Verwendung von netzwerkbasierter Anwendungserkennung und ACLs zur Blockierung des "Code Red"-Wurms

Inhalt

Einführung

Dieses Dokument enthält eine Methode zur Blockierung des "Code Red"-Wurms an den Netzwerkeingangspunkten durch Network-Based Application Recognition (NBAR) und Access Control Lists (ACLs) in der Cisco IOS® Software auf Cisco Routern. Diese Projektmappe sollte zusammen mit den empfohlenen Patches für IIS-Server von Microsoft verwendet werden.

Hinweis: Diese Methode funktioniert nicht auf Cisco Routern der Serie 1600.

Hinweis: Ein Teil des P2P-Datenverkehrs kann aufgrund der Art seines P2P-Protokolls nicht vollständig blockiert werden. Diese P2P-Protokolle ändern dynamisch ihre Signaturen, um DPI-Engines zu umgehen, die versuchen, ihren Datenverkehr vollständig zu blockieren. Daher wird empfohlen, die Bandbreite zu begrenzen, anstatt sie vollständig zu blockieren. Die Bandbreite für diesen Datenverkehr wird reduziert. Bieten Sie viel weniger Bandbreite. Lassen Sie die Verbindung jedoch bestehen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Quality of Service (QoS)-Dienstrichtlinien unter Verwendung der Befehle der modularen QoS-Befehlszeilenschnittstelle (CLI).
- NBAR
- ACLs
- Richtlinienbasiertes Routing

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt. Die Konfiguration in diesem Dokument wurde auf dem Cisco 3640 getestet, auf dem Cisco IOS 12.2(24a) ausgeführt wird.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Blockieren des "Code Red"-Wurms

Als Erstes sollten Sie gegen "Code Red" vorgehen, indem Sie den Patch anwenden, der von Microsoft erhältlich ist (siehe Links in Abschnitt Methode A: Verwenden Sie eine ACL unten). Dies schützt anfällige Systeme und entfernt den Wurm von einem infizierten System. Wenn der Patch jedoch nur auf Ihre Server angewendet wird, verhindert er, dass der Wurm die Server infiziert, und hält die HTTP GET-Anfragen nicht davon ab, auf die Server zuzugreifen. Es besteht noch die Möglichkeit, dass der Server mit einer Flut von Infektionsversuchen bombardiert wird.

Die in diesem Ratgeber beschriebene Lösung wurde in Zusammenarbeit mit dem Microsoft-Patch entwickelt, um die HTTP GET-Anfragen mit Code Red an einem Netzwerkeingang zu blockieren.

Diese Lösung versucht, die Infektion zu blockieren, löst jedoch keine Probleme, die durch das Erstellen einer großen Anzahl von Cache-Einträgen, Adjacencies und NAT/PAT-Einträgen verursacht werden, da der einzige Weg zur Analyse des Inhalts der HTTP GET-Anforderung darin besteht, eine TCP-Verbindung herzustellen. Das folgende Verfahren hilft nicht, sich vor einer Prüfung des Netzwerks zu schützen. Sie schützt jedoch eine Site vor dem Befall durch ein externes Netzwerk oder reduziert die Anzahl der Infektionsversuche, die ein Computer ausführen muss. In Kombination mit der Filterung eingehender Anrufe verhindert die Filterung ausgehender Anrufe, dass infizierte Clients den "Code Red"-Wurm in das globale Internet verbreiten.

Unterstützte Plattformen

Für die in diesem Dokument beschriebene Lösung ist die klassenbasierte Markierungsfunktion der Cisco IOS-Software erforderlich. Insbesondere die Möglichkeit, einen beliebigen Teil einer HTTP-

URL abzugleichen, verwendet die HTTP-Subport-Klassifizierungsfunktion in NBAR. Die unterstützten Plattformen und die Mindestanforderungen für die Cisco IOS-Software werden nachfolgend zusammengefasst:

Plattform	Cisco IOS-Software mindestens
7200	12,1(5)T
7100	12,1(5)T
3745	12,2(8)T
3725	12,2(8)T
3660	12,1(5)T
3640	12,1(5)T
3620	12,1(5)T
2600	12,1(5)T
1700	12,2(2)T

Hinweis: Sie müssen Cisco Express Forwarding (CEF) aktivieren, um NBAR verwenden zu können.

Klassenbasierte Kennzeichnung und Distributed NBAR (DNBAR) sind auch auf den folgenden Plattformen verfügbar:

Plattform	Cisco IOS-Software mindestens
7500	12,1(6)E
FlexWAN	12,1(6)E

Erkennen des Infektionsversuchs in den IIS-Webprotokollen

Der erste Infektionsversuch sendet eine große HTTP GET-Anforderung an den Ziel-IIS-Server. Die ursprüngliche "Code Red"-Struktur ist unten dargestellt:

```
2001-08-04 16:32:23 10.101.17.216 - 10.1.1.75 80 GET /default.ida
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNN%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u
7801%u9090%u9090%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a 403
```

Der "Code Red" II-Fußabdruck ist unten dargestellt:

```
2001-08-04 15:57:35 10.7.35.92 - 10.1.1.75 80 GET /default.ida XXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX%u9090
%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%
u9090%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a 403 -
```

Beachten Sie, dass die GET-Anforderung immer nach einer Datei mit der Dateierweiterung .ida sucht. Dies ist eine allgemeine Zeichenfolge für alle Infektionsversuche und kann daher als Anpassungskriterien für klassenbasierte Markierungen in IOS verwendet werden. Der Rest der GET-Anforderung ist nicht unbedingt konsistent, da er lediglich versucht, einen Pufferüberlauf zu

erstellen. Dies lässt sich durch den Vergleich der beiden obigen Einträge erkennen.

Es wird nun berichtet, dass der Unterschied zwischen diesen beiden Signaturen auf eine neue Variante des Wurms "Code Red" zurückzuführen ist, der CodeRed.v3 oder CodeRed.C genannt wird. Der ursprüngliche Stamm "Code Red" enthält die Zeichenfolge "NNNNN" in der GET-Anforderung, während der neue Stamm "XXXXXXXX" enthält. Weitere Informationen finden Sie in der Symantec Advisory .

Am 6. August 2001 um 18:24 Uhr EDT haben wir einen neuen Fußabdruck aufgenommen. Seitdem haben wir erfahren, dass dies der Fußabdruck ist, der vom eEye-Schwachstellenscanner hinterlassen wird.

```
2001-08-06 22:24:02 10.30.203.202 - 10.1.1.9 80 GET /x.ida AAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=X 403 HTTP/1.1 -
```

Das Verfahren zum Blockieren von "Code Red" in diesem Gutachten kann diese Scanversuche auch blockieren, indem die Definition der Klassenzuordnung, wie im nächsten Abschnitt gezeigt, optimiert wird.

Eingehende "Code-Red"-Hacks mithilfe der IOS-klassenbasierten Markierungsfunktion markieren

Um den Wurm "Code Red" zu blockieren, verwenden Sie eine der drei unten beschriebenen Methoden. Alle drei Methoden klassifizieren schädlichen Datenverkehr mithilfe der Cisco IOS MQC-Funktion. Dieser Datenverkehr wird dann wie unten beschrieben verworfen.

Methode A: ACL verwenden

Diese Methode verwendet eine ACL auf der Ausgabeschnittstelle, um die als "Code Red" markierten Pakete zu verwerfen. Verwenden Sie das folgende Netzwerkdiagramm, um die Schritte in dieser Methode zu veranschaulichen:

Die folgenden Schritte sind für die Konfiguration dieser Methode erforderlich:

1. Klassifizieren Sie eingehende "Code Red"-Hacks mit der klassenbasierten Markierungsfunktion der Cisco IOS-Software, wie unten gezeigt:

   ```
   Router(config)#class-map match-any http-hacks
   Router(config-cmap)#match protocol http url "*default.ida*"
   Router(config-cmap)#match protocol http url "*cmd.exe*"
   Router(config-cmap)#match protocol http url "*root.exe*"
   ```

   Die obige Klassenzuordnung sucht innerhalb von HTTP-URLs und ordnet eine der angegebenen Zeichenfolgen zu. Beachten Sie, dass neben der Standarddatei "Code Red"

weitere Dateinamen angegeben wurden. Sie können diese Methode verwenden, um ähnliche Hackerversuche zu blockieren, z. B. den Sadmind-Virus, der in den folgenden Dokumenten erläutert wird:http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS00-078.asphttp://www.sophos.com/virusinfo/analyses/unixsadmind.html

2. Erstellen Sie eine Richtlinie, und verwenden Sie den **Befehl set**, um eingehende "Code Red"-Hacks mit einer Richtlinienzuordnung zu kennzeichnen. In diesem Dokument wird ein DSCP-Wert von 1 (in Dezimalstellen) verwendet, da dieser Wert wahrscheinlich von keinem anderen Netzwerkverkehr übertragen wird.Hier markieren wir eingehende "Code Red"-Hacks mit einer Richtlinienzuordnung namens "mark-inbound-http-hacks".
```
Router(config)#policy-map mark-inbound-http-hacks
Router(config-pmap)#class http-hacks
Router(config-pmap-c)#set ip dscp 1
```

3. Wenden Sie die Richtlinie auf der Eingabeschnittstelle als Richtlinie für eingehenden Datenverkehr an, um ankommende "Code Red"-Pakete zu kennzeichnen.
```
Router(config)#interface serial 0/0
Router(config-if)#service-policy input mark-inbound-http-hacks
```

4. Konfigurieren Sie eine ACL, die mit dem DSCP-Wert 1 übereinstimmt, wie in der Dienstrichtlinie festgelegt.
```
Router(config)#access-list 105 deny ip any any dscp 1
Router(config)#access-list 105 permit ip any any
```

   Hinweis: Die Cisco IOS Software-Versionen 12.2(11) und 12.2(11)T unterstützen das **log-**Schlüsselwort auf der ACL bei der Definition von Klassenzuordnungen für die Verwendung mit NBAR (CSCdv48172). Wenn Sie eine frühere Version verwenden, verwenden Sie nicht das **log-**Schlüsselwort auf der ACL. Auf diese Weise werden alle Pakete anstelle von CEF-Switched prozessgeschaltet, und NBAR funktioniert nicht, da CEF erforderlich ist.
5. Wenden Sie die ausgehende Zugriffskontrollliste auf die Ausgabeschnittstelle an, die mit den Ziel-Webservern verbunden ist.
```
Router(config)#interface ethernet 0/1
Router(config-if)#ip access-group 105 out
```

6. Überprüfen Sie, ob Ihre Lösung wie erwartet funktioniert. Führen Sie den Befehl **show access-list** aus, und stellen Sie sicher, dass der Wert "Matches" für die deny-Anweisung inkrementiert wird.
```
Router#show access-list 105
Extended IP access list 105
 deny ip any any dscp 1 log (2406 matches)
 permit ip any any (731764 matches)
```
   Im Konfigurationsschritt können Sie auch das Senden von nicht erreichbaren IP-Nachrichten mit dem Befehl **no ip unreachable** interface-level deaktivieren, um zu vermeiden, dass der Router übermäßige Ressourcen ausgibt.Diese Methode wird nicht empfohlen, wenn Sie den DSCP=1-Datenverkehr gemäß der Beschreibung im Abschnitt Methode B auf Null 0 weiterleiten können.

Methode B: Policy-Based Routing (PBR) verwenden

Diese Methode verwendet richtlinienbasiertes Routing, um markierte "Code Red"-Pakete zu blockieren. Wenn die Methoden A oder C bereits konfiguriert sind, müssen Sie die Befehle in

dieser Methode nicht anwenden.

Die folgenden Schritte sind für die Implementierung dieser Methode erforderlich:

1. Klassifizieren Sie den Datenverkehr, und markieren Sie ihn. Verwenden Sie die Befehle **class-map** und **policy-map**, die in Methode A dargestellt sind.
2. Verwenden Sie den Befehl **service-policy**, um die Richtlinie als eingehende Richtlinie auf der Eingabeschnittstelle anzuwenden und "Code Red"-Pakete anzuzeigen. Siehe Methode A.
3. Erstellen Sie eine erweiterte IP-Zugriffskontrollliste, die mit den als "Code Red" markierten Paketen übereinstimmt.
   ```
   Router(config)#access-list 106 permit ip any any dscp 1
   ```
4. Verwenden Sie den **route-map**-Befehl, um eine Routing-Richtlinie zu erstellen.
   ```
   Router(config)#route-map null_policy_route 10
   Router(config-route-map)#match ip address 106
   Router(config-route-map)#set interface Null0
   ```
5. Wenden Sie die route-map auf die Eingabeschnittstelle an.
   ```
   Router(config)#interface serial 0/0
   Router(config-if)#ip policy route-map null_policy_route
   ```
6. Stellen Sie sicher, dass die Projektmappe mit dem Befehl **show access-list wie erwartet funktioniert**. Wenn Sie ausgehende ACLs verwenden und die ACL-Protokollierung aktiviert haben, können Sie auch die Befehle **show log** verwenden (siehe unten):
   ```
   Router#show access-list 106
   Extended IP access list 106
    permit ip any any dscp 1 (1506 matches)

   Router#show log
   Aug 4 13:25:20: %SEC-6-IPACCESSLOGP:
    list 105 denied tcp A.B.C.D.(0) -> 10.1.1.75(0), 6 packets
   Aug 4 13:26:32: %SEC-6-IPACCESSLOGP:
    list 105 denied tcp A.B.C.D.(0) -> 10.1.1.75(0), 6 packets
   ```
   Wir können die Entscheidung für den Rückruf an der Eingangs-Schnittstelle des Routers treffen, anstatt eine Ausgangszugriffskontrollliste für jede Ausgangsschnittstelle zu benötigen. Auch hier empfehlen wir, das Senden von nicht erreichbaren IP-Nachrichten mit dem Befehl **no ip unreachables** zu deaktivieren.

Methode C: Klassenbasiertes Policing verwenden

Diese Methode ist im Allgemeinen die skalierbarste Methode, da sie weder von PBR- noch von Output-ACLs abhängt.

1. Klassifizieren Sie den Datenverkehr mithilfe der Befehle **für die Klassenzuordnung**, wie in Methode A gezeigt.
2. Erstellen Sie eine Richtlinie mit dem Befehl **policy-map**, und verwenden Sie den Befehl **Police**, um eine Drop-Aktion für diesen Datenverkehr anzugeben.

```
Router(config)#policy-map drop-inbound-http-hacks
Router(config-pmap)#class http-hacks
Router(config-pmap-c)#police 1000000 31250 31250
 conform-action drop exceed-action drop violate-action drop
```

3. Verwenden Sie den Befehl **service-policy**, um die Richtlinie als eingehende Richtlinie auf die Eingabeschnittstelle anzuwenden und die "Code Red"-Pakete zu verwerfen.
```
Router(config)#interface serial 0/0
Router(config-if)#service-policy input drop-inbound-http-hacks
```

4. Stellen Sie sicher, dass Ihre Lösung mit dem Befehl **show policy-map interface (Richtlinienzuordnung anzeigen)** wie erwartet funktioniert. Stellen Sie sicher, dass Sie inkrementelle Werte für die Klasse und die individuellen Anpassungskriterien sehen.
```
Router#show policy-map interface serial 0/0

Serial0/0

  Service-policy input: drop-inbound-http-hacks

    Class-map: http-hacks (match-any)
      5 packets, 300 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: protocol http url "*default.ida*"
        5 packets, 300 bytes
        5 minute rate 0 bps
      Match: protocol http url "*cmd.exe*"
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol http url "*root.exe*"
        0 packets, 0 bytes
        5 minute rate 0 bps
      police:
        1000000 bps, 31250 limit, 31250 extended limit
        conformed 5 packets, 300 bytes; action: drop
        exceeded 0 packets, 0 bytes; action: drop
        violated 0 packets, 0 bytes; action: drop
        conformed 0 bps, exceed 0 bps, violate 0 bps

    Class-map: class-default (match-any)
      5 packets, 300 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

Einschränkungen für NBAR

Beachten Sie bei der Verwendung von NBAR mit den Methoden in diesem Dokument, dass die folgenden Funktionen von NBAR nicht unterstützt werden:

- Mehr als 24 gleichzeitige URLs, HOSTs oder MIME-Typenübereinstimmungen
- Übereinstimmung über die ersten 400 Byte in einer URL hinaus
- Nicht IP-basierter Datenverkehr
- Multicast- und andere Nicht-CEF-Switching-Modi
- Fragmentierte Pakete
- Pipellierte HTTP-Anfragen
- URL/HOST/MIME/Klassifizierung mit sicherem HTTP
- Asymmetrische Datenströme mit Stateful-Protokollen

- Pakete, die vom Router mit NBAR ausgehen oder für diesen bestimmt sind

Sie können NBAR nicht auf den folgenden logischen Schnittstellen konfigurieren:

- Schneller EtherChannel
- Schnittstellen, die Tunneling oder Verschlüsselung verwenden
- VLANs
- Dialer-Schnittstellen
- Multilink PPP

Hinweis: NBAR kann ab Cisco IOS Release 12.1(13)E auf VLANs konfiguriert werden, wird jedoch nur im Software-Switching-Pfad unterstützt.

Da die NBAR nicht zur Klassifizierung des Ausgangsdatenverkehrs auf einer WAN-Verbindung verwendet werden kann, bei der Tunneling oder Verschlüsselung verwendet werden, wenden Sie sie stattdessen auf andere Schnittstellen am Router an, z. B. die LAN-Schnittstelle, um eine Eingangsklassifizierung durchzuführen, bevor der Datenverkehr zur Ausgabe an die WAN-Verbindung umgeleitet wird.

Weitere Informationen zu NBAR finden Sie unter den Links in den zugehörigen Informationen.