

GMO confirms the AI penetration-testing tool ARTEX behind attacks on Japanese companies

Source copy kept by wheresthe.ai for the story “GMO confirms the AI penetration-testing tool ARTEX behind attacks on Japanese companies” (<https://wheresthe.ai/d/jp-china-made-ai-tool-artex-used-in-cyberattacks-on-japanese-2026-10/>).

Source: <https://gmo-cybersecurity.com/blog/20261019/>

Text saved 20 Oct 2026 (the page as published).

SHA-256 of the saved text: dcbd95c31ae140b50a60254af0b21d65f6a370c3455db095171a206f4669f99b

相次ぐ不正アクセスの攻撃元の多くがAIであることを確認

公開日：2026.10.19 更新日：2026.10.19

GMOサイバー犯罪対策センターの福森です。 前回の記事 の続報です。日本企業を狙った侵害事案において攻撃元インフラを調査したところ、AIによる自律型ペネトレーションテストシステムであるARTEXが使われていることを確認いたしました。前回の記事ではフォレンジックログからAIによる攻撃である可能性が高いと推定しておりましたが、それを裏付ける結果となりました。

類似の事件として、2026年9月下旬より発生した韓国の金融機関を標的とした攻撃キャンペーンにARTEXが使われていたことをCrowdStrike社が報じましたが、同じ手口で日本の企業も攻撃してきていることが推察されます。
<https://www.crowdstrike.com/en-us/blog/unknown-threat-actor-uses-artex-to-target-south-korean-finance/>

標的を絞った攻撃キャンペーン

さらに外部機関と連携して調査を進めた結果、あくまで我々が観測できる範囲に限った話になりますが、少なくともその攻撃元インフラからはほぼ日本のみを標的としていることもわかりました。今回調査した攻撃元インフラでは日本企業約20社を標的としており、そのうち9社は同業種のサイトでした。CrowdStrike社の調査結果と併せて考察すると、国と業種を絞った攻撃キャンペーンを行っており、キャンペーンごとに別の攻撃用ホストを用意して攻撃を実行してきていることが見てとれます。

他にもあったAIを使った攻撃インフラ

その見立てを元にしてさらに調査を進めることで、同じように日本企業ばかりを狙ったAIを使った攻撃インフラを6台発見しました。それぞれの攻撃インフラで主な標的としていた業種は以下の通りです。

攻撃インフラ1: デジタルギフト・小売り流通 攻撃インフラ2: 教育・ギフト・印刷 攻撃インフラ3: ポイントギフト・マーケティング 攻撃インフラ4: 保険・金融 攻撃インフラ5: EC メディア・物流 攻撃インフラ6: EC

標的とされていたと我々が確認した日本企業のうち、2026年9~10月ですでに情報漏えいのリリースを出している企業は8社あり、同一の攻撃グループによる犯行により複数の被害が発生していることを示しています。さらなる被害防止のため、これらの情報は法執行機関に共有いたしました。

日本と韓国だけを狙っているのか、他の国は攻撃していないのか、については現在調査中で、また何かわかりましたらブログで紹介します。

シェア

セキュリティ診断のことなら お気軽にご相談ください

セキュリティ診断で発見された脆弱性と、具体的な内容・再現方法・リスク・対策方法を報告したレポートのサンプルをご覧ください。

お問い合わせ 資料ダウンロード