Distributed via @police
http://www.npa.go.jp/cyberpolice/

平成 27 年 10 月 23 日

Topic

UDP を利用するプロトコルを悪用するリフレクター攻撃の観測状況について

国内外の IP アドレスに対するリフレクター攻撃[i]と思われるパケットを確認しました。インターネット利用者は、管理する機器がリフレクター攻撃の踏み台として悪用されることのないように、再度確認を実施することを推奨します。

1 リフレクター攻撃の観測について

警察庁では、DNS、NTP、SSDP、SNMP 等の UDP を利用するプロトコルを悪用するリフレクター攻撃について、これまで注意喚起[ii]を実施してきました。昨今、国内外においてリフレクター攻撃の発生が多数確認されるようになり、リフレクター攻撃の脅威は現実のものとなりつつあります。警察庁ではリフレクター攻撃の発生状況の把握及び国内の重要インフラ事業者等に対する攻撃の検知を目的として、新たな観測システムの運用を開始しています。

同システムは、リフレクター攻撃の踏み台として利用できると誤認させ、到達するパケットを観測するもので、これにより、リフレクター攻撃の発生時間や攻撃対象等の情報を収集することが可能となります（図1）。

---

[i] リフレクター攻撃は「DRDoS（Distributed Reflection Denial of Service）攻撃」とも呼ばれます。

[ii] 「DNS リフレクション攻撃に対する注意喚起について」（平成 25 年4月 11 日）
http://www.npa.go.jp/cyberpolice/detect/pdf/20130411.pdf
「NTP サーバを踏み台としたリフレクター攻撃（NTP リフレクター攻撃）に対する注意喚起について」（平成 26 年1月 17 日）
http://www.npa.go.jp/cyberpolice/detect/pdf/20140117.pdf
「情報技術解析平成 25 年報」（平成 26 年2月 27 日）
http://www.npa.go.jp/cyberpolice/detect/pdf/H25_nenpo.pdf
「UDP を利用するプロトコルを悪用する各種リフレクター攻撃に対する注意喚起について」（平成 26 年7月 11 日）
http://www.npa.go.jp/cyberpolice/detect/pdf/20140711.pdf
「UPnP に対応したネットワーク機器を踏み台とした SSDP リフレクター攻撃に対する注意喚起について」（平成 26 年 10 月 17 日）
http://www.npa.go.jp/cyberpolice/detect/pdf/20141017.pdf
「SNMP リフレクター攻撃に対する注意喚起について」（平成 26 年 11 月 26 日）
http://www.npa.go.jp/cyberpolice/detect/pdf/20141126.pdf
「情報技術解析平成 26 年報」（平成 27 年3月 12 日）
http://www.npa.go.jp/cyberpolice/topics/?seq=15688

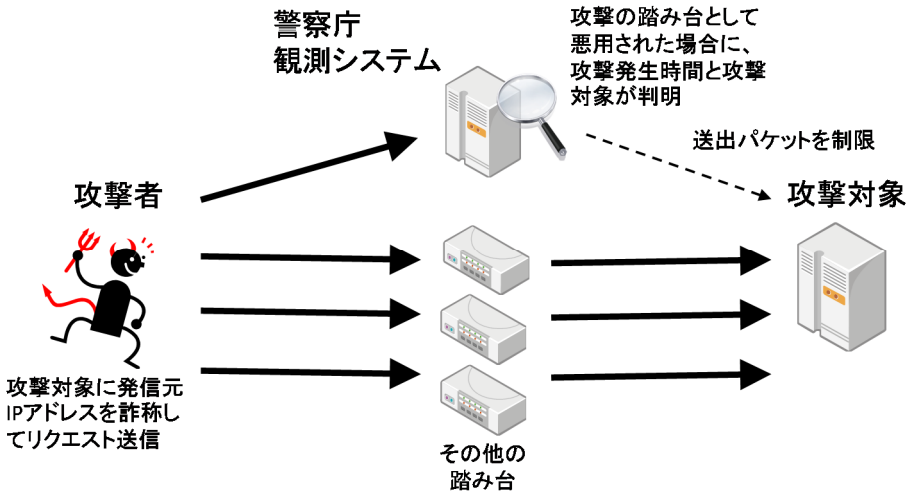

図1　警察庁におけるリフレクター攻撃観測システムの原理

同システムにおける観測パケットの検知件数は、表1のとおりです。

表1　警察庁の観測システムにおけるプロトコル別の観測パケット数

プロトコル	検知件数 （1 日当たり）
NTP	8,368,408
CHARGEN	2,850,229
DNS	456,101
SSDP	56,425
SNMP	234

2　推奨する対策

（1）一般的な対策

管理する機器が、様々なリフレクター攻撃の踏み台として悪用されないために、次の対策を実施することを推奨します。

- 使用していない不要なサービスは停止する。サーバ等のコンピュータだけではなく、ネットワーク機器においても、意図せずに外部へ不要なサービスを公開していないか確認を実施する。
- 外部に公開する必要がないサービスは、インターネットからの通信を遮断する。
- 不特定多数に公開する必要がないサービスについては、適切なアクセス制限や認証を実施する。
- 不特定多数に公開する必要があるサービスについては、リフレクター攻撃の踏み台として悪用されないように、適切な設定への変更を実施する。

（2）ブロードバンドルータにおける対策

一般家庭や小規模な組織においては、インターネットに接続するために使用されるブロードバンドルータが、数多く利用されています。リフレクター攻撃には、これらのブロードバン

ドルータも、設定が適切ではない場合には踏み台として悪用されていると考えられます。このことから、これまでの注意喚起と同様となりますが、以下の対策を実施することを推奨します。

- ブロードバンドルータの製造元、貸与している ISP や回線事業者等が公開している最新バージョンのファームウェアや、攻撃の踏み台となることを回避する設定変更方法を確認してください。
- 最新バージョンのファームウェアが未適用であれば、適用を実施してください。
- 攻撃の踏み台となることを回避する設定がされていなければ、設定変更を実施してください。
- 製造終了から年月が経過して、製造元における対応が打ち切られている機種も存在します。この場合には、ブロードバンドルータの交換を検討してください。