ガンブラー攻撃についての調査ご報告

ガンブラーはウイルスではない？

昨今ニュースなどでも話題になっている”ガンブラー”とはホームページからウイルスをダンロードさせる攻撃を総称したもので、以下のような不正な攻撃が行われます。

攻撃者による不正アクセスの主な手順は以下のとおりです。

(1) 攻撃者は不正に取得したアカウント情報を用いて多くの方が閲覧する一般企業や個人のホームページを改竄し、海外の悪質なホームページへ誘導するコード(JavaScript)を挿入します。改竄されたホームページは見た目が変わらないため、すぐには気づかれ難いのが特徴です。

(2) 誘導先の海外のホームページには、パソコンにインストールされている様々なソフトウェアの脆弱性を利用して勝手にウイルスをインストールするための罠が仕掛けられています。

(3) 脆弱性のあるソフトウェアがパソコンにインストールされていた場合、改竄されたホームページを閲覧するだけで悪質なプログラムが自分のパソコンにインストールされています。

(4) インストールされた悪質なプログラムはパソコンに保存されているホームページのアカウント情報（FTP接続用のIDとパスワード）を攻撃者に転送します。

(5) 送信されたアカウント情報は攻撃者に利用され、新たなホームページの改竄が行われます。

この (1) ～ (5) の繰り返しによりガンブラー攻撃用のサイトが次々に作成され、ホームページを閲覧したユーザに被害が拡大しています。

企業にとってのリスクとは

企業にとって、ガンブラー攻撃により自社のブランド・信用が損なわれることは非常に大きなリスクとなります。ガンブラー攻撃で改竄されたホームページは単に閲覧者のパソコンを危険に晒すだけではなく、閲覧者が使用するブラウザやセキュリティソフトの機能で「危険なホームページ」としてアクセスが遮断されてしまうこともあります。一度でも危険なホームページと表示されたホームページに閲覧者は再び訪問してくれるでしょうか？

これまで、大手企業以外のホームページ改竄などの事件が新聞やテレビのニュースに取り上げられることはほとんどありませんでした。しかしガンブラー攻撃のように閲覧しただけでウイルスに感染するようなケースでは、企業の知名度や顧客の数に関係なく全ての企業がホームページの改竄と自社の信用低下のリスクに直面することになります。

目次

調査の目的および方法

自社の WEB サイトがガンブラー攻撃に関与していないことを確認するために、以下２つの確認が必要となります。

- コンテンツ制作会社およびコンテンツ更新用アカウントを保持するお客様環境の全てのパソコンがウイルスに感染していないこと
- Web サイトに配置されているコンテンツファイルにガンブラー攻撃用の不正なコードが挿入されていないこと

そこで当社では、”お客様コンテンツの作成・更新を実施している事業者”および”コンテンツの置き場所としてのホスティングサービスを提供している事業者”として以下２つの調査を実施いたしました。

【調査その１】

当社パソコン環境がウイルスに感染していないことを確認するため、社内の全てのパソコンにおいてハードディスクに保存されている全てのファイルのウイルス検査を実施しました。

【調査その２】

お預かりしているお客様コンテンツにガンブラー攻撃用の不正なコードが挿入されていないことを確認するため、弊社独自の検査プログラムによってサーバ上で検査を実施しました。

当社の安全管理体制

当社では、世界的なセキュリティベンダーであるサーバ向け Dr.WEB 製品の日本国内総代理店として日頃から社内の安全管理体制について注視しています。

社員のパソコンの安全管理を社員任せにすることはなく、社内の全パソコンを一括管理できる統合型のセキュリティソフトを導入し運用しています。

調査その１～弊社パソコン環境の検査～

以下の 2 つの商用アンチウイルスソフトで社内の全パソコンのハードディスクに保存されている全てのファイルのウイルス検査を行いました。

- Dr.WEB
- Symantec Endpoint Protection

実施日：２０１０年１月１２～１５日

調査対象パソコン：約４０台

検査の結果、ウイルスが検出されたパソコンは１台もありませんでした。

また今回のガンブラー攻撃で脆弱性が利用されている以下のソフトウェアについて、最新バージョンがインストールされていることを弊社セキュリティ担当者が１台ずつ、全てのパソコンに対して確認しました。

- Adobe FlashPlayer およびブラウザのプラグイン
- Adobe Reader
- Java Runtime Environment(JRE)

調査その 2 ～お客様コンテンツの検査～

共有型レンタルサーバでお預かりしているお客様のサーバコンテンツに対して、ガンブラー攻撃によって不正に改竄されたファイルが無いかどうかを独自の検査プログラムにて検査を行いました。

対象ドメイン：sorize.com（例）

実施日時：２０１０年1月１５日

##############################
sorize.com

Summary:
OK　　- 1380 file(s)
NG　　- 0 file(s)
SUSPICIOUS - 0 file(s)

##############################

OK とは、不正に改竄された形跡の無いファイル。NG とは、不正に改竄されているファイル。SUSPICIOUS とは、不正に改竄されている疑いのあるファイルです。

まとめ

当社にて実施した二つの調査により、検査実施日時において以下 2 点が確認できたことになります。

1. 弊社パソコン環境がウイルスに感染していないこと
2. お客様コンテンツがウイルスに感染していないこと

従いまして、当社のレンタルサーバサービス共有型をご利用で、かつホームページの更新を全て当社に依頼されているお客様につきましては、自社ホームページがガンブラー攻撃に関与していないと考えることができます。また、御社ホームページへのアクセスの遮断や自社の信用低下などを招きかねないリスク要因を最小限に抑えられていると評価することができます。

サーバ側の調査方法

商用の高性能アンチウイルスエンジンの Dr.WEB によるサーバファイルのフルスキャンに加えて、当社独自調査によって採集したガンブラーの攻撃パターンのパターン認識検索も行いました。

株式会社ネットフォレスト

横浜市中区南仲通 4-39-2 箕田関内ビル 5F

045-663-6277

045-663-6278

sales@netforest.ad.jp

人々とネットワークをつなぐ創造企業

Web サイトのアドレス:

http://www.netforest.ad.jp/

不正アクセスから企業を守るには

当社の共有型レンタルサーバ以外のサーバをご利用のお客様は早急にサーバ側にあるファイルに問題がないかご確認ください。また、お客様ご自身でホームページを更新している場合は、過去に更新作業を行った可能性のあるパソコン全てのウイルススキャン及びブラウザプラグインソフト（Flash Player、Adobe Reader、 Acrobat および JRE 等）の最新版へのアップデートを行ってください。

当社サービスのご紹介

当社のレンタルサーバサービス共有型をご利用のお客様向けに、WEB サイト用ウィルスチェックサービスのご提供準備を進めております。ご提供時期は 2 月上旬、価格は月額 980 円 (税別)を予定しております。
本サービスは、お客様 WEB サイトのファイルに対して毎日 1 回定刻に実施したウイルス検査の結果と FTP 利用有無情報などをメールでお知らせするものです。現在準備中のため、内容に一部未定の部分もございますが、詳細につきましては営業にお問い合わせください。