JPRS トピックス＆コラム

■Bot経由でDNSサーバーを広く薄く攻撃
～DNS水責め攻撃の概要と対策～

「DNS水責め攻撃」と呼ばれる攻撃手法が、2014年初頭から世界的に観測されています。今回はこの攻撃手法の概要と、現時点における対策について解説します。

■DNS 水責め攻撃の特徴

DNS 水責め攻撃では、攻撃対象のランダムなサブドメインに対する DNS 問い合わせが攻撃に使われます。

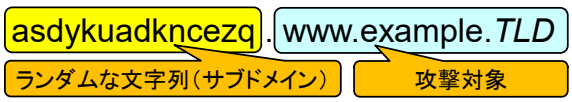

図 1：攻撃に使われる問い合わせパターンの例

この問い合わせはカミンスキー型攻撃手法で用いられるものと同一であり、「**ランダム DNS クエリ攻撃**」や「**ランダムサブドメイン攻撃**」などとも呼ばれています。

▼攻撃の目的と攻撃対象

DNS 水責め攻撃ではカミンスキー型攻撃手法と異なり、キャッシュポイズニングを目的とした攻撃パケット（偽の DNS 応答）が検出されません。そのため、この攻撃が最初に観測された 2014 年初頭の段階では、攻撃者の真の目的が判然としませんでした。

その後、2014 年 5 月から 7 月にかけ、数多くのドメイン名がこの攻撃の被害を受け、アクセス不能の状態に陥りました。その際の攻撃パターンや攻撃対象の分析結果から[1]、攻撃対象のドメイン名を管理する権威 DNS サーバーに大量の DNS 問い合わせを送り付けることでサービス不能の状態にし、そのドメイン名をアクセス不能の状態に陥らせることが攻撃者の目的であったと考えられています。

▼ISP のフルリゾルバーにも被害が発生

前述した 2014 年 5 月から 7 月の攻撃では権威 DNS サーバーに加え、複数の ISP を含む数多くのフルリゾルバー（キャッシュ DNS サーバー）も過負荷の状態となり、一時的にサービス不能の状態に陥りました。

[1] 複数の報告者から、攻撃対象となったドメイン名の多くが中国・台湾・香港の EC サイトやカジノサイトなどであったと報告されています。

■Water Torture = 水責め

2014 年 2 月にこの攻撃について報告した米国 Secure64 Software が、この攻撃手法を「Water Torture（水責め）」と命名しました[2]。同社では命名の由来をかつて中国などで行われていた「Chinese Water Torture[3]（中国式水責め）」であるとしています。

■DNS 水責め攻撃の概要

DNS 水責め攻撃の概要を、以下の図で説明します。

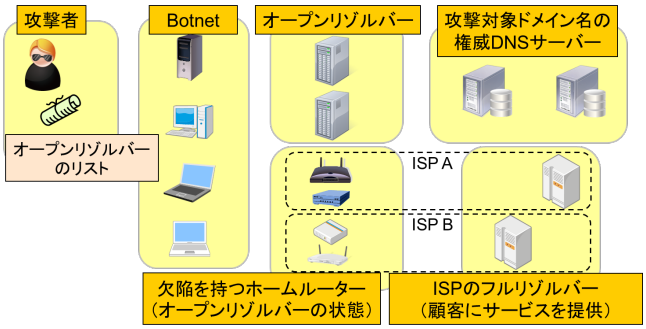

図 2：DNS 水責め攻撃の登場人物

▼攻撃者・Botnet

DNS 水責め攻撃を実行する**攻撃者**は、インターネット上の**オープンリゾルバーのリスト**を持っています。

また、攻撃者は多数の PC などにより構成される Botnet を遠隔操作することで、攻撃を実行します。

▼オープンリゾルバー・欠陥を持つホームルーター

このオープンリゾルバーのリストにはフルリゾルバーの他、本来受け付けてはならない WAN 側からの問い合わせを受け付けて処理してしまう、**欠陥を持つホームルーター**も掲載されています。これらは外部から見た場合、**いずれもオープンリゾルバーとして動作**します。

[2] Water Torture: A Slow Drip DNS DDoS Attack
https://secure64.com/water-torture-slow-drip-dns-ddos-attack/

[3] Wikipedia: Chinese water torture
https://en.wikipedia.org/wiki/Chinese_water_torture

▼ISP のフルリゾルバー

ISP のフルリゾルバーは、自身の顧客に名前解決サービスを提供します。

DNS 水責め攻撃では顧客側に設置された多数のホームルーターから ISP のフルリゾルバーに、大量の DNS 問い合わせが送られます。そのため、**そのフルリゾルバーがオープンリゾルバーではない場合にも、攻撃の被害を受ける可能性があります。**

▼攻撃対象ドメイン名の権威 DNS サーバー

攻撃対象ドメイン名を管理(収容)する権威 DNS サーバーです。

DNS 水責め攻撃では攻撃対象の権威 DNS サーバーに大量の DNS 問い合わせを送り付け、サービス不能の状態にします。そのため、そのサーバーが複数のドメイン名を管理している場合、**攻撃対象以外のドメイン名も攻撃の巻き添えになる可能性があります。**

■DNS 水責め攻撃の仕組み

DNS 水責めによる攻撃例を以下に示します。

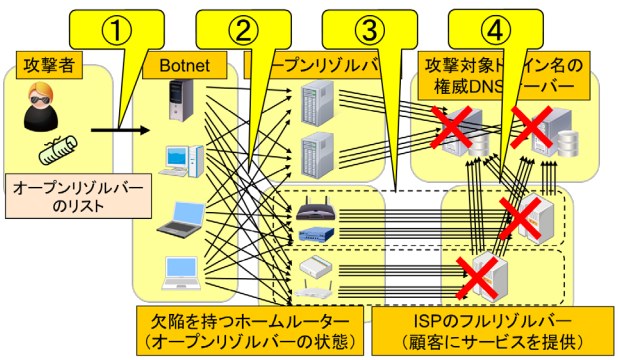

図 3:DNS 水責め攻撃の仕組み

① Botnet に対し、リストに掲載されているオープンリゾルバー[4]に、攻撃対象ドメイン名のランダムなサブドメインを DNS 問い合わせするように指令します。

② 規制回避のため、各 Bot からの DNS 問い合わせは低い頻度で送られます。しかし、使われる Bot の台数が大量であるため、各オープンリゾルバーには大量の問い合わせが到達します。

③ 問い合わされた名前はキャッシュに存在しないため、**権威 DNS サーバーへの問い合わせが毎回発生します。**ホームルーターの場合、**ISP のフルリゾルバーに問い合わせが転送されます。**

④ 攻撃対象の権威 DNS サーバー、及び ISP のフルリゾルバーに**問い合わせが集中します。**結果としてこれらのサーバーが過負荷となり、サービス不能の状態に陥ります。

▼DNS の仕組みを攻撃にそのまま利用

このように、DNS 水責め攻撃ではランダムなサブドメインを付加することで**キャッシュ機能を無効化**することで、**DNS の仕組みを攻撃にそのまま利用しています。**また、DNS リフレクター攻撃[5]と異なり問い合わせ元の IP アドレスを偽装する必要がなく、根本的な対策を実施しにくいことに特徴があります。

■攻撃対策

現時点における DNS 水責め攻撃の代表的な対策として、以下のものが実施されています。

▼ISP における IP53B の実施

IP53B(Inbound Port 53 Blocking)は、顧客側の 53/udp(DNS)へのアクセスを ISP 側でブロックすることにより、ホームルーターの欠陥を外部から利用できなくするものです。DNS リフレクター攻撃の対策としても有効であることから、IP123B(NTP)と共に国内外の ISP において、導入が進められています[6]。

▼フルリゾルバーにおける対策

DDoS 対策機器やロードバランサーにおける対策、BIND 9 の fetches-per-zone/fetches-per-server 機能や Unbound の ratelimit 機能の利用などが実施されています。

しかし、これらは攻撃発生後の事後対策となること、また、対策の実施により対象のドメイン名に対する DoS 自体は成立してしまうことに注意が必要です。

---

[4] 前述のようにこのリストにはフルリゾルバーの他、欠陥を持つホームルーターの WAN 側の IP アドレスも記載されています。

[5] JPRS トピックス&コラム No.3 を参照。

[6] IP53B/IP123B の実施にあたり、2014 年 7 月 22 日に JAIPA など 5 団体による「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」が改定されています。

