第5回 SECURITY USERS CONFERENCE
～ 『侵入前提』のサイバーセキュリティ対策 ～

開催レポート

2018.7.12(THU)

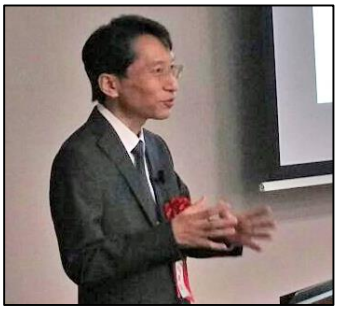
2018年7月12日（木）、ベルサール東京日本橋にて、株式会社インテリジェント ウェイブ主催「第5回セキュリティユーザカンファレンス ～『侵入前提』のサイバーセキュリティ対策～」を開催いたしました。

本ユーザカンファレンスでは、タイトルにもあるように ～『侵入前提』のサイバーセキュリティ対策～ と題して、攻撃者に侵入されても、迅速に対応可能な製品群を紹介する機会として、ご案内させていただいたところ、過去最多のお客様にご来場いただくことができました。

当日のセミナー風景

基調講演 『防衛大学校におけるネットワークセキュリティ』

防衛大学校 情報工学科 工学博士 中村 康弘 氏



防衛大学校 情報工学科
工学博士 中村 康弘氏

オープニングの基調講演は、防衛大学校 情報工学科 教授 工学博士 中村 康弘教授より、「防衛大学校におけるネットワークセキュリティ」 ～その実態と対応策～ と題して、ご講演いただきました。
トピックとしては、3部構成となります。

1. 過去のセキュリティ事案
2. 走査活動（攻撃予兆）の観測
3. 信頼性に基づくセキュリティ

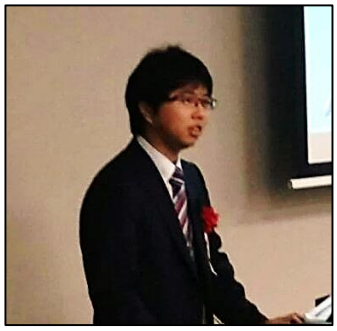
過去のセキュリティ事案では、防衛大学校でおきたインシデントの特徴および攻撃手法の変遷について、標的型攻撃を題材とし、過去の標的型メールが、防衛省職員や卒業生になりすまし、特定の個人を狙った攻撃が主流であったのに対し、現在では実在する企業から、「アカウントの不正利用が発生したこと」を語り、セキュリティ設定の再設定を強制させる攻撃が主流になっていることをご紹介いただきました。これらの攻撃に対し防衛大学校では、セキュリティ全般の見直しに着手し、物理的に通信手段を制限したり、情報セキュリティのリテラシーを高めるため、再度セキュリティの教育を実施したこと、そして最終的にはサイバー防衛隊を新設したことなどを、順序だてて非常に分りやすく、しかも専門的な切り口でお話いただきました。

続く走査活動（攻撃予兆）の観測では、インターネットからの防衛大学校への不審な偵察活動に関して、学校側が保有する有閑グローバルIPアドレスとハニーポットシステムによる観測活動について、詳しくお話いただきました。中村教授によると、これら観測活動は、アジアの特定の国からの定期的なアクセスであったことや、南米からの不正な偵察活動の期間や到着したパケットのペイロードの中身が非常に特徴的であること、また偵察活動自体が検知しにくく、攻撃者の意図も分り辛い旨を詳細にご説明いただきました。

最後の信頼性に基づくセキュリティでは、UNIXシステムの産みの親であるケン・トンプソンによるトンプソン・ハックのバックドア生成機能におけるその天才的な手法・手口を例とし、現在主流であるデジタル証明書のトラストアンカーでは、ブラウザにデフォルトで組み込まれた上位ルート認証局を無闇に信用・使用していること、そしてこれらが信頼の連鎖になっていることに対して、問題を提起されていました。

基調講演に続いて、インテリジェント ウェイブの各種セキュリティソリューションを順次紹介しました。まずはTrapsの製品紹介から。

国内でのオンプレミスの実績・経験を活かし、満を持してクラウド版をリリース
次世代エンドポイントセキュリティ対策「Traps　Ver5.0」（Palo Alto Networks社）



株式会社インテリジェント ウェイブ
高橋　一巨

既存のエンドポイントのセキュリティ対策製品の課題として、「シグネチャベースの従来型アンチウィルス製品の限界」、「AIや動的解析のみの実装では防ぎきれない(単一機能実装製品の弱点の存在)」、またマルウェア対策だけでなく、「脆弱性を悪用した攻撃に対しての防御の必要性」をご紹介させていただきました。 それらに対して、Trapsの機能及び多層防御の有用性について説明し、冒頭ご説明した課題に対する解決策を提示、 さらにTrapsの新バージョンである「Traps5.0」より実装された「クラウド環境」においての優位点や新たに追加された新機能についてご紹介させていただきました。

セッションの後半では、Traps5.0の導入の簡便さ、初期導入費用及び運用コスト削減、操作性・運用性が以前のバージョンに比べ大幅に向上したこと、またTrapsを導入可能な環境が拡張されたこと、 さらに将来Trapsに対する展望として「EDR機能の実装の方針」についても簡潔にご紹介させていただきしました。

攻撃者を囮情報で炙り出し、攻撃経路を排除する 「Deceptions Everywhere」（illusive networks社）

illusive networks社のDeceptions Everywhereでは、攻撃者がターゲットのシステム内に侵入し、被害を拡大させる”ラテラルムーブメント（横展開）”の仕組みがどういったものであるか、またすでに侵入されることを前提としたセキュリティ対策がいかに重要であるかについてご説明するとともに、製品の特徴である攻撃者視点でのリスク可視化およびリアルタイムならではの侵入検知・フォレンジック取得の有効性をご紹介させていただきました。

また欺瞞技術（デセプション製品）の進化の過程、類似製品であるハニーポット型製品と比較したDeceptions Everywhereの優位性について、新機能Attack Surface Managerによる攻撃リスクの事前管理・軽減手法や実際のコンソールイメージ（アタッカービュー、分析ダッシュボード等）による製品機能を元にご紹介させていただきました。

株式会社インテリジェント ウェイブ
川岡　晃

自律解析エンジンでプロキシログを分析し、隠れた脅威を発見「SecBI」（SecBI社）

株式会社インテリジェント ウェイブ
市瀬　裕子

Proxyサーバの通信ログ自動解析エンジンSecBIでは、セキュリティの多層防御とログ統合・相関分析製品（SIEMなど）導入中または、導入を予定している組織が直面する、ログの相関分析の運用の困難性、つまり「誰が毎日、どのような方法で膨大なログを分析するのかという問題」の解決策として、本製品では、機械学習エンジンをフルに活用し、攻撃の予兆を検出し、本来、分析活動の主体であるシニアアナリストのワークロード不足やスキル不足を支援する機能についてご紹介させていただきました。

本製品はエージェントレスであり、Proxyサーバのログを解析エンジンに送付（Collection）するだけで、機械学習エンジン（Autonomous Investigation）により脅威を判定し、それらを可視化（Visualization）します。これにより、中村教授が基調講演でも紹介されたような、攻撃者による偵察や不正な活動自体が検知しにくい通信を自動でクラスタ（グルーピング）化・解析し、不正な通信ログをグラフ化したり、不正な通信先や時間帯などの詳細な解析結果を出力する製品としてご紹介させていただきました。

CSIRTやSOCの運用負荷を軽減するインシデント対応支援ITPAツール「eyeShare」（ayehu社）

株式会社インテリジェント ウェイブ
秋山　茎一郎

ITPA（ITプロセスオートメーション）ツールであるayehu社のeyeShareは、複数のセキュリティ製品の導入による製品の増加と慢性的な人手不足というCSIRT/SOCの運用の問題を解決するソリューションとして、ご紹介させていただきました。
本製品は、コーディング不要な独自のワークフローを用いて、現在のオペレーション業務を自動化することにより、担当者ごとのスキルに依存しない、統合的なITオペレーション業務環境を実現します。それにより、セキュリティインシデントへの対応スピード向上を図り、セキュリティ運用にかかる負担を軽減・効率化します。

本製品は、イスラエルayehu社の長年にわたる運用ノウハウと最先端技術を背景に開発され、海外で180社を超える導入実績のある製品としてご紹介させていただきました。

マルウェアの実行が不可能な状況を作り出す第3世代のエンドポイント保護「Morphisec」（ Morphisec社）

本製品は現在まさに販売を開始したばかりの製品です。
企業を狙う標的型攻撃の起点は80%がエンドポイントであり、かつアプリケーションの脆弱性を悪用するエクスプロイト攻撃の割合も増加している現状に対し、既存のマルウェアテクニックからの推測による検知には限界があるため、新たなアプローチとして「攻撃対象の場所を変化させることで攻撃を成立させない」という手法でエンドポイントを保護するソリューション、「Morphisec」が有効であるということをご紹介させていただきました。

本製品もイスラエルで開発されたものであり、昨年2017年7月には世界で初めて「CCleaner」のバックドアを発見した実績のある強力なソリューションであることなどをご紹介させていただきました。

株式会社インテリジェント ウェイブ
茂木　康高

最新のイスラエル動向

株式会社インテリジェント ウェイブ
手塚　弘章

最後のセッションでは、恒例であるイスラエルの最新セキュリティ動向をご紹介させていただきました。

セッションの冒頭ではイスラエルの政治動向であるアメリカ大使館の移転問題から始まり、全世界的にはサイバー攻撃の解析アナリストが人材不足になっている状況をご説明させていただきました。
またソリューションとして、機械学習を利用する攻撃がトレンドになっておりセキュリティ対策にも機械学習が多用されていること、そしてサイバーインテリジェンスは、『単にインテリジェンスを提供』するモデルから『インテリジェンスを（積極的に）活用した不正取引検知ソリューション』に変遷しつつあり、単にサイバー攻撃への対策から攻撃による不正取引の検知に拡大しつつあることをご紹介させていただきました。

また最先端のソリューションとして、下記2つのスタートアップ企業のソリューションをご紹介させていただきました。
・インシデント発生時にアナリストが行う、アラート調査と付帯するセキュリティログの解析や判断、そしてインシデントレポート作成を自動的に行い、機械学習により知識ベースを拡大するアナリストロボット。
・セキュリティ対策に時間、人材、費用の負担が大きい中小企業向けに ISO-27001（ISMS）に則りセキュリティ運用を監視、評価を行い、かつ改善アドバイスを行うアプライアンス。

以上を今後のソリューションとしてご紹介し、カンファレンスの締めくくりとさせていただきました。

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。

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6回セキュリティユーザカンファレンスについて（2018年12月予定）

第6回セキュリティユーザカンファレンスは、2018年12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.