

## Web 2.0 の脅威をクラウドで阻止

ミッコ・バリマキ  
ブルーコートシステムズ チーフサイエンティスト



今やサイバー犯罪は巨額を稼ぎ出す規模になっており、サイバー犯はまるで企業組織のように利益を追求しています。ビジネス用途、個人用途を問わず、Web 2.0 に代表されるコラボレーション環境やインタラクティブ性が注目を浴びる中、サイバー犯もまたこの特性に狙いを付けているのです。SaaS

(Software as a Service) やソーシャルメディア、ブログ、Ajax などの Web 2.0 技術は、誰でも参加できる使い勝手の良さやオープンな環境が特徴です。ところが Web 2.0 は、外部への露出部分が多い分だけ攻撃されるリスクも高まり、従来のセキュリティ上の境界にいくつもの穴を開けてしまうことから、セキュリティリスクの潜む死角が増えることになりました。

サイバー犯の狙いは、ずばりカネです。Web 上で自らのテクニックをひけらかすことではありません。あらゆる手口で財産を盗み出そうとしています。

*Web 2.0 の世界では、脅威がどこに潜んでも不思議ではありませんが、マルウェア自体は必ずリンク先にあります。たとえ JavaScript が使用されていても、実行ファイルをダウンロードする URL が必ず存在するのです。*

### ボットネット運用とトラップで餌食に

迷惑メールや迷惑投稿の 80% 以上に何らかの URL が含まれており、Web 上でのマルウェア（ウイルスなど攻撃プログラム）感染の 70% は本物の Web サイトで発生しています。サイバー犯は、個人情報や財産を盗むためにありとあらゆる手を使うため、Web 上の至るところに脅威が潜んでいます。最近のサイバー犯がマルウェアや悪意あるコンテンツをばらまく際に、主に Web 上でのボットネット（乗っ取った大量の PC で構成したネットワーク）運用とトラップという 2 つの手口が使われています。

ボットネット運用という手法は、闇市場まがいの商品販売やマルウェアのばらまきに使われており、ユーザーがアクセスするだけで勝手にマルウェアがダウンロードされる状況に誘導するのが一般的です。本物の Web ページへのリンクを記載した迷惑メールやブログ投稿を大量配布して検索エンジンのランキングを不正操作する手口は、ユーザーを偽 Web サイトに誘導する常套手段になっています。Web 上には

膨大なコンテンツがあることを考えると、検索エンジン各社がこうした不正操作を見抜いて対処することは容易ではありません。

サイバー犯は、悪意のある Web ページへのリンクを含めた投稿を、世界中のブログやソーシャルメディアに無差別投稿します。また、話題のイベントなど注目度の高いテーマに関する Web ページを制作し、そこにも悪意ある Web ページへのリンクを含めておきます。これは巨大な投網でユーザーを一網打尽にするようなものです。ユーザーは、検索エンジンのランキングが不正操作されているとは知らずに、検索結果に並んでいる偽サイトにアクセスします。すると、マルウェアが仕掛けられたサイトに強制誘導

されます。こうした検索エンジンの操作は、リンク先掲載者に紹介手数料を支払うサイトで少しでも手数料を稼ぐ手段としてずいぶん前から利用されていますが、最近はセキュリティ対策ソフトを装った攻撃プログラムがこの手法を大々的に悪用しています。

偽のセキュリティ対策ソフトは、「あなたの PC がマルウェアに感染しています」といった嘘の警告を出してユーザーを不安に陥れ、有料のマルウェア駆除を持ちかけます。マルウェアに対する消費者の不安を煽り、何とか安心したいというニーズにつけ込みます。感染した PC のマルウェア駆除を提案されたユーザーは、ついついクレジットカード番号などを無防備に渡してしまいます。その後、偽セキュリティ対策ソフトが感染 PC の修復を適当に処理することもありますが、ひどい場合には修復と称してさらに多くのマルウェアを仕込むことさえあります。いずれにせよ、ユーザーの PC に密かにプログラムなどを送り込めるチャンスをサイバー犯に与えてしまったことになりません。

トラップはさらに卑怯な目的に使われます。というのも、埋め込み HTML（いわゆるインラインフレーム、iframe）が本物の Web サイト内に表示されるように細工しておき、ユーザーがリンクをクリックしたとたん、一連のイベントが開始されて最終的に

マルウェアを起動させる手口です。iframe は、ファイアウォールや静的 URL フィルタリング、レピュテーションスコアリングなどの従来のセキュリティ対策には引っかけられません。しかも実際の悪意あるサイトの隠れ蓑として大量のサブドメインが使われるため、脅威を抑制しにくくなっています。

さらに、裏側ではマルウェアをばらまくための仕組みが非常に巧妙化しています。これは“トラブルの連鎖”を生みます。例えば、迷惑メールや無差別投稿によるリンクのばらまき、リンクファーム（リンク数を稼ぐために、特定の集団内で不自然な相互リンクを張り巡らす行為）、検索エンジンのランキング操作のために、さまざまなサイトが利用されています。ここからマルウェアのリレーを繰り返す、最終的に実際の攻撃プログラムが収められているホストに接続します。サイバー犯は何段階も続くステップの裏に隠れているため、簡単にシッポをつかむことはできません。マルウェアが置かれたホストは補足しにくく、頻繁に変化しています。

*WebPulse が持つコミュニティ監視機能の実効性の高さから言えば、Web 2.0 環境でも Web 1.0 と同じ安心感が生まれます。企業にとっては防御態勢を強化できる一方、Web 2.0 アプリケーションのメリットを余すところなく活用できるようになります。*

### トラブルの連鎖を断ち切るために

Web 2.0 の脅威がトラップによるものだろうと、ポットネット運用によるものだろうと共通の弱点があります。Web 2.0 の世界では、脅威がどこに潜んでも不思議ではありませんが、マルウェア自体は必ずリンク先にあります。たとえ JavaScript が使用されていても、実行ファイルをダウンロードする URL が必ず存在するのです。

その URLこそが急所ですから、クラウドベースのコミュニティ監視サービスであるブルーコートの WebPulse™ は、この URL を徹底利用します。WebPulse は独自に URL を 1 つ 1 つ吟味するため、動的な Web リンクを使ってマルウェアや悪意あるコンテンツを配布するような脅威に対して威力を発揮します。5400 万に及ぶブルーコートユーザーのデータを基に、クラウド内の悪意ある URL を探し出し、ユーザーがうっかりアクセスしないように先手を打ちます。

WebPulse のダイナミックリンク分析機能は、URL フィルタリング技術とアンチマルウェア技術を連携させ、ダイナミックリンクを利用した Web 上の脅威に対抗します。クラウド接続のコミュニティ上で多様なユーザー層を結びつけることにより、集団の力で強力な防御態勢を築きます。このユーザーコミュニティからのリアルタイムに提供されるデータには、まだ危険度が評価されていない新しい Web リンクやコンテンツなどがあります。危険度評価に基づくカテゴリ分け、脅威エンジン、機械解析、専門家による危険度評価など、複数の分析手法を組み合わせた迅速な脅威評価で、マルウェア、フィッシング、悪意あるコンテンツを検出します。

新しい Web コンテンツに対するクラウドベースの危険度評価は非常に迅速に実行されるため、いちいちデータベースをダウンロードする負荷もなく、コミュニティの全メンバーを保護できます。

ユーザーの PC のセキュリティに問題がある場合、そこを突かれて被害が広がらないように WebPulse が防御します。例えばマルウェアに感染

している場合、マルウェアが外部にあるサイバー犯のコンピュータと通信したり、外部から新たなプログラムなどをダウンロードしたりしますが、WebPulse のダイナミックリンク分析機能がこうした動作を阻止します。ブルーコートの ProxySG は、組織内に潜むマルウェアを一掃し、ユーザーがうっかりマルウェアをダウンロードしない防御態勢を確立します。

WebPulse が持つコミュニティ監視機能の実効性の高さから言えば、Web 2.0 環境でも Web 1.0 と同じ安心感が生まれます。企業にとっては防御態勢を強化できる一方、Web 2.0 アプリケーションのメリットを余すところなく活用できるようになります。

[WebPulseの詳細はこちらをご覧ください。](#)

ブルーコートシステムズ合同会社

〒105-0021 東京都港区東新橋 1-9-2 汐留住友ビル 16 階

Tel 03-6251-9111(代表) Fax 03-6251-9112 Mail: Japan.info@bluecoat.com URL <http://www.bluecoat.co.jp>

Copyright©2009 Blue Coat Systems, Inc. All rights reserved worldwide.

Blue Coat, Blue Coat のロゴはアメリカ合衆国およびその他の国々における Blue Coat Systems, Inc. の商標または登録商標です。その他の製品名及び会社名は各社の登録商標または商号である可能性があります。仕様は予告なく変更となることがあります。