

弊社サービスの改ざんに関するお詫びとご報告

この度、弊社サービス”アドサーバーVASCO の一部バージョン“におきまして、第三者による悪意的な攻撃を受け、一部データが改ざんされました。これにより、当該期間に弊社サーバーより配信された HTML を閲覧したユーザーの皆様が、悪意あるサイトにアクセスしてしまう事象が発生いたしました。このサイトではウイルスに感染する恐れがあったことが判明いたしました。該当のユーザの皆様には、ご迷惑をお掛けしましたことを深くお詫びいたしますと共に、ウイルススキャン／駆除の実施をお願い致します。尚、今回の根本原因となる脆弱なプログラム自体を削除しており、サービスは正常に動作しております。

記

1. 期間

弊社による調査の結果、9月24日 21:30 頃～9月24日 23:30 頃

弊社サイトから悪意あるサイトへ転送されることにより、今回の事象が発生しておりますので、詳細かつ正確な時間については弊社では記録がございません。弊社にて確認したところ9月24日 23:30 頃には悪意あるサイトへの転送は停止しておりました。

2. 事象の詳細について

- ・弊社サービスに潜在していた脆弱なプログラムに対し、不正な悪意ある攻撃を受け、プログラムが改ざんされました。
- ・弊社プログラムが改ざんされたことにより HTML 内の prepend カラムに第三者の外部 WEB へアクセスする 1x1 ピクセルの iframe タグが挿入されました。
- ・iframe タグ内に、URL 短縮サービスを利用して、悪意あるサイトへ誘導リンクが挿入されていました。
- ・当該誘導リンクは、9/24 23:30 には転送中止の措置が取られていました。(弊社確認)
- ・誘導リンクにより悪意あるサイトへアクセスした場合には、マルウェア「security tool」が設置してありました。
- ・このマルウェアは、ユーザが誤ってダウンロードすることによりインストールされてしまう可能性があるものであります。
- ・弊社プログラムの改ざんを9月25日 1:07 に修正し、対応を完了いたしました。

3. 感染した可能性のあるお客様へのお願い事項

今回感染可能性のあったマルウェア「security tool」のインストールは多くのセキュリティ対象製品の最新版にて、対応済みであり、未然に予防できるものであったと報告されております。そのため、このマルウェアがインストールされているか否かの確認のため、お手数ですが、お手持ちのウイルス対策ソフトを最新の状態にして、ウイルススキャンの実施をお願い致します。

お持ちでない場合は、各セキュリティ会社のホームページにあるオンラインスキャンをお試しください。

明らかに「security tool」がインストールされてしまった場合に、ブラウザが起動せず、オンラインスキャンが実行できない場合がございます。そのような場合に、駆除の方法の詳細等について、以下 URL のような情報が提供されております。そちらをお試し頂きますよう、お願い申し上げます。

参考 URL <http://sec.sourcenext.info/support/securitytool.html>

弊社サービスをご利用いただいているお客様に大変ご迷惑をお掛けしましたことを重ねてお詫び申し上げます。

4. 本件における連絡先

user-support@microad.jp までお問い合わせください。

なお、弊社と致しましては第三者からの不正アクセスの被害を確認したとして、渋谷警察署に被害届を提出し、対応を進めて参ります。

敬具