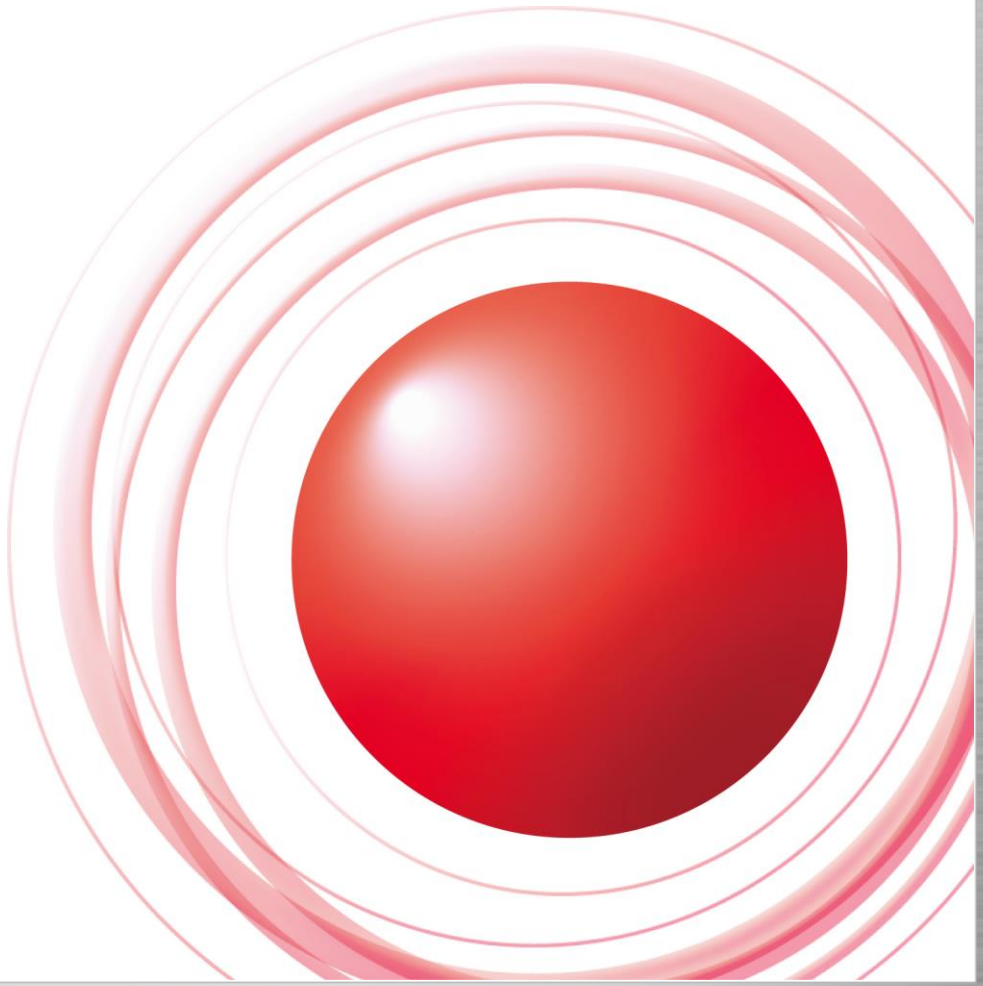
IIJ Technical WEEK 2013
セキュリティ動向2013

IIJ
Internet Initiative Japan



2013/11/21

株式会社インターネットイニシアティブ
サービスオペレーション本部
セキュリティ情報統括室
齋藤衛

Ongoing Innovation

2013年セキュリティ動向

2013年に注目したセキュリティ関連動向

利用者を取り巻く状況

企業などを取り巻く状況

ホームルータのセキュリティ

2013年に注目したセキュリティ関連動向

- (遠隔操作ウイルス)
- 銀行の認証（暗号表を含む）盗むウイルス（Banking Malware）の流行
- 3月にヨーロッパで発生した300Gbps規模のDDoS攻撃
- 3月20日韓国で発生したサイバーテロ
- 企業に対する攻撃(標的型攻撃など)の継続
- Exploit kitを利用したWeb改ざん~マルウェア感染事件
- 頻発するリスト型攻撃による不正ログイン事件
- E. Snowdenの告発に端を発して明らかになった、NSAなどの国家組織による通信の傍受
- ホームルータのセキュリティの現状とその影響
- Webコンテンツそのものの脆弱性、CMSやプラットフォーム(Apache Struts2 など)の脆弱性を悪用した企業ホームページなどの改ざん
- ccTLD単位のドメインハイジャックなどの事件
- 日本におけるパーソナルデータの取り扱い検討

国家組織による通信の傍受

- 元CIA/NSA契約職員 E. Snowdenによる暴露
- 米国だけではなく複数の諜報活動が明らかに
  - ただし、技術的に不明瞭な一般報道が多く、真実を見極めるためには検証が必要。
- 考察すべき事柄
  - なぜ国家はこのような組織を作って世界中の通信を傍受、暗号解読などを実施しているのか。
  - 我々の通信は傍受されているのか。
    - 「技術的に可能」であったことを実際にやっていることが明らかになった。
    - 通信サービスを利用するときに、第三者に傍受される可能性を念頭に置いて利用する必要がでてきた。
  - この状況を受容できるか。
  - 自分の通信を守ることは可能か。

利用者を取り巻く状況

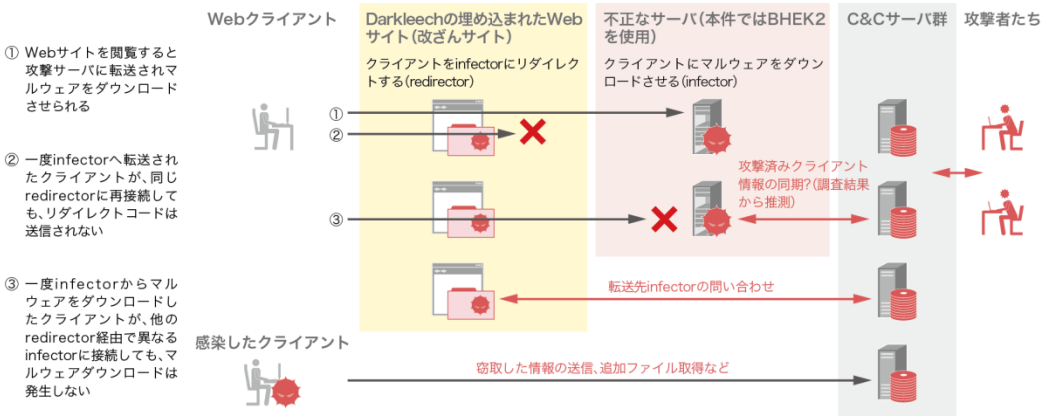
ネットワークサービスを利用するための認証情報を窃取、権限を悪用される事件が継続。一般Webサイトの改ざんにより、通常の閲覧でマルウェアに感染。利用者の保持するICT機器の運用状況や設定、機器そのものの脆弱性などによって、様々な事件が発生している。また、スマートフォンアプリやネットワークサービスなどにおける、不正な情報取得が継続。一方で、パーソナルデータの正当な取得と取扱いについて検討が行われている。

- 認証情報の窃取
  - Banking Malwareの流行
    - 主にオンラインバンキングの認証を盗むためのマルウェア。
    - 追加の認証を提供する暗号表を盗む試み。
    - 従来型フィッシングも継続。
  - 頻発するリスト型攻撃
    - 特定のネットワークサービス事業者に侵入して盗んだ認証情報（ID・パスワードのペアなど）をもとに、他の事業者に適用することで、認証情報を使いまわしている利用者の権限を不正に取得する。
  - 対策として「ID・パスワードの使いまわしやめよう」キャンペーンや、事業者側での多要素、多段階認証の導入。

2013年セキュリティ動向

利用者を取り巻く状況(2)

- Web感染型マルウェアとExploit kit
  - Exploit Kit は攻撃者側の分業体制
    - マルウェア感染サイトに誘導するためのコンテンツ改ざん、マルウェア配布のプラットフォームとアクセス制御、マルウェア配布者、マルウェア作成者。
  - 新たな対策施策として総務省ACTIVEプロジェクトなど
- 利用者の保持するICT機器
  - スマートフォンのセキュリティ
  - ホームルータのセキュリティ(後述)



ドライブバイダウンロード攻撃の流れと解析を妨害する仕組み
IIR Vol 19「日本国内のWebサイト改ざんとドライブバイダウンロード」より
http://www.iij.ad.jp/company/development/report/iir/019.html

http://www.active.go.jp/

企業などを取り巻く状況

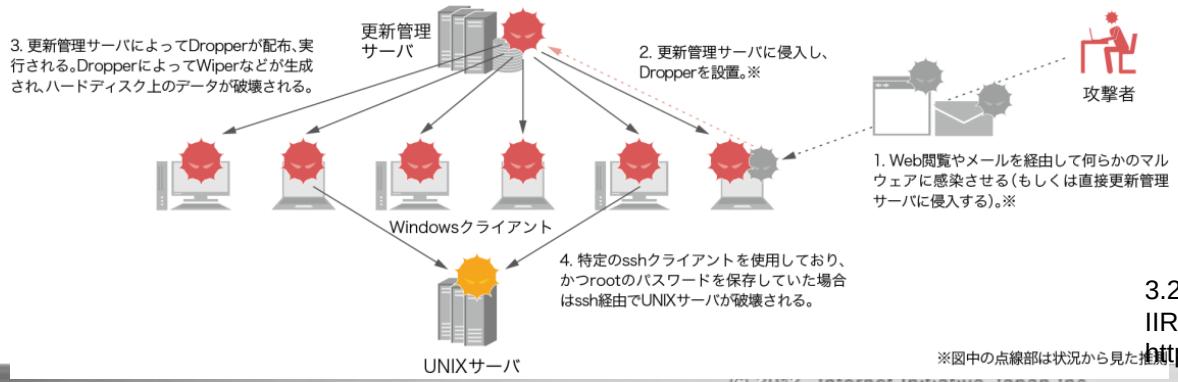
企業などのセキュリティ境界を越え、侵入するための攻撃（標的型攻撃など）は依然として継続。脆弱性を悪用したWeb改ざんや、威力行為としてのDDoS攻撃もなくなっていない。スマートフォン、タブレットなど新しいICT環境の導入が一般的になり、関連する事件も増加。

- 標的型攻撃
  - 国の関係機関や大手企業への諜報活動としての標的型攻撃のみならず、一般企業のこの攻撃の発生が目立つ。
  - 攻撃者側の分業化。攻撃環境の選択や、マルウェアのチューニングなどにおいて、攻撃実行者の変更できる範囲が非常に狭い様子が見てとれる(参照:IIR Vol21「連続する標的型メール攻撃」P23 表-1)。
  - 関連して、水飲み場攻撃(Watering Hole Attack)も話題に。
    - Web感染型マルウェア事件だが、Infectorにおいて接続元アドレスにより感染範囲を政府、報道機関など特定分野ごとに制御。

2013年セキュリティ動向

企業などを取り巻く状況

- DDoS攻撃の現状
  - 概況
    - 発生頻度に関する状況は変わらず。世界的には100Gbps超(～300Gbps)の事例が複数。IIJ観測に基づく規模感は4Gbps(ピーク時10Gbps)超程度。
    - 9/18に中国からの攻撃はなかった(ように見える)。
    - DDoS攻撃手法としてのDNS Amplification 攻撃、DNS Open Resolver が多数存在することが注目され、対策が検討される。
- 3月20日韓国で発生したサイバーテロ（3.20大乱）
  - 報道機関など複数の企業内の管理サーバに侵入し、企業内におけるソフトウェアのアップデート手法を悪用。
  - 目的が破壊行為(HDDのMBR情報削除、再起動)。



3.20大乱におけるマルウェア感染の流れ
IIR Vol 19「韓国3.20大乱」より
http://www.iij.ad.jp/company/development/report/iir/019.html

2013年セキュリティ動向

ホームルータのセキュリティ

家庭内ネットワークの現状とホームルータ

ホームルータに関連するセキュリティの現状
ホームルータのセキュリティ上の問題は誰のリスクとなるのか
この問題の解決に向けて

家庭内ネットワークの現状とホームルータ

家庭内ネットワーク

- 家庭内ネットワークの現状
  - 「白物」家電のネットワーク接続(外出先からスマートフォンで制御)
  - 白物家電への情報通信技術(ICT)の応用(無線LANリモコン)
  - （自ら通信機能を持つ白物家電）
  - ICT側のセキュリティ問題が家庭へ！ということを危惧。
- 家庭用機器の脆弱性の例
  - インターネットプリンタ
    - 韓国製、台湾製などのプリンタに認証迂回可能な脆弱性が発見され、自在に印刷されてしまう可能性が(2012/12)。
    - Google に約80,000万台の米国製プリンタのWeb管理インタフェースがキャッシュされている(2013/01)。
  - インターネット監視カメラ
    - 韓国製インターネットTVの脆弱性でインターネット側からカメラ機能を有効にすることができ、TVを見ている様子を盗撮される(2012/11)。
    - 同インターネットTVの管理画面にアクセスできてしまう脆弱性で、カメラ機能を有効に(2013/08)
  - インターネット録画システム
    - 中国製DVR録画システムで、インターネット側から無認証で操作可能であることが発見される。世界中で58,000台(2013/01)
  - UPnPの脆弱性(libupnp)(後述)

家庭内ネットワークの現状とホームルータ

本日のメインテーマ:ホームルータ

- CPE:Customer Premises Equipment(顧客宅内機器)
  - 多くの場合、利用者が家電量販店などで購入。
- ホームルータの主な機能
  - 管理インタフェース(Web UI)
  - インターネットに接続するための機能(PoE終端、NATなど)
  - 家庭内ネットワークを構築するための機能(有線、無線LAN、DHCP、UPNP、DNS resolverなど)
  - インターネットと宅内ネットワークのセキュリティ境界(FWなど)
  - サーバアプリケーション(NAS、プリントサーバなど)
  - その他機能(暗号関連、疑似DMZなど)

- ホームルータの管理者権限を外部の第三者に奪われた時、どのようなリスクが考えられるか。

2013年セキュリティ動向

ホームルータのセキュリティ

家庭内ネットワークの現状とホームルータ

ホームルータに関連するセキュリティの現状

管理インタフェースにかかわる脆弱性

Universal Plug and Play

DNSにかかわる設定ミス(DNS Open Resolver)

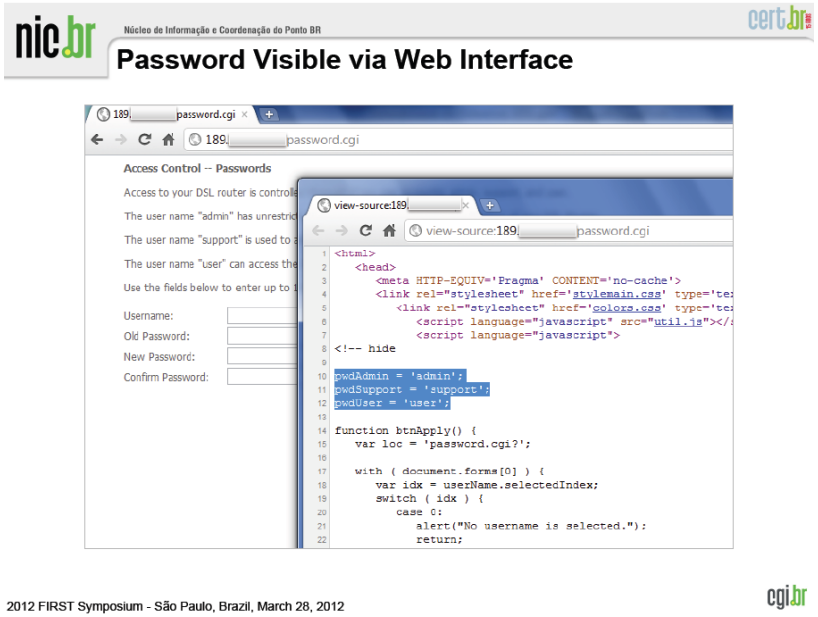
ホームルータのセキュリティ上の問題は誰のリスクとなるのか

この問題の解決に向けて

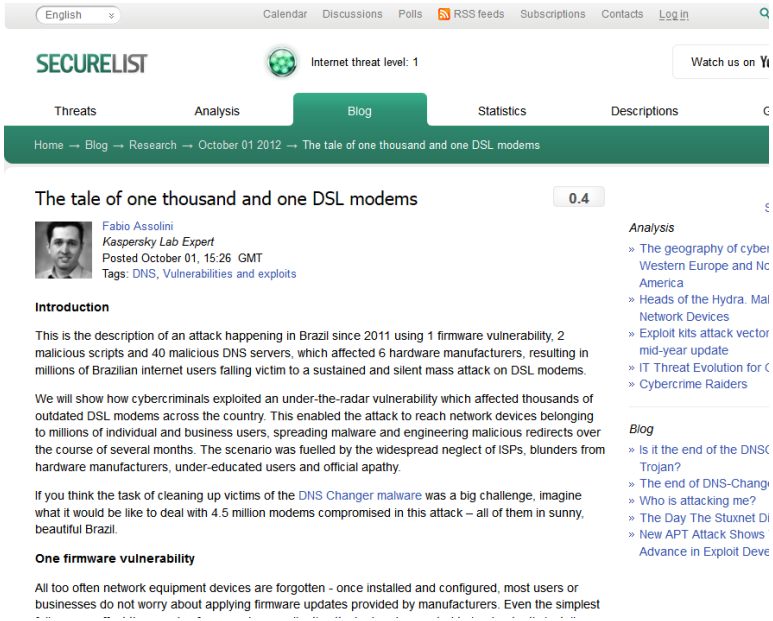
管理インタフェースにかかわる脆弱性

国外の事例

- 2011年ブラジルやヨーロッパ
  - ホームルータやADSLModemの脆弱性を悪用し、インターネット側から直接参照用DNSサーバの設定を変更。
  - 2011年最大450万台。2012年1月時点で30万台の設定が変更されていた。
  - 偽のサーバに接続させることで銀行やSNSのID盗用や不正プラグインのインストール。



Phishing and Banking Trojan
Cases Affecting Brazil
http://www.cert.br/docs/palestras/certbr-firstsymposium2012.pdf



The tale of one thousand and one DSL modems
http://www.securelist.com/en/blog/208193852/The_tale_of_one_thousand_and_one_DSL_modems

管理インタフェースにかかわる脆弱性

国内の事例

- 日本国内で販売されている、あるホームルータの脆弱性
  (https://www.telecom-isac.jp/news/news20120730.html)
  - デフォルト設定の問題
    - 管理パスワードマニュアル記載。
    - デフォルト設定でインターネット側からUIへのアクセス制御が不十分。
    - マニュアルには危ないので変更しろ、制限しろとは書いてある。
  - PPPoE接続用ID・パスワードの平文保存（侵入されたら盗まれる）。


Telecom-ISAC Japan

Telecom-ISAC Japan 2013/08/30

脆弱性保有ブロードバンドルータの状況調査
および対策について

情報通信基盤の安心・安全を確保するために活動している一般財団法人日本データ通信協会テレコム・アイザック推進会議（所在地：東京都港区、会長：飯塚久夫、以下、Telecom-ISAC Japan）は、国内主要通信事業者、ISP（インターネットサービスプロバイダ）の業界団体として、インターネットの安定運用に関わる事象の検出および対処に取り組んでおります。

1. 背景・概要

Telecom-ISAC Japanでは昨年7月30日に以下の注意喚起を行い、その状況を追い続けておりました。

【注意喚起】ロジテック製ルータの脆弱性、および、利用者が行うべき必要対策
https://www.telecom-isac.jp/news/news20120730.html

その結果、本年5月頃より発生している不正アクセスインシデントのいくつかは、本脆弱性の悪用によって得られた情報を攻撃者が利用したものであることが判明しました。そのため、主管省庁とも相談のうえ、会員企業および製品ベンダーによる対策実行について、状況調査から協力し支援していくことにいたしました。

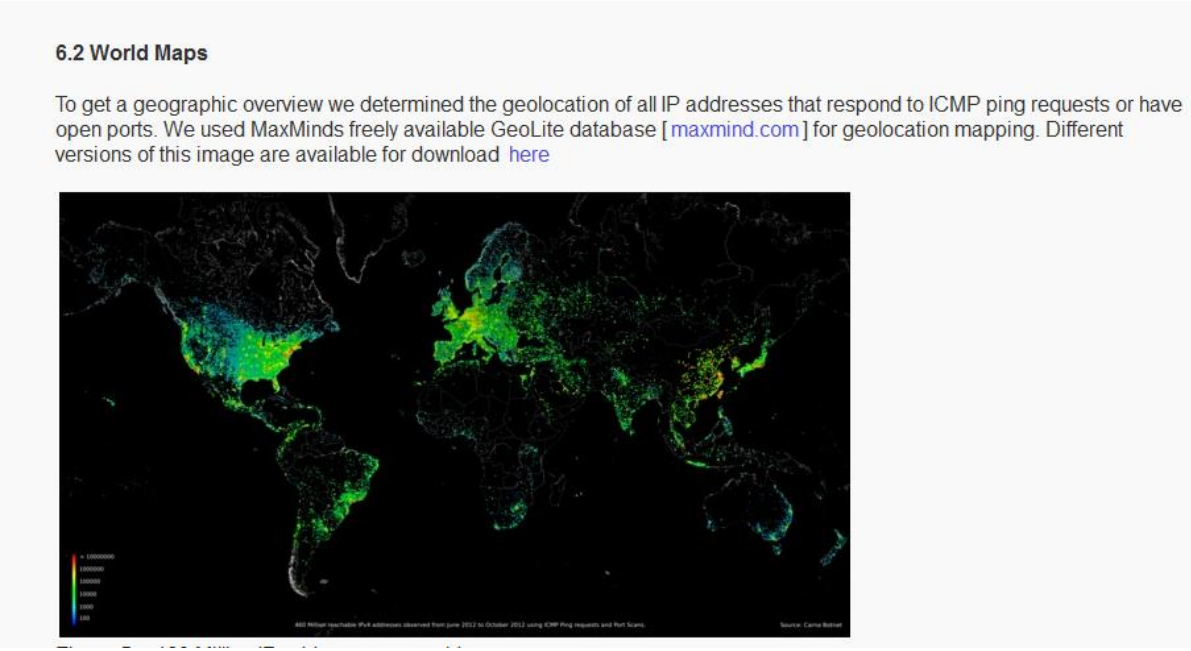
https://www.telecom-isac.jp/news/news20130830.htm

- 対策状況
  - 2012年3月に問題認識。5月に注意喚起。修正ファームウェアは2012年9月にリリースされ、機器メーカとしての対策は終了との認識。
  - 業界団体、各ISPからの注意喚起(2012年7月)。
  - しかし依然として数十万台が脆弱なままで残っている。
  - 再びメーカーやISP、業界団体から注意喚起(2013年08月)。
- 事件とのかかわり
  - 正当なユーザがオプションサービスに勝手に加入させられる。
  - 正当なユーザの接続が乗っ取られた。
  - 踏み台にして足跡を消す。

管理インタフェースにかかわる脆弱性

その他の事件

- Internet Census 2012　(http://internetcensus2012.bitbucket.org/paper.html)
- 2013/03に公開された匿名の論文。インターネットの現状を調査。
- 42万台のセキュリティ上の問題（管理認証がadmin/adminなど）の装置を勝手に使って、インターネット全体を調査。IPアドレスの存在確認やポートスキャンなど。
- 利用可能だったのは2000万台だったとしている(ホームルータの割合は不明)。
- 匿名の1名による行為。


6.2 World Maps

To get a geographic overview we determined the geolocation of all IP addresses that respond to ICMP ping requests or have open ports. We used MaxMinds freely available GeoLite database [maxmind.com] for geolocation mapping. Different versions of this image are available for download here

2013年セキュリティ動向

ホームルータのセキュリティ

家庭内ネットワークの現状とホームルータ

ホームルータに関連するセキュリティの現状

管理インタフェースにかかわる脆弱性

Universal Plug and Play

DNSにかかわる設定ミス(DNS Open Resolver)

ホームルータのセキュリティ上の問題は誰のリスクとなるのか

この問題の解決に向けて

Universal Plug and Playの脆弱性

問題の概要

- libUPnP(Universal Plug and Play)
  - 2013/01、ライブラリに複数の脆弱性が見つかり修正。CVE-2012-5958 CVE-2012-5959 CVE-2012-5960 CVE-2012-5961 CVE-2012-5962 CVE-2012-5963 CVE-2012-5964 CVE-2012-5965
  - 家庭用のホームルータやWebカメラ、IP電話機器など多数の機器で利用されているため、各社から注意喚起が実施された。
    - Rapid7、「Portable SDK for UPnP Devices (libupnp) contains multiple buffer overflows in SSDP」（http://www.kb.cert.org/vuls/id/922681）
    - JPCERT/CC、「Portable SDK for UPnP の脆弱性に関する注意喚起（https://www.jpcert.or.jp/at/2013/at130006.html）
  - Rapid7のレポートでは、対象は全世界で2300万以上とされる。UDPパケットひとつで外部から操作される可能性がある。
  - 組み込み系機器の脆弱性対応の現状。

Universal Plug and Playの脆弱性

問題の概要

- Universal Plug and Play
  - そもそもUPnPは家庭内など、限定的な範囲でリソースを共有する目的の実装であり、インターネット側から利用できるだけで危険と考えるべき。
  - UPnPプロトコルにはほかにも複数の問題が存在する。
    - UPnP対応CPEデバイスにインターネット側からアクセス可能な場合、port ネゴシエーションを悪用して内部ネットワークの任意のIPアドレスにポートスキャンが可能となる。
  - 世界で4000万～5000万のネットワーク対応機器がインターネット側からアクセス可能であるとの指摘もある。
  - SHODANによると日本国内でインターネット側からSSDPに応答するIPアドレスは270万台以上(世界中では28,612,883)。
  - 脆弱性保有台数に関する定量的データはない。

Top Countries	
China	7,114,638
Japan	2,795,619
United States	2,681,912
Korea, Republic of	2,328,184
Canada	1,364,776

www.shodanhq.com による1900/udpの検索結果

2013年セキュリティ動向

ホームルータのセキュリティ

家庭内ネットワークの現状とホームルータ

ホームルータに関連するセキュリティの現状

管理インタフェースにかかわる脆弱性

Universal Plug and Play

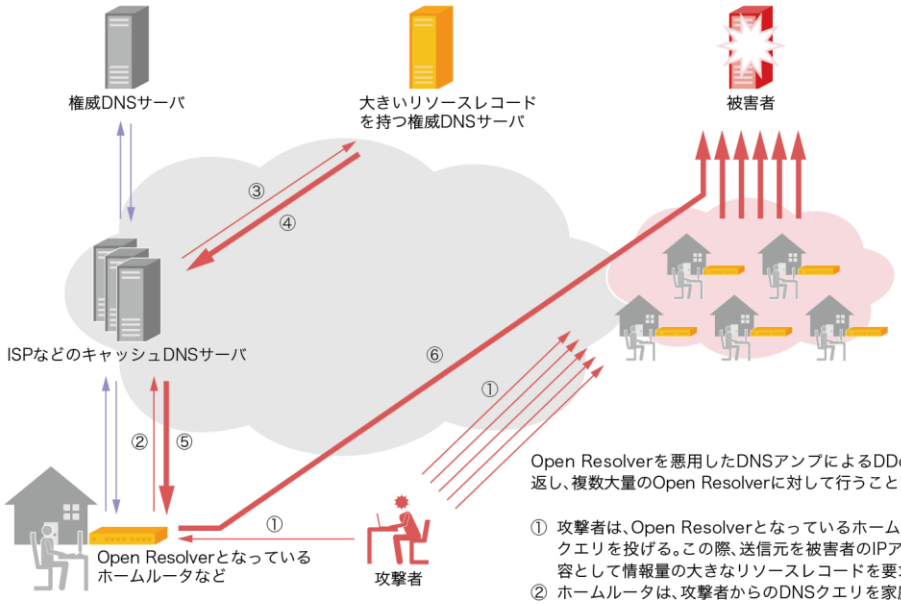
DNSにかかわる設定ミス(DNS Open Resolver)

ホームルータのセキュリティ上の問題は誰のリスクとなるのか

この問題の解決に向けて

DNSにかかわる設定ミス(DNS Open Resolver)

問題の概要



通常のDNS名前解決では、紫の線で示した通り、家庭内ネットワークの機器がホームルータに対してDNSクエリを送付し、ホームルータはISPなどの外部のキャッシュDNSサーバにそのクエリを転送する。ISPなどのDNSサーバは最終的にインターネット上の権威DNSサーバにクエリを送ることで、クエリに対応するリソースレコードをレスポンスとして得る。このレスポンスをホームルータに転送し、ホームルータはクエリを出した機器にレスポンスを渡す。

Open Resolverを悪用したDNSアンプによるDDoS攻撃では、次の手順を繰り返し、複数大量のOpen Resolverに対して行うことで、DDoS攻撃を発生させる。

① 攻撃者は、Open Resolverとなっているホームルータに対し、攻撃用のDNSクエリを投げる。この際、送信元を被害者のIPアドレスに詐称し、クエリの内容として情報量の大きなリソースレコードを要求する。
② ホームルータは、攻撃者からのDNSクエリを家庭内ネットワークからの要求と同様に処理し、ISPなどのDNSサーバに転送する。
③ ISPなどのDNSサーバでは、正当な利用者からの通信であるため、攻撃用のDNSクエリと正当なDNSクエリとを判別することができず、当該攻撃DNSクエリをインターネット上の権威DNSサーバに送付する。
④ 攻撃DNSクエリの内容に応じて、権威DNSサーバから情報量の大きなリソースレコードが、攻撃用のレスポンスとしてISPのDNSサーバに送付される。
⑤ ISPのDNSサーバは攻撃用のレスポンスをホームルータに転送する。
⑥ ホームルータは受け取った攻撃用のレスポンスを、送信元に転送する。この際送信元は攻撃者が詐称した被害者のIPアドレスとなっている。

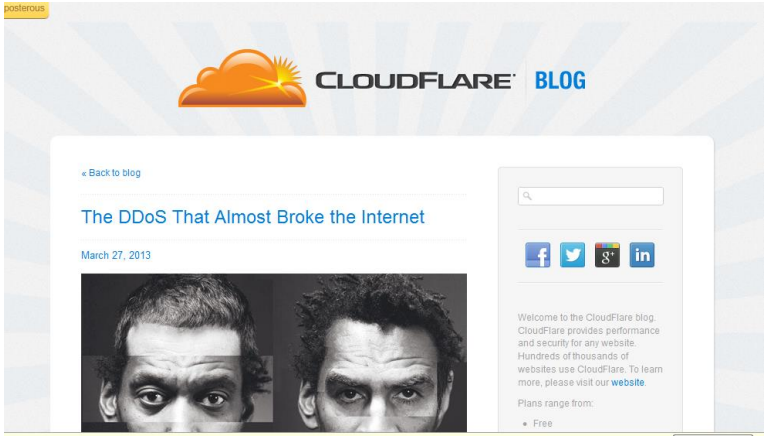
IIR Vol.20「ホームルータのセキュリティ」(http://www.iij.ad.jp/company/development/report/iir/020.html)より

- 概要
  - 多くのRRを持つripe.netなどへのqueryが攻撃に利用される。
  - 故意に多くのRRを登録した攻撃用のドメインも存在している(ddostheinter.netなど)
- 原因
  - 家庭内に提供する機能を、デフォルト設定で制限していない。

DNSにかかわる設定ミス(DNS Open Resolver)

事例:Spamhausに対する攻撃で 300Gbps

- 迷惑メール対策団体 Spamhaus に対する攻撃
  - 攻撃者不明（特定の迷惑メール送信業者によるものという憶測）。
  - 3月中旬から2週間程度継続。
  - 当初Spamhausの持つシステムに対して60Gbps~120Gbps程度の攻撃。
  - 当該環境が「固い」ことがわかったので、攻撃者はヨーロッパのインターネットエクスチェンジ(IX)に矛先を変更。
  - 設定ミスでDNSのopen resolver(インターネット側から利用できてしまう設定の緩い機器)となっている機器を踏み台にして300Gbpsの通信の集中を作り出す。

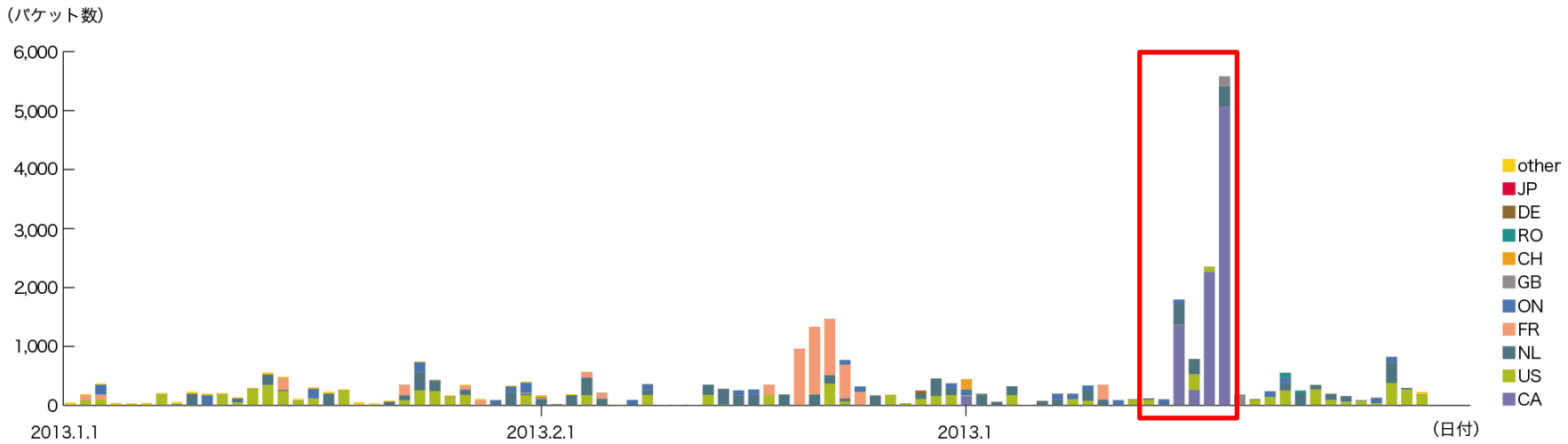


http://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet

DNSにかかわる設定ミス(DNS Open Resolver)

ハニーポットでの観測情報

- **DNSのopen resolverを悪用したDDoS攻撃**

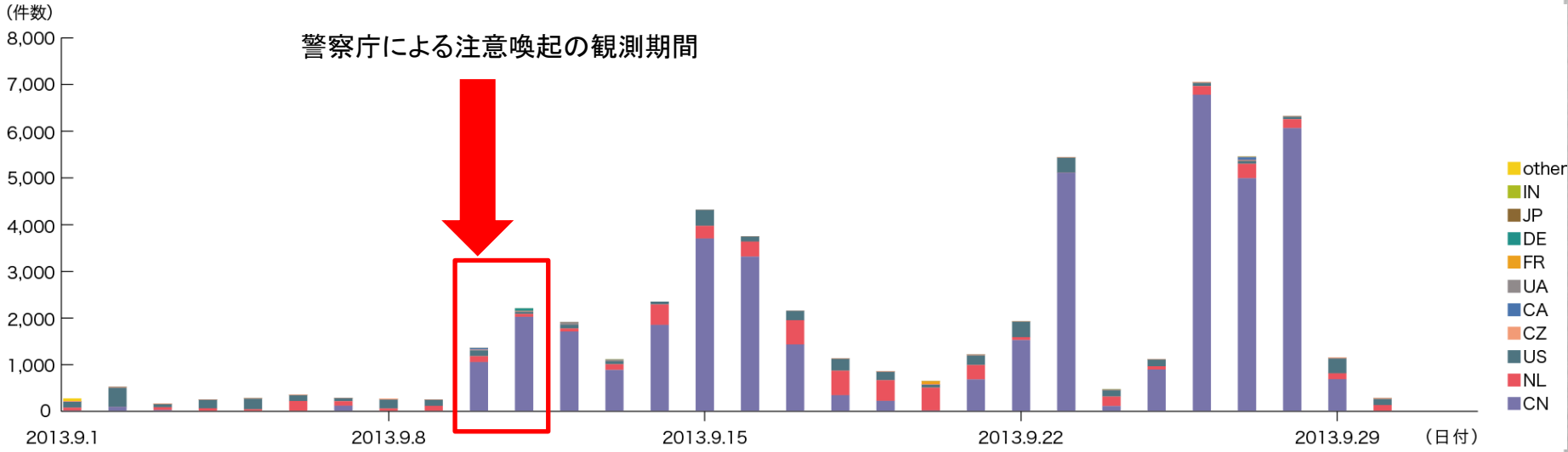


IIR Vol.19より：IIJで観測したOpenResolver悪用の様子(2013:Q1)

- Spamhaus への攻撃は、3月18日から22日ごろにかけて行われたと報告されているが、その期間攻撃に合致するような通信はIIJでは検出されず。
- 3月15日から18日にかけてカナダのIPアドレスからの通信が急増。この通信は、カナダの特定の事業者の2つのIPアドレスからに見えるもので、到着した通信の内容から、この2つのIPアドレスを狙ったDNSアンプ攻撃の試みであることが判明。

DNSにかかわる設定ミス(DNS Open Resolver) (2)

ハニーポットでの観測情報(2)



ハニーポットに到着した53/UDPの通信(IIR Vol.21 P7)

9月には警察庁より、中国を発信元とする53/UDPに対するアクセスが増加しているとして注意喚起が行われた。図-2にハニーポットに到着した53/UDPの通信について、発信元IPアドレスの国別分類を示すが、9月10日以降中国を送信元とした通信が非常に多くなっていることがわかる。

DNSにかかわる設定ミス(DNS Open Resolver)

対策と被害の状況

- CloudFlareによるapricot2013(2013/02月)の発表では、日本にもOpen resolverがそれなりに存在し、攻撃に加担しているとされている。
- 同様な手法によるDDoS攻撃の継続(**Prolexic** 167Gbpsなど)。
- Openresolvers.orgなどによる継続的な調査と警告(ただし、調査の手法や精度に難あり。referral などOpen Resolver以外にも増幅要因がある)。
- uRPF(BCP38)の推奨

- IIJの観測では、多くの攻撃者は攻撃前にDNS Open Resolver に関する調査を実施していない。だたやみくもに DNS queryを投げつけることで、DDoS攻撃に成功している様子がうかがえる(ただし、中国の一人を除く)。

Where are the open Recursors?

Country	Open Recursors	Country	Open Recursors
Japan	4625	Bangladesh	103
China	3123	New Zealand	98
Taiwan	3074	Cambodia	13
South Korea	1410	Sri Lanka	7
India	1119	Nepal	7
Pakistan	1099	Mongolia	5
Australia	761	Laos	4
Thailand	656	Bhutan	2
Malaysia	529	New Caledonia	2
Hong Kong	435	Fiji	2
Indonesia	349	Maldives	2
Vietnam	342	Papua New Guinea	1
Philippines	151	Afghanistan	1

www.cloudflare.com 18

http://www.apricot2013.net/__data/assets/pdf_file/0009/58878/tom-paseka_1361839564.pdf

2013年セキュリティ動向

ホームルータのセキュリティ

家庭内ネットワークの現状とホームルータ

ホームルータに関連するセキュリティの現状

ホームルータのセキュリティ上の問題は誰のリスクとなるのか

この問題の解決に向けて

ホームルータのセキュリティ上の問題は誰のリスクとなるのか

リスクの種類

- 個人のリスク
  - 個人とその通信にかかわる情報の漏えい。
  - 物理的被害。
- インターネット全体にとってのリスク
  - 多数の家庭環境が乗っ取られることによる犯罪などへの悪用や、DDoS攻撃など大量通信の発生。
  - 記録機能に乏しいホームルータが踏み台となることで、犯罪行為などで足跡を消すために悪用される。
- 企業など組織にとってのリスク
  - 従業員の利用する情報通信機器（特にノートパソコンやスマートフォンなど、持ち運び可能な機器）が家庭で汚染される可能性がある。
    - 社員が日常的に持ち歩いている私物スマートフォンの位置情報
    - BYODへの影響（家庭でマルウェアに感染したスマートフォンで仕事の情報に触れていいかどうか）
    - 従業員の持つ会社支給のスマートフォンが家庭で汚染される可能性
    - 標的型攻撃への応用（家族との通信の様子を知られることで、仕事場への攻撃に悪用される）

家庭内ネットワークの現状とホームルータ
マルウェアによる設定変更事件
管理インタフェースにかかわる脆弱性
Universal Plug and Play
DNSにかかわる設定ミス(DNS Open Resolver)
ホームルータのセキュリティ上の問題は誰のリスクとなるのか
この問題の解決に向けて

この問題の解決に向けて

精度の高い実態調査

- TelecomISAC Japan「**ネットワークデバイスの脆弱性保有状況調査**」
  - インターネット側から管理インタフェースへの接続
  - インターネット側UPnP/SSDPの受け入れ
  - DNS Amp/OpenResolver

  の3つについて調査を実施中。
- 調査の結果、全容を把握したあとに対策の検討を開始する。
- 調査結果
  (2013/11時点で非公開)

Telecom-ISAC Japan

Telecom-ISAC Japan 2013/06/17

ネットワークデバイスの脆弱性保有状況調査について

情報通信基盤の安心・安全を確保するために活動している一般財団法人日本データ通信協会テレコム・アイザック推進会議(所在地:東京都港区、会長:飯塚久夫(NECビッグローブ株式会社)、以下、Telecom-ISAC Japan)は、国内主要通信事業者、ISP(インターネットサービスプロバイダ)の業界団体として、インターネットの安定運用に関わる事象の検出および対処に取り組んでおります。

I. 背景・概要

Telecom-ISAC Japanでは数年前より、ルータなどのネットワークデバイスの脆弱性問題について議論を重ね、対策検討を行ってまいりました。

本年2月にはUPnPの脆弱性が国内外で指摘され、3月にはDNSのOpen Resolverを踏み台とした大規模なDoS攻撃が発生するなど、ネットワークデバイスの脆弱性を利用したサイバー攻撃の脅威が高まっております。

さらに、ネットワークデバイスの脆弱性を悪用されるとサイバー攻撃の踏み台に利用されるだけでなく、ネットワーク内への不正侵入やデバイス内保存情報の不正取得などの被害に及ぶ場合もあります。

Telecom-ISAC Japanでは、このような攻撃被害の最小化を図っていくために、日本国内のネットワークに接続するデバイスの脆弱性保有について、実態把握を目的とした調査を6月以降順次行ってまいります。

II. 調査内容・時期について

この調査は、予め了解をいただいたISPのIPアドレス帯に対して、ネットワークにつながるデバイスがどのような状態であるかを、簡易な通信コマンドで確認するものです。ネットワーク利用者に負荷をかけるものや、通信の内容を見るようなものでは一切ありません。

https://www.telecom-isac.jp/news/news20130617.html

対策に向けて

- なぜホームルータは脆弱なまま放置されるのか
  - 利用者の問題:
    - 利用者は家電のように扱い、情報通信機器として「運用」していない。
  - 機器の問題:
    - デフォルト設定。
    - 管理者認証がデフォルトでadmin/admin。
    - パスワードをplain textで保存。
    - 設定確認手法や通信記録の機能が未成熟。
    - 対策ファームウェアをリリースしても使ってもらえない。
- この現状に、家庭内ネットワークに新しい装置がどんどんどんどん追加されている(状況を放置すれば悪化する)。

この問題の解決に向けて

対策に向けて(2)　対策活動を家庭に持ち込むためには

- 利用者として
  - 家庭内ネットワークに接続する装置の把握。
  - それぞれのファームウェアバージョンの把握、設定の健全性の確認、日常的な動作ログの確認。
  - これらを補助するツール。
- 製品開発者として
  - デフォルトで「安全な製品」を作ることを目指す。
  - 問題と修正ファームウェアの認知手法の向上。
  - 自動アップデートなど利用者の手間の軽減手法の確立。
- サービスプロバイダとして
  - 利用者に紹介した製品について開発者と協力して対処する。
  - 外部からの設定の健全性の確認。
  - CPEデバイスマネージドサービス / Walled Garden の推進。

- 第4の通信上の規制の検討
  - 管理インタフェース IP80B　　おそらく困難
  - UPnP/SSDP IP1900B、URLフィルタ的対策　　おそらく容易
  - DNS IP53B/OP53B　　頑張れば可能

最後に

- お願い

- 今日、家に帰ったらホームルータにログインし、以下の作業をしてください。
  - ホームルータのファームウェアが最新であることを確認。
  - 管理者のID、パスワードを変更。
  - ホームルータの設定を見直して、外部から勝手に利用されないことを確認。

まとめ

- 最近のセキュリティ動向
- ホームルータのセキュリティ

IIJ Internet Initiative Japan

ご清聴ありがとうございました

お問い合わせ先　IIJインフォメーションセンター
TEL：03-5205-4466（9：30～17：30 土/日/祝日除く）
info@iij.ad.jp
http://www.iij.ad.jp/

Ongoing Innovation