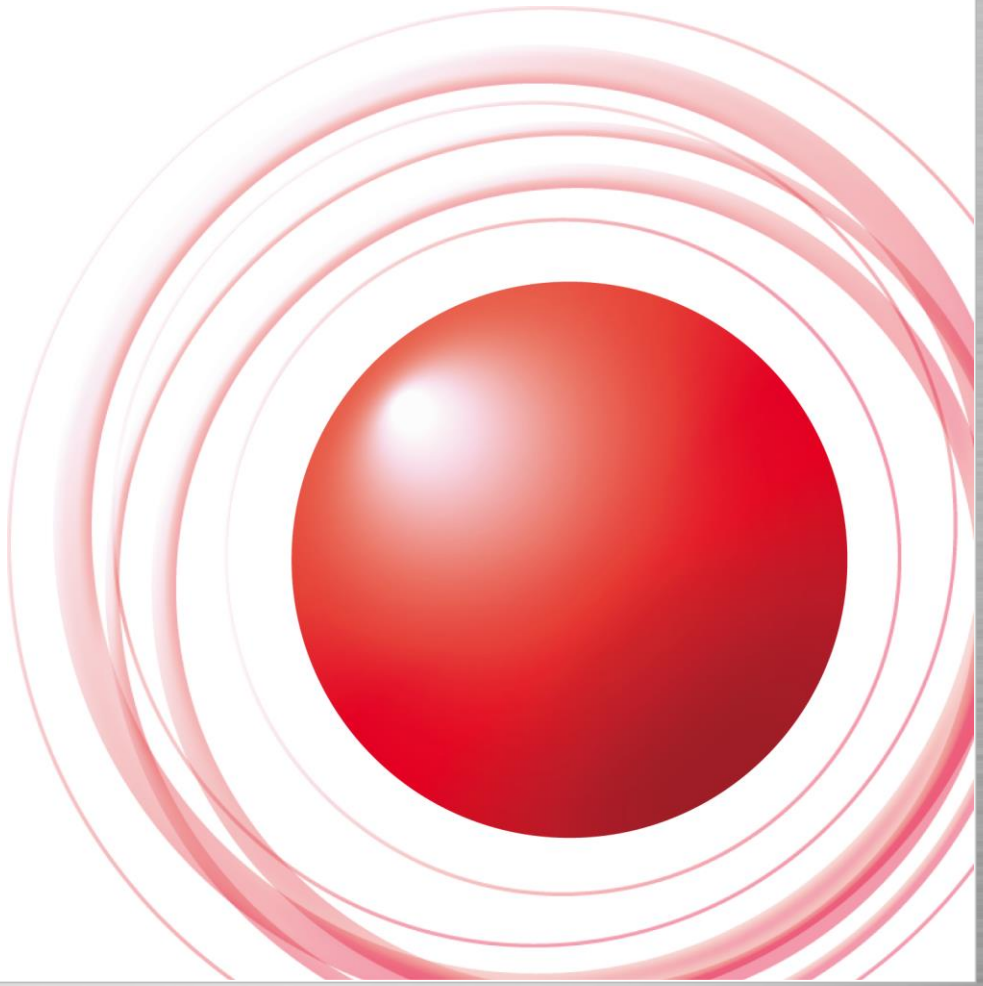
沖縄ICTフォーラム2013 in 宮古島

サイバーセキュリティ最前線:
宅内危機！ CPEデバイスのセキュリティ

IIJ
Internet Initiative Japan



2013/06/28

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
（TelecomISAC Japan　運営委員）
齋藤衛

Ongoing Innovation

宅内機器の脆弱性

脆弱性の例とリスク

CPEデバイス

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)

この問題の解決に向けて

宅内機器の脆弱性

脆弱性の例とリスク

- 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(2012/11)。
- 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)

- それぞれ、脆弱性によりこれらの機器の機能が第三者に悪用された時には、プライバシーの侵害など個人生活の範囲の影響が考えられる。

宅内機器の脆弱性

CPEデバイス

- CPE:Customer Premises Equipment（顧客宅内機器）
- ホームルータ
  - インターネットに接続するための機能(PoE終端、NATなど)
  - 宅内ネットワークを構築するための機能(有線、無線LAN、DHCP、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）
  - 管理インタフェース（Web UI）

- ホームルータの設定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。

宅内機器の脆弱性

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

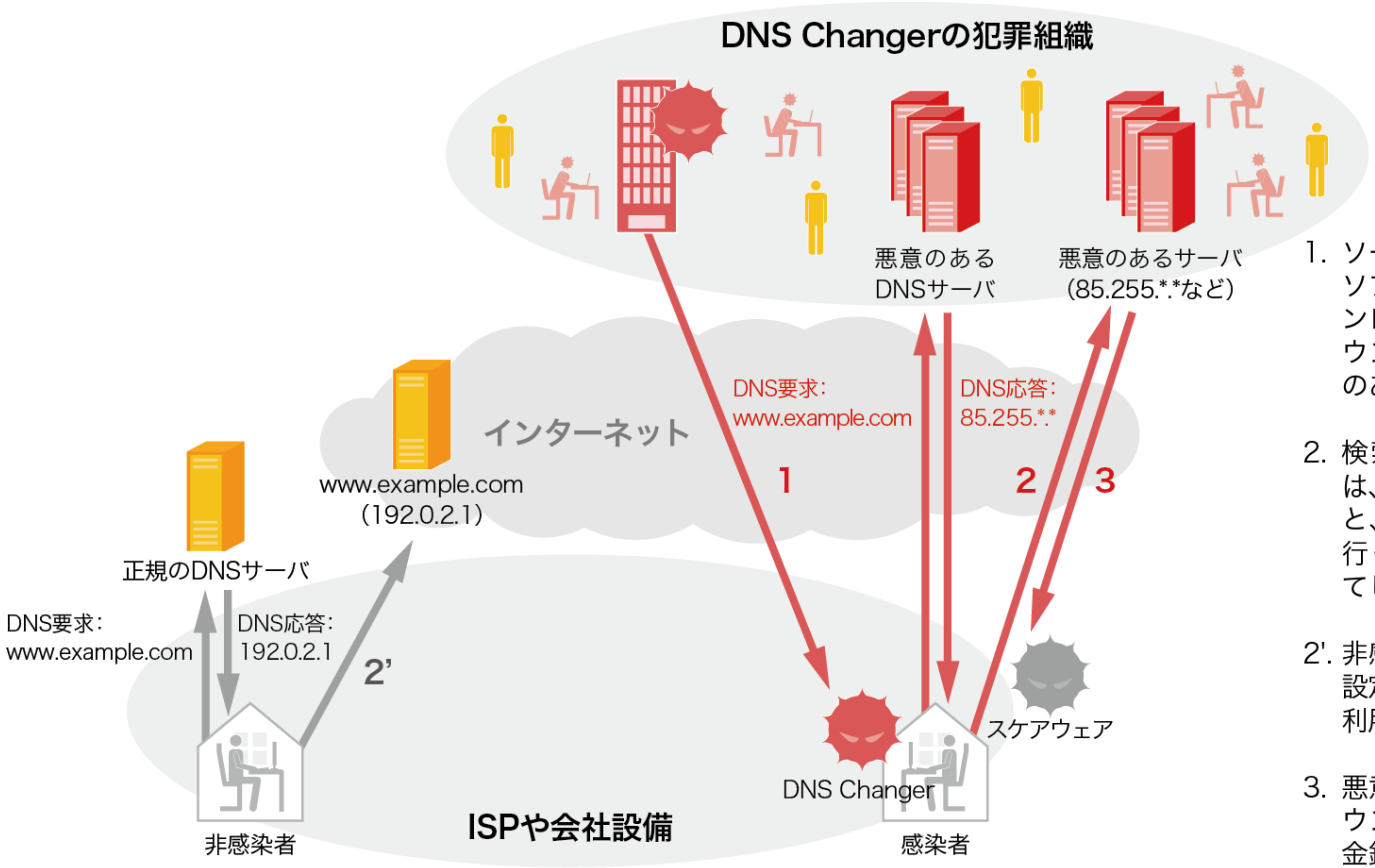
Universal Plug and Play

DNSにかかわる設定ミス(DNS Open Resolver)

この問題の解決に向けて

マルウェアによる設定変更事件

DNS Changer



1. ソーシャルエンジニアリング(動画再生ソフトウェアに偽装したファイルをダウンロードさせるなど)やドライブバイダウンロードで感染させ、DNS設定を悪意のあるサーバに書き換える。

2. 検索エンジンなど、特定のサイト(例では、www.example.com)にアクセスすると、悪意のあるDNSサーバに問い合せに行くため、悪意のあるサーバに誘導されてしまう。

2'. 非感染者の場合、ISPなどのDNSサーバが設定されて正常なDNSの応答が返るため、利用者の要求通りのサーバに接続される。

3. 悪意のあるサーバからスケアウェアをダウンロードさせるなどして、利用者から金銭を詐取する。

IIJ Internet Infrastructure Review (IIR) Vol.15 より
http://www.iij.ad.jp/company/development/report/iir/015.html

マルウェアによる設定変更事件

DNS Changer(2)

- 偽DNSのエントリ1万4千
  - 検索エンジン Google, Yahoo!,Bing, Ask.com
  - 広告事業 Google Ads, Overture,Doubleclick
  - ソフトウェア更新サーバ マイクロソフト、アドビ、セキュリティ対策ソフト
  - アダルトサイト、出会い系サイト
  - ドメイン事業者 (使用されていないドメインのハイジャック)
  - wikileaks.orgなどのアクセス数の多いサイト
  - マルウェアTDSSなどのサーバ
- 利用者の被害
  - 検索結果からの不正サイトへの誘導
    - 検索結果のHTMLの改ざんなどではなく、DNSクエリにより検索結果をクリックしたことを検知し、DNSのレスポンスを改ざんした
  - FAKEAVのライセンス料
- 広告産業への被害
  - 有名サイトの広告の置き換え
- その他
  - 犯人グループが用意した広告へのアフィリエイト課金

トレンドマイクロ「Rove Digitalの壊滅」より
https://inet.trendmicro.co.jp/doc_dl/select.asp?type=1&cid=81

マルウェアによる設定変更事件

DNS Changer(3)

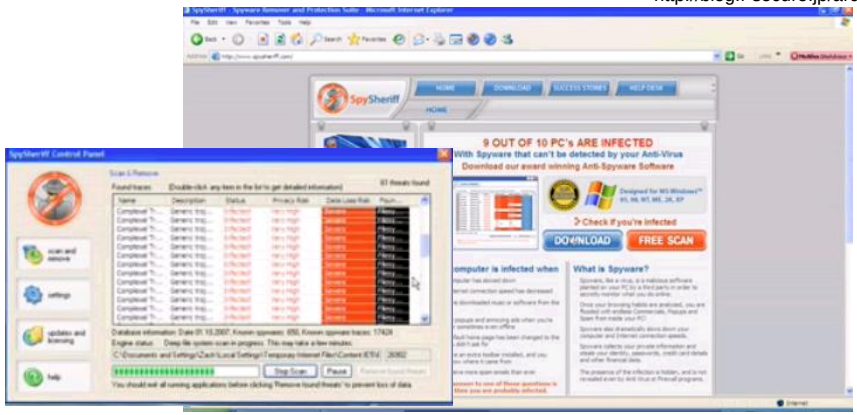
- MBRに感染し、駆除後も再起動により再び設定変更をする。
- ホームルータのDNSの設定変更を試みる(IIJでは実際の被害は未確認)
  - UTSTARCOM,routers from BNSL(India),D-Link,Linksys,OpenWRT/DD-WRT,A-Link,Netgear,ASUS ZVMODELVZ Web Manager, SMC など(ISCのMerike KaeoによるNanog54 Security BoFの発表資料より)
- スケアウェア(FAKEAV)のインストール。

FAKEAV(AntiMalware)の様子
http://www.threatexpert.com/report.aspx?md5=9f09ff8dba53c3f3734295528297d015

FAKEAV(Protection Center)の様子
http://www.mcafee.com/japan/security/virD.asp?v=DNSChanger.bu

FAKEAV(MacGuard)の様子
http://blog.f-secure.jp/archives/50605046.html

FAKEAV(WindowsAntiSpyware)の様子
http://www.gfi.com/blog/movie-time-dns-changer-trojan/



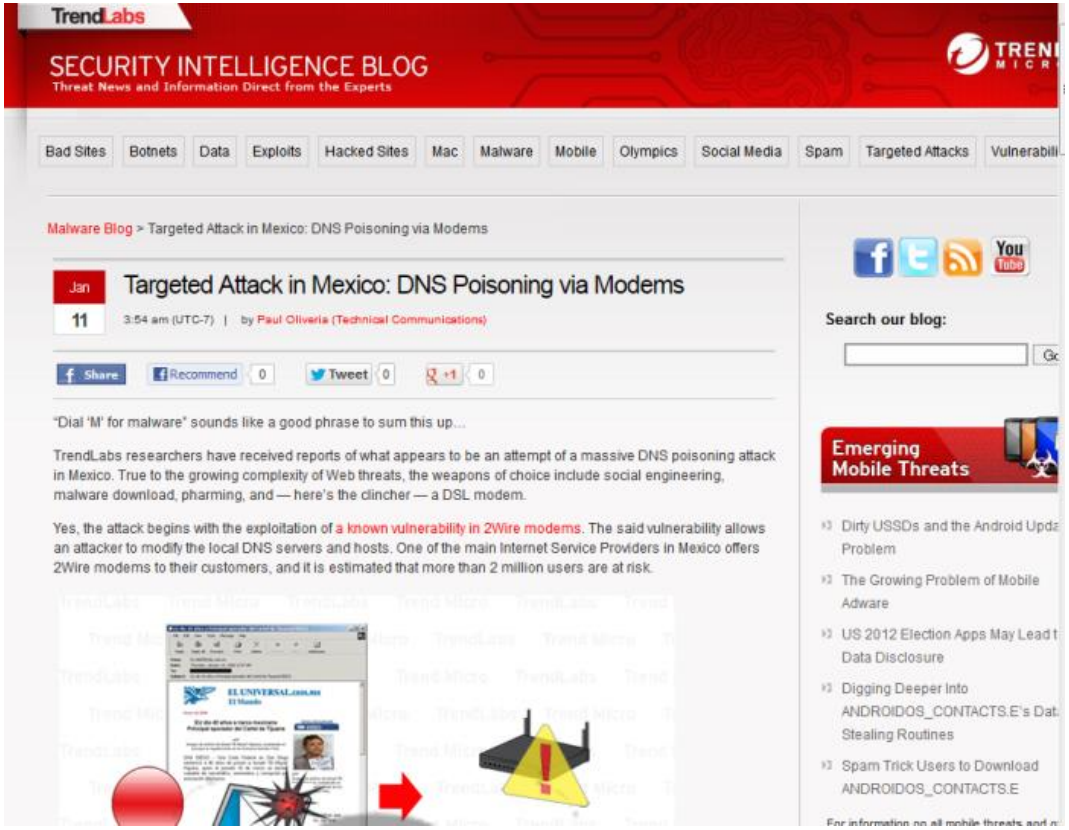
FAKEAV(SpySheriff)の様子 http://www.youtube.com/watch?v=ve5KU01JYA8

マルウェアによる設定変更事件

その他のマルウェアによるホームルータ設定変更事件

2012年メキシコ

- ウイルスがルータの設定を変更し、銀行*banamex.com*へのアクセスを偽装サーバに。



Targeted Attack in Mexico: DNS Poisoning via Modems
http://blog.trendmicro.com/trendlabs-security-intelligence/targeted-attack-in-mexico-dns-poisoning-via-modems/

宅内機器の脆弱性

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

事例

対策と被害の状況

Universal Plug and Play

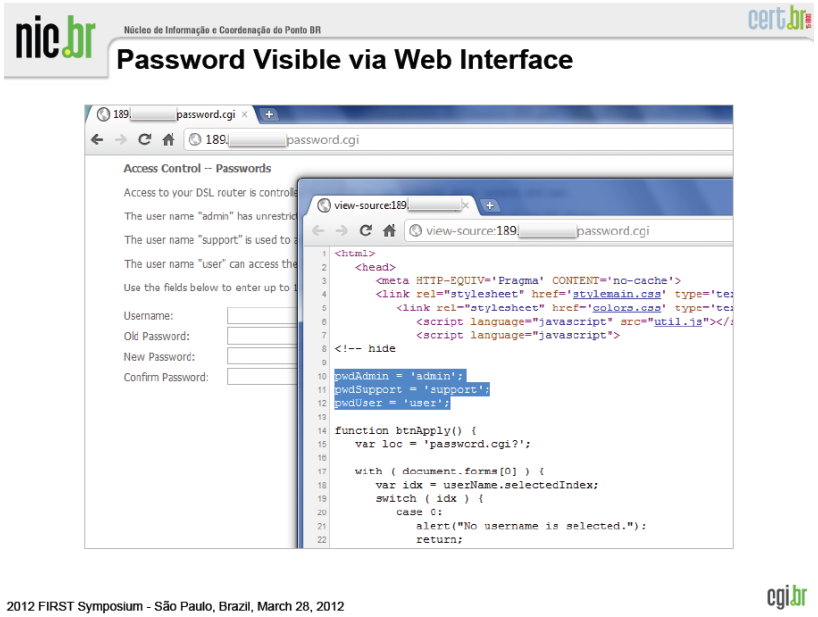
DNSにかかわる設定ミス(DNS Open Resolver)

この問題の解決に向けて

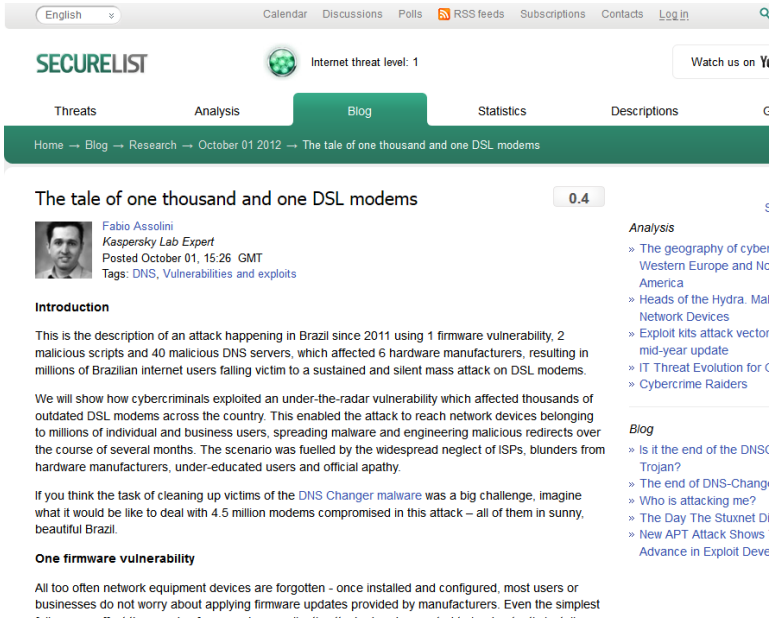
管理インタフェースにかかわる脆弱性

国外の事例

- 2011年ブラジルやヨーロッパ
  - ホームルータやADLSModemの脆弱性を悪用し、インターネット側から直接管理者権限で参照用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。
  - 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ホームルータの脆弱性
- 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へのアクセス制御なし。
  - 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。
- PoE接続用ID・パスワードの平文保存。

Telecom-ISAC Japan
Telecom Information Sharing and Analysis Center Japan

Telecom-ISAC Japan 2012/07/30
2012/09/24 更新

【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

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、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. 概要

ロジテック株式会社(以下、ロジテック)より、「ロジテック 300Mbps無線LANブロードバンドルータの一部において、セキュリティに脆弱性があることが判明」したと5月16日に、そして、「セキュリティを強化したファームウェア」を公開したと5月24日にアナウンスがありました。

ロジテック製300Mbps無線LANブロードバンドルータ
(LAN-W300N/R、LAN-W300N/RS、LAN-W300N/RU2)に関するお詫びとお願い
http://www.logitec.co.jp/info/2012/0516.html?link_id=out_oshirase_20120516_2_2

「この脆弱性により、インターネット接続に必要な「PPPoEの認証ID」および「PPPoEの認証パスワード」が外部より取得される可能性」があることから、インターネットの安全な利用に及ぼす影響の大きさを鑑みて、Telecom-ISAC Japanでは、この脆弱性に関する注意喚起をいたします。該当ルータの利用者は以下の対策を全て実行することを強く推奨いたします。

1. ファームウェアのバージョンアップ

https://www.telecom-isac.jp/news/news20120730.html

管理インタフェースにかかわる脆弱性

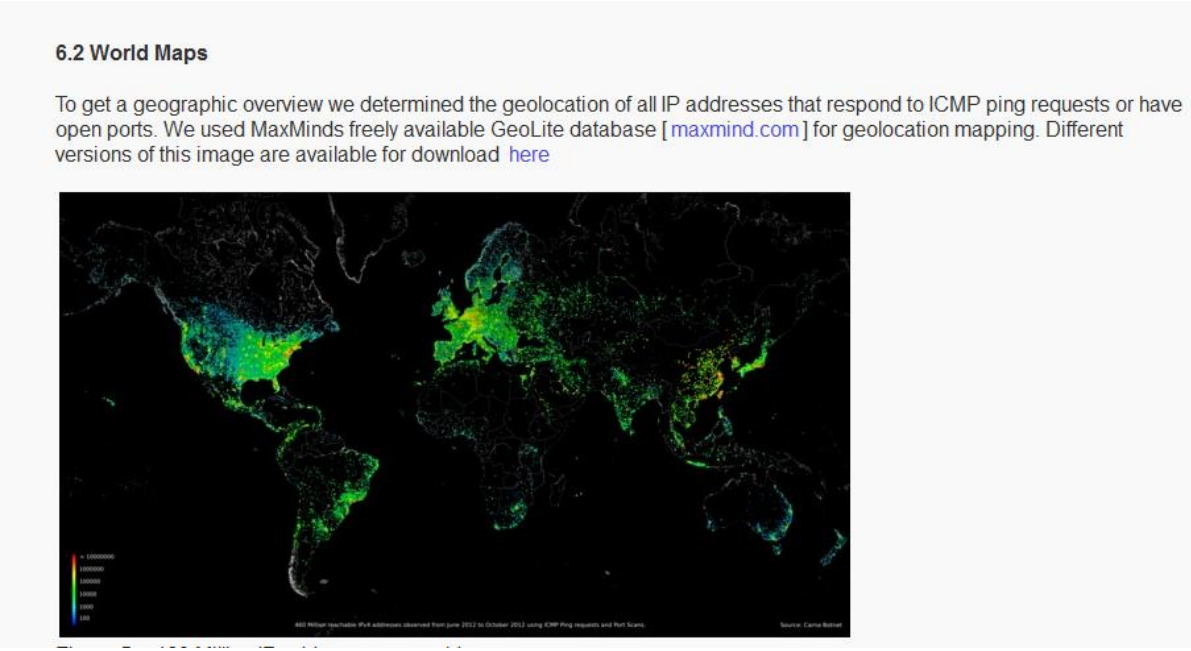
対策と被害の状況

- 対策状況
  - 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。
  - ■ ■ ■ ■ ■ ■ ■は■ ■ ■ (2013/06時点)。
  - 年末年始に■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■イベントが。
- 被害状況
  - ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■かもしれない。
  - 勝手に■ ■ ■ ■ ■ ■ ■ ■ ■させられ、■ ■ ■ ■ ■ ■ ■ ■される かもしれない。
  - ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■かもしれない。
  - 不正ログインについてプレスリリースを打って、インターネットウォッチとかに記事として載ってしまうかもしれない。

管理インタフェースにかかわる脆弱性

対策と被害の状況

- Internet Census 2012　(http://internetcensus2012.bitbucket.org/paper.html)
- 2013/03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。
- 実際に利用可能だったのは2000万台だったとしている。
- 匿名の1名による行為。



宅内機器の脆弱性

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

問題の概要

DNSにかかわる設定ミス(DNS Open Resolver)

この問題の解決に向けて

Universal Plug and Play

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
  - 家庭用のブロードバンドルータや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。

Universal Plug and Play

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。

www.shodanhq.com による1900/udpの検索結果

宅内機器の脆弱性

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

Libupnpの脆弱性

DNSにかかわる設定ミス(DNS Open Resolver)

問題の概要

事例

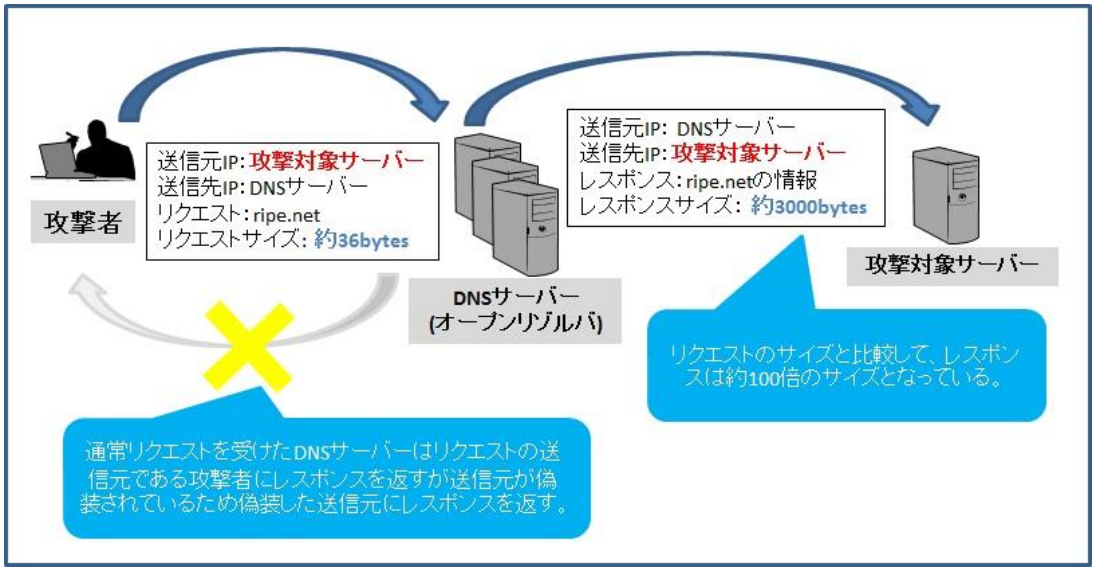
対策と被害の状況

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

- 概要



IBM/ISS Tokyo SOC Report より
https://www-304.ibm.com/connections/blogs/tokyo-soc/entry/dnsreflection?lang=ja

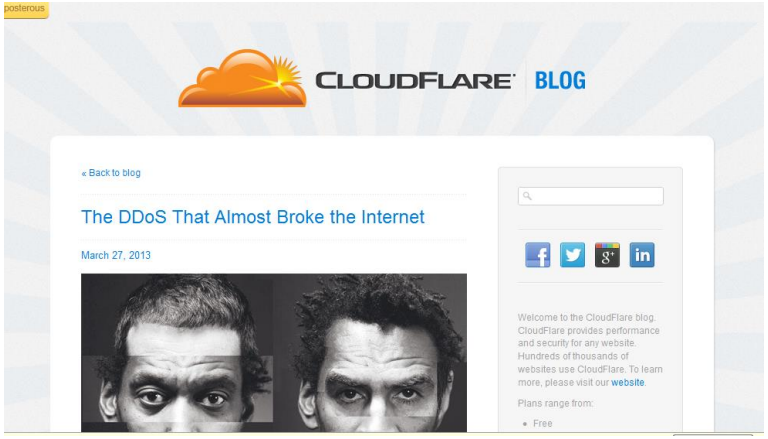
  - 多くのRRを持つripe.netなどへのqueryが攻撃に利用される。
  - 故意に多くのRRを登録した攻撃用のドメインも存在している(■ ■ ■ ■ ■ ■.netなど)

- 原因
  - ホームルータで家庭内に提供する機能をデフォルト設定などで適切に制限していない。

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。
  - ホームルータの設定で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。

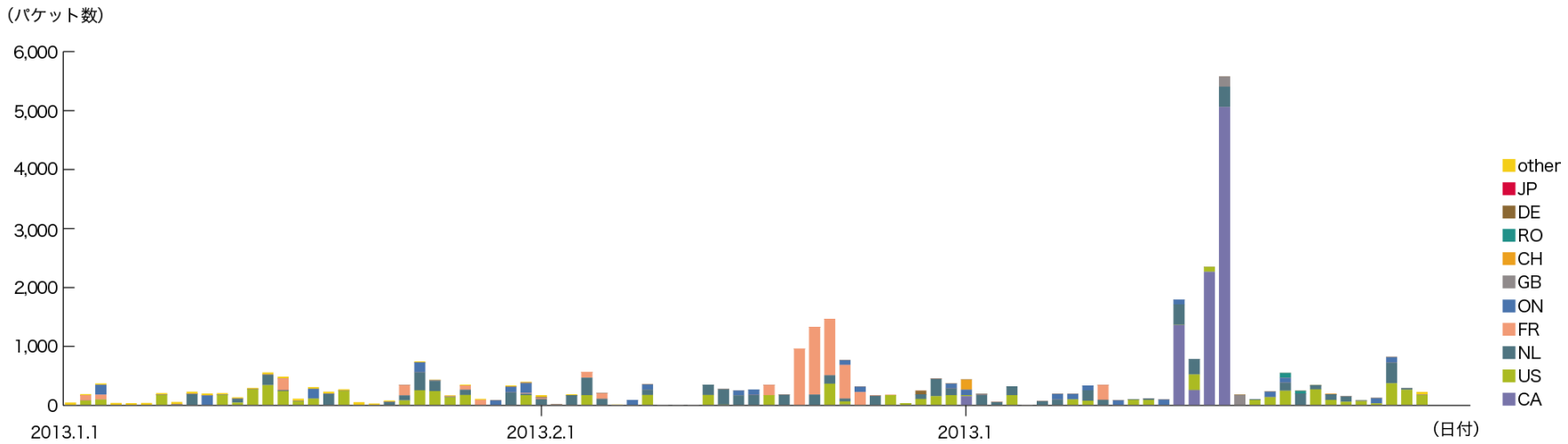


http://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet

DNSにかかわる設定ミス(DNS Open Resolver)

事例

- **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)

対策と被害の状況

- CloudFlareによるapricot2013の発表では、日本もそれなりに攻撃に加担していたとされている。
- 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（ただし strict mode じゃないと意味がない！）

- IIJの観測では、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。

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

宅内機器の脆弱性

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

Libupnpの脆弱性

DNSにかかわる設定ミス(DNS Open Resolver)

この問題の解決に向けて

精度の高い実態調査

対策の検討

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、全容を把握しあとに対策の検討を開始する。
- ■■■■■■■
  - ■■■■■■■■■
  - ■■■■■■■■■
  - ■■■■■■■■■

  - インターネットユーザ8千万人
  - 1世帯当たりの人数2.13人
  - インターネット接続世帯 3755万世帯
  - 粗々で約■■台がどれかの問題に該当

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CPEデバイスは脆弱なまま放置されるのか
  - 家庭をインターネットに接続するための装置であり、いったん動き出すと、利用者はそれ以上その設定が健全かどうかの確認をしない。
  - 利用者から専用機器に見えており、ソフトウェア/ファームウェアをアップデートするところに思い至らない。
  - 利用者は一度設定した機器の状態を確認するような「運用」を行っていない。
  - PCなどと違い、自動アップデートなどの仕組みが整備されておらず、対策がリリースされても気づきにくい。
  - 利用者は新しいファームウェアの存在を知ったとしても、通信を中断するリスク、設定をし直すリスクから適用しにくい。
  - CPEデバイスの動作ログが未熟であり、第三者に悪用されたことを記録（その記録をもとにした検知、警告）が実施しにくい。
  - 一般に、人は他者のリスクを自分の問題として把握しにくい。多少攻撃に悪用されていたとしても、インターネットが利用できていればそれでよい。
- この環境に、新しい装置がどんどんどんどん追加されていっている（状況を放置すれば悪化するのみ）。

対策に向けて(2)

- 何が必要なのか(みんなでやれば何とかなる前提では)
- 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
  - 「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。

対策に向けて(3)

- 何が必要なのか(どうにもならない前提では)
- 第4の通信上の規制も視野に入る
  - IP80B　　たぶんありえない
  - IP1900B、URLフィルタ的対策　　たぶん容易
  - IP53B/OP53B　　たぶん頑張れば可能 (white listなど)

まとめ

- 宅内機器の脆弱性
- 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)
- この問題の解決に向けて

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