Búsqueda de DNS/PTR Problemas de visibilidad de paquetes en capturas de paquetes de FTD 7.4

Problema

Cuando la inteligencia de seguridad la bloquea, la captura de paquetes de Defensa contra amenazas de firewall (FTD) no muestra consultas DNS a los dominios malintencionados que están bloqueados por la inteligencia de seguridad de FTD. Los eventos de conexión en el FTD perimetral muestran el tráfico del servidor DNS que consulta el dominio y confirman que FTD está bloqueando estas respuestas de consulta a través de la inteligencia de seguridad. Sin embargo, el mismo evento también muestra una coincidencia en una regla de política de acceso de FTD que normalmente no se espera. El problema parece estar relacionado con la forma en que la inteligencia de seguridad y los paquetes de búsqueda de PTR (DNS inverso) interactúan en los FTD al bloquear consultas de dominio malintencionadas. Esto puede mostrar un evento que coincide con una regla de seguridad.

Entorno

- Cisco Secure Firewall Firepower 7.4 (Firepower Management Center (FMC) / cdFMC / FDM) (aplicable a todos los sistemas que utilizan inteligencia de seguridad)
- Versión del software: 7.4.2 / 7.4.2.4 (aplicable a todos los sistemas que utilizan inteligencia de seguridad)
- Dispositivo perimetral Firepower que supervisa el tráfico DNS entre el servidor DNS Infoblox y la nube CIRA
- Inteligencia de seguridad configurada para bloquear amenazas de minería de cifrado DNS
- Topología de laboratorio que incluye dispositivos FPR2110 y FPR2100 para la reproducción
- DNS query targeting domain: static.vdc.vn
- Clasificación de amenazas: amenaza de minería de criptografía DNS
- Captura de paquetes y eventos de conexión analizados en un dispositivo Firepower
- Servidor DNS Infoblox como infraestructura DNS interna

Resolución

1. Analice los eventos de conexión en el FTD para confirmar que las consultas DNS del servidor DNS al dominio externo están siendo bloqueadas por la inteligencia de seguridad debido a un dominio malintencionado. Se anota una dirección IP de origen y destino específica y el evento puede incluso indicar una coincidencia en una regla de política de acceso que permite la búsqueda PTR inicial de origen a destino. Sin embargo, el mismo evento también muestra un mensaje Bloqueado por la inteligencia de seguridad al tiempo que indica claramente la dirección URL de la consulta.

```
Evento de conexión
```

Ejemplo:

Dominio: static.vdc.vn
Acción: Bloqueado (amenaza de minería de cifrado DNS)

2. Inicie una captura de paquetes en el FTD dirigida al tráfico DNS entre las direcciones IP relevantes. En un análisis de Wireshark de las capturas de la dirección IP de origen, no se encuentra ninguna consulta DNS específica para el dominio malicioso en la salida de captura de paquetes.

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

```
(no hay salida para los paquetes esperados)
```

- Según la documentación de Cisco, el filtrado de inteligencia de seguridad es una fase temprana del control de acceso. Si un paquete coincide con una lista de bloques de inteligencia de seguridad, se puede descartar antes de realizar una inspección adicional y antes de que otras políticas lo procesen (incluido el control de acceso, la captura de paquetes y la inspección de DNS).
- El filtrado de inteligencia de seguridad se produce antes de la inspección que utiliza muchos recursos.
- A veces, los mecanismos de captura de paquetes estándar del dispositivo no capturan los paquetes bloqueados por la inteligencia de seguridad.
- Las reglas de prefiltrado evaluadas antes de que la inteligencia de seguridad también puedan afectar a la visibilidad.

3. Utilice el comando system support url-si-debug en FTD CLISH para rastrear las búsquedas PTR entre las IP de origen y de destino para comprender cómo y dónde se procesa y bloquea el tráfico dentro del FTD y observe los puertos de origen para los paquetes.

```
> system support url-si-debug


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

4. Utilice los puertos de origen como referencia para correlacionar con las capturas de paquetes y los registros del seguimiento de soporte del sistema. Este es el mejor método para encontrar el ps asociado. Como se ve en este siguiente ejemplo, los paquetes relacionados se muestran como búsquedas PTR (DNS inverso) en lugar de consultas DNS normales. Es por eso que no se puede encontrar la consulta de dominio malicioso al buscar capturas de la dirección IP de origen. Estos tipos de `paquetes llegan a una política de acceso` que se muestra en un evento, incluso si la misma conexión se muestra como bloqueada por la inteligencia de seguridad.

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

5. Revise los paquetes de respuesta a estas búsquedas PTR desde el destino y se podrá ver el dominio malicioso. Esto hace que el FTD bloquee finalmente la conexión mediante inteligencia de seguridad, ya que ahora ve el dominio malicioso.

```
981 2026-01-29 20:41:12.631818Z DSTIP SRCIP DNS 126 static.vnpt.vn Respuesta estándar a la
consulta 0xc5c3 PTR 23.172.189.113.in-addr.arpa PTR static.vnpt.vn OPT
```

Coordine con el equipo del cliente para investigar si se observan consultas de DNS inverso o patrones de tráfico inesperados para determinadas IP relacionadas con la amenaza de minería de criptografía. Para permitir el tráfico específico o analizarlo más a fondo, agregue las IP necesarias a la lista No bloquear o permita el uso del prefiltro según corresponda. Esto puede permitir la inspección y visibilidad subsiguientes en la captura de paquetes.

- Agregue direcciones IP a la lista Do-Not-Block (No bloquear) de Security Intelligence si es

necesario realizar un análisis más detallado.

- Si se permite en el prefiltro, el tráfico puede eludir el bloque de inteligencia de seguridad.

Causa

La causa raíz es que la búsqueda de PTR (DNS inverso) pasa a través del FTD inicialmente por la regla de acceso, ya que aún está pendiente de la inspección de inteligencia de seguridad. El paquete de respuesta para la búsqueda de PTR contiene el nombre de dominio malintencionado. Cuando una respuesta de PTR coincide con una entrada de la lista de bloqueo de inteligencia de seguridad (como la asociada a la amenaza de minería de cifrado de DNS), el paquete se descarta. Como resultado, el dominio malintencionado sólo se encuentra en la respuesta de búsqueda de PTR y los eventos a veces muestran una coincidencia tanto en una regla de permiso de acceso como en un bloqueo de inteligencia de seguridad.

Contenido relacionado

- Guía de configuración de dispositivos de Cisco Secure Firewall Management Center, 7.4: Acerca de la inteligencia de seguridad
- Soporte técnico y descargas de Cisco
- ID de error de Cisco CSCwt16755 - DOC: las búsquedas de PTR superan el FTD por la política de CA, pero la inteligencia de seguridad bloquea la respuesta

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).