公開サーバの脆弱性を狙った攻撃シナリオと対策ポイント

今日では多くの企業が公開サーバを運用し、ネット販売やキャンペーンサイト等を活用したビジネスを展開しています。こうした公開サーバの運用においては、ビジネスのメリットが大きい反面、サイバー犯罪者に狙われやすいリスクがあり、実際に公開サーバが攻撃され顧客の個人情報やクレジットカード情報等が漏えいした事例が複数報道されています。

公開サーバの脆弱性を狙う攻撃者は一体どのようなシナリオで攻撃を仕掛けてくるのでしょうか。公開サーバの脆弱性を狙う攻撃シナリオとその対策ポイントを 3 つのフェーズ（①調査フェーズ ②攻撃フェーズ ③侵害後フェーズ）に分け、本ドキュメントでは ①調査フェーズ について解説します。

調査フェーズについて

「Heartbleed」や「Shellshock」といったクリティカルな脆弱性が明らかになり、攻撃コードが公開されるといった状況でない限り、攻撃者が少ない攻撃回数 で公開サーバを侵害することは困難です。攻撃者は、まずターゲットのサーバが攻略できそうかどうか、脆弱性がありそうかどうかを確認するため、ポートスキャンや複数の攻撃通信によって調査を行います。

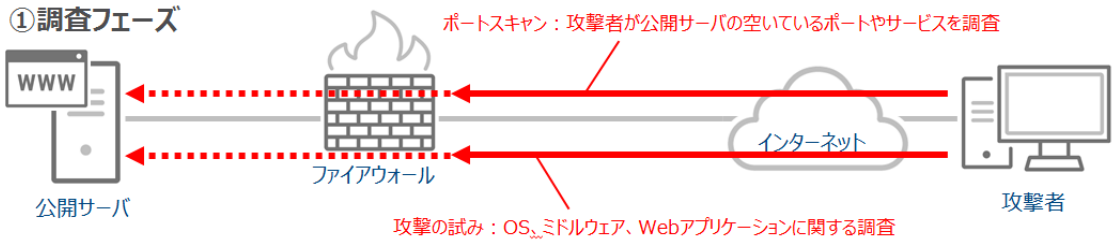

図 1：攻撃シナリオ ： 調査フェーズイメージ

こうした通信は、既存のファイアウォールで止められるものもありますが、完全にブロックすることは難しいでしょう。例えば、ポートスキャンのツールでも、ファイアウォール等の機器をすり抜けるオプションが用意されているものがあり、こうした調査行為の通信は公開サーバに届く可能性があります。
自社の公開サーバがこうした調査行為に遭った場合、どのような対策が必要になるのでしょうか。

調査フェーズの対策ポイント

調査フェーズの対策では、ポートスキャンや攻撃通信を防ぐことで、自社の公開サーバの攻略は難しいという印象を攻撃者に与えることが重要です。その結果、攻撃者が自社の公開サーバに対する攻撃をあきらめる可能性があります。

攻撃者は調査フェーズで見つけた公開サーバの脆弱な箇所を起点に次の攻撃を仕掛けてきます。まずは、既存ファイアウォールでポートスキャン等の調査行為を防ぎましょう。しかし、前述したとおり、ファイアウォールですべてを防ぐことは難しいため、トレンドマイクロでは、こうしたセキュリティリスクを解決するために、統合型サーバセキュリティソリューション「Trend Micro Deep Security™（以下、「Deep Security」）」を活用したセキュリティ強化をお勧めします。

対策ポイント	内容	対策
ファイアウォールで脅威を軽減	ポートスキャンや攻撃通信を軽減する	既存ファイアウォール
OS、ミドルウェアに対する攻撃をブロック	ポートスキャンやOS、ミドルウェアを狙った攻撃通信をブロックする	Deep Security（IPS（侵入防御））
Webアプリケーションに対する攻撃をブロック	Webアプリケーションを狙った攻撃通信をブロックする	Deep Security（IPS（侵入防御））
攻撃元の通信をブロック	検知した攻撃元IPアドレスから来る通信をファイアウォールまたはサーバ側で完全にブロック	Deep Security（ファイアウォール）

図 2：攻撃シナリオ：調査フェーズでの対策ポイント

OS、ミドルウェアに関する情報収集を目的とした調査行為や Web アプリケーションの脆弱性を狙った攻撃通信を検知・ブロックする対策が必要になってきます。Deep Security には、OS やミドルウェア、Web アプリケーションの脆弱性を狙った攻撃をブロックする「IPS（侵入防御）」機能が実装されています。また、Deep Security のログから攻撃通信の送信元を特定することで、同じ送信元からの攻撃通信を全てファイアウォールでブロックする対策も有効です。ファイアウォールで通信をブロックする場合、以下 2 つの方法があります。

1．外側ファイアウォールでブロック：インターネットと企業との境界にあるファイアウォールでブロック。この場合、ファイアウォールの設定変更を誤って、全社の通信に影響がでるリスクもある。
2．サーバ側のファイアウォールでブロック：Deep Security のようにサーバ側のファイアウォール機能でブロック。

このようなセキュリティ対策を講じることで、自社で気が付くことができるため、先手を打った対策が打てます。そして、ポートスキャンや攻撃通信を防ぎ、自社のセキュリティレベルの高さを示すことができれば、攻撃者を調査フェーズであきらめさせることができ、公開サーバのセキュリティ強化につながります。

公開サーバのセキュリティ対策
http://www.trendmicro.co.jp/jp/business/solutions/server-security/index.html

様々なサーバ環境に合わせたセキュリティ対策を実現
Trend Micro Deep Security
http://www.trendmicro.co.jp/jp/business/products/tmds/index.html