2008 年 7 月 18 日

国内企業サイトなど約１万ページが改ざん。被害拡大の一因は、不当な営業活動を広げる偽セキュリティソフトウェア

現在、「TROJ_ASPROX（アスプロクス）」ファミリを悪用した SQL インジェクションによる正規 Web サイト改ざん被害が増加していることをお知らせします。
ここでは、最新の脅威とその対策手法についてご紹介いたします。

2008 年 3 月より、日本を標的とした SQL インジェクションによる正規 Web サイトの改ざん被害が広まっています。その被害は、4 ヶ月経過した今なお、深刻なものです。調べによれば、全世界で最大 21 万、日本国内においても約 1 万のウェブページで次の疑わしいコードが記載されていることを確認しています（2008 年 7 月 17 日時点）。

```
src=http://www.{BLOCKED}.mobi/ngg.js
```

図 1 改ざんサイトに見られる不正なリンク

被害サイトは、不動産、食品、自動車部品会社などのほか、大学や個人のサイトまで広範囲にわたっています。
リージョナルトレンドラボの解析結果より、改ざんを計画した悪意あるユーザの狙いが明らかとなっています。なぜ、彼らはその被害を広げているのか。その一例について紹介します。

■「TROJ_ASPROX」を悪用したSQLインジェクション

今回の攻撃は「TROJ_ASPROX」ファミリを悪用した無差別 SQL インジェクション攻撃です。これにより、正規 Web サイトの改ざんが行われます。TROJ_ASPROX は感染したパソコンで勝手に TCP の 80 番ポートを開き、Web プロキシ・サーバとして動作させる不正プログラムです。
攻撃者は、潜在的に脆弱な Microsoft Active Server Pages で作成されたフォーム（例：ログインページ、検索ページ、フィードバックページなどの入力要求を受け付けているもの、または動的にページを生成しているもの）を使用する正規サイトを探しだします。
検索されたページに対し、SQL インジェクション攻撃を仕掛けることで、ウイルス感染サイトへ転送させるコードを埋め込む改ざん攻撃が行われます。
IFRAME タグが埋め込まれたページにアクセスしたユーザは、不正な JavaScript「JS_IFRAME.ABJ」をダウンロードさせられ、さらに別のマルウェアをダウンロードさせられる連鎖攻撃が行われます。

トレンドマイクロ株式会社

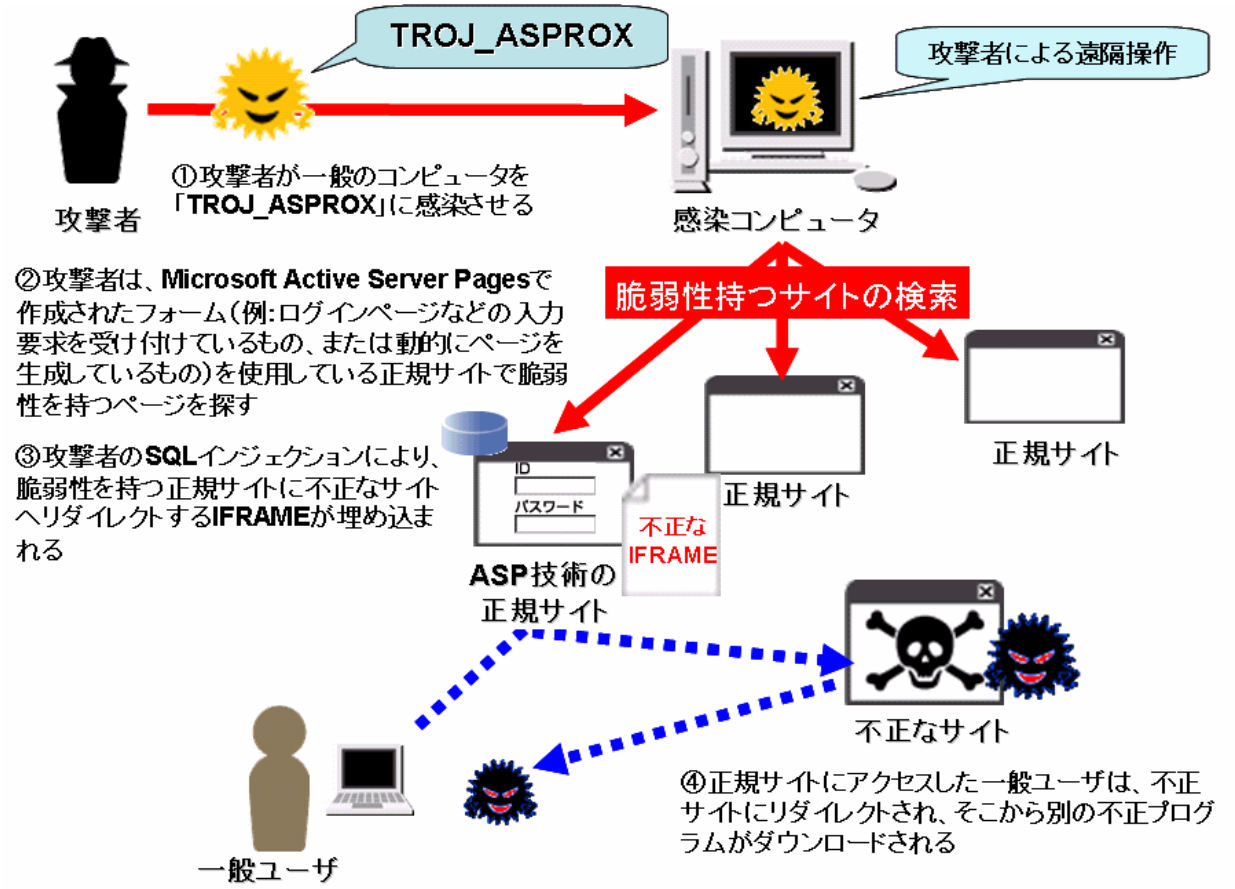

図 2　「TROJ_ASPROX」を悪用した SQL インジェクションによる正規 Web サイトの改ざん攻撃フロー

■不正なJavaScriptから知る攻撃者の標的

不正な JavaScript は、攻撃者の考える標的について我々にヒントを与えています。次のコードは「JS_IFRAME.ABJ」のごく一部です。

```
window.status="";
n=navigator.userLanguage.toUpperCase();
if((n!="ZH-CN")&&(n!="UR")&&(n!="RU")&&(n!="KO")&&
(n!="ZH-TW")&&(n!="ZH")&&(n!="HI")&&(n!="TH")&&
(n!="UR")&&(n!="VI")){
```

図 3 改ざんサイトに見られる不正なリンク

JavaScript で記述されたそのコードでは、改ざんサイトに接続してきた利用者の言語を特定しています。中国語圏(繁体字/簡体字)、インド圏(ウルドゥ語/ヒンディ語)、ロシア語、韓国語、ベトナム語であることが特定された場合、意図的にその処理が無視されます。
言語を特定していることから、広範囲ながら標的型攻撃といえます。

■ 偽セキュリティソフトウェア「ADW_XPSECURITY.CE」

不正な JavaScript は攻撃者により、頻繁な入れ替えが行われています。設置ドメインの数は 250 サイト以上確認されており、セキュリティ対策業者からの追跡から逃れようとしている意図が感じられます。
我々は、連鎖攻撃の末端がユーザに及ぼす影響について注意深く調査しました。その結果、攻撃者の明確な意図が見受けられる転送先を特定しました。それが、不当な営業活動を広げる偽セキュリティソフトウェア「ADW_XPSECURITY.CE」です。
不正 JavaScript によってダウンロードされる偽セキュリティソフトウェアは、その振る舞いから、明らかに不当な営業活動といえます。
ユーザの意志に関係なく、自動インストール/実行される「ADW_XPSECURITY.CE」は、ランダムな名前のファイルを作成し、これらファイルを検索によって検出されたウイルスとして表示させます。

図 4　「ADW_XPSECURITY.CE」自らが作成したファイルをウイルスとして検出、警告

■ 不当な営業活動

偽セキュリティソフトウェア「ADW_XPSECURITY.CE」は検出したウイルスの駆除には、製品購入、登録が必要であると登録サイトへの誘導が促されます。

図５　「ADW_XPSECURITY.CE」による製品登録を促す画面と製品購入ウェブサイト

もちろん、自らウイルスを作成するようなセキュリティソフトウェアの購入は勧められません。
更に、こうした不当な営業活動を行う組織に行き渡ったセンシティブな個人情報（氏名や住所、生年月日、カード番号など）の行方も心配されます。不当な手段で知り得た情報は、第三者への転売など、不法行為への悪用の危険性が考えられます。
今回報告の、サイト改ざんと偽セキュリティソフトウェア販売は確認されている攻撃事例の一例に過ぎません。攻撃者は刻一刻と手を代えて不当な手段で金銭を得ようと考えています。

■ ウェブサイト管理者がすべきこととは

ウェブサイトの改ざんはもはや他人事ではありません。いま、管理者が直ちに実施すべきことは、ウェブサーバのアクセスログを調査することです。
独立行政法人 情報処理推進機構（IPA）では、無償で簡易的に危険な攻撃と思われる痕跡の確認を支援するツール「iLogScanner」を公開しています。専門の技術者を直ちに手配できないような場合には、こうしたツールの支援を受け、アクセスログ解析を行うことを推奨します。
現在、流行している攻撃においては特に、「ngg.js」を含む不正なリンクが含まれていないか確認することも有効です。
アクセスログ解析の結果、攻撃の痕跡が見つからずとも安心すべきではありません。潜在的に脆弱なページを抱えている可能性も考えられます。
マイクロソフト社では、「マイクロソフト セキュリティ アドバイザリ (954462)：ユーザー データ入力の未検証を悪用した SQL インジェクション攻撃の増加」 にて、この種の問題に対処できる 3 つセキュリティツールを公開しています。

1. UrlScan version 3.0 Beta：Internet Information Services（IIS）が処理する HTTP リクエストの種類を制限
2. Microsoft Source Code Analyzer for SQL Injection Community Technology Preview：SQL インジェクションに関するソースコード分析ツール
3. HP Scrawlr：Hewlett-Packard 社開発の SQL インジェクション攻撃を受ける可能性の調査ツール

アクセスログ解析後の次の一手として、こうしたツールの利用も有効です。
より強固な事前予防策として、Web アプリケーションファイヤウォール（WAF：Web Application Firewall、ウェブに対する接続内容を見て、不正なアクセスに対しては、そのリクエストまたはレスポンスを拒否する機能）の導入や、システムコンポーネントに対する定期的なコードレビューと、そのプロセスの正式な組み込み、すなわち脆弱性を徹底的に排除できる運用体制の構築をこの機会に検討することが推奨されます。

トレンドマイクロ株式会社

■ 利用者がすべきこととは

トレンドマイクロでは、一連の攻撃脅威から保護する Web レピュテーション技術を既に投入しています。
こうした不正サイトへのリダイレクトをブロックする先進機能を積極的に取り入れていくも有効です。
もちろん、従来から知られている基本といえる対策も、おろそかにすべきではありません。

- 総合セキュリティソフトの利用とアップデートによる最新状態の維持。
- OS のみならず、アプリケーションの脆弱性に対する速やかな修正。
- いかなるメールにおいても、記載の URL、添付ファイルについて安易にクリックしない。
- 疑わしきサイトへ安易に近づかない。

リージョナルトレンドラボでは、引き続き ASP 技術を採用しているウェブサイトに対する改ざん攻撃の動向について分析を行っていきます。

■ 参考情報

Trend Micro Security Blog:「ASP 技術を採用しているウェブサイトにて改ざん被害が広がる」(2008 年 7 月 17 日)
http://blog.trendmicro.co.jp/archives/1434
Trend Micro Security Blog:「改ざん被害拡大の一因は、不当な営業活動を広げる偽セキュリティソフトウェア」(2008 年 7 月 18 日)
http://blog.trendmicro.co.jp/archives/1446
ウイルスニュース:「SQL インジェクションによる正規 Web サイト改ざんと Web サイト経由の不正プログラム感染を警告」(2008 年 7 月 17 日)
http://jp.trendmicro.com/jp/threat/security_news/virusnews/article/20080717131610.html
TrendLabs Malware Blog:「YAMSIA (Yet Another Massive SQL Injection Attack)」(英語記事:2008 年 7 月 18 日)
http://blog.trendmicro.com/yamsia-yet-another-massive-sql-injection-attack/
トレンドマイクロのウイルス解析/防御技術「Web レピュテーション」
http://jp.trendmicro.com/jp/threat/technique/wrs/

独立行政法人 情報処理推進機構 (IPA):「ウェブサイトの脆弱性検出ツール iLogScanner」
http://www.ipa.go.jp/security/vuln/iLogScanner/index.html
マイクロソフト セキュリティ アドバイザリ (954462):「ユーザー データ入力の未検証を悪用した SQL インジェクション攻撃の増加」
http://www.microsoft.com/japan/technet/security/advisory/954462.mspx

トレンドマイクロ株式会社