セキュリティ

ITマネジメント（内部統制）

ホワイトリストが落とし穴に！？

Webフィルタリングが無効化される手口とは？

マルウェアに感染する経路は、メールとWebアクセスによるものがほとんどを占めています。このうちWebアクセスにおけるリスク対策については、ブラックリストやホワイトリストを使ってアクセスを制限する「Webフィルタリング」が効果的といわれており、多くの企業がその種のソリューションを導入しています。しかしサイバー攻撃者も、Webフィルタリングによる対策をすり抜けようと、日々知恵を絞っています。ここでは、サイバー攻撃者がどうやってWebフィルタリングをかいくぐるのか、その手口について解説します。

正規のWebサイトが「マルウェア配布サイト」に変身？

マルウェアに感染する経路は、メールに添付されたファイルを実行するほか、メールに記載されたURLをクリックし、マルウェアの配布サイトへの誘導や、ネットサーフィン中にマルウェア配布サイトにアクセスしてしまうといったケースが大半です。かつてのマルウェアの配布サイトは、いかにも怪しげなジャンルのサイトを装っていました。しかし最近では、一見違和感のないWeb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。

2012年ごろから、セキュリティの分野では「水飲み場攻撃」という言葉が話題になりました。この攻撃は、特定の業種や業界の人がアクセスするWebサイトを改ざんし、マルウェアの感染を狙う一種の標的型攻撃です。野生の世界で、肉食動物が水飲み場の近くに隠れて待機し、水を飲みに集まってくる草食動物を狙うのに似ていることから、その名が付けられました。

水飲み場攻撃では、対象となる企業や組織のWebサイトをプログラムの脆弱性などを突いて改ざんしますが、目立たぬように感染活動を行うので、長期間にわたって感染が気づかれないケースも少なくありません。最近では、水飲み場攻撃という言葉をあまり聞かなくなりましたが、これはサイバー攻撃者の狙いが特定のWebサイトではなく、さまざまな人がアクセスする一般的なWebサイトへと移行したからです。

改ざんされたWebサイトからダウンロードされるマルウェアについても、危険なものが増えています。これまでは、ユーザーが利用するオンラインバンキングを乗っ取る「バンキングマルウェア」が主流でしたが、現在はPC内部のファイルを暗号化して使用不能な状態にし、復号のための“身代金”を要求する「ランサムウェア」や、PCのCPUパワーやメモリを勝手に使って仮想通貨を得る「マイニングマルウェア」なども増加しています。

ホワイトリストすら無効化する巧妙な手口

こうしたマルウェア対策に広く活用されているのが「Webフィルタリング」です。多くのWebフィルタリング製品／サービスは、「ブラックリスト」「ホワイトリスト」「カテゴリー」の3つの機能を搭載しており、ユーザーがWebサイトにアクセスしようとした際に、そのURLを3つの機能によりチェックし、危険なWebサイトへのアクセスをブロックします。

ブラックリストとは危険と判断されたWebサイトのリストで、ホワイトリストは安全なサイトのリストです。ブラックリストに載っているWebサイトへのアクセスを禁止、あるいはホワイトリストに載っているものへのアクセスのみ許可する、といった使い方をします。カテゴリーは、Webサイトのカテゴリーによってアクセスを制御する機能です。この機能を持つ製品では、すべてのWebサイトが「ショッピング」「SNS」「ギャンブル」「不明」といったカテゴリーで細かく分類されており、ユーザー企業は業務と関係ないカテゴリーのWebサイトへのアクセスをブロックすることで、マルウェアへの感染や無用なインターネットサーフィン等を防ぐわけです。

しかし、こうした対策も前述のようにホワイトリストのサイトが改ざんされる攻撃に対しては効果がありません。なぜなら、そのサイトは攻撃を受けるまではまったく無害なものであり、業務で使われたりしているからです。改ざんされているといっても、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。こうしたサイトへ脆弱性のあるPCでアクセスすると、スクリプトが実行され、ウィルスウイルス感染や、マルウェア配布サイトに誘導されてしまうのです。

過去、攻撃に利用されたことがある、或いは利用される可能性があるIPへのアクセスをブロックすることで攻撃を防ぐ機能を搭載している製品やサービスもありますが、サイバー攻撃者は短い時間でIPアドレスを刻々と変化させることで、検知から逃れようとします。

日々、巧妙化するサイバー攻撃。「Webフィルタリング」の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ているのです。

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。