新しく出現したドメインのセキュリティカテゴリを包括で有効にする

内容

はじめに

このドキュメントでは、Cisco Umbrellaの「Newly Seen Domains」(NSD)セキュリティカテゴリについて説明します。

背景説明

Newly Seen Domains(NSD)は、Cisco Umbrella DNSサービス（ホームユーザ向けの無料のOpenDNSサービスを含む）のユーザが過去24時間以内に最初に照会したドメインを特定するセキュリティカテゴリです。 このセキュリティカテゴリは他のセキュリティカテゴリと同様に機能し、既存のセキュリティ設定または新しいセキュリティ設定の一部として有効にすることができます。ドメインは24時間リストに残ります。

Cisco Umbrellaによるドメインの「新たに認識された」ものとしての定義

新しいドメインは、新しいマルウェアキャンペーンの一環として作成されることがよくあります。これらのキャンペーンの背後にある悪意のある攻撃者は、新しいドメインを使用します。これは、従来のシグニチャベースの方法では、既知の悪意のあるWebサイトをブロックするために攻撃者を認識しないためです。たとえば、フィッシングキャンペーンでは、ユーザにリンクのクリックを促す主要なスパムキャンペーンに付随する新しいドメインを作成できます。リンクはこのキャンペーンの一部として認識されておらず、既知の悪意のあるドメインの標準リストによってブロックされていません。これらのリストにリンクが追加される前に、犯罪者はデータを盗み、マルウェアをインストールし、ネットワークアクセスを取得するのに十分な時間があります。

Newly Seen Domains(NSD)セキュリティカテゴリは、DNSログをチェックして、これまで見たことがないドメインのルックアップを行うことで動作します。無効なクエリの量が多いため、ドメインを新しく認識されるようにマークするには、クライアントクエリが適切な応答を受信する必

要があります。ドメインが最初に認識されると、24時間リストに追加されます。この期間が経過すると、ドメインは新しく表示されなくなり、リストから削除されます。

レポートには、ドメインが照会された時点でそのドメインが属していたカテゴリが記録されます。したがって、クエリ時に新しく検出されたものとしてドメインが分類された場合、アクティビティ検索レポートまたはセキュリティアクティビティレポートにそのようなカテゴリがレポートされます。ただし、リストからドメインの有効期限が切れても、ドメインに関する最新のデータ(特に新しいDestinationsまたはIdentitiesレポートを使用する場合のInvestigate ConsoleやInvestigate API)でそのドメインを調査しても、新しく検出されたドメインは表示されなくなりました。つまり、数日後にドメインを再訪問しても、新しくUmbrellaで見られるようには表示されません。これは意図的に行われていますが、最初の混乱を招く可能性があります。

Newly Seenドメインの唯一の定義は、新たに認識されるドメインという正確な定義です。その結果、新たに検出されたドメインの大部分は悪意のあるドメインではなく、このセキュリティカテゴリで正規のドメインの検出が行われると予想されます。特に、コンテンツを提供するためにランダム化されたサブドメインを生成するAkamaiやCloudfrontなどの特定のサービスやCDNに対して、この問題に対する予防策が実装されています。FacebookやGoogleなどの人気の高いドメインに対する従来の保証も、これらのドメインを含めないために使用されています。

また、完全修飾ドメイン名（2番目のレベルのドメインまたは2番目のレベルのドメインのサブドメイン）のみが、新たに認識されるドメインと見なされます。トップレベルドメインと国番号トップレベルドメインは、ドメインの大規模なグループのブロックを避けるために、新しく認識されるドメインには含まれません。

実装に関する重要な注意事項

一部の不要な検出が予想される場合は、このレポートを監査モードまたは検出のみモードで使用し、ブロックしたりアクションを実行したりしないことを強くお勧めします。デフォルトでは、セキュリティ設定でこのカテゴリを使用できるユーザは、レポートで新しく表示されたドメインを検出として認識します。つまり、この機能はデフォルトではブロックなしで有効になります。ほとんどの場合、ユーザはレポートを使用して、カテゴリに一致するトラフィックを確認し、その情報を使用してこれらのドメインをより詳細に調査し、自動的にブロックするのではなく、セキュリティの脅威を示す可能性があるかどうかを判断します。

もう1つの大きな注意点は、ドメインへの最初のクエリーが許可されていることです。これは、そのドメインへのクエリがCisco Umbrellaで以前に検出されたことがないためです。そのため、このクエリは口ギングシステムによって処理されず、Newly Seen Domainsカテゴリに含まれることになります。ドメインが最初に照会されてから、カテゴリに一致するドメインのリストに表示されるまでの時間は約5分ですが、それ以上の時間がかかる可能性があります。これは、Cisco Umbrellaでは（処理時間とボリュームが原因で）DNSクエリーログを100 %処理する必要がないためです。

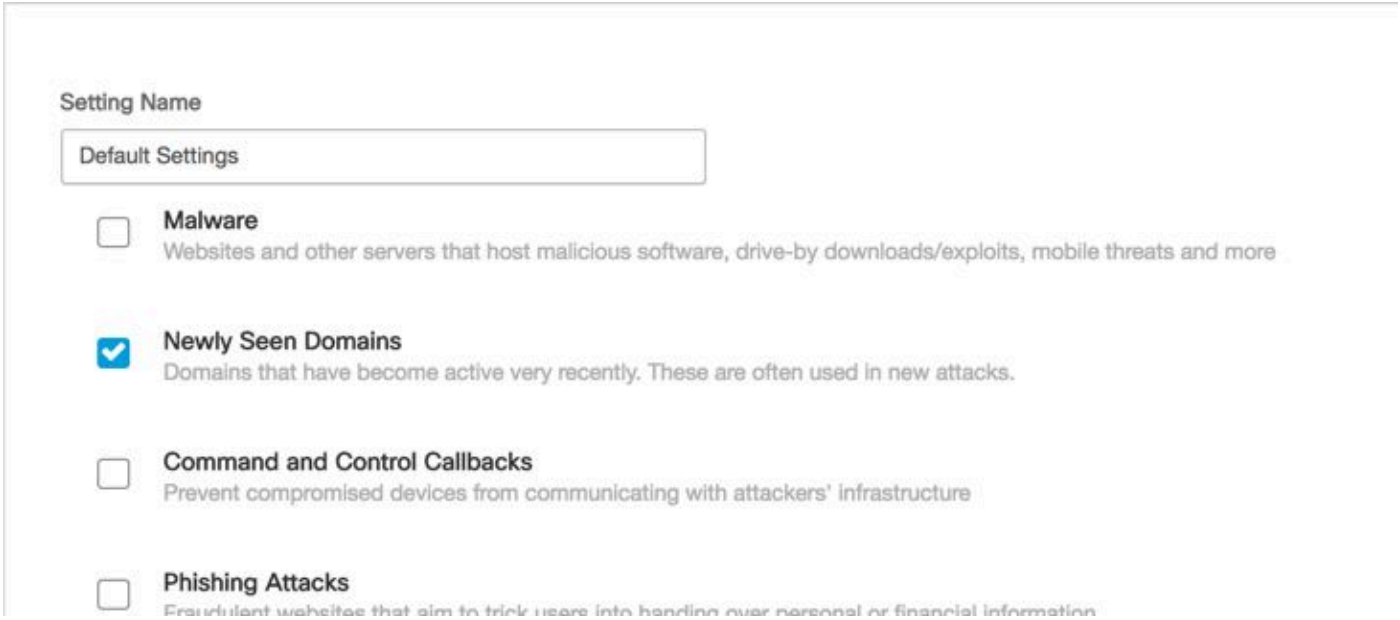
新しく検出されたドメインのプロキシ化

Umbrellaインテリジェントプロキシを使用しているお客様も、NSDカテゴリの一部のドメインがプロキシされていることを確認します。これは仕様です。Umbrella Labsチームは、これらの新しいドメインのプロキシ処理で収集したデータを使用して、マルウェアのカテゴリにただちに追加できるかどうかを判断します。これに伴う副次的な影響の1つとして、プロキシ処理されているNewly Seen Domainに送信される非標準トラフィックがプロキシレベルで廃棄される問題があります。インテリジェントプロキシは、従来Webトラフィックに使用されていたポート80および443のみをプロキシします。これは、カテゴリがブロックされているかどうかにかかわらず、プロキシが有効な場合に自動的に発生します。新しく表示された1つのドメインがプロキシされないようにするには、適切な許可リストに追加します。

インテリジェントプロキシに関する詳細は、Enable the Intelligent Proxyのドキュメントを参照してください。

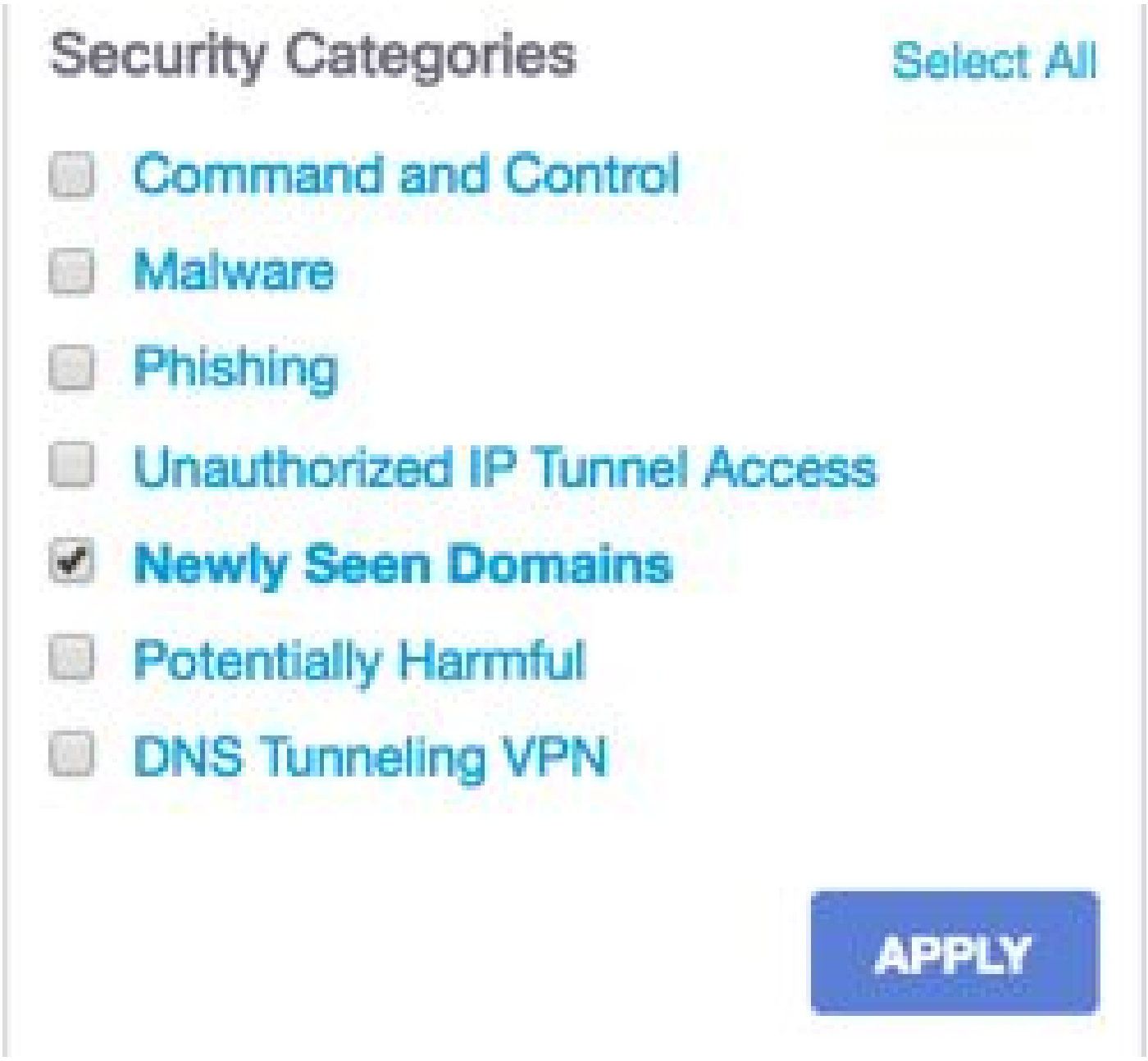
新しく認識されたドメインを有効にする

Newly Seen Domainセキュリティカテゴリは、Policies > Security Settingsで他と同様に有効にし、既存のセキュリティ設定を編集できます。 または、Policy Configuration Wizard自体の中で実行することもできます。



115014822286

新しく検出されたドメインは、アクティビティ検索などの特定のレポートでフィルタリングすることもできます。



115015007423

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。