2024 年 1 月

2024 年 1 月にリリースされた、シスコのクラウドベースの機械学習によるグローバル脅威アラートに関するアップデートです。

追加の脅威検出

新しい脅威検出をポートフォリオに追加しました。

- Balada Injector

また、既存の脅威検出のインジケーターも更新しました。

Balada Injector

Balada Injector は、WordPress ベースの Web サイトに感染するマルウェアです。バックドアを仕込んで、偽のサポートページ、宝くじ当選サイト、プッシュ通知詐欺など、安全性に問題のあるサイトに訪問者をリダイレクトします。最新の Balada Injector キャンペーンは、Popup Builder バージョン 4.2.3 以前のクロスサイト スクリプティング（XSS）脆弱性（T1189）である CVE-2023-6000 について WPScan が報告した後に開始されました。これらの侵害された Web サイトは、マルウェアを配布するためのフィッシングメール（T1566.001）で使用され、さまざまなマルウェアファミリを展開できます。

お使いの環境で Balada Injector が検出されたかどうかを確認するには、[Balada Injector脅威の詳細（Balada Injector Threat Detail）] をクリックして、グローバル脅威アラートで詳細を表示します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。