平成 28 年1月 25 日

インターネット観測結果等

（平成 27 年 12 月期）

- 宛先ポート 53413/UDP に対するアクセスが増加
- D-Link 社製ルータの脆弱性の探索が目的と考えられるアクセスを観測

1 宛先ポート 53413/UDP に対するアクセスが増加

定点観測システムでは、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1）。

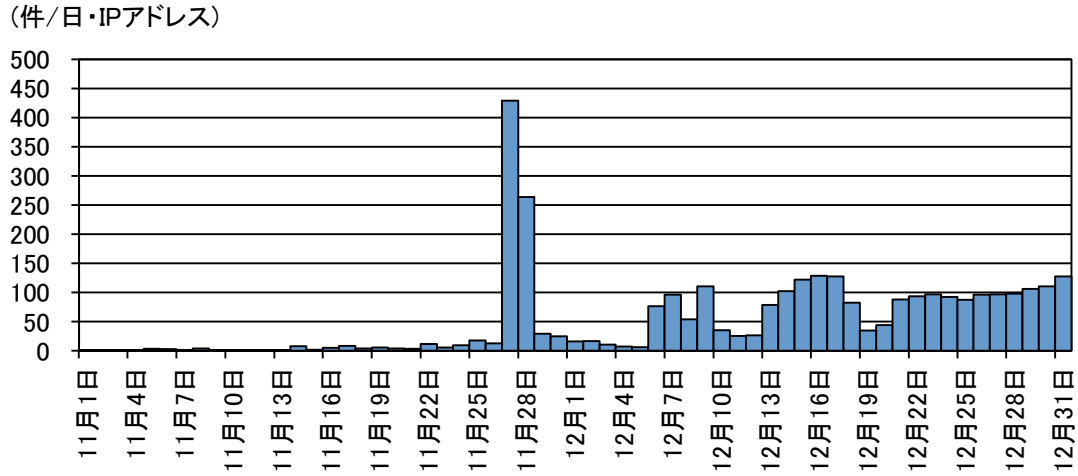

図1　宛先ポート 53413/UDP に対するアクセス件数の推移（H27.11.1～12.31）

53413/UDP は Netis[i]社製のルータで使用されるポートであり、平成 26 年8月にセキュリティ対策企業が外部から簡単にアクセスできる脆弱性[ii]を公表しました。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]して以降継続的に観測しており、平成 27 年8月にはアクセスの増加を観測[iv]しました。

今期は、11 月下旬にアクセスの急増を観測した後、12 月にかけて継続して観測しており、平成 27 年8月のアクセスの増加と比較しても増加率が大きく、Netis 社製ルータの探索行為が更に活発化している可能性があります。また、アクセスの中には当該ルータに対して不正プログラムのダ

---

[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）」（平成 26 年 10 月7日）
http://www.npa.go.jp/cyberpolice/detect/pdf/20141007_2.pdf

[iv] 「インターネット観測結果等（平成 27年8月期）」（平成 27 年9月 25 日）
http://www.npa.go.jp/cyberpolice/topics/?seq=16942

ウンロード及び実行を試みていると思われるものも確認でき、12 月 15 日に注意喚起を実施[i]しました。攻撃に悪用されないために、以下のセキュリティ対策を推奨します。

- 管理用のパスワードは、推測されにくいものに変更する。
- メーカ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。

2 D-Link 社製ルータの脆弱性の探索が目的と考えられるアクセスを観測

D-Link 社製ルータについては、コマンドインジェクションやバッファオーバーフロー等複数の脆弱性が公表[ii]されており、脆弱性が悪用されると第三者から任意のコードが実行されるおそれがあります。また、これらの脆弱性を実証するためのプログラム(PoC[iii])も平成 27 年5月及び 11 月に複数公開されていることを確認しています。

定点観測システムでは、脆弱性のある D-Link 社製ルータの探索が目的と思われるアクセスを、11 月下旬から 12 月上旬にかけて観測しました(図2)。

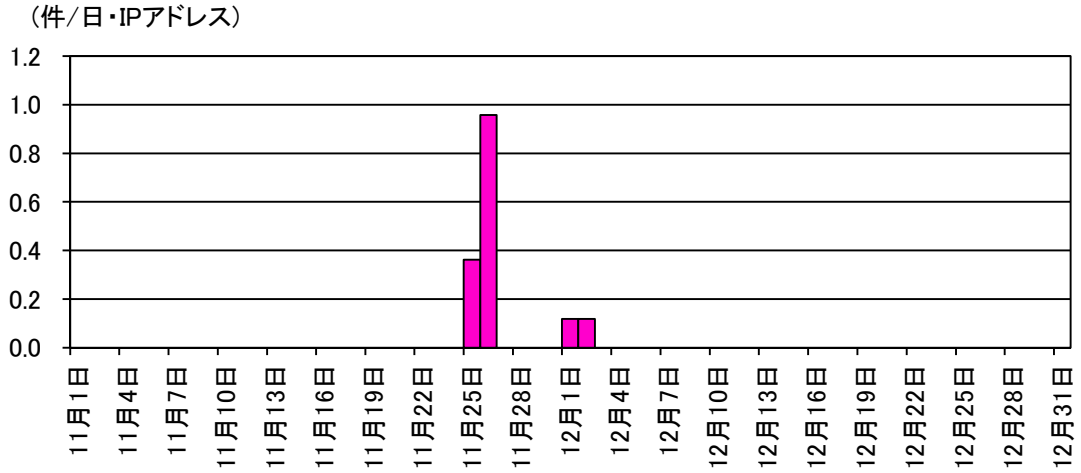

図2 脆弱性のある D-Link 社製ルータの探索が目的と考えられるアクセス件数の推移
(H27.11.1～12.31)

D-Link 社により当該脆弱性に対するパッチが公開されていることから、D-Link 社製ルータを利用する組織や個人においては、最新のパッチが適用されているか確認するとともに、未適用の場

---

[i] 「IoT 機器を標的とした攻撃について」(平成 27 年 12 月 15 日)
http://www.npa.go.jp/cyberpolice/topics/?seq=17323

[ii] 例えば公表されている脆弱性のとして次のものがあります。
「D-Link DIR-645 Wired/Wireless ルータのファームウェアにおける任意のコマンドを実行される脆弱性」
http://jvndb.jvn.jp/ja/contents/2015/JVNDB-2015-001591.html
「D-Link DIR-645 Wired/Wireless ルータのファームウェアにおけるスタックベースのバッファオーバーフローの脆弱性」
http://jvndb.jvn.jp/ja/contents/2015/JVNDB-2015-001592.html

[iii] Proof of Concept の略。脆弱性を利用した攻撃が可能であることを示すためのプログラムのこと。

合は早急に適用することを推奨します。また、ルータを外部からアクセスさせる必要がある場合は、IP アドレスを制限するなどの適切なアクセス制限を実施することを推奨します。