Probleme mit der Paketsichtbarkeit bei der DNS/PTR-Suche in FTD 7.4-Paketerfassungen

Problem

Wenn die Firewall Threat Defense (FTD)-Paketerfassung durch die Sicherheitsinformationen blockiert wird, zeigt sie keine DNS-Abfragen an die schädlichen Domänen an, die durch die FTD-Sicherheitsinformationen blockiert werden. Verbindungsereignisse auf dem Perimeter FTD zeigen den Datenverkehr vom DNS-Server an, der die Domäne abfragt, und bestätigen, dass die FTD diese Abfrageantworten mithilfe von Sicherheitsinformationen blockiert. Das gleiche Ereignis zeigt jedoch auch eine Übereinstimmung mit einer FTD-Zugriffsrichtlinienregel an, die normalerweise nicht erwartet wird. Sicherheitsinformationen und PTR-Lookup-Pakete (Reverse DNS) interagieren auf FTDs, wenn schädliche Domänenabfragen blockiert werden. Dies kann ein Ereignis anzeigen, das sowohl mit einer Zugriffsregel als auch mit Sicherheitsinformationen übereinstimmt.

Umwelt

- Cisco Secure Firewall Firepower 7.4 (FirePOWER Management Center (FMC) / cdFMC / FDM) (anwendbar auf alle Systeme, die Sicherheitsinformationen nutzen)
- Softwareversion: 7.4.2 / 7.4.2.4 (anwendbar auf alle Systeme, die Sicherheitsinformationen nutzen)
- Perimeter: FirePOWER-Gerät überwacht DNS-Datenverkehr zwischen Infoblox DNS-Server und CIRA Cloud
- Sicherheitsinformationen zur Blockierung von DNS-Crypto-Mining-Bedrohungen
- Labortopologie mit FPR2110- und FPR2100-Geräten zur Wiedergabe
- DNS-Abfrage-Zieldomäne: static.vdc.vn
- Bedrohungsklassifizierung: DNS-Verschlüsselung, um Bedrohungen abzuwehren
- Paketerfassungs- und Verbindungsereignisse, die auf einem FirePOWER-Gerät analysiert werden
- Infoblox DNS Server als interne DNS Infrastruktur

Auflösung

1. Analysieren Sie Verbindungsereignisse auf dem FTD, um zu bestätigen, dass DNS-Abfragen vom DNS-Server an die externe Domäne aufgrund einer schädlichen Domäne von der Sicherheitsintelligenz blockiert werden. Eine bestimmte Quell- und Ziel-IP-Adresse wird erfasst, und das Ereignis kann sogar eine Übereinstimmung mit einer Zugriffsrichtlinienregel angeben, die die anfängliche PTR-Suche von Quelle zu Ziel zulässt. Das gleiche Ereignis zeigt jedoch auch eine Blocked by-Sicherheitsintelligenz mit klarer URL für die Abfrage an.

```
Verbindungsereignis
```

Beispiel:

Domäne: static.vdc.vn
Aktion: Gesperrt (DNS crypto mining-Bedrohung)

2. Initiieren Sie eine Paketerfassung auf der FTD, die auf DNS-Verkehr zwischen den relevanten IP-Adressen abzielt. In einer Wireshark-Analyse der Erfassungen von der ursprünglichen IP-Adresse wird keine DNS-Abfrage speziell für die schädliche Domäne in der Paketerfassungsausgabe gefunden.

```
FTD# capture CAP-Schnittstellenübereinstimmung udp host SRCIP host DESTIP eq 53
```

```
(keine Ausgabe für die erwarteten Pakete)
```

- Laut Cisco-Dokumentation ist die Filterung von Sicherheitsinformationen eine frühe Phase der Zugriffskontrolle. Wenn ein Paket mit einer Liste von Sicherheitsinformationsblöcken übereinstimmt, kann es vor der weiteren Überprüfung und vor der Verarbeitung durch andere Richtlinien (einschließlich Zugriffskontrolle, Paketerfassung, DNS-Überprüfung) verworfen werden.
- Die Sicherheitsinformationsfilterung erfolgt vor der ressourcenintensiven Überprüfung.
- Von Sicherheitsinformationen blockierte Pakete werden manchmal nicht von den standardmäßigen Paketerfassungsmechanismen auf dem Gerät erfasst.
- Vor der Sicherheitsintelligenz ausgewertete Vorfilterregeln können ebenfalls die Transparenz beeinflussen.

3. Verwenden Sie den Befehl system support url-si-debug in der FTD-CLISH, um PTR-Suchvorgänge zwischen Quell- und Ziel-IPs zu verfolgen, um zu verstehen, wie und wo der Datenverkehr innerhalb der FTD verarbeitet und blockiert wird, und notieren Sie die Quell-Ports für die Pakete.

```
> System support url-si-debug
```

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

4. Verwenden Sie die Quell-Ports als Referenz für die Korrelation mit Paketerfassungen und Protokollen von der Systemunterstützungs-Ablaufverfolgung. Dies ist die beste Methode, um die zugehörigen IP-Adressen zu finden. Wie in diesem nächsten Beispiel gezeigt, werden die zugehörigen Pakete als PTR-Abfragen (Reverse DNS) statt normaler DNS-Abfragen angezeigt. Aus diesem Grund kann die schädliche Domänenabfrage nicht gefunden werden, wenn Erfassungen von der ursprünglichen IP-Adresse betrachtet werden. Diese `Pakettypen treffen auf einen Zugriff -Richtlinie`, die bei einem Ereignis auch dann angezeigt wird, wenn die gleiche Verbindung als durch Sicherheitsinformationen blockiert angezeigt wird.

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

5. Überprüfen Sie die Antwortpakete auf diese PTR-Suchvorgänge vom Ziel aus, und die schädliche Domäne kann angezeigt werden. Dies veranlasst die FTD, die Verbindung letztendlich durch die Sicherheitsinformationen zu blockieren, da sie jetzt die schädliche Domäne sieht.

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

Wenden Sie sich an das Kundenteam, um zu untersuchen, ob bei bestimmten IPs im Zusammenhang mit der Crypto Mining-Bedrohung umgekehrte DNS-Abfragen oder unerwartete Datenverkehrsmuster beobachtet werden. Um bestimmten Datenverkehr zuzulassen oder weiter zu analysieren, fügen Sie die erforderlichen IPs der Liste "Nicht blockieren" hinzu, oder lassen Sie sie ggf. über einen Vorfilter zu. Dies ermöglicht eine spätere Überprüfung und Transparenz bei der Paketerfassung.

- Fügen Sie der Liste "Security Intelligence Do-Not-Block" (Sicherheitsinformationen - Nicht blockieren) IP-Adressen hinzu, wenn weitere Analysen erforderlich sind.
- Wenn diese Option im Vorfilter zugelassen wird, kann der Datenverkehr den Block mit den Sicherheitsinformationen umgehen.

Ursache

Die Ursache liegt darin, dass die PTR-Suche (Reverse DNS) die FTD zunächst nach der Zugriffsregel durchläuft, da die Prüfung der Sicherheitsinformationen noch aussteht. Das Antwortpaket für die PTR-Suche enthält dann den schädlichen Domänennamen. Wenn eine PTR-Antwort mit einem Eintrag in der Liste der Sicherheitsinformationsblöcke übereinstimmt (z. B. mit der DNS-Krypto-Mining-Bedrohung verknüpft), wird das Paket verworfen. Die schädliche Domäne wird daher nur in der Antwort der PTR-Suche gefunden und zuweilen eine Übereinstimmung sowohl mit einer Zulassungsregel als auch mit einer Blockierungsregel für Sicherheitsinformationen anzeigen.

Verwandte Inhalte

- Cisco Secure Firewall Management Center Device Configuration Guide, 7.4: About Security Intelligence
- Technischer Support und Downloads von Cisco
- Cisco Bug-ID CSCwt16755 - DOC: PTR-Suchläufe passieren FTD durch AC-Richtlinie, aber die Antwort wird durch Sicherheitsinformationen blockiert

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.