平成 27 年9月 25 日

インターネット観測結果等

（平成 27 年8月期）

- 発信元ポート 53/UDP からのアクセスが増加
- 宛先ポート 53413/UDP に対するアクセスが増加
- 宛先ポート 111/UDP に対するアクセスが増加

1 発信元ポート 53/UDP からのアクセスが増加

警察庁の定点観測システムでは、7月下旬から、53/UDP を発信元ポートとするアクセスの増加を観測しました（図 1）。

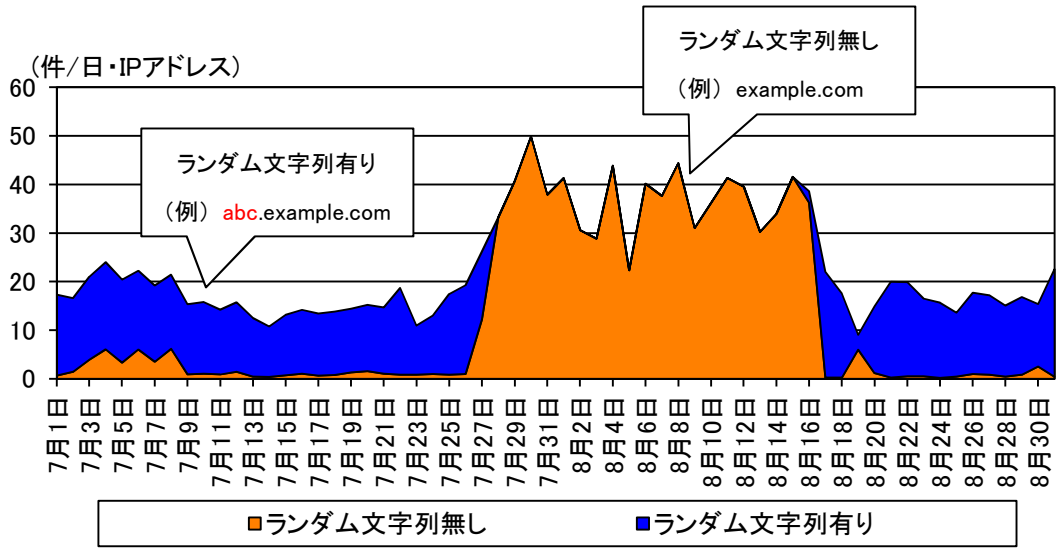

図 1 発信元ポート 53/UDP からのアクセス件数の推移（H27.7.1～8.31）

発信元ポート 53/UDP からのアクセスの内容を確認すると、大多数は DNS の問い合わせに対する回答であり、オープン・リゾルバを悪用した新たな DDoS 攻撃によるものであると考えられます[i]。

増加したアクセスには、DNS クエリとして、攻撃対象のドメイン名にランダムな文字列を含まないアクセスが観測され、従来とは異なる傾向がみられました。このようなアクセスが増加した背景は不明ですが、53/UDP を発信元とするアクセスが継続して観測されていることから、オープン・リゾルバの状態にある機器は、攻撃の踏み台とされる可能性が高いため、利用している機器がオープン・リゾルバとなっていないかを改めて確認するとともに、同状態となっている機器を発見した場合には適切な対策を実施することを推奨します。

---

i 「情報技術解析平成 26 年報～6.3 オープン・リゾルバを悪用する新たな DDoS 攻撃手法に関する観測状況」（平成 27 年3月 12 日）
http://www.npa.go.jp/cyberpolice/detect/pdf/H26_nenpo.pdf

2　宛先ポート 53413/UDP に対するアクセスが増加

53413/UDP を宛先ポートとするアクセスの増加を観測しました（図 2）。

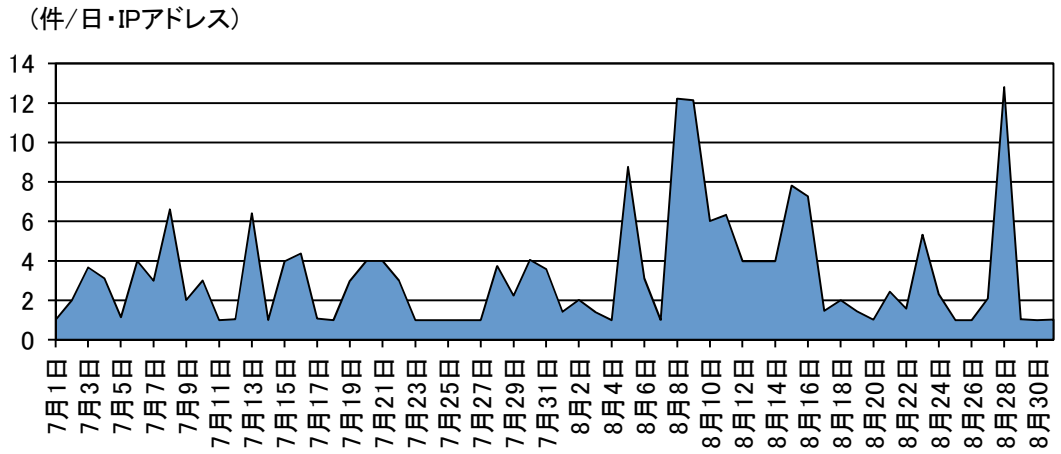

図 2　宛先ポート 53413/UDP に対するアクセス件数の推移（H27.7.1～8.31）

53413/UDP は、Netis[i]製のルータで使用されているもので、平成 26 年8月に外部から簡単にアクセスできる脆弱性[ii]が確認されました。定点観測システムでも同年8月 27 日に、アクセスの急増を確認[iii]して以降、継続して観測しています。

今期のアクセスの増加は、Netis 製ルータの探索行為が再び活発化した可能性があります。また、アクセスの中には、不正プログラムのダウンロード及び実行を試みるものも確認できたことから、脆弱性を放置したままの状態であれば、攻撃に利用される危険性があります。そのため、ルータについても、パソコン等と同様にセキュリティ対策を施すことが必要です。

ルータのセキュリティ対策としては、以下のようなものがあります。

- 管理用のパスワードは、推測されにくいものに変更しておく。
- メーカ等のウェブサイト等で脆弱性情報を確認し、脆弱性がある場合は、ファームウェアのアップデート等の対策を行う。
- 無線 LAN 機能を使用する場合は、強度な暗号を利用し、必要な端末からのみ利用できるようにフィルタリングを行う。

[i] 2000 年に設立されたネットワーク機器メーカで、中国深圳市に本社を置く Netcore 社のグループ企業のひとつ
http://www.netis-systems.com/

[ii] 「UDP ポートを開放した状態にする Netis 製ルータに存在する不具合を確認」
http://blog.trendmicro.co.jp/archives/9725

[iii] 「インターネット観測結果等（平成 26 年8月期）」
https://www.npa.go.jp/cyberpolice/detect/pdf/20141007_2.pdf

3 宛先ポート 111/UDP に対するアクセスが増加

111/UDP を宛先ポートとするアクセスの増加を観測しました（図 3）。

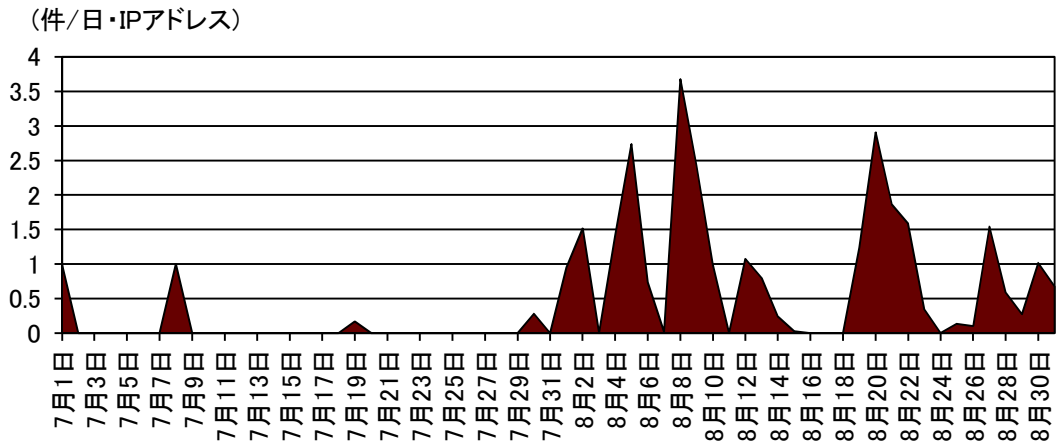

図 3 宛先ポート 111/UDP に対するアクセス件数の推移（H27.7.1～8.31）

111/UDP は、SunRPC[i]で利用されるポートです。SunRPC は、Cisco 社製「セキュリティアプライアンスソフトウェア」（以下「Cisco ASA」という。）でも使用されています。Cisco ASA には、SunRPC を含む複数の脆弱性[ii]があることが確認されており、7月９日には、このうちの一つを使用する攻撃を確認したとの情報[iii]が公表され、定点観測システムにおいても、当該脆弱性に関連する IKE のプロトコルで使用される 500/UDP を宛先ポートとするアクセスの増加を観測しました[iv]。

Cisco ASA で使用されている SunRPC の脆弱性[v]は、悪用されると攻撃の対象となったソフトウェアがサービス不能に陥るなどの可能性があるものです。

今回のアクセス増加と、脆弱性の関連性は不明ですが、脆弱性のある機器の探索行為が活発化したとも考えられるため、ソフトウェアを最新バージョンに更新するなどして、脆弱性を修正することを推奨します。

---

[i] Sun Microsystems 社が開発した遠隔からシステムを利用するためのプロトコル。

[ii] 「Multiple Vulnerabilities in Cisco ASA Software」
http://www.cisco.com/cisco/web/support/JP/112/1126/1126286_cisco-sa-20141008-asa-j.html

[iii] 「Cisco 社製セキュリティアプライアンスソフトウェアの 脆弱性に関する注意喚起」
https://www.jpcert.or.jp/at/2015/at150021.html

[iv] 「インターネット観測結果等（平成 27 年7月期）」
https://www.npa.go.jp/cyberpolice/topics/?seq=16760

[v] 「Cisco ASA ソフトウェアの SunRPC インスペクションエンジンにおけるサービス運用妨害（DoS）の脆弱性」
http://jvndb.jvn.jp/ja/contents/2014/JVNDB-2014-004661.html