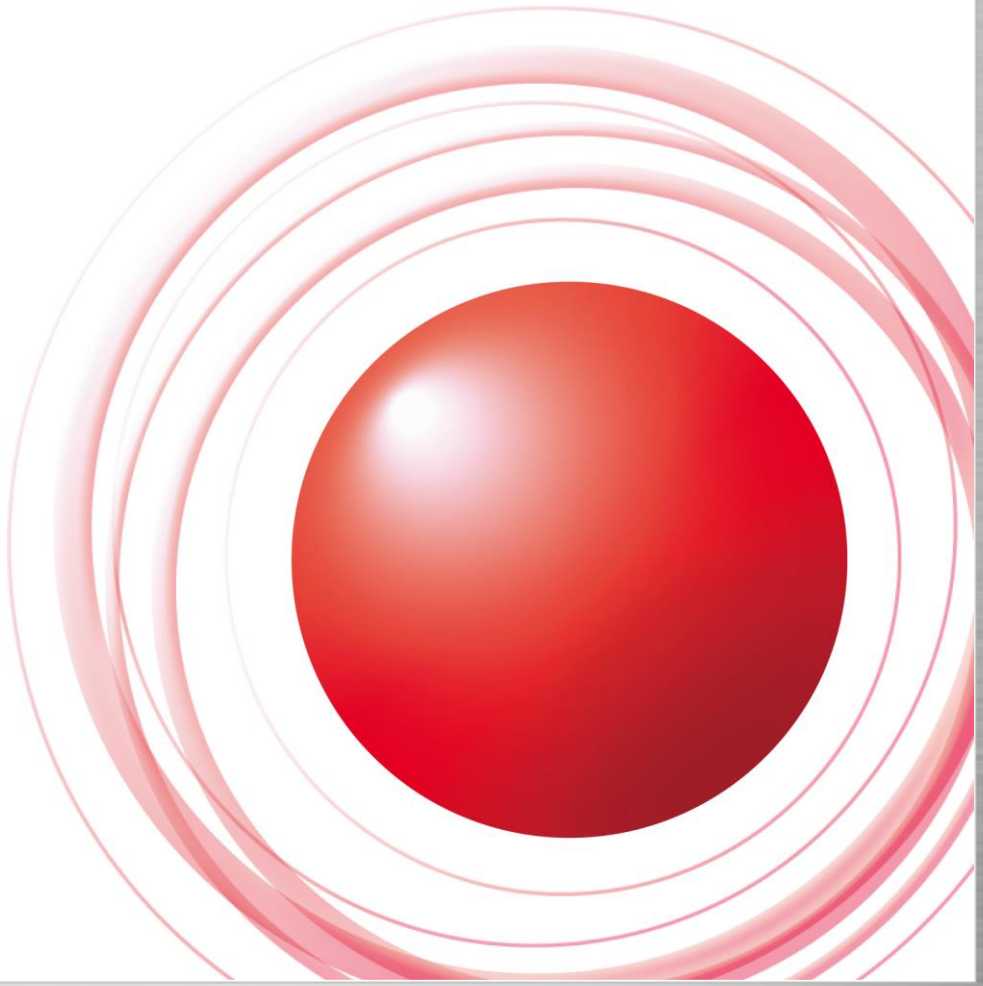
IIJ Technical WEEK 2016

セキュリティ動向2016

~ ランサムウェアとMirai bot について ~

Internet Initiative Japan

wizSafe
安全をあたりまえに



2016/11/11
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

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)。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。

wizSafe

私たちはセキュリティのイニシアティブを取り続ける ～Lead Initiative of Internet Security～

ITにおけるあらゆる脅威から対象を守り、安心安全を実現する先端技術を先んじて技術に取り組むチャレンジャー

部署再編前

- サービス関連部署
- ソリューション関連部署
- ビッグデータ関連部署

部署再編後（2016年4月1日付）

セキュリティ本部

セキュリティ情報統括室

セキュリティ情報の収集、分析、対策立案、対策状況把握
セキュリティ情報の発信業務、外部組織での活動

セキュリティビジネス開発部

セキュリティサービス・ソリューションの企画開発に関する業務
（技術企画、開発推進、市場調査、販売促進、マーケティング）

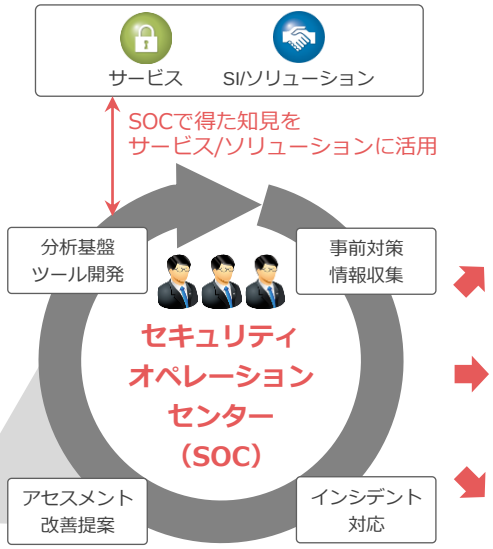
セキュリティビジネス推進部

セキュリティサービス・ソリューションの提供、運営
セキュリティ運用および顧客サポート業務の企画、実装及び遂行

各部署と連携

IIJテクノロジーユニット

MVNO事業部、ネットワーク本部、クラウド本部、
サービス基盤本部



情報発信

技術レポート・ブログ

国内外の活動に
積極的に参画

- Telecom-ISAC Japan
- FIRST
- JNSA
- ISOG-J
- 日本シーサート協議会

インターネット業界団体（一例）

私たちが目指すこと

企業/組織

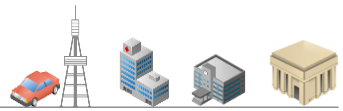
IT利用者が本来やりたいことに専念できる環境づくり

各種産業の商材開発

各産業でIIJのセキュリティを活用した商材開発に貢献

家庭

家庭における「安心安全なITライフスタイル」の提案



ランサムウェア

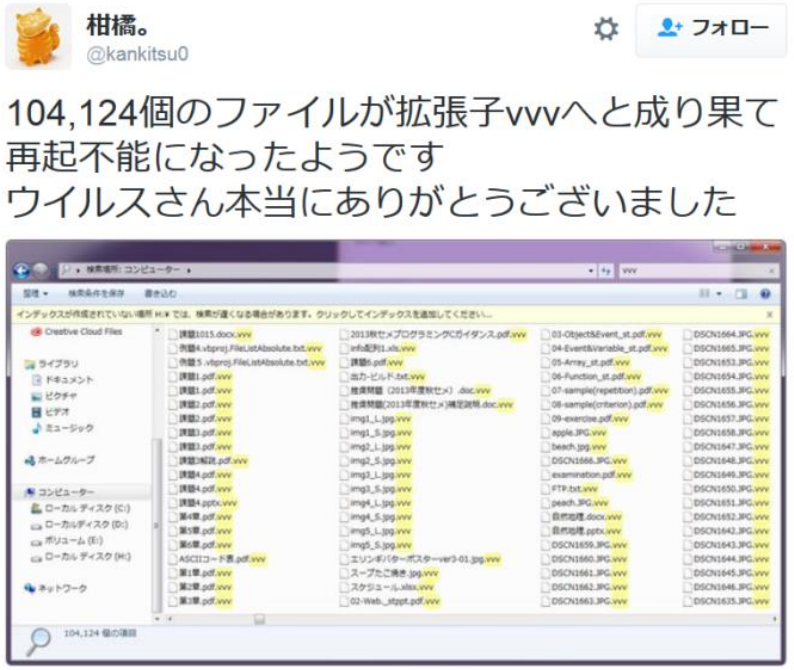
Mirai Botについて

wizSafe

ランサムウェア

事件

- vvvウイルス(TeslaCrypt2.2)
  - 2015年１2月、主に２ちゃんねるまとめサイトのウェブ広告で展開されたマルバタイジングにより、複数の個人が感染(感染数は不明)。
  - 同時に企業などのメールアドレスに、メール添付型で感染活動を行う。
  - 直接マルウェアを添付するパターンと、マルウェアをダウンロードするJavascriptをパターンがあり、特に後者は企業などに設置されたふるまい検知などの最新の対策設備をすり抜けた。
  - 身代金支払いはビットコイン。



wizSafe

ランサムウェア

事件(2)

- 2016/2/5米国LAの病院Hollywood Presbyterian Medical Center
  - ランサムウェアにより患者の情報にアクセスできなくなる。
  - 病院の救急サービスが米国時間2月12日から「散発的に影響を受けている」ことを認めており、先の医師は電子メールサービスの停止に言及している。患者の個人情報やレントゲン写真、CTスキャンデータ、検査結果といった医療記録にアクセスできないため、患者にとって状況は極めて危険なものとなっている。結果として、数多くの患者が治療を受けられず、一部は他の病院に移送されている（http://japan.zdnet.com/article/35077922/）。
  - 身代金40BTC（約17,000USD、190万円)を支払い、2/15には電子カルテが復旧。

http://hollywoodpresbyterian.com/default/assets/File/20160217%20Memo%20from%20the%20CEO%20v2.pdf

HOLLYWOOD PRESBYTERIAN MEDICAL CENTER

February 17, 2016

I am writing to talk to you about the recent cyber incident which temporarily affected the operation of our enterprise-wide hospital information system.

It is important to note that this incident did not affect the delivery and quality of the excellent patient care you expect and receive from Hollywood Presbyterian Medical Center ("HPMC"). Patient care has not been compromised in any way. Further, we have no evidence at this time that any patient or employee information was subject to unauthorized access.

On the evening of February 5th, our staff noticed issues accessing the hospital's computer network. Our IT department began an immediate investigation and determined we had been subject to a malware attack. The malware locked access to certain computer systems and prevented us from sharing communications electronically. Law enforcement was immediately notified. Computer experts immediately began assisting us in determining the outside source of the issue and bringing our systems back online.

The reports of the hospital paying 9000 Bitcoins or $3.4 million are false. The amount of ransom requested was 40 Bitcoins, equivalent to approximately $17,000. The malware locks systems by

wizSafe

ランサムウェア

ランサムウェア感染の様子

- メール添付やWeb感染を通じてPCに感染。
- HDDのファイルをすべて暗号化してしまう。暗号化の処理にはファイル数やサイズに応じて相応の時間がかかる。
- ネットワークドライブ上のファイルも暗号化する。状況によっては切断されているドライブの再接続を行う。
- 暗号化を行っている間は、マルウェアの動作を調査するようなアプリケーション（アンチウイルスソフト、パフォーマンスメーターや、コマンドプロンプトなど）の起動を阻害することがある。
- 復元を阻害するために、VSS(Volume Shadow Copy Service)で作成したファイルを削除する。
- （外部と通信しないと暗号化できないものと単独で動作するものがある）。
- 暗号化が終了すると、復号手法の入手方法を示すメッセージを残し、自分自身を削除する。

wizSafe

ランサムウェア

概要

- ランサムウェア
  - HDDを暗号化して利用者がアクセスできないようにし、復号鍵の提供に金銭を要求する金銭目的のマルウェア。
  - Windows, Linux , スマートフォン
    - スマートフォンについては遠隔操作の仕組みを使った強制ロック、パスコードの変更などもランサムウェアの一種と考えることができる。
- 歴史
  - 2005年 TROJ_GPCODE,TROJ_PGPCODER(trencmirco)
  - 2010年 WinLock
  - 2012年 Reveton
  - 2014年 TorLocker 日本語化（カランサムウェア）
  - 2015年 CryptoLocker,TorLocker,CTB-Lockerなど
- アフィリエイト(ransomware-as-a-service)ビジネスモデル
  - ランサムウェア開発者は感染活動を行わない。
  - 感染拡大を行う第三者をアンダーグラウンドで募集。マルウェアを販売。
  - 感染者が身代金を支払う（復号鍵を要求する）タイミングで、金銭の25%程度を感染者が開発者に支払う。

wizSafe

ランサムウェア

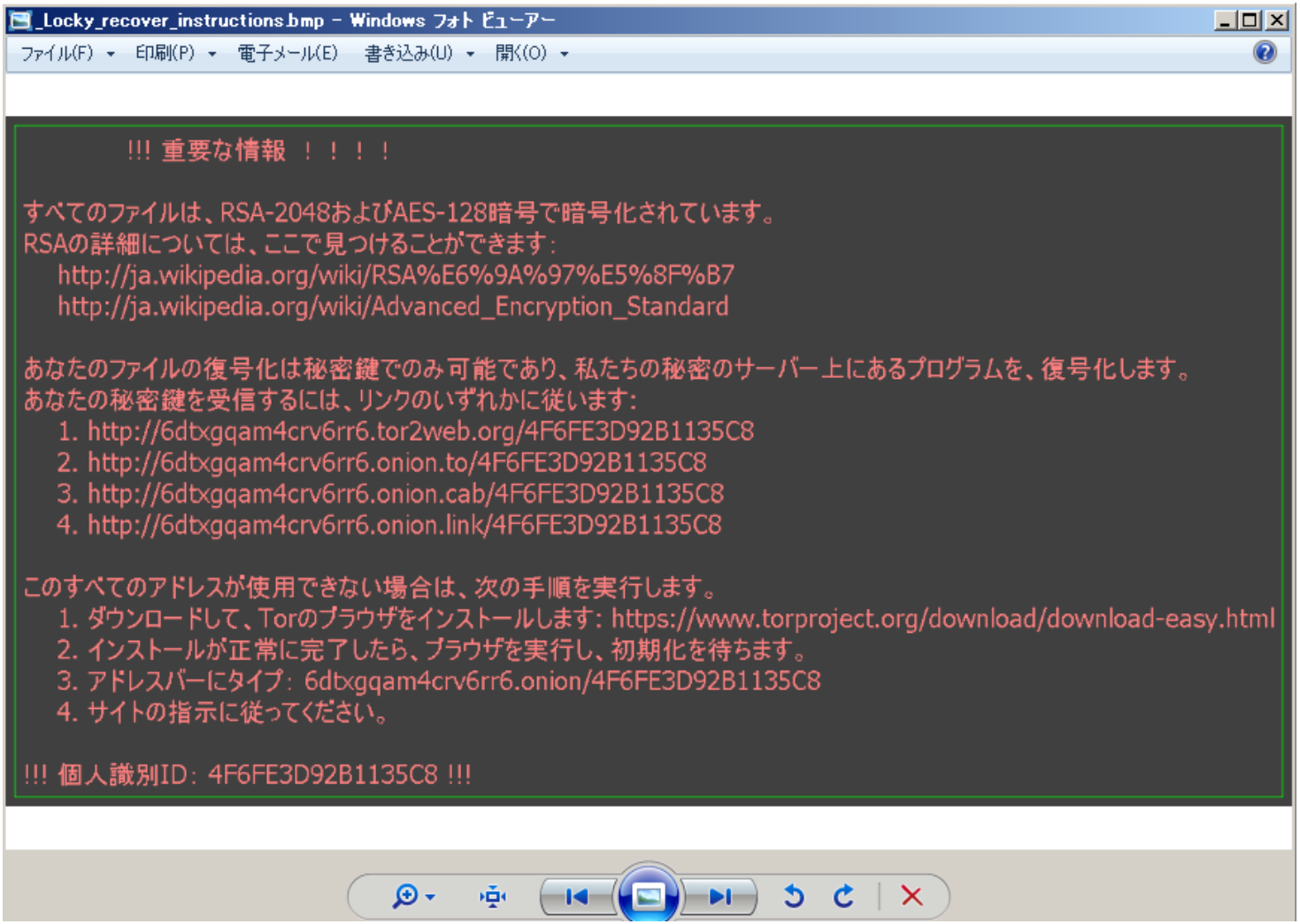
ランサムウェアの解析結果から(TeslaCrypt)(2)

- TeslaCrypt2.2
  - 出現時期
    - 2015年の12月。
  - 侵入経路
    - Angler Exploit kit
    - Nuclear Exploit kit
    - メール
  - C&Cサーバ
    - 分散度合いは少なく、１日１サーバ程度で、２～３日ごとに変化。
  - オフラインの状態でも暗号化する
    - お試しでファイルの復号が１つ可能とし暗号化されたファイルをアップロードさせる。
      - ファイルの先頭部分に暗号化されたセッションキーが入っているため、攻撃者はこのアップロードで鍵を回収する。
        - » これにより、オフラインでの暗号化が可能になる。
  - 暗号化方式
    - 暗号方式は2.0と大幅に変わっていないため、復号できる場合がある。
  - 拡張子
    - .vvv、.ccc、.abcなど。
  - 暗号化されると拡張子がvvvに変化することから、日本国内においてはvvvウイルスとも呼ばれている。
  - proxyを越えて通信が可能
  - myexternalip.com/rawにアクセスして、感染端末のグローバルIPドレスを取得
  - vssの削除を行い、復元を難しくする

wizSafe

ランサムウェア

ランサムウェアの解析結果から(Locky)(1)



wizSafe

ランサムウェア

ランサムウェアの解析結果から（まとめ）

	CryptoWall3.0	CryptoWall4.0	TeslaCrypt2.0	TeslaCrypt2.2	TeslaCrypt3.0	TeslaCrypt4.0	Locky
出現時期	2015年1月	2015年11月	2015年7月	2015年12月	2016年2月	2016年3月	2016年2月
IPアドレス確認	ip-addr.esに接続	なし	ipinfo.ioに接続	myexternalip.comに接続	なし	なし	なし
Proxy対応	非対応	対応	非対応	対応	対応	対応	非対応
オフラインでの暗号化	不可	不可	可能	可能	可能	可能	不可
VSS削除	実施	実施	実施	実施	実施	実施	実施
備考	・IPアドレス確認や、サーバとの鍵交換が行えない場合、暗号化されない		・CryptoWallの脅迫文を盗用 ・公開ツールで復元可能	・日本国内ではVVVウイルスとも呼ばれた ・公開ツールで復元可能		・3.0のバグ修正 暗号化ファイルの拡張子廃止	・接続中ではないネットワーク共有に対しても再接続、暗号化を試みる

IIR Vol 31. 各種のランサムウェアとその対策、より
http://www.iij.ad.jp/company/development/report/iir/031/01_04.html

wizSafe

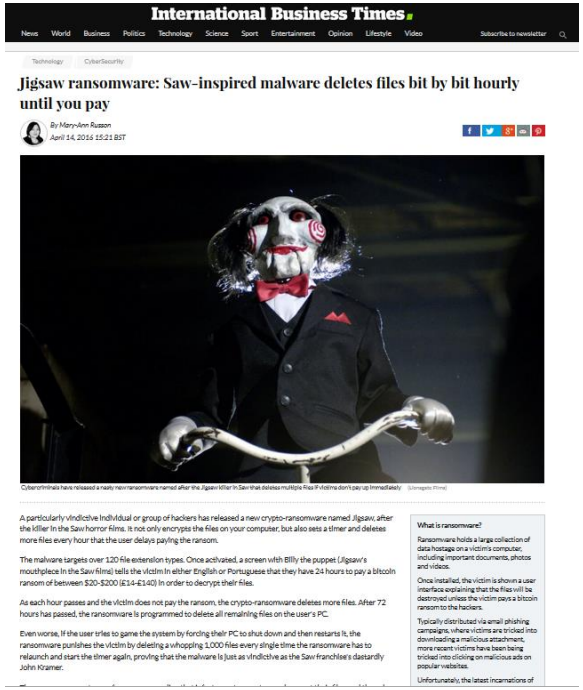
ランサムウェア

新しいランサムウェア

- PETYA
  - 求人への応募を模したメールにて感染。
  - ファイル単位ではなくHDD全体を暗号化。
  - HDDのMBRを上書きして起動を阻害。

http://blog.trendmicro.co.jp/archives/13106

- Jigsaw
  - 1時間ごとにファイルを削除していくランサムウェア。
  - 削除されるファイルの数は指数的に増加。
  - 再起動するとペナルティとして1000ファイル削除。



http://www.ibtimes.co.uk/jigsaw-ransomware-saw-inspired-malware-deletes-files-bit-by-bit-hourly-until-you-pay-1554862

wizSafe

ランサムウェア

新しいランサムウェア(2)

・スマートＴＶに感染したマルウェア

http://news.kddi.com/kddi/cable-service/smart-tv-box/201604041725.html

wizSafe

ランサムウェア

ランサムウェア対策

- 暗号化処理は時間がかかる（ファイルアクセスの異常検知で早期発見の可能性）。
- サーバ等いくつかのインターネット上のサービスへのアクセス阻害で動作しない場合もある（完全オフラインで暗号化処理を実施するものもある）。
- 身代金は払わないほうが良いのか！？
  - 一部のランサムウェアは仕組み上、自分で復元できる可能性がある。
  - 端末であればPC故障手順（クリーンインストール）。
  - 重要なファイルの復号を依頼すると、暴露系の事件に発展する可能性がある。
  - 一度身代金を払うと、繰り返し狙われる可能性がある。
  - どうしてもファイルの内容を取り返したいのであれば、身代金を払うことも検討には値する。ただし、身代金を払っても復号できない可能性も考慮する。
- バックアップ
  - たとえば「3-2-1 ルール」(trendmicro林さんから)
    1. 少なくとも3つのデータのコピーを保持
    2. 最低でも2つの異なるメディアにコピーを保管
    3. 1つのバックアップコピーをオフサイト（クラウドなど）に保存
  - 短期間（たとえば毎日）のバックアップ
  - 復元手法の確認

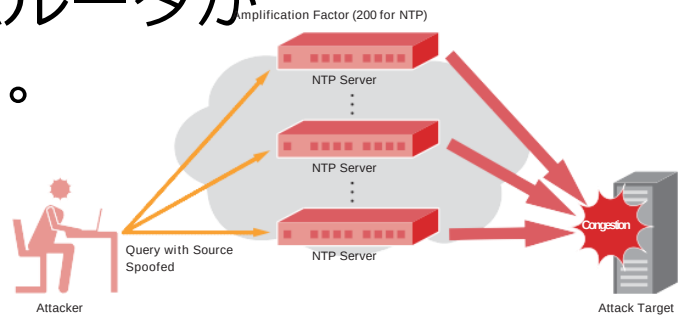
ランサムウェア
Mirai Botについて

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。



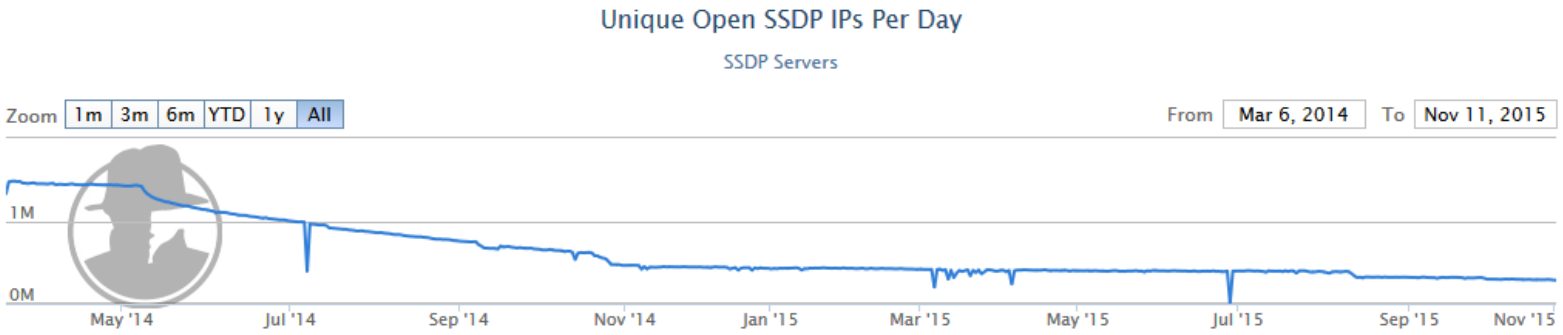
Internet Initiative Japan Inc., Internet Infrastructure Review (IIR) Vol.23, 1.4.2 DrDoS Attacks and Countermeasures (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol23_EN.pdf)

wizSafe

MiraiBot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 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

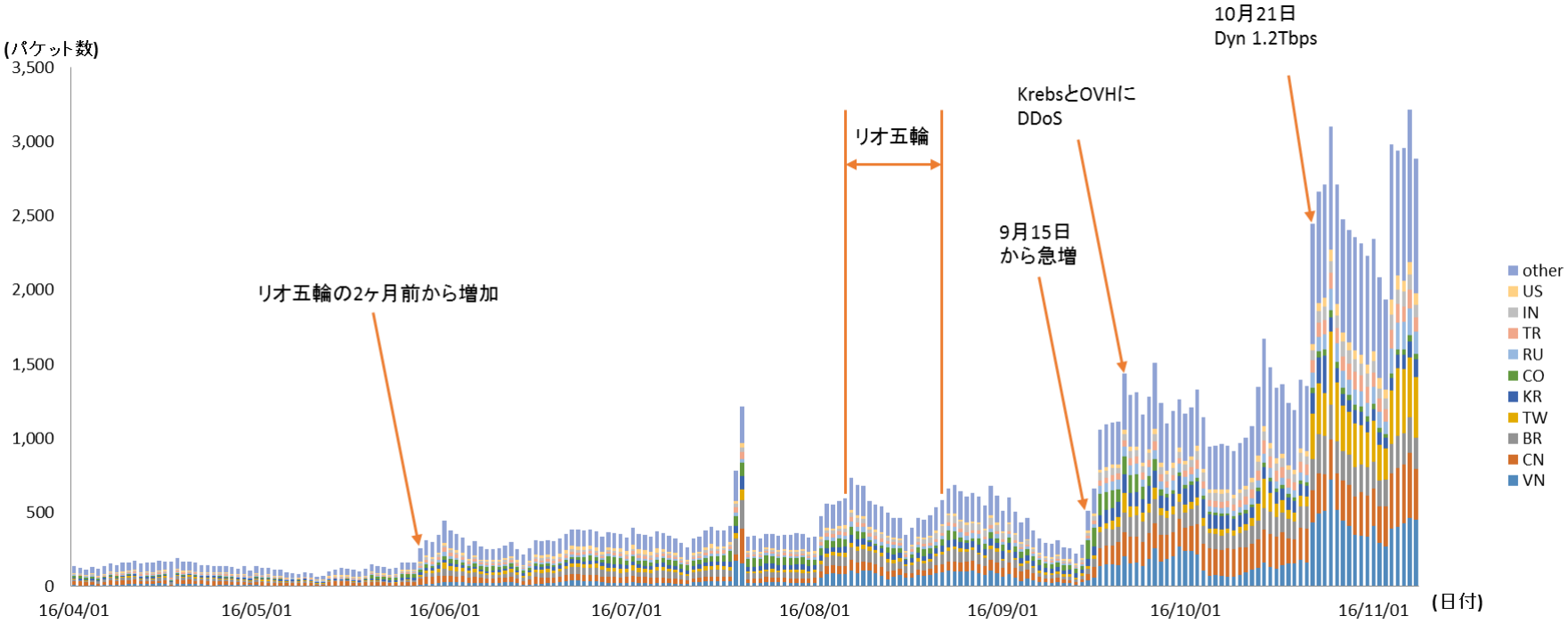
IoT Bot (Mirai bot)によるDDoS攻撃と関連タイムライン（2）

- 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

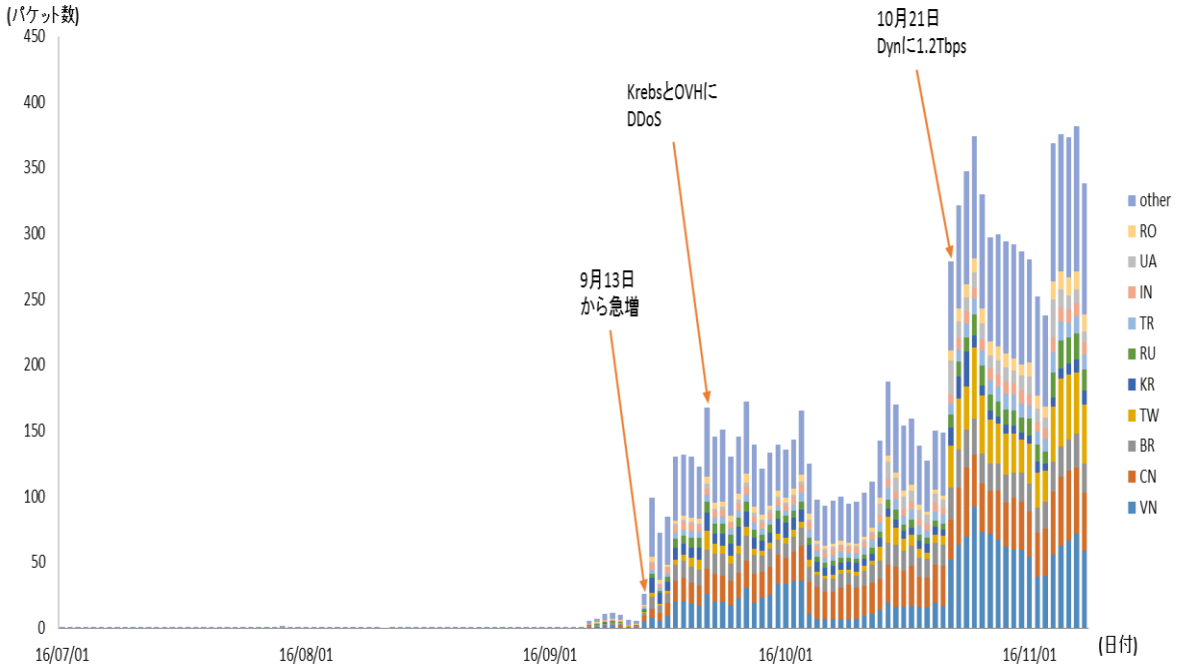


ハニーポットに到着した23/TCP通信の推移（日別・国別・一台あたり）

wizSafe

Mirai Botについて

感染活動の観測(2)



※7月以前はほぼゼロのため省略

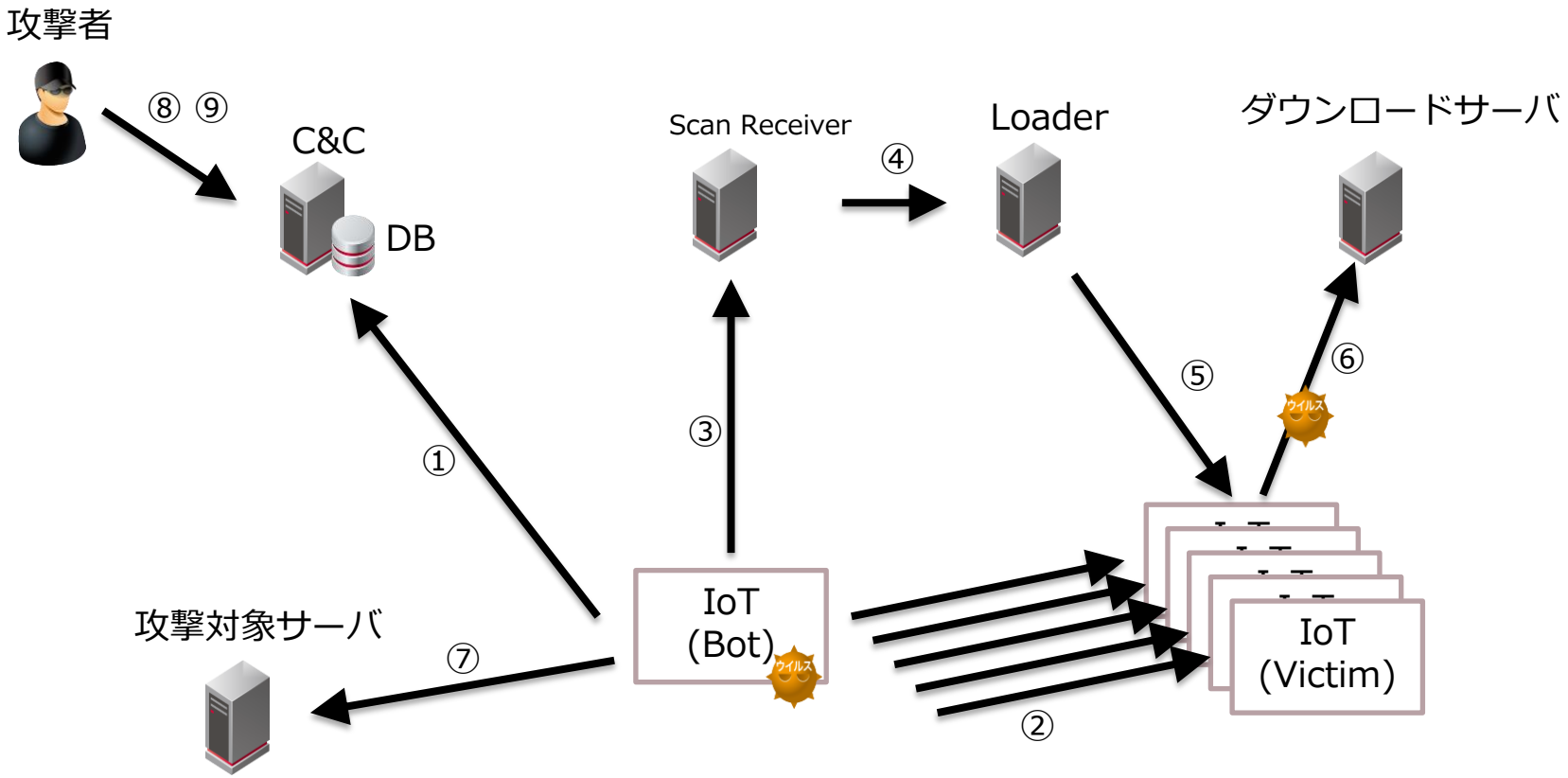
ハニーポットに到着した2323/TCP通信の推移（日別・国別・一台あたり）

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/
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

- ランサムウェア
- 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