JPCERT CC®

SHODAN を悪用した攻撃に備えて

ー制御システム編ー

一般社団法人 JPCERT コーディネーションセンター
制御システムセキュリティ対策グループ

2015 年 6 月 9 日
(初版)

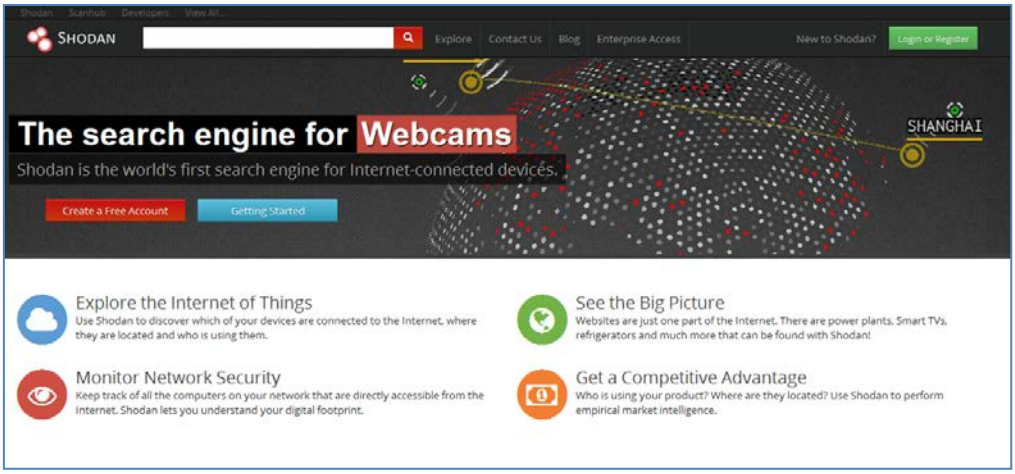
1 SHODAN とは？

1.1 SHODAN とは？

SHODAN とは、インターネット上に公開されている様々な機器(表 1 参照)に関する情報をデータベース化し、インターネット上のサービスとして検索可能にする Web サービスです。例えば、インターネットに公開されている Web サーバを検索したいときは、SHODAN の Web サービス(https://www.shodan.io)にアクセスし､対象のドメイン名やIPアドレス＋ポート番号80(または443)を指定して検索することで、目的の Web サーバの情報を取得することができます。また、特定プロトコルのポート番号を指定して検索することで、そのプロトコルをサポートする世界中の機器をリストアップすることもできます。

SHODAN は、インターネットの全域に対してデータ収集のための探索を行っていると考えられ、そのためインターネットからアクセス可能な状態で設置されている機器は、設置者の意図にかかわらず SHODAN のデータベースに登録されている可能性があります。

一般に、リクエストに対してレスポンスを返すような通信機能を搭載した機器は、送付するリクエストを工夫し、返ってくるレスポンスに含まれる情報を分析することにより、遠隔からネットワーク経由で機器(搭載され稼働しているソフトウェアを含む)の種類や一部の設定情報を割り出すことができます。SHODAN は、種々のプロトコルでインターネット・アドレスの全域にわたって網羅的に接続を試みて得られた情報を整理してデータベース化しています。



[図 1　SHODAN トップページ(https://www.shodan.io)]

[表 1　SHODAN で検索可能な機器例]

Web サーバ	Web カメラ
ルータやスイッチ	NAS
複合機	NW 対応家電（TV・レコーダなど）
ビル管理システム	制御システム（HMI/PLC など）

1.2 SHODAN の制御システムへの対応

当初、SHODAN は各種サーバ、ネットワーク機器といった一般的な IT 機器を検索対象としてデータベースに情報を蓄積していました。その後、プラントなどで使用される制御システムにも対応しました。表 2 に主に SHODAN が対応する制御システム関連プロトコルの一例を示します。

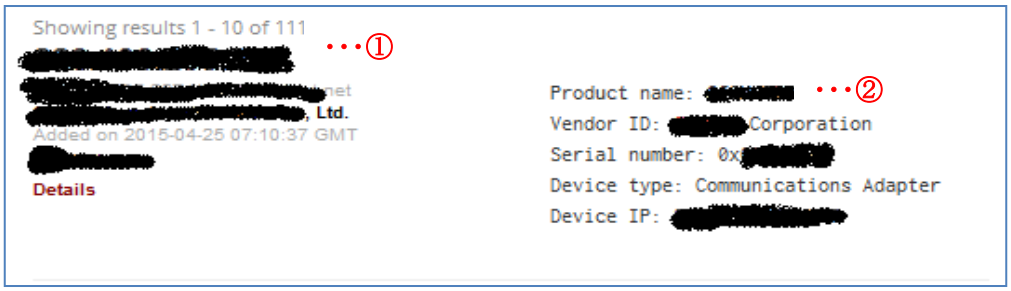
[表 2　SHODAN が対応する制御システム関連プロトコル例]

プロトコル名称	ポート番号/プロトコル(tcp/udp)
EtherNet/IP	44818/tcp,udp
Modbus	502/tcp
DNP3	20000/tcp,udp
BACnet	47808/udp
CodeSys	1200/tcp,udp , 2455/tcp,udp
HART-IP	5094/tcp,udp
Omron FINS	9600/tcp,udp

これらプロトコルをサポートする制御システムをインターネットからアクセス可能な場所に設置している場合は、SHODAN のデータベースに制御システムが登録されてしまっている可能性があります。

1.3 SHODAN を使用した検索例

SHODAN を使用して、制御システム関連製品を検索した結果の表示例を[図 2]に示します。



[図 2　SHODAN での検索結果例]

① ：IP アドレス関連情報(IP アドレス、プロバイダ名、地域情報など)
② ：製品関連情報(製品名、ベンダ名、シリアル番号、デバイスタイプ、IP アドレス)
※検索結果の表示内容は、検索対象のプロトコル、製品などにより異なります。

2 SHODAN を使用した「制御システムへの攻撃」について

SHODAN は、使い方によっては攻撃対象となる制御システムの探索に悪用することができます。攻撃者は、SHODAN を使用して脆弱な制御システムを探索し、攻撃を仕掛けることができます。特に、制御システムは、セキュリティパッチが適用されていなかったり、適切なアクセス制御が行われていないケースが多かったりするため、攻撃が行われるとシステムの停止など、可用性に大きな影響を及ぼしかねません。

以下に、攻撃シナリオの一例を示します。

CASE:1　不特定のアセットオーナを対象とする攻撃例

- 脆弱性情報や攻撃ツールなどから、攻撃対象とする制御システムを選定する
- 攻撃対象の制御システムを SHODAN で検索するためのキーワード(ベンダ名、機種名など)を選定する
- 選定したキーワードを SHODAN で検索する
- 検索結果としてリストアップされた対象機器の IP アドレスに対して、攻撃ツールなどを使用して情報収集または攻撃を実行する

CASE:2　特定のアセットオーナを対象とする攻撃例

- 何らかの方法で攻撃対象の IP アドレスを特定する
- SHODAN にて、攻撃対象の IP アドレスをキーワードに検索する
- 攻撃対象で稼働するサービス一覧から、攻撃可能なサービスに対して攻撃を仕掛ける

攻撃対象となり得るのは、インターネットからアクセス可能な制御システムで、かつアクセス制御を行っていない制御システムに限ります。（インターネットからアクセスができない、またはアクセス制御により特定の対象以外と通信ができない制御システムは、SHODAN のデータベースには登録されません。）

3 アセットオーナが行うべき対策

2 章で示したように、SHODAN を使用すれば比較的容易に制御システムを探しだすことが可能です。まずは、自社の制御システムが SHODAN で検索され得る状態にないか確認してください。

(確認手順)

1) インターネット接続をしているネットワーク機器のグローバル IP アドレスを調べる
2) 調べた IP アドレスを SHODAN で検索する
3) 検索結果に自社の制御システムに関する情報が含まれていないか確認する

もし、検索結果に自社のシステムが表示された場合は、その機器の認証機能の有無やパスワードの強度など、不正アクセスされる危険性がないか調査してください。

※SHODAN は、定期的に機能アップしているため、今後も対応するプロトコルの追加や精度の向上が図られる可能性があります。このため、定期的な確認作業を推奨します。

具体的な対策については、以下の独立行政法人情報処理推進機構(IPA)の資料をご参照ください。

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」
～「SHODAN」を活用したインターネット接続機器のセキュリティ検査～
https://www.ipa.go.jp/files/000036921.pdf

4 おわりに

本資料を作成している 2015 年 5 月の時点で SHODAN を悪用した攻撃が国内で発生したという情報はありませんが、水面下で将来の攻撃のための情報収集に使用されている可能性は否定できません。制御システムでは、何らかの事故が起きた場合に人命にも影響することがあるため、できる限りの対策をとることが望まれます。