FTD 7.4パケットキャプチャでのDNS/PTRルックアップパケットの可視性の問題

お問い合わせ内容

セキュリティインテリジェンスによってブロックされると、ファイアウォール脅威対策(FTD)パケットキャプチャは、FTDセキュリティインテリジェンスによってブロックされている悪意のあるドメインに対するDNSクエリを表示しません。 境界FTDの接続イベントは、ドメインに照会しているDNSサーバからのトラフィックを示し、FTDがセキュリティインテリジェンスによってこれらのクエリ応答をブロックしていることを確認します。 ただし、同じイベントでも、通常は予想されないFTDアクセスポリシールールの一致が示されます。 この問題は、悪意のあるドメインクエリをブロックする際に、FTDでSecurity Intelligence(SA)とPTR（逆DNS）ルックアップパケットがどのように相互作用するかに関連しています。 これにより、アクセスルールとセキュリティインテリジェンスの両方に一致するイベントを表示できます。

環境

- Cisco Secure Firewall Firepower 7.4(Firepower Management Center(FMC)/cdFMC/FDM)（セキュリティインテリジェンスを使用するすべてのシステムに適用）
- ソフトウェアバージョン：7.4.2 / 7.4.2.4（セキュリティインテリジェンスを使用するすべてのシステムに適用）
- Infoblox DNSサーバとCIRAクラウド間のDNSトラフィックを監視する境界Firepowerデバイス
- DNS暗号化マイニングの脅威をブロックするように構成されたセキュリティインテリジェンス
- 再現用のFPR2110およびFPR2100デバイスを含むラボトポロジ
- ドメインを対象としたDNSクエリ： static.vdc.vn
- 脅威の分類：DNS暗号化マイニングの脅威
- Firepowerデバイスで分析されたパケットキャプチャと接続イベント
- 内部DNSインフラストラクチャとしてのInfoblox DNSサーバ

解決策

1. FTDの接続イベントを分析して、DNSサーバから外部ドメインへのDNSクエリが、悪意のあるドメインによりSecurity Intelligenceによってブロックされていることを確認します。 特定の送信元および宛先IPアドレスが記録され、イベントでは、送信元から宛先への最初のPTRルックアップを許可するアクセスポリシールールに一致を示すこともできます。 ただし、同じイベントでも、クエリーのURLを明確に示しながら、Blocked by security intelligenceと表示されます。

接続イベント

例：

ドメイン：static.vdc.vn
アクション：ブロック（DNS暗号化マイニングの脅威）

2. 関連するIPアドレス間のDNSトラフィックをターゲットとするFTDでパケットキャプチャを開始します。 送信元IPアドレスからのキャプチャのWireshark分析では、パケットキャプチャの出力に、悪意のあるドメインに特化したDNSクエリは見つかりません。

```
FTD# capture CAP interface match udp host SRCIP host DESTIP eq 53
```

（予想されるパケットの出力なし）

- シスコのドキュメントによると、セキュリティインテリジェンスフィルタリングはアクセスコントロールの初期の段階です。 セキュリティインテリジェンスブロックリストに一致するパケットは、以降の検査の前、および他のポリシー（アクセスコントロール、パケットキャプチャ、DNS検査など）によって処理される前にドロップされる可能性があります。
- セキュリティインテリジェンスフィルタリングは、リソースを大量に消費するインスペクションの前に実行されます。
- セキュリティインテリジェンスによってブロックされたパケットは、デバイス上の標準パケットキャプチャメカニズムによってキャプチャされない場合があります。
- Security Intelligenceの前に評価されたプレフィルタルールも、表示に影響を与える可能性があります。

3. FTDのCLISHでsystem support url-si-debugコマンドを使用して送信元と宛先のIP間のPTRルックアップをトレースし、FTD内でのトラフィックの処理方法とブロック場所を把握して、パケットの送信元ポートを記録します。

```
>システムサポートurl-si-debug
```

```
SRCIP 37046 -&gt; DSTIP 53 17 AS=0 ID=39 GR=1-1 InsightDnsListEventHandler: num_list_matched
```

```
[1], status 0x00010000, INSIGHT_FOUND (0x00010000) | SHMDB (1), static.vnpt.vn, si_list [
1048652 ]
SRCIP 49094 -&gt; DSTIP 53 17 AS=0 ID=42 GR=1-1 InsightDnsListEventHandler: num_list_matched
[1], status 0x00010000, INSIGHT_FOUND (0x00010000) | SHMDB (1), static.vnpt.vn, si_list [
1048652 ]
SRCIP 48508 -&gt; DSTIP 53 17 AS=0 ID=12 GR=1-1 InsightDnsListEventHandler: num_list_matched
[1], status 0x00010000, INSIGHT_FOUND (0x00010000) | SHMDB (1), static.vnpt.vn, si_list [
1048652 ]
```

4. 送信元ポートを参照として使用し、システムサポートトレースからのパケットキャプチャおよびログと関連付けます。 これは、関連付けられたPSを見つけるための最良の方法です。 次の例で示すように、関連するパケットは、通常のDNSクエリではなく、PTR (逆DNS) ルックアップとして表示されます。 これが、送信元IPアドレスからキャプチャを見ても悪意のあるドメインクエリが見つからない理由です。 これらのタイプのパケットは、同じ接続が「Blocked by security intelligence」と表示される場合でも、イベントに対して表示されるアクセスポリシーにヒットします。

```
8847 2026-01-29 20:41:15.940854Z SRCIP DSTIP DNS 98 Standard query 0x20ef PTR 23.172.189.113.in-
addr.arpa OPT
9582 2026-01-29 20:41:18.348889Z SRCIP DSTIP DNS 98 Standard query 0x8b58 PTR 23.172.189.113.in-
addr.arpa OPT
10190 2026-01-29 20:41:21.556901Z SRCIP DSTIP DNS 98 Standard query 0x636a PTR
23.172.189.113.in-addr.arpa OPT
11362 2026-01-29 20:41:24.652950Z SRCIP DSTIP DNS 99 Standard query 0xf6f5 PTR
135.238.166.113.in-addr.arpa OPT
13670 2026-01-29 20:41:27.964885Z SRCIP DSTIP DNS 98標準クエリ0xfb40 PTR 23.172.189.113.in-
addr.arpa OPT
```

5. 宛先からのこれらのPTRルックアップへの応答パケットを確認すると、悪意のあるドメインが検出される可能性があります。 これにより、FTDは悪意のあるドメインを認識するようになり、セキュリティインテリジェンスによって最終的に接続をブロックします。

```
981 2026-01-29 20:41:12.631818Z DSTIP SRCIP DNS 126 static.vnpt.vn Standard query response
0xc5c3 PTR 23.172.189.113.in-addr.arpa PTR static.vnpt.vn OPT
```

顧客チームと連携して、暗号マイニングの脅威に関連する特定のIPについて、逆DNSクエリや予期しないトラフィックパターンが見られるかどうかを調査します。 特定のトラフィックを許可するか、さらに分析するには、必要なIPをDo-Not-Blockリストに追加するか、またはプレフィルタで許可します。 これにより、パケットキャプチャで後続のインスペクションと可視性が可能になります。

- さらに分析が必要な場合は、IPをSecurity Intelligence Do-Not-Blockリストに追加します。
- prefilterで許可すると、トラフィックはセキュリティインテリジェンスブロックをバイパス

できます。

原因

根本的な原因は、PTR（逆DNS）ルックアップが最初にアクセスルールによってFTDを通過し、まだセキュリティインテリジェンスの検査を待っていることです。 PTRルックアップの応答パケットには、悪意のあるドメイン名が含まれています。 PTR応答がセキュリティインテリジェンスブロックリスト(SIB)のエントリ（DNS暗号化マイニング脅威に関連付けられているものなど）と一致すると、パケットはドロップされます。 その結果、悪意のあるドメインはPTRルックアップ応答でしか見つからず、イベントによってAllow for accessルールとBlock for security intelligenceの両方で一致が示されることがあります。

関連コンテンツ

- Cisco Secure Firewall Management Centerデバイス設定ガイド7.4：セキュリティインテリジェンスについて
- シスコのテクニカルサポートとダウンロード
- Cisco Bug ID CSCwt16755:DOC:PTRルックアップはACポリシーによってFTDを渡すが、応答がセキュリティインテリジェンスによってブロックされる

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。