平成 26 年 6 月 27 日

インターネット観測結果等

(平成 26 年 5 月期)

- ビル管理システムに対する探索行為の継続
- BIND の脆弱性に対する探索行為と考えられるパケットの検知

1 ビル管理システムに対する探索行為の検知

3月中旬から検知していた、代表的なビル管理システムである「BACnet」の探索行為と考えられる宛先ポート 47808/UDP に対する「Read-Property」のパケットを、引き続き観測しています（図1）。

警察庁では、4月[i]及び5月[ii]に注意喚起を実施しているので、対策等については、そちらを確認して下さい。

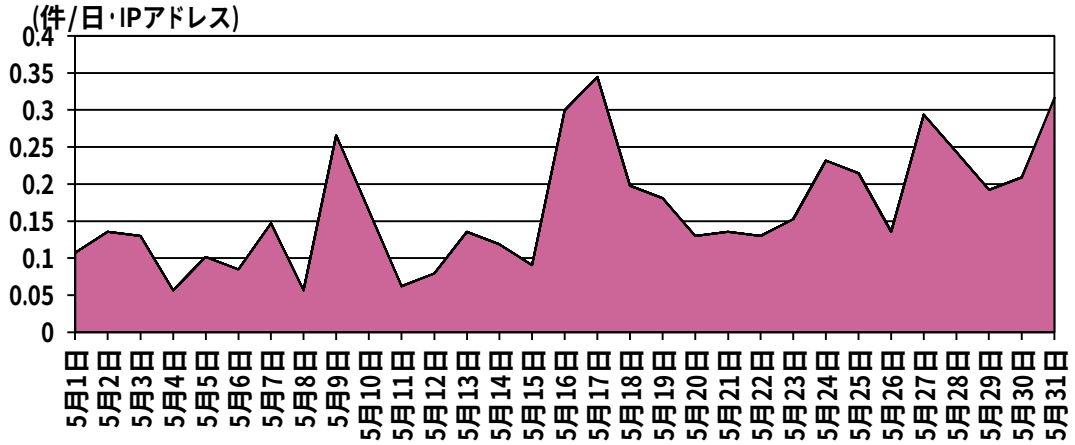

図1　宛先ポート 47808/UDP に対するアクセス件数の推移

[i] 「ビル管理システムに対する探索行為の検知について」（平成 26 年4月4日）
http://www.npa.go.jp/cyberpolice/detect/pdf/20140404.pdf

[ii] 「ビル管理システムに対する探索行為の検知について（第2報）」（平成 26 年5月8日）
http://www.npa.go.jp/cyberpolice/detect/pdf/20140508.pdf

2 BIND の脆弱性に対する探索行為と考えられるパケットの検知

5月8日に BIND の脆弱性（CVE-2014-3214）[i,ii]が公表されました。この脆弱性は、BIND における特定のバージョン（9.10.0）において、特定の属性を持つ応答を返す問い合わせ処理の不具合により、DNS サービスが停止する可能性があるものです。警察庁の定点観測システムにおいては、5月9日以降、BIND のバージョン情報を問い合わせるパケットを継続的に観測しています（図2）。

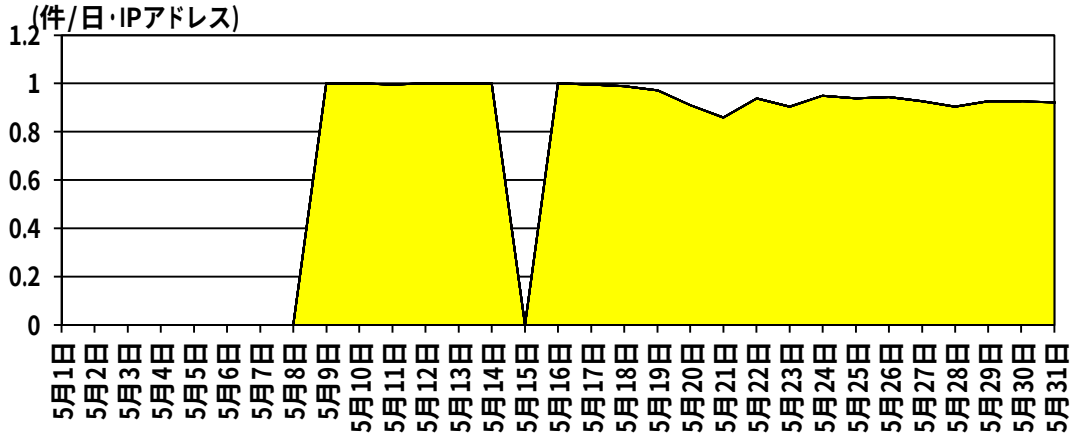

図2　BIND のバージョン情報を問い合わせるパケット数の推移

[i] 「（緊急）BIND 9.10.0 の脆弱性（DNS サービスの停止）について（2014 年5月9日公開）」
http://jprs.jp/tech/security/2014-05-09-bind9-vuln-prefetch.html/

[ii] 「ISC BIND の named のプリフェッチの実装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-2014-002447.html