DoS攻撃即応-WG

2013年11月28日

Telecom-ISAC-Japan ステアリングコミッティ運営委員
DoS攻撃即応WG主査
株式会社インターネットイニシアティブ
齋藤　衛

Telecom-ISAC Japan
Telecom Information Sharing and Analysis Center Japan

WG活動目的

本活動を通じて、DDoS攻撃への迅速な対応と複数事業者による協調対処の仕組みを検討、実現

日本国内におけるDDoS攻撃発生の予測、早期検出、迅速かつ適切な対応の実現を目指す。

- ✓ 『電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン』に基づく協調対応の実現
- ✓ DDoS攻撃発生状況の確認と即応能力の向上
  - ●攻撃予告情報への対応
  - ●攻撃発生状況の共有
  - ●攻撃観測情報に基づいた状況確認
  - ●攻撃発生後の状況取りまとめと共有及び公開
- ✓ DDoS攻撃対処能力の向上
  - ●攻撃への自動対応方法の検討
  - ●自社網内の攻撃者への対応の検討
  - ●その他の施策の検討

活動概要

➢現在までの活動状況

- 協調対処に向けて、情報共有体制の構築
  - 情報共有については2013年1月より試験運用中
- 協調対処に向けた技術的検討
- 利用者側の立場でのDDoS攻撃対策まとめ
  - DDoS攻撃のリスクとその対処についてまとめ、提言を実施予定
- 重要インフラ事業者Webサイトの応答時間測定
  - CEPTOAR Councilの協力のもと、重要インフラ企業の申告に基づき応答時間を計測。
  - 監視URL数（監視URL：2087）(2013年11月現在)
- 事件の情報共有
  - DNS Amp攻撃の兆候について
  - 個別同時多発攻撃に関する状況

DDoS攻撃の状況

➢2013年概況

- 頻度
  - 発生頻度はかわらず、もしくは増加傾向。

- 規模
  - 国外では 300Gbps(2013/03欧州)、167Gbps(米国)など、非常に大規模な攻撃が発生。
  - 国内でも10Gbpsを超える攻撃が頻繁に発生。

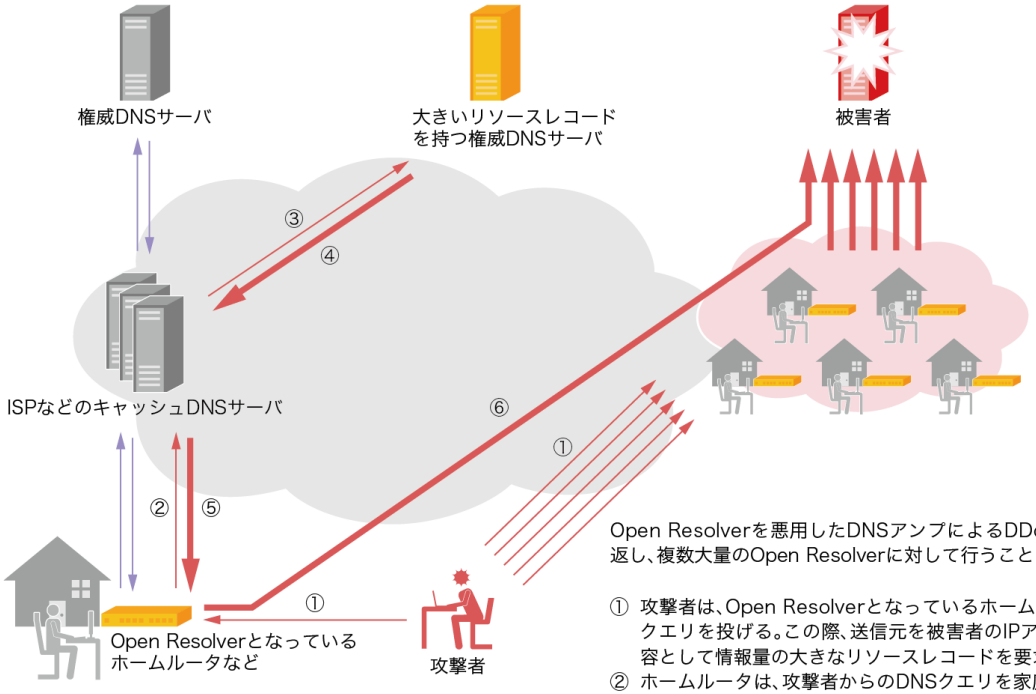
- 歴史的背景による攻撃
  - 本年は目立った攻撃は発生せず。一方で、攻撃の対応能力を測るかのように、短時間の攻撃が散見された。

- 攻撃手法
  - 大規模な攻撃に関連してDNS Amplification 攻撃に注目。
  - DNS運用者連絡会SiG,サイバー攻撃即応スキーム検討WG,脆弱性保有ネットワークデバイス調査WGなど、他の活動と連携する必要性。
  - 一方で、従来型の攻撃手法も依然として悪用されている。

DNS Amplification攻撃

➢概要

- 大きなRRを持つ権威サーバのqueryが攻撃に利用される。
- 故意に大きなのRRを登録した攻撃用のドメインも存在している。



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。

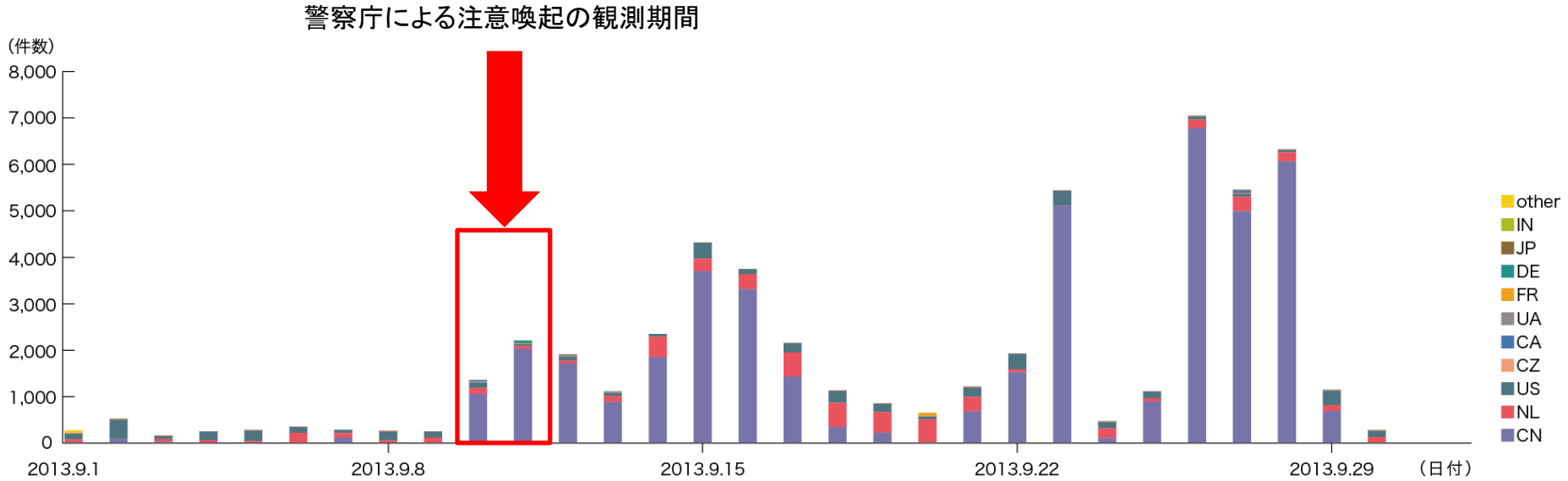
① 攻撃者は、Open Resolverとなっているホームルータに対し、攻撃用のDNSクエリを投げる。この際、送信元を被害者のIPアドレスに詐称し、クエリの内容として情報量の大きなリソースレコードを要求する。
② ホームルータは、攻撃者からのDNSクエリを家庭内ネットワークからの要求と同様に処理し、ISPなどのDNSサーバに転送する。
③ ISPなどのDNSサーバでは、正当な利用者からの通信であるため、攻撃用のDNSクエリと正当なDNSクエリとを判別することができず、当該攻撃DNSクエリをインターネット上の権威DNSサーバに送付する。
④ 攻撃DNSクエリの内容に応じて、権威DNSサーバから情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

DNS Amplification攻撃

➢概況

- DNSのOpen Resolverとなっている装置を踏み台とした攻撃は散発的に発生している。
- 大規模攻撃によりISPの関連設備に影響を与える場合も。
- 攻撃の事前にスキャンをした形跡はごく少数であり、状況はあまりよくないことを示している。

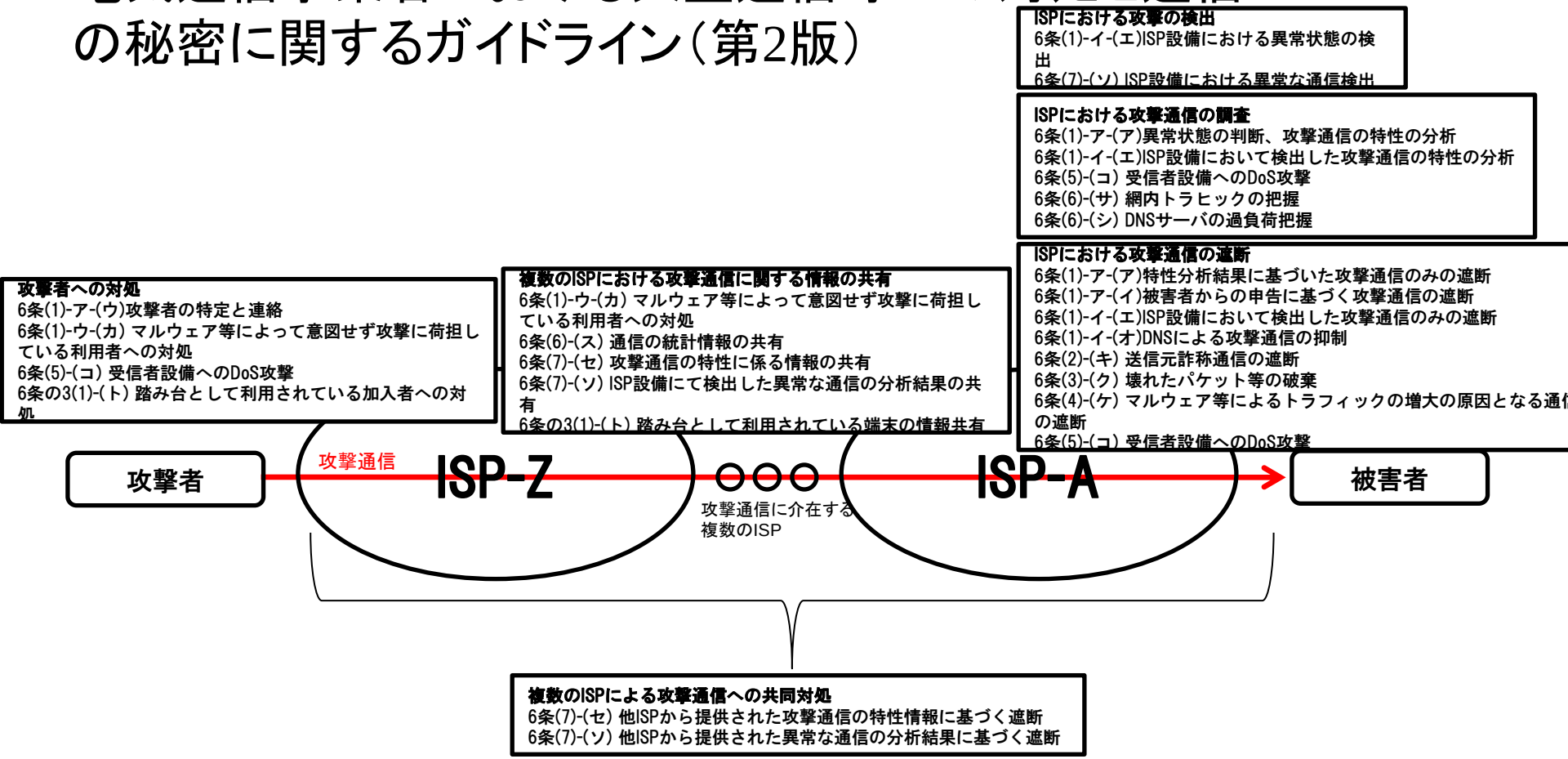


ハニーポットに到着した53/UDPの通信

Internet Initiative Japan , **Internet Infrastructure Review（IIR）Vol.21**より
（http://www.iij.ad.jp/company/development/report/iir/021.html）

DoS攻撃対策活動と通信の秘密の検討

電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン（第2版）



※この図はガイドライン内において、DDoS攻撃への対応の各段階に関する言及部分を列記したもの。
項番に対応する文章は言及内容をまとめたもので、実際の文章での表現とは異なる場合がある。

大量通信等のガイドラインにおけるDDoS攻撃対策

DoS攻撃対策活動と通信の秘密の検討

- 前提：影響範囲によるDDoS攻撃全体の分類
  - 個別ネットワークの問題
  - 特定のISPの事業に影響する規模の問題
  - 複数のISPの事業に影響する問題

- 今後の検討テーマ
  - 事業者間の情報共有の在り方
  - 事業者間の共同対処の在り方
  - 攻撃を実施している者、もしくは攻撃の可能性のある設備を恣意的に見つける活動の根拠