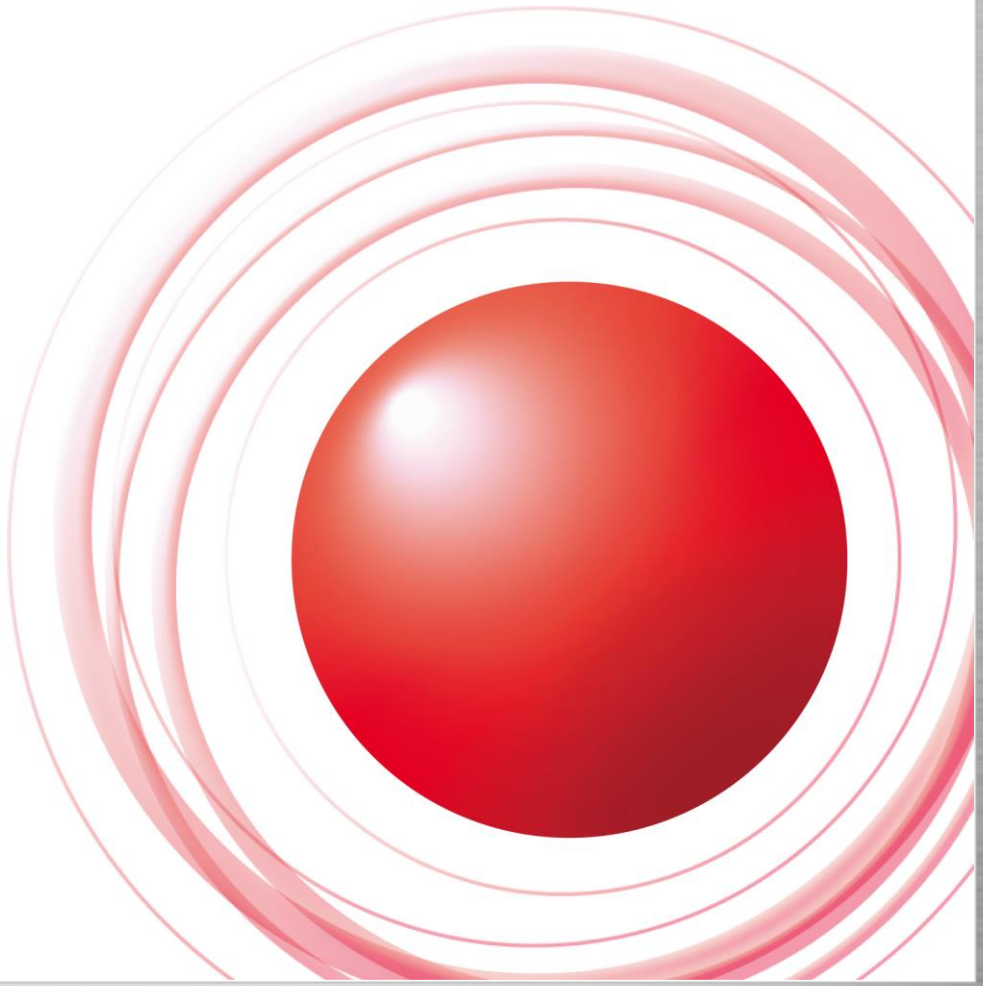
サイバーセキュリティセミナー 知らないと怖い！サイバーセキュリティの現状と今後

「IoT×AIで加速する第４次産業革命に立ち向かうために」 ~IoT全盛時代のリスクとMiraiボットについて~



2016/11/24
JNSA「脅威を持続的に研究するWG」
株式会社インターネットイニシアティブ
セキュリティ本部長
齋藤 衛

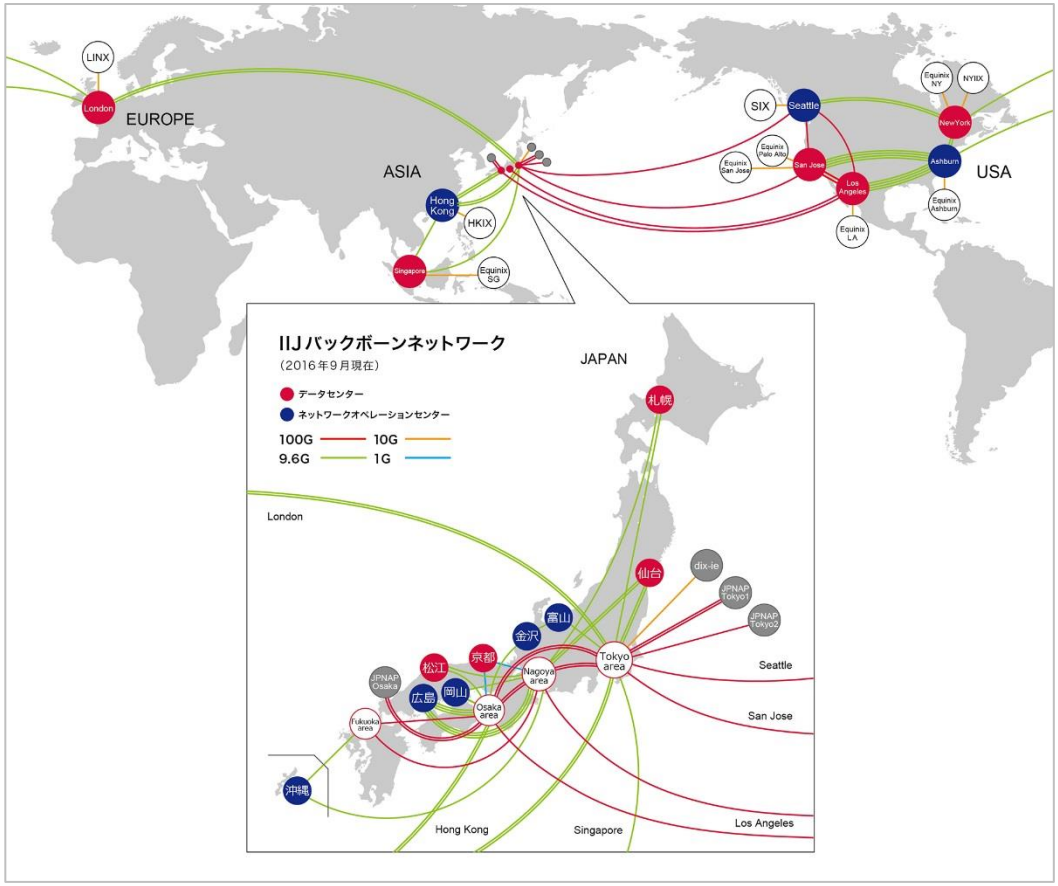
Ongoing Innovation

wizSafe

IIJについて

国内最大級のバックボーンネットワークを構築、運営

大容量の高速デジタル回線で、DC（データセンター）及びNOC（ネットワークオペレーションセンター）間を接続。世界的にも評価の高い運用/監視技術が、日本のインターネットを支えています。



松江データセンターパーク

2011年4月に島根県松江市に開設した、日本初のコンテナ型データセンター。低コストで高いサーバ収容効率や容易な拡張を実現。

外気冷却を利用し、全体の消費電力を約40%削減。

wizSafe

自己紹介

齋藤　衛（さいとう　まもる）

株式会社インターネットイニシアティブ セキュリティ本部長
1967年生まれ。1993年中央大学大学院 理工学研究科 管理工学専攻修了。

1995年株式会社インターネットイニシアティブに入社。法人向けファイアウォールサービスに従事の後、法人向けセキュリティサービスの 開発(マネージドセキュリティサービス、IDSサービス、DDoS対策サービスなど)、セキュリティサービス担当プロダクトマネージャを経て、現職。

2001年よりIIJグループの緊急対応チーム IIJ-SECTの活動を行う(IIJ-SECTは2002年にFIRSTに加盟)。ICT-ISAC Japan (旧テレコムアイザックジャパン)、日本セキュリティオペレーション事業者協議会、テレコム・セプターなど複数の団体の運営委員。内閣官房、総務省、警察庁などの研究会やWGなど複数の場で活動を行う。共訳書として「ファイアウォール構築 第二版」(オライリー・ジャパン) 。IIJ-SECTの活動は平成21年度「経済産業省商務情報政策局長表彰（情報セキュリティ促進部門）」を受賞。

平成27年より兵庫県警察サイバーセキュリティ対策アドバイザー。厚生労働省社会保障審議会年金事業管理部会委員。日本年金機構アドバイザー。

IoT全盛時代のリスク

Mirai Botについて

wizSafe

IoT全盛時代のリスク

IoTとは

- IoT(Internet of Things)
  - 通信機能を持つ装置が、装置同士やクラウド環境などと自律的に相互通信を行うことで機能を提供するようになるネットワーク環境。
    - 従来単体で動作していた装置のネットワーク化。
    - 人が介在しないで自律的に動作。
    - ネットワークに接続された装置の数が爆発的に増える。

- 今日IoTがある場所
  - 家庭：スマートフォン、エアコン、スマートTV、スマートメータなど。
  - オフィス、会場施設など：ビル施設管理システム、監視カメラなど。
  - 公共の場所：自動販売機、デジタルサイネージ、テレメトリー（遠隔計測）システム、コンビニのスマート端末やATMなど。

- 今日のIoTの実装
  - Windows,組み込みLinux、Androidなど。
  - 脆弱性などの問題が内在しないわけがない。

wizSafe

2016年におけるIoT

- 個人生活にかかわるもの
  - スマートフォン、タブレット、Google 眼鏡、Apple 時計
  - ヘルスケアデバイス
  - 自動車
- 家庭にかかわるもの
  - スマート家電(TV、DVR,エアコン、電子レンジ、トイレなど)
  - スマートメータ
  - HEMS（Home Energy Management System、電気、ガスなど）
  - リモコン

wizSafe

IoT全盛時代のリスク

2016年におけるIoT

- 公共の場にかかわるもの
  - ATM，自動販売機
  - デジタルサイネージ
  - 監視カメラ
- 企業等にかかわるもの
  - 照明
  - エアコン
  - 入退室管理
  - 監視カメラ

デジタルサイネージ（品川駅）

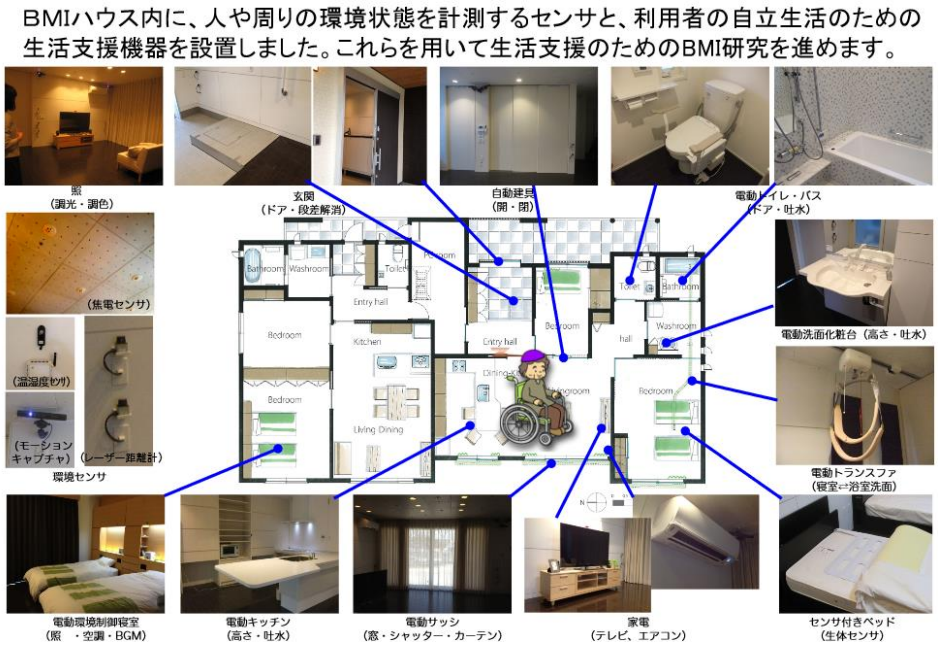
牛丼屋の券売機

wizSafe

近未来におけるIoT

- 家庭に数百～1,000個くらいのIoT装置があることを想定。
- BMIハウス
  - 総務省予算（高齢化社会対応）。京都府に実在。高齢者や障がい者などの自立、健常者との共同生活の実験。
  - 「家の形をしたロボット」。

http://www.atr.jp/topics/CNS20121101/cns20121101_ATR.pdf



wizSafe

IoT全盛時代のリスク

実際の事件

News & Trend 日経コンピュータ

テレビや冷蔵庫がスパムの踏み台に

IoTを狙ったサイバー攻撃が本格化

2014/02/13

勝村 幸博＝日経コンピュータ （筆者執筆記事一覧）

出典：日経コンピュータ 2014年2月6日号p10
（記事は執筆時の情報に基づいており、現在では異なる場合があります）

記事一覧へ >>

シェア ツイート B! ブックマーク

セキュリティベンダーの米プルーフポイントは2014年1月中旬、インターネットに接続されたテレビや冷蔵庫などを悪用した、大規模なスパム（迷惑メール）送信を確認したとして注意を呼びかけた。2013年末から2014年初頭にかけた2週間で、10万台以上の機器から75万通以上のスパムが送られたという。今後、IoT（モノのインターネット）を悪用したサイバー攻撃は確実に増える。ベンダーとユーザーの両方が警戒する必要がある。

インターネットにつながる機器の悪用は、国内でも以前から確認されている。悪用される主な原因は、パスワードを設定しないといった設定の不備や、ファームウエアの脆弱性だ。例えば2004年、ネットに接続できる東芝製HDDレコーダーがスパムの踏み台に悪用された。最近では、2013年4月以降、ロジテックの無線LANルーターが乗っ取られ、DDoS（分散サービス妨害）攻撃に悪用されている。

Baby Monitor Hacking Alarms Houston Parents

By Alana Abramson Aug 13, 2013 12:43pm

A Houston couple is still shaken after saying they heard the voice of a strange man cursing and making lewd comments in the bedroom of their 2-year-old daughter.

When Marc Gilbert and his wife Lauren entered the room, the voice cursed them as well.

The creepy voice — which had a British or European accent — was coming from the family's baby monitor that was also equipped with a camera. A hacker apparently had taken over the monitor.

The incident occurred on Aug. 10 as Marc Gilbert was doing the dishes after his birthday dinner and he heard strange noises coming from his daughter Allyson's room while she was sleeping, Gilbert said.

"Right away I knew something was wrong," he told ABC News.

As he and his wife got closer to the room, they heard the voice calling his daughter an "effing moron," and telling her,"wake up you little slut."

Baby monitor hacked by man who verbally abused couple's two-year-old daughter

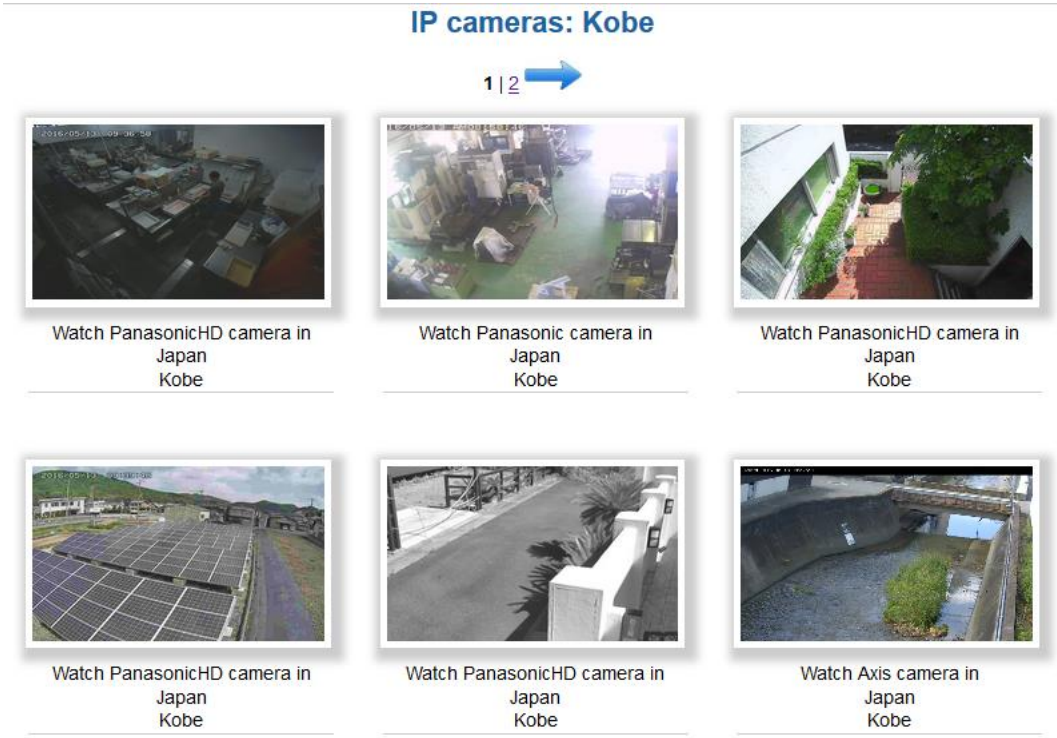
Dad Marc Gilbert was horrified to discover a stranger's voice coming from the baby monitor, calling his sleeping child an "effing moron" and a "little slut"

wizSafe

IoT全盛時代のリスク

実際の事件(3)

- インターネット側から参照可能な監視カメラ



http://www.insecam.org/en/bycity/Kobe/?page=1

wizSafe

IoT全盛時代のリスク

実際の事件(4)

2014年5月　サンフランシスコ

熊野市　地震、テロ情報を誤送信　Jアラート改修で操作ミス

【熊野】熊野市は十一日、同日午後の全国瞬時警報システム（Jアラート）改修作業中、業者の操作ミスでシステムに登録している市民四百七十三人に対し、地震速報や大規模テロ情報などを誤って送信したと発表した。システム自体に故障はなく、市は誤送信後、登録者に誤報であることを連絡し、大きなトラブルには至っていない。

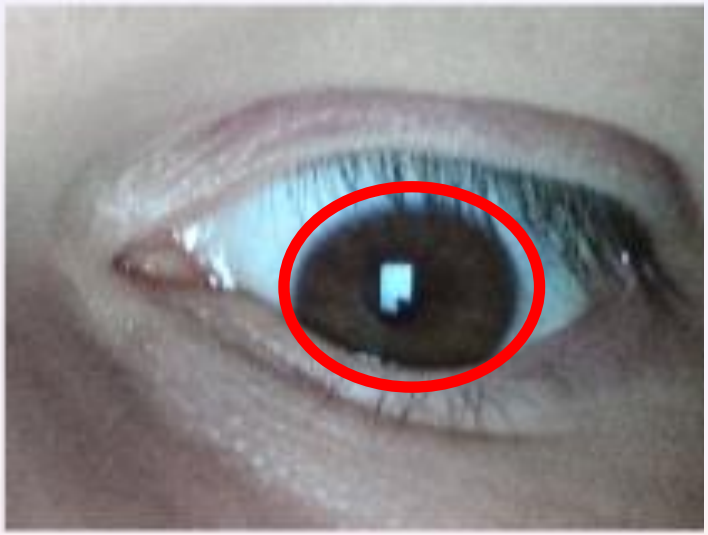
市防災対策推進課によると同日午後一時二十二分、市役所本庁舎にある行政無線放送室で災害やテロなどの情報を市行政情報として流すJアラート設備の取り換え作業を実施していたところ、業者が操作を誤り、実際には発生していない震度4―7までの地震速報六項目や高さ別の津波警報二項目のほか、ゲリラ攻撃▽航空攻撃▽ミサイル攻撃▽大規模テロ―の四項目の計十二項目の情報が一分おきに登録者の携帯電話やパソコンのメールアドレスに送信されたという。

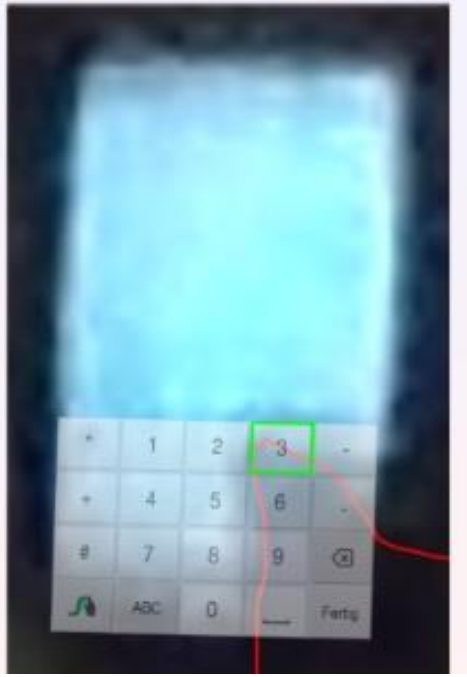
同システムによる市行政情報は、地震速報などの緊急速報が登録者に瞬時に伝わるメール配信サービス。平成二十一年五月の運用開始以来誤送信は初めてで、同課は「登録者の方には大変ご迷惑をお掛けし、深くおわびしたい」としている。

2014年6月 三重県

実際の事件 (5)

- 必要以上に高性能な装置(WOOT2014発表より)
- スマートフォンの自分撮り用カメラ





IoT全盛時代が引き起こす問題

- 攻撃の可能性
  - IoT装置の脆弱性（Linux搭載の家電に脆弱性がないわけがない）。
  - 運用の問題、認証などの問題（家庭内の装置が現時点でどのような扱いを受けているかを考えれば明らか）。
  - IoT装置はどこにでもある状況で全体的にあるレベルを維持できるか（企業、家庭はいいとしても、公共の場所は誰が面倒見るのか？）
  - インターネットや携帯網などのネットワークサービスへの攻撃は存在する。通信が途絶したときに問題が起こるか。

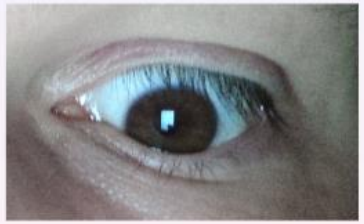
- 備えるべき問題
  - プライバシーの侵害
  - 物理的被害やテロへ、新しいテロ

wizSafe

IoT全盛時代のリスク

プライバシーの侵害

- 個人生活を取り巻く装置への侵犯は直接的にプライバシーの侵害を招く。
- IoT装置が積極的に取得している情報
  - 画像、映像、音声、センサー情報（温度、湿度、電気ガス水道利用量、など）
- IoT装置の性能により過度に取得される情報
  - スマートフォンのカメラで操作中の人の瞳に映った画像を盗撮。
  - スマートフォンの加速度センサを用いた盗聴。
- 改正個人情報保護法のもとで合法的に取得されるパーソナルデータ
- 消極的に取得された情報から洩れるプライバシー
  - 特定の情報から言外の意味を読み取ることができる場合がある(消極的取得)。
  - 例：ガスメータ。月に一回の検診では利用量総量しか伝わらないが、常時利用量を取得することによりガス会社にガス器具の利用時間が伝わるようになる。つまり、ガス器具を使っていない不在の時間が伝わることになる。
  - 例：脈拍の乱れから、動揺していることがわかる。



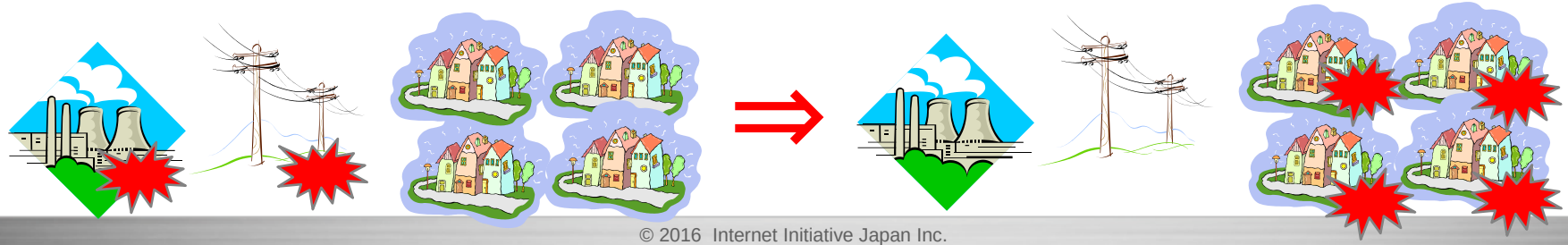
wizSafe

IoT全盛時代のリスク

物理的被害やテロへ

- IoT装置の誤動作、乗っ取り、動作停止
  - 家電の誤動作から火災など。
  - 電気ガス水道など生活インフラに対する影響。
    ⇒　IoT装置はサイバーテロを引き起こす可能性がある。

- 新しいテロ
  - 発電所や送電網を機能させなくするのが従来の想定。
  - 受電する家庭や企業すべてを機能不全にすることでも同じ被害を与えることができる。
  - 機能不全（電気は来ているが電圧が不安定）も想定。



IoT全盛時代のリスク

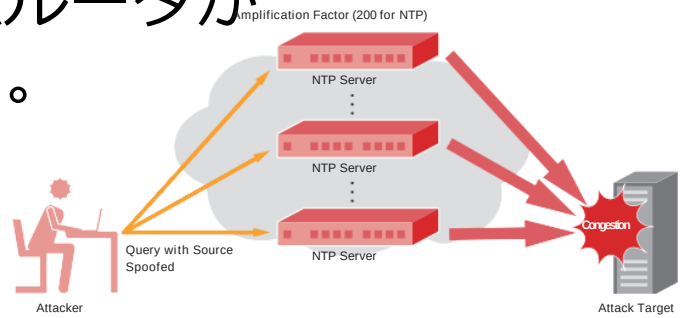
Mirai Botについて

wizSafe

Mirai Botについて

DrDoS(Distributed reflection Denial of Service)攻撃

- ホームルータなどの装置を踏み台にして、少量のデータ(命令)を送付し、多量の応答を得ることにより増幅された通信を、IPアドレスの詐称を用いて被害者に送付する。
- 通信プロトコルとしてDNS、NTP、SNMP、SSDPなどが悪用された実績があり、IPSec/IKEなど他のプロトコルも悪用の可能性が指摘されている。
- 背景として、脆弱性やデフォルト設定の問題、ユーザによる設定ミスなどを抱えるホームルータがインターネット上に多数存在する。



Internet Initiative Japan Inc., Internet Infrastructure Review (IIR) Vol.23, 1.4.2 DrDoS Attacks and Countermeasures (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol23_EN.pdf)

wizSafe

Mirai Botについて

問題を有するホームルータへの対策(ICT-ISAC Japanの各種活動より)

- 2012年 脆弱性を持つ特定のルータに関する調査（ルータ脆弱性問題WG）。L社特定ルータ(30万台以上)。対策に2年以上要した。
- 2013年10月から個人ユーザが購入しそうなホームルータを購入し、脆弱性を調査（ルータ脆弱性問題WG）。大方問題はなさそうと一旦判断。2014年の再調査で、特定条件で脆弱である機種の発見(B社ルータ)。
- 2013年 DNSのOpenResolverによる攻撃が2013年に大きく話題となったが、国内でもDNSを使ったDrDoSの発生を確認。日本国内が被害者となる場合と、踏み台となって攻撃に加担する場合の両方(DoS即応WG) 。
- 2013年8月、日本国内に存在する踏み台となる装置の数をスキャンして調査（脆弱性保有ネットワークデバイス調査ＷＧ）。WG参加ISPの中の有志から、個人ユーザに供するネットワークの空間を調査。
  - ① 管理画面の乗っ取りの可能性が否定できないNW機器 = 6万台以上
  - ② DNS open resolverとして機能する NW機器 = 12万台以上
  - ③ ssdp リクエストに反応するNW機器 = 108万台以上
    (実際の調査から推定した全国換算値。この調査ではSNMP,NTPなどは未調査)

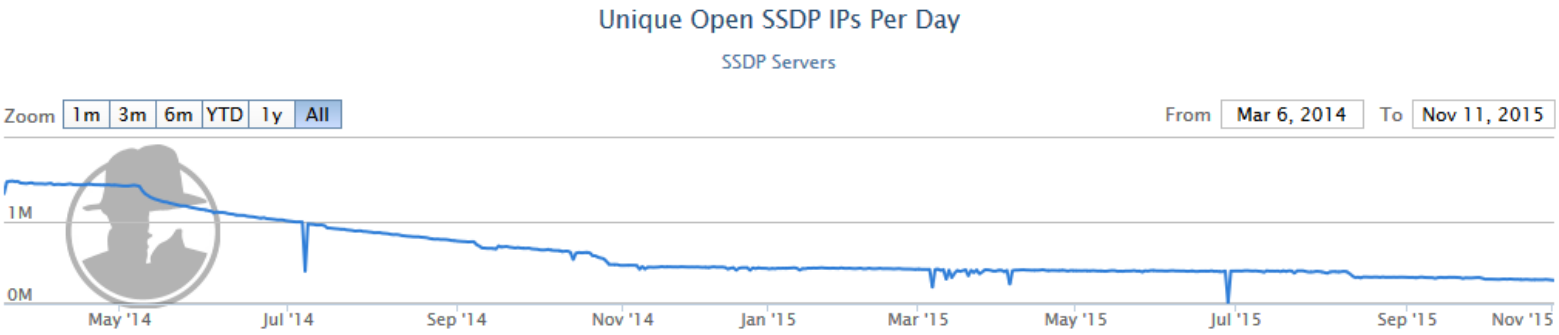
  他の組織の調査と数が合わないことに注意。
- 2014年1月NTPによるDrDoSで100Gbpsの攻撃が発生 (DoS即応WG)

wizSafe

Mirai Botについて

DrDoSに加担するホームルータの状況

- ホームルータの問題による脅威
  - ホームルータの設定が変更され、通信を操作される。
  - ホームルータの接続情報（ISPのIDとパスワード）が盗まれて悪用される。
  - DrDoSなどの踏み台として悪用される。
- ホームルータの脆弱性は認知され、国内メーカやISPによる対策の努力が行われている。
- 結果として国内ではDrDoSの踏み台となるホームルータの数は減少傾向にある。
- しかし、国外においてはまだまだ対策が進んでいない（本年発生したある攻撃では99%が国外の踏み台を利用）。
- この手法による最大級のDDoS攻撃は605Gbps(2016/01 BBC公式Web)



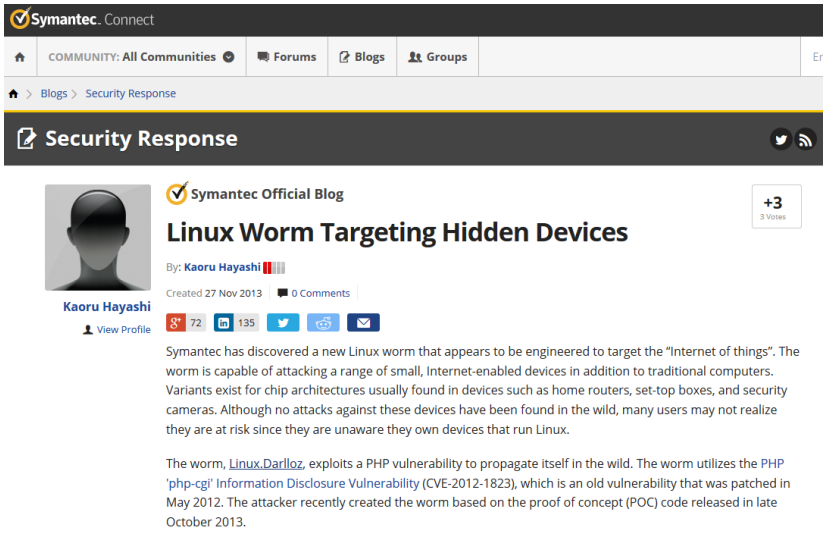
https://ssdpscan.shadowserver.org/stats/ssdp_jp.html

wizSafe

Mirai Botについて

IoTボット

- 組み込み機器ウイルス、ワーム、ボット
  - 組み込みLinuxなどをプラットフォームとした組み込み機器に感染していく。
  - デフォルトの認証情報やプラットフォーム共通の脆弱性を悪用して感染。このため、ホームルータ、HDDレコーダ、監視カメラなど、表面上はまったく異なるものが感染対象となる。
  - 感染後は外部からの操作により、情報漏えいや攻撃の踏み台などの被害が発生している。



http://www.symantec.com/connect/blogs/linux-worm-targeting-hidden-devices

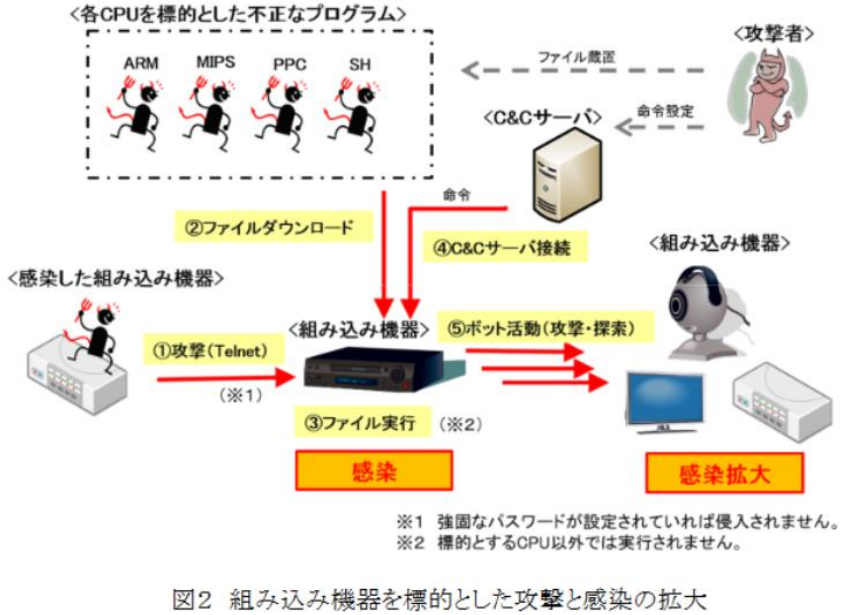


図2 組み込み機器を標的とした攻撃と感染の拡大

IoT機器を標的とした攻撃の観測について
http://www.npa.go.jp/cyberpolice/detect/pdf/20151215_1.pdf

wizSafe

Mirai Botについて

IoT Bot (Mirai bot)によるDDoS攻撃と関連タイムライン

- リオ五輪
  - 数か月前から23/tcpへのスキャンが増加。
  - リオ五輪関連サイト540GbpsのDDoSはIoTボットによるもの。
- 9/20 Brian Krebs の Krebs on security（セキュリティ事件を追うblog）
  - 620Gbpsの攻撃を受けた。
  - Akamaiの無料利用継続を拒否されたためgoogle の無料のDDoS対策機能 Project Shield に移行。
  - DrDoSではなくIoT Botnet によるもの。GRE トンネル破たんを狙っており、DDoS対策サービスの導入者を攻撃する意図も見える。
- 9/22 フランス OVH
  - 1Tbpsを越える攻撃が発生した。
  - 150,000台のIoTを装置によるIoT botnetによるもの。
  - IoT装置から被害者に向かったTCP接続による攻撃である。

wizSafe

Mirai Botについて

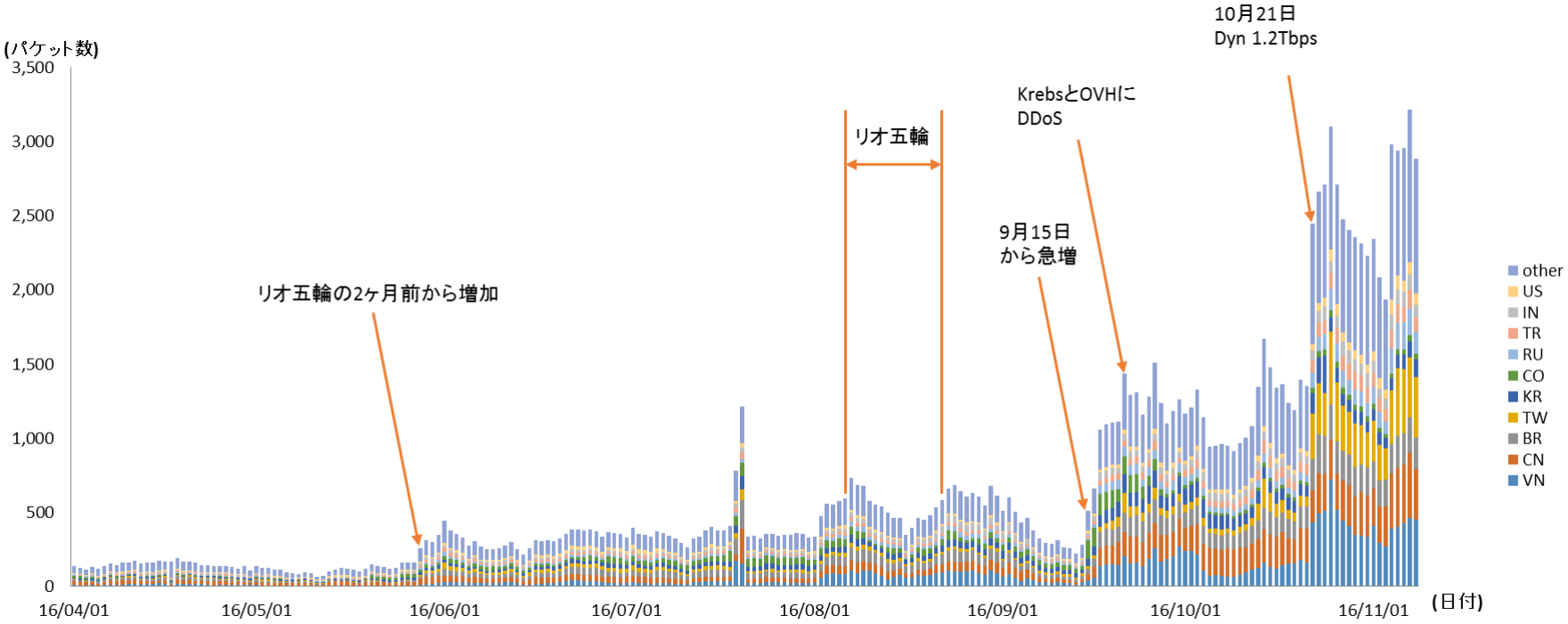
IoT Bot (Mirai bot)によるDDoS攻撃と関連タイムライン（2）

- 9/30 Iot Botnet Mirai ,Open source software として Hacker Forumsで公開（のちにGithubに転載）。
  - 匿名アカウントAnna-senpaiによるもの。
  - 誰でも使える状態に。
- 10/21 Dyn に 1.2Tbps (current world record)
  - 10万アドレスから通常の40-50倍のTCP,UDPパケットを受信。
  - また大量の DNSパケットを受信 。 DNS recursive queryであったため影響が拡大した。ただし、Dyn自身は1.2Tbpsとは認めていない。

wizSafe

Mirai Botについて

感染活動の観測



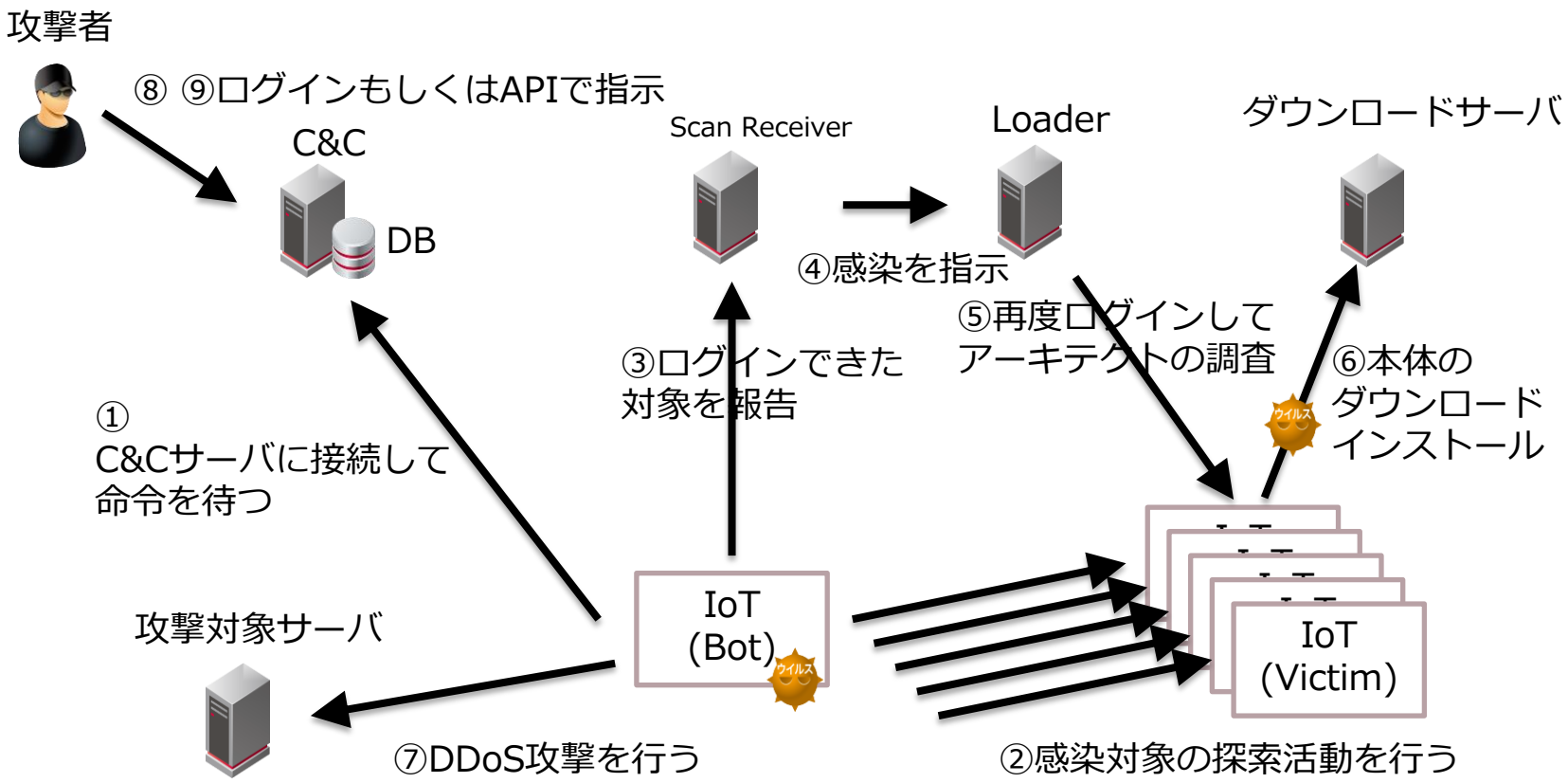
ハニーポットに到着した23/TCP通信の推移（日別・国別・一台あたり）

wizSafe

Mirai Botについて

Mirai botの分析(ソースコードより)

※詳細はIIR Vol33 (12月上旬公開予定)にて紹介



wizSafe

Mirai Botについて

Mirai botの分析(ソースコードより)(2)

1. 感染後Mirai botは下記の動作を行う
    1. 他のMirai botの動作停止
    2. 管理インタフェースへのアクセスの禁止(22,23,80/tcpへの接続を奪う)
    3. C&Cサーバへ接続し命令を待つ。また、定期的にハートビートを送信。
2. スキャン
    1. ランダムなIPアドレスを生成し、23/tcpのスキャンを行う。うち一部のアドレスは除外。
    2. 10回に1回の割合で2323/tcpのスキャンを行う。
    3. 接続に成功したら、ハードコードされた認証情報でログインを試みる。
    4. この動作はMirai bot 起動中は常に行っている。
3. Scan Receiverへのログイン報告
    1. インターネット上のIoT装置にログインに成功すると、ハードコードされたScan Receiverサーバの48101/tcpに接続、ログインに接続したアドレスと認証情報を送信する。
4. Loader 感染サーバへの指示
    1. Scan Receiver は受け取った情報をデコードして 感染サーバ Loaderに渡す。

wizSafe

Mirai Botについて

Mirai botの分析(ソースコードより)(3)

5. 感染活動
    1. Loaderは受け取ったアドレスを認証情報を用いてIoT機器にログイン。
    2. /bin/echo のバイナリ解析によりCPUアーキテクチャを判別する。
6. 感染
    1. Loaderにハードコードされた情報に従って、 Wetまたはtftpでダウンロードサーバからbot本体の実行ファイルをダウンロードし、実行する(１．に戻る）。
7. 攻撃指令
    1. C&Cサーバから攻撃指令を受け取ると、指定されたDDoS攻撃のパケットを送出する。
8. ボットネット管理者のログイン
    1. ボットネット管理者はC&CサーバにTelnetで接続して管理を行う。
9. ボットネット管理者向けのAPI
    1. 管理者は101/tcpに接続することでAPI経由でボットネットを利用することができる。

※ Mirai bot の各システム間の通信は すべて平文で行われる。

wizSafe

Mirai Botについて

Mirai Botには誰が感染するのか

- 認証とアーキテクチャーが揃うと感染
  - アーキテクチャ：x86,spc,sh4,ppc,mpsl,mips,m68k,arm,arm7

ハードコードされた認証情報

ユーザー名	パスワード
root	xc3511
root	vizxv
root	admin
admin	admin
root	888888
root	xmhdipc
root	default
root	juantech
root	123456
root	54321
support	support
root	(none)
admin	password
root	root
root	12345
user	user
admin	(none)
root	pass
admin	admin1234
root	1111
admin	smcadmin
admin	1111
root	666666
root	password

Username/Password	Manufacturer	Link to supporting evidence
admin/123456	ACTi IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/anko	ANKO Products DVR	http://www.cctvforum.com/viewtopic.php?f=3&t=44250
root/pass	Axis IP Camera, et. al	http://www.cleancss.com/router-default/Axis/0543-001
root/Vizxv	Dahua Camera	http://www.cam-it.org/index.php?topic=5192.0
root/888888	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/666666	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/7ujMko0vizxv	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
root/7ujMko0admin	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
666666/666666	Dahua IP Camera	http://www.cleancss.com/router-default/Dahua/DH-IPC-HDW4300C
root/dreambox	Dreambox TV receiver	https://www.satellites.co.uk/forums/threads/reset-root-password-plugin.101146/
root/zlxx	EV ZLX Two-way Speaker?	?
root/juantech	Guangzhou Juan Optical	https://news.ycombinator.com/item?id=11114012
root/xc3511	H.264 - Chinese DVR	http://www.cctvforum.com/viewtopic.php?f=56&t=34930&start=15
root/hi3518	HiSilicon IP Camera	https://acassis.wordpress.com/2014/08/10/i-got-a-new-hi3518-ip-camera-module-s/
root/klv123	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/klv1234	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/jvbzd	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/admin	IPX-DDK Network Camera	http://www.ipxinc.com/products/cameras-and-video-servers/network-cameras/
root/system	IQinVision Cameras, et. al	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/meinsm	Mobotix Network Camera	http://www.forum.use-ip.co.uk/threads/mobotix-default-password.76/
root/54321	Packet8 VOIP Phone, et. al	http://webcache.googleusercontent.com/search?q=cache:W1phozQZURUJ:community.freepbx.org/t/packet8-atas-phones/411
root/00000000	Panasonic Printer	https://www.experts-exchange.com/questions/26194385/Default-User-Password-for-Panasonic-DP-C405-Web-Interface.html
root/realtek	RealTek Routers	
admin/1111111	Samsung IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/xmhdipc	Shenzhen Anran Security Camera	https://www.amazon.com/MegaPixel-Wireless-Network-Surveillance-Camera/product-reviews/B00EB6FNDI
admin/smcadmin	SMC Routers	http://www.cleancss.com/router-default/SMC/ROUTER
root/ikwb	Toshiba Network Camera	http://faq.surveillixdvrsupport.com/index.php?action=artikel&cat=4&id=8&artlang=en
ubnt/ubnt	Ubiquiti AirOS Router	http://setuprouter.com/router/ubiquiti/airos-airgrid-m5hp/login.htm
supervisor/supervisor	VideoIQ	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/<none>	Vivotek IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/1111	Xerox printers, et. al	https://atyourservice.blogs.xerox.com/2012/08/28/logging-in-as-system-administrator-on-your-xerox-printer/
root/Zte521	ZTE Router	http://www.ironbugs.com/2016/02/hack-and-patch-your-zte-f660-routers.html

https://krebsonsecurity.com/2016/10/who-makes-the-iot-things-under-attack/

wizSafe

Mirai Botについて

Mirai Botには何ができるのか

- 感染活動
- DDoS攻撃

C&Cサーバへのコマンド
-[< BotCount>]<atk cmd> <ip_addr>/<mask>[,<ip_addr>/<mask>…] <duration> <flags>

DDoS攻撃機能一覧

攻撃ID	コマンド	攻撃内容	攻撃詳細
0	udp	UDP flood	UDPパケットを大量に送り付ける。
1	vse	Valve source engine specific flood	Source Engine用のUDP Floodを行う。
2	dns	DNS resolver flood using the targets domain, input IP is ignored	指定したドメイン名に対してDNS水責め攻撃を行う。
3	syn	SYN flood	SYNパケットを大量に送り付ける。
4	ack	ACK flood	ACKパケットを大量に送り付ける。
5	stomp	TCP stomp flood	DDoS対策機器等をバイパスすることを意図した攻撃。 TCPセッション確立後に、大量のACKパケットを送り付ける。
6	greip	GRE IP flood	GREでカプセル化したIP-UDPパケットを大量に送り付ける。
7	greeth	GRE Ethernet flood	GREでカプセル化したETH-IP-UDPパケットを大量に送り付ける。
8	なし	Proxy knockback connection	未実装のため、詳細不明。
9	udpplain	UDP flood with less options. optimized for higher PPS	設定項目を少なくし、高速化を図ったUDP Flood。
10	http	HTTP flood	HTTP GETなどのリクエストを大量に送り付ける。

wizSafe

Mirai Botについて

IoT Bot (Mirai bot)をやっつけるために

- 感染の可能性のある機器の母集団がつかみにくい
  - 認証とアーキテクチャーが揃う機器が感染対象。
- 感染全容がつかみにくい
  - 感染後 22,23,80/tcpを閉じるためスキャンできない。
- IoTBotから発せられたDDoS攻撃は制御しにくい？
  - DrDoS に対して制御しにくい場合もある。
- 既存のマルウェア対策手法が使えないか？
  - 「IoT機器」が広範であるためユーザを特定したとしてサポートしにくい。
  - 「IoT機器」機器用のアンチウイルスソフトはありましたっけ？
  - 「電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン」的手法
    - URLフィルタ： IoT機器に対する制御に関して、事前同意の在り方について要検討
    - DNSでフィルタ： DNSは参照するが、ハードコードされた8.8.8.8など外部DNSを使う。
      他社のDNSの通信を奪ってよいという議論はしていない。
- ボットネットに参加してみるという手法が話題だが
  - ボットに下る指令はわかるが、ボットネットの全体像などはわからない。

wizSafe

Mirai Botについて

IoT Bot (Mirai bot)をやっつけるために(2)

- PCのワームやボットはだれがやっつけたか
  - Confikerワーム(2008)を最後に姿を消した。
  - マイクロソフトがやっつけた。Windows XP SP2でファイアウォールをデフォルトオンにしたため。その後も脆弱性が発見されたが攻撃が困難に。
  - （標的型攻撃とかWeb感染マルウェアとか、より面倒な方向に。）
- IoT装置メーカ個別に調整できるか
  - 中国のHangzhou Xiongmai TechnologyはDynのDDoS攻撃に加担した防犯カメラやIPカメラ4.3百万台のリコールを発表。

wizSafe

Mirai Botについて

IoT Bot (Mirai bot)をやっつけるために(3)

- 一般ユーザへの啓発活動はやるとして
- 1Tbps以上の攻撃にはDDoS対策で備えるとして

- 過激なIoTBot対策の検討をしておいた方がよいかもしれない
  - telnet をスキャンするときにログインしてよいか
  - C&Cサーバへの通信を｛傍受、分析、遮断｝してよいか
  - 他社のDNSサーバに向かった通信を{傍受、分析、遮断}よいか
  - IoT機器全般に何等か通信規制を行うべきではないか

wizSafe

まとめ

- IoT全盛時代のリスク
- Mirai Botについて

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