分散型サービス拒絶（DDoS）攻撃を防ぐ対策

目次

概要

このホワイト ペーパーでは、分散型サービス妨害（DDoS）攻撃が画策される方法の理解、DDoS 攻撃に使用されるプログラムの認識、攻撃を防ぐ対策の適用、攻撃を受けている疑いがある場合の証拠の収集、およびホストのセキュリティに関する詳細な学習などに役立つ情報を取り上げています。

DDoS 攻撃の基本について

次の図を参照してください。

上の図では、**Client** の背後に攻撃を企てる人が存在します。 **Handler** は、侵入されるホストで、特別なプログラムを実行しています。 それぞれのHandlerには複数のAgentを制御する機能があります。 **Agent** は侵入されるホストで、特別なプログラムを実行しています。 それぞれのAgentは、標的に向けられたパケットを流すために使用されます。

攻撃者は、次の 4 つのプログラムを使用して DDoS 攻撃を開始することが確認されています。

1. Trinoo
2. TFN
3. TFN2K
4. Stacheldraht

攻撃者が DDoS を実行するには、数百から数千の侵入されるホストが必要です。 このようなホストとして通常は Linux および SUN のコンピュータが使用されますが、 他のコンピュータにもツールを移植できます。 ホストに侵入するプロセスと、ツールをインストールするプロセスは、自動化されています。 攻撃者のプロセスは、次のステップに分割できます。

1. 非常に多数のホスト（100,000 台以上）が無防備であるかどうかを検出するスキャンを開始します。
2. アクセスを確立するために、無防備なホストに侵入します。
3. 各ホストにツールをインストールします。
4. 侵入したホストを使用して、さらにスキャニングと侵入を行います。

プロセスが自動化されているため、攻撃者は 1 台のホスト当たり 5 秒以内で侵入とインストール

を実行できます。 言い換えれば、1 時間もかけずに数千台のホストに侵入できることになります。

攻撃の実行に使用される一般的なプログラムの特性

ハッカーが分散型サービス拒絶攻撃に使用する一般的なプログラムがあります。

- TrinooClient（クライアント）、Handler（ハンドラ）、および Agent（エージェント）間の通信では、次のポートを使用します。`1524 tcp`
  `27665 tcp`
  `27444 udp`
  `31335 udp`**注:** 上記のポートは、このツールの*デフォルトのポート*です。 ポートの番号は容易に変更できるため、これらのポートは説明および例としてだけ使用してください。
- TFNClient（クライアント）、Handler（ハンドラ）、およびAgent（エージェント）間の通信では、ICMP ECHO パケットと ICMP ECHO REPLY パケットを使用します。
- StacheldrahtClient（クライアント）、Handler（ハンドラ）、および Agent（エージェント）間の通信では、次のポートを使用します。`16660 tcp`
  `65000 tcp`
  `ICMP ECHO`
  `ICMP ECHO REPLY`**注:** 上記のポートは、このツールのデフォルトのポートです。 ポートの番号は容易に変更できるため、これらのポートは説明および例としてだけ使用してください。
- TFN2KClient（クライアント）、Handler（ハンドラ）、および Agent（エージェント）間の通信では、特定のポートを使用しません（たとえば、ポートは実行時に与えられるか、あるいはプログラムによってランダムに選択されます）。代わりに、UDP、ICMP、および TCP パケットを組み合わせて使用します。DDoS プログラムの詳細な分析については、次のドキュメントを参照してください。

注: 次のリンク先は、シスコ管理外の外部の Web サイトです。

The DoS Project's "trinoo" distributed denial of service attack tool

The "Tribe Flood Network" distributed denial of service attack tool

The "stacheldraht" distributed denial of service attack tool

DDoS ツールやその変種についてのその他の情報は、次の Packet Storm の Web サイトで参照できます：Index of Distributed Attack Tools 。

防止

次に、分散型サービス拒絶攻撃を防ぐために推奨する方法について説明します。

1. **接続の上流側の端にあるルータの入力インターフェイスで、ip verify unicast reverse-path インターフェイス コマンドを使用します。**この機能は、インターフェイスで受信された各パケットを検査します。 発信元 IP アドレスについて、パケットが受信したインターフェイスと同じ インターフェイスに戻る経路が CEF テーブル内にない場合、ルータはその パケットをドロップします。ユニキャスト RPF の機能は、SMURF 攻撃（および発信元 IP アドレスの偽装を用いる他の攻撃）を ISP の POP（リースとダイヤルアップ）で止めることです。この機能により、ネットワークとカスタマー、および他のインターネットを保護できます。ユニキャスト RPF を使用するには、ルータで「CEF スイッチング」または「CEF 分散型ス

イッチング」を有効にします。 CEF スイッチングの場合は、入力インターフェイスを設定する必要はありません。 CEF がルータで実行されている間は、個々のインターフェイスに他のスイッチング モードを設定できます。 RPF は入力側の機能であり、インターフェイスまたはサブインターフェイスを有効にし、ルータで受信されたパケットに対して動作します。ルータで CEF を動作することは非常に重要です。 RPF は CEF がないと動作しません。 ユニキャスト RPF は、11.2 または 11.3 のイメージではサポートされません。 ユニキャスト RPF は、AS5800 などの CEF をサポートするプラットフォームの 12.0 に含まれます。 したがって、AS5800 の PSTN/ISDN ダイヤルアップ インターフェイスでは、ユニキャスト RFP を設定できます。

2. すべての RFC-1918 アドレス空間を、Access Control Lists（ACL）を使用してフィルタ処理します。次の例を参照してください。`access-list 101 deny ip 10.0.0.0 0.255.255.255 any`
```
access-list 101 deny ip 192.168.0.0 0.0.255.255 any
access-list 101 deny ip 172.16.0.0  0.15.255.255 any
access-list 101 permit ip any any

interface xy
   ip access-group 101 in
```
フィルタ処理できる特殊用途の IPv4 アドレス空間に関する別の情報源が、IETF のドラフト（現在は期限切れ）「IANA に登録された特殊用途の IPv4 アドレス空間の記録」です。
3. イングレスとイーグレス フィルタリング（RFC-2267 を参照 ）を、ACL を使用して適用します。次の例を参照してください。`{ ISP Core } -- ISP Edge Router -- Customer Edge Router -- { Customer network }`ISP のエッジ ルータでは、カスタマーのネットワークに属する発信元アドレスを持つトラフィックだけを受け入れるようにします。 カスタマー側のネットワークでは、カスタマーのネットワーク ブロック以外の発信元アドレスを持つトラフィックだけを受け入れるようにします。 次に示す例は、ISP のエッジ ルータ用の ACL です。`access-list 190 permit ip {customer network} {customer network mask} any`
```
access-list 190 deny ip any any [log]

interface {ingress interface} {interface #}
```
`ip access-group 190 in` 次に示す例は、カスタマー エッジ ルータ用の ACL です。`access-list 187 deny ip {customer network} {customer network mask} any`
```
access-list 187 permit ip any any

access-list 188 permit ip {customer network} {customer network mask} any
access-list 188 deny ip any any

interface {egress interface} {interface #}
ip access-group 187 in
```
`ip access-group 188 out` Cisco Express Forwarding（CEF）を実行できる場合は、ACL での長さをかなり短くできるため、ユニキャストRPFを有効にすることで処理効率が上がります。 ユニキャスト RPF をサポートするには、ルータ上で CEF を有効にするだけです。 この機能が有効にされているインターフェイスは、CEF スイッチ インターフェイスである必要はありません。
4. CAR を使用して、ICMP パケットにレート制限を適用します。次の例を参照してください。
```
interface xy
 rate-limit output access-group 2020 3000000 512000 786000 conform-action transmit exceed-action drop access-list 2020 permit icmp any any echo-reply
```
5. SYN パケットにレート制限を設定します。次の例を参照してください。`access-list 152 permit tcp any host eq www`
```
access-list 153 permit tcp any host eq www established

interface {int}
rate-limit output access-group 153 45000000 100000 100000
conform-action transmit exceed-action drop
```

```
 rate-limit output access-group 152 1000000 100000 100000
conform-action transmit exceed-action drop
```
上の例で、次のように置き換えます。リンクの帯域幅の最大値に **45000000**SYN フラッド レートの 50 ～ 30 % の間の値に **1000000***通常のバースト レートと最大バースト レート*を正確な値に置き換えますバースト レートを 30% より大きく設定すると、多くの正当な SYN はドロップされる可能性があることに注意してください。 バースト レートをどこに設定するかの参考には、show interfaces rate-limit コマンドを使用して、インターフェイスの適合レートと超過レートを調べてください。 この操作の目的は、SYN に必要最低限のレート リミットを与えて、再度実行することです。**警告**：最初に通常の状態（攻撃が発生する前）で SYN パケットの容量を測定し、これらの値を使用して制限することを推奨します。 この計測を適用する前には、数字を慎重に検証してください。SYN 攻撃が特定のホストを対象とする場合、そのホストで IP フィルタリング パッケージを導入することを検討します。 このようなパッケージの 1 つに IP Filter があります 。 詳細な実装方法については、「IP Filter 例」 を参照してください。

証拠の確保と警察への連絡

可能であれば、バックエンド解析のために攻撃トラフィックのサンプルを取得します（一般に「パケット キャプチャ」と呼ばれる）。 パケット フローに対応する十分な処理能力を持つ Solaris または Linux ワークステーションを使用します。 そのようなパケット キャプチャを取得するには、tcpdump プログラム（Windows、Solaris、および L inux オペレーティング システムで使用可能）または snoop プログラム（Solaris OS のみで使用可能）を使用します。 次に、これらのプログラムの使い方の基本的な例を示します。

```
tcpdump -i interface -s 1500 -w capture file
  snoop -d interface -o capture file -s 1500
```
この例の MTU サイズは 1500 に設定されています。 MTU が 1500 より大きい場合、このパラメータを変更します。

米国に在住で警察に届け出を出す場合は、地域の FBI フィールド オフィスに連絡します。 詳しい情報については、国家基盤保護センターの Web サイトで入手できます。 ヨーロッパには統一窓口がありません。 地元の警察に連絡して、サポートを依頼してください。

シスコがユーザの代わりに警察に連絡することはできません。 お客様から最初の連絡が行われた後であれば、シスコ PSIRT チームは司法機関に協力できます。

一般的なホストのセキュリティに関する資料は、CERT/CC の Web ページを参照してください。

関連情報

- **Cisco ルータを使用したパケットフラッドの識別とトレース**
- **ワームの軽減に関する技術的詳細**
- **Cisco ルータにおけるセキュリティの向上**
- **シスコ製品のセキュリティ上の問題への対応**
- **シスコのセキュリティ**
- **テクニカルサポートとドキュメント - Cisco Systems**