平成 26 年 7 月 6 日

Topic

ビル管理システムに対する探索行為の検知について（第3報）

6月26日及び7月1日に、ビル管理システムの探索と考えられるアクセスが増加したのを検知しました。当該アクセスは、新たな手法で、広く探索活動を行っている可能性があります。ビル管理システムの管理者は、早期に対策を行うことを推奨いたします。

1 ビル管理システムの探索について

警察庁の定点観測システムでは、3月中旬以降、ビル管理システムの探索と考えられる47808/UDP に対するアクセスを継続して検知しています[1,2]。6月26日及び7月1日には、アクセスの増加を検知しました。当該アクセスを分析したところ、3月中旬以降から継続的に検知している「ReadProperty」のパケットとは異なり、「ReadPropertyMultiple」というBACnetシステムに接続された機器の情報を、一つの命令で複数確認することが可能なパケットで、複数のセンサーで検知されました（図）。

このことから、今回検知したパケットは、新たな手法で、広く探索活動を行っている可能性があります。

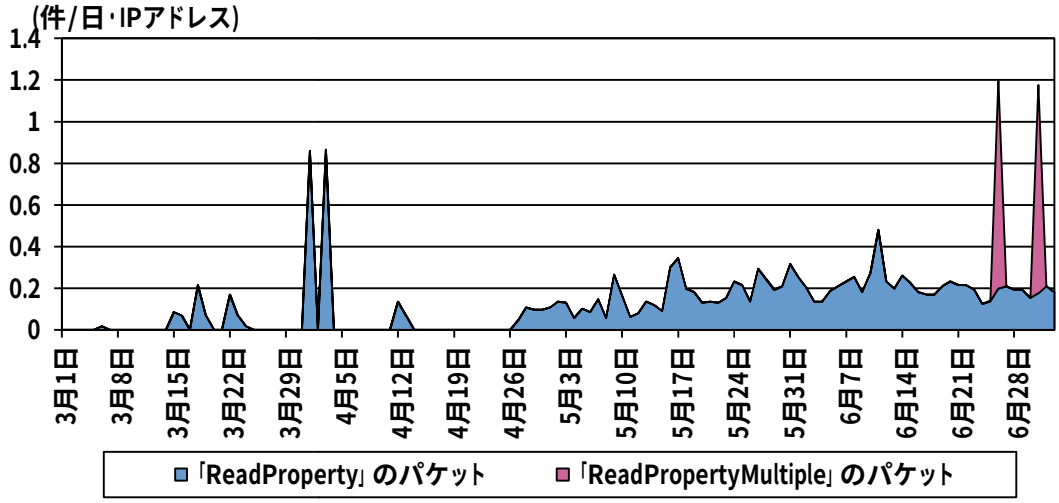

図 ビル管理システムの探索と考えられるアクセス（H26.3.1～H26.7.4）

[1] ビル管理システムに対する探索行為の検知について
http://www.npa.go.jp/cyberpolice/detect/pdf/20140404.pdf
[2] 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）
http://www.npa.go.jp/cyberpolice/detect/pdf/20140508_1.pdf

2 推奨する対策（初版の再掲）

今後、BACnet に留まらず、ビル管理システムを対象とした探索活動や攻撃が発生することも懸念されるため、ビル管理システムの管理者は、以下の対策を実施することを推奨します。

(1) 使用製品の最新セキュリティ情報の確認

ア ソフトウェアのアップデート

イ ハードウェアのファームウェア更新

(2) インターネットへの不要な公開の停止

インターネット上から、システムにアクセスする必要がない場合には、インターネットへの公開を停止する。

(3) ネットワークセキュリティの確認

外部からの接続に対して、適切なアクセス制限が設定されているか確認する。