JPRS トピックス＆コラム

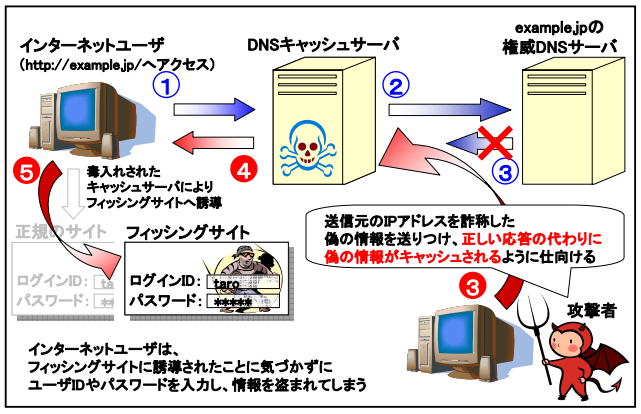
新たなるDNSキャッシュポイズニングの脅威 ～カミンスキー・アタックの出現～

DNSに不正なデータを記憶させドメイン名の乗っ取りを図る「DNSキャッシュポイズニング」と呼ばれる攻撃の危険性が高まっています。この攻撃の概要と対策について解説します。

■キャッシュ機能とDNSキャッシュポイズニング

DNS には、問合せによって得られた IP アドレスや権威 DNS サーバ名などの情報を一時的に記憶し、名前解決の際にそれらを再利用することで処理の効率化を図る、という機能があります。これを DNS の**キャッシュ機能**といい、DNS キャッシュサーバや一部の DNS クライアントに実装されています。キャッシュ機能は DNS サーバへの問合せ数を大幅に減少させ、DNS やネットワークの負荷を全体に軽減させるという重要な役割を担っています。

しかし、この機能を悪用し、偽のデータをキャッシュに記憶させることでドメイン名の乗っ取りやフィッシングなどを図る「**DNS キャッシュポイズニング**（DNS cache poisoning）」と呼ばれる攻撃が知られています。



DNS キャッシュポイズニングの概要

「ポイズニング」は、毒性を持つものが内部に取り込まれることにより正常な機能が阻害されることを表しており、「毒入れ」とも呼ばれています。

■DNS キャッシュポイズニングのしくみ

DNS では主要な通信プロトコルとして UDP を使用します。UDP では TCP と異なり、相手との通信前の折衝やデータの到達確認を行いません。そのため、UDP は TCP に比べてデータ到達の信頼性は下がりますが、相手との通信に必要な手間が少ないため、一度のやりとりで通信が完了し、かつサーバにおいて数多くのクライアントからの要求をできる限り短時間で処理する必要のあるプロトコルに向いたものであるといえます[1]。

しかし、UDP はその特性から、TCP に比べ通信データの偽造が容易であるという短所があります。そのため DNS では、処理毎に毎回異なった「ID」をつけ、問合せ内容とともに ID の一致も合わせてチェックすることにより、応答の正当性を確認しています。

しかし、現在の DNS プロトコルでは、悪意を持った第三者が、

①発信元として DNS サーバの IP アドレスを偽装し、
②問合せに使われた UDP ポートと同じポートに、
③問合せに使われた ID と同じ ID をつけ、
④本来の DNS 応答よりも先に応答を返す

ことができた場合、問合せ元はそれが偽のデータであることを判別できないため、DNS キャッシュポイズニングが成立してしまうことになります。

■DNS キャッシュポイズニングと TTL 値の関係

ここまでで解説した DNS キャッシュポイズニングの脆弱性そのものは、以前から知られていました。従来の DNS キャッシュポイズニング攻撃では、通常の DNS 応答、例えば www.example.jp に対し攻撃を試みる場合、www.example.jp の問合せに対する応答そのものを偽造する形で行われていました。

この場合、DNS キャッシュポイズニングが成功する可能性は、該当するデータの有効時間（TTL: Time To

[1] DNS が 20 年以上もの間その基本仕様を大きく変更することなく、急成長したインターネットを現在まで支え続けてこられたのは、通信プロトコルとしてコストの少ない UDP が採用されていたことが大きな要素の一つであった、といえるでしょう。

Copyright © 2008 株式会社日本レジストリサービス
※掲載内容は2008年9月現在のものです。

Live）の設定値に依存します。つまり、キャッシュが有効である間は目的とする名前に対する外部への問合せが行われないため、権威 DNS サーバ側で長い TTL を設定することにより、DNS キャッシュポイズニングに関する危険性をある程度軽減することができます。

TTLが有効な間、DNSキャッシュサーバは
その名前の外部ネットワークへの検索を行わない
↓
TTLが有効な間はそのDNSキャッシュサーバに対し、
従来の方法でのDNSキャッシュポイズニングはできない

DNS キャッシュポイズニングと TTL の関係

■新たに発見された攻撃方法

しかし、セキュリティ研究者のダン・カミンスキー氏が、より効率的に DNS キャッシュポイズニングを実行する方法を発見し、その方法が 2008 年の 7 月に明らかにされたことから、DNS キャッシュポイズニング攻撃に対する危険性が、**従来に比べ急激に高まりました**。この方法は「**カミンスキー・アタック**（Kaminsky Attack、あるいは Kaminsky's attack）」と呼ばれています。

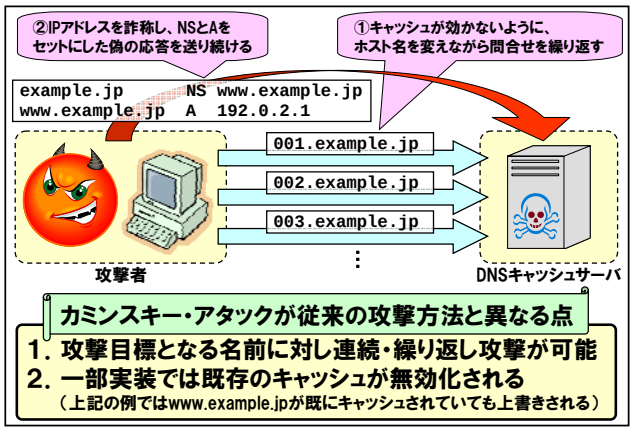
カミンスキー・アタックでは、攻撃対象の名前（例: www.example.jp）と**同じドメイン名内の存在しない名前**（例: 001.example.jp）の問合せを攻撃目標となる DNS キャッシュサーバに対して送り（あるいは、その名前を検索させるように仕向け）、その直後に「私はその名前（001.example.jp）を知らないが、www.example.jp が知っている。その IP アドレスは xxx.xxx.xxx.xxx（攻撃者が用意した偽のサーバの IP アドレス）である」という偽の応答情報を、ID を変化させながら DNS キャッシュサーバに大量に送りつけます[2]。もし、偽の応答が前節で解説した条件を満たした場合、DNS キャッシュポイズニングが成立してしまいます。

現在の DNS プロトコル（RFC 1035）では、DNS の ID は 16 ビットと定められているため、ID は最大でも 65,536 通りとなります。この値は現状のインターネットにおいて総当り攻撃に対し必ずしも十分な耐性を有しているとはいえません。

[2] 攻撃者は偽のサーバ上で、example.jp の偽の権威 DNS サーバをあらかじめ動作させておきます。

また、カミンスキー・アタックでは、問合せる名前を毎回変化させることにより、攻撃目標となる名前に対する攻撃を連続して繰り返し行うことができるようになります。従来の DNS キャッシュポイズニングではポイズニングが一度失敗した直後に同じ名前に対して即座に再攻撃を試みることは不可能でしたが、カミンスキー・アタックではそれが可能となります。

さらに、一部の DNS キャッシュサーバの実装ではカミンスキー・アタックで攻撃を受けた場合、通常の名前検索で攻撃対象の名前が既にキャッシュされている場合であっても、それを無視する形で偽の情報が上書きされてしまうことから、攻撃対象データの TTL の設定値やキャッシュ情報の有無にかかわらず、外部からの DNS キャッシュポイズニングが成立してしまうことがあります。



カミンスキー・アタックの概要

■DNS キャッシュポイズニングの脅威

DNS キャッシュポイズニングにより偽のデータを記憶させられてしまった場合、その被害はその DNS キャッシュサーバを参照している数多くのクライアントに及びます。また、DNS はほぼ全てのインターネットサービスが使用しているため、DNS キャッシュポイズニングはインターネット全体にかかわる問題です。

特に、今回のカミンスキー・アタックは危険性が非常に高く、インターネット全体にとって大きな脅威であり、早急な対策が必要になります。

次節では、カミンスキー・アタックを含む、DNS キャッシュポイズニングへの対策方法について解説します。

Copyright © 2008 株式会社日本レジストリサービス

■DNS キャッシュポイズニングへの対策方法

1. 問合せ UDP ポートのランダム化…各ベンダからのパッチの適用を

従来の DNS キャッシュサーバの実装では、問合せに使うUDPポート番号は1つに固定されているか、あるいは決められた範囲の限られたポートを使用するものがほとんどでした。これを問合せごとに毎回変える(ランダム化)ように変更することで、総当り攻撃に対する耐性を高めることができます。そのため今回、問合せUDPポート番号をランダム化するための緊急パッチが、各ベンダからリリースされました。

UDP ポート番号をランダム化することにより、DNS キャッシュポイズニングが成功する確率を、ID のみがランダムでポート番号が固定である場合に比べ、大幅に低下させることができます。

あるDNSキャッシュサーバに対し、
DNSキャッシュポイズニングが成立する確率

$$P_S = \frac{R \times W}{N \times Port \times ID}$$

R: 攻撃対象1台あたりに送るパケット量(pps)
W: 攻撃可能な時間(問合せ⇒応答のRTT)
N: 攻撃対象レコードを保持する権威DNSサーバの数
Port: 問合せに使われるUDPポート番号の数
ID: DNSのID (16bit = 65,536)

上記式において、
➢UDPポート番号が固定 ⇔ *Port* = 1
➢UDPポート番号がランダム ⇔ *Port* = 65,536

となるため、UDPポート番号をランダム化することにより、DNSキャッシュポイズニングが成立する確率P_Sを小さくすることができる。

UDP ポート番号ランダム化の効果

カミンスキー・アタックでは UDP ポート番号が固定であった場合、**数秒～数十秒程度の攻撃で DNS キャッシュポイズニングを成立させることができる**、という報告が既に行われています。DNS キャッシュサーバを運用されている方は各ベンダから至急パッチを入手し、適用しましょう。

各ベンダからのパッチに関する情報は、後述の CERT/CC の Web ページにまとめられています。

US-CERT Vulnerability Note VU#800113
<http://www.kb.cert.org/vuls/id/800113>

2. オープンリゾルバは危険…適切なアクセスコントロールやフィルタリングの適用を

インターネット上のどこからの DNS 再帰検索要求でも受け付ける状態になっている DNS キャッシュサーバを「オープンリゾルバ」といいます。オープンリゾルバは DNS Amp 攻撃[3]の踏み台に使われる危険性がある等、本来好ましくない設定ですが、DNS キャッシュポイズニングの攻撃者からみた場合オープンリゾルバには、**攻撃者が任意のタイミングで、任意のドメイン名に対するキャッシュポイズニング攻撃を始めることができる**ため、非常に危険な状態です。

また、DNS サーバでアクセスコントロールが適切に設定されていても、発信元 IP アドレスを偽装した DNS データが外部から到達可能であった場合、そのデータを受け取った DNS キャッシュサーバが反復検索を始めてしまうおそれがあります。

そのため、DNS キャッシュポイズニングを防ぐためには DNS サーバにおける対策だけでは不十分であり、内部ネットワークの IP アドレスを詐称したデータが外部から到達することがないよう、ネットワークにおいてもフィルタリング等の適切な対策をとる必要があります。

3. 権威 DNS サーバは狙われやすい…機能分割と反復検索機能の無効化を

権威 DNS サーバは、それぞれのドメイン名を管理するためのサーバとしてインターネット上に広く公開されます。権威 DNS サーバの IP アドレスは誰でも知ることができるため、権威 DNS サーバがもしオープンリゾルバの状態になっていた場合、非常に危険な状態であるといえます。

本来、権威 DNS サーバと DNS キャッシュサーバは DNS の構成上別の機能であるため、権威 DNS サーバと DNS キャッシュサーバを別のサーバ(あるいは別の IP アドレス)に分割し、権威 DNS サーバでは反復検索機能を無効にしておきましょう。

---

[3] DNS Amp 攻撃の概要と対策については、JPRS トピックス&コラム No.003「DDoS にあなたの DNS が使われる」をご参照ください。

Copyright © 2008 株式会社日本レジストリサービス

■根本的な解決方法は DNSSEC の導入—しかし普及促進が課題

ここまでで解説した方法により、各組織の DNS キャッシュサーバにおける、DNS キャッシュポイズニングに対する危険性を下げることができます。しかし、危険性を根本的になくすことはできません。

DNS キャッシュポイズニングの危険性をなくすためには、**DNSSEC** の導入が必要になります。DNSSEC では電子署名の技術により DNS 応答の正当性が確認できるため、DNS キャッシュポイズニングによる毒入れそのものが極めて困難になります。

しかし、DNSSEC を導入するためには、関連する DNS サーバ(権威 DNS サーバ、DNS キャッシュサーバの双方)を、すべて DNSSEC 対応のものにする必要があります。このため DNSSEC の導入には、その普及をどう進めていくかが大きな課題となっています。

■攻撃の検知と防御—現時点における試み

前述のとおり DNS キャッシュポイズニングを防止するための根本的な対策は DNSSEC の導入です。しかし DNSSEC の普及には今後ある程度の時間を要すると予想されるため、現時点において DNS キャッシュポイズニング攻撃を効率よく検知し、効果的な防御を行うための手法が研究開発・発表されはじめています。

カミンスキー・アタックをはじめとする DNS キャッシュポイズニング攻撃では、通常の運用ではほとんど検出されない、問合せ時の ID や UDP ポート番号と一致しない、不正な DNS 応答が観測されます。これを効率よく検知することで不正な DNS 応答をブロックしたり、必要に応じてより信頼性の高い TCP での再問合せを行ったりする等、さまざまな対策が提案、実装されています。

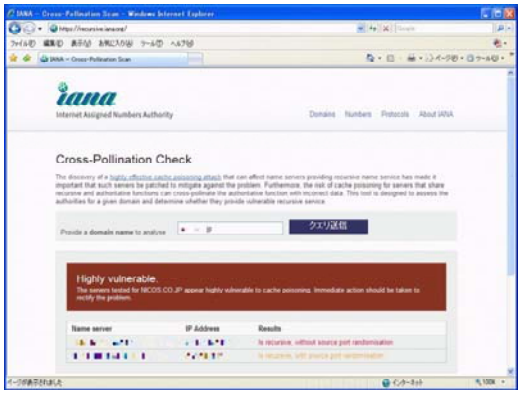
また、根本的な対策である DNSSEC についても、TLD や RIR 等において導入が始まっています。

■自分の DNS サーバをチェックするには

ICANN/IANA では、DNS の管理者が権威 DNS サーバの設定状況をチェックするための Web ページを開設しています。

この Web ページでは、①指定するドメイン名の権威 DNS サーバがオープンリゾルバになっていないか、②もしオープンリゾルバになっている場合、問合せ UDP ポート番号が固定されていないか、の2点をチェックすることができます。

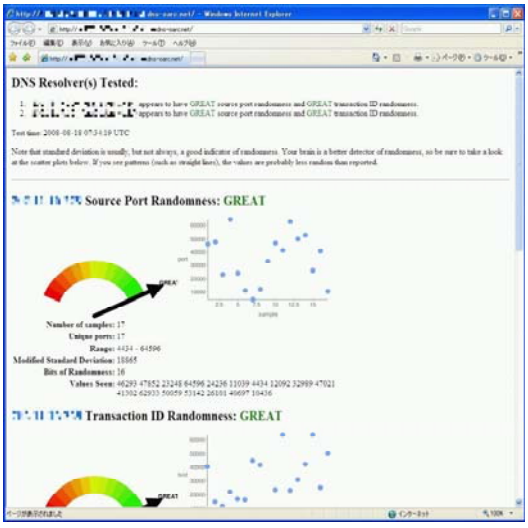
IANA – Cross-Pollination Scan
<https://recursive.iana.org/>



チェック結果の出力例(IANA)

また、DNS に関する調査・分析活動や情報交換の場を提供している DNS-OARC(DNS Operations, Analysis, and Research Center)では、ユーザが現在使っている DNS キャッシュサーバの ID と UDP ポート番号が十分なランダム性を備えているかどうかをチェックできる Web ページを開設しています。

Web-based DNS Randomness Test | DNS-OARC
<https://www.dns-oarc.net/oarc/services/dnsentropy>



チェック結果の出力例(OARC)

Copyright © 2008 株式会社日本レジストリサービス