セキュリティ

ITマネジメント（内部統制）

次世代のマルウェア対策は

脅威への知性を備えた、高機能Webフィルタリング

かつては「怪しいWebサイトにアクセスしなければ大丈夫」ともいわれていた「マルウェア対策」。しかし、最近では企業や組織の正規サイトが改ざんされ、マルウェア配布サイトとして悪用されるケースが増えています。巧妙化するサイバー攻撃に対して、有効な対策とされているのが「次世代のWebフィルタリング」です。ここでは、NTT Comの提供するセキュリティサービスを例に仕組みと効果について解説します。

企業サイトがマルウェア配布サイトとして悪用される

サイトの改ざんにはサイトのシステムの脆弱性が利用されますが、マルウェアを感染させるときは、閲覧者のPCの脆弱性が狙われます。脆弱性とは、セキュリティホールとも呼ばれている「ソフトウェアの不具合」のことです。WindowsやアドビのFlash Player、Adobe Readerなどの脆弱性が利用されるケースが多いのですが、セキュリティアップデートやパッチを適用することで脆弱性を解消し、こうした攻撃を防ぐことができます。

しかし、セキュリティアップデートやパッチの適用には時間がかかり、ユーザーがPCにインストールされている全てのソフトウェアのバージョンを把握し、脆弱性の管理を行うのは手間がかかるとともに、抜け漏れが発生しやすくなります。そのため、現在では危険性の高いWebサイトへのアクセスを自動制御してくれる「Webフィルタリング」が広く活用されています。

そんな中で、最近は企業や組織の正規サイトが改ざんされて、マルウェア配布サイトとして悪用されるケースが増えています。改ざんといっても、短い命令文（スクリプト）が追加されているだけなので、サイトの見た目はまったく変わりません。こうしたサイトは、誰にも気づかれずマルウェア配布サイトとなっているのです。こうした攻撃に対して、Webフィルタリングの機能を強化することで対抗しようという試みが始まっています。

サイト改ざんには、「評判」機能で対抗

日々、巧妙化するマルウェア対策をより強固にするため「次世代Webフィルタリング」ともいえる機能を搭載した製品／サービスが登場しています。その1つが「レピュテーション機能」です。レピュテーションは「評判」という意味で、カテゴリーだけでなく複数の要素によってWebサイトの安全性を判断する手法です。その要素には、「マルウェア感染」「改ざん履歴」「フィッシング」「スパムメール送信元」「IPアドレス」「更新履歴」などがあります。こうした情報を常時収集し、レピュテーション専用のデータベースに蓄積していきます。

そして、ユーザーがあるWebサイトにアクセスしようとすると、Webレピュテーション機能がそのWebサイトについてのデータベースを参照し、危険な要素がないかチェックします。例えば、過去に改ざんされた履歴があり、IPアドレスが頻繁に変更されている場合は、「危険なWebサイトである可能性が高い」と判断されます。このように複数の要素からWebサイトの安全性をチェックするのがWebレピュテーション機能です。

NTT Comの「Enterprise Cloud」で利用できるManaged WAFでは、攻撃通信や不正アクセスの検知/防御を行うWAF（Webアプリケーションファイアウォール）機能、アンチウイルス機能に加え、IPレピュテーション機能をセットとすることで、より強固なWebアプリケーションサーバーへのセキュリティを提供しています。

Webフィルタリングを強化する「脅威インテリジェンス」

「スレット（脅威）インテリジェンス」という手法もあります。スレットインテリジェンスとは、サイバー攻撃に関わるあらゆる情報を集積し、相関分析を行うものです。Webレピュテーションでは、製品／サービスを提供する企業が独自に情報を収集するのに対し、スレットインテリジェンスでは世界中の公開情報や、複数の組織・ベンダーが持っている「脅威の情報」を収集します。こうして集められた情報によって、「ホワイトリストのWebサイトである○○が改ざんされている」といったアラートが共有され、アクセスがブロックされます。

例えば、NTT Comの総合リスクマネジメントサービス「WideAngle マネージドセキュリティサービス」では、より高精度な悪性Webサイト情報サービスとして「Active Blacklist Threat Intelligence」（アクティブ ブラックリスト スレット インテリジェンス）を提供しています。

アクティブ ブラックリスト スレット インテリジェンスでは、国内の企業や官公庁に導入されているセキュリティ機器などで検知したサイバー攻撃の情報を、セキュリティオペレーションセンターの分析基盤に収集。独自の手法で精査し、悪性Webサイトをブラックリスト化します。この最新のブラックリストがユーザーのネットワーク機器へ自動的かつリアルタイムで提供されます。「今、その時」に行われているサイバー攻撃の情報を活用しているため、精度が高く、Webフィルタリングの機能を大幅に強化します。

ホワイトリストに載るようなWebサイトでさえ100%安心とは言えなくなった現在、Webフィルタリングにも、「Webレピュテーション」や「スレットインテリジェンス」といった新たな機能が必須になっていきます。また、こうした次世代のWebフィルタリングは、エンドポイント用のセキュリティ対策ソフト、ゲートウェイ用の次世代ファイアウォールや次世代IPS、あるいはUTM（統合脅威管理）などにも搭載されるケースが増えています。

関連サービス

Managed WAF	Managed WAF は、Enterprise Cloud 2.0 のテナント内で利用することができ、Webアプリケーションサーバーに対する不正アクセスや攻撃通信などのセキュリティ脅威を検知/防御する機能を提供します。脆弱性を突いた攻撃通信、不正アクセス、ウイルス感染など、様々なセキュリティ脅威からお客さまのWebアプリケーションサーバーを守る為に必要なセキュリティ機能をオールインワンで提供します。
WideAngle マネージドセキュリティサービス Active Blacklist Threat Intelligence	WideAngle MSSの運用に加え、世界最大級のネットワーク サービス プロバイダーとしての運用で得られるノウハウを活用し、脅威検知のための「独自ブラックリスト」として蓄積しています。国内はもちろん、グローバルでの運用ノウハウも活用して、国内外で異なる傾向を持つ攻撃に備えることができます。
OCN IWSaaSサービス	クラウド上に設置されたWebセキュリティゲートウェイを経由することで、不正なWebサイトへのアクセス制限や不正プログラムのダウンロードを防ぐことが可能となります。また、クラウド型で提供するため、クライアントへのソフトウェアインストールおよびパターンファイルのアップデートも必要なく常に最新のものが提供されます。