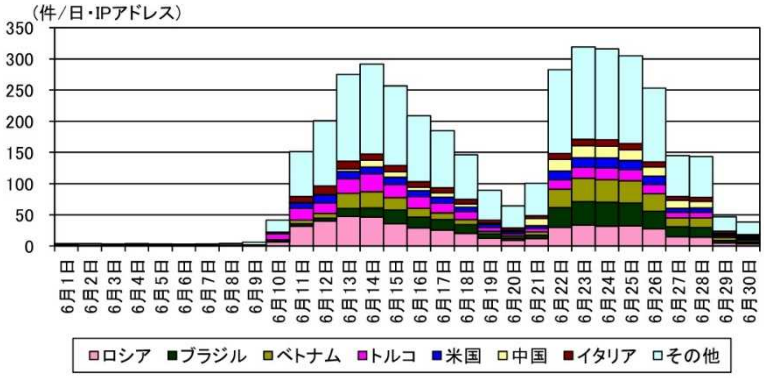
モノづくりプリザーブ
Preservation for Industries in kyoto
モノプリ・ニュース！ 第31号

IoT機器へのサイバー攻撃に注意！！

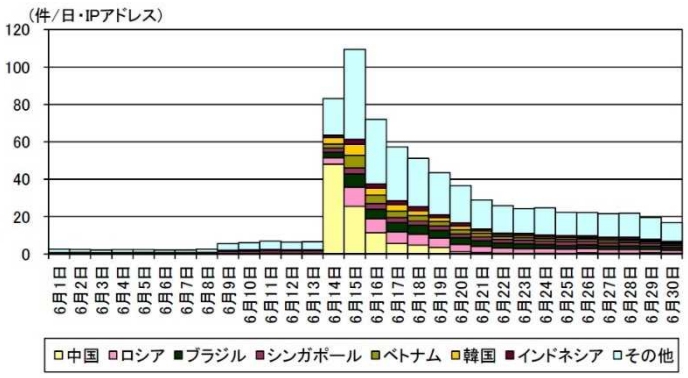
Miraiボットからのアクセス増加中！

６月10日以降、宛先ポート80/TCP及び8000/TCPに対するMiraiボットの特徴を持ったアクセスが増加しています。

警察庁@police 「宛先ポート80/TCP、8080/TCP、8888/TCP等に対するアクセスの増加について」
https://www.npa.go.jp/cyberpolice/detect/pdf/20180613.pdf参照



80/TCPに対するアクセス



8080/TCPに対するアクセス

発信元を調査したところ、多くでネットワークビデオレコーダ等の様々なIoT機器に搭載されているWebサーバソフトウェア「XiongMai uc-httpd」が稼働していました。

Miraiボットとは

Mirai及びその亜種に感染し、攻撃者の命令を受け付け、遠隔操作が可能となった状態のIoT機器をMiraiボットと呼んでいます。
平成28年10月、米国で発生した大規模なDNSサーバへのDDoS攻撃でもMiraiボットが使用されたといわれています。

対策

- IoT機器を直接インターネットに接続せず、ルータを使用する。
- ファイアーウォール等によって不必要な外部からのアクセスを遮断し、特定のIPアドレスからのみ、アクセスを許可する。
- ユーザ名及びパスワードは、初期設定のままで使用しない。
- 製造元のウェブサイト等でぜい弱性情報を確認し、ぜい弱性がある場合はアップデートを行う。

京都府警察本部モノづくりプリザーブ事務局　075-451-9111(内線 5821)