Publication: Tsushin Kogyo Shimbun (Telecommunications Industry Newspaper, Japan)
Date: 2011/11/28
Subject: How to Prevent Targeted Cyber Attacks – Implementation of Cloud Technology
Keynote Speech by Mr. Nir Zuk (CTO, Palo Alto Networks) at NetEvents 2011

通信興業新聞

平成23年11月28日

米パロアルト 標的型サイバー攻撃を

世界の主要テレコム関連企業のトップが一堂に会し、市場の最新動向や共通課題、技術展望について議論する「ネットイベント2011――APACプレスサミット」が11月16日、17日の両日、タイのプーケットで開催された。初日の基調講演には、世界でサイバー攻撃が頻発している状況を踏まえ、米パロアルトネットワークスの創業者兼CTOのニア・ズーク氏が登壇し、モダンマルウェアの防御策について語った。この中でズーク氏は、「企業や組織のウイークポイントを徹底的に探して攻撃してくる標的型攻撃は防御できる。パロアルトの次世代ファイアウォールとクラウド型セキュリティサービス『ワイルドファイア』はそのための有効な選択肢となる」と述べた。

パロアルトCTOのニア・ズーク氏は「ネットイベント」初日の基調講演冒頭で、ソニーのプレイステーションネットワークを狙った大規模なサイバー攻撃についての見解を示すとともに、最近のセキュリティ攻撃の特徴を次のように説明した。

「ソニーに対してハッカーが新しい攻撃を仕掛けたことで、多くの顧客を失った。時期を同じくして、複数の企業も同様のサイバー攻撃を受けたが、共通しているのは、これまでにない新しい方法『モダンマルウェア』による攻撃が行われたこと。もはや既存のセキュリティ対策では止めることができない。そこで、まずは敵について知ることが大切だ」

ズーク氏は、最近のセキュリティ攻撃が、①クライアントPCにマルウェアを仕掛ける、②クライアントPCの脆弱性を突く、③クライアントPCに悪意のあるプログラムをダウンロードさせる、④クライアントPCにバックチャンネルを仕掛ける、⑤機密情報を盗む――の5つのステップを踏んで行われると述べた上で、「最初のステップは、攻撃対象企業の社員やエンドユーザが狙われるようになってきた。SNSやメッセンジャーを用いて、知り合いを装ってマルウェアを仕掛けたPDFファイルやパワーポイントの資料を送りつける。知人から受け取ったデータだと、疑わずに開いてしまう。これまでの攻撃と異なり、データセンターにあるウェブサーバではなく、その先にいる個人、エンドユーザが最初の標的となってきている。これが新しいアタッカーの特徴だ」と指摘した。

こうしたセキュリティ攻撃をブロックするには5つのすべてのステップにおいて、何らかの対策を打つ必要があると訴えた。ただし、既存のIPSやウイルス対策ソフトでは対処しきれないと指摘。「モダンマルウェアの防御においては、対応のスピードがカギになる。現在のIPSやウイルス対策ソフトはシグネチャの作成に2~3カ月かかっており、これでは遅すぎる。また、広範囲にわたって攻撃が試みられる可能性もあることから、セキュリティリサーチ作業の自動化も必須だ。パロアルトが提供している次世代ファイアウォールならば、こうした新たな攻撃、『モダンマルウェア』から企業を守ることができる」と強調した。

パロアルトが提供する次世代ファイアウォールは、すべてのアプリケーションおよび社員やユーザの特性を識別して可視化するとともに、リアルタイムでのコンテンツの検査を行うアプライアンスとして、暗号化された通信にも対応しているという。

同氏は11月に発表した、標的型攻撃をブロックするクラウド型のセキュリティサービス「ワイルドファイア」の有効性もアピールした。同サービスは、顧客の環境で検知した信頼できないゾーンから受信したファイルをクラウド環境上の仮想サンドボックス環境で実行することで振る舞いベースによりマルウェアを検知し、そのマルウェアに対するシグネチャを自動的に生成して配信するというサービス。PAシリーズのOSの最新版「PAN-OS4・1」に搭載される。具体的な機能としては、①ポリシー条件に対するURLカテゴリの追加、②ユーザID機能におけるユーザ識別機能の追加、③レポート機能の日本語対応――などが現在、70以上の振る舞いを検査することができ、検査を行うサーバは日本にも設置されるという。

同社の菅原継顕マーケテ

ネットイベント会場（上）と基調講演するニア・ズーク氏

パロアルト
次世代FWを投入
マクローリン社長「仮想化に注力」

パロアルトネットワークスは11月7日、ブランチオフィス向け次世代ファイアウォール製品「PA-200」、リモートアクセス製品グローバルプロテクト」の最新版、ファイアウォールサービス「ワイルドファイア」を発表した。「PA-200」は同社の次世代ファイアウォール製品のエントリーモデルで、大規模企業のブランチオフィスでの利用を想定した製品。一方の「グローバルプロテクト」は、SSL-VPNモジュールの「ネットコネクト」を統合し、アイパッド、アイフォーン、マックOSXといったアップル製品をサポートしたもの。

「ワイルドファイア」はクラウド環境上の仮想サンドボックス環境でファイルを実行することにより振る舞いベースでマルウェアを検知し、そのマルウェアに

マクローリン社長

「PA-200」

PSやウイルス対策ソフトがシグネチャの作成に2~3カ月かかっていた時間を短縮し、シグネチャの配信をマルウェアの検知から24時間以内で可能になった。さらに「将来的には1時間にまで短縮する予定だ」（ズーク氏）。

さらにワイルドファイアについてズーク氏は、「標的型攻撃を防御するためサンドボックスを利用したクラウドサービスとなる。検知を回避する能力を備えた未知のマルウェアによる標的型攻撃が多発している現状に対応し、悪意のあるファイルを仮想クラウドベースの環境で自動的に実行し

基調講演の

規模なサイバ

被害が深刻化

的型攻撃を防御

で、企業や組織

ポイントを徹底

攻撃してくる

防御できる。

新製品「ワイル

サービスはそ

な選択肢と

次世代ファイ

品群への自信

グネチャ定期

を通じて提供

マルウェアが

のか、誰が

ったのか、そ

だアプリは何

析結果も提供

明した。

情報通信機器 及び
通信ケーブル・電線、工事材料の専門商社
原電電気株式会社

通信興業新聞

通信興業新聞社
発行所 東京都中央区銀座7－3－13
発行人 鈴木 茂
郵便番号 104-0061
電話 (03)3572-4488(代)
FAX (03)3572-4866
振替口座 00170-6-100661