平成 26 年5月 8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2報）

ツールを使用したビル管理システムの探索が増加しています。複数のホストから、このツールを使用したアクセスが継続的に行われており、今後も、広く探索活動が発生することが懸念されます。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 ツールを使用した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検知していました[1]。このアクセスを分析したところ、BACnetシステムを対象とした探索ツールによるアクセスが大半を占めていることが判明しました（図1）。このツールは、3月下旬に公開されており、実際にツールが動作することを確認しています。4月下旬以降は、複数のホストから、このツールを使用したアクセスが継続的に行われており、今後も、広く探索活動が発生することが懸念されます。

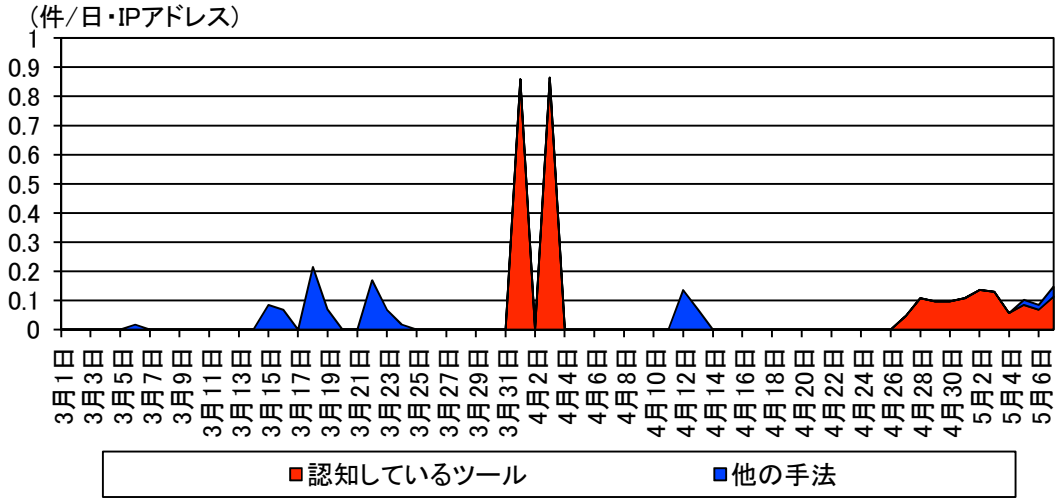

図1 探索ツールを使用したビル管理システムの探索と考えられるアクセス
（H26.3.1～H26.5.7）

[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 推奨する対策（初版の再掲[1]）

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。