平成 26 年 7 月 11 日

Topic

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

リフレクター攻撃の踏み台となる機器の探索行為と考えられるアクセスが、DNS や NTP 以外の複数のプロトコルにも拡大しています。管理する機器が攻撃の踏み台とならないように、十分に注意を払う必要があります。

1　リフレクター攻撃の踏み台となる機器の探索行為の対象プロトコルの拡大について

警察庁においては、DNS や NTP といったプロトコルを悪用するリフレクター攻撃（リフレクション攻撃）や、その踏み台として悪用可能なサーバ等の機器の探索行為と考えられるアクセスの増加については、これまでも注意喚起[i]を実施してきたところです。

しかしながら、DNS や NTP に限らず、以下の条件を満たすプロトコルはリフレクター攻撃に悪用される危険性があります。

- 通信時にセッションの確立が不要な UDP を利用するプロトコル
- サーバに対するリクエストのパケットサイズと比較して、応答パケットのサイズが大きくなるプロトコル
- サーバにリクエストを行う際に、認証等が不要であるプロトコル
- 第3者が自由にリクエストを送信できるサーバが、インターネット上に多数存在するプロトコル

US-CERT からは、この様な条件を満たし、リフレクター攻撃に悪用される可能性があるプロトコルが具体的に挙げられ、注意喚起[ii]が実施されています。

警察庁の定点観測システムにおいては、DNS 以外にも、この様なプロトコルに対するアクセスの増加を3月から観測しています（図1、表1）。これらのアクセスの中には、リフレクター攻撃の踏み台として悪用可能な機器の探索を目的とするアクセスが多数含まれていると考えられます。

---

[i] 「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
「中国を発信元とする再帰問い合わせ可能な DNS サーバの探索行為の増加について」（平成 25 年9月 11 日）
http://www.npa.go.jp/cyberpolice/detect/pdf/20130911.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
「発信元 IP アドレスを偽装したオープン・リゾルバの探索行為の増加について」（平成 26 年2月 17 日）
http://www.npa.go.jp/cyberpolice/detect/pdf/20140217.pdf

[ii] 「Alert (TA14-017A) UDP-based Amplification Attacks」（平成 26 年1月 17 日）
http://www.us-cert.gov/ncas/alerts/TA14-017A

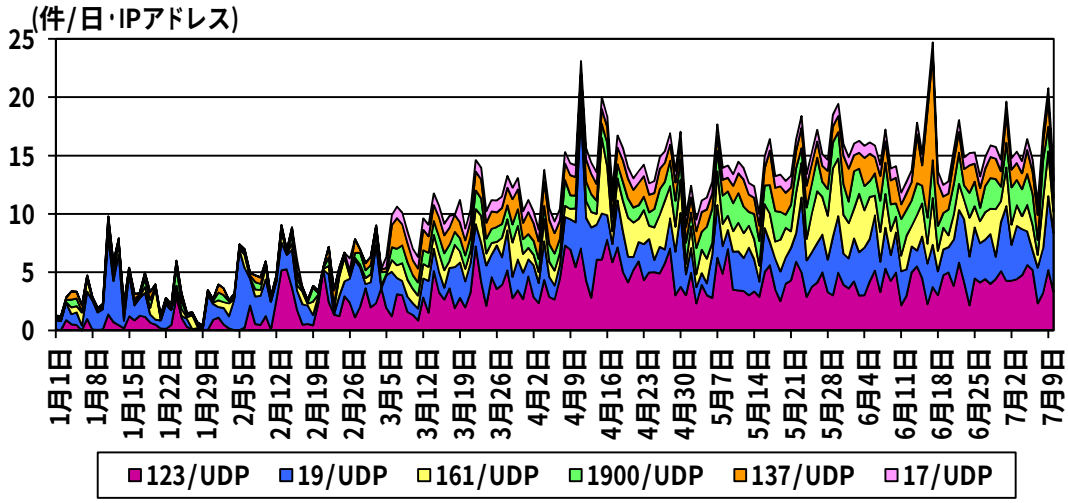

図1　リフレクター攻撃に悪用される可能性があるプロトコルに関するアクセス件数の推移
（H26.1.1～H26.7.10）

表1　定点観測システムにおいてアクセスが観測されているリフレクター攻撃に悪用される可能性があるプロトコル

ポート	プロトコル	概要
123/UDP	NTP	ネットワーク経由で機器の時刻同期を行うプロトコル。
19/UDP	CHARGEN	サーバから適当な文字列を返すプロトコル。ネットワーク試験等の目的で使用される。
161/UDP	SNMP	ネットワーク経由で機器の監視や制御を行うプロトコル。
1900/UDP	SSDP	UPnP においてネットワークに接続された機器の通知や探索に使用されるプロトコル。
137/UDP	NetBIOS	Microsoft Windows の名前解決に使用されるプロトコル。
17/UDP	QOTD	サーバから設定された短い文章を返すプロトコル。ネットワーク試験等の目的で使用される。

2　各種リフレクター攻撃の踏み台とならないために推奨する対策

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。

(1) 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。

(2) 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。

(3) 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。

(4) 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。