予測型脅威インテリジェンスの新サービス「Early DGA Detection Feed」

2023年5月3日

脅威が日々高まる現在の状況において、組織のセキュリティチームが取れる唯一の選択肢は、常に脅威アクターの一歩先を行く形で積極的に動き続けることです。そこで、WhoisXML APIは最近、不正プロパティを追跡する既存の脅威インテリジェンスフィードを補完する新サービス「Early DGA Detection Feed」を開始しました。この予測型脅威インテリジェンスサービスでは、アルゴリズムによって作成された新規のドメイン名を機械学習と人工知能によって追跡することで、不正行為を目的としたドメイン名をその登録時に特定します。

脅威インテリジェンスにDGAドメイン検知を組み込むメリット

脅威アクターは、アルゴリズムで大量のドメインを作成・登録することで知られています。彼らは、従来のセキュリティエンジンによる検知を避けるため、そうしたドメイン名を悪用するタイミングを意図的に遅らせることがよくあります。

このような行為は、ドメイン名が動員されてコマンド＆コントロール（C&C）サーバー、マルウェアやフィッシングのホストなどの攻撃手段として機能した時に、組織やセキュリティチームの意表をつくことになります。セキュリティソリューションで悪意あるドメイン生成アルゴリズム（DGA）ドメインの存在を発見できたとしても、すでに被害が生じている可能性があります。

しかし、DGAドメインを登録の時点で検出できれば、被害の軽減策を準備したり予防的にブロックしたりすることができ、ひいては最適なセキュリティの実践と厳格なゼロトラストポリシーの実装が可能になります。

Early DGA Detection Feedについて

当社のEarly DGA Detection Feedは、機械学習とAIによってのみ認識できる不審なドメイン名の登録パターンを特定し、DGAドメインを事前に予測します。これらのドメイン名はすでにフィルタリングおよびグループ化されているため、セキュリティチームや研究者の処理時間やコンピューティング資源を節約することができます。

DGAドメインのファイルは毎日提供され、WHOISの登録情報やIPアドレスの紐付けなど、詳細な文脈情報が充実しています。そうしたデータから、悪意あるドメイン名の足跡や隠れたつながりを明らかにすることができます。

「最近のゼロデイ攻撃の増加から、問題が発生してから対応するセキュリティ対策ではもはや組織を十分に保護できないことが明らかです。当社のEarly DGA Detection Feedがあれば、手遅れになる前にセキュリティチームが不審なプロパティを把握できます。」と、Whois XML APIのField CTOで世界的に有名な業界エキスパートであるEd Gibbsは述べています。

Early DGA Detection Feedは、ほとんどのシステムにシームレスに統合できるよう、CSVファイル形式でご提供しています。

サンプルをこちらでダウンロードしていただけます。詳細につきましては、こちらまでお気軽にお問い合わせください。