NICTER 観測レポート 2016

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で捉えた 2016 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．2016 年は家庭用のルータや Web カメラといった，いわゆる IoT 機器に感染するマルウェア（Mirai 等）が大流行し，それらの機器を悪用した過去最大規模の DDoS 攻撃（サービス不能攻撃）も発生しました．ダークネット観測は Mirai を含む能動的に感染を拡げていくワームタイプのマルウェアの攻撃活動を把握するのに効果的な手法です．本レポートでは，それらのマルウェアの出現時期の観測結果についても触れていきたいと思います．

2. ダークネット観測とは

はじめに「ダークネット観測」という一般には耳慣れない用語について説明します．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を指します．未使用とはつまり，サーバやコンピュータが接続されていないということですので，普通にインターネットを使っている限りダークネット宛てに通信を送ることはないはずです．例えば，IP アドレスはインターネット上の住所で，ダークネットはその中で人が住んでいない住所，つまり空き家と考えてみてください．誰も住んでいない空き家に訪ねてくる人は普通居ませんよね．ところが実際に観測してみると，この空き家，ダークネットに日々大量の通信が届いています．では，これらの通信の正体は何かというと，主にマルウェアが次の攻撃先を探すための通信なのです．通常，マルウェアは次に攻撃できるコンピュータがインターネット上のどこにいるのかわかりませんので，ランダムにあるいは順番に宛先を選択して通信を送り，その応答を待つことで探索（スキャン）を行います．その通信は実在するサーバやコンピュータ等にも届く一方，ダークネットにも届いているというわけです．その結果，ダークネットに届く通信（パケット）を観測することでインターネット上で発生しているサイバー攻撃（特にワームタイプのマルウェアの感染状況）の大局的な傾向が把握できるという仕組みになっています．

我々は 2005 年に NICTER プロジェクトを開始してから約 12 年以上に渡ってダークネット観測を行っています．参考までに，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，観測対象のダークネット規模が大きくなればなるほどより多くのスキャン活動が観測できますので，我々は国内外の様々な組織と協力して 2005 年の約 1.6 万アドレスから 2016 年には約 30 万アドレスまで観測規模を拡大してきました．表 1のうち年間総観測パケット数[*1]は観測 IP アドレス数に大きく影響を受けますので，一番右の列の正規化した値，つまり 1 つの IP アドレスを 1 年間観測した時に届くパケット数がインターネット上のスキャン活動の活発さを測るには適しています．この値を見てみると，特に 2013 年の約 6 万パケットから 2014 年に約 11 万，2015 年に約 21 万，2016 年が 47 万と毎年観測パケット数が倍増し続けていることがわかります．後半でも述べますが，この倍増の原因が Mirai に代表されるような IoT 機器を攻撃対象としたマルウェアの登場であり，今もなお活発な攻撃活動が行われている状況を示しています．本レポートでは特に 2016 年の 1 年

[*1] 年間総観測パケット数はあくまで，NICTER で観測しているダークネットの範囲に届いたパケットの個数であり，これを日本全体への攻撃件数と考えるのは適切ではありません．

表1: ダークネット観測パケット数の年間統計

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

間について，統計情報といくつかの観測事象について報告したいと思います．

3. 統計情報

3.1. プロトコル別統計

2016 年の観測状況についてもう少し詳しく見ていきます。まず，図 1に日毎の観測パケット数を示します．ここでは TCP と UDP のプロトコル別で集計したグラフを示しています．図 1を見ると，UDP パケットに関しては 7 月 23 日から 8 月前半にかけて一時的な急増が見られるものの年間を通してわずかに減少傾向を示しています．その一方で，TCP パケットは年間を通して明らかな増加傾向を示していますので，表 1における 2015 年から 2016 年にかけての観測パケット数の増加は明らかに TCP パケットの増加によるものだということがわかります．そこで日毎の TCP パケットの送信元 IP アドレスのユニーク数（以降，攻撃元 IP アドレス数）をカウントしたものが図 2になります．図を見ると時折大きなピークを示しながら攻撃元 IP アドレス数が増加している様子がわかります．DHCP による IP アドレスの切り替わりの影響や NAT 環境下で複数の機器が感染している可能性もありますので，この観測されている攻撃元 IP アドレス数をそのまま感染機器の台数とみなすのは難しいですが，パケット数だけでなくスキャンを行っている機器数自体も増加傾向を示していることは間違いなさそうです．

3.2. 宛先ポート別パケット数割合

次に，具体的にどのようなサービスがスキャンされているのかを見るために，図 3に年間の宛先ポート番号別のパケット数を集計したものを示します．一番多いのは 23/TCP となっており観測されたパケットの半数以上がこのポート番号宛てのパケットでした．23/TCP は Telnet というプロトコルがデフォルトで使用するポート番号で，ID とパスワードを使って遠隔のコンピュータにログインして操作するためのプロトコルです．ここ最近メディアでも多く取り上げられていますが，今，家庭用ルータや Web カメラ，デジタルビデオレコーダなど多数の機器上で Telnet が動作しており，さらにそれらがインターネットからアクセス可能な状態かつ製造時に設定された簡易な ID とパスワード（例えば ID とパスワードが共に admin など）のまま稼働している状況が明らかになっています．2016 年に大きな話題となった Mirai や他の Telnet を狙うマルウェアはこうした機器を攻撃対象として，23/TCP へのスキャンで機器を探索し，見つかった場合は良く利用される ID とパスワードの組を色々試してログインを試みます．ログインができれば後はマルウェア本体をダウンロードして実行することで容易にその機器を制御下に置くことができるわけです（Mirai の動作については IIJ 社のレポート [1] で詳細解説されていますのでそちらをご参照ください）．また，Telnet はデフ

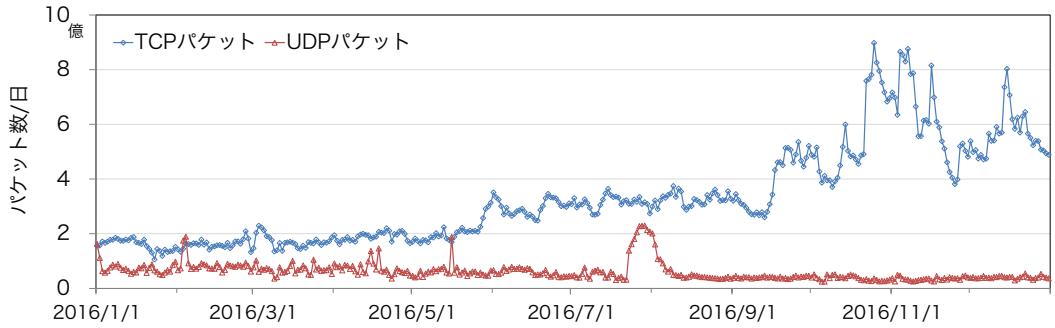

図1: 日毎の観測パケット数統計

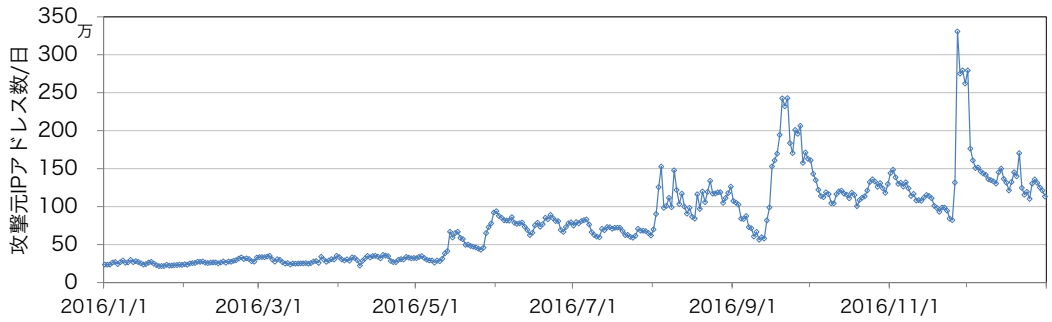

図2: 日毎の攻撃元 IP アドレス数統計（TCP）

ォルトでは 23/TCP を利用しますが機器によっては異なるポートで Telnet を動作させているケースもあります．しかし，図 3で上位に位置している 2323/TCP や，それ以外にも 5358/TCP，6789/TCP などの異なるポート番号で Telnet を動作させている場合でも，既にそれらのポート番号へのスキャンが数多く観測されていますので，Telnet のポート番号を変更すれば安全ということではありません．

また，Telnet は現状最も簡単に様々な機器に侵入できる経路のため活発な攻撃が行われているのであって，IoT 機器への攻撃は Telnet だけに限りません．例えば，図 3で 2 番目に多い 53413/UDP は Netis/Netcore 社製のルータに存在した脆弱性 [8] を狙ったもので，図 1で 2016 年 7 月中盤から 8 月前半にかけて UDP パケットが増加しているのは 53413/UDP に対するスキャンの増加が原因です．また最近は 22/TCP や 2222/TCP で動作する SSH に対して ID とパスワードでのログインを試みるマルウェア [5] も登場していますので，Telnet だけ対応すれば安全ということではない，という認識が重要です．

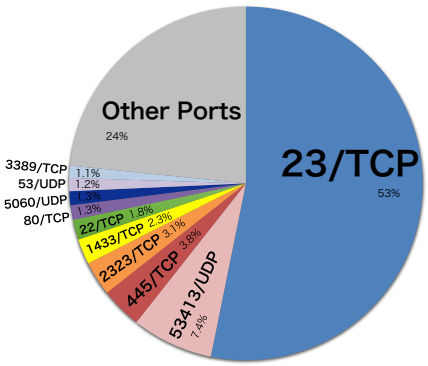

図3: 宛先ポート番号別の年間観測パケット数割合

3.3. 顕著な攻撃活動の増加事例

2016 年で特に攻撃元 IP アドレス数の急増が観測された 4 つの宛先ポート（23/TCP，2323/TCP，5555/TCP，7547/TCP）について図 4に攻撃元 IP アドレス数の推移を示します．2323/TCP は Mirai がスキャンするポート番号として知られていますが，図を見ると 9 月 6 日に 2323/TCP に対するスキャンが観測されはじめ，そ

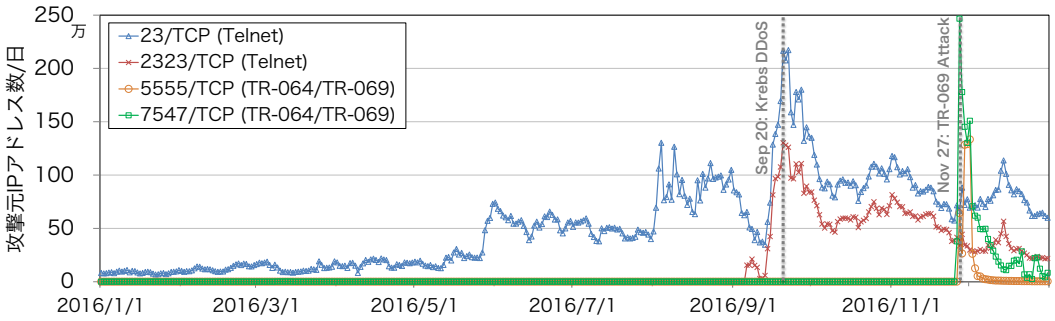

図4: 2016 年に急増した宛先ポート別の攻撃元 IP アドレス数統計

の後急増し 9 月 20 日には 1 日に約 130 万アドレスからのスキャンが観測されている様子がわかります．このような攻撃元 IP アドレス数の急増は新たなマルウェアのパンデミック（感染爆発）時に典型的に見られる傾向です．9 月 20 日付近は Krebs On Security というセキュリティ系ブログサイトに対して Mirai 感染機器を悪用した 620Gbps もの DDoS 攻撃が発生したとされる日です [2]．ダークネット観測でもまさにこの日に最も活発な 23/TCP と 2323/TCP へのスキャン活動が観測されていました．GitHub にリークされた Mirai のソースコードを見ると，Mirai は固定の送信元ポート番号，TCP ヘッダのシーケンス番号が宛先 IP アドレスと同じ値，パケット毎に異なる IP ヘッダの ID 値，各宛先 IP アドレスに対して 1 パケットだけ送信，といった特徴を持つスキャンを行うことがわかります．実際にダークネット観測でも攻撃の約 1 週間前の 9 月 14 日にこの特徴を持つスキャンが観測されはじめていました．ところが面白いことに，9 月以前の 23/TCP へのスキャンを調べてみると上記の特徴の一部分だけ異なる（IP ヘッダの ID 値が固定）スキャンが 8 月頭の攻撃元 IP アドレス数が急増した時に観測され始めていることがわかりました．我々は，リークされたバージョンよりも前の Mirai がこの 8 月の時期に登場し，その後 9 月にアップデートされた可能性が高いと考えています．

また,5555/TCP と 7547/TCP を見ると,11 月後半に攻撃元 IP アドレスの急増が観測されています．7547/TCP は TR-069 や TR-064 というホームゲートウェイやその配下にある機器を制御するための管理プロトコルで利用されています．このポートの対するスキャンが急増したのと同じ時期に，ドイツの Deutsche Telekom の大量の顧客ルータが TR-069 の脆弱性を悪用して感染を拡げるマルウェアの影響で障害に見舞われたと報告されています [6]．5555/TCP についても 7547/TCP の代わりに利用されているケースがあるようで 7547/TCP と同様の増減を示しています．

参考までに，表 2に 9 月 20 日のピーク時に 23/tcp もしくは 2323/TCP にアクセスしてきた攻撃元 IP アドレスの国分布と，11 月 27 日のピーク時に 7547/TCP もしくは 5555/TCP にアクセスしてきた攻撃元 IP アドレスの国分布を示します．表を見ると，ともにブラジルが最も多く観測されていますが，2 位以下の傾向はかなり異なっていることがわかります．特にイランやイギリスなどはダークネット観測で上位に上がることは稀な国ですので興味深い傾向です．全体的に TR-069/TR-064 のケースでは Telnet のケースよりも攻撃元 IP アドレスが特定の国に偏っている傾向が見えます．Deutsche Telekom の攻撃事案では，ZyXEL 社の製品を基にした DSL モデム/ルータが狙われたという話ですが [7, 3]，この攻撃元 IP アドレスの国分布傾向の違いは，攻撃対象となる脆弱な機器の分布状況が影響していると考えています．ちなみに，7547/TCP と 5555/TCP に対する日本国内のアドレスからのスキャンはほとんど観測されていないことから，日本国内で配布されている機器への影響はほとんど無かったと考えられます．

3.4. 日本からの攻撃観測状況

ここで，特に日本からの攻撃活動，つまり日本国内にある機器の感染状況，について見てみましょう．表 5に日毎の 23/TCP 宛てのスキャンのうち日本国内の攻撃元

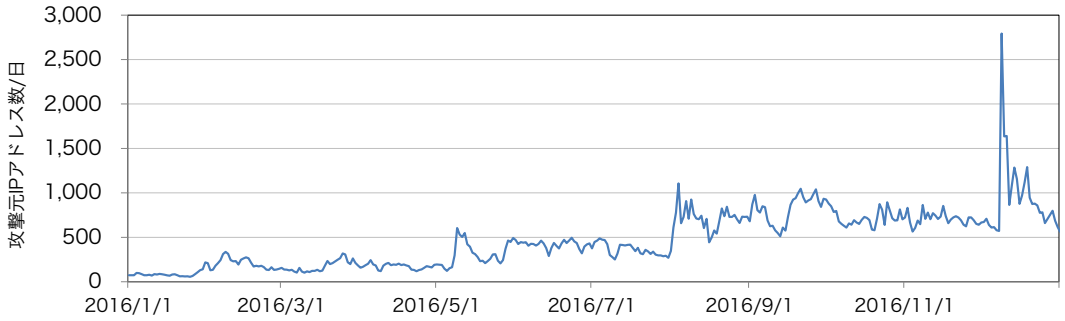

図5: 23/TCP に対する日本国内からの攻撃元 IP アドレス数統計

表2: 各ピーク時の攻撃元国分布

9/20 (23/TCP or 2323/TCP)			11/27 (7547/TCP or 5555/TCP)		
国	#IPs	割合	国	#IPs	割合
ブラジル	456,778	約 21%	ブラジル	1,206,589	約 49%
ベトナム	283,997	約 13%	イラン	334,510	約 14%
インド	225,457	約 10%	イギリス	272,590	約 11%
中国	190,843	約 9%	トルコ	187,296	約 8%
ロシア	129,979	約 6%	チリ	84,755	約 3%
インドネシア	98,752	約 4%	イタリア	83,816	約 3%
コロンビア	82,806	約 4%	アイルランド	53,869	約 2%
メキシコ	49,605	約 2%	タイ	40,418	約 2%
トルコ	44,161	約 2%	アルゼンチン	34,861	約 1%
アルゼンチン	43,779	約 2%	インド	32,123	約 1%
その他	593,654	約 27%	その他	138,675	約 6%

IP アドレス数の推移を示します．表を見ると，1 日におよそ 500 アドレスから 1,000 アドレス程度が観測されている状況が分かります．12 月初めに大きなピークが観測されていますが，これはある国内 ISP のモバイルネットワーク用のアドレス帯から多くのスキャンが観測された影響です．ピークは 2 週間程度で収まりその後は同様の増加は観測されていません．500 ～ 1000 アドレスを多いと見るか少ないと見るかは難しいところですが，他国と比較した場合，1 日に数万から数十万アドレスが観測される国が多数ある中，相対的に少ない観測数だとは言えるかと思います．

繰り返しになりますが，DHCP による動的な IP アドレス割り当ての影響や，マルウェアの中には C&C サーバからの指令によってスキャンのタイミングを制御されているものもありますので，観測された IP アドレス数＝感染台数とみなすのは難しいです．しかしながら，1 日単位の集計であれば動的 IP アドレスの変更の影響はある程度軽減されていますので，図 5の観測数は感染機器数の下限に近い値を示していると考えています．つまり，少なくとも日本国内だけを見ると 1000 台規模の機器が感染していると我々は見積もっています．

4. 対策について

特に 2016 年度に顕著な攻撃増加が観測された IoT 機器のセキュリティ対策では，将来的に設置される機器の安全性確保と，既にマルウェア感染している多数の機器への対処の両方が重要になってきます．ここでは，いくつかの観点から課題を述べたいと思います．

4.1. 感染状況の把握・情報共有

まず，既に多数の機器がマルウェアに感染している現状においては，正確な感染状況の把握が非常に重要になります．ダークネット観測は攻撃活動を把握する一つの有効な観測手法ですがそれだけでは不十分です．囮システムであるハニーポットによって実際のマルウェア検体を収集・解析したり，インターネット上を能動的にスキャンすることで攻撃対象となり得る機器の分布を調べたりするなど，複数の観測手法を組み合わせることで継続的かつ網羅的な情報収集を行う必要があります．また，得られた情報を適切な関係機関と情報共有することで，脆弱な機器の修正等の対策に結びつけていくことが重要です．

4.2. 製造側・設置側による対策

今後設置されていく機器に関して最も重要な対策としては，機器製造時に各機器上で不要なサービスをインターネット上からアクセス可能な状態で動作させないということです．Web カメラやルータにおいてユーザが利用

時にインターネット側からアクセスできる必要があるケースは稀だと思います．現状の攻撃の多数が Telnet へのログイン試行であることを考えると，不要なサービスをデフォルトで停止しておくことで脅威は大きく軽減できます．仮にリモートログインが必要な状況であっても，可能であれば SSH の公開鍵認証を使ったり，最低でも適切な IP アドレスからのみのアクセスを許可するといった設定を行うことが望ましいです．

一方，機器の製造側はインターネットからのアクセスを想定していないにも関わらず，設置時に別の業者によってインターネットからアクセス可能な状態で設置されているケースもあります．基本的には機器側での対処が望ましいですが，実際に不適切な設定の機器が多数存在しており，また機器製造側と設置側が異なる場合が多いことを考慮しますと，機器を設置する側も危険性を認識して必要に応じた適切な設定を行うことが重要です．

4.3. ユーザ側の確認・対策

ユーザ側も自衛の観点から，自らの環境に設置された機器の状況を把握しておくことが望ましいです．各機器に対してインターネット側からのアクセスが可能か，その機器の脆弱性などが公開されていないか，修正パッチは提供されているか，ファームウェアは最新版に更新されているか，など把握しておくと良いでしょう．

4.4. 設置された機器の運用・管理

IoT 機器は PC やサーバとは異なり，設置後の運用・管理が十分に行われていない現状があります．ユーザ側で適切な管理ができれば良いですが，コンピュータに詳しくない方も多数存在している状況で，機器の管理やアップデート等の運用作業を全てユーザ任せにしてしまうのは現実的な対応とは言い難いかもしれません．昨今の PC のようにユーザがあまり意識することなく自動的にアップデートを行う仕組みも必要になるかもしれません．一方で，機器の中には非常に安価な一方でそもそも販売後のファームウェア修正などが適切に行われない機器もあると思いますが，こうした機器の問題にいかに対応していくかも重要な課題となります．

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，2016 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．特に 2016 年は Mirai の登場によって IoT 機器に対する非常に活発な攻撃活動が観測された点が象徴的でした．2008 年に大規模感染を引き起こした Conficker ワームは登場から 6 年が経った時点でも 1 日に世界中の 100 万アドレス以上からのアクセスが観測されていたという報告 [4] があります．おそらく各種 IoT 機器のマルウェア感染と攻撃活動は 2017 年も引き続き活発に観測されると予想していますので，今後も継続した観測と分析を行っていく予定です．

参考文献

[1] Internet Infrastructure Review (IIR) Vol.33. http://www.iij.ad.jp/company/development/report/iir/033/01_04.html, 2016.

[2] KrebsOnSecurity Hit With Record DDoS. https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/, 2016.

[3] New Mirai Worm Knocks 900K Germans Offline. https://krebsonsecurity.com/2016/11/new-mirai-worm-knocks-900k-germans-offline/, 2016.

[4] M. Asghari, Hadi Ciere and M. van Eeten. Post-mortem of a zombie: Conficker cleanup after six years. 24th USENIX Security Symposium (USENIX Security 15), 2015.

[5] M. Malik and P. Kálnai. New Linux/Rakos threat: devices and servers under SSH scan (again). http://www.welivesecurity.com/2016/12/20/new-linuxrakos-threat-devices-servers-ssh-scan/l, 2016.

[6] P. Paganini. More than 900k routers of Deutsche Telekom German users went offline. http://securityaffairs.co/wordpress/53871/iot/deutsche-telekom-hack.html, 2016.

[7] J. B. Ullrich. TR-069 NewNTPServer Exploits: What we know so far. https://isc.sans.edu/forums/diary/TR069+NewNTPServer+Exploits+What+we+know+so+far/21763/, 2016.

[8] T. Yeh. UDP ポートを開放した状態にする Netis 製ルータに存在する不具合を確認. http://blog.trendmicro.co.jp/archives/9725, 2014.