

ブルーコートでガンブラーを完全防御

ブルーコートシステムズ シニアコンサルタント

小林 岳夫

国内におけるガンブラーの猛威は日に日に増すばかりです。ある統計によれば、報告されているだけでも、この3ヶ月間という短い期間に372件もの被害件数があるとされています。その脅威による被害は、今後も止まることなく、増加の一途をたどることが予測されます。

ここでは、今やあまりにも有名なガンブラーの手口の手法やメカニズムについての言及は省き、どうすればこの脅威を完全に防ぐことができるのか、また、どのような安全な方法で効果的に防御することが可能なのかに焦点を当ててお伝えします。

ガンブラーの攻撃特性

ガンブラーとは、一種の悪意のあるマルウェアになりますが、その真の脅威は実際のマルウェア本体にあるのではなく、その攻撃手法にあると弊社では考えています。そうした意味では、ガンブラーは、マルウェアそのものの名称というよりはむしろ、その攻撃手法を示す広義での脅威名称とも言えます。

そして、ガンブラーに対する対策として最も重要となるのは、以下の攻撃特性を予め見極め、その特性をふまえた無駄のない強固なソリューションを実施することにあります。

<ガンブラーの攻撃特性>

- ① Web(HTTP/HTTPS)を利用して閲覧したユーザーを感染させる。
- ② 善良かつ有名なWebサイトに難読化されて埋め込まれた不正なコード(HTMLヘッダやスクリプトなど)によって、ユーザーが全く気付かない状態で悪意のあるサイトへリダイレクトされる。
- ③ ユーザーのPC上のアプリケーションの脆弱性について、マルウェア自体をダウンロードさせる為のWebサイト(URL)が必ず存在する。
- ④ 感染PC上での通信モニタリングを開始して、特にWebサーバー管理用のFTPアカウント(ユーザー名、パスワードhttp://japan.internet.com/webtech/20091118/4.htmlド)を漏洩させる。

感染初期段階からの対策

ブルーコートは、Webにフォーカスした機能群をベースに、常に、セキュアWebゲートウェイのマーケットリーダーとして、効果的なソリューションをお客様へ提供しています。

ブルーコートであれば、これらのWeb固有の特性を考慮したピンポイントでの防御が可能となります。

ブルーコートのURLフィルタリング機能であるBlue Coat WebFilterを補完するクラウドサービス、"WebPulse"のダイナミック・リンク解析機能により、ガンブラーによる感染手口の初期の段階で、全てのWebPulseユーザーをその脅威から確実に回避することができます。

具体的には、善良な Web サイト上に埋め込まれた不正な HTML ヘッダーやスクリプトによって、ユーザーが悪意のあるサイトにリダイレクトされると、リダイレクト先サイトへのアクセスを WebPulse がリアルタイムに評価し、悪意のあるサイトへのアクセス自体を確実に検出して防御します。

ここで肝心なことは、善良なサイトに不正な仕組みが埋め込まれていても、その善良なサイト自体に変わりがない為、この時点においては WebPulse ではユーザーからのアクセスをブロックしないという点です。過敏にブロックしてしまうことにより、場合によっては、善良なサイトを閉鎖に追い込みかねないからです。

ブルーコート の階層型防御で、ネットワーク上の脅威から徹底防御

WebPulse は全世界 6,200 万人で構成されるマルウェアや有害なサイトに対する共同防衛網であり、1 企業だけでは対処不可能な、ネットワーク上に存在するハッカーに乗っ取られた無数のサーバーで構成される犯罪網に対する防御体制を講じることを可能にします。

6,200 万ユーザーで形成される共同防衛網である WebPulse は、セキュリティ脅威に対して業界でも類を見ない検出能力と精度を誇ります。万が一 WebPulse で検出できないような事態に備え、ProxySG の SGOS 上のポリシー処理エンジンを使って検出できなかったサイトからの実行ファイルなどのダウンロードを完全防御する、また、ProxyAV (Kaspersky, McAfee, Sophos, Panda から選択) からダウンロード・ファイルをスキャンしてマルウェアを検出・防御する、といったハイブリッド型の階層化防御システムを構築することも可能です。

コラボレーションやインタラクティブ性を実現する Web2.0 の利用や、様々なアプリケーションの Web 化が急速に進む中、企業における全体の通信に占める Web 利用の割合の増加に加えて、最重要通信における Web 化の傾向も見受けられます。

ブルーコートの提供する階層型防御アーキテクチャーによって、ガンブラーはもとより、ネットワーク上に蔓延する様々な脅威からユーザーを守り、安全かつ快適にネットワークを利用できる環境を提供することが可能になります。

ブルーコートはマルウェア対策に関しても数多くの実績を有しています。詳細については、以下の資料も併せてご参照ください。

- ・ Web2.0 の脅威をクラウドで阻止

<http://www.bluecoat.co.jp/solutions/businessneeds/secureweb/200910StopWeb2.0.pdf>

- ・ WebPulse : 集団でサイバー犯罪を監視

<http://www.bluecoat.co.jp/solutions/businessneeds/secureweb/200910WebPulse.pdf>

- ・ 新たな脅威には共同防衛が物を言う Web 2.0 の世界

http://www.bluecoat.co.jp/solutions/businessneeds/CustNL-websecurity_jp.pdf

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

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

Copyright©2010 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。