「悪性ボットが迷子になる」— STCLab『BotManager』、ランサムウェア・悪性ボットを無力化する AI 動的防御技術を公開

～ リアルタイムアドレス変換とコード難読化で、ランサムウェアの侵入経路・悪性ボットをブロック ～

【2026年4月xx日】トラフィックマネジメント企業の STCLab（共同代表：パク・ヒョンジュン、キム・ハドン）は、自社のボット検出・ブロックソリューション「BotManager」に「ダイナミック URL」と「コード難読化」技術を導入し、ランサムウェアおよび悪性ボットに対する防御体制を大幅に強化したと、xx日に発表しました。

■ 攻撃対象の Web 環境そのものを「予測不能」に

今回追加された機能の核心は、攻撃者がターゲットとする Web 環境そのものを予測不可能な状態にする点にあります。特に、日本の企業や公共機関を中心に被害が急増しているランサムウェアの侵入経路をブロックし、悪性ボットを利用した自動化攻撃を根本から封じ込めることに重点を置いています。

ランサムウェアとは、攻撃者が Web の脆弱性や自動化された悪性ボットを通じて内部システムへ侵入した後、データを暗号化し、復号の対価として金銭を要求するサイバー攻撃手法です。近年、日本では製造業・医療機関・公共機関を問わずランサムウェア被害が相次いでおり、その初期侵入手段として悪性ボットや自動化スクリプトが活用されるケースが増加していることから、業界内で広く注目を集めています。

■ セッション単位で URL をリアルタイム変換、悪性ボットの経路再利用を無効化

STCLab が新たに適用したダイナミック URL 技術は、アクセスアドレスをセッション単位でリアルタイムに変換する方式です。これにより、特定の時点で生成されたアクセス経路は該当ユーザーおよびセッションにおいてのみ有効となり、外部に共有されたアドレスや事前に取得されたアドレスは、実際のアクセス時点では使用できない状態になります。その結果、悪性ボットが自動でスキャンしたり経路を再利用したりする形での侵入試みを、根本的に無力化することが可能です。

近年では、AI ベースの自動化攻撃が経路を再利用したり、変換後の URL のパターンを追跡することでダイナミック URL 技術を突破しようとする試みも見られます。これに対し

STCLab は、以下のような精緻なオプションを追加し、こうした高度な試みも確実にブロックできるよう対応しました。

- セキュリティキーセットの変更サイクル設定
- リクエスト有効期限の制限
- 切り替え猶予時間の設定

これにより、悪性ボットがダイナミック URL のパターンを学習・再利用することを根本から防止し、強固なセキュリティレイヤーを実現しています。

■ コード難読化と AI スコアリングで検出精度をさらに強化

ボット検出エージェントのセキュリティ性能も同時に強化されました。STCLab はコード難読化技術を適用し、検出スクリプトの構造や動作方式を外部から容易に解析できないようにしました。これにより、攻撃者がセキュリティロジックをリバースエンジニアリングしたり、検出を回避したりしようとする試みを、より困難にします。

さらに、アクセスログをリアルタイムで分析し、各リクエストのリスクを評価する AI スコアリング機能も追加。ランサムウェアの初期侵入試みを含む自動化ベースの異常アクセスに対して、より精密な対処が可能となり、全体的な防御レベルも一段と向上しました。

■「検出・ブロック」から「攻撃が成立しない環境の構築」へ

今回のアップデートにより、BotManager は単にボットを検出・ブロックするにとどまらず、ランサムウェア侵入に利用される悪性ボットや自動化攻撃そのものが機能しにくい環境を構築する方向へと、対応範囲を拡大しました。正規ユーザーの利用フローへの影響を最小限に抑えつつ、異常アクセスや自動化リクエストのパターンに対してはより精密に対応できる、多層セキュリティ体制を実現しています。

STCLab 共同代表のパク・ヒョンジュン氏とキム・ハドン氏は、次のようにコメントしています。

「日本においてランサムウェアによる企業・機関への被害が増加し続けるなか、その初期侵入経路として悪性ボットが頻繁に活用されています。今回の機能強化により、悪性ボットをリアルタイムで無力化し、企業や機関が安全なデジタル環境でビジネスを継続できるよう、積極的に支援してまいります。」