C11 DNS キャッシュ保持に関する脆弱性"ghost domain"の研究

発表者 1BDRM001 有水智大
指導教員 菊池浩明 教授

Research on "ghost domain" a vulnerability of the DNS cache

Abstract：In 2012, a vulnerability on DNS cache which malicious domain name remains available even after it was removed from the authoritative DNS name servers. In this research, we investigate current main public DNS name servers whether ghost domain name vulnerability is still active or not we clarify the risk of the vulnerability.

1. はじめに

悪意あるホストは,ドメインネーム DNS をフィッシング,ボットネット指揮統制およびマルウェア配布等の様々な悪意のある目的に使用する.これらの不正行為の対策は,上位 DNS サーバから悪意のあるドメインを削除することである.しかし,この対策は不十分である.なぜならば上位 DNS サーバから取り除かれた後も,悪意のあるドメインネームが稼働し続けることを可能にする DNS 実装の脆弱性が Haixin Duan ら[1]によって報告された.彼らは 19,045 のパブリック DNS サーバを用いた実験で,ドメインネームが無効にされた,サーバの 70%以上が,TTL が終了した 1 週間後まだ名前解決することを示した.このキャッシュ DNS サーバ脆弱性を「幽霊ドメイン名」と呼ぶ.

本研究では,現在の主なパブリック DNS サーバに幽霊ドメイン名脆弱性が存在するか次の４つの調査を行う.（１）脆弱性の割合（２）幽霊ドメインの生存期間の調査（３）国毎の脆弱性の割合（４）脆弱性の DNS ソフトウェア毎の調査.これらの調査を基にパブリック DNS が行っている対策や傾向を考察する.

2. 技術的背景

NS レコードは,ドメインとそのドメインの DNS サーバを指定するレコードである.NS レコードは子ゾーンにも存在し,親ゾーンとどちらの NS レコードを優先するかは,NS レコードの信頼度（trustworthiness）によって決まる.DNS のプロトコル仕様を定めた RFC2181[2]では,子ゾーンの NS レコードを親よりも高い信頼度に設定するように規定されている.よって,現在のキャッシュ DNS サーバの実装では,子ゾーンの NS レコードを優先的に使用するものが主流である.

幽霊ドメイン脆弱性は,この信頼度を子ゾーンのものを高く設定する点を利用し,「NS レコードは A」という親の情報よりも「NS レコードは変更して B になった」という子の情報を優先させる.NS レコードが変わったことでキャッシュの置き換えが行われ,TTL 値が更新されてしまう.既にキャッシュされているデータと同じ信頼度を持っているデータを受けとった場合,データを置き換えるかどうかは現在の DNS プロトコルでは定められておらず,実装依存となっている.

3. 実験

3.1 実験概要

以下の４点について明らかにするため,実験を行う.

１．パブリック DNS サーバの脆弱性を持つ割合
２．幽霊ドメインの生存期間
３．国毎の脆弱性の割合
４．DNS ソフトウェア毎の脆弱性を持つ割合

3.2 実験環境

研究室内にある 2 台の DNS サーバを用いて実験を行った.2 台の詳細を表１に示す.

表１ 実験機材詳細

DNS 名	型名	スペック	OS
noisy	Dell PowerEdge 2650	Xeon 2.3GHz 1GB	Linux Redhat 9
drossel	DellPower Edge410	Xeon 2.4GHz 4GB	Cent OS 5.3

3.3 調査対象

調査するパブリック DNS には,public-dns.tk[3]が公開しているパブリック DNS のデータベースを用いた.2,972 個のアドレスから,A レコード問い合わせに対して timeout するものを除いた 2,791 件について調査した.

3.4 実験方法

２台のサーバを用いて１つを権威 DNS サーバ A とし,もう１つの DNS サーバへドメインの委任を行う B とする.調査対象パブリック DNS を C とする.実験の概略を図１に示す.以下の手順で実験を行った.ゾーン TTL 値は 3600 に設定した.

1. C から host1.ghost.cs.dm.u-tokai.ac.jp の A レコードを検索,キャッシュを残す.(図中 1)
2. A の cs ゾーンから ghost ドメインを削除,named を再起動する.（図中 2）
3. 別のパブリック DNS から host1.ghost.cs.dm.u-tokai.ac.jp にアクセスできないことを確認する.
4. C から host1.ghost.cs.dm.u-tokai.ac.jp にアクセスできることを（キャッシュが残っていることを）確認する.
5. B の ghost ゾーンのネームサーバを drossel から drossel2 に変更,named を再起動する.（図中 3）
6. 600s 以内に C から drossel1.ghost.cs.dm.u-tokai.ac.jp NS レコード検索をする.この応答の NS レコードは 2.1 節で述べた通り,1 で受け取った応答と同じ信頼度を持つ.これによりキャッシュを上書きさせ,TTL 値が延長する.（図中 4,5）
7. 600s 過ぎた後に調査対象のパブリック DNS から host1.ghost.cs.dm.u-tokai.ac.jp にアクセスできれば,脆弱性があると判定する.

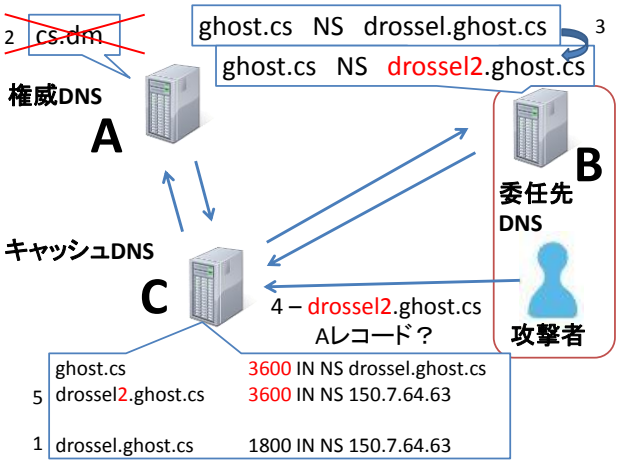

図１　実験概略

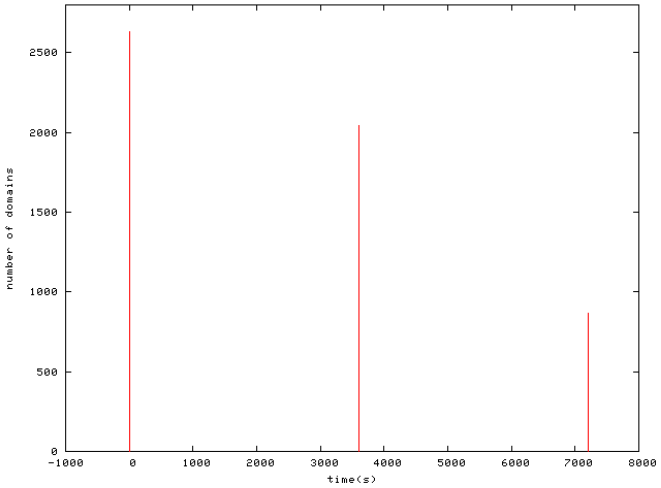

図２ 幽霊ドメインの生存数

3.5 結果

実験１の主要パブリック DNS の脆弱性の結果を表２に示す.Google 以外の主要パブリック DNS においては,脆弱性が確認された.幽霊ドメインの生存数の時間推移を図２に示す.幽霊ドメイン脆弱性を確認できたものが 2,791 件中 2,045 件であった.2 時間後には 869 件まで減少した.実験２の国毎の脆弱性を持つパブリック DNS の割合を表３に示す.ドメインの地理情報は public-dns.tk の情報に基づいている.

3.6 考察

[1]の脆弱性が発見されてから 11 か月程度経過した 2013 年 1 月現在でも脆弱性が残っており,パブリック DNS はその危険性を理解した上で利用することがユーザに求められる.

主要パブリック DNS において脆弱性が確認されたが,幽霊ドメインが生存したのは 1 時間のみであった.

Bind は幽霊ドメイン脆弱性に対してパッチを当てており,アップデートすることで脆弱性に対策することができる.Bind のパッチはキャッシュの更新を行う際に NS 名の更新は行うが TTL の延長は行わず値を保持させるものである.本実験において Google 以外の主要パブリック DNS は最初のキャッシュ更新を許しているため,Bind を用いていないか,パッチを当てずに異なる方法で対策を行っていると考えられる.

幽霊ドメインの生存数が時間経過とともに減少していくのはキャッシュの定期的な削除を行っているためであり,キャッシュを削除する頻度が DNS 毎に異なるため,段階的に減少していくと考えられる.

幽霊ドメイン脆弱性を持つパブリック DNS の割合が一番多い国はイタリアである.割合が上位の国はヨーロッパ圏に多い.

表２ 主要パブリック DNS の脆弱性の有無

	IP アドレス	脆弱性
Google	8.8.8.8	なし
	8.8.4.4	なし
DNS Advantage	156.154.70.1	有
	156.154.71.1	有
OpenDNS	208.67.222.222	有
	208.67.220.220	有
Norton	198.153.192.1	有
	198.153.194.1	有
GTEI DNS	4.2.2.1	有
	4.2.2.2	なし

表３ 脆弱性を持つパブリック DNS の国毎の割合

	DNS 数	脆弱性有	割合
イタリア	74	27	0.365
日本	97	28	0.289
ベルギー	35	9	0.257
ドイツ	285	72	0.253
カナダ	38	9	0.237
中国	67	15	0.224
スウェーデン	509	108	0.212
アメリカ	888	180	0.203
オランダ	72	13	0.181
フランス	102	18	0.176
イギリス	212	33	0.156

4. おわりに

DNS キャッシュ保持に関する脆弱性をついた攻撃に対するパブリック DNS の対応状況を調査した.パブリック DNS の約 3 割に脆弱性が残ることを明らかにした.幽霊ドメイン脆弱性をついた攻撃を検知することを今後の課題とする.

参考文献

[1] Haixin Duan, Jian Jiang, Jinjin Liang,"Ghost Domain Names: Revoked Yet Still Resolvable", NDSS Symposium 2012.
[2] RFC 2181, Clarifications to the DNS Specification, Internet Standard,1997.
[3] Public DNS Server List http://public-dns.tk/