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

平成 28 年6月 18 日

インターネット観測結果等

（平成 28 年5月期）

- Docker API に対するアクセスが急増
- H.323 プロトコルに使用される宛先ポート 1720/TCP 及び 11720/TCP に対するアクセスが増加

1 Docker API に対するアクセスが急増

コンテナ型仮想実行環境の管理ソフトウェアである Docker には、遠隔からネットワーク経由での操作も可能となる API[i]が準備されています。同 API には、初期設定では UNIX ドメインソケット[ii]が使用されますが、設定を変更することにより、任意の TCP ポートで待ち受けを行いネットワーク経由での操作を行うことが可能です。この際に使用されるポートとして、暗号化されない通信のために 2375/TCP が、SSL（TLS）で暗号化された通信のために 2376/TCP が IANA に登録[iii]されています。

警察庁の定点観測システムにおいては、平成 27 年6月以降、宛先ポートを 2375/TCP とした Docker API に対するアクセスを断続的に観測していましたが、平成 28 年5月 25 日から 29 日の間に同アクセスの急激な増加を観測しました（図1及び図2）。

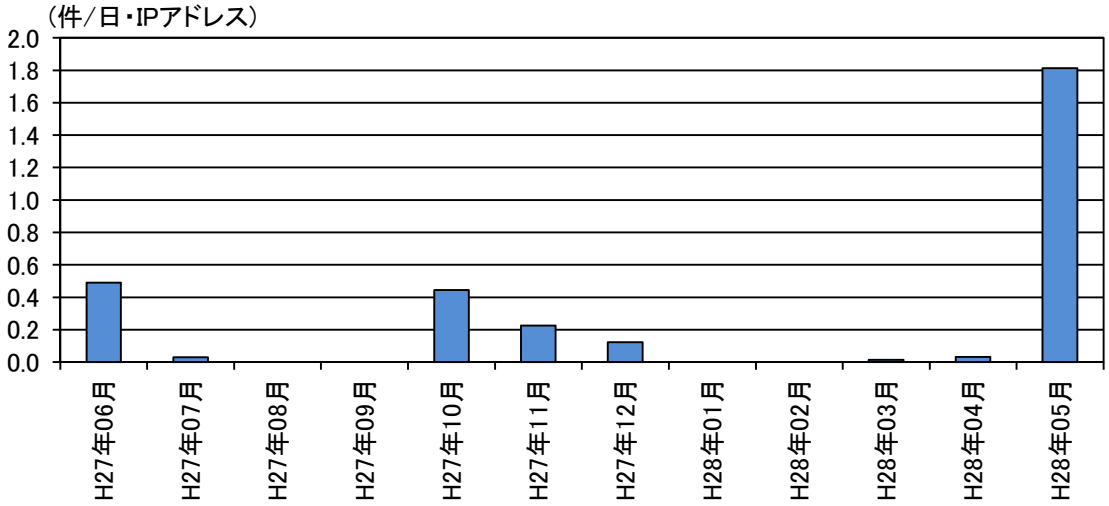

図1 宛先ポートを 2375/TCP とする Docker API に対するアクセス件数の月別推移
（H27.6.1～H28.5.31、1日当たりの平均値）

[i] https://docs.docker.com/engine/reference/api/docker_remote_api/

[ii] Linux（UNIX）において、同一 OS 内で動作しているプロセス間で通信を行うための仕組みの一種。

[iii] http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml?search=docker

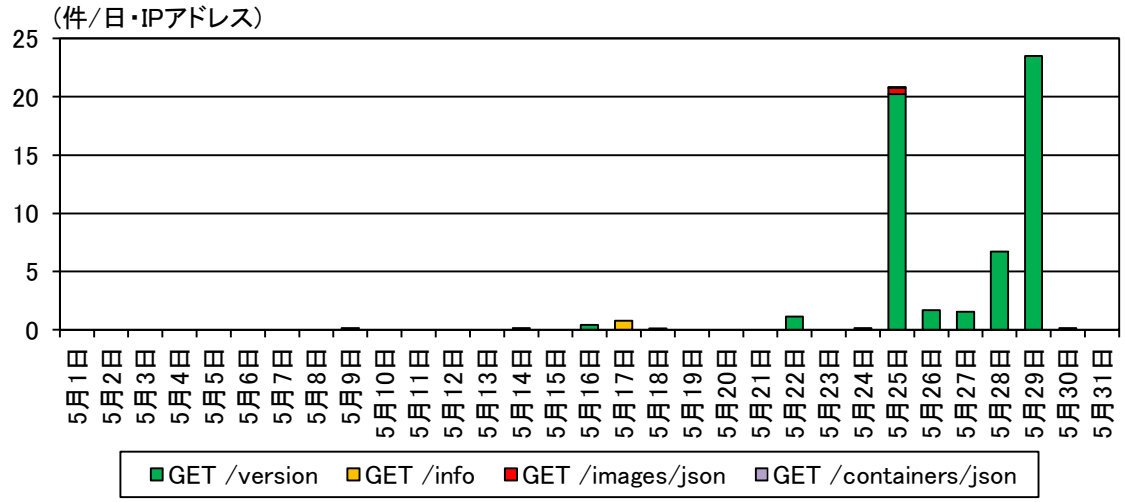

図2　宛先ポートを 2375/TCP とする Docker API に対するアクセス件数の API 種別ごとの推移

観測したアクセスは、Docker API を用いて、Docker のバージョン情報や、Docker が稼動しているサーバの情報、コンテナやコンテナイメージの情報をリクエストするものでした（表1）。これらのアクセスは、外部からアクセス可能な API を探索したり、API を通じて情報の窃取を試みる目的があると考えられます。

表1　今期に観測した Docker API に対するアクセス

API 種別	観測したリクエスト	API の用途
GET /version	GET /version HTTP/1.1	Docker のバージョン情報を取得する。
GET /info	GET /info HTTP/1.1	Docker が稼動しているサーバの情報を取得する。
GET /images/json	GET /images/json HTTP/1.1	コンテナイメージの情報を取得する。
	GET /v1.18/images/json HTTP/1.1	
GET /containers/json	GET /containers/json HTTP/1.1	コンテナの情報を取得する。
	GET /containers/json?all=1 HTTP/1.1	

さらに、外部から Docker API に対してアクセスできることが判明した場合には、攻撃者が API を悪用して、外部からコンテナを不正に作成し攻撃の踏み台等として悪用したり、ホストマシンへの侵入を行う危険性も考えられます。このため、Docker を利用している場合には、以下の対策を実施することを推奨します。

- ネットワーク経由で外部から、Docker API にアクセスできるように設定されていないか確認する。

- API に外部からアクセスする必要がない場合には、外部からの接続を遮断する。
- 外部から API による操作を行う必要がある場合には、特定の IP アドレスのみに接続を許可する、VPN 経由でのアクセスに制限する等の適切なアクセス制限を実施する。
- 不特定の IP アドレスから API にアクセスする必要がある場合には、証明書による認証[i]を実施する。

[i] https://docs.docker.com/engine/security/https/

2 H.323 プロトコルに使用される宛先ポート 1720/TCP 及び 11720/TCP に対するアクセスが増加

今期は、1720/TCP 及び 11720/TCP を宛先ポートとするアクセスの増加を観測しました。1720/TCP 及び 11720/TCP はテレビ電話等の音声・動画通信用のプロトコルである H.323 において使用されるポートです。同ポートに対するアクセスの内容を確認したところ、H.323 による呼の確立を試みる「Call Signalling」メッセージを含むアクセスが多数を占めていました（図3）。

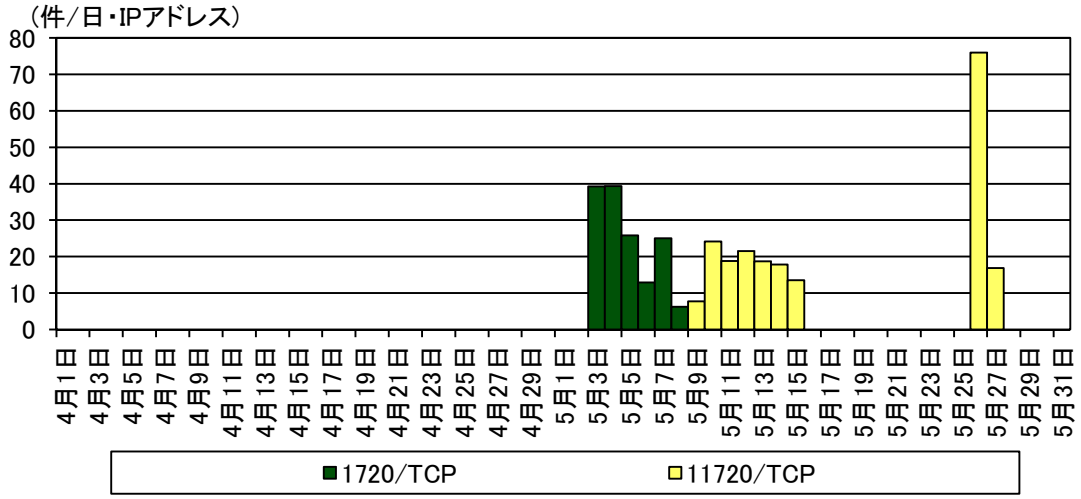

図3 宛先ポート 1720/TCP 及び 11720/TCP に対する「Call Signalling」メッセージを含むアクセス件数の推移（H28.4.1～5.31）

同アクセスの内容を確認したところ、発信元機器のプロダクト ID が同一の名称となっているなど、複数の共通点が見られました。また、アクセスの発信元を確認したところ、同時期に多数の IP アドレスから接続が行われており（図4）、当該 IP アドレスに対してウェブブラウザで 80/TCP ポートにアクセスすると、その約8割で IP 電話交換機用のソフトウェアである「Asterisk」の設定・管理用ツールである「FreePBX」の管理画面が表示されました（図5）。

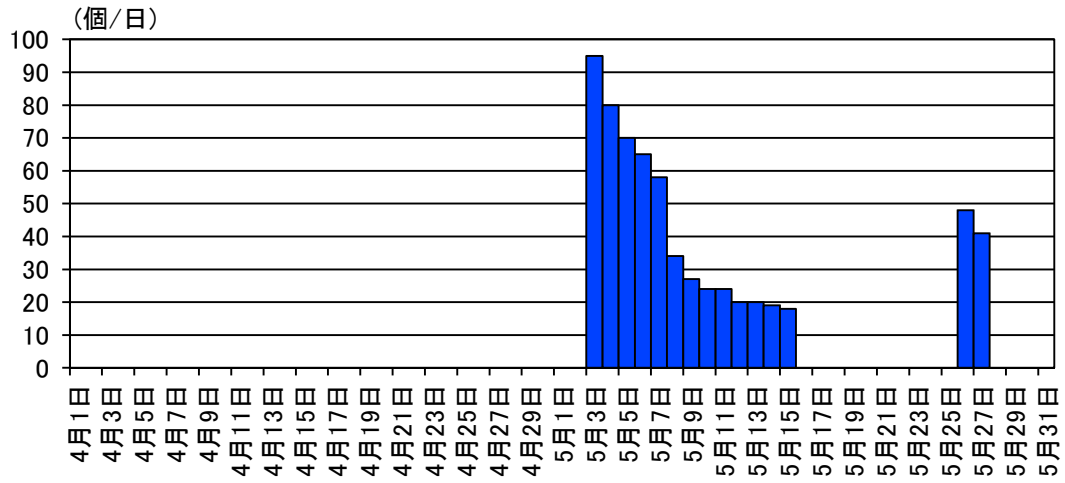

図4「Call Signalling」メッセージを含むアクセスの発信元 IP アドレス数の推移
（H28.4.1～5.31）

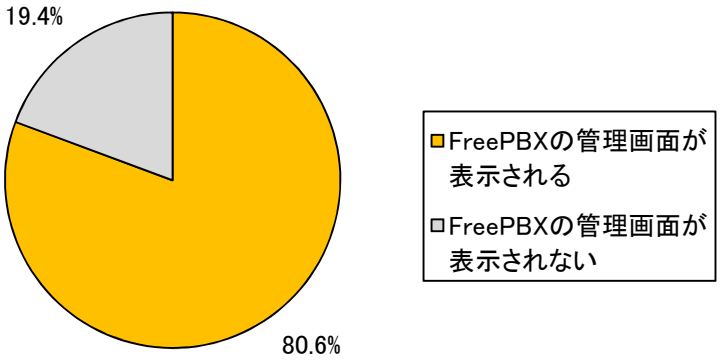

図5「Call Signalling」メッセージを含む発信元 IP アドレスのうち、FreePBX の管理画面が表示される比率

FreePBX には過去に重大な脆弱性[i]が複数公表されており、適切な対策を実施していない場合、第三者に任意のコードを実行される可能性があります。このことから、攻撃者が FreePBX の脆弱性を悪用して、これら発信元 IP アドレスのホストに対して不正な操作を行い、踏み台として悪用している可能性も考えられます。このため、FreePBX を使用している場合には、以下の対策を実施することを推奨します。

[i] 「FreePBX の admin/libraries/view.functions.php における任意の PHP コードを実行される脆弱性」
http://jvndb.jvn.jp/ja/contents/2014/JVNDB-2014-001428.html
「FreePBX の recordings/misc/callme_page.php における任意のコマンドを実行される脆弱性」
http://jvndb.jvn.jp/ja/contents/2012/JVNDB-2012-004164.html

- FreePBX を最新バージョンにアップデートする。
- FreePBX の管理画面に対する外部からのアクセスを遮断する、特定の IP アドレスのみに許可する等の適切なアクセス制限を実施する。

また、警察庁においては IP 電話の不正な利用等が目的と考えられる SIP の探索行為について繰り返し注意喚起[i]を実施しています。今回の 1720/TCP 及び 11720/TCP に対するアクセスについては攻撃者の意図は明らかではありませんが、H.323 においても意図せずに第三者から悪用されることを未然に防止するために、前述の注意喚起を参照して同様の対策を実施することを推奨します。

[i] 「5060/UDP に対するアクセスの増加について」（平成 22 年7月 14 日）
http://www.npa.go.jp/cyberpolice/detect/pdf/20100714.pdf
「SIP サーバの探索と考えられるアクセス増加の注意喚起について」（平成 25 年9月6日）
http://www.npa.go.jp/cyberpolice/detect/pdf/20130906.pdf
「SIP サーバの探索と考えられるアクセスの増加について」（平成 28 年 3 月 10 日）
http://www.npa.go.jp/cyberpolice/topics/?seq=17865