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

平成 26 年 10 月 17 日

Topic

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

UPnP (Universal Plug and Play) で使用されるプロトコル SSDP (Simple Service Discovery Protocol) を悪用した SSDP リフレクター攻撃を確認しています。管理するネットワーク機器が攻撃の踏み台として悪用されないために対策を行うことを推奨します。

1 UDP を利用するプロトコルを悪用するリフレクター攻撃

警察庁においては、DNS や NTP といった UDP を利用する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。

警察庁では、ネットワーク機器同士の接続機能である UPnP (Universal Plug and Play) で使用されるプロトコル SSDP (Simple Service Discovery Protocol) を悪用した SSDP リフレクター攻撃が行われた事例を確認しています。

2 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

(1) UPnP に対応したネットワーク機器の探索

攻撃者は、攻撃の踏み台とするネットワーク機器の探索を行います (図1)。攻撃者は、SSDP で使用されるポート 1900/UDP に対して機器情報の送信を要求する「M-SEARCH」というメッセージを送信し、その応答があるか否かで攻撃の踏み台とするネットワーク機器を探索しています。

この探索のアクセスについては、警察庁の定点観測システムにおいて、平成 26 年9月上旬頃から増加を確認しています (図2)。

ここで、攻撃者は「M-SEARCH」メッセージに応答を返すネットワーク機器、つまり、UPnP に対応し、かつ外部からのアクセスに対して FW (ファイアウォール) によるアクセス制限等の対策が行われていないネットワーク機器を SSDP リフレクター攻撃の踏み台として悪用します。

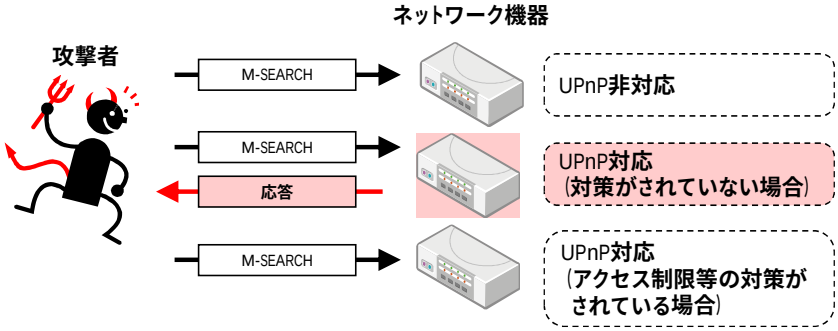

図1 攻撃の踏み台とするネットワーク機器の探索

[i] 「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

Copyright 2014 Cyber Force Center, NPA JAPAN

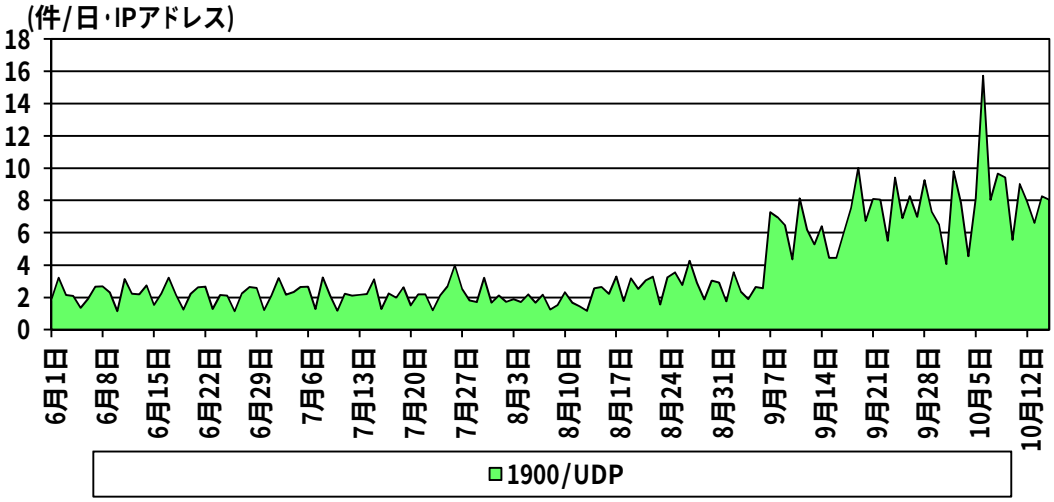

図2　宛先ポート 1900/UDP に対するアクセス件数の推移（H26.6.1～H26.10.15）

(2) SSDP リフレクター攻撃

攻撃者は、探索により発見したネットワーク機器を踏み台として悪用し、SSDP リフレクター攻撃を行います（図3）。攻撃者は、踏み台とするネットワーク機器に対して、発信元を攻撃対象に偽装した「M-SEARCH」メッセージを送信します。踏み台とされたネットワーク機器は、攻撃対象に対して応答を返しますが、攻撃者がこのメッセージを大量に送信すると、攻撃対象には大量のデータが送信されます。ネットワーク機器からの応答は、「M-SEARCH」メッセージのデータサイズより大きくなるため、直接、攻撃者が攻撃対象にデータを送信するよりも、効率的にデータ送信を行うことができます。

また、攻撃の踏み台とされたネットワーク機器についても、負荷が増大するため、正常な動作が妨害される可能性があります。

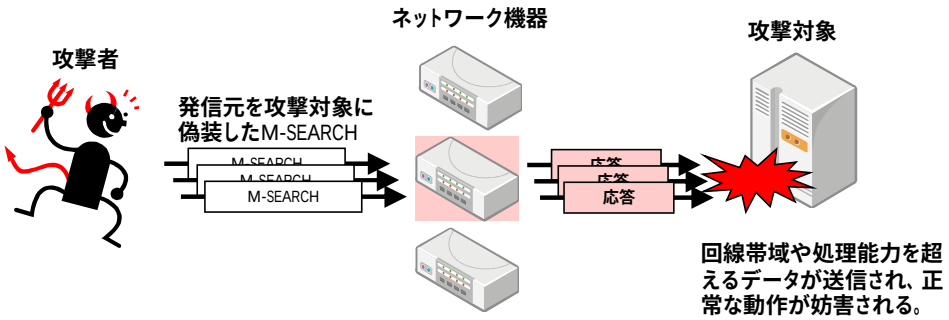

図3　SSDP リフレクター攻撃

警察庁では、平成 26 年 10 月上旬に対策が不十分なネットワーク機器を踏み台として、特定のホストに対して攻撃が行われた事例を確認しています。今後も、同様の手法を使用した攻撃が発生することが懸念されます。

Copyright 2014 Cyber Force Center, NPA JAPAN

3 SSDP 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

管理するネットワーク機器が、SSDP 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) 外部からの SSDP プロトコルの通信（宛先ポート 1900/UDP のパケット）を FW により遮断する。

(2) ネットワーク機器の UPnP 機能を使用していない場合は、停止する。

(3) ネットワーク機器の UPnP 機能を使用する場合は、外部からの「M- SEARCH」メッセージに対して、応答しない設定を行う。

Copyright 2014 Cyber Force Center, NPA JAPAN