# Verständnis von Snort 3: Stateful Signature Evaluation Byte_Jump

## Inhalt



## Einleitung

In diesem Dokument werden die neuen Techniken beschrieben, die in Snort 3 ab Version 7.4 hinzugefügt wurden.

## Hintergrundinformationen

- Das Erkennungsmodul von Snort 3 arbeitet im Blockmodus. Dieser Ansatz bietet zwar einen Leistungsvorteil und eine (relativ) einfache Implementierung, hat jedoch einige Einschränkungen bei der Erkennung von Signaturen, die sich über mehrere Datenblöcke erstrecken.
- Um die Benutzerfreundlichkeit zu verbessern, wurden in Snort bereits einige Verbesserungen implementiert:
  1. Flowbits ermöglichen es dem Regelschreiber, den Netzwerkfluss mit einer benutzerdefinierten Eigenschaft zu markieren. Diese Eigenschaft kann für jedes Paket aus dem Fluss festgelegt, gelöscht und getestet werden (dies ist eine Möglichkeit, auf eine größere Signatur über Pakete zu schließen).
- Ein Stream-Modul sammelt Wire-Pakete in einem neu erstellten Paket, das ein größerer und

aussagekräftigerer Block ist als ein unformatiertes Paket. Die Auswertung von IPS-Regeln mit dem neu erstellten Paket bietet mehr Chancen, das gesamte Bild zu sehen und einem größeren Muster (der Signatur) zuzuordnen.
- In einigen Fällen stellt das neu aufgebaute Paket nicht nur neue Daten dar, sondern umfasst auch einen Teil der bereits durch die Erkennung verarbeiteten früheren Daten; auch dieser Block akkumulierter Daten ermöglicht es, Signaturen zu erkennen, die sich (bis zu einem gewissen Grad) rückwärts im Fluss erstrecken.
- Ein Stream-Splitter unterteilt den Fluss in Blöcke, aber der Cut-Point ist möglicherweise ein Schwachpunkt, den der Angreifer nutzen könnte, um die Erkennung von Mustern zu vermeiden. Daher verfügt Snort über einen Jitter-Mechanismus, der die Aufteilung unvorhersehbarer macht. Dies macht die Analyse für den Angreifer noch komplizierter.

# Neuerungen

Die Stateful-Signatur-Bewertung ist eine neue Technik, die der Liste hinzugefügt werden kann. Es erweitert die Erkennungsfunktionen, indem es die IPS-Regelauswertung über mehrere Blöcke hinweg ermöglicht. Eine Regel stimmt daher nicht sofort falsch überein, wenn der aktuelle Block keine Daten enthält, sondern wartet stattdessen darauf, dass weitere Daten eingehen.

# Unterstützte Plattformen

## Software- und Hardware-Mindestanforderungen

| Min. unterstützte Manager-Version | Verwaltete Geräte | Min. unterstützte Version des verwalteten Geräts erforderlich | Hinweise |
|---|---|---|---|
| Management Center 7.4.0 | FTD | 7.4.0 | Nur Snort 3 |
| Geräte-Manager 7.4.0 | Alle FTD, die das FDM-Management unterstützen | 7.4.0 | Nur Snort 3 |

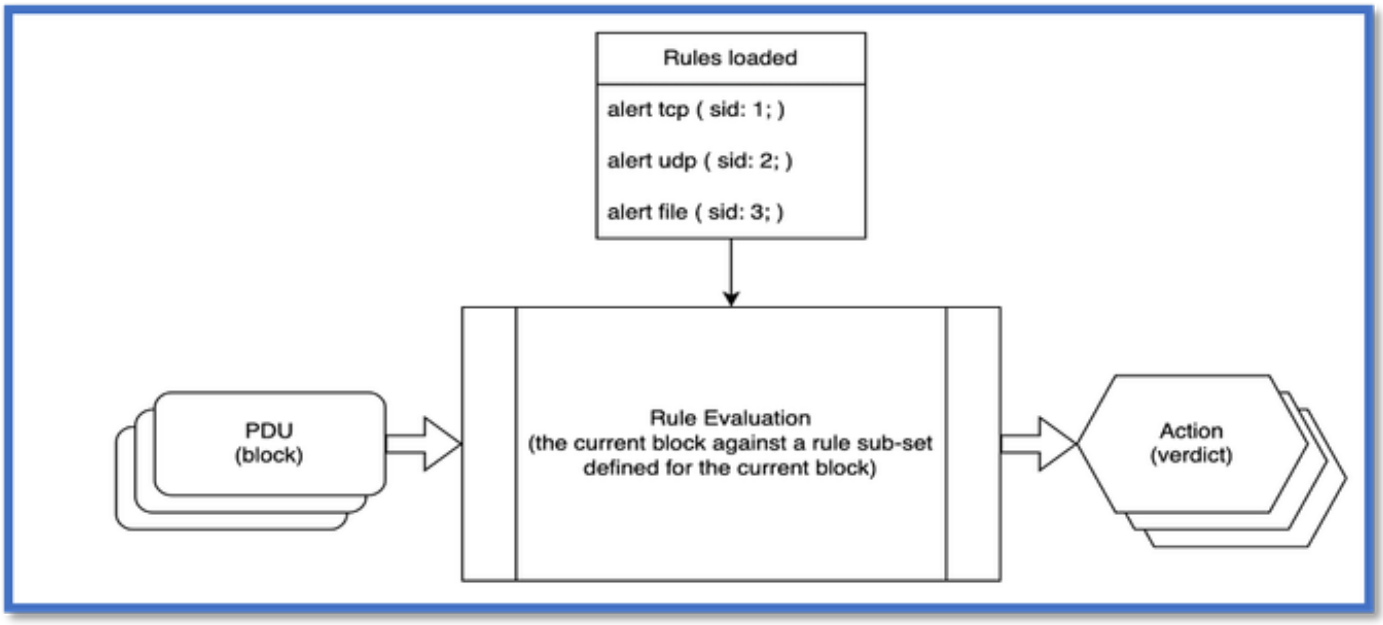
# Funktionsdetails

## Beschreibung der Funktionsmerkmale

Wie funktioniert es?

Der Erkennungsmodul-Workflow ist im Diagramm dargestellt. In der

Datenverkehrsverarbeitungsstufe sind bereits alle Regeln geladen, und das Modul akzeptiert Datenblöcke einzeln, wertet Regeln aus und definiert die Aktionen, die für den Prozess-Stateful-Signatur-Bewertungsblock ausgeführt werden sollen.




Hinweise zur Regelung:

1. Nachdem eine Regeluntermenge für den aktuellen Datenblock definiert wurde, wird jede Regel aus diesem Datenblock unabhängig von anderen Regeln ausgewertet.
2. Jeder Datenblock wird unabhängig von anderen Blöcken ausgewertet.
3. Der Datenblock ist eine Abstraktion für einen Satz von IPS-Puffern, die für das aktuelle Paket ausgewertet werden.
4. Aktion ist eine Liste von Aktionen, die für das aktuelle Paket ausgewertet werden; das endgültige Urteil wird später bestimmt.

Um zu verstehen, wie die Stateful-Signaturauswertung funktioniert, sehen Sie sich an, wie eine gemeinsame IPS-Regel ausgewertet wird und wie Datenblöcke einen Stream bilden können.

Gemeinsame Regelauswertung

Eine IPS-Regel kann in folgender Form dargestellt werden:

```
action protocol source → destination ( option_1: parameters; option_2: parameters;
option_3: parameters; gid: 1; sid: 1; meta_option_1; meta_option_2; meta_option_3; )
```

Dabei gilt:

Aktion - IPS-Aktion auf dem Paket, wenn die Regel ausgelöst wird

Protokoll - Übereinstimmendes Protokoll

Quelle, Ziel - IP-Adresse und Port

option_1, option_2, option_3 - IPS-Optionen, die Teil der Regelauswertung sind

gid, sid - ein eindeutiges Paar, das die Regel identifiziert (sie sind wie Metadatenoptionen)

meta_option_1, meta_option_2, meta_option3 - Regelmetadaten wie eine Nachricht, ein Klassentyp oder ein Verweis, diese Optionen sind nicht an der Regelauswertung beteiligt.

- Protokoll, Quelle und Ziel bilden einen Regelheader. Er fungiert als Filter für einen Netzwerkfluss (der zur Evaluierung akzeptiert werden muss). Alles in Klammern ist ein Regelkörper. IPS-Optionen (außer Regelmetadaten) aus dem Regelkörper sind diejenigen, die für den Datenblock ausgewertet werden. Sie erfüllen die folgenden Aussagen:
- -Optionen werden nur in der Reihenfolge von links nach rechts bewertet.
    1. kann einer von zwei Haupttypen sein.
    2. buffer setter, wählt die Option den IPS-Puffer für das aktuelle Paket.
- Andere (Mustersuche, Mathematikoperation, Cursormanipulation, Flussbitoperation)
- Ein Cursor wird verwendet, um die Position im ausgewählten IPS-Puffer zu verfolgen.

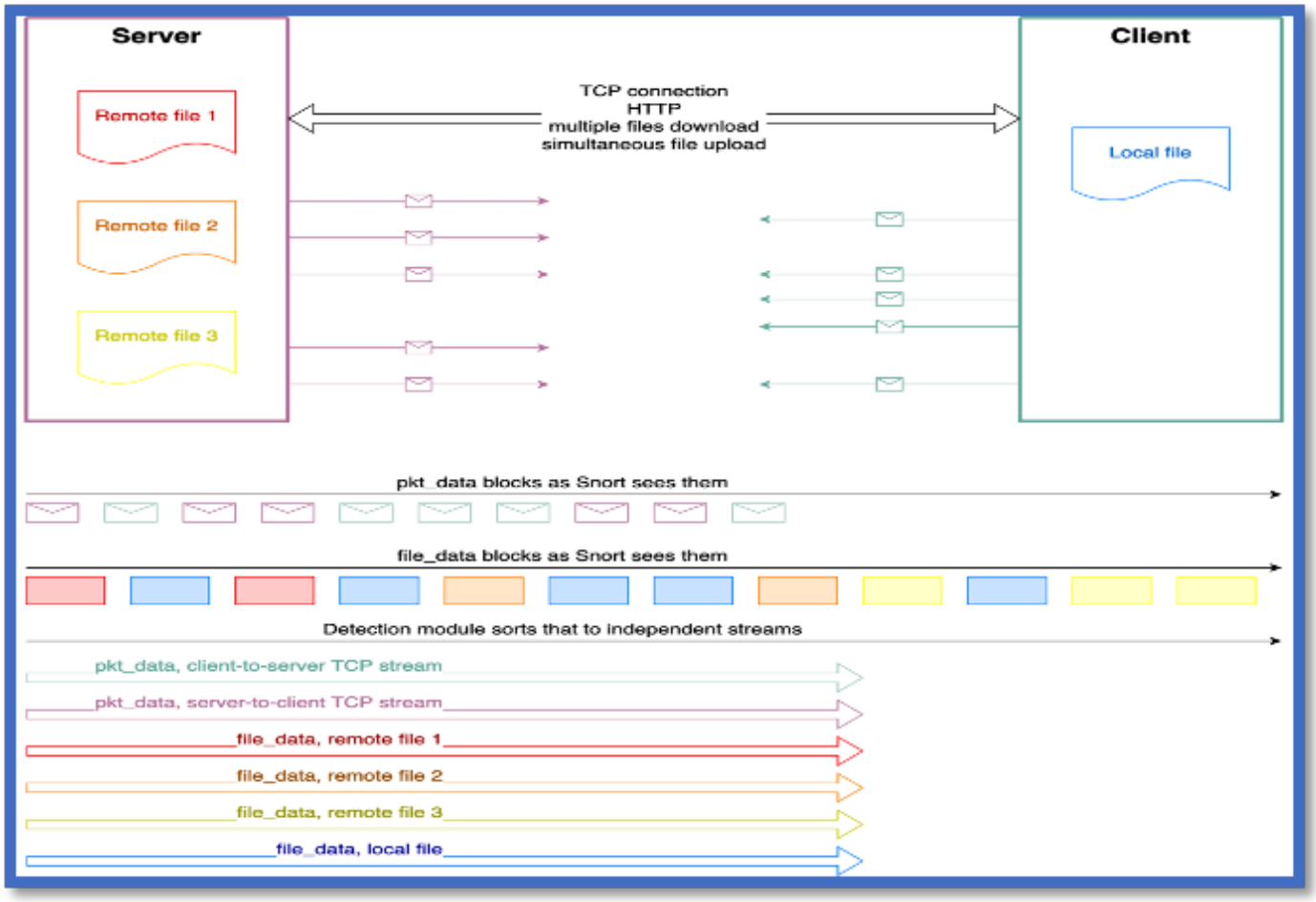
- Eine Option kann entweder:
    1. 'absolut', d. h. es ist nicht von der Cursorposition abhängig
    2. 'relativ', d. h. es beginnt seine Auswertung von der Cursorposition
- Wenn eine Option versucht, den Cursor aus dem ausgewählten IPS-Puffer zu setzen, schlägt sie fehl, und die gesamte Regel stimmt nicht überein (aufgrund fehlender Daten).
- Der letzte Punkt ist eine Einschränkung des Erkennungsmoduls. Wenn Snort über unbegrenzte Ressourcen verfügen könnte, würde es alle erkannten Daten zwischenspeichern, um Regeln immer wieder auszuwerten, wenn Daten verfügbar werden (mehr Wire-Pakete kommen an).

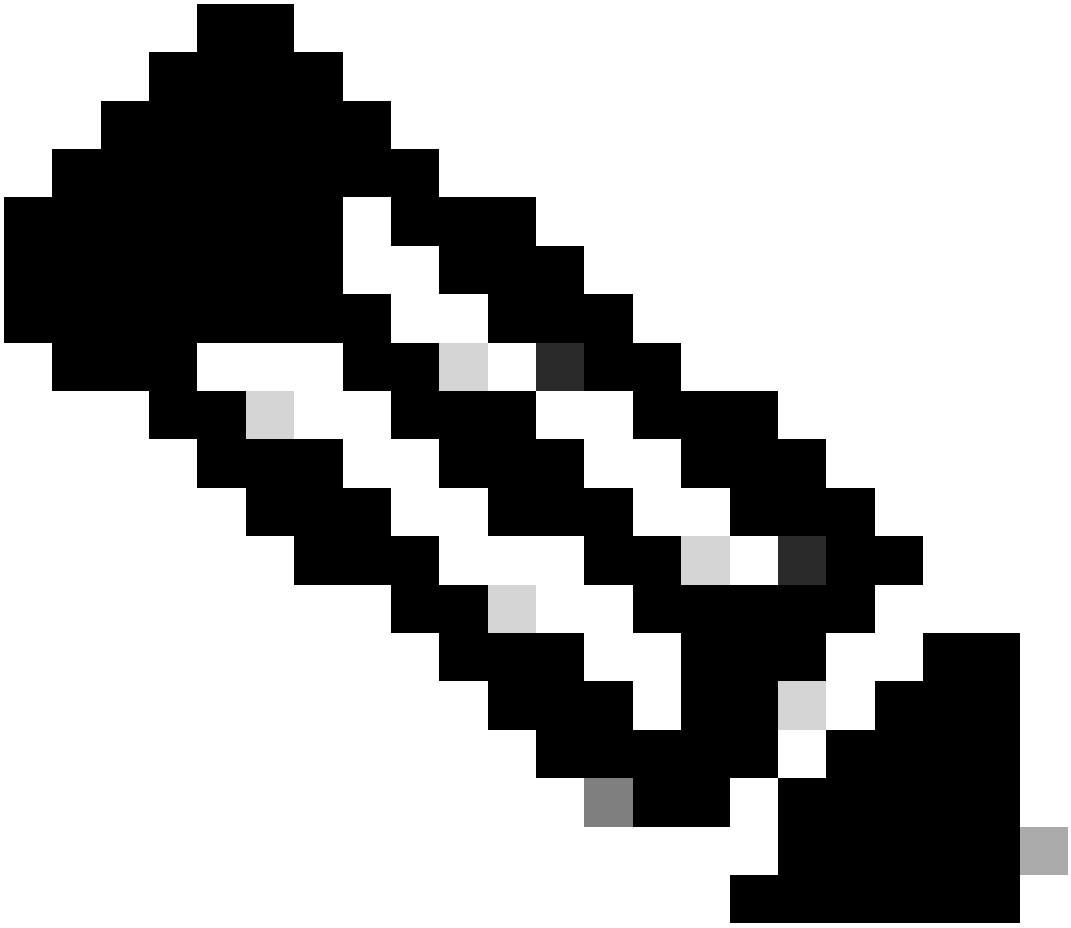
# Datenstrom- und IPS-Puffer

- Der Datenstrom ist ein Bytestrom in einer zusammenhängenden Form von derselben Quelle. Es handelt sich um ein neues Konzept zur Unterstützung der zustandsbehafteten Evaluierung. Die Regelauswertung zwischen Blöcken muss innerhalb derselben logischen Daten erfolgen (ob es sich um eine Datei, einen reinen TCP-Stream oder JavaScript-Text handelt).

- Im Allgemeinen könnte ein vom Erkennungsmodul empfangener Datenblock:
    - stammen aus einem anderen IPS-Puffer (z. B. sind pkt_data und file_data nicht identisch).
    - Zu einem anderen Datenstrom gehören
    - Kein Stream (Puffer, die aus einem Rohpaket generiert werden)
    - Kein zusammenhängender Stream (ICMP, UDP)
    - Nicht in der richtigen Reihenfolge (HTTP Partial Response)
    - Enthalten wiederholte Daten (ein akkumulierter Block, wie in http_inspect.script_detection oder HTTP Chunked Response)
- Das Erkennungsmodul kann nur nach bestimmten Elementen sortieren, um Blöcke aus

demselben Datenstrom zu verketten. Andernfalls würde der Auswertungsprozess unerwünschte Interferenzen durch verschachtelte Blöcke erkennen.





Hinweis: Das Beispiel hier zeigt einen Fall, in dem ein HTTP-Client mehrere Dateien gleichzeitig hoch- und herunterlädt.

- Derzeit können nur zwei IPS-Puffer einen Stream darstellen: pkt_data und file_data, wobei:
  1. pkt_data aus zwei Streams für TCP-Protokoll (Client-zu-Server- und Server-zu-Client-Richtung)
  2. file_data muss Streams für Dateien, MIME-Anhänge und andere Protokolldaten bilden (z. B. HTTP-HTML-Seite und/oder anderer Content-Type).
- Die Stateful-Evaluierung erfolgt ausschließlich innerhalb des Datenstroms.

## Fortsetzung der Regel

- Der Abschnitt endet früher mit einer Anweisung, dass die IPS-Option nicht übereinstimmt, wenn der Cursor aus dem aktuellen IPS-Puffer gesetzt wird. Wenn der IPS-Puffer jedoch einen Datenstrom bildet, greift die Funktion zur Auswertung der Stateful-Signatur ein und speichert den Regelbewertungskontext im Snort-Flow-Objekt. Der gespeicherte Evaluierungskontext (Zustand) wird als Regelfortsetzung bezeichnet. Die Bewertung der

zustandsbehafteten Signatur verschiebt das endgültige Urteil der Regel, bis weitere Daten verfügbar sind.

- Die Fortsetzung der Regel besteht aus drei Hauptteilen: dem Namen des IPS-Puffers, der Pufferquelle und der Zielcursor-Position (die Pufferquelle ist eine eindeutige Kennung für den Datenstrom).
- Wenn ein Datenblock vom Erkennungsmodul verarbeitet wird, finden die folgenden Aktionen statt:-
    - Die Stateful-Signaturauswertung erstellt eine Regelfortsetzung und fügt sie an den Fluss an, wenn:
        - IPS-Option (byte_jump, content, pcre oder irgendetwas anderes, das die Cursorposition aktualisiert) setzt den Cursor hinter den aktuellen IPS-Puffer
        - Der aktuelle IPS-Puffer unterstützt den Datenstrom.
        - Der aktuelle IPS-Puffer bildet gerade einen Datenstrom.
- Die Stateful-Signaturauswertung zieht die gerade erstellte Regelfortsetzung zurück und entfernt sie aus dem Fluss, wenn:
    - Die IPS-Regel wurde für den aktuellen Datenblock ausgelöst (die Regel stimmt mit anderen Stellen des Blocks überein)
- Die Stateful-Signaturauswertung lehnt ausstehende Regelfortführungen ab und entfernt sie aus dem Fluss, wenn:
    - Der IPS-Puffer bildet keinen zusammenhängenden Datenstrom (die Blöcke enthalten z. B. wiederholte Daten, oder es besteht eine Lücke (ein Teil der Daten wurde verpasst, oder der Block ist nicht in der richtigen Reihenfolge).
- Die Stateful-Signaturauswertung aktualisiert die gewünschte Cursorposition und stellt neue Daten bereit, wenn:
    - Die Pufferquelle aus der Regelfortsetzung entspricht der ausgewählten Pufferquelle
    - IPS-Puffer bildet einen zusammenhängenden Stream
- Die Stateful-Signaturauswertung sendet die Regelfortsetzung an das IPS-Regel-Modul zurück, wenn:
    1. Die Cursorposition zeigt auf den ausgewählten IPS-Puffer (d. h., der Puffer erhielt schließlich alle Daten, die für die Regelauswertung erforderlich waren).

## Benutzerkonfigurationen

- Da Regelkontinuitäten Speicher benötigen, kann Snort nicht eine unbegrenzte Anzahl von ihnen speichern. Es gibt eine Konfigurationsoption, um den Grenzwert zu steuern:
    1. Detection.max_continuations_per_flow = 1024: maximale Anzahl von Fortsetzungen, die gleichzeitig im Flow gespeichert werden { 0:65535 }
- Wenn die Stateful-Signaturauswertung den Grenzwert erreicht, wird die älteste Fortsetzung der Regel durch eine neue ersetzt.
- Die älteste Regelfortsetzung, die sich auf dem Fluss befindet, ist zu lange vorhanden, d. h., sie erfüllt immer noch nicht die Bedingung, die Regelauswertung fortzusetzen.
- Darüber hinaus gibt es zahlreiche Möglichkeiten zur Feinabstimmung der IPS-Regeln (die im Vordergrund stehen müssen) und der (ggf. erforderlichen) Grenzwerte:
    1. detection.cont_creations: Gesamtzahl der erstellten Fortsetzungen (Summe)
    2. detection.cont_calls: Gesamtzahl der zurückgerufenen Fortsetzungen (Summe)
    3. detection.cont_flows: Gesamtzahl der Flüsse, die Fortsetzung verwenden (Summe)

4. detection.cont_evals: Gesamtzahl der Condition-Metal-Fortsetzungen (Summe)
5. detection.cont_match: Gesamtzahl der abgeglichenen Fortsetzungen (Summe)
6. detection.cont_mismatch: Gesamtzahl der nicht übereinstimmenden Fortsetzungen (Summe)
7. detection.cont_max_num: Höchstzahl gleichzeitiger Kontinuitäten pro Fluss (max)
8. detection.cont_match_spacing: Gesamtzahl der Bytes, die von übereinstimmenden Fortsetzungen übersprungen wurden (Summe)
9. detection.cont_mismatch_spacing: Gesamtzahl der Bytes, die von falsch übereinstimmenden Fortsetzungen übersprungen wurden (Summe)

# Fehlerbehebung

Die Funktion stellt eine Erweiterung des vorhandenen Erkennungsprozesses dar und kann daher nicht explizit behoben werden. Bei Fehlern in der Erkennung müssen Regeln, Konfigurationen oder Datenverkehr überprüft werden.

# Beispielproblem

## Problem: Beschreibung

- Nehmen wir an, eine Signatur muss gleichzeitig den Anfang der Datei und ihren Schwanz überprüfen.
- Beispielsweise müssen wir in einer Zieldatei dieser Struktur (Header, Body, Metadaten) sehen, ob eine der Metadaten einen Wert von 0 hat.

- Dateibytes: e1 f3 22 03 7f ff xx xx ... xx 01 00 02 00 wobei

    - e1 f3 22 03 - 4 Bytes für magische Zahl, die den Dateityp identifiziert
    - 7f ff - 2 Byte für Körpergröße
    - xx xx ... xx - 32 KB an Daten
    - 01 00 02 00 - 4 Byte Metadaten im Tag-Wert-Format (jeweils 1 Byte)
- IPS-Regel würde wie folgt aussehen: Warnungsdatei ( Datei_Daten; Inhalt:"|e1f32203|",fast_pattern; byte_jump:2,0,relative; Inhalt:"00",innerhalb:4, relativ; Sid: 1; )

    - Dabei gilt

        - Das Dateiprotokoll stellt sicher, dass die Regel nur neu erstellte Pakete akzeptiert (unformatierte Pakete werden nicht für die Stateful-Signatur-Bewertung verwendet).
        - Die Option "file_data" wählt einen Dateidatenpuffer aus, der einen Stream bilden kann.
        - Die erste Inhaltsoption ist ein schnelles Muster, das nach der magischen Zahl sucht (wenn dies der beabsichtigte Dateityp ist).
        - byte_jump liest die Größe des Dateikörpers und springt über den Dateikörper
        - Die zweite Inhaltsoption führt die abschließende Überprüfung auf

Metadatenwerte durch. Der Parameter begrenzt die Suchtiefe und macht die Option relativ.

### Problem: Lösung

Die Regel würde wie folgt evaluiert:

Auf dem 1. Paket (Größe 8 kB), das einen Datei-Header und einen Teil des Hauptteils enthält:

1. IPS-Pufferdatei_daten ist ausgewählt. Der Cursor zeigt auf das 0. Byte e1.
2. Die schnelle Musteroption passt die Cursorposition direkt nach der magischen Zahl an und zeigt auf das Byte 7f.
3. Die byte_jump-Option liest zwei Byte des Dateikörpers. Der Cursor wird um diese beiden Bytes aktualisiert. Dann berechnet byte_jump einen Sprung für mehr als 32768 Bytes.
4. Bei der Stateful-Signaturauswertung wird eine Regelfortsetzung erstellt, bei der 24578 Byte mehr benötigt werden ( 32768 - (8 kB - 4 Byte Header - 2 Byte Körpergröße)).
5. Die gesamte Regel stimmt nicht überein, da die Option byte_jump die Cursorposition nicht so weit setzt.

Auf dem zweiten Paket (mit einer Größe von 16 kB), das den Dateitext enthält:

1. Die Stateful-Signatur-Bewertung erkennt die Fortsetzung der ausstehenden Regel.
2. Er wählt den Puffer anhand seines Namens aus und erkennt, dass file_data verfügbar ist und die neue Datengröße 16384 ist.
3. Der aktualisierte Cursor zeigt, dass 8194 Bytes noch benötigt werden ( 24578 - 16384 )
4. Die Regel wird nicht fortgesetzt.

Auf dem 3. Paket (mit 8198 Größen), das den Dateitext und Metadaten enthält:

1. Die Stateful-Signatur-Bewertung erkennt die Fortsetzung der ausstehenden Regel.
2. Es wählt den Puffer anhand seines Namens aus und erkennt, dass file_data verfügbar ist und die neue Datengröße 8198 ist.
3. Der aktualisierte Cursor zeigt an, dass der Puffer genügend Daten hat, die Cursorposition ist 8194.
4. Die Stateful-Signatur-Bewertung löscht die Regelfortsetzung.
5. Die Stateful-Signatur-Auswertung setzt die Regelauswertung der 2. Inhaltsoption fort, wobei der Cursor auf Byte 01 zeigt.
6. Die Inhaltsoption findet eine Übereinstimmung im 2. durchsuchten Byte.
7. Die ganze Regel wird endlich ausgelöst.

## Einzelheiten zu Einschränkungen und häufige Probleme

### Einschränkungen und andere Überlegungen

- Aufgrund der Stateful-Signaturauswertung verwirft Snort alle ausstehenden Regelfortführungen, wenn die Konfiguration neu geladen wird. Beachten Sie, dass die Regelkontinuitäten trotz des Löschens immer noch den Snort-Speicher belegen, bis der

nächste Datenblock an das Erkennungsmodul gesendet wird.
- Die Regellatenzfunktion für die IPS-Regel in der Stateful-Evaluierung verhält sich genauso wie bei einer allgemeinen Regelbewertung. Die Auswertezeit für Regelteile auf verschiedenen Datenblöcken wird zusammengefasst. Wenn die Zeit den Grenzwert überschreitet, führt die Regelauswertung einen Kurzschluss aus und beendet sie früher.
- Flowbits-Operationen behalten ihre Bedeutung bei, obwohl sie immer noch wie 'statische' Optionen funktionieren.
  Innerhalb eines aktuell bekannten Kontexts wird ein Flussbit-Set/Clear/Test-Vorgang durchgeführt. Wenn die flowbit-Option also in einer Regelfortsetzung ausgewertet wird, würde sie die aktuelle Umgebung (festgelegte flowbits) berücksichtigen und nicht die Umgebung, in der die Regel mit der Auswertung begonnen hat.

Außerdem muss ein Regelschreiber auf die schnelle Musterposition achten.

Auch wenn es sich um einen beliebigen Teil der Regel handeln kann, wird die Option für das schnelle Muster vor der gesamten Regel ausgewertet. Dies löst eine Regelauswertung aus. Für eine auf der Stateful-Signaturauswertung basierende Regel bedeutet dies, dass der Fortsetzungspunkt der Regel nach der Option für das schnelle Muster liegen muss.
Darüber hinaus kann die Auswertung der IPS-Regel mehrere Regelkontinuitäten umfassen (eine nach der anderen, nicht zur gleichen Zeit). Da jede Option aus dem Regelkörper fortgesetzt werden kann, kann der Regel-Writer zusätzliche Prüfungen an verschiedenen Stellen des Datenstroms mit derselben IPS-Regel durchführen.

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.