DNS運用の「見抜く」を探る

～セキュリティを考える際のポイントと最近のインシデント事例から～

2017年6月2日

Internet Week ショーケース in 名古屋

株式会社日本レジストリサービス（JPRS）

森下 泰宏

講師自己紹介

- 森下 泰宏（もりした やすひろ）
  - 日本レジストリサービス（JPRS） 技術広報担当
  - 主な業務内容：ドメイン名・DNSに関する技術広報活動全般

本日の内容

1. セキュリティを考える際のポイント
2. 最近のインシデント事例から
   - 権威DNSサーバーを標的としたDDoS攻撃
   - DNSを情報伝達手段として利用するマルウェア
3. DNS運用の「見抜く」のために必要な要素・項目

1. セキュリティを考える際のポイント

ポイント：攻撃と防御の理解

- 攻撃の理解
  - 何がどういう方法で攻撃されるか

攻撃対象と攻撃手法の理解

- 防御の理解
  - 何から何をどう守るか

想定すべき攻撃、守るべきターゲット、
とるべき対策・体制の理解

  - 守れることと守れないことは何か

対策の有効範囲の理解

攻撃の理解：何がどういう方法で攻撃されるか

- 攻撃対象による分類
  - ① DNSそのものを攻撃
  - ② 他者への攻撃をDNSで媒介
- 攻撃手法による分類
  - Volumetric attacks
  - Protocol attacks
  - Application attacks

DNSの機能を妨害してサービス不能にする

DNSを攻撃の手段として利用する
（偽サイトに誘導、攻撃の増幅など）

回線容量（帯域）をあふれさせる

プロトコル仕様の弱点を突く

実装・アプリケーションのバグや機能を利用

対象と手法によるDNS関連攻撃の分類

- 以下の6種類に分類可能（マトリックス図）

どういう方法で

何が ＼ 攻撃手法	a. Volumetric attacks（回線容量）	b. Protocol attacks（プロトコル仕様）	c. Application attacks（実装・アプリ）
①DNSそのもの	①-a	①-b	①-c
②他者（DNSで媒介）	②-a	②-b	②-c

- 例えば・・・
  - ①-a：DNSそのものが、大容量のトラフィックで攻撃される

    →権威DNSサーバーやフルリゾルバーへのDDoS攻撃はこれに該当

それぞれの攻撃の例

攻撃手法 / 攻撃対象	a. Volumetric attacks（回線容量）	b. Protocol attacks（プロトコル仕様）	c. Application attacks（実装・アプリ）
①DNSそのもの	①-a	①-b	①-c
②他者（DNSで媒介）	②-a	②-b	②-c

★①-a：権威DNSサーバーへの大量データ送信によるDDoS攻撃

★①-b：権威DNSサーバーへのTCP SYN Flood攻撃

①-c：BINDの脆弱性を突いたDoS攻撃

②-a：オープンリゾルバーを利用したDNSリフレクター攻撃

②-b：キャッシュポイズニングによる偽サイトへの誘導

★②-c：DNSを情報伝達手段として利用するマルウェア

★「最近のインシデント事例から」で紹介

DNSに特有のポイント

- 攻撃に対する気付き
  - DNSを利用した他者への攻撃（踏み台）は気付かれにくい
    - DNSの機能（サービス）は動作しているため

対策が遅れる場合が多い

- DNSのしくみ（の弱点）を攻撃に利用
  - DNSリフレクター攻撃
    - 主な通信がUDPで、応答が問い合わせよりも常に大きい
  - ランダムサブドメイン（DNS水責め）攻撃
    - 問い合わせ名にランダムサブドメインを付加し、キャッシュを無力化

防御の理解①：何から何をどう守るか

- 何から：想定される攻撃（敵）の明確化
  - 誰が何を使って攻撃して来るか（対象と手法）
- 何を：守るべきターゲットの明確化
  - 自分を守る（DNSサービスを守る、DNSデータを守る）
  - 他者を守る（自分の顧客（利用者）を守る、第三者を守る）
- どう：投入する対策や構築する体制の明確化
  - 今、どんな脅威にさらされているのか
    - とるべき対策やその優先度を考える上での出発点
  - 対策のための投資（人・物・金）をどうするか

防御の理解②：守れるものと守れないもの

攻撃手法 / 攻撃対象	a. Volumetric attacks（回線容量）	b. Protocol attacks（プロトコル仕様）	c. Application attacks（実装・アプリ）
①DNSそのもの	①-a	①-b	①-c
②他者（DNSで媒介）	②-a	②-b	②-c

- ポイント：各対策がマトリックス図のどの部分に該当するか
  - ①-a：サーバー・回線の増強、IP Anycast、複数のプロバイダーの利用など
  - ①-b：SYN Cookieなど
  - ①-c：脆弱性の修正、複数の実装を併用、外部DNSサービスの利用など
  - ②-a：BCP38、リゾルバーでのアクセス制限、DNS RRL、IP53Bなど
  - ②-b：DNSSEC検証、実装における工夫、プロトコルの改良など
  - ②-c：レジストラでの認証強化、レジストリロック、クエリログの取得など

マトリックス図を全部埋められる対策は存在しない

2. 最近のインシデント事例から

本日紹介するインシデント事例

① 権威DNSサーバーを標的としたDDoS攻撃

② DNSを情報伝達手段として利用するマルウェア

①権威DNSサーバーを標的としたDDoS攻撃

- 最近の状況
  - ルートサーバーに対するDDoS攻撃（2016年6月）
    - 古典的なSYN Flood攻撃が用いられた
  - 国内組織・サービスに対するDDoS攻撃（2016年8～9月）
    - Webサーバーに加え、権威DNSサーバーも攻撃対象となった
  - Dynのサービスインフラに対するDDoS攻撃（2016年10月）
    - マネージドDNSサービスに対する大規模な攻撃
    - 大量のIoTデバイスが悪用された（Miraiを用いたBotnetによる攻撃）

権威DNSサーバーを標的としたDDoS攻撃事例の報告が相次いでいる

最近のDDoS攻撃の特徴

- 攻撃規模の飛躍的な増大
- 攻撃手法の巧妙化
  - 「複数の手法を組み合わせた、複雑かつ高度な攻撃」が恒常化
    - Dynの分析レポート（2016年10月26日公開）

> The Friday October 21, 2016 attack has been analyzed as a complex & sophisticated attack, using maliciously targeted, masked TCP and UDP traffic over port 53.
>
> Dyn Analysis Summary Of Friday October 21 Attack
> <https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/> より引用

- 攻撃ツールの進化と利用の容易さから、手軽な攻撃が流行
  - 他人のツールを利用するだけで「複雑かつ高度な攻撃」が可能に

できることはあるのか？

- 数百Gbpsクラスの攻撃をまともに食らったら非常に厳しい
  - 最後は、物量作戦（資源投入）になりがち
    - 例：IP Anycastやサーバーの分散化などによる、大規模なスケールアウト
    - さまざまなサービスプロバイダーがソリューションを発表・提供
- 攻撃を受ける以前にできること
  - 起こりうることを見抜き、備える
    - 攻撃の効果軽減
    - 情報提供用チャンネルの確保（特にサービス提供者）
  - 起こりつつあることを見抜き、早期に対策する
    - 攻撃の検知・緩和

対策：攻撃の効果軽減

- サービスダウンした際の被害を最小限に留めるための備え
- 複数のDNSプロバイダーを併用する（サービスの冗長化）
  - データの管理において注意が必要
    - 下記資料のp.29～36に詳細な解説あり

参考：DNSにまつわるセキュリティのあれこれ（IIJ 島村充氏）
<http://www.iij.ad.jp/company/development/tech/techweek/pdf/161111_04.pdf>

- TTL値を無用に短くするのを避ける
  - 特に、NSやネームサーバーホスト名のA/AAAAのTTL値に注意
    - ゾーンの$TTL設定は、NSやネームサーバーホスト名にも適用されることに注意

対策：情報提供用チャンネルの確保

- サービスやWebサイトがダウンしている間も提供（利用）可能な、情報提供用のチャンネルを別途確保する
  - 顧客や組織内外の関係者に、障害状況や対応状況を伝達
    - 自身の障害のため、アナウンスを読んでもらえない状況を回避
- 運用事例
  - Dyn Status Updates <https://www.dynstatus.com/>
    - サービス状況提供用、自社インフラに依存しない形で以前から運用
    - 2016年10月の障害の際、Webと電子メールによる緊急の情報提供を実施
  - Twitterなど、外部のサービスの利用
    - 2016年8～9月の障害の際、さくらインターネットや技術評論社が実施

対策：攻撃の検知・緩和

- 攻撃の検知
  - 権威DNSサーバーにおけるトリガーの例
    - 未見かつ複数のIPアドレスから、多数のDNSクエリが到達する
    - 同一IPアドレスから、同内容のDNSクエリが頻繁に到達する
      - かつ、リソースレコードのTTL値よりも明らかに短い

  ⇒ 適切な攻撃検知と、適切なフィルタリングの組み合わせが有効
- 攻撃の緩和
  - ネットワーク・サーバーにおける緩和策の例
    - 上流ISPとの連携
    - 権威DNSサーバーの複数ネットワーク・サービスへの配置

②DNSを通信手段として利用するマルウェア

- 従来の手法：DNSのデータ（RDATA）を通信に利用
  - DNSトンネリング（DNS tunneling）と呼ばれている
  - TXTレコードが使われることが多い
- 最近、DNSクエリのQNAMEを通信に利用するマルウェアが、相次いで報告された
  - QNAME：問い合わせの名前情報（ドメイン名）

Botと指令サーバー間の通信

- 遠隔操作ウイルスの制御にDNSクエリを利用する事例

遠隔操作ウイルスの制御にDNSプロトコルを使用する事案への注意喚起
（株式会社ラック、2016年2月1日）
<http://www.lac.co.jp/security/alert/2016/02/01_alert_01.html>

– DNSクエリのQNAMEを、Botと指令サーバー間の通信に利用

<30文字以上の文字列>.<5種類のサブドメイン>.example.jp

- 指令サーバーとの通信データ？
- 標的名 or 作戦名？
- 攻撃者の制御下にあるドメイン名

DNSクエリによる情報の抜き取り

- WindowsベースのPOS端末に感染、抜き取ったクレジットカード情報をDNSクエリで送信するマルウェアの事例

MULTIGRAIN – Point of Sale Attackers Make an Unhealthy Addition to the Pantry
（米国FireEye社、2016年4月19日）
<https://www.fireeye.com/blog/threat-research/2016/04/multigrain_pointo.html>

– DNSクエリのQNAMEに、クレジットカード情報を載せる

log.<Base32エンコードされた文字列>.example.jp

カード番号・有効期限・セキュリティコードを
1024bit RSA公開鍵で暗号化した後、Base32エンコード

攻撃者の制御下にあるドメイン名

DNSクエリが通信に利用される背景

- 攻撃者にとってメリットがある
  - DNSクエリログが取られていないことが多い
  - 外部に対するDNSクエリがフィルターされていないことが多い
  - 使うドメイン名を頻繁に変更して、フィルターの回避を図れる
  - 標的にインターネット到達性がなくても、情報を抜き取れる
    - フルリゾルバー（キャッシュDNSサーバー）経由で情報を入手
- 感染や機密情報の抜き取りを検出するための仕組みが必要

攻撃を「見抜く」ための材料集めと仕組み作り

提案されている対策

① 内部向けフルリゾルバーでのDNSクエリログ取得・保存・調査
- 被害に遭ったことを知る
- 何かあった際、さかのぼって調査できるように備えておく

② ①に加え、エンタープライズネットワークでのOP53Bの適用
- 組織が提供しているリゾルバー以外の利用を制限
- US-CERTが推奨：

Alert (TA15-240A) Controlling Outbound DNS Access
<https://www.us-cert.gov/ncas/alerts/TA15-240A>

③ アプライアンス製品などの導入検討
- いくつかのベンダーからソリューションが発表・提供されている

通信の秘密への配慮

- ISPが顧客向けネットワークにこれらの対策を適用する場合、「通信の秘密」への配慮が必要
- 対策の適用が違法性阻却事由（正当業務行為・正当防衛・緊急避難）に該当するかどうかを、慎重に確認する必要あり

参考：通信の秘密とは？（IP Meeting 2006発表資料）
<https://www.nic.ad.jp/ja/materials/iw/2006/main/ipmeeting/ipmeeting2006-03.pdf>

3. DNS運用の「見抜く」のために必要な要素・項目

①気付き

- 普段と何か違う、何か様子がおかしい、など
  - Webブラウザーの表示、システムの反応、DNSの応答、etc.
    - 何だか重い、という感覚が障害発見のきっかけになる場合が多い
  - 「気付き」はシステムやネットワークの状況などに限らない
    - 日常業務におけるさまざまな気付き
    - 日常生活におけるさまざまな気付き

②状況把握

- 普段の状況を把握することで、普段と違うことを把握できる
  - 知る（気付く）ための仕組み作り
    - トラフィックの異常な変化や異常なクエリの検出、アラートの伝達
    - 各種ログの取得・分析
  - 普段の積み重ねと有事に対する備え
    - 見抜くための感覚の向上
    - 有事を想定したシステム設計・設定の実施

③仕組み作り

- 知る（気付く）ための仕組み作り
  - 予防・早期発見・早期対応につなげる
  - 被害を小さくできたり再発を防止できたりする場合がある
- 適切、かつ機能する（見抜ける）仕組み作り
  - 新たな攻撃手法に対応するための仕組み作り

④普段の積み重ねと備え

- 見抜くための感覚（直感）の向上を図る例
  - 触る（サーバー、システム、ネットワーク、etc.）
  - 普段のトラフィックパターンや傾向の把握
  - 運用対象の技術仕様（仕組み）や動作の把握（勉強）
- 有事を想定したシステム設計・設定の例
  - 複数のDNSプロバイダーの併用
  - 対外的なリレーションや連絡網の確保

⑤周囲や社会の理解

- 日常の積み重ねや備えは、得てして適切に評価されない

「しっかり運用していても、普段は頑張りを認められづらい」
「障害を起こすと大変怒られる」

（IIJ 島村充氏の発表資料（前出）より引用）

- こうした取り組みが、周囲や社会に理解されることが重要
  - 経営者・上司による、組織としての理解
  - 組織内・組織外に対する啓発活動
  - ひいては、技術者・運用者の社会的プレゼンスの向上

おわりに

- 本パートで取り上げた五つの項目

  ①気付き　②状況把握　③仕組み作り
  ④普段の積み重ねと備え　⑤周囲や社会の理解

- DNS運用の「見抜く」は、日々の運用の中にある
  - サービスを安定、かつ安全に動かし続けるための継続的な活動
- そして、その取り組みが内外で正しく理解されることも重要
- というわけで、日々の運用と「見抜く」の両立は大変ですが…

DNSをよりよく、楽しく支えていくため、
みんなで力を合わせてがんばっていきましょう

謝辞

- 本資料は2016年12月1日に開催したInternet Week 2016 ランチセミナーの内容をベースにしており、開催後にいただいたご意見をもとにDNS運用者にとってよりよい内容となるよう、改訂を加えています。
- 貴重なご意見をいただいた方々に、この場を借りてお礼申し上げます。

That’s it!