Problèmes de visibilité des paquets de recherche DNS/PTR dans les captures de paquets FTD 7.4

Problème

Lorsqu'elle est bloquée par la sécurité adaptative, la capture de paquets FTD (Firewall Threat Defense) n'affiche pas les requêtes DNS vers les domaines malveillants qui sont bloqués par la sécurité adaptative FTD. Les événements de connexion sur le FTD de périmètre affichent le trafic du serveur DNS qui interroge le domaine et confirment que le FTD bloque ces réponses de requête via la sécurité adaptative. Toutefois, le même événement affiche également une correspondance sur une règle de stratégie d'accès FTD qui n'est généralement pas attendue. Le problème semble lié à la façon dont les paquets Security Intelligence et PTR (reverse DNS) Lookup interagissent sur les FTD lors du blocage des requêtes de domaine malveillant. Cela peut afficher un événement qui correspond à la fois à une règle d'accès et à la sécurité adaptative.

Environnement

- Cisco Secure Firewall Firepower 7.4 (Firepower Management Center (FMC) / cdFMC / FDM) (applicable à tous les systèmes utilisant l'intelligence de sécurité)
- Version du logiciel : 7.4.2 / 7.4.2.4 (applicable à tous les systèmes utilisant l'intelligence de sécurité)
- Périphérique Firepower surveillant le trafic DNS entre le serveur DNS Infoblox et le cloud CIRA
- Security Intelligence configuré pour bloquer les menaces d'exploration de données de chiffrement DNS
- Topologie de TP impliquant des périphériques FPR2110 et FPR2100 pour la reproduction
- Domaine de ciblage de requête DNS : static.vdc.vn
- Classification des menaces : menace d'exploration de données de chiffrement DNS
- Événements de capture de paquets et de connexion analysés sur le périphérique Firepower
- Serveur DNS Infoblox comme infrastructure DNS interne

Résolution

1. Analysez les événements de connexion sur le FTD pour confirmer que les requêtes DNS du serveur DNS vers le domaine externe sont bloquées par Security Intelligence en raison d'un domaine malveillant. Une adresse IP source et de destination spécifique est notée et l'événement peut même indiquer une correspondance sur une règle de stratégie d'accès qui autorise la recherche PTR initiale de la source vers la destination. Cependant, le même événement affiche également un Blocked by security intelligence tout en indiquant clairement l'URL pour la requête.

```
Événement de connexion
```

Exemple :

Domaine : statique.vdc.vn
Action : Bloqué (menace d'exploration de cryptage DNS)

2. Lancez une capture de paquets sur le FTD ciblant le trafic DNS entre les adresses IP concernées. Dans une analyse Wireshark des captures à partir de l'adresse IP d'origine, aucune requête DNS n'est trouvée spécifiquement pour le domaine malveillant dans le résultat de capture de paquets.

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

```
(aucun résultat pour les paquets attendus)
```

- Selon la documentation Cisco, le filtrage Security Intelligence est une phase précoce du contrôle d'accès. Si un paquet correspond à une liste de blocage Security Intelligence, il peut être abandonné avant une inspection plus poussée et avant d'être traité par d'autres politiques (y compris le contrôle d'accès, la capture de paquets, l'inspection DNS).
- Le filtrage Security Intelligence se produit avant l'inspection gourmande en ressources.
- Les paquets bloqués par Security Intelligence ne sont parfois pas capturés par les mécanismes de capture de paquets standard sur le périphérique.
- Les règles de préfiltre évaluées avant Security Intelligence peuvent également affecter la visibilité.

3. Utilisez la commande system support url-si-debug dans FTD CLISH pour suivre les recherches PTR entre les adresses IP source et de destination afin de comprendre comment et où le trafic est traité et bloqué dans le FTD et noter les ports source pour les paquets.

```
> support système url-si-debug
```

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

4. Utilisez les ports source comme référence pour établir une corrélation avec les captures de paquets et les journaux à partir de la trace de prise en charge du système. C'est la meilleure méthode pour trouver les paquets associés. Comme le montre cet exemple suivant, les paquets associés s'affichent sous forme de recherches PTR (reverse DNS) au lieu de requêtes DNS normales. C'est pourquoi la requête de domaine malveillant ne peut pas être trouvée lors de l'examen des captures à partir de l'adresse IP d'origine. Ces types de `paquets atteignent une stratégie d'accès` qui s'affiche sur un événement même si la même connexion s'affiche comme bloquée par l'intelligence de sécurité.

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

5. Vérifiez les paquets de réponse à ces recherches PTR à partir de la destination et le domaine malveillant peut être vu. Cela déclenche le FTD pour finalement bloquer la connexion par la sécurité de l'intelligence comme il voit maintenant le domaine malveillant.

```
981 2026-01-29 20:41:12.631818Z DSTIP SRCIP DNS 126 static.vnpt.vn Réponse de requête standard
0xc5c3 PTR 23.172.189.113.in-addr.arpa PTR static.vnpt.vn OPT
```

Coordonnez-vous avec l'équipe du client pour rechercher si des requêtes DNS inversées ou des modèles de trafic inattendus sont observés pour des adresses IP données liées à la menace d'exploration de données. Pour autoriser un trafic spécifique ou pour l'analyser plus en détail, ajoutez les adresses IP requises à la liste Do-Not-Block ou autorisez via un préfiltre, selon le cas. Cela peut permettre une inspection et une visibilité ultérieures de la capture de paquets.

- Ajoutez des adresses IP à la liste de sécurité intelligente à ne pas bloquer si une analyse plus approfondie est requise.
- L'autorisation dans le préfiltre permet au trafic de contourner le bloc Security Intelligence.

Motif

La cause principale est que la recherche PTR (DNS inversée) passe d'abord par la règle d'accès car elle est toujours en attente d'inspection de la sécurité intelligente. Le paquet de réponse pour la recherche PTR contient alors le nom de domaine malveillant. Lorsqu'une réponse PTR correspond à une entrée de liste de blocage de la sécurité intelligente (telle qu'associée à une menace d'exploration de données de chiffrement DNS), le paquet est abandonné. Par conséquent, le domaine malveillant se trouve uniquement dans la réponse de recherche PTR et les événements montrent parfois une correspondance à la fois sur une règle d'autorisation d'accès et sur un bloc pour la sécurité intelligente.

Autres informations utiles

- Guide de configuration des périphériques Cisco Secure Firewall Management Center, 7.4 : À propos de Security Intelligence
- Assistance technique de Cisco et téléchargements
- ID de bogue Cisco CSCwt16755 - DOC : les recherches PTR passent FTD par la stratégie AC, mais la réponse est bloquée par Security Intelligence

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.