FTD 7.4 패킷 캡처의 DNS/PTR 조회 패킷 가시성 문제

문제

보안 인텔리전스에 의해 차단되는 경우 FTD(방화벽 위협 방어) 패킷 캡처는 FTD 보안 인텔리전스에 의해 차단되는 악의적인 도메인에 대한 DNS 쿼리를 표시하지 않습니다. 경계 FTD의 연결 이벤트는 도메인을 쿼리하는 DNS 서버의 트래픽을 표시하고 FTD가 보안 인텔리전스를 통해 이러한 쿼리 응답을 차단하는지 확인합니다. 그러나 동일한 이벤트는 일반적으로 예상하지 않는 FTD 액세스 정책 규칙에 대한 일치 항목도 표시합니다. 이 문제는 악의적인 도메인 쿼리를 차단할 때 FTD에서 보안 인텔리전스 및 PTR(역방향 DNS) 조회 패킷이 상호 작용하는 방식과 관련된 것으로 나타납니다. 이는 액세스 규칙 및 보안 인텔리전스와 일치하는 이벤트를 나타낼 수 있습니다.

환경

- Cisco Secure Firewall Firepower 7.4(FMC(Firepower 관리 센터) / cdFMC / FDM)(보안 인텔리전스를 사용하는 모든 시스템에 적용 가능)
- 소프트웨어 버전: 7.4.2 / 7.4.2.4(보안 인텔리전스를 사용하는 모든 시스템에 적용 가능)
- Infoblox DNS 서버와 CIRA 클라우드 간의 DNS 트래픽을 모니터링하는 경계 Firepower 디바이스
- DNS 암호화 마이닝 위협을 차단하도록 구성된 보안 인텔리전스
- FPR2110 및 FPR2100 디바이스가 포함된 랩 토폴로지
- DNS 쿼리 대상 도메인: static.vdc.vn
- 위협 분류: DNS 암호화 마이닝 위협
- firepower 디바이스에서 분석된 패킷 캡처 및 연결 이벤트
- Infoblox DNS 서버를 내부 DNS 인프라로 사용

해결

1. FTD의 연결 이벤트를 분석하여 DNS 서버에서 외부 도메인으로의 DNS 쿼리가 악의적인 도메인으로 인해 보안 인텔리전스에 의해 차단되고 있는지 확인합니다. 특정 소스 및 대상 IP 주소가 기록되며, 이 이벤트는 소스에서 대상으로의 초기 PTR 조회를 허용하는 액세스 정책 규칙과 일치하는

항목을 나타낼 수도 있습니다. 그러나 동일한 이벤트에서는 쿼리의 URL을 명확히 표시하면서 보안 인텔리전스에 의해 차단됨을 보여 줍니다.

연결 이벤트

예:

도메인: static.vdc.vn
작업: 차단됨(DNS 암호화 마이닝 위협)

2. 관련 IP 주소 간의 DNS 트래픽을 대상으로 하는 FTD에서 패킷 캡처를 시작합니다. 원본 IP 주소에서의 캡처를 분석한 Wireshark에서는 패킷 캡처 출력의 악성 도메인에 대한 DNS 쿼리를 찾을 수 없습니다.

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

(예상 패킷에 대한 출력 없음)

- Cisco 설명서에 따르면 보안 인텔리전스 필터링은 액세스 제어의 초기 단계입니다. 패킷이 보안 인텔리전스 블록 목록과 일치하는 경우 추가 검사 전에 삭제되고 다른 정책(액세스 제어, 패킷 캡처, DNS 검사 포함)에 의해 처리되기 전에 삭제될 수 있습니다.
- 보안 인텔리전스 필터링은 리소스 집약적인 검사 전에 발생합니다.
- 보안 인텔리전스에 의해 차단된 패킷은 때때로 디바이스의 표준 패킷 캡처 메커니즘에 의해 캡처되지 않습니다.
- 보안 인텔리전스가 가시성에 영향을 미치기 전에 평가된 사전 필터 규칙도 있습니다.

3. FTD 내에서 트래픽이 처리 및 차단되는 방법과 위치를 이해하고 패킷의 소스 포트를 메모하려면 FTD CLISH에서 system support url-si-debug 명령을 사용하여 소스 IP와 대상 IP 간의 PTR 조회를 추적합니다.

```
> 시스템 지원 url-si-debug
```

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

4. 소스 포트를 참조로 사용하여 시스템 지원 추적의 패킷 캡처 및 로그와 상관관계를 파악합니다. 이 방법은 연결된 PS를 찾는 가장 좋은 방법입니다. 다음 예에서 볼 수 있듯이, 관련 패킷은 일반 DNS 쿼리 대신 PTR(역방향 DNS) 조회로 표시됩니다. 원본 IP 주소에서 캡처를 볼 때 악의적인 도메인 쿼리를 찾을 수 없는 이유입니다. 이러한 패킷 유형은 동일한 연결이 보안 인텔리전스에 의해 차단됨으로 표시되더라도 이벤트에 표시되는 액세스 정책에 충돌합니다.

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

5. 대상에서 이러한 PTR 조회에 대한 응답 패킷을 검토하면 악성 도메인을 확인할 수 있습니다. 그러면 FTD가 보안 인텔리전스에 의해 연결을 차단하도록 트리거됩니다. 이제 악성 도메인을 확인할 수 있습니다.

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

고객 팀과 협력하여 암호화 마이닝 위협과 관련된 지정된 IP에 대해 역방향 DNS 쿼리 또는 예기치 않은 트래픽 패턴이 관찰되었는지 조사합니다. 특정 트래픽을 허용하거나 더 자세히 분석하려면 필요한 IP를 차단 안 함 목록에 추가하거나 사전 필터를 통해 적절히 허용하십시오. 이렇게 하면 패킷 캡처에서 후속 검사 및 가시성이 허용됩니다.

- 추가 분석이 필요한 경우 Security Intelligence Do-Not-Block 목록에 IP를 추가합니다.
- 프리필터에서 허용하면 트래픽이 보안 인텔리전스 블록을 우회할 수 있습니다.

원인

근본 원인은 PTR(역방향 DNS) 조회가 여전히 보안 인텔리전스 검사 보류 중이므로 액세스 규칙에 의해 FTD를 초기에 통과하기 때문입니다. PTR 조회에 대한 응답 패킷에는 악의적인 도메인 이름이 포함됩니다. PTR 응답이 DNS 암호화 마이닝 위협과 연결된 보안 인텔리전스 블록 목록 항목과 일치하면 패킷이 삭제됩니다. 따라서 악의적인 도메인은 PTR 조회 응답에서만 발견되며 이벤트는 액세스 허용 규칙과 보안 인텔리전스에 대한 차단 모두에서 일치하는 결과를 표시하기도 합니다.

관련 콘텐츠

- Cisco Secure Firewall Management Center Device Configuration Guide, 7.4: About Security Intelligence
- Cisco 기술 지원 및 다운로드
- Cisco 버그 ID CSCwt16755 - DOC: PTR 조회가 AC 정책에 의해 FTD를 통과하지만, 보안 인텔리전스에 의해 응답이 차단됨

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.