Distributed via @police http://www.npa.go.jp/cyberpolice/

平成 26 年4月 4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

ビル管理システムを探索していると考えられるパケットを検知しています。ビル管理システムが攻撃を受けた場合、システムを任意に操作される恐れがあります。事前に必要な対策を実施することを推奨します。

1 宛先ポート 47808/UDP に対するアクセスの検知について

警察庁の定点観測システムでは、3 月中旬以降、宛先ポート 47808/UDP に対するアクセスを検知しています（図1）。47808/UDP は、ビル管理システムで使用される通信プロトコル用標準規格「BACnet」で定義されているポートであり、このアクセスは、BACnet に基づいて構成されたシステム（BACnet システム）を探索している可能性があります。

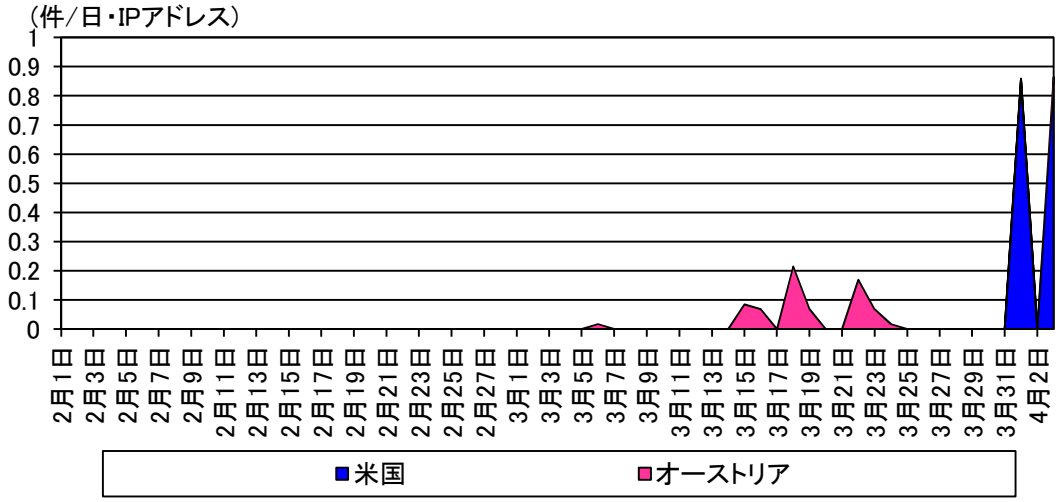

図1 宛先ポート 47808/UDP に対する発信元国・地域別アクセス件数の推移
（H26.2.1～H26.4.3）

同アクセスを分析したところ、BACnet システムに接続された機器の情報を確認する「Read-Property」のパケットであり、BACnet システムの探索行為であると考えられます。過去には、BACnet に関連するソフトウェアの脆弱性が報告されており[1,2]、攻撃を行うための調査を行っている可能性も考えられます。

[1] 「JVNVU#757804 Cisco Network Building Mediator 製品群に複数の脆弱性」（平成 22 年6月3日）
https://jvn.jp/vu/JVNVU757804/

[2] 「JVNVU#660688 SCADA Engine BACnet OPC Client におけるバッファオーバーフローの脆弱性」（平成 23 年2月7日）
https://jvn.jp/vu/JVNVU660688/

Copyright 2014 Cyber Force Center, NPA JAPAN

2　攻撃者によるビル管理システムへの侵入

ビル管理システムは、インターネットを介した遠隔監視等が可能です。適切な対策を施さずにビル管理システムをインターネットに接続している場合、攻撃者に進入され、システムを任意に操作される恐れがあります。

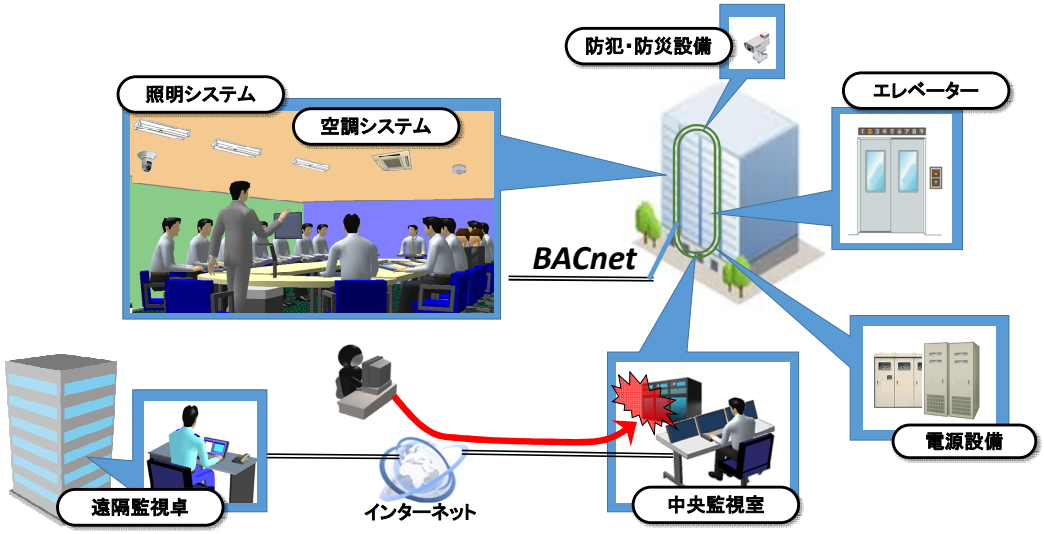

図2　攻撃者によるビル管理システムへの侵入

3　推奨する対策

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。

Copyright 2014 Cyber Force Center, NPA JAPAN