ITビジネスモデル委員会報告
2016年度　その２

トレンドマイクロ株式会社

「脅威動向・脅威の課題とその対策」

講師　セキュリティエキスパート本部

RTL　セキュリティスペシャリスト　　山田　敏寛　様

2016．6．29（水）　トレンドマイクロ株式会社（新宿マインズタワー）にて

プレゼン内容のポイントと質疑

１．今回は
　　下記項目について、お話をして頂いた

　　（１）RTL紹介
　　（２）脅威動向説明
　　（３）ウイルスデモ(遠隔操作)
　　（４）脅威の課題とその対策

２．質疑
　　・最近、車のセキュリティが問題になってきているが、この方面への対応は？
　　⇒対応しているが詳細は不明

感想

□標準型攻撃を具体的に見る事も、どんな方法で感染させるかなども見たことがなかったので、今回の攻撃手法の紹介から、本人が気づくこともなく簡単に個人情報や、企業内のPCを乗っ取られてしまうということに、脅威を感じる事が出来ました。
今後のIoTの時代には、もっと高度な仕掛けで甚大な被害が発生すると考えられ、一般企業で専門の人材がいない中、対策を考える、又は高度なセキュリティ面のコンサル人材の不足が、大きな社会問題となりますね。

□セキュリティ関連のセミナーを色々聞いてきましたが、今回のような、ビデオで手順を説明してもらったり、実機で流れに沿って説明していただく事で、非常に判り易かった。当社社内での勉強会でも活かしていきたいと思います。有難う御座いました。

□今までで一番興味深い内容でした．市場ニーズもあり、ビジネスにも結びつけやすいものだと思います

感想（続き）

□セキュリティの基礎から最新の技術や事例などは、とても参考になりました。
社内でも数千台のPC／Serverを利用しており、又、クラウドサービスも提供
していますので、専門チームでの日々の取り組みや、社内個々人への徹底が
必要かと思います。セキュリティ対策のニーズは益々広がりを見せているので、
事業面や営業面での取り組みは必要かと思います。

□今回のセミナーは私にとって大変新鮮でした。
自分自身のウイルス対策やサイバー攻撃などの認識は古い情報のままで、
現状の脅威と全く様変わりしている事に驚きました。特に企業が気づけない
間にサイバー攻撃によって重要な情報が痕跡無く持ち出されている事象は
非常に考えさせられました。
また時々アプリの脆弱性に関する記事やニュースを耳にしますが、今までは
聞き流していました。
最近の脅威はWebを閲覧しただけで、閲覧している使用者が知らない間に
脆弱アプリを自動検知してその隙間をついてウイルスが埋め込まれる。と言う
手法について、非常に脅威を感じました。
脆弱性について問題になるアプリとして、JAVA、IE、Adobe製品が特に要注意
との事。こちらも新たな情報として認識させて頂きました。

感想（続き）

□トレンドマイクロ社の脅威対応体制ならびに最近の脅威動向についてお話を伺いました。標的型攻撃ではメール文章や添付ファイルのアイコンなど巧妙に作成されており、かつ、メール送信元も偽装されているなど、気づかないうちに攻撃を受けているケースが多発しているとの事でした。
GUIを持った攻撃ツールでの脅威デモでは、いとも簡単に標的型攻撃ができることを目の当たりにし、驚きと同時に恐怖を覚えました。我々のお客様層においてはセキュリティに対する認識が非常に乏しいですが、このデモを見れば考えが変わるのではないかと感じました。
また、正規サイト汚染については、不正広告をクリックしなくても表示しただけでランサムウェアに感染してしまう事例もあるとの事で、こちらについても対策が必要な事が改めて理解できました。
さらには、ベンダーが脆弱性プログラムを公開してから7日経つとその脆弱性を突いた攻撃が行われるとの事で、脆弱性パッチの早期適用が非常に大切であるという事も学びました。
セキュリティ対策は保険と同じで被害にあわないとその重要性を感じにくいですが、今日のお話しを伺って重要性を再認識いたしました。

感想（続き）

□脅威ムービーと脅威デモが印象的で大変有意義でした。
偵察活動や侵入活動は話では当然の事として理解しているものの、ムービーで改めて見ることで認識を深める事が出来ました。また、侵入活動の失敗事例や成功事例は、ユーザーとして現実に攻撃を経験している立場なので更なる注意が必要と感じました。
デモでは便利な？ツールをご紹介頂き、攻撃が以外と容易に出来ることを知り驚きました。外部からのサイバー攻撃への3つの対策である、入口対策、出口対策、内部対策は当社でもアプライアンス製品を中心に推進をしていますが、まだまだ対策が不十分なお客様もいますので、更なる活動強化を図って行きたいと思います。また、今後益々、マシンラーニングやデーブラーニングなどのAIを搭載した新しいセキュリティ製品が登場してくると思いますので、製品の動向にも注意して参ります。

□今注目の標的型メールなどの最新の脅威動向について、学ぶことができた。
特に実際の標的型攻撃の手法の映像や、遠隔操作不正プログラムのデモ、ランサムウェア感染映像などは、IT業界に身を置く立場として、大きなインパクトであった。
また、現状の脅威は、一般的企業での標準対応となっている「ウィルス対策ソフト」レベルでは、防ぎようがないという事実を認識したが、対応可能なソリューションは、中小企業では、高額かつ複雑すぎるとの印象を持った。（続く）

感想（続き）

IT販売店により、「脅威対策ソリューションインテグレーション＋管理運用」
のサービスが強く求めらることが予想される。
より簡易に利用できるクラウド型の対策サービスが将来的には求められる
と思われる。

□トレンドマイクロ社と当社もお付き合いはありますが、リージョナルトレンドラボ
（RTL）を訪問させてもらうのは初めてでした。
グローバルなオフィス拠点、時差を活かしてのフィリピン、アメリカラボ、
その国、地域に特化した脅威を考慮した配置には、万全の体制、対応である
ことが伺えました。
脅威の動向については、過去は愉快犯、自分の腕を世に知らしめることから
金目的に変わっていっていることや、気づけない攻撃が多発している点など
わかりやすく説明いただけました。
また、動画、デモでも具体的な脅威と攻撃の様子、お客様にも訴求しやすい
内容と思っています。
脅威との戦いに終わりは無いのでしょうが、当社、お客様、個人ユーザーとしても
その対策（入口、出口、内部対策）の重要性があらためて感じられたプレゼンで
ありました。

編集後記

　今回は最新のセキュリティ対策の状況を聞きたいということで、トレンドマイクロ株式会社のRTL（リージョンナルトレンドラボ）の見学と講義をお願いした。
デモをみて驚いたのは、Web広告を見ただけで感染してしまうタイプの不正プログラムと、攻撃目標を1年以上掛けて調査し、侵入し、攻撃先が気がつかないうちに、重要データを盗まれたり、改ざんされるという攻撃があることであった。攻撃に気がついて調査する場合、三年分のログをとっておく必要があるという話にも納得であった。
最低限、最新のセキュリティツールを導入し、常に更新しておくことの重要性を認識させられたセミナーでした。

下記URLから今回のプレゼン内容がダウンロード出来ます（会員限定）

https://www.jcssa.or.jp/memberJCSSA/dl2.php