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

平成 27 年 10 月 14 日

Topic

# 産業制御システムで使用される国内メーカー製の特定の PLC を標的としたアクセスの観測について

国内のメーカーが製造する特定の PLC[i]を標的としたアクセスを継続して観測しています。これらのアクセスは特定の PLC の探索を試みているものと考えられることから、システムの管理者は、管理する機器の設定を確認し適切な対策を行うことを推奨します。

## 1 国内メーカー製の特定の PLC を標的としたアクセスの観測について

警察庁の定点観測システムでは、3月下旬頃から、国内メーカー製の特定の PLC（以下「特定 PLC」という。）で使用されるポートに対して複数の発信元からのアクセスを継続して観測しています。

この特定 PLC では、管理ソフトウェアとの接続に 5006/UDP、5007/TCP 等のポートが使用されます。これらのポートにアクセスして特定 PLC に係る情報を取得するツールがインターネット上に公開されていることを確認しています。

定点観測システムにおいて観測したアクセスを分析したところ、このツールの特徴を示すパケットを多数観測しています（図1）。

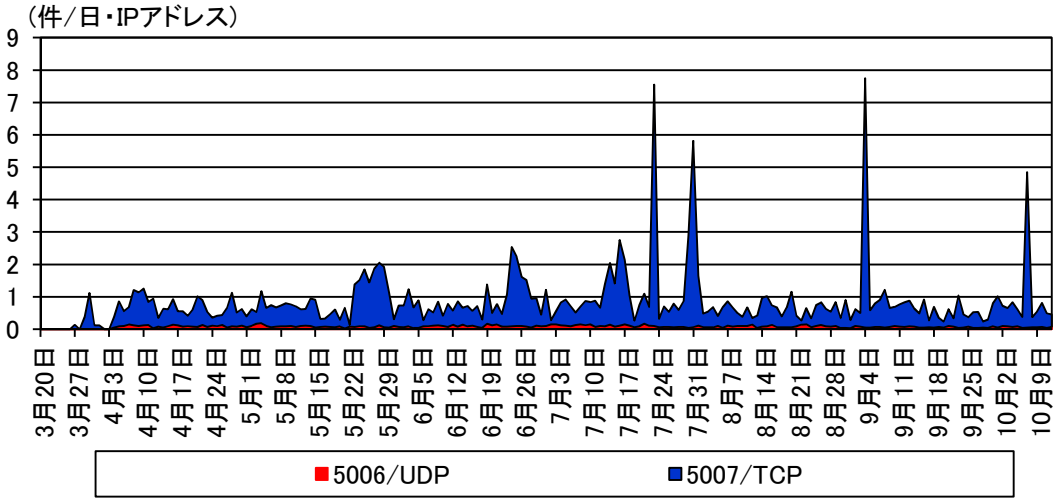


図1 特定 PLC を標的とした宛先ポート別アクセス件数の推移（H27.3.20～10.12）

これらのアクセスについては、インターネット上に接続されている機器に関する情報を収集及びデータベース化し、インターネットからの検索を可能にする Web サービスを提供する組織からのアクセスを継続して観測しています。

[i] PLC（Programmable Logic Controller の略）とは、プログラム可能なフィールド機器（バルブ、メータ、ファン等）の監視・制御装置のこと。

Copyright 2015 Cyber Force Center, NPA JAPAN

この検索サービスを提供する組織のウェブサイト（以下「検索サイト」という。）から特定のPLCに関する情報を検索したところ、日本に割り当てられたIPアドレスが複数表示されることを確認しています（図2）。

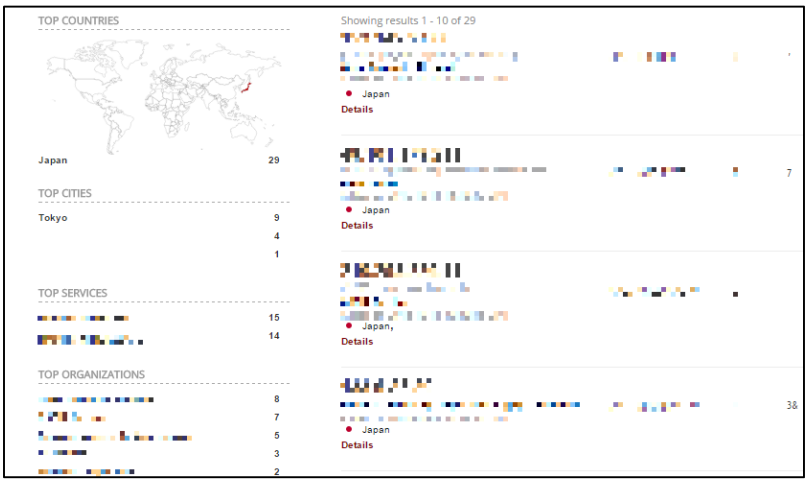


図2　特定 PLC の検索結果

この検索サイトが悪用されると、検索された機器やシステムが攻撃の標的となり被害を受ける可能性も考えられます。

## 2　対策

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。

- 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不要な公開を停止する。
- インターネット側からアクセスする場合には、不特定の IP アドレスからは接続できないように、適切なアクセス制限を実施する。

その他、管理する機器の状況を確認するため、検索サイトを活用し[i]意図せずにインターネットに公開されていないか確認することも有効です。

[i] IPA テクニカルウォッチ「増加するインターネット接続機器の不適切な情報公開とその対策」（IPA）
https://www.ipa.go.jp/security/technicalwatch/20140227.html
SHODAN を悪用した攻撃に備えて　－制御システム編－（JPCERT/CC）
https://www.jpcert.or.jp/ics/report0609.html

Copyright 2015 Cyber Force Center, NPA JAPAN