

バリュードメイン

デジロックは当初ウイルス混入について否定を繰り返していたものの、問題発生から2週間後の7月21日ついに改竄の事実を認めることとなった。

今回の騒動についてバリュードメインとアクセスアナライザーのサイト上で下記の通り発表がされた。

ログインページにおける不正表示について

<http://www.value-domain.com/info.php?action=press&no=20090721-1>

お客様 各位

平素はバリュードメインをご利用いただき誠にありがとうございます。

下記内容で、ログインページにおきまして不正表示がございました。

症状

7月6日、ログインページにて、ウィルスダウンロードを誘導するページへのリンクが設置されておりました。ウィルスについては下記が参考になります。

Microsoft Video ActiveX コントロール の脆弱性(MS09-032)について

<http://www.ipa.go.jp/security/ciadr/vul/20090707-ms-activex.html>

事実・経緯

7月6日朝に、新しい機能に対応するため本番用ウェブサーバーのメンテナンス作業を行いました。その際の流れは、下記の通りとなります。

通常、メンテナンス時は、普段は停止中である代替用ウェブサーバー(202.222.31.78)をアクセス可能にし、本番用ウェブサーバー(202.222.31.77)からウェブページをコピーし、DNSの切り替えと、データベースサーバー側での受け入れ認証設定の変更を行い、本番用サーバーの作業をします。また、本番用サーバーがアクセス不能である場合は、割り当てIPを即座に切り替えて、障害に対応できるようになっています。メンテナンス終了時、また、障害解消時に、本番用サーバーに戻し、運用を再開します。

そのメンテナンス時に利用した代替用ウェブサーバーにて、不正改ざんページが設置されておりました。

同日夜、メンテナンスが終了し、および、DNSの切り替えが反映されると共に症状は解消されました。

原因・調査結果

代替ウェブサーバーでの書き換えについて、本番用、代替サーバー内、およびDBサーバー等のログ等の調査を行いました。システム的な乗っ取りは確認できず、手動アップロードであると確認しました。また、本番用のログインページの表示はプログラムで生成していますが、不正ページはプログラムで動作する形ではなく、静的なHTMLファイルが書かれているページ・HTMLテンプレートでした。

代替サーバー自体の運用に問題あり、ウェブサーバーを停止し、対策を行いました。

根本的な解決策ではありませんが、少なくとも症状を回避するには、代替サーバーに本番用サーバーの最新データを強制上書きして運用すべきでした。ログインページ自体の開発、変更をしばらく行っていなかったため、代替サーバーの不正なページファイルの変更時間の方が、本番用サーバーよりも新しかったため、上書きされずに不正なファイルが残り、表示されてしまいました。

復旧後の調査でございますが、代替サーバーでの調査では、ログインページ以外の動作はなく、その他の被害はございませんでした。また、DBサーバーへのアクセス等も調査を行いました。パケットでのフィルタ、ソフトウェアでのフィルタ等を行っているため、アクセスはございませんでした。

ブラウザIEで、ログアウトされている状態で、新しくログインページを開いたお客様が閲覧された可能性があると存じますが、ログ、最終ログイン時間等の判断で、約90アカウントと判断しております。6日朝～夜に新しくログインした履歴のあるお客様のアカウントにおきましては、注意表示をするようにしております。また、ログインユーザ名が特定できたお客様には、個別にお詫びと確認のメール連絡を差し上げています。

対応に関する不手際、時間など、問題自体以外にも、多々問題があり、大変申し訳なく思っております。特に遅くなった情報提供、アナウンスについての体制、姿勢を深く反省し、今後の改善につなげて参りたいと存じます。

この度は、ご利用の皆様には、ご迷惑、ご心配をおかけし、大変申し訳ございませんでした。

今後ともよろしく願い申し上げます。

以上です。

アクセスアナライザー

解析サーバーの不具合について(2009/07/21)

<http://ax.xrea.com/index.php?action=200907>

お客様 各位

平素はアクセスアナライザーをご利用いただき誠にありがとうございます。

下記内容で、アクセス解析用のサーバーにおきまして不具合がございました。

内容

分散しておりますデータ解析用のサーバーの2番目のサーバーにおいて、7月7日頃から改ざんされ、不正なページ（10日頃までウィルスが自動ダウンロードされていた）へリンクするスクリプトが設置されておりました。21日までにサーバーを交換し最新版のソフトウェア、設定に切り替え、運用を再開しています。

原因・経緯

サーバー、ソフトウェア共に、外部に構築依頼しておりましたが、昨年、同様の問題（ホームページ編集用のパスワードが受託者以外に漏れていた問題）があった以後から、管理を引き継いでおりました。正直に申し上げますと、委託契約を解除し、そのままシステムを引き継ぎましたが、1番目の解析用サーバーは、昨年、自社管理のシステムに移して運用中でございましたが、2番目のサーバーについては、直接の問題対象外であったということもあり、システム移行作業を怠り、前システムのまま、つまり、類似の問題が解消されない状態で運用されておりました。

この度、2番目、合わせて3番目のサーバーについて自社システムに切り替え、運用を再開しました。

対応に関する不手際、対応時間など、問題自体以外にも、多々問題があり、大変申し訳なく思っております。本件について猛省し、再度、セキュリティ対策を講じたいと存じます。

この度は、ご迷惑、ご心配をおかけし、大変申し訳ございませんでした。

今後ともよろしく願い申し上げます。

以上です。

2009/07/21 06:00 AM