Problemi di visibilità dei pacchetti di ricerca DNS/PTR nelle acquisizioni di pacchetti FTD 7.4

Problema

Quando viene bloccato da funzionalità di intelligence di sicurezza, l'acquisizione pacchetti FTD (Firewall Threat Defense) non visualizza query DNS sui domini dannosi bloccati dall'intelligence di sicurezza FTD. Gli eventi di connessione nell'FTD perimetrale mostrano il traffico proveniente dal server DNS che esegue query sul dominio e confermano che l'FTD sta bloccando queste risposte alle query tramite funzionalità di intelligence di sicurezza. Tuttavia, lo stesso evento mostra anche una corrispondenza in una regola dei criteri di accesso FTD che in genere non è prevista. Il problema è correlato all'interazione tra i pacchetti di ricerca di intelligence di sicurezza e PTR (reverse DNS) nei FTD quando vengono bloccate le query sui domini dannosi. Questo può visualizzare un evento che corrisponde sia a una regola di sicurezza.

Ambiente

- Cisco Secure Firewall Firepower 7.4 (Firepower Management Center (FMC) / cdFMC / FDM) (applicabile a tutti i sistemi che utilizzano l'intelligence di sicurezza)
- Versione del software: 7.4.2 / 7.4.2.4 (applicabile a tutti i sistemi che utilizzano l'intelligence di sicurezza)
- Dispositivo Perimeter Firepower per il monitoraggio del traffico DNS tra il server DNS Infoblox e il cloud CIRA
- Intelligence di sicurezza configurata per bloccare le minacce di data mining di crittografia DNS
- Topologia di laboratorio che coinvolge i dispositivi FPR2110 e FPR2100 per la riproduzione
- Dominio destinazione query DNS: static.vdc.vn
- Classificazione minacce: minaccia di data mining di crittografia DNS
- Eventi di acquisizione e connessione dei pacchetti analizzati sul dispositivo Firepower
- Server DNS Infoblox come infrastruttura DNS interna

Risoluzione

1. Analizzare gli eventi di connessione sull'FTD per confermare che le query DNS dal server DNS al dominio esterno sono bloccate dall'intelligence di sicurezza a causa di un dominio dannoso. Vengono annotati un indirizzo IP di origine e di destinazione specifico e l'evento può persino indicare una corrispondenza in una regola dei criteri di accesso che consente la ricerca PTR iniziale dall'origine alla destinazione. Tuttavia, lo stesso evento mostra anche un blocco dall'intelligence di sicurezza, indicando chiaramente l'URL per la query.

```
Evento connessione
```

Esempio:

Dominio: static.vdc.vn
Azione: Bloccato (minaccia di data mining di crittografia DNS)

2. Avviare l'acquisizione di un pacchetto sull'FTD indirizzato al traffico DNS tra gli indirizzi IP pertinenti. In un'analisi Wireshark delle acquisizioni dall'indirizzo IP di origine, non viene trovata alcuna query DNS specifica per il dominio dannoso nell'output di acquisizione del pacchetto.

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

```
(nessun output per i pacchetti previsti)
```

- In base alla documentazione di Cisco, il filtro della funzionalità di intelligence di sicurezza è una fase iniziale del controllo di accesso. Se un pacchetto corrisponde a un elenco di blocchi della funzionalità di intelligence di sicurezza, può essere eliminato prima di un'ulteriore ispezione e prima di essere elaborato da altri criteri (tra cui il controllo di accesso, l'acquisizione di pacchetti, l'ispezione DNS).
- I filtri di Security Intelligence vengono applicati prima dell'ispezione che richiede un uso intensivo delle risorse.
- I pacchetti bloccati dall'intelligence di sicurezza a volte non vengono acquisiti dai meccanismi standard di acquisizione sul dispositivo.
- Anche le regole di prefiltro valutate prima di Security Intelligence possono influire sulla visibilità.

3. Usare il comando system support url-si-debug nella clip FTD per tracciare le ricerche PTR tra gli IP di origine e di destinazione per capire come e dove il traffico viene elaborato e bloccato all'interno della FTD e annotare le porte di origine per i pacchetti.

```
> supporto del sistema url-si-debug
```

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

4. Utilizzare le porte di origine come riferimento per stabilire una correlazione con le acquisizioni e i registri di pacchetti dalla traccia di supporto del sistema. Questo è il metodo migliore per trovare i pacchetti associati. Come mostrato nell'esempio seguente, i pacchetti correlati vengono visualizzati come ricerche PTR (DNS inverso) anziché come normali query DNS. Per questo motivo non è possibile trovare la query del dominio dannoso quando si esaminano le acquisizioni dall'indirizzo IP di origine. Questi tipi di `pacchetti` hanno `incontrato un criterio di accesso` che viene visualizzato in un evento anche se la stessa connessione risulta bloccata da funzionalità di sicurezza.

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

5. Esaminare i pacchetti di risposta a queste ricerche PTR dalla destinazione e il dominio dannoso può essere visto. Questo attiva l'FTD per bloccare alla fine la connessione da parte dell'intelligence di sicurezza mentre vede ora il dominio dannoso.

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

Coordinarsi con il team del cliente per verificare se sono state osservate query DNS inverse o modelli di traffico imprevisti per determinati indirizzi IP correlati alla minaccia di data mining. Per autorizzare il traffico specifico o analizzarlo ulteriormente, aggiungere gli indirizzi IP richiesti all'elenco degli indirizzi da non bloccare o autorizzare tramite prefiltro, a seconda dei casi. In questo modo è possibile eseguire ispezioni successive e visualizzare i pacchetti acquisiti.

- Se è necessaria un'ulteriore analisi, aggiungere gli indirizzi IP all'elenco degli indirizzi non bloccati per l'intelligence di sicurezza.
- L'autorizzazione nel prefiltro consente al traffico di ignorare il blocco Security Intelligence.

Causa

La causa principale è che la ricerca PTR (DNS inverso) passa attraverso l'FTD inizialmente per regola di accesso, in quanto è ancora in attesa di ispezione della funzionalità di intelligence di sicurezza. Il pacchetto di risposta per la ricerca PTR contiene quindi il nome di dominio dannoso. Quando una risposta PTR corrisponde a una voce dell'elenco di blocco della funzionalità di intelligence di sicurezza (ad esempio associata a una minaccia di data mining della crittografia DNS), il pacchetto viene scartato. Di conseguenza, il dominio dannoso viene trovato solo nella risposta di ricerca PTR e talvolta gli eventi mostrano una corrispondenza sia nella regola Consenti per l'accesso che nel blocco per la funzionalità di intelligence di sicurezza.

Contenuto correlato

- Guida alla configurazione dei dispositivi di Cisco Secure Firewall Management Center, 7.4: Informazioni sulla Security Intelligence
- Supporto tecnico Cisco e download
- ID bug Cisco CSCwt16755 - DOC: le ricerche PTR superano il limite FTD dei criteri AC, ma la risposta viene bloccata dalla Security Intelligence

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).