

IPv6 と侵入防御：IPv6 を考慮したセキュリティ対策とは

http://www.checkpoint.co.jp/securitycafe/main_topic.html



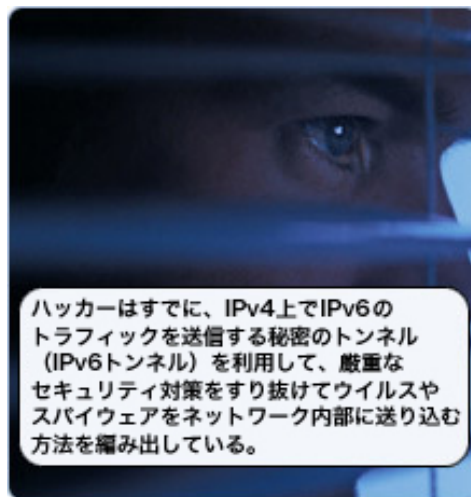
IPv4 の後継となるインターネット・プロトコル IPv6 が登場したとき、技術者と政府関係者は、ネットワーク界の一大変革であるとしてそろって歓迎の意を表明しました。この新しいインターネット・プロトコルは、あらゆるモバイル・デバイスにアドレスを割り当ててもなお余りが出るほどの、天文学的ともいえる数のアドレスをサポートしています。米国政府は2006年、すべての連邦政府機関に対し、2008年中にバックボーンを IPv6 に移行するよう義務付けました。この規定により、民間においても IPv6 の普及が進むと見込まれており、実際、すでに多くの企業が IPv6 への移行に踏み切っています。

興味深いのは、IPv6 のトラフィックをやりとりするのに、必ずしもネットワークが IPv6 をサポートしている必要はないということと、ネットワークに対する攻撃に利用することが可能ということです。ハッカーはすでに、IPv4 上で IPv6 のトラフィックを送信する秘密のトンネル (IPv6 トンネル) を利用して、厳重なセキュリティ対策をすり抜けてウイルスやワーム、スパイウェアをネットワーク内部に送り込む方法を編み出しています。大手の市場調査会社はまだ、この IPv6 を利用した攻撃を大きく取り上げることはしていませんが、近年、この種の攻撃は数多く報告されています。本稿では、問題の深刻さ、自社に影響があるかどうかを確認する方法、この攻撃からネットワークを保護する方法について解説します。

IPv6 が必要な理由

IPv6 を利用した攻撃について解説する前に、IPv6 自体について説明します。IPv6 では、IPv4 よりも圧倒的に多くのネットワーク・アドレスを利用できるというだけでなく、セキュリティの面からも魅力的な機能が数多く提供されます。IPv6 は、信頼性が高く、セットアップが容易で、設定が自動的に行われます。また IPv6 はアドレス空間が広大で、アドレスの割り当て密度を低くできることから、IPv6 を使用したネットワークは悪意あるスキャンの影響を受けにくくなります。これは、自己複製するワームにとっても不都合なネットワークであるということの意味します。つまり、IPv6 ネットワークは本質的に安全性の高いネットワークだということです。

とはいえ、IPv6 も完璧というわけではありません。セキュリティ侵害のほとんどはアプリケーション・レベルで発生しており、IPv6 を適切に導入したとしても、それだけで単純にセキュリティが強化されるとはいえません。また、設定が不適切なサーバ、設計に問題のあるアプリケーションやサイトを IPv6 で保護することもできません。そしておそらく最大の問題は、この新プロトコルがどれだけ複雑であるかをまだ誰も正確には把握できていないために、攻撃者が IPv6 を利用して不正な活動を長期にわたり隠蔽することができてしまうという点です。物騒な話に聞こえるかもしれませんが、これは決して絵空事ではありません。



IPv6 の現状

簡単に言ってしまうと、IPv6 トンネルはどこにでも存在しています。IPv6 は、すべての Unix プラットフォームにおいてデフォルトで有効にされており、また Windows でも Windows 2000 SP2 以降であれば簡単に追加することができます。このため、既存のネットワークに IPv6 トンネルを構築することは比較的容易に行えてしまいます。

IPv6 トンネルはおそらくどのネットワークにも存在しており、探し方と探す場所さえ分かればそれを見つけ出すことは決して難しくありません。ネットワーク管理者は、このトンネルがハッカーに見つけられないようにする必要があります。

このトンネルが攻撃に利用可能であるということをハッカーが最初に発見したのは 2001 年 12 月のことで、それ以来、この手法は現在に至るまで使われ続けてきました。今日、この種の攻撃のほとんどでは「トロイの木馬」の手法が用いられています。つまり、IPv6 トンネルを経由することにより、IPv4 での標準的なセキュリティ対策をすり抜けてネットワーク内部に潜入できるようにしているのです。こうしてネットワーク内部に到達したウイルスなどのマルウェアは、外部にいるハッカーから命令を受け、不正活動を開始します。この攻撃はネットワーク内部から行われるため、基本的な侵入防御システム (IPS) で事前に検出することはできません。また、ほとんどの IPS 製品はまだ IPv6 (IPv6 over IPv6 や IPv6 over IPv4 トンネル) をサポートしていないため、この種の攻撃は検出されないままネットワークに侵入できてしまいます。

IPv6 を利用した攻撃を防ぐには

IPv6 トンネルはどこにでも存在するので、この種の攻撃からネットワークを保護するためには、トンネルを探し出して無効にする必要があります。そのための第 1 ステップは、目立たずに隠れている IPv6 トラフィックを、少なくとも 1 つのレイヤでは確実に認識できる仕組みを整えることです。注意が必要なのは、これは IPv6 アドレスを管理することを目的としたものではないということです。IPv6 アドレスの管理は、全く種類の異なる別のタスクです。ここで行うのは、内向きと外向きのすべてのインターネット・トラフィックを検査して、IPv6 のデータを見つけ出すことです。つまり、許可されていない通信が行われていないかどうかトラフィックを監視するのです。

すべてのトラフィックを監視してデコードすることにより、ネットワークのどこに IPv6 トンネルがあるのかを的確に把握することができます。トンネルが見つかったら、ハッカーに発見される前にそれらを無効にします。トンネルを無効にするのはポートをブロックするのと同じくらい簡単な作業で、ごく短時間で行うことができますこれらのトンネルをすべて無効にすれば、ハッカーがセキュリティ対策をすり抜けてネットワーク内部に密かにデータを送り込むことはできなくなります。これにより、ネットワークのセキュリティが飛躍的に高まり、機密性の高い企業データを脅威から保護できるようになります。

チェック・ポイントのアプローチ

チェック・ポイントの IPS-1 は、危険性のある不正な IPv6 トラフィックを遮断する機能を備えています。大規模環境にも対応する IPS-1 の侵入防御機能は、Hybrid Detection Engine を搭載することにより、誤検出の少ない、正確で精度の高い検出を実現しています。このエンジンは IPv6 を完全にサポートしているため、現時点では検出が困難な IPv6 を利用した攻撃も確実にブロックすることができます。これにより、IPv4 環境であるか IPv6 環境であるかを問わず、あらゆるネットワークの安全性を高めることが可能になります。