティ対策を常に補う形で、お客様のシステムを守る為に"攻撃を受けること"を前提としたセキュリティ対策を今後ともさらに推し進めて参ります。

WiFiWall　2.4GHZ

【WiFiWallの紹介】
2018年6月にWPA2のKRACKs脆弱性を回避するWPA3が、公表されました。ただし現時点では設置済みアクセスポイントWiFiやデバイスがWPA3をサポートをするには数年かかる上に、たとえ、VPNを使用していてもインターネット接続からVPN確立までの時間で十分にクレデンシャル情報などが搾取される可能性があります。
WifiWallは、現在接続中のネットワークを常時監視し、危険を検知すると警告を出す、あるいは強制切断するポータブルデバイスです。
【イスラエル出張所の開設】
2018年8月にテルアビブに出張所を開設しました。今後新製品の評価・試験・トレーニングなどを実施していく予定です。

懇親会の様子

各種セッションを終えてから会場を移しての参加者懇親会も開催されました。今回の懇親会ではインテリジェント ウェイブのセキュリティ商材とIT-One社にもご協力いただき、次の4製品（Morphisec、Traps、SecBI、CWATクラウドサービス）のデモ環境を展示しました。

お忙しいところお時間を割いて会場に残っていただけた参加者の皆様とは各組織の現状の状況をお話しいただいたり、当社の活動のアイデアになる様な情報をいただいたり、訪問デモによる詳細な情報交換のご依頼をいただいたりすることができました。また、パートナー企業様の取扱い製品と紹介した製品の連携・連動ができないか？など興味深いご相談もいただき、有意義な情報交換の場所とさせていただくことができました。

第7回セキュリティユーザカンファレンスについて（2019年7月予定）

第7回セキュリティユーザカンファレンスは、2019年7月頃の開催を予定しております。
詳細につきましては、改めてメールでご案内差し上げますと共に、当社コーポレートサイトにも掲載してまいります。
今後も皆様にお役立て頂けるセミナーを開催出来ますよう、社員一同邁進して参りますので、引き続き、ご参加いただければ幸いです。
次回カンファレンス、および今回の講演に関するお問い合わせは、下記窓口までお願いいたします。

カンファレンス窓口

株式会社インテリジェント ウェイブ　セキュリティソリューション本部
E-mail：iwi_security@iwi.co.jp

株式会社インテリジェント ウェイブのプライバシーポリシーは下記URLをご参照ください。
http://www.iwi.co.jp/company/principlepolicy/detail/privacypolicy.html

INTELLIGENT WAVE INC.

Copyright © 2018,INTELLIGENT WAVE INC. All rights reserved.