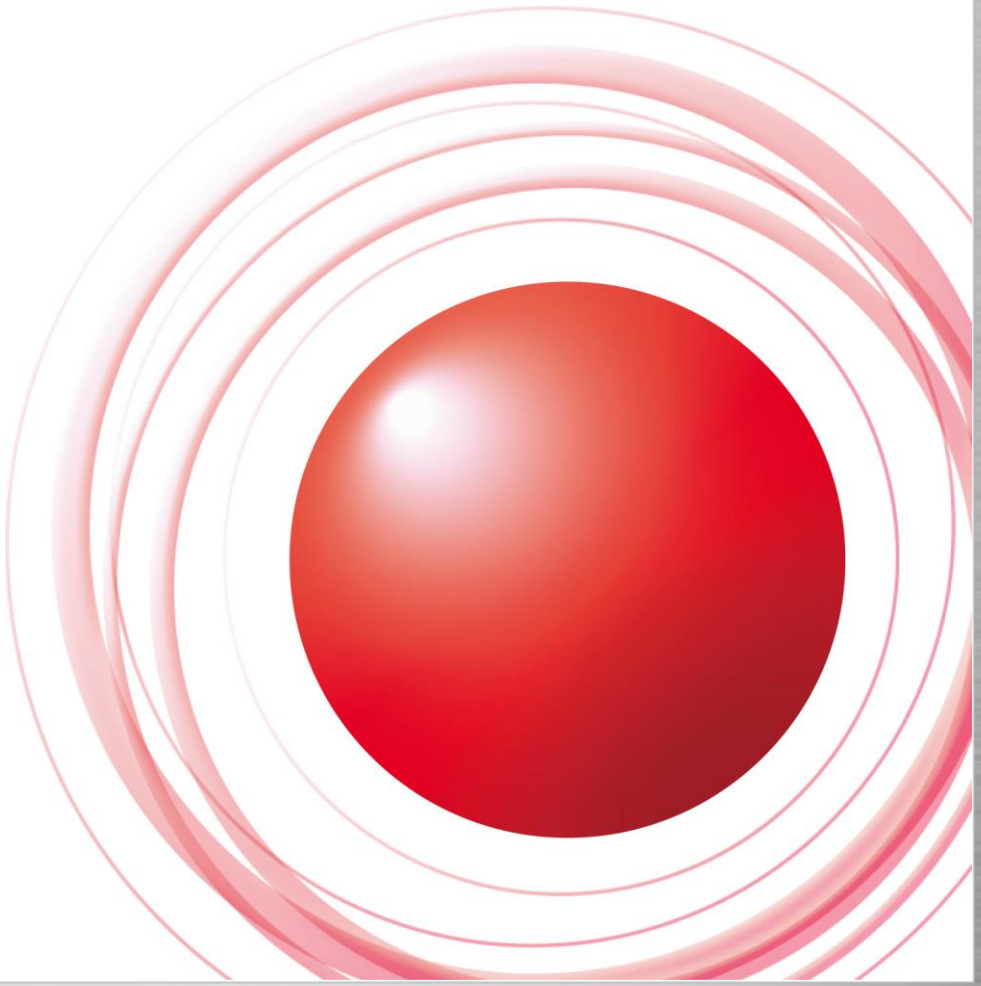
Dynへの攻撃の顛末



株式会社
インターネットイニシアティブ
島村 充
<simamura@iij.ad.jp>

Ongoing Innovation

Dynとは？

むか～し、昔。まだみんなが動的IPアドレス割当の回線で自宅サーバを運用していた頃。

DynDNSというDynamic DNSの(無料の)有名なサービスがありました。

アレを運営していた(る)会社です。

昔は無料でした。2014年4月頃に有償化したそうです。

今更Dynamic DNS？

今回の話はDynamic DNSとは関係なく…

Dyn社は現在、世界的に著名なDNSホスティングサービス/ドメイン名レジストラ会社。

2016年11月にOracle社に買収されました

そんな著名なDNSホスティング事業者に対して、日本時間 2016/10/21(金)未明、事件は起こった…

何が起こったか？

Dynの権威DNSサーバに対する、(超)大規模なDDoS攻撃 (1.2Tbps)

世界中の著名サイトが6時間ほどダウン

- Airbnb[12]
- Amazon.com[9]
- Ancestry.com[13][14]
- *The A.V. Club*[15]
- BBC[14]
- *The Boston Globe*[12]
- Box[16]
- *Business Insider*[14]
- CNN[14]
- Comcast[17]
- CrunchBase[14]
- DirecTV[14]
- *The Elder Scrolls Online*[14][18]
- Electronic Arts[17]
- Etsy[12][19]
- FiveThirtyEight[14]
- Fox News[20]
- *The Guardian*[20]
- GitHub[12][17]
- Grubhub[21]
- HBO[14]
- Heroku[22]
- HostGator[14]
- iHeartRadio[13][23]
- Imgur[24]
- Indiegogo[13]
- Mashable[25]
- National Hockey League[14]
- Netflix[14][20]
- *The New York Times*[12][17]
- Overstock.com[14]
- PayPal[19]
- Pinterest[17][19]
- Pixlr[14]
- PlayStation Network[17]
- Qualtrics[13]
- Quora[14]
- Reddit[13][17][19]
- Roblox[26]
- Ruby Lane[14]
- *RuneScape*[13]
- SaneBox[22]
- Seamless[24]
- *Second Life*[27]
- Shopify[12]
- Slack[24]
- SoundCloud[12][19]
- Squarespace[14]
- Spotify[13][17][19]
- Starbucks[13][23]
- Storify[16]
- Swedish Civil Contingencies Agency[28]
- Swedish Government[28]
- Tumblr[13][17]
- Twilio[13][14]
- Twitter[12][13][17][19]
- Verizon Communications[17]
- Visa[29]
- Vox Media[30]
- Walgreens[14]
- *The Wall Street Journal*[20]
- Wikia[13]
- *Wired*[16]
- Wix.com[31]
- WWE Network[32]
- Xbox Live[33]
- Yammer[24]
- Yelp[14]
- Zillow[14]

https://en.wikipedia.org/wiki/2016_Dyn_cyberattack#Affected_services

誰が？なんのために？

誰:

犯行声明が幾つか出ているが、信憑性が薄く、誰がやったかは判明していない。
指名手配も未だされていない。

目的:

Dynの技術者がNANOG68で対DDoSの発表をしたことに対する報復とも、Electric Artsの新作ゲームに対するDDoSとも言われているが、犯人が不明なので判然としない。

被害の拡大

- ダウンしたサイトは、Dynの権威DNSサーバのみをNSレコードとして設定していた

  権威DNSを複数サービスや自社運用で分散していれば(直接狙われたところ以外は)ダウンすることは避けられたはず。

- 短すぎるTTLによる弊害

  CDN/GSLBの利用時に、(常に)TTLを短くしておくことが多いが、権威DNSサーバが落ちたときにキャッシュDNSサーバに残っているキャッシュが早々に消えてしまう。

  TTLが1日など長ければ、被害が軽微だった可能性も。

攻撃手法

Mirai(botnet)を利用してDDoS攻撃

- Miraiについては初日の「DDoSトレンド2016」で詳解がなされました。

  IIJでも解説しています。 (その1, その2)

- パスワードがザル・デフォルトなホームルータ・WebカメラなどのIoT機器に侵入・感染してbotnetを形成し、DDoS攻撃。
- 9末にsource codeが公開 (githubに転載)

  感染機器: 公開前21万台、公開後49万台

  Dynインシデント後減ったとも言われている

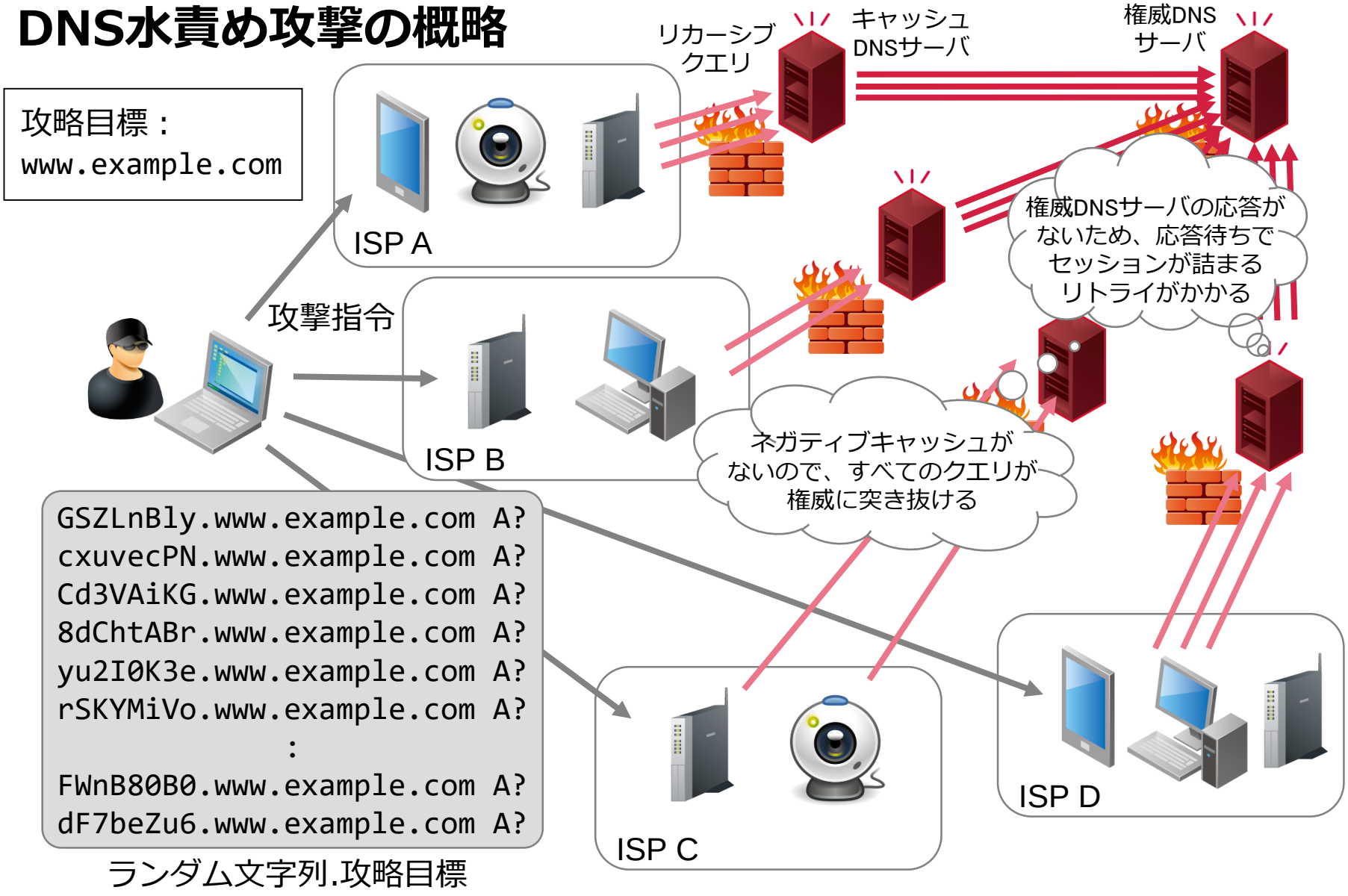
攻撃手法

Miraiには色々な攻撃手段が実装されている

- UDP/SYN/ACK/TCP stomp/GRE/HTTP flood
- Valve source engine flood
- DNS水責め攻撃 (ランダムサブドメインアタック)

攻撃手法

DNS水責め攻撃の概略



攻撃手法

IoT機器→キャッシュDNSサーバ→Dyn権威DNSサーバの経路でDNS水責め攻撃

- 権威サーバの応答がないとキャッシュサーバがリトライしてしまい、トラフィックがさらに増える

Miraiの戦果

- 9末: セキュリティニュースを発信するジャーナリストのblogに対しDDoS攻撃(620Gbps)

  DDoSサービスの運営者が存在を暴露されたことに対して報復したとみられる

  (無償で提供していた)Akamaiが音を上げ、最終的にGoogleのProject Sheildで保護

- 10末: Dynの権威DNSサーバに対してDDoS攻撃

  その後、Miraiかは不明だが StarHub, Dyn(再), GoDaddy, eNom がDDoS攻撃に遭っている

- 11末: ドイツテレコム配布の90万台のWiFiルータを一斉にcrashさせる

  侵入後のマルウェア感染(乗っ取り)に失敗してのcrashとみられている

攻撃への加担をどう防ぎますか？

- ちょっと前はリフレクション攻撃に加担しないように、BCP38しよう！と言っていた
  - MiraiはIPアドレスを詐称しません

    DNSリゾルバーは設定されてるもの(なければpublic DNS)を使うので、キャッシュDNSサーバが権威DNSサーバへの直接の攻撃元となりますが。
- firm updateに期待？
  - ユーザーがきちんと適用してくれますか？

    無理ですよね (自動適用ならともかく、)
  - メーカーが全ての機器を改修しますか？

    EoSを過ぎても何年も動き続ける機器

攻撃への加担をどう防ぎますか？

- 侵入経路を塞ぐ (IP23B? IP2323B?)
  - 他の侵入経路だったらどうしましょう？

    エンドユーザーは全員CGN配下に… とか？？
- DNSでC&Cサーバをshinkhole?
  - Miraiは進化してDGAを使うようになったそうで、shinkholeしづらくなりました
  - C&Cサーバの名前解決をpublic DNSや自前でやられたら？

    網側でIPアドレスでfilterしたりしますか？？

    C&Cサーバ(のIPアドレス)なんて代えはいくらでも…

攻撃への加担をどう防ぎますか？

さて、どうしたものでしょう…