CSC

セカンダリDNSサービスの事例

オンライン資産を守る、優れたセキュリティ戦略

他人事ではありません

2016年10月21日、マネージドドメインネームシステム（DNS）の大手プロバイダーが分散型サービス妨害攻撃（DDoS）を受け、運用不能に陥りました。この攻撃の恐ろしいところは、DNSプロバイダーの可用性やサービスを停止するだけでなく、企業のウェブサイトやアプリケーションが断続的に停止して、多くの大手ユーザー企業側にも被害が広まることです。

このような攻撃を経験した後で実感するのは、DDoS攻撃、特にDNSを対象とした攻撃は、誰もがその脅威から逃れられないという現実です。しかし、それと同じぐらい不安を煽ったのは、被害を受けた各社は何も間違ったことをしていないという事実です。その時点では、多くのコンサルタントが勧める対策を取っていました。つまりマネージドサービスにドメイン名管理を一括委託したのです。しかし、バックアップ対策が取られなかったことが、致命的な結果につながりました。

10月21日の攻撃は、DDoS攻撃が将来組み立てられる方法が根本的に変化することを示しています。この攻撃はMiraiボットネットというマルウェアを使って行われました。MiraiボットネットはセキュリティカメラやDVR、家庭用ルーターなど、インターネットに接続されている非典型的なデバイスで構成されています。これらの乗っ取られたデバイスは、危険なほど強力な大量兵器を作り出しました。Miraiボットネットは、これまでとは桁違いの破壊的DDoS攻撃を仕掛けました。あまりに効果的なため、ボットネットは非常に危険な「先駆者」となりました。

ここで最も重要なのは、この攻撃によって、DNSが新たな要件を必要とする貴重な機会となったということです。特に企業は1つのDNSサービスだけに、オンラインのプレゼンスをすべて委ねるべきではありません。1つのDNSプロバイダーだけに頼っていた組織は、結局、単一障害点にすべてを委ねたため、現実面で多大な影響を被りました。もし、これらの企業がDNS管理を複数のサービスに分散していたら、そのサイトや、アプリ、その他のオンラインの資産は、攻撃の真っ最中でもダウンせずに済んだでしょう。

さらに問題を悪化させたのは、現代のサイバー犯罪の恐ろしいスピード性です。サイバー攻撃を限定する強固な戦略を取っていても、6か月も経てばそれは旧式な戦略になってしまいます。DNS攻撃では特にこの傾向が顕著で、サイバー犯罪者は常にDNSの脆弱性をターゲットにして混乱させる新しい方法を実現しているのです。

本ドキュメントはNeustar®による「The Case for a Secondary DNS Service（セカンダリDNSサービスの事例）」に基づいて作成されました。

新しい技術を導入し、セキュリティ戦略を常に新しくすることで、企業はDNSのセキュリティを最小限のコストと手間で効果的に更新できます。

DNSのジレンマについて詳しく説明します

今日のインターネット時代において、エンタープライズのセキュリティは主にオンラインの境界（つまりネットワーク境界）の保護に焦点を当てています。その理由は、マルウェアや危険因子をネットワークに入れさえしなければ、データや事業を保護できるという理論です。しかし、サイバー犯罪者は執念深く、適応力があります。一つドアを閉めれば、別の窓を開けるというイタチごっこです。そのため、最近のサイバー犯罪者は、オンライン上でのプレゼンスを成り立たせているプロトコル、つまりDNSを攻撃することで、組織に影響を与え、混乱させることができると気が付くのに、それほど時間はかかりませんでした。

その重要性にも関わらず、これまでセキュリティに関してDNSはこれまであまり深刻に捉えられていませんでした。リクエストの転送に使用されるパブリックプロトコルとして解釈されており、それ自体がセキュリティの脆弱性とは見られていませんでしたが、DoSその後DDoSへと発展した「サービス拒否」攻撃により、これらはすべて変わりました。DNSサーバーにリクエストを大量に送りつけるこの攻撃により、サイバー犯罪者は組織のウェブサイトやアプリケーションを無期限にダウンさせることができます。ウェブサイトやアプリケーションの可用性はDNSと密接に関わっているため、セキュリティの重要性が一躍認識されるようになりました。

DNSサーバーの攻撃にまず必要なのは、その物理アドレスです。独自のドメイン名をホストすると、インターネットのスキルが少々ある者なら誰でもDNSアドレスを容易に見ることができます。インターネットに精通したユーザーなら、30秒以下で、保護されていないDNSアドレスを見つけることが可能です。当然ながら、セキュリティコンサルタントは、組織に対し、セキュリティが確保された効率的な手法でDNSリクエストの処理を行うよう、外部DNSプロバイダーを使用するよう勧めます。

権威あるDNSの適切なセキュリティ対策

権威あるDNSサービスを守るために組織ができる最も重要な対策は、プライマリとセカンダリDNSソリューションを実装することです。Miraiボットネットの攻撃以来、業界アナリスト（ガートナーなど）は、パフォーマンスとセキュリティ向上のため、セカンダリDNSを持つことを組織に推奨しています。

セカンダリDNSサービスを冗長DNSプロバイダーと混同してはいけません。これは、プランAが失敗した場合に備えてプランBを用意することではありません。これは、2つの信頼できるネットワーク間でDNSトラフィックを効果的に分割する、よりスマートなプランAを構築することなのです。この戦略は単一のテイクダウンDDoS攻撃に対してブランドを防ぐだけでなく、2つのネットワーク間で負荷を分割させることでDNSの冗長性を向上させます。

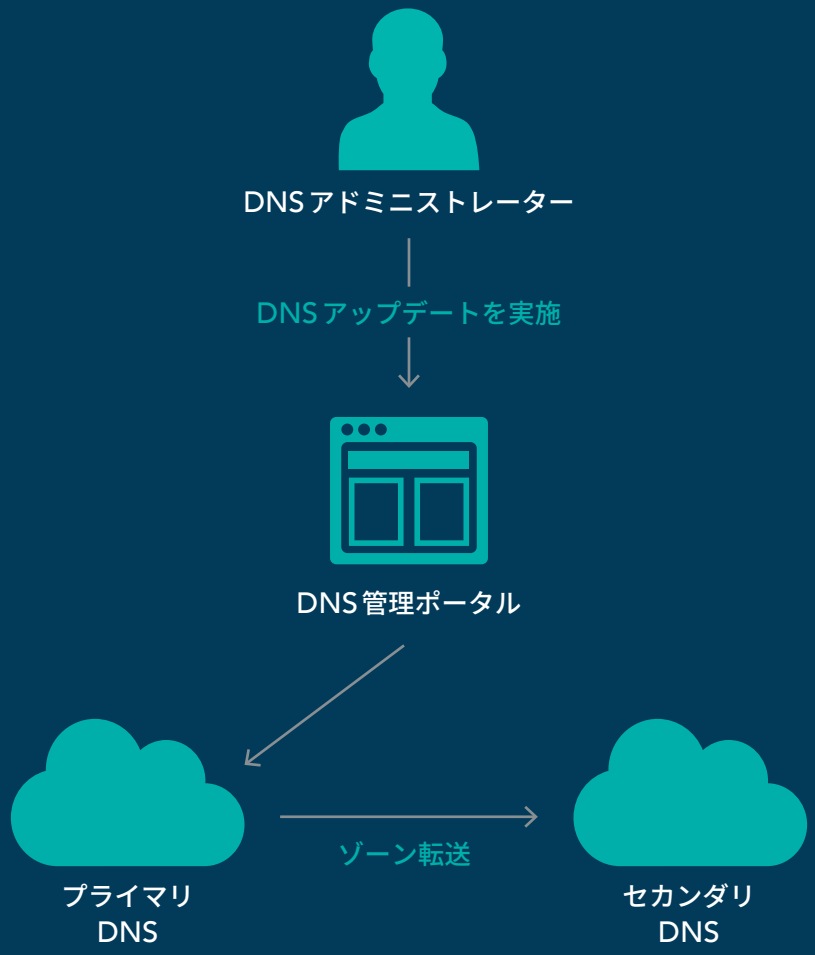
まずは、セカンダリ マネージドDNSサービスを見つけることが、DNSセキュリティ強化に向けた第一歩と言えます。次に、マネージドDNSネットワークに対して自社内に専用のDDoSリスク低減サービスを提供するDNSプロバイダーを選ぶことが大切です。インターネットに接続されている機器が多いほど、ボットネット軍隊の「兵隊」の数や種類が増えるため、DDoSの別の保護層は組織にとって効果的です。さらに良いことには、エアギャップネットワークを介して、DNSをインターネット上で「隠し」、直接の露出を避ければ、DNSに対する攻撃数を劇的に減らすことができます。

権威あるDNSの強化セキュリティ対策には次のようなものがあります。

- プライマリおよびセカンダリマネージドDNSサービス
- DNSネットワークに対して自社内に専用のDDoSリスク低減サービスを持つDNSプロバイダーを選択する
- DNSシステムをインターネットに直接露出させない

プライマリおよびセカンダリDNSの仕組み

1. DNSアドミニストレーターがDNS管理ポータルにログインする
2. DNSアドミニストレーターがDNSレコードをアップデートする
3. DNSネットワークを通じて変更を伝播する
4. セカンダリDNSにアップデートがあったことが伝えられ、アップデートされたレコードを受信するためDNSゾーン転送を実施する



信頼できる安全なパートナーと提携し、DNS攻撃への対策を一層強化する

英語のことわざに「鎖の強さは、その中の一番弱い輪の強さである」とあるように、セキュリティはあなたの最も弱い部分に左右されます。必要なセキュリティを提供できるプロバイダーと協力する必要があります。CSCは現在のマーケットで最もセキュリティを重視する、エンタープライズ向けドメイン、DNS、デジタル証明書のプロバイダーです。当社はシステムの安全性を確保するためセキュリティポリシーを実施、またスタッフは脅威を認識し、低減する訓練を受けており、365日年中無休の体勢でお客様のデジタル資産を守っています。当社のセキュリティ対策において重要なことは、適切なパートナーを選択して提携することです。

CSCはNeustarと提携しています。それは、Neustarは、現在のデジタル環境においてDNS運用に求められる可用性、拡張性、セキュリティを提供する能力を備えたエンタープライズクラスのプロバイダーだからです。Neustarは、組織をあらゆる種類の脅威から保護する高度なDNSセキュリティソリューション構築に重点的に投資を行ってきました。当社のドメインおよびデジタル証明書管理サービス、CSCセキュリティセンター℠と共に、CSCは、ファイヤーウォールの外にあり、DNSキャッシュ汚染、ドメイン名ハイジャック、ドメインシャドウイング、DDoS、マルウェア、フィッシングなど様々な危険に晒されているデジタル資産すべてをクライアントが安全に管理できるようにします。

CSCセキュリティセンターと当社のDNS管理サービスが、サイバー犯罪の脅威からお客様をお守りする方法について、ぜひ詳細をお問い合わせください。

CSCは、ドメイン名、DNS、デジタル証明書などの基本的なインターネット資産内に存在する盲点を開示することにより、セキュリティ体制に多大な投資を行っている企業をサポートします。CSCは独自のセキュリティソリューションを活用することで、企業をサイバー資産からのデジタル資産への脅威から保護し、GDPRなどのポリシーによる、収益の損失、ブランドへの中傷、重大な経済的ペナルティを回避します。CSCは、インターネット資産と共に、偽造サイト、詐欺、IP侵害を介して悪用されるオンラインブランドを保護、監視および緩和し、多くの世界最大手ブランドの保護およびアドバイザリーサービスを提供しています。詳細につきましては、cscdigitalbrand.services/jpをご覧ください。

cscdigitalbrand.services/jp