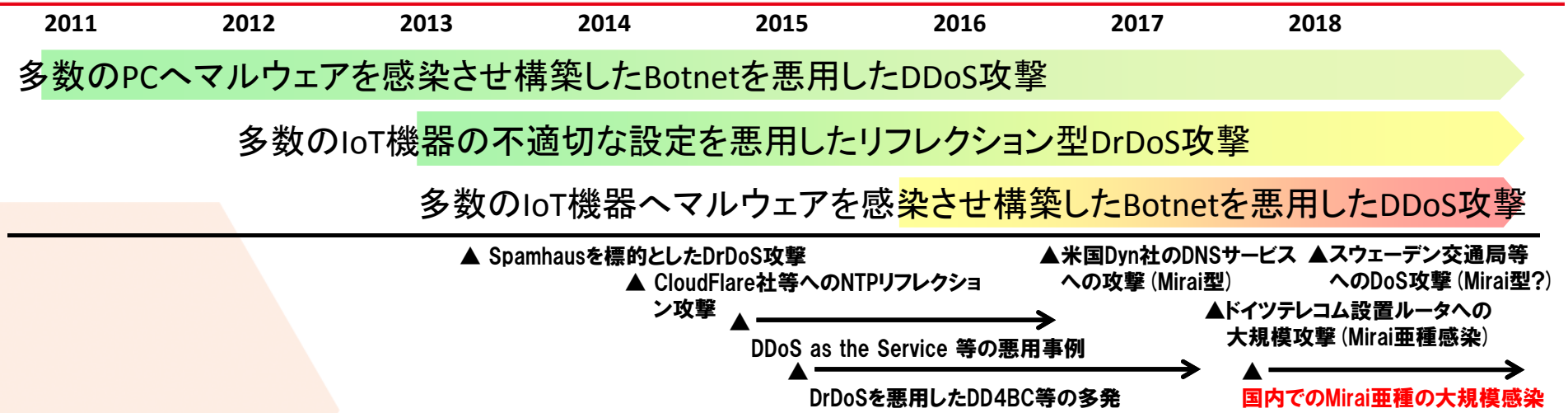
IoT機器の脆弱性対応について
～サイバー攻撃事例から～

2018/03/06

一般社団法人 ICT-ISAC
脆弱性保有ネットワークディバイス調査WG

ICT-ISAC JAPAN
ICT Information Sharing And Analysis Center Japan

IoT機器を悪用したDDoS攻撃



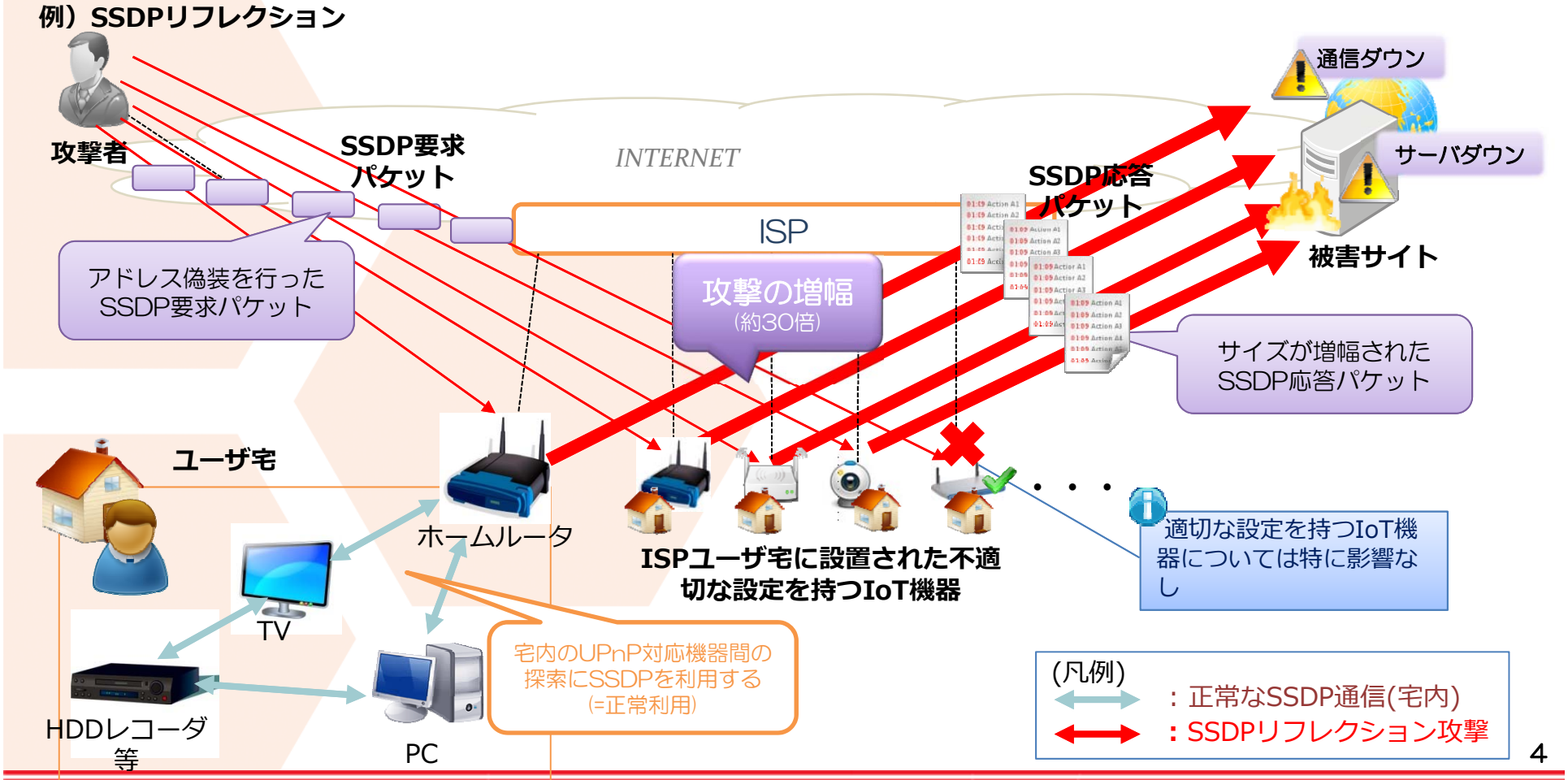
- 旧来のDDoS攻撃は、大量のPCへ DoS攻撃を行うマルウェアを感染させBotnetを構築し、そのBotnetを悪用して一斉に攻撃対象に悪性通信を発生させるDDoS攻撃が主流
  - 本手法では、マルウェア感染PCを大量に確保する必要があるなど大量通信を発生するための準備に多大なコストが必要である等の問題があった
- 2013年3月に発生したSpamhausへの大規模DrDoS攻撃などに代表されるDNSなどの増幅型リフレクション攻撃が発生
  ホームルータやインターネットカメラ等のインターネット側からのリクエストに応えてしまう不適切な設定を悪用したDrDoS攻撃が日常化
  - DNSリフレクションのみならず NTP、CharGEN、SSDP (UPnP)など多数のプロトコルを悪用
  - 機器ベンダや通信事業者の努力により悪用できる機器は減少傾向
- ホームルータやインターネットカメラ等のファームウェアの脆弱性を悪用することでマルウェアに感染可能であることが発覚、悪用することでPC等と比べ安易にマルウェア感染による大規模なBotnet構築を行えることから大規模なDDoS攻撃基盤が構築されると共に大規模攻撃が発生

IoT機器を悪用したDDoS攻撃事例

	国外事例	国内事例	
2011年9月		国政機関、東京都、JAL等、多数のサイトへのDoS攻撃など、国内への一斉サイバー攻撃が発生 一部でIoTの不適切な設定を悪用したリフレクション攻撃	**DrDoS攻撃(リフレクション型DDoS攻撃)** ホームルータやインターネットカメラなどのIoT機器の、インターネット側からのリクエストに応えてしまう不適切な設定を悪用
2012年9月			
2013年3月	Spamhausを標的としたDrDoS攻撃 (DNSリフレクション)		
2014年4月	CloudFlare社等を標的とした NTPリフレクション攻撃		
2014年9月		オンラインゲーム運営サイトへのDDoS攻撃による業務妨害の容疑で高校１年の男子生徒(16)が書類送検（「負荷テストサービス」を利用)	
2014年8月		国内主要ISP等におけるDNSサーバ障害の多発 **[事例1]**	
2015年7月		国内インターネット銀行・証券企業への金銭要求を目的とするDrDoS攻撃の発生 **[事例2]**	
2016年10月	米国Dyn社のDNSサービスを標的とした BotnetによるDDoS攻撃（Mirai） **[事例3]**		**Mirai型Botnet DDoS攻撃** IoT機器のファームウェアの脆弱性を悪用することでマルウェアに感染させボットネット化構築したMirai型ボットネットを悪用してDDoS攻撃を発生
2016年11月	ドイツテレコム設置ルータでの Mirai型マルウェア大規模感染攻撃		
2017年10月	スウェーデンの複数の交通機関、スウェーデン産業省交通局を標的とした BotnetによるDDoS攻撃（Mirai型?）		
2017年11月		国内IoT機器でのMirai型マルウェアの大規模感染が発生 **[事例4]**	

リフレクション攻撃の仕組み

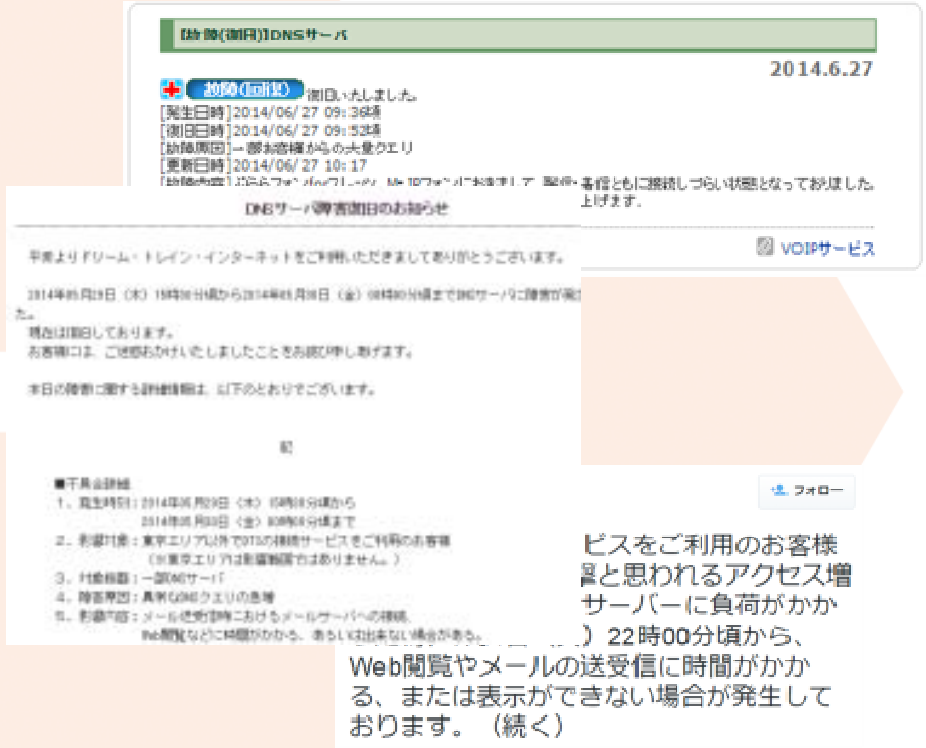
- DrDoS攻撃のリフレクションで悪用される、DNSフォワーディング、UPnP(SSDP)等は本来ユーザ宅内のローカル環境向けに使用されるプロトコルである。
- しかし、インターネットとの境界に設置されているIoT機器のこれらプロトコルに不適切な設定があった場合、インターネット側からの通信に対してもIoT機器は(本来は行うべきでない)応答を返してしまう。
- 攻撃者はこれを利用し、当該IoT機器を踏み台として被害サイトに対するDoS攻撃を行うことが可能になる。



[事例1]国内主要ISP等におけるDNSサーバ障害の多発(2014～)

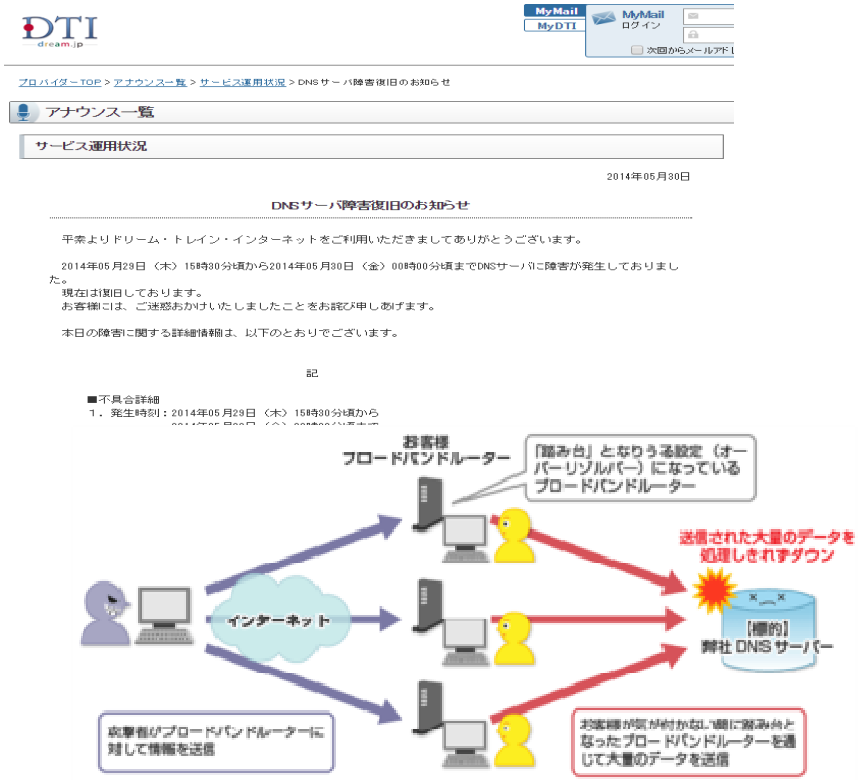
- 2014年5～7月頃、DTI・ぷらら・ケイ・オプティコム(eo光)等複数のISPにおいてDNSサーバを原因とする大規模な通信障害が多発。本障害は**各ISP社のDNSサーバを標的としたDNSリフレクション攻撃**であったと見られている
- 従来のDNSリフレクション攻撃はDNSサーバの先にいるターゲット(被害ユーザ)へ大量トラフィックを送り込むことが目的であるが、本攻撃はドメイン名検索がNGとなるような特殊なDNSクエリを大量に送り込むことで**「DNSサーバ自体のリソースを枯渇」**させることが目的であった様子
- 攻撃者の目的に関しては未だ不明であるが、一説として使用された検索ドメインに「appledaily.com」(香港メディア、蘋果日報のドメイン名)が観測されたことから、当時発生していた香港反政府デモとの関連で同社サイトへの攻撃意図があったと見る向きもある

ISP各社が伝えるDNS障害について



(出典)
http://info.dream.jp/trouble/20140530_12088.html
http://www.plala.or.jp 故障情報)
https://twitter.com/eosupport/status/484133990194884608

ブロードバンドルータを踏み台としたDNS攻撃について



(出典)
http://info.dream.jp/trouble/20140530_12088.html
http://support.eonet.jp/news/194/

［事例2］金銭(Bitcoin)を要求するDDoS攻撃: DD4BC

Subject：DDOS ATTACK!
From：DD4BC Team <dd4bct@gmail.com>
本文（一部抜粋）：

```
Your site is going under attack unless you pay 25 Bitcoin.

Pay to 198QaeuJ6oMeuan2p5gyDx75odweMWzNXH

Please note that it will not be easy to mitigate our attack, because
our current UDP flood power is 400-500 Gbps, so don't even bother. At
least, don't expect cheap services like CloudFlare or Incapsula to
help...but you can try. :)

Right now we are running small demonstrative attack.
Don't worry, it will not be that hard (it shouldn't crash your site)
and it will stop in 1 hour. It's just to prove that we are serious.
Check UDP traffic. :)

We are aware that you probably don't have 25 BTC at the moment, so we
are giving you 24 hours.
Find the best exchanger for you on
https://localbitcoins.com or
http://howtobuybitcoins.info
You can pay directly through exchanger to our BTC address, you don't
even need to have BTC wallet.
```

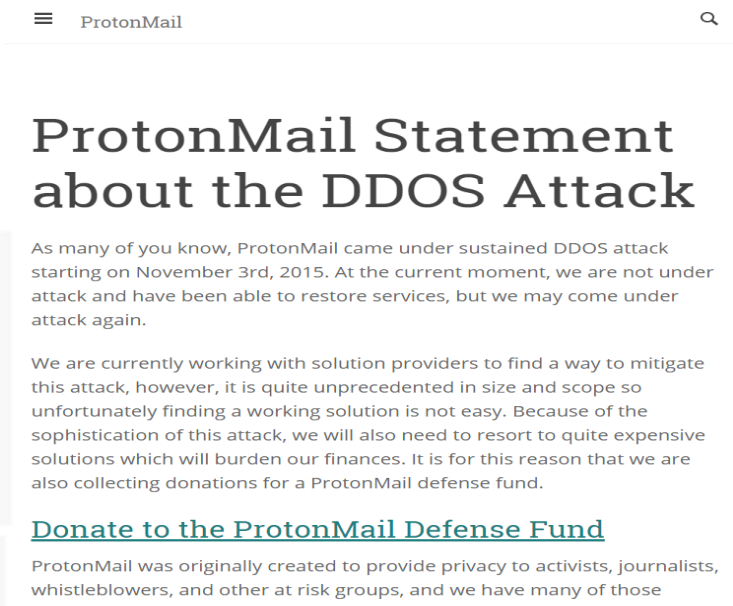
(出典) https://www.facebook.com/nfoservers/posts/10154560880780717

- DD4BC
  - 小規模なDDoS攻撃後、メールにてBitcoinを支払わなければ更なる攻撃（400Gbps）を実施する旨の脅迫を行う攻撃グループ。実際にはそこまでの攻撃能力は無いものと見られており、世界的に見ても400Gbps規模の攻撃が行われた実績は無い。
  - 2015年5～7月、日本国内の銀行・証券会社に対してDDoS攻撃（10～40Gbps）が行われ、一時的にHPやネットバンキングサイトへのアクセスに障害が発生した。

(出典) akamai「CASE STUDY: SUMMARY OF OPERATION DD4BC」より抜粋

- Armada Collective
  - DD4BCと同様にDDoS攻撃に伴って金銭（Bitcoin）を要求する攻撃グループ
  - 2015年11月3日（現地時間）、スイスProton Technologiesのメールサービス「ProtonMail」へ最大100GbpsものDDoS攻撃が行われ、同社がBitcoinにて約6000$支払ったにも関わらず、攻撃は6日間に渡り継続された。

- Phantom Squad
  - 2017年9月から国内企業に対しDDoS攻撃の停止と引き換えに金銭を要求するメールが大量に送付


ProtonMail

ProtonMail Statement about the DDOS Attack

As many of you know, ProtonMail came under sustained DDOS attack starting on November 3rd, 2015. At the current moment, we are not under attack and have been able to restore services, but we may come under attack again.

We are currently working with solution providers to find a way to mitigate this attack, however, it is quite unprecedented in size and scope so unfortunately finding a working solution is not easy. Because of the sophistication of this attack, we will also need to resort to quite expensive solutions which will burden our finances. It is for this reason that we are also collecting donations for a ProtonMail defense fund.

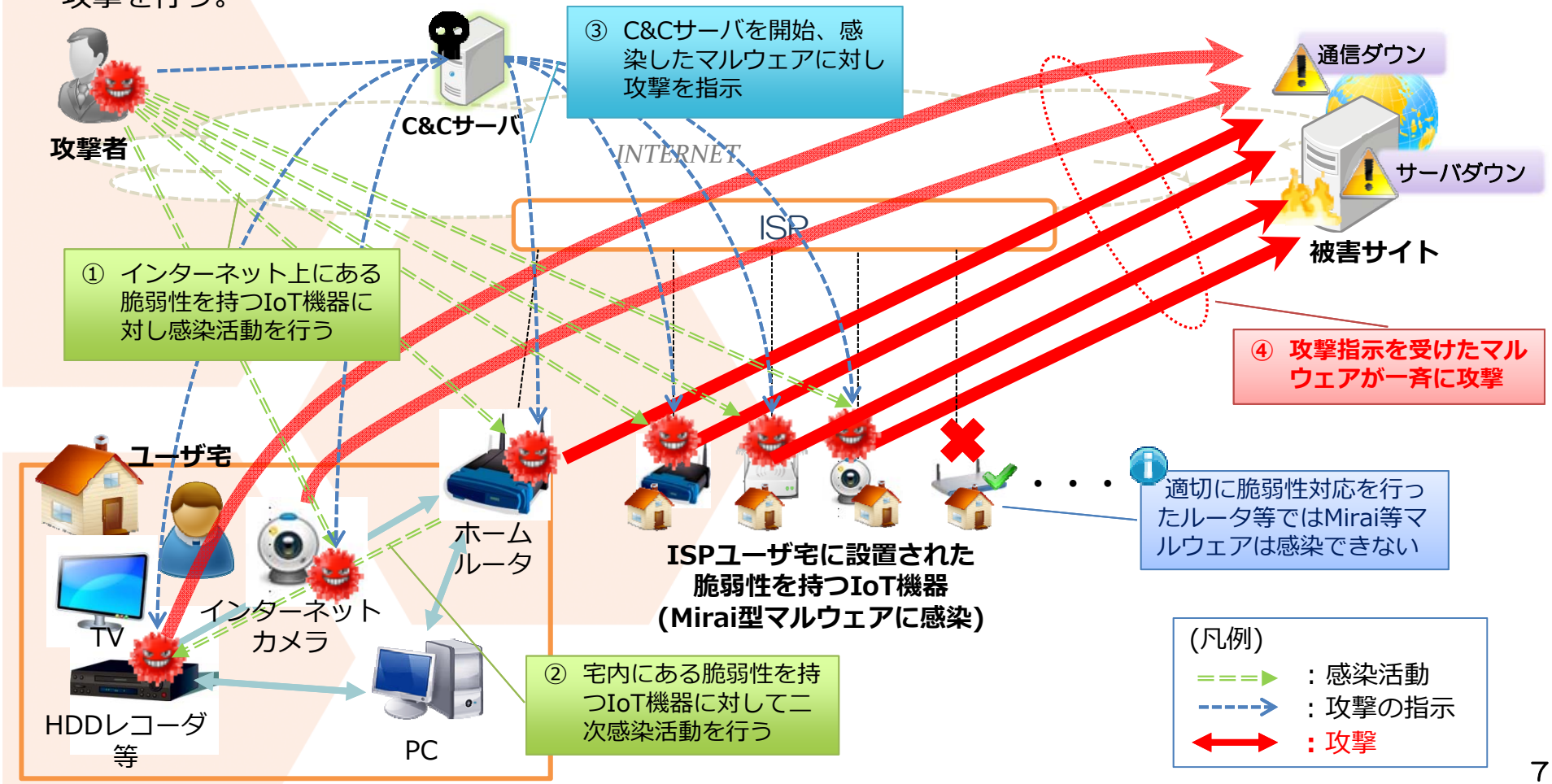
Donate to the ProtonMail Defense Fund

ProtonMail was originally created to provide privacy to activists, journalists, whistleblowers, and other at risk groups, and we have many of those

(出典)
https://protonmaildotcom.wordpress.com/2015/11/05/protonmail-statement-about-the-ddos-attack/

Mirai型マルウェアの感染と攻撃の概要

- IoT機器の多くはファームウェアと呼ばれるソフトウェアによって動作している。Mirai型マルウェアはこのファームウェアの脆弱性を悪用し、悪性コードをIoT機器上に感染させ動作させる。
- インターネット側から通信が行えるIoT機器が主な感染対象となる。
  感染済IoT機器の二次感染活動によってインターネットと通信できない機器でも感染は起りえる。
- 感染後、C&Cサーバ等を介して攻撃者からの指示を受けると一斉に攻撃対象サイト(被害サイト)に対して、攻撃を行う。



[事例3] IoT機器を感染対象としたマルウェア：Mirai

- 2016年10月 米国Dyn社のサービスを標的とした大規模DDoS攻撃が発生
- TwitterやSpotify、Netflix、WSJなどの大手サイトがアクセスしにくくなる事象が発生。
  米国を中心に約6時間にわたってサービスが利用できなかった。
- 本攻撃は電子機器メーカーHangzhou Xiongmai Technologyの防犯カメラ（DVR）やIPカメラなど10万台以上のIoT機器の脆弱性を悪用し感染させたMiraiと名付けられたマルウェアからの悪性通信によって引き起こされた。
- Mirai系マルウェアに感染しているIoT機器は、主に工場出荷時のID/パスワードを使っており簡単に感染させられるものであることが指摘されている

攻撃概要

(出典)
Cyber Attack dot Net

感染地域

(出典)
Downdetector

- 2016年11月には英国人男性ハッカー(逮捕済み)によってドイツテレコムが各家庭に設置したルータ約90万台にMirai型マルウェアの感染を狙ったサイバー攻撃が行われる。顧客のサービスに障害が発生。ネットにアクセスできないなどの影響が出た。
- 2017年10月スウェーデンの交通機関や当局のネットワークを提供しているISPであるTDCとDGCへの大規模DDoS攻撃が発生。
  - 列車運行を管理する産業省交通局のシステムが麻痺。列車の運行停止や遅延が発生。
    列車遅延は一日中続いた。
  - サイトやメールシステムもダウンしたため、遅延情報も通知できなかった。交通局では局員個人のFacebookアカウントで乗客に情報提供を実施するなど混乱が発生した。

[事例4] 国内IoT機器でのMirai型マルウェアの大規模感染が発生

- 2017年12月、2017年11月初旬より国内でMirai亜種の感染が拡大していることが、NICT、@Police、JPCERT/CC、ICT-ISACなど複数の機関から注意喚起が行われた。
- 感染に用いられている脆弱性は複数存在するものの、その多くにおいてRealtek SDKに依拠する脆弱性を悪用したものがあり、複数ベンダで製造・販売されているホームルータ製品で採用されている模様である。
- 現在の所、この感染したマルウェアからの顕著な攻撃は観測されていないものの大規模なDDoS攻撃の可能性が示唆されている。
- 感染数については正確にわかっていないものの数万～数十万であることが推測されている模様。

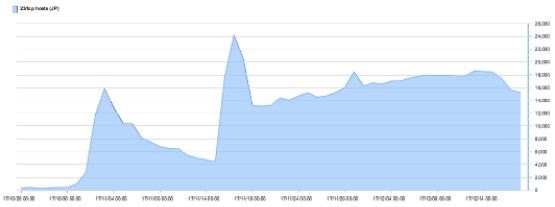


図1. 日本国内からの 23/TCP にアクセスするユニークIPアドレス数（日毎）

2. 23/TCP（国内）と 52869/TCP

10月31日頃から，日本国内のIPアドレスを送信元とする，23/TCPへのスキャンが増加しています．送信元のユニークIPアドレス数は，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日頃から再度IPアドレス数が増加しています．ピーク時のユニークIPアドレス数は約2.4万で，12月18日現在，約1.5万ホスト[5]を観測しており，現在も右肩上がりで感染が拡大しているように見えますので，今後も注意深く観察する必要があります．

この事象と同時に，我々の運用するハニーポットでは，Mirai 亜種をダウンロードする 52869/TCP 宛の攻撃通信（ペイロード1）を観測しています．分析の結果，このペイロードは 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（CVE-2014-8361[6]）を攻撃する通信であることがわかりました．さらに調査を進めた結果，古いファームウェアバージョンで動作しているロジテック社製の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，これらの機器がMirai亜種に感染した結果，日本国内における 23/TCP 宛のスキャンが増加した可能性が高いことを確認しました．

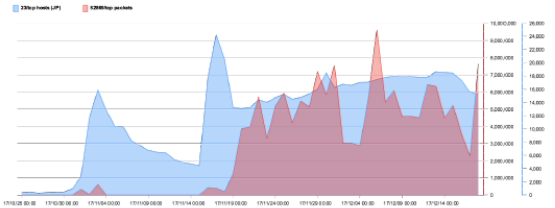


図2. 52869/TCP へのスキャンと23/TCPへのスキャンの増加

(出典)
http://www.nicter.jp/report/2017-01_mirai_52869_37215.pdf

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

平 成 29 年 12 月 19 日

存在するルータを標的とした宛先ポート 52869/TCP に
セス及び日本国内からの Telnet による探索を実施す
の観測等について

存在するルータを標的とした宛先ポート 52869/TCP に対するアクセス及
らの Telnet による探索を実施するアクセスの観測しました。これら
ロジテック株式会社は同社が販売するブロードバンドルータの脆弱性及びその
に注意喚起しています。該当製品の利用者は適切な対策を早急に実施するこ
す。

存在するルータを標的とした 52869/TCP に対するアクセスの観測

定点観測システムにおいて、平成 29 年 11 月 1 日から宛先ポート 52869/TCP に対
り増加を観測しました(図1)。

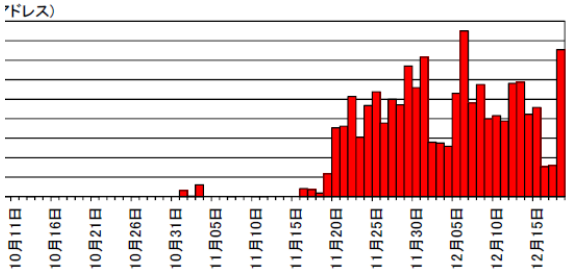


図1 宛先ポート 52869/TCP に対するアクセス件数の推移(H29.10.1～12.18)

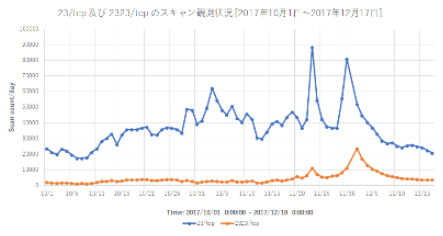
(出典)
http://www.npa.go.jp/cyberpolice/detect/pdf/201712191.pdf

<<< JPCERT/CC Alert 2017-12-19 >>>

Mirai 亜種の感染活動に関する注意喚起
https://www.jpcert.or.jp/at/2017/at170049.html

I. 概要

2017年11月ごろより、国内において Mirai の亜種による感染活動が確認されています。Mirai やその亜種などのマルウエアに感染した機器は、ボットネットに取り込まれ、攻撃者により遠隔から命令をうけて、DDoS 攻撃などに悪用される可能性があります。



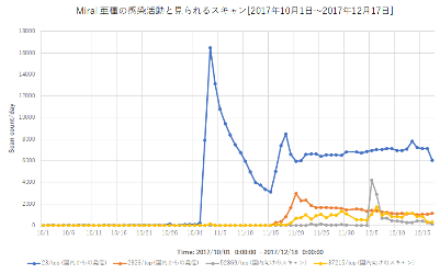


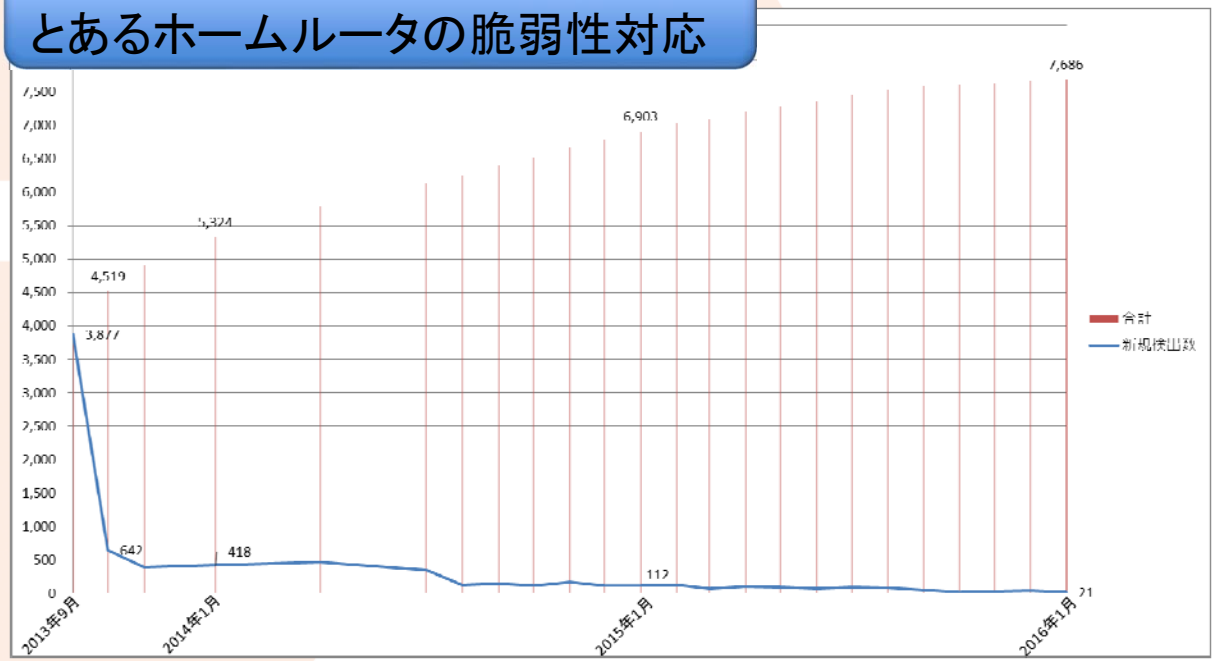
図1: 定点観測システム TSUBAME における Mirai 亜種とみられる感染活動に関するスキャン
クリックすると拡大されます

(出典)
https://www.jpcert.or.jp/at/2017/at170049.html

IoT機器のセキュリティ上の問題点

- **IoT機器の脆弱性の悪用は認知しずらい**
  - サイバー攻撃の多くは**不適切な設定**や**ファームウェア(ソフトウェア)の脆弱性**を悪用して攻撃してきます。
  - しかしながらIoT機器の利用者は、本来の目的を達成するための設定ができればよく(ISP接続をする、カメラによる動画確認をする等)、**セキュリティ上の設定の適切さやソフトウェアの状況の確認に比較的無関心**である。
  - さらにIoT機器は所有者(利用者)の目のつかないところで動作していることが多く、目的通り動作している限りは顧みられることは稀で、**購入後の脆弱性の確認やソフトウェアのアップデート状況の確認を怠りがちである**。

T-ISAC-Jの取組みによる
とあるホームルータの脆弱性対応



利用者が一度購入した機器の
脆弱性対応は、
利用者のリスク認知の観点から
非常に困難となる

IoT機器のセキュリティ上の提案

これまでのIoT機器を踏み台にしたサイバー攻撃事例で悪用されているのは「不適切な設定」、「利用者に認識されていない脆弱性」であり、PCやスマートフォン等では普通に対処されていることである。
IoT機器も同等の対策を行うことで大半の攻撃を防ぐことが可能と考えられる。

- **セキュリティを確保が急務であるIoT機器**
  - IoT機器が踏み台となるサイバー攻撃の大半はDDoS攻撃であり**インターネット側から悪用**

    ■ インターネット接続の境界に設置される/インターネットとの通信が可能な機器
    (ホームルータ、インターネットカメラ、インターネット家電 等)

- **販売後の脆弱性発覚時のセキュリティ確保**
  - **不適切な設定**や**ファームウェア(ソフトウェア)の脆弱性**を悪用して攻撃してきます。 これらは初期販売時、工場出荷時には脆弱性として認知されていない場合が多く、これらの設定の変更や脆弱性対応が利用者によって行われなければならない場合が多々存在する

    ■ ファームウェア更新手段の簡易化 / 設定変更手段の簡易化
    (ハードウェアスイッチ等での更新の実現、ベンダからの強制更新機能の実現 、
    接続ISP等からのレンタルモデルの推奨などの検討 等)

- **IoT機器の初期設定/利用時のセキュリティ確保**
  - IoT機器がサイバー攻撃に悪用される場合、機器が採用している各種プロトコルが悪用される。設定等に使われるプロトコルは認証機能を持つ場合もあることから

    ■ 各種プロトコルの工場出荷時ID/パスワードの変更を推奨
    (初期利用時におけるID/パスワードの強制変更機能の実現 など)