アンラボ・セキュリティレター

Press Ahn

2015.3　Vol.15

ハッカーの標的、POS システム

POS システムを狙う脅威と AhnLab EPS

ハッカーの標的、POS システム

2013年、クリスマス商戦の開幕「ブラックフライデー」シーズンに米国の大型流通メーカーで顧客の個人情報の流出事件が発生。これは日常よく使われる決済システム「POS」がハッカーの攻撃対象になった上、2300億ウォンという莫大な金銭的被害が発生したことから、世界を驚かせた。これまで専門家らの警告にもかかわらず見落としていたPOSシステムのセキュリティ脅威が、現実のものとなったのである。実際、POSシステムを狙ったハッキング事件が発生したのは今に始まったことではない。2009年に初めてPOSマルウェアが発見されて以降、毎年脅威は増加する一方でPOSシステム環境に適したセキュリティ対策は不十分な状態だ。
今回のコラムではPOSシステムが持つ特殊性とPOSシステムを脅かすセキュリティ脅威、そしてPOSシステムに特化したアンラボのセキュリティソリューション「AhnLab EPS」を紹介した。

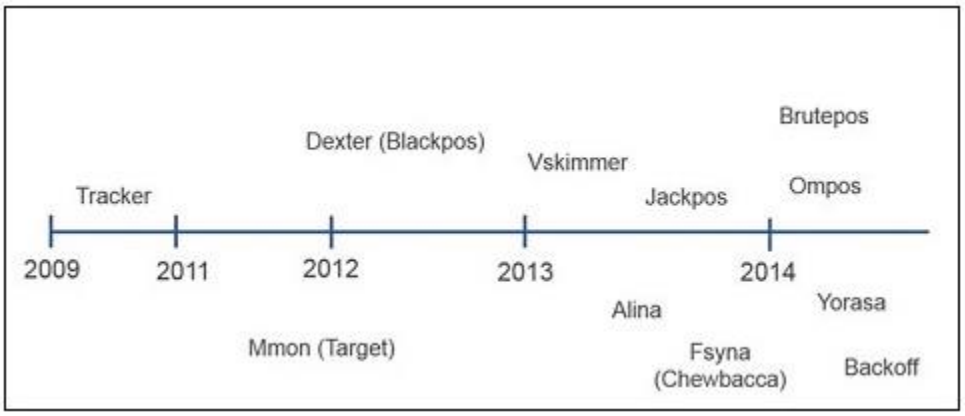
なぜ POS システムなのか

アンラボが毎年発表する「情報セキュリティトレンドレポート」では、POSシステムへの攻撃が本格化することを予測していた。展望では今年はPOS端末への攻撃だけでなく、POSシステムの製造元を対象にハッキングの試みが発生するなど、より多様で強力な攻撃方法が登場すると予想した。
ここで、なぜハッカーがPOSシステムを狙うのか、POSシステムとは何かを見てみよう。

[図1] POSシステムの運用方法 *出典：epson-biz.com

POS（Point of Sales）システムは、店舗販売と同時に品目・価格・数量などの流通情報をコンピューターに入力して、情報を分析・活用する管理システムである。これにより品物の会計はもちろんのこと、頻繁に売上高の動向を把握して在庫管理をするなど、商品管理において重要な役割を担うコアシステムなのだ。今では支払い・会計・営業状況・在庫管理などの運用情報提供に加えて様々なポイントや会員情報などの顧客管理用にも使用されている。最近いくつかのサービスプロバイダは、POSの顧客情報と顧客のデバイス位置情報やアプリ（APP）の使用データなど、多様なデータの融合により顧客へのサービス改善に向けた情報も提供しており、この分野はクラウド連携とともに、今後ますます発展していくものと見られる。

このようにPOSシステムの使用度がはますます高まる中、重要な情報を取り扱っているにも関わらずセキュリティ対策は不十分な状況だ。一般的に、POSプログラムはシステムメモリ1GB程度の低仕様端末で運用され、セキュリティ対策ソリューションどころかWindows更新プログラムも正常にアップデートされないような状況なのである。またPOSシステムでインターネット検索をするなど、簡単に脅威にさらされてしまう環境も問題だ。
結論から言えばハッカーがPOSシステムを狙う理由は明確だ。セキュリティが脆弱なのに対して価値ある重要な情報を大量に保有しているからだ。



[図2] 2009年~2014年に発見された主なPOS用マルウェア

POS システムの脆弱性と対策の限界

様々な接続によるネットワークセキュリティ脅威

大型流通店舗ではPOSシステムと支払いの承認ネットワークを別々の専用線から使用する。しかし前述の通り、様々な顧客管理情報と連携するため、実際は他のネットワークにも接続されている。中小規模の会社や小売店の場合は、パブリック（public）インターネットや携帯電話（Cellular）を介してPOSシステムを接続して支払いの承認をしたり、サービス型ソフトウェア（Software as a Service、SaaS）のクラウドベースPOSで運営されることもある。これではセキュリティホールが存在しないほうがおかしい状況で、特に無線インターネットと接続している場合は、なおさら侵入される可能性が高くなる。

サービス終了OSを使用

現在ほとんどのPOSシステムは、サービスが終了したWindows XPとこれをベースにしたWEPOS（Windows Embedded for Point of Service）、POSReady2009（Windows Embedded POSReady2009）を使用している。XP系列のOSは2001年にリリースされ、多数の脆弱性や攻撃手法が発見されてきた。すでにサービス終了のOSであるため、セキュリティパッチなどの更新サービスが提供されないだけに非常に脆弱なのだ。

アプリケーション脆弱性

POSシステムでは汎用OS以外にもリモート制御プログラム、Internet Explorer、Adobe Reader、MS Officeなど様々なプログラムも一緒にインストールして使用している。これによって一般のデスクトップ同様に脆弱性が生じるしかなく、ブラウザ、PDF、DOCなどの文書は、Java脆弱性を突かれてマルウェア感染を引き起こし、攻撃者はPOSシステムを手中に収めることができる。

インターネット、外部ストレージの使用

スタッフが個人用PCを使用するかのようにPOSシステムを使用すると脅威にさらされる可能性が高くなる。USBメモリから音楽ファイルをコピーしたり、電子メール、SNSなどの個人的なインターネットの使用、ドキュメント作業など、POSシステム以外のプログラムとメディア、ネットを使用することでマルウェアの侵入だけでなく高度化した攻撃の脅威にさらされてしまう。

だが多様な脆弱性や社会工学的手法など多くの脅威にさらされているにも関わらず、現状セキュリティはアンチウイルスソフトウェアの使用とデータの暗号化、暗号通信程度にとどまっている。マルウェアに掌握されたPOSシステムではデータの暗号化や暗号通信が無意味になる上、シグネチャベースのアンチウイルスソフトウェアの場合はすでにマルウェアに対して脆弱といえる。もちろん低仕様の端末と制限的なネットワーク速度という環境上、常にシグネチャを更新して定期的にスキャンするウイルス対策ソフトウェアを作動させるのは難しいという点も考慮しなければならない。

POS システム、一般 PC とは異なるアプローチが必要

POSシステムのハッキングは、クレジットカード情報とカードを使用した顧客情報、ポイントや会員情報まで奪取し、カードの複製や取得情報の2次、3次に渡る取引きなど、様々な犯罪に悪用される可能性がある。一度突破されてしまえば被害が甚大であるだけにPOSシステムのセキュリティは一般PCよりも強力な仕様が求められ、多角的な対策が必要だ。

基本的なステップとして、まずPOSシステムのログインパスワードを複雑に設定・定期的に変更して、なるべくVNC、Remote Desktopなどのリモート制御プログラムを使用しないようにする。実際に昨年の某フォーラムで進行したプロジェクトでは、「pos12345」、「posadmin」のように推定されやすいパスワードとリモート接続でPOSシステムの権限を奪取し、マルウェアを感染させてクレジットカード情報を盗むことができると説明していた (http://www.theregister.co.uk/2014/07/09/botnet_brute_forces_pos/)。

また決済に必要なネットワーク接続のほか、パブリックインターネットの接続やWi-Fiなどはすべて使用しないようにし、やむを得ずインターネット接続が必要な場合はファイアウォールを使用して必要な接続だけを許可する。さらにスタッフ教育よって個人的なネット利用や外付けストレージ、文書作業など不要なプログラムを使用しないようにする。

そして何よりも重要なのはすべての攻撃の起点となるマルウェアの侵入と実行を遮断しなければならない。POSなどの特殊なシステムは、一般的なPCとは異なり使用するアプリケーションが明確に定義されるため、非常に限定的な作業を遂行することになる。しかしこのような特殊な環境においても、汎用OSをベースにして同じく脅威にさらされることで、一般PC同様のセキュリティシステムを適用せざるえない状況だ。よってPOSシステム用に適した必要最低限のプログラムやリソースのみを限定使用させる環境構成が必要だ。一般PC向けアンチウイルスソフトウェアでは、標的型攻撃や高度化された脅威をブロックすることが難しいからだ。

加えてアンチウイルスソフトウェアは、定期的なシグネチャの更新やディスクスキャン等を実行する必要があるため、低仕様で運用されるPOSシステムに過負荷を与えて支払いの遅延や通信障害などを発生させる可能性もある。

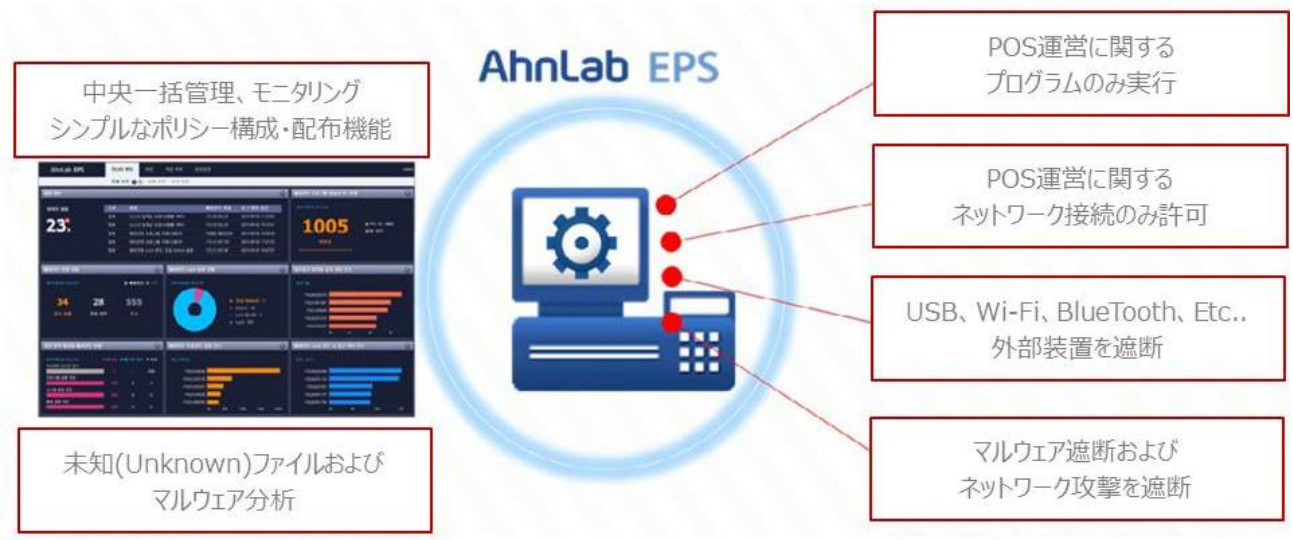
このような理由からPOSシステムのセキュリティアプリケーションコントロール製品が注目されているが、これらの製品は管理者の専門的な知識をもとにアプリケーション使用/遮断に関する高度なポリシー管理能力が求められる。それにセキュリティ製品ではなく管理製品であるため、マルウェアの侵入・感染有無の検知だけでなく悪質の有無まで判断・対応するには、セキュリティ専門家の管理が必要だ。だが中小規模商店でここまで管理することは難しいため、アプリケーションコントロール製品は仮に導入されたとしても長期的な管理は厳しいだろう。

[図3] 一般的なオフィスPC vs. POSシステム環境

POS システム専用セキュリティソリューション「AhnLab EPS」

AhnLab EPS（Endpoint Protection System）は、POSのような特殊目的を持つエンドポイント（fixed function devices）専用セキュリティソリューションだ。本製品はシステムの安定的な運用のための感度が高く、ポリシーによって許可されたプログラムのみ使用可能にする自動化端末および制御用システムなどに最適化されたソリューションである。

高度な運用能力を要するアプリケーションコントロール（Application Control）製品とは異なり、インテリジェントなホワイトリスト（WhiteList）ベースに運営システム上必要なプログラムの実行・ネットワーク接続・システムリソースのみ使用可能にする。これによりPOSと関連のない不要なプログラムの実行を遮断して、マルウェアの侵入とアクションを抑制できる。



[図4] AhnLab EPSの主要機能

AhnLab EPSの主な機能は次の通りだ。

✓ 強力なマルウェア検知・拡散防止機能

■サーバーで保有するマルウェア検知・駆除エンジンによってAgentのインシデント拡散防止

■IP、ポート遮断および外部ストレージのAUTORUN防止による感染遮断

■OSパッチのアップデート有無に関係なくセキュリティ性を確保

✓ 非業務プログラムの実行および不要なストレージをブロック

■許可されたアプリケーションおよびネットワーク接続のみ使用できるように管理

■非業務用のストレージを接続遮断

✓ 超軽量化されたセキュリティおよび端末制御ソリューション

■Agentがインストールされる端末の制御システムメモリ、CPU使用率を最小化

■リソースを使用するすべての作業は、別のサーバーで実行

✓ 中央集中型管理システム

■ダッシュボードからすべてのAgentを一元管理

■Agentグループ機能によるスピーディなアクセス

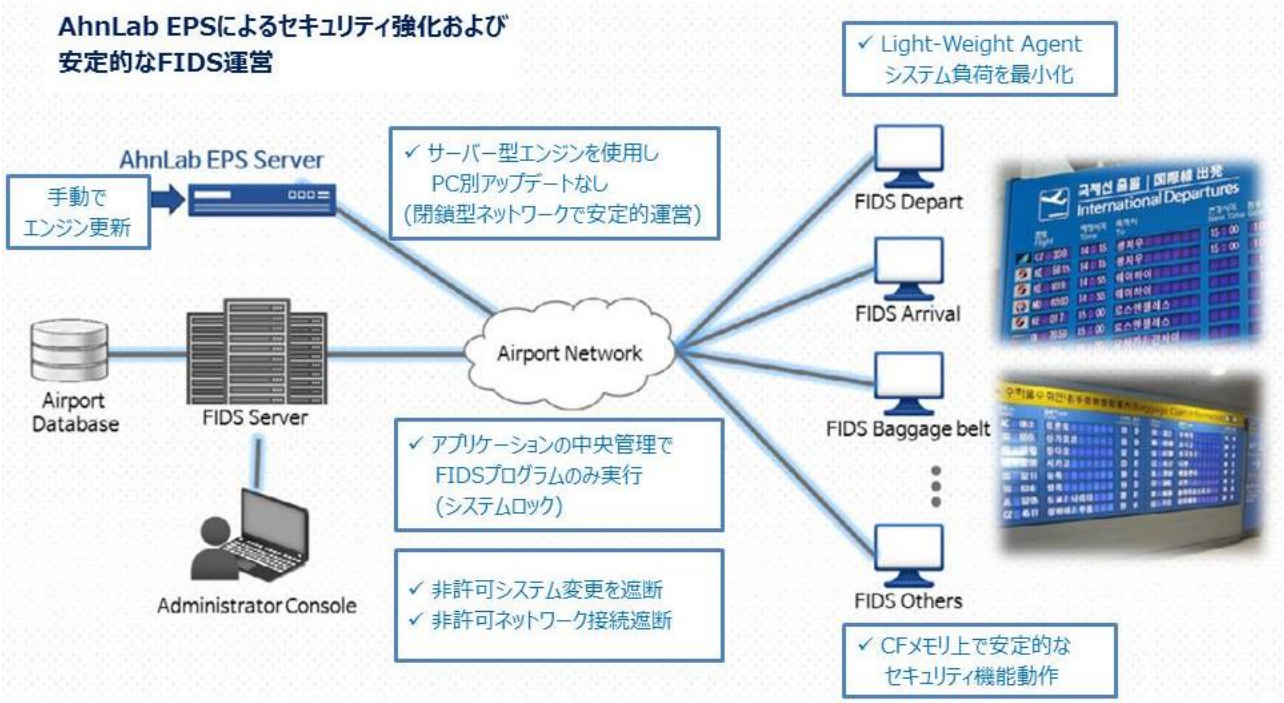
■Agentがインストールされていない端末をチェックし、リモートでシステムチェック

■アラート機能とログ管理

AhnLab EPSは高度なホワイトリスト方式のアプリケーション制御機能を搭載し、優れたユーザビリティによりセキュリティの専門知識がなくても運用が可能で、中央管理システムによって加盟店の運用負担を軽減させる。またAhnLab EPSサーバーのマルウェア分析エンジンにより、アンチウイルス機能の定期更新とネットワークやシステムリソースを使用することなく悪質なコードを検知・遮断できる。さらにシステムリソースをほとんど使用せずに実行可能ファイルに対するリアルタイム分析も可能だ。これはPOS端末のマルウェア対応と未知（Unknown）の脅威を分析することも可能にし、別途のアンチウイルスソリューションを追加購入/インストールする必要がないことを意味する。

本製品は、強力なモード機能によりPOSシステム運用に必要なアプリケーション使用設定や外部ストレージ、ネットワーク接続制御技術で外部からの攻撃と未知の脅威からシステムを保護することができる。また、サーバーから提供されるマルウェアの検知・分析機能とセキュリティポリシー管理によって、すべてのシステムが常に安全なファイルで動作するように維持する。これは事前に危険要素を徹底的に遮断することでPOSシステムの運用性を重視し、さらに検知・対応機能によりポリシー強化まで可能にする。

AhnLab EPSは韓国ではダイソー、Shinsegaeデパートなど大型流通業者のPOSシステムに採用され、パフォーマンスと安定性の面ですでに検証済みの製品だ。また半導体や家電の生産ライン、産業設備制御、キオスク（KIOSK）、ATMなどの様々な分野で運用中だ。



[図5] A空港のAhnLab EPS構築事例

実際に韓国のA空港に導入されたケースを紹介する。この空港のFIDSは1800台以上、HDDなしの低仕様端末にWindows XP Embeddedシステムで構成され、一般的なアンチウイルスソフトウェア以外セキュリティ対策が施されていない状態だった。しかし、システム使用率が高く持続的なシグネチャパターンの更新が必要なアンチウイルスソフトウェアでは、負荷がかさみ対応に限界があった。これらの問題を解決するため、アンチウイルスソフトウェアの代わりにAhnLab EPSを導入することに。端末制御とセキュリティ機能の両方を持つ本製品が採用されることで、FIDSシステムの運用に影響を与えることなく安定的な保護環境を構築した。

AhnLab EPSは特殊目的のシステム専用のソリューションであり、システムリソースと関連業務のプロセスに影響を与えずにマルウェア対策と制御が可能だ。これにより情報流出防止と生産性の向上・管理・運用コストの削減を実現できるだろう。

http://jp.ahnlab.com

http://global.ahnlab.com

http://www.ahnlab.com

アンラボとは

株式会社アンラボは、業界をリードする情報セキュリティソリューションの開発会社です。
1995年から弊社では情報セキュリティ分野におけるイノベーターとして最先端技術と高品質のサービスをご提供できるように努力を傾けてまいりました。今後もお客様のビジネス継続性をお守りし、安心できるIT環境づくりに貢献しながらセキュリティ業界の先駆者になれるよう邁進してまいります。
アンラボはデスクトップおよびサーバー、携帯電話、オンライントランザクション、ネットワークアプライアンスなど多岐にわたる総合セキュリティ製品のラインナップを揃えております。どの製品も世界トップクラスのセキュリティレベルを誇り、グローバル向けコンサルタントサービスを含む包括的なセキュリティサービスをお届け致します。

AhnLab

〒101-002 東京都千代田区外神田4-14-1 秋葉原ＵＤＸ ８階北 | Tel：03-5209-8610 (代)