平成 26 年 11 月 26 日

Topic

SNMP リフレクター攻撃に対する注意喚起について

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である SNMP（Simple Network Management Protocol）を悪用した SNMP リフレクター攻撃を企図するアクセスの増加を確認しています。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 SNMP に対応した機器を踏み台とした攻撃を企図するアクセスの増加

(1) 宛先ポート 161/UDP に対するアクセス

警察庁では、10 月中旬頃から宛先ポート 161/UDP に対するアクセスの増加を観測しています（図 1）。このポートは、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である SNMP（Simple Network Management Protocol）で使用されています。

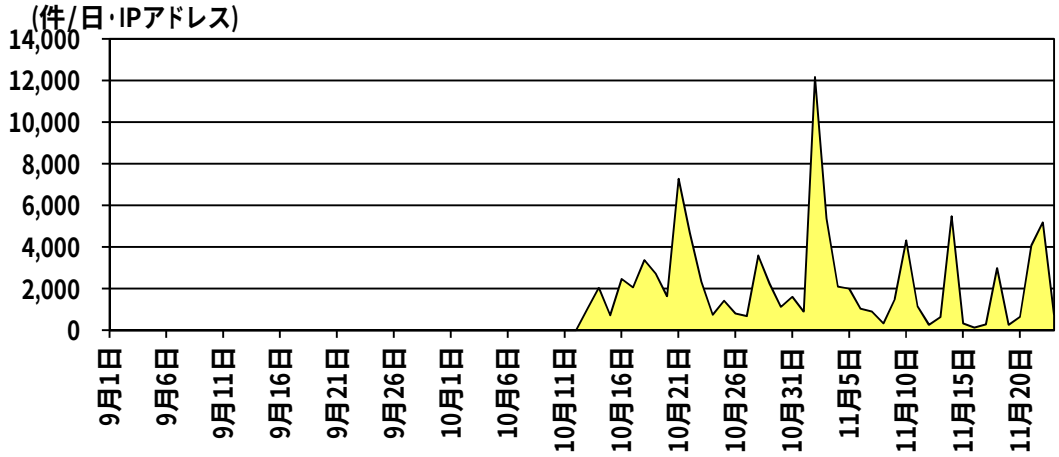

図1 宛先ポート 161/UDP に対するアクセス件数の推移

これらのアクセスは、SNMP に対応した機器（SNMP エージェント）から、複数の管理データ（MIB:Management Information Base）をまとめて取得する「GetBulkRequest」と呼ばれるリクエストを行うものであり、これは本来、管理する機器の監視を目的として送信されるものです。また、SNMP のバージョンが SNMPv2 に対応した機器（SNMPv2 エージェント）、また、SNMP コミュニティ名が初期値の「public」に設定されている機器を対象として送信されていました。

警察庁で検知したこれらのアクセスは、一部のセンサーでは全く観測されていません。攻撃者は、事前に何らかのスキャンを行い、攻撃の踏み台となる機器を選定してこれらのアクセスを行っていると推測されます。

(2) SNMP に対応した機器を踏み台としたリフレクター攻撃

攻撃者は、発信元の IP アドレスを攻撃対象の IP アドレスに詐称し、踏み台となる SNMP 対応機器に対してアクセスを行い、攻撃対象に対するリフレクター攻撃（リフレクション攻撃）を企図していると考えられます。このアクセスが、対策の行われていない SNMPv2 エージェントに行われた場合、発信元の IP アドレス（攻撃対象）に対して、大量のデータを送信してしまう可能性があります（図2）。

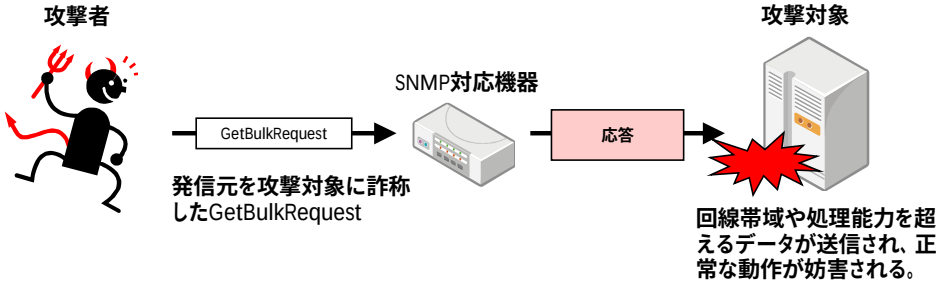

図2　SNMP に対応した機器を踏み台としたリフレクター攻撃

警察庁が観測したこれらのアクセスは、GetBulkRequest の MIB 複数取得数（max-repetitions）が「2250」にセットされているなどの共通点が確認されたことから、なんらかのツールを使用するなど、共通の手法により生成されたパケットであると考えられます。

警察庁では、SNMP を含めた UDP を利用するプロトコルを悪用するリフレクター攻撃について、これまでも注意喚起[i]を実施してきたところですが、以下の対策を行うことを推奨いたします。

2　SNMP 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、SNMP 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 SNMP 通信（宛先ポート 161/UDP のアクセス）を FW により遮断する。
(2) 不要な SNMP エージェントは停止する。
(3) SNMPv3 に対応した機器を使用して、認証・暗号の設定を行う。
(4) SNMP コミュニティ名には、初期値の「public」等、推測可能なものの使用は避ける。

[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