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

令和元年12月25日

レポート

DockerAPIを標的とした探索行為の増加等について

- DockerAPIを標的とした探索行為の増加
- リモートデスクトップの脆弱性(CVE-2019-0708)を標的としたアクセスの増加
- 宛先ポート26/TCPに対するMiraiボットの特徴を有するアクセスの増加

1 DockerAPIを標的とした探索行為の増加

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]が提供されています。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は、暗号化されない通信として2375/TCPが、SSL(TLS)で暗号化された通信として2376/TCPが、Docker Swarm[iii]のRPCインターフェイス用として2377/TCPがIANAに登録[iv]されています。また、IANAには登録されていませんが、4243/TCPがDockerにおいて使用されることもあります。

警察庁のインターネット定点観測においては、令和元年11月上旬から宛先ポート2375/TCP、2376/TCP、2377/TCP及び4243/TCPに対するアクセスの増加を観測しました(図1)。

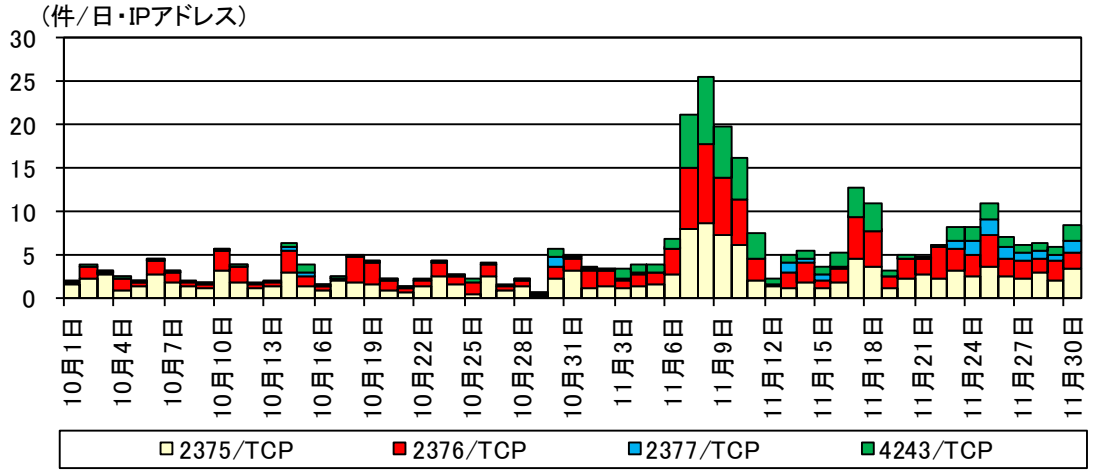

図1 宛先ポート2375/TCP、2376/TCP、2377/TCP及び4243/TCPに対するアクセスの推移(R1.10.1～11.30)

[i] https://docs.docker.com/develop/sdk/

[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] 標準Docker APIで操作できるクラスタリング用ツール。

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

観測したアクセスは、Docker API を用いて、Docker のバージョン情報取得をリクエストするものがほとんどでした（図2）。

図2　観測したアクセスの例（一部マスキング）

今回観測したアクセス等の稼働状況の調査により、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。Docker は、これまで多くの脆弱性が発見されており、最近では令和元年7月に Docker のコードインジェクションの脆弱性が公表[i]され、同年 11 月には、この脆弱性の検証結果が公表[ii]されています。また、セキュリティニュースサイトにて、Docker API に対する探索行為が増加しており、不正プログラムにより暗号資産の採掘に悪用されていると報道[iii]されています。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。

- 公開されている修正プログラムを適用し、ソフトウェアを最新の状態にしてください。
- 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してください。
- 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してください。
- 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してください。また、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してください。
- 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[iv]を実施してください。

---

[i] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-14271

[ii] Docker、これまでで最も深刻な cp コマンドの脆弱性 CVE-2019-14271 を修正（paloalto NETWORKS）
https://unit42.paloaltonetworks.jp/docker-patched-the-most-severe-copy-vulnerability-to-date-with-cve-2019-14271/

[iii] A hacking group is hijacking Docker systems with exposed API endpoints（ZDNET）
https://www.zdnet.com/article/a-hacking-group-is-hijacking-docker-systems-with-exposed-api-endpoints/
ハッカーグループ、不用心な Docker（ドッカー）環境を求め大規模スキャン 仮想通貨モネロの不正マイニングが目的（COINTELEGRAPH）
https://jp.cointelegraph.com/news/hackers-mass-scanning-web-for-docker-platforms-to-mine-cryptocurrencies

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

2 リモートデスクトップの脆弱性（CVE-2019-0708）を標的としたアクセスの増加

警察庁のインターネット定点観測において、令和元年5月以降から散発的に観測していたMicrosoft Windows の遠隔操作に使用するリモートデスクトップサービスの脆弱性（CVE-2019-0708）を標的としたアクセスですが、令和元年 10 月以降から当該アクセスの増加を観測しました（図3）。

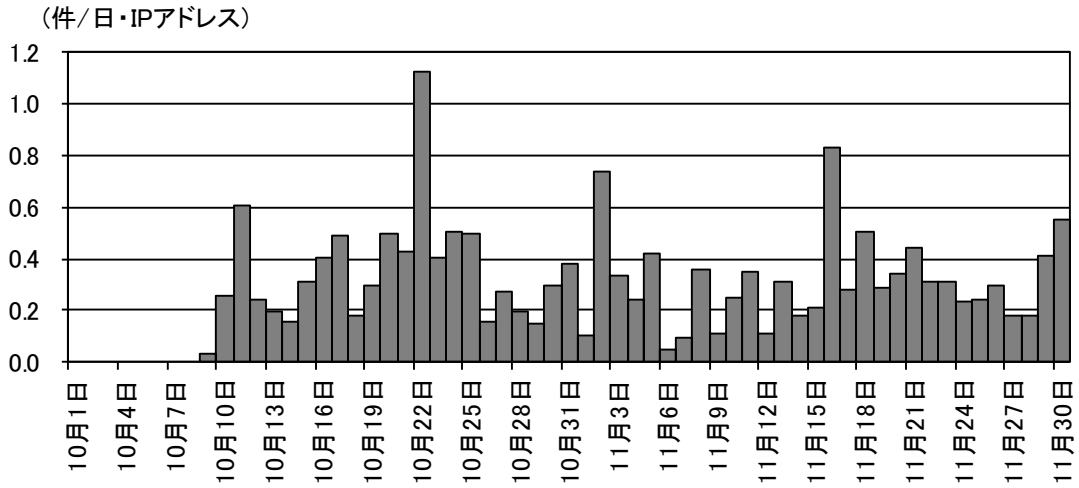

図3 リモートデスクトップサービスの脆弱性（CVE-2019-0708）を標的としたアクセスの推移（R1.10.1～11.30）

当該脆弱性は通称「BlueKeep」と呼ばれており、攻撃対象のシステムに細工した接続要求を送信することで、任意のコードを実行することが可能とされています。当該脆弱性が公表された後、既に特定の条件でブルースクリーンを発生させる検証コード（PoC [i]）が存在していることを確認しています。また、当該脆弱性の存在を確認するためのリモートスキャンツールがインターネット上に公開されています。

今回のアクセスでもリモートデスクトップの接続要求において、特定の通信チャネルの文字列を含むパケットを観測しています（図4）。

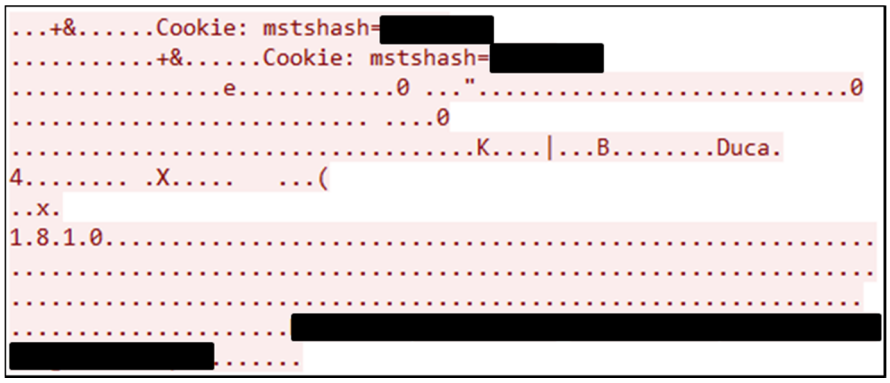

図4 観測したアクセスの例（一部マスキング）

[i] Proof of Concept の略。

また、同アクセスのうち、IP ヘッダの TTL 値が 100 以上 120 以下のアクセスが多かったことから、着信元（送信元）となっている機器の多くは Microsoft Windows が動作していると考えられます。

マイクロソフト社によると、当該脆弱性は既に悪用され、その認知件数は増加傾向[i]であることから、改めて確認するよう注意喚起[ii]を行っています。今のところ、暗号資産の採掘を実施する不正プログラムへの感染を狙う攻撃を観測しているとのことでしたが、今後、当該脆弱性を悪用した自己増殖機能を有する不正プログラムに組み込まれ、被害が拡大する危険性があります。

リモートデスクトップサービスの利用者は、改めて以下の対策を参考にセキュリティ対策を行うことを推奨します。

- マイクロソフト社が公開する修正プログラムを適用し、OS を最新の状態にしてください。
- リモートデスクトップサービスを使用しない場合、当該サービスを無効にしてください。
- リモートデスクトップサービスを用いてインターネット経由で接続する場合には、特定の IP アドレスのみにアクセスを許可するなどの適切なアクセス制限を実施してください。
- リモートからアクセス可能なユーザを必要最小限に限定してください。
- ユーザ名及びパスワードは推測されにくいものにしてください。
- 3389/TCP 以外のポートを用いてリモートデスクトップサービスを運用している場合であっても、上記の対策を講じることを強く推奨します。

[i] Microsoft works with researchers to detect and protect against new RDP exploits（Microsoft）
https://www.microsoft.com/security/blog/2019/11/07/the-new-cve-2019-0708-rdp-exploit-attacks-explained/

[ii] ［あらためて確認を］ RDP の脆弱性に対するセキュリティ更新プログラムの適用を推奨（Microsoft）
https://msrc-blog.microsoft.com/2019/11/25/rdpvulnerabilities/

3　宛先ポート 26/TCP に対する Mirai ボットの特徴を有するアクセスの増加

警察庁のインターネット定点観測において、宛先 IP アドレスと TCP シーケンス番号[i]の初期値が一致する Mirai ボットの特徴を有するアクセスを継続的に観測しています（図5）。

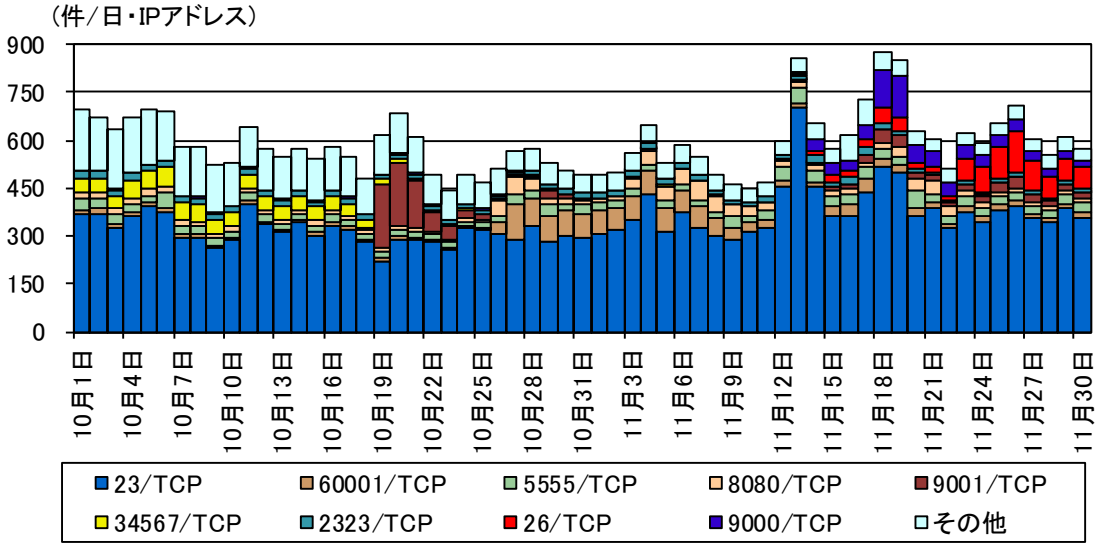

図5　Mirai ボットの特徴を有する宛先ポート別アクセス件数の推移
（R1.10.1～11.30）

Mirai ボットの特徴を有するアクセスのうち、令和元年 11 月中旬より宛先ポート 26/TCP に対するアクセスの増加を観測しました（図6）。

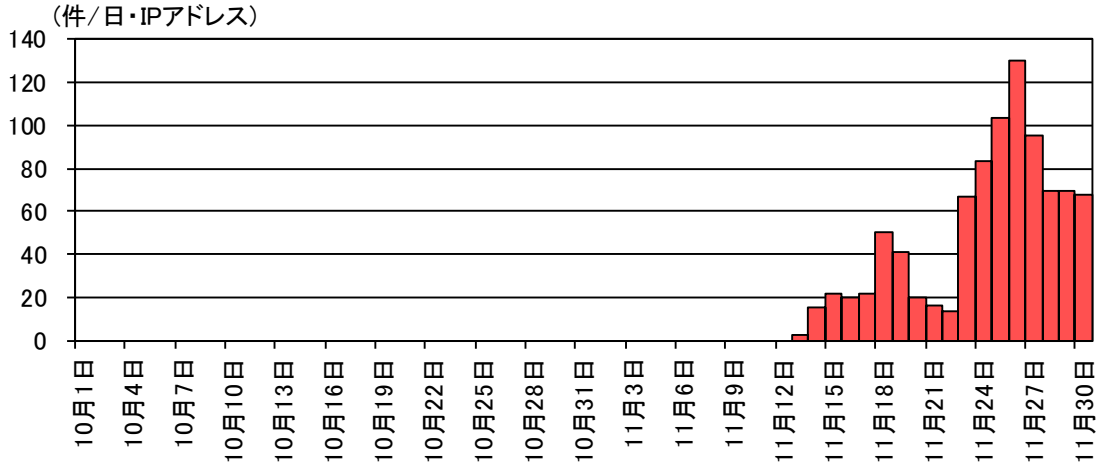

図6　宛先ポート 26/TCP に対する Mirai ボットの特徴を有するアクセス件数の推移（R1.10.1～11.30）

[i] TCP パケットの送受信状況を管理するための番号で、通常は TCP 通信の開始時にランダムな番号が初期値として設定され、進行に合わせて増加します。また、この初期値を特に ISN（Initial Sequence Number）といいます。

観測したアクセスには、遠隔制御用の TELNET の接続を試みるものが含まれていました（図7）。また、IP ヘッダの TTL 値が 64 以下のアクセスがほとんどであったことから、着信元（送信元）となっている機器の多くは Linux が動作しており、不正プログラムに感染したルータやウェブカメラ等が、不正プログラムの感染拡大のための新たな標的として宛先ポート 26/TCP に対してアクセスを試みていると考えられます。

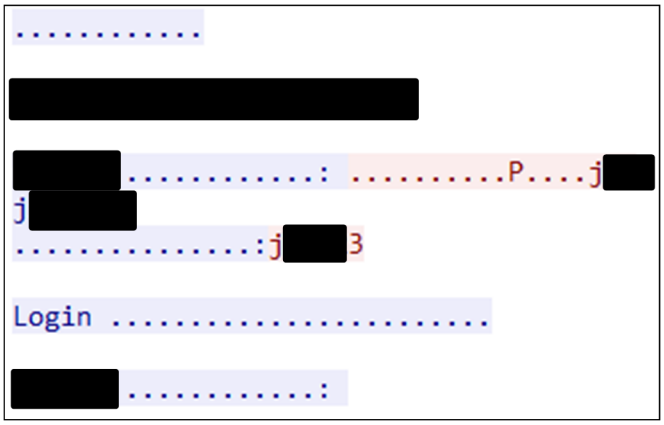

図7　観測したアクセスに TELNET 応答した例（一部マスキング）

宛先ポート 26/TCP に対するアクセスの同一の着信元（送信元）からは、23/TCP、9000/TCP、9001/TCP 等を宛先ポートとするアクセスも観測しています（図8）。

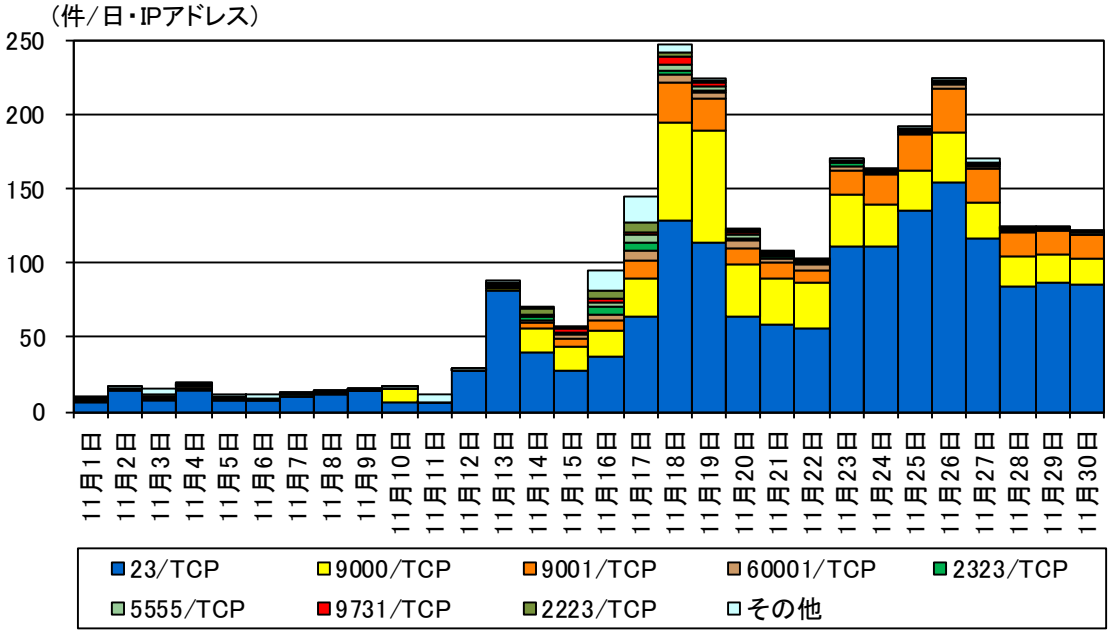

図8　宛先ポート 26/TCP に対するアクセスの着信元 IP アドレスからの他の宛先ポートへのアクセスの推移（R1.11.1～11.30）

IoT 機器の利用者は、以下の対策を参考に、総合的にセキュリティ対策を行うことを推奨します。

- 製造元のウェブサイト等で周知される脆弱性情報に注意を払い、脆弱性が存在する場合にはファームウェアのアップデートや、必要な設定変更等の適切な対策を速やかに実施してください。
- 製品によっては、ファームウェアの自動アップデート機能が存在するものもあります。このような製品を使用している場合には、同機能を有効にしてください。
- IoT 機器をインターネットに接続する場合には、直接インターネットに接続せずに、ルータ等を使用してください。
- インターネットからのアクセスを許可する場合は、必要なポートのみに限定してください。また、必要な IP アドレスのみにアクセスを許可する、VPN を用いて接続することも検討してください。
- 必要がない限りは、ルータの UPnP 機能を無効にしてください。
- ユーザ名及びパスワードは初期設定のままで使用せず、必ず変更してください。また、ユーザ名及びパスワードを変更する際は、推測されにくいものにしてください。
- 製造終了から年月が経過した製品は、製造元のサポートが終了し、脆弱性への対応が実施されない場合があります。そのような製品を使っている場合には、サポート中の製品への更新を推奨します。