

モダンマルウェアの脅威から組織を守る次世代ファイアウォール

次世代ファイアウォールと WildFire サービスで実現する標的型攻撃防御

特定の企業や団体を狙った標的型のサイバー攻撃による情報漏洩事件が相次いでいます。その中でも標的型攻撃とよばれる新しい脅威では、重要な機密情報を標的に密かに攻撃が進行するため、従来の情報漏洩事件と比べ被害が深刻化しています。従来のファイアウォールやアンチウイルス、アンチスパイウェアなどで防御できないことが、さらに深刻さを深めています。次世代ファイアウォールとそれに追加された新たなマルウェア検知サービス「WildFire」は、こうした標的型攻撃の脅威への対応を可能にしました。

Google や Yahoo など 30 社を超える企業が攻撃を受け、アカウントやパスワードが漏洩した「オペレーション オーロラ」、イランの原子力関連組織が標的にされた「スタックス ネット」、石油・エネルギー・製薬関連企業を狙った「ナイトドラゴン」などが、海外での標的型攻撃として知られています。国内でも大手ゲーム機器メーカーや防衛産業企業、政府機関が標的にされた情報漏洩事件が明らかになるなど、標的型攻撃の脅威があらためて喧伝されました。

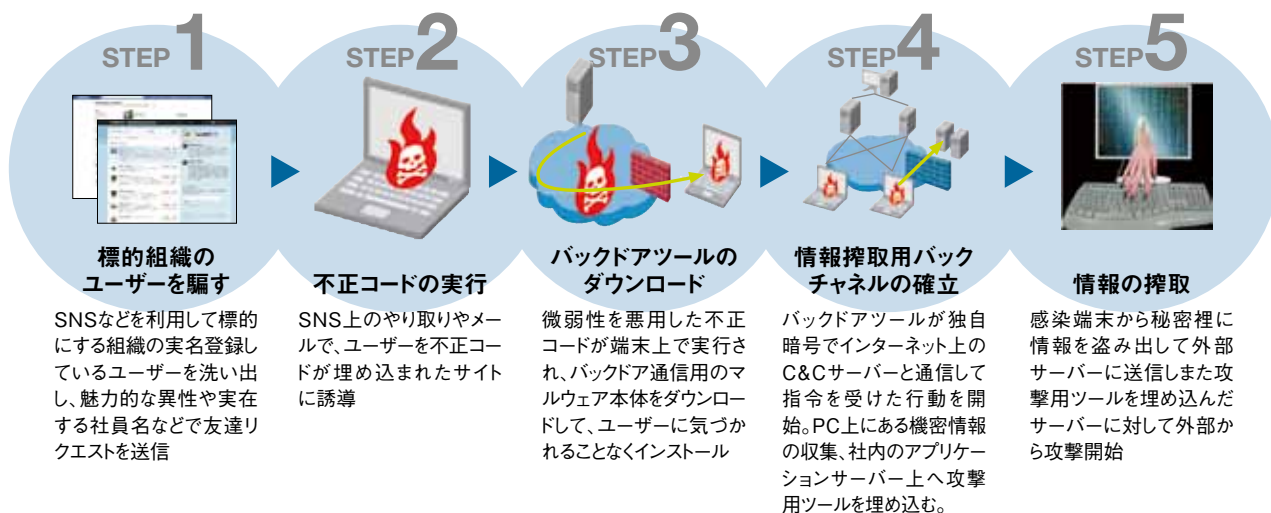
標的型攻撃の特徴

- 重要なデータを確実に搾取するために特定の組織やホストをターゲットとして巧みに攻撃
- 従来のサイバー攻撃のように不特定多数を対象にマルウェアをばらまくものではない。ウイルス対策ベンダーがマルウェア検体（サンプル）を入手できることは希。そのため、新種、亜種のパターンファイル（シグネチャ）が作成できず、従来のセキュリティ対策での防御は困難
- 標的攻撃で使われるマルウェアは単体ウイルスでなく、「モダンマルウェア」と呼ばれるネットワークアプリケーション。ネットワークを活用しながら本体をダウンロードして自身を機能強化したり、ネットワークセキュリティを回避するよう高度に設計

モダンマルウェアはこうしてデータを搾取する!

モダンマルウェアは、人間の心理的な隙や、行動のミスにつけ込んで個人が持つ秘密情報を入手する手法（ソーシャルエンジニアリング）を特徴とします。標的とする組織の従業員を狙って巧みに接触し、脆弱性を悪用してウイルスやスパイウェアなど複数の既存攻撃を組み合わせ、深く静かに進行して情報を搾取します。その多くは次のようなステップで進行します。

モダンマルウェアの感染から被害発生までの5つのステップ



従来のセキュリティ対策で防御が困難だった、こうしたモダンマルウェアによる標的型攻撃に対して

次世代ファイアウォールは**3つの対策**で防御します。

対策 **1** 脅威の侵入経路を狭める

対策 **2** モダンマルウェアの侵入を検出・ブロックする

対策 **3** 侵入を許した感染端末をできる限り早く発見する

モダンマルウェアによる標的型攻撃に対して、 3つの対策で防御します

対策

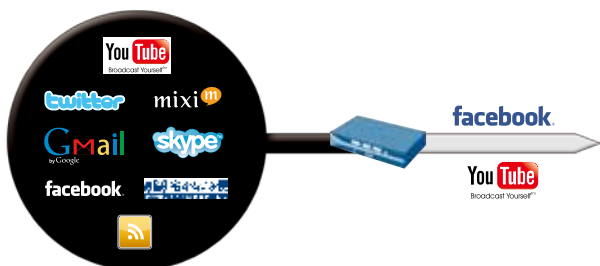
1

脅威の侵入経路を狭める

App-ID による
アプリケーションレベルで通信制御

次世代ファイアウォールのApp-ID機能は、すべてのトラフィックをアプリケーションレベルで可視化・制御することができます。これによりモダンマルウェアの進入経路となり得るアプリケーション通信を制限し、潜在的なリスクを低減できます。

- SNSアプリケーションの社内利用を制限またはブロック
- Webメール、SkypeやWindows Live MessengerのようなP2P技術を利用したメッセージングアプリケーション、Web型のファイル共有アプリケーションの通信を制御
- 拠点間やセグメント間などの社内アプリケーション通信も監視・制御することで、万が一社内に侵入された場合でも被害を最小化



対策

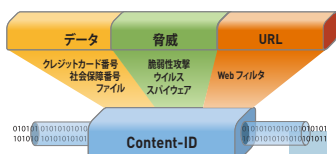
2

マルウェアの侵入を食い止める

Content-ID + WildFire による
モダンマルウェア防御

次世代ファイアウォールのContent-IDというスキャンエンジン、アプリケーションに埋もれたウイルスやスパイウェア、脆弱性攻撃をシグネチャベースで検知・ブロックします。さらに、シグネチャが未対応でContent-IDを通過した未知のマルウェアは、クラウド型の未知マルウェア検知サービス「WildFire」によって検知します。

- マルチギガビットの高速スキャンによりシグネチャベースで脆弱性攻撃、マルウェア、バックドア通信といった脅威から幅広く防御
- SSL暗号通信、トンネル通信、圧縮ファイルなどに埋もれた脅威や機密ファイル持ち出しの検知
- WildFireにより、未知のマルウェアであっても振り舞いベースで発見して、迅速にシグネチャを提供し対応



● ストリームベースの高速スキャンによりアプリケーションに埋もれた脅威を検知

● SSL暗号通信、トンネル通信、圧縮ファイルなどに埋もれた脅威や機密ファイルもブロック

● 仮想実行(sandbox)環境でプログラムを実行することで振り舞いベースでマルウェアを検知

● 迅速にシグネチャを自動生成し対応



対策

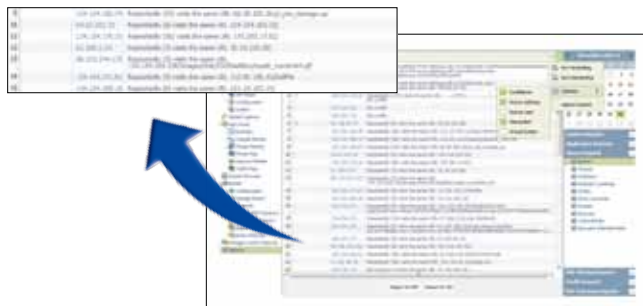
3

侵入を許した感染端末を できる限り早く発見

ポットネット検知レポートの活用

万が一、モダンマルウェアが侵入してしまった場合でも、感染した端末を迅速に検知し、被害の拡大を防止することが重要です。次世代ファイアウォールのポットネット検知レポートは、ポットネットの通信をその特長から検出し、感染した疑いのある端末を割り出します。

- 不明なプロトコルやIRCといったアプリケーション通信が多いなどの特長からバックドア通信を検出
- HTTP通信を偽装したバックドア通信も検知可能
- 感染した疑いのある端末をリストアップし、定期的にレポート



標的型攻撃に対応!

モダンマルウェアを制御する WildFire

WildFireは、標的型攻撃に使われるモダンマルウェアに対処可能なクラウド型未知マルウェア検知サービスです。ファイルをクラウド上にある仮想環境で一旦実行してインストール後の端末上での挙動を明らかにすることにより、未知のマルウェアであっても検知することが可能です。

- クラウドサーバー上に用意された仮想サンドボックス環境でファイルを実行することで、その振り舞いを元にマルウェアを検知
- 特定されたマルウェアの本体やバックドア通信に対するシグネチャを自動的に生成しインターネットを経由して配信
- マルウェアの活動に関するフォレンジックと分析を提供(ターゲットとなったマシン上での動作、マルウェアの伝染に用いられたアプリケーション、マルウェアの配信に利用されているURLのリスト)

※WildFireを用いた実証試験データによると、検査対象となった35,387個のファイルのうち、7%以上が未知のマルウェアでした。そのマルウェアの57%は、どのウイルス対策ベンダー製品でも検知できず、またウイルス報告サイトでも未発見のものでした。

既知のファイルと比較	シグネチャ自動生成
サンドボックス環境で実行	管理用 Webポータル

