FTD 7.4封包擷取中的DNS/PTR查詢封包可見性問題

問題

當被安全情報阻止時，防火牆威脅防禦(FTD)資料包捕獲不會顯示對正被FTD安全情報阻止的惡意域的DNS查詢。周界FTD上的連線事件顯示來自查詢域的DNS伺服器的流量，並確認FTD正通過安全情報阻止這些查詢響應。但是，相同事件也顯示FTD訪問策略規則上的匹配項，這通常不是預期的匹配項。該問題似乎與阻止惡意域查詢時，安全情報和PTR（反向DNS）查詢資料包在FTD上的互動方式有關。這可能顯示與訪問規則匹配的事件安全情報。

環境

- 思科安全防火牆Firepower 7.4(Firepower管理中心(FMC)/cdFMC/FDM)（適用於使用安全智慧的所有系統）
- 軟體版本：7.4.2/7.4.2.4（適用於使用安全情報的所有系統）
- 監視Infoblox DNS伺服器和CIRA雲之間的DNS流量的周邊Firepower裝置
- 配置為阻止DNS加密挖掘威脅的安全情報
- 涉及用於複製的FPR2110和FPR2100裝置的實驗拓撲
- DNS查詢目標域：static.vdc.vn
- 威脅分類：DNS加密挖掘威脅
- 在Firepower裝置上分析資料包捕獲和連線事件
- 作為內部DNS基礎設施的Infoblox DNS伺服器

解析

1.分析FTD上的連線事件，以確認安全智慧因惡意域而阻止了從DNS伺服器到外部域的DNS查詢。註明了特定的源和目標IP地址，該事件甚至可以表明訪問策略規則上的匹配，該規則允許從源到目標的初始PTR查詢。但是，同一事件還顯示了被安全智慧阻止的，同時清楚地說明了查詢的URL。

連線事件

範例：

域：static.vdc.vn
Action:已阻止（DNS加密挖掘威脅）

2.在FTD上啟動資料包捕獲，目標為相關IP地址之間的DNS流量。在Wireshark對源IP地址捕獲的分析中，在資料包捕獲輸出中找不到專門針對惡意域的DNS查詢。

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

（預期資料包沒有輸出）

- 根據思科文檔，安全情報過濾是訪問控制的一個早期階段。如果資料包匹配安全情報阻止清單，則可以在進一步檢查之前丟棄該資料包，然後再由其他策略（包括訪問控制、資料包捕獲、DNS檢查）進行處理。
- 安全情報過濾在資源密集型檢查之前進行。
- 安全情報阻止的資料包有時不會被裝置上的標準資料包捕獲機制捕獲。
- 在安全情報之前評估的預過濾器規則也會影響可見性。

3.使用FTD CLISH中的system support url-si-debug命令追蹤來源和目的地IP之間的PTR查詢，以瞭解流量在FTD中處理及封鎖的方式和位置，並記錄封包的來源連線埠。

```
>系統支援url-si-debug

SRCIP 37046 -&gt;DSTIP 53 17 AS=0 ID=39 GR=1-1 InsightDnsListEventHandler:num_list_matched
[1]，狀態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]，狀態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]，狀態0x00010000,INSIGHT_FOUND(0x00010000) | SHMDB(1), static.vnpt.vn， si_list [ 1048652 ]
```

4.使用源埠作為參考，與來自系統支援跟蹤的資料包捕獲和日誌相關。這是查詢相關ps的最佳方法。如下面的示例所示，相關資料包顯示為PTR（反向DNS）查詢，而不是正常的DNS查詢。這就是在檢視源IP地址的捕獲時找不到惡意域查詢的原因。這些型別的資料包會命中訪問策略，訪問策略在事件上顯示，即使同一連線顯示為「被安全情報阻止」(Blocked by security intelligence)。

```
8847 2026-01-29 20:41:15.940854Z SRCIP DSTIP DNS 98標準查詢0x20ef PTR 23.172.189.113.in-
addr.arpa光纖
9582 2026-01-29 20:41:18.348889Z SRCIP DSTIP DNS 98標準查詢0x8b58 PTR 23.172.189.113.in-addr.arpa
```

OPT
10190 2026-01-29 20:41:21.556901Z SRCIP DSTIP DNS 98標準查詢0x636a PTR 23.172.189.113.in-addr.arpa OPT
11362 2026-01-29 20:41:24.652950Z SRCIP DSTIP DNS 99標準查詢0xf6f5 PTR 135.238.166.113.in-addr.arpa OPT
13670 2026-01-29 20:41:27.964885Z SRCIP DSTIP DNS 98標準查詢0xfb40 PTR 23.172.189.113.in-addr.arpa OPT

5.檢查來自目標的這些PTR查詢的答複資料包，可以看到惡意域。這將觸發FTD最終通過安全情報阻止連線，因為它現在看到惡意域。

981 2026-01-29 20:41:12.631818Z DSTIP SRCIP DNS 126 static.vnpt.vn標準查詢響應0xc5c3 PTR 23.172.189.113.in-addr.arpa PTR static.vnpt.vn OPT

與客戶小組協調，調查是否觀察到與加密挖掘威脅相關的給定IP存在任何反向DNS查詢或意外流量模式。若要允許特定流量或進一步分析該流量，請將所需的IP新增到「不阻止」清單中，或根據需要通過預過濾器進行允許。這樣可以在資料包捕獲中允許後續檢查和可見性。

- 如果需要進一步的分析，請將IP新增到安全情報不阻止清單。
- 允許進入預過濾器允許流量繞過安全情報阻止。

原因

根本原因是PTR（反向DNS）查詢最初通過訪問規則的FTD，因為它仍在等待安全情報檢查。PTR查詢的響應資料包隨後包含惡意域名。當PTR響應與安全情報阻止清單條目（例如與DNS加密挖掘威脅關聯）匹配時，資料包將被丟棄。因此，惡意域僅在PTR查詢答覆中找到，有時事件會在「允許訪問」規則和「阻止安全情報」上顯示匹配。

相關內容

- 思科安全防火牆管理中心裝置配置指南7.4：關於安全情報
- 思科技術支援與下載
- 思科錯誤ID CSCwt16755 - DOC:PTR查詢通過FTD by AC策略，但響應被安全情報阻止

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。