FTD 7.4数据包捕获中的DNS/PTR查找数据包可视性问题

问题

当被安全情报阻止时，防火墙威胁防御(FTD)数据包捕获不会显示对被FTD安全情报阻止的恶意域的DNS查询。周边FTD上的连接事件显示来自查询域的DNS服务器的流量，并确认FTD通过安全情报阻止这些查询响应。但是，同一事件还显示FTD访问策略规则上的匹配项，这通常不是预期的匹配项。此问题似乎与安全情报和PTR（反向DNS）查找数据包在阻止恶意域查询时如何在FTD上交互有关。这可以显示匹配访问规则的事件安全情报。

环境

- 思科安全防火墙Firepower 7.4(Firepower管理中心(FMC)/cdFMC/FDM)（适用于使用安全情报的所有系统）
- 软件版本：7.4.2/7.4.2.4（适用于使用安全情报的所有系统）
- 周界Firepower设备监控Infoblox DNS服务器和CIRA云之间的DNS流量
- 配置为阻止DNS加密挖掘威胁的安全情报
- 涉及用于复制的FPR2110和FPR2100设备的实验拓扑
- DNS查询目标域：static.vdc.vn
- 威胁分类：DNS加密挖掘威胁
- 在Firepower设备上分析数据包捕获和连接事件
- 作为内部DNS基础设施的Infoblox DNS服务器

分辨率

1.分析FTD上的连接事件，以确认安全情报因恶意域而阻止了从DNS服务器到外部域的DNS查询。已注明特定源和目标IP地址，事件甚至可以表明访问策略规则上的匹配项，该规则允许从源到目标的初始PTR查找。但是，同一事件还显示被安全情报阻止的，同时明确说明查询的URL。

连接事件

示例：

域名：static.vdc.vn
操作：已阻止（DNS加密挖掘威胁）

2.在FTD上启动针对相关IP地址之间的DNS流量的数据包捕获。在对来自源IP地址的捕获进行Wireshark分析时，在数据包捕获输出中找不到专门针对恶意域的DNS查询。

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

（预期数据包没有输出）

- 根据思科文档，安全情报过滤是访问控制的一个早期阶段。如果数据包与安全情报阻止列表匹配，则可以在进一步检查之前将其丢弃，然后再由其他策略（包括访问控制、数据包捕获、DNS检查）进行处理。
- 安全情报过滤发生在资源密集型检查之前。
- 安全情报阻止的数据包有时不会被设备上的标准数据包捕获机制捕获。
- 在安全情报影响可视性之前评估预过滤器规则。

3.使用FTD CLISH中的system support url-si-debug命令跟踪源IP和目标IP之间的PTR查找，以了解流量在FTD中处理和阻止的方式和位置，并记录数据包的源端口。

```
> System Support url-si-debug
```

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

4.使用源端口作为参考，与来自系统支持跟踪的数据包捕获和日志相关联。这是查找相关ps的最佳方法。如下例所示，相关数据包显示为PTR（反向DNS）查找，而不是正常的DNS查询。这就是在查看来自源IP地址的捕获时找不到恶意域查询的原因。这些类型的数据包会命中一个访问策略，该访问策略在事件上显示，即使同一连接显示为“被安全情报阻止”（Blocked by security intelligence）。

```
8847 2026-01-29 20:41:15.940854Z SRCIP DSTIP DNS 98标准查询0x20ef PTR 23.172.189.113.in-addr.arpa
OPT
9582 2026-01-29 20:41:18.348889Z SRCIP DSTIP DNS 98标准查询0x8b58 PTR 23.172.189.113.in-addr.arpa
```

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

5.检查来自目标的这些PTR查找的应答数据包，可以看到恶意域。这会触发FTD按安全情报最终阻止连接，因为它现在看到恶意域。

981 2026-01-29 20:41:12.631818Z DSTIP SRCIP DNS 126 static.vnpt.vn标准查询响应0xc5c3 PTR 23.172.189.113.in-addr.arpa PTR static.vnpt.vn OPT

与客户团队协调，调查是否观察到与加密挖掘威胁相关的给定IP的任何反向DNS查询或意外流量模式。若要允许特定流量或进一步分析该流量，请将所需的IP添加到“不阻止”列表，或根据需要通过预过滤器允许。这样可以在数据包捕获中允许后续检查和可见性。

- 如果需要进一步分析，请将IP添加到安全情报Do-Not-Block列表。
- 允许在预过滤器中允许流量绕过安全情报阻止。

原因

根本原因是PTR（反向DNS）查找最初通过访问规则的FTD，因为它仍在等待安全情报检测。PTR查找的响应数据包随后包含恶意域名。当PTR响应与安全情报块列表条目（例如与DNS加密挖掘威胁相关联）匹配时，数据包将被丢弃。因此，恶意域只在PTR查找回复中找到，有时事件会在“允许访问”规则和“阻止安全情报”上显示匹配。

相关内容

- 思科安全防火墙管理中心设备配置指南，7.4：关于安全情报
- 思科技术支持和下载
- 思科漏洞ID CSCwt16755 - DOC:PTR查找通过FTD的交流策略，但响应被安全情报阻止

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。