




[NetEvents]モダンマルウェアは必ず防御できる - Paloalt創業者Zurk氏

マイナビニュース 2011年11月17日（木）08:30

アジア太平洋のプレス/アナリスト向けテクノロジー・カンファレンス「NetEvents APAC Press and Analyst

Summit」が11月16日・17日に、タイのプーケットで開催されている。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、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。

同氏は開口一番、「今年に入り、**RSA**、ソニーの**PlayStation Network**を狙った大規模なサイバー攻撃が行われたが、こうしたモダンマルウェアによる攻撃は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」と述べたうえで、「まずは、敵について知ることが大切」として、最近のセキュリティ攻撃の特徴を説明した。

○攻撃の全ステップにおいて対策が必要

ズー

ク氏は、最近のセキュリティ攻撃を「クライアントPCにマルウェアを仕掛ける」、「クライアントPCの脆弱性を突く」、「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」、「クライアントPCにバックチャンネルを仕掛ける」、「機密情報を盗む」という5つのステップを踏んで行われると述べた。

「最

初のステップは、**SNS**やメッセージャーを用いて、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、**Web**サーバではなく、エンドユーザーが狙われるようになってきている」

同氏は、セキュリティ攻撃をブロックするには、これら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」と同氏。「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1週間程度かかっており、これでは遅すぎる。また、作業

の自動化も必須だ」

○パロアルトが出した解はクラウドサービス「WildFire」

こうしたなか、「われわれが提供している次世代ファイアウォールならば、モダンマルウェアから企業を守ることができる」と、ズーク氏は述べた。

同社が提供している次世代ファイアウォールは、「アプリケーション」「ユーザー」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だ。これらは暗号化された通信にも対応している。

同

氏は今月発表した、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「WildFire」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ものだ。

現在のところ、シグネチャの配信はマルウェアを検知してから24時間以内となっているが、将来的には1時間にまで短縮する予定だという。

同氏はWildFireでは、シグネチャの自動生成・配信に加えて、マルウェアによってレジストリを書き換えられたファイルを元に戻すことも可能だと説明した。

国内でも大規模なサイバー攻撃に関する報道を聞かない日がないくらい、被害が深刻化している。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に対し、もはや打つ手はないとも言われているが、ズーク氏は「標的型攻撃は防御できる」と自信を見せる。

標的型攻撃に戦々恐々としている企業や組織にとって、パロアルトの製品とサービスは有効な選択肢となるであろう。