平成 26 年 11 月 13 日

インターネット観測結果等

(平成 26 年9月期)

- Bash の脆弱性を標的としたアクセスの検知
- 1900/UDP (SSDP) に対するアクセスの増加
- 53/UDP (DNS) に対するアクセスの増加

1 Bash の脆弱性を標的としたアクセスの検知

平成 26 年9月 24 日に、ユーザと OS を仲介するソフトウェアである「シェル」の一種である「Bash」(Bourne-Again Shell) に、深刻な脆弱性が明らかとなり、25 日午前5時以降、警察庁の定点観測システムにおいても、当該脆弱性の有無を確認するアクセスを観測しており、@police で注意喚起を行いました。

脆弱性が明らかになった直後は、当該脆弱性の有無についての探索行為が観測されていましたが、26 日以降は攻撃を試行したと思われるアクセスを観測しており (図1)、10 月9日に第2報で注意喚起[ii]を行いました。

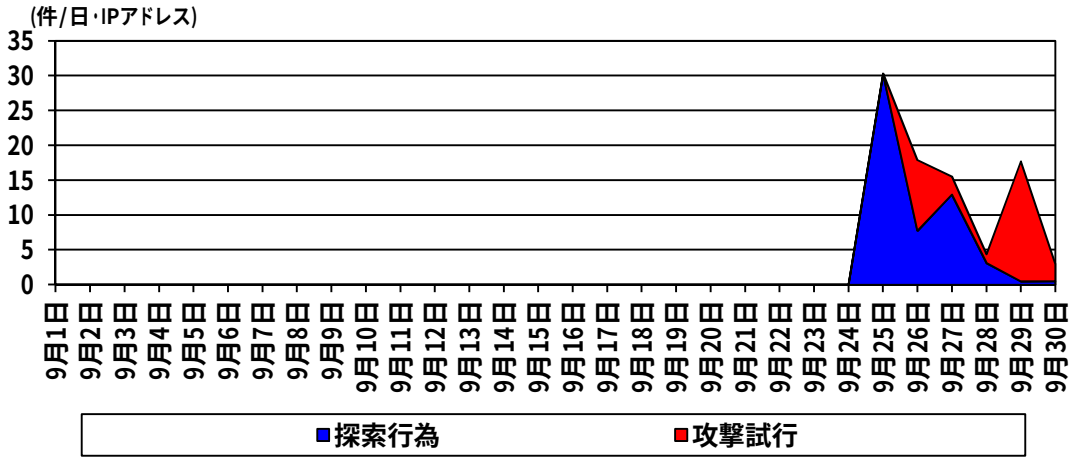

図1 Bash の脆弱性を標的としたアクセス件数の推移

観測された探索と思われるパケットの内容の例としては、次のようなものがありました。

```
GET / HTTP/1.0
User-Agent: () { :; }; /bin/ping -c XXX.XXX.XXX.XXX
Accept: */*..
```

i 「Bash の脆弱性を標的としたアクセスの観測について」(平成 26 年9月 25 日)
http://www.nap.go.jp/cyberpolice/detect/pdf/20140925-2.pdf
ii 「Bash の脆弱性を標的としたアクセスの観測について (第2報)」(平成 26 年 10 月9日)
http://www.nap.go.jp/cyberpolice/detect/pdf/20141007.pdf

これは、ping コマンドに対する応答により、対象機器の脆弱性の有無を調査しているものと思われます。

2 1900/UDP (SSDP) に対するアクセスの増加

9月7日以降、宛先ポート 1900/UDP に対するアクセスが増加しています (図2)。1900/UDP は、SSDP (Simple Service Discovery Protocol) で使用されるポートで UPnP (Universal Plug and Play) 機器を探索するために使用されるものです。

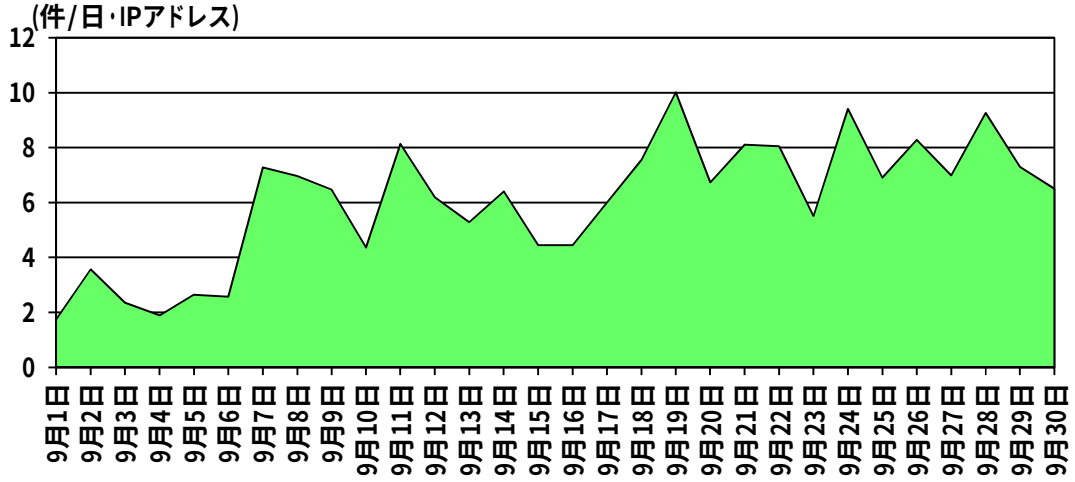

図2 宛先ポート 1900/UDP に対するアクセス件数の推移

観測されたほとんどのパケットは、マルチキャストアドレス (239.255.255.250) に対する M-SEARCH メッセージであり、UPnP 機器を探索しているものと考えられます (図3)。

```
M-SEARCH * HTTP/1.1
Host:239.255.255.250:1900
ST:upnp:rootdevice
Man:"ssdp:discover"
MX:3
```

各項目の意味
・ST (Search Target) ：探索対象
upnp:rootdevice はルートデバイスのみを検索する。
・Man (Mandatory Extension) ：必須拡張項目
常に「ssdp:doscover」が指定される。
・MX (Maximum Wait) ：最大待ち時間
3 は 3 秒を表す。

図3 観測された主なパケット

1900/UDP は、リフレクター攻撃[i]にも使用される可能性があるポートであり、DoS 攻撃の踏み台となる機器の探索を行っている可能性もあります。

10 月 17 日に、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

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

われた事例を確認したことから、注意喚起[i]を実施しています。

3　53/UDP (DNS) に対するアクセスの増加

9月中旬頃から宛先ポート53/UDPに対するアクセスが増加しています。53/UDPは、DNSに使用されるポートです。

同アクセスの内容を分析した結果、53/UDPに対するアクセスの半数は、特定IPアドレスからのものであり（図4）、アクセスの増加は、この特定 IP アドレスからのアクセスが要因でした。このアクセスの UDP ペイロード内容は、特定ドメインの ANY レコード若しくは A レコードを要求するものがほとんどでした。

同アクセスは、DNS リフレクター攻撃に悪用可能である再帰問い合わせ可能な DNS サーバ（オープンリゾルバ）を探索しているものと考えられます。

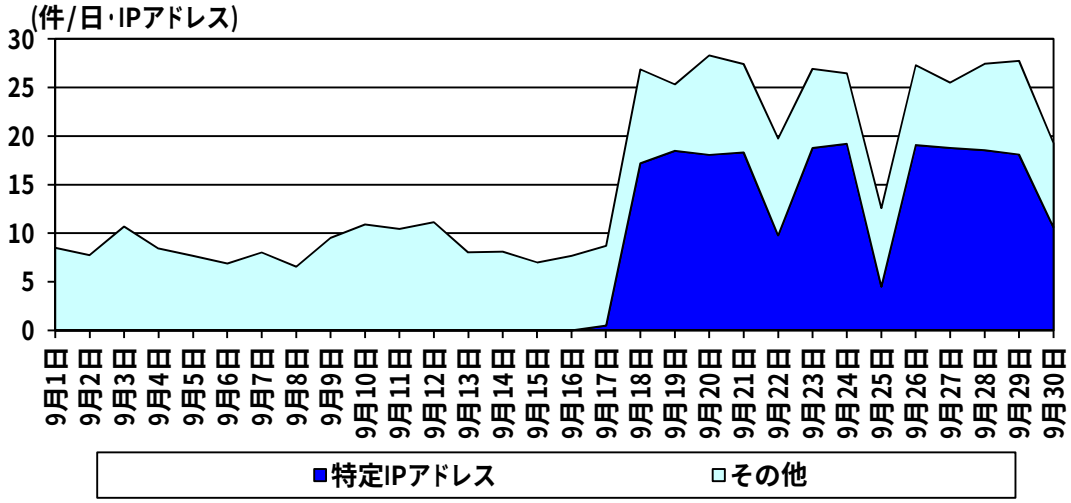

図4　宛先ポート 53/UDP に対するアクセス件数の推移

---

i 「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