Problemas de visibilidade de pacote de pesquisa DNS/PTR em capturas de pacote FTD 7.4

Problema

Quando bloqueado pela inteligência de segurança, a captura de pacotes FTD (Firewall Threat Defense) não exibe consultas DNS para os domínios mal-intencionados que estão sendo bloqueados pela inteligência de segurança do FTD. Os eventos de conexão no FTD do perímetro mostram o tráfego do servidor DNS que consulta o domínio e confirmam que o FTD está bloqueando essas respostas de consulta por meio da inteligência de segurança. No entanto, o mesmo evento também mostra uma correspondência em uma regra de política de acesso do FTD que normalmente não é esperada. O problema aparece relacionado a como os pacotes de Inteligência de Segurança e Pesquisa PTR (DNS reverso) interagem nos FTDs ao bloquear consultas de domínio mal-intencionadas. Isso pode mostrar um evento que corresponde a uma regra de acesso e a uma regra de acesso. inteligência de segurança.

Ambiente

- Cisco Secure Firewall Firepower 7.4 (Firepower Management Center (FMC) / cdFMC / FDM) (aplicável a todos os sistemas que usam inteligência de segurança)
- Versão do software: 7.4.2 / 7.4.2.4 (aplicável a todos os sistemas que usam inteligência de segurança)
- Perímetro Dispositivo Firepower monitorando o tráfego DNS entre o servidor DNS Infoblox e a nuvem CIRA
- Inteligência de segurança configurada para bloquear ameaças de mineração de criptografia DNS
- Topologia de laboratório envolvendo dispositivos FPR2110 e FPR2100 para reprodução
- Domínio de destino da consulta DNS: static.vdc.vn
- Classificação da ameaça: Ameaça de mineração de criptografia DNS
- Eventos de captura e conexão de pacotes analisados no dispositivo Firepower
- Servidor DNS do Infoblox como infraestrutura de DNS interna

Resolução

1. Analise eventos de conexão no FTD para confirmar se as consultas DNS do servidor DNS para o domínio externo estão sendo bloqueadas pelo Security Intelligence devido a um domínio mal-intencionado. Um endereço IP de origem e de destino específico é anotado e o evento pode até mesmo declarar uma correspondência em uma regra de política de acesso que permite a pesquisa PTR inicial da origem para o destino. No entanto, o mesmo evento também mostra um Bloqueado por inteligência de segurança ao declarar claramente a URL da consulta.

```
Evento de conexão
```

Exemplo:

Domínio: static.vdc.vn
Ação: Bloqueado (ameaça de mineração de criptografia DNS)

2. Inicie uma captura de pacotes no FTD que tenha como alvo o tráfego DNS entre os endereços IP relevantes. Em uma análise do Wireshark das capturas do endereço IP de origem, nenhuma consulta DNS é encontrada especificamente para o domínio mal-intencionado na saída da captura de pacotes.

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

```
(sem saída para os pacotes esperados)
```

- De acordo com a documentação da Cisco, a filtragem de Inteligência de Segurança é uma fase inicial do controle de acesso. Se um pacote corresponder a uma Lista de Bloqueios de Inteligência de Segurança, ele poderá ser descartado antes de uma inspeção adicional e antes de ser processado por outras políticas (incluindo controle de acesso, captura de pacotes, inspeção DNS).
- A filtragem de inteligência de segurança ocorre antes da inspeção que consome muitos recursos.
- Os pacotes bloqueados pelo Security Intelligence às vezes não são capturados pelos mecanismos de captura de pacotes padrão no dispositivo.
- As regras de pré-filtro avaliadas antes da Inteligência de segurança também podem afetar a visibilidade.

3. Utilize o comando system support url-si-debug no FTD CLISH para rastrear pesquisas PTR entre IPs de origem e destino para entender como e onde o tráfego está sendo processado e bloqueado no FTD e observe as portas de origem dos pacotes.

```
> system support url-si-debug
```

```
37046 SRCIP -&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 ]
49094 SRCIP -&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 ]
48508 SRCIP -&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. Use as portas de origem como referência para correlacionar com capturas de pacotes e logs do rastreamento de suporte do sistema. Este é o melhor método para encontrar os ps associados. Como visto neste próximo exemplo, os pacotes relacionados mostram como pesquisas PTR (DNS reverso) em vez de consultas DNS normais. É por isso que a consulta de domínio mal-intencionado não pode ser encontrada ao examinar capturas do endereço IP de origem. Esses tipos de `pacotes atingem uma` política de acesso que mostra em um evento, mesmo que a mesma conexão mostre como Bloqueada pela inteligência de segurança.

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

5. Revise os pacotes de resposta para essas pesquisas PTR a partir do destino e o domínio mal-intencionado pode ser visto. Isso aciona o FTD para bloquear a conexão por inteligência de segurança, pois agora ele vê o domínio mal-intencionado.

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

Coordene com a equipe do cliente para investigar se alguma consulta DNS reversa ou padrões de tráfego inesperados são observados para determinados IPs relacionados à ameaça de mineração de criptografia. Para permitir o tráfego específico ou analisá-lo melhor, adicione os IPs necessários à lista Não Bloquear ou permita via pré-filtro, conforme apropriado. Isso pode permitir a inspeção e a visibilidade subsequentes na captura de pacotes.

- Adicione IPs à lista Não bloquear do Security Intelligence se for necessária uma análise mais detalhada.

- A permissão no pré-filtro permite que o tráfego ignore o bloco de Inteligência de Segurança.

Causa

A causa raiz é que a Pesquisa PTR (DNS reverso) passa pelo FTD inicialmente pela regra de acesso, pois ainda está aguardando a inspeção de inteligência de segurança. O pacote de resposta para a pesquisa PTR contém o nome de domínio mal-intencionado. Quando uma resposta PTR corresponde a uma entrada da lista de Bloqueios de Inteligência de Segurança (como associada à ameaça de mineração de criptografia DNS), o pacote é descartado. Como resultado, o domínio mal-intencionado é encontrado apenas na resposta de Pesquisa PTR e os eventos às vezes mostram uma correspondência em uma regra de permissão para acesso e em um Bloqueio para inteligência de segurança.

Conteúdo relacionado

- Guia de configuração de dispositivos do Cisco Secure Firewall Management Center, 7.4: Sobre inteligência de segurança
- Suporte técnico e downloads da Cisco
- ID de bug Cisco CSCwt16755 - DOC: pesquisas PTR passam FTD pela política AC, mas a resposta é bloqueada pela inteligência de segurança

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.