平成 28 年5月 27 日

インターネット観測結果等

（平成 28 年4月期）

- CCTV システムを標的としたアクセスを観測
- 国内メーカー製の特定の PLC[i]を標的としたアクセスの増加

1 CCTV システムを標的としたアクセスを観測

CCTV(Closed-Circuit-Television)システムとは、特定の建物や施設内での有線テレビで用いられ、主に監視カメラのモニターとして使われるシステムです。

平成 28 年3月下旬に、海外のセキュリティブログにおいて、インターネットに接続されている CCTV システムが不正に操作され、任意のコマンドが実行される脆弱性が公表されました。当該脆弱性は細工された HTTP GET リクエストを送信することにより、任意のコマンドを実行できるというものです。前述のセキュリティブログには、当該脆弱性を実証するための具体的な手順も示されていました。

警察庁の定点観測システムにおいては、4月3日から4月 14 日にかけて当該脆弱性を標的としていると考えられるアクセスを観測しました（図1）。

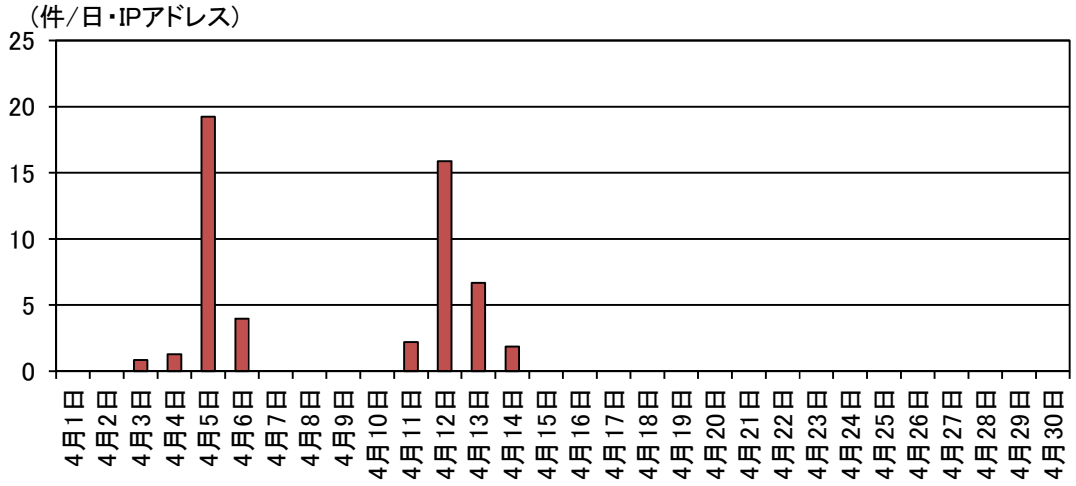

図1 CCTV システムに対する脆弱性を標的としたアクセス件数の推移

当該アクセスは、脆弱性が存在する CCTV システムに対して実際にコマンドを送っているものがほとんどでした。また、含まれていたコマンドの内容としては、ネットワーク通信で用いられる nc コマンド及びファイル内容を表示させるcatコマンドがほとんどでした。特に、nc コマンドは特定の

[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。

IP アドレス及びポート番号を指定しているものが多くみられました(図2)。

図 2　観測したアクセスの例(内容の一部についてはマスキングを実施)

システム管理者には、利用している CCTV システムの状況を確認し、インターネットからの通信を遮断したり、外部からアクセスさせる必要がある場合は、適切なアクセス制限を実施したりするなどの対策を実施することを推奨します。

2　国内メーカー製の特定の PLC を標的としたアクセスの増加

警察庁の定点観測システムでは、平成 27 年 10 月[i]に観測した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するアクセスの増加を再度観測しました。

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は、このツールの特徴を示すパケットを4月中旬ごろから多数観測しています(図3)。

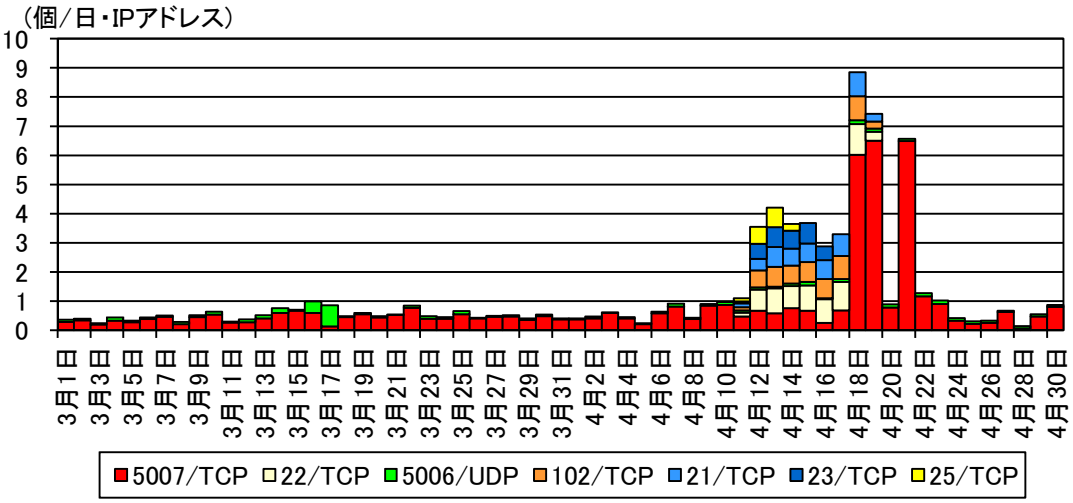

図3　特定 PLC を標的とした宛先ポート別アクセス件数の推移(H28.3.1～4.30)

4月中旬までのアクセスは、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

[i] 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
https://www.npa.go.jp/cyberpolice/detect/pdf/20151014.pdf

びデータベース化し、インターネットからの検索を可能としたWebサービスを提供する組織からのアクセスがほとんどでした。しかし、今回のアクセス増加については、前述の組織とは異なる複数の発信元からのアクセスが増加していました。これらの発信元は複数のポートにアクセスしているため、脆弱性の探索を行っていると考えられます。そのため、システムの管理者には、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